aws

管理指南

Amazon WorkSpaces

Amazon WorkSpaces: 管理指南

Table of Contents

什麼是 Amazon WorkSpaces？

Amazon 使您 WorkSpaces 能夠提供虛擬, 基於雲的 Microsoft 視窗, Amazon Linux, 或 Ubuntu Linux 桌面為您的用戶, 被稱為 WorkSpaces. WorkSpaces 無需採購和部署硬體或安裝複雜軟體。您可以在需求變更時快速新增或移除使用者。使用者可以從多個裝置或 Web 瀏覽器存取其虛擬桌面。

有關更多信息，請參閱 Amazon WorkSpaces。

功能

- 選擇您的作業系統 (Windows、Amazon Linux、Ubuntu Linux)，然後從一系列硬體組態、軟體組態和 AWS 區域中選取。如需詳細資訊，請參閱 Amazon WorkSpaces 套裝軟體和the section called “建立自訂映像和套件”.
- 選擇您的通訊協定：PCoIP 或 WorkSpaces 串流通訊協定 (WSP)。如需詳細資訊，請參閱 Amazon 協議 WorkSpaces。
- Connect 到您的， WorkSpace 然後從您離開的地方接起。 WorkSpaces提供持久的桌面體驗。
- WorkSpaces 提供每月或每小時計費的彈性 WorkSpaces。如需詳細資訊，請參閱WorkSpaces 定價。
- 對於 Windows 桌面，您可以自備授權和應用程式，或從 AWS Marketplace for Desktop Apps 購買。
- 為您的使用者建立獨立的受管目錄，或將您的內部部署目錄連線 WorkSpaces 到內部部署目錄，讓使用者可以使用其現有的認證來取得企業資源的順暢存取權。如需詳細資訊，請參閱 目錄。
- 使用相同的工具來管理您 WorkSpaces 用來管理內部部署桌面的工具。
- 使用多重要素驗證 (MFA) 以提供額外的安全防護。
- 使用 AWS Key Management Service (AWS KMS) 來加密靜態資料、磁碟 I/O 和磁碟區快照。
- 控制允許使用者存取其的 IP 位址 WorkSpaces。

架構

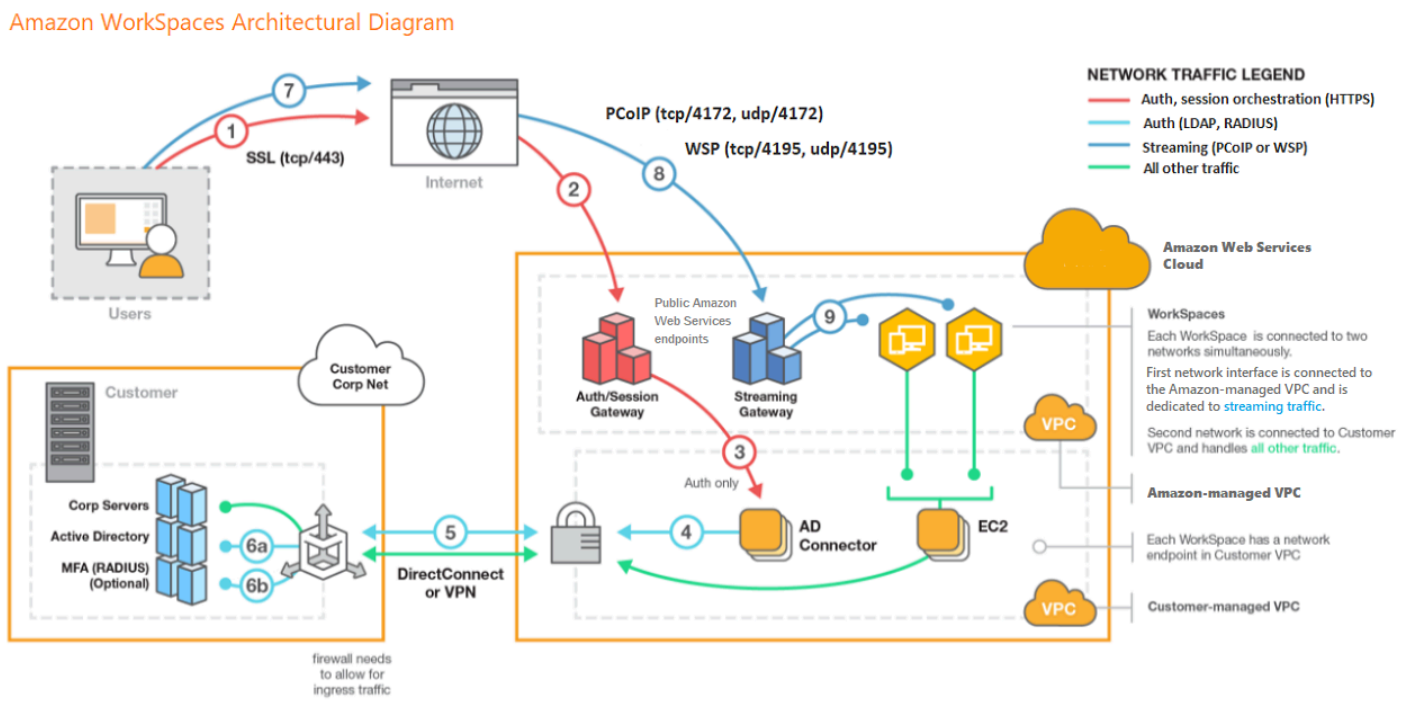
對於 Windows 和 Linux WorkSpaces，每個 WorkSpace 都與虛擬私有雲 (VPC) 以及用於儲存和管理您 WorkSpaces和使用者資訊的目錄相關聯。如需詳細資訊，請參閱 the section called “VPC 要求”。目錄是透過 AWS Directory Service 管理，其提供了下列選項：Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Director (也稱為 AWS Managed Microsoft AD)。如需詳細資訊，請參閱 AWS Directory Service管理員指南。

WorkSpaces 使用您的 Simple AD、AD Connector 或AWS受管理的 Microsoft AD 目錄來驗證使用者。使用者可以從支援的裝置使用用戶端應用程式來存取它們 WorkSpaces，或是 Windows 的網頁瀏覽器，然後使用其目錄認證登入。 WorkSpaces 登入資訊會傳送至驗證閘道，該閘道會將流量轉送至的 WorkSpace目錄。驗證使用者之後，串流流量會透過串流閘道起始。

對於所有驗證和工作階段相關資訊，用戶端應用程式會使用透過連接埠 443 的 HTTPS。用戶端應用程式使用連接埠 4172 (PCoIP) 和連接埠 4195 (WSP) 來進行像素串流，以 WorkSpace 及連接埠 4172 和 4195 進行網路健康狀態檢查。如需詳細資訊，請參閱 用戶端應用程式的連接埠。

每個介面都 WorkSpace 有兩個相關聯的彈性網路介面：用於管理和串流的網路介面 (eth0) 和一個主要網路介面 (eth1)。主要網路介面具有 VPC 所提供的 IP 位址，該 IP 位址來自目錄所使用的相同子網路。這可確保來自您的流量 WorkSpace 可以輕鬆到達目錄。VPC 中資源的存取是由指派給主要網路介面的安全群組控制。如需詳細資訊，請參閱 網路介面。

下圖顯示的架構 WorkSpaces。



存取您的 WorkSpace

您可以在支援的作業系統上使用支援的網頁瀏覽器，使用支援裝置的用戶端應用程式連線到您 WorkSpaces 的。

> **Note**
>
> 您無法使用網頁瀏覽器連線到 Amazon Linux WorkSpaces。

有下列裝置的用戶端應用程式：

- Windows 電腦
- macOS 電腦
- Ubuntu Linux 18.04 電腦
- Chromebook
- iPad
- Android 裝置
- Fire 平板電腦
- 零用戶端裝置 (PCoIP 僅支援 Terdici 零用戶端裝置)。

在視窗、macOS 和 Linux 電腦上，您可以使用以下網頁瀏覽器連接到視窗和 Linux WorkSpaces：

- Chrome 53 和更新版本 (僅限 Windows 和 macOS)
- Firefox 49 和更新版本

如需詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的用WorkSpaces 戶端。

定價

註冊後AWS，您可以使用免費方案優惠免 WorkSpaces費開始使用。 WorkSpaces 如需詳細資訊，請參閱WorkSpaces 定價。

使用時 WorkSpaces，您只需為使用量付費。我們會根據套裝軟體和您啟動的數量向 WorkSpaces 您收費。的定價 WorkSpaces 包括使用簡單 AD 和 AD Connector，但不包括使用AWS受管理的 Microsoft AD。

WorkSpaces 提供每月或每小時計費 WorkSpaces。使用每月計費時，您可以支付固定費用以無限制使用，這對於使用 WorkSpaces 全職工作的用戶來說是最好的。使用小時計費時，您只需支付少量的固定月費 WorkSpace，再加上執行中每小時的低小 WorkSpace 時費率。如需詳細資訊，請參閱WorkSpaces 定價。

如需支援地區的相關資訊，請參閱WorkSpaces 定價。

如何開始

若要建立 WorkSpace，請嘗試下列其中一個自學課程：

- 開始使用 WorkSpaces 快速設定
- 使用 AWS Managed Microsoft AD 啟動 WorkSpace
- 使用 Simple AD 啟動 WorkSpace
- 使用 AD Connector 啟動 WorkSpace
- 使用信任的網域啟動 WorkSpace

您可能還想探索這些資源，以了解有關 Amazon 的更多信息 WorkSpaces：

- 在雲端佈建桌面
- 部署 Amazon 的最佳實踐 WorkSpaces
- Amazon WorkSpaces 資源 — 包括白皮書、部落格文章、網路研討會和 re: Invent 工作階段
- Amazon WorkSpaces 問題

開始使用 WorkSpaces 快速設定

在本教學課程中，您將了解如何使用 WorkSpaces 和 AWS Directory Service，佈建虛擬雲端式 Microsoft Windows、Amazon Linux 或 Ubuntu Linux 桌面 (也稱為 WorkSpace)。

本教學課程使用快速設定選項來啟動 WorkSpace。只有在您從未啟動 WorkSpace 時，才可使用此選項。或者，請參閱 使用 WorkSpaces 啟動虛擬桌面。

> **Note**
>
> 下列 AWS 區域支援快速設定：
>
> - 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 (新加坡)
> - 亞太區域 (雪梨)
> - 亞太區域 (東京)
>
> 若要變更您的區域，請參閱選擇區域。

任務

開始之前

開始之前，請確定符合下列要求：

- 您必須有 AWS 帳戶才能建立或管理 WorkSpace。使用者不需要 AWS 帳戶即可連線到其 WorkSpaces 並加以使用。
- 並非每個區域都可以使用 WorkSpaces。確認支援的區域，然後為您的 WorkSpaces 選取一個區域。如需支援區域的詳細資訊，請參閱各個 AWS 區域的 WorkSpaces 定價。

繼續之前，檢閱和瞭解以下內容也很有幫助：

- 當您啟動 WorkSpace 時，您必須選取 WorkSpace 套件。如需詳細資訊，請參閱 Amazon WorkSpaces 套件和 Amazon WorkSpaces 定價。
- 當您啟動 WorkSpace 時，您必須選取要搭配套件使用的通訊協定 (PCoIP 或 WorkSpaces 串流協定 [WSP])。如需詳細資訊，請參閱 Amazon 協議 WorkSpaces。
- 啟動 WorkSpace 時，您必須指定使用者的設定檔資訊，包括使用者名稱和電子郵件地址。使用者藉由指定密碼來完成其設定檔。有關 WorkSpaces 和使用者的資訊儲存在目錄中。如需詳細資訊，請參閱 目錄。

快速設定的用途

快速設定可代表您完成以下任務：

- 建立 IAM 角色，以允許 WorkSpaces 服務建立彈性網路介面並列出您的 WorkSpaces 目錄。此角色具有名稱 `workspaces_DefaultRole`。
- 建立虛擬私有雲端 (VPC)。如果您要改用現有的 VPC，請確定其符合 設定虛 VPC WorkSpaces 中所述的要求，然後遵循 使用 WorkSpaces 啟動虛擬桌面 中所列的其中一個教學課程中的步驟。選擇您要使用的 Active Directory 類型對應的教學課程。
- 在 VPC 中設定 Simple AD 目錄，並為 Amazon WorkDocs 啟用該目錄。這個 Simple AD 目錄用於儲存使用者和 WorkSpace 資訊。經由快速設定建立的第一個 AWS 帳戶 是您的管理員 AWS 帳戶。† 此目錄還具有管理員帳戶。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。
- 建立指定的 AWS 帳戶 並將其新增至目錄。
- 建立 WorkSpaces。每個 WorkSpace 都會收到公用 IP 位址，以提供網際網路存取。執行模式為 AlwaysOn。如需詳細資訊，請參閱 管理 WorkSpace 執行模式。
- 傳送邀請電子郵件給指定的使用者。如果您的使用者沒有收到邀請電子郵件，請參閱 傳送邀請電子郵件。

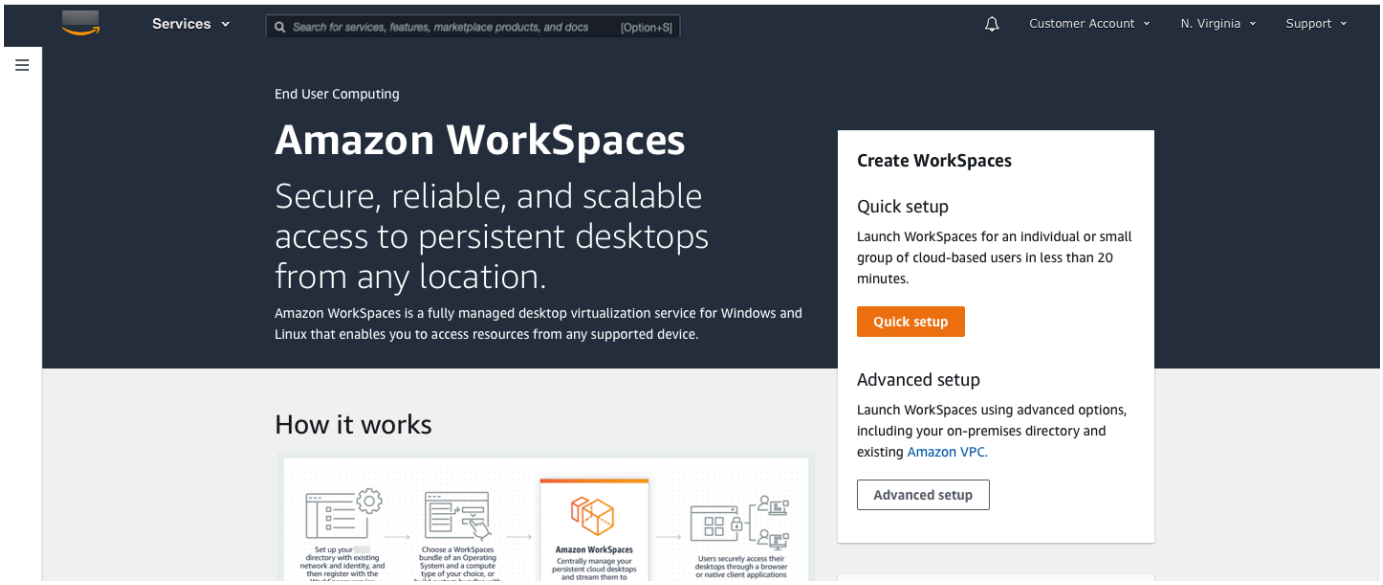
經由快速設定建立的第一個 AWS 帳戶是您的管理 AWS 帳戶。您無法從 WorkSpaces 主控台更新此 AWS 帳戶。請勿與任何人共用此帳戶的資訊。若要邀請其他使用者使用 WorkSpaces，請為他們建立新的 AWS 帳戶。

步驟 1：啟動 WorkSpace

您可以使用快速設定，在幾分鐘內啟動您的第一個 WorkSpace。

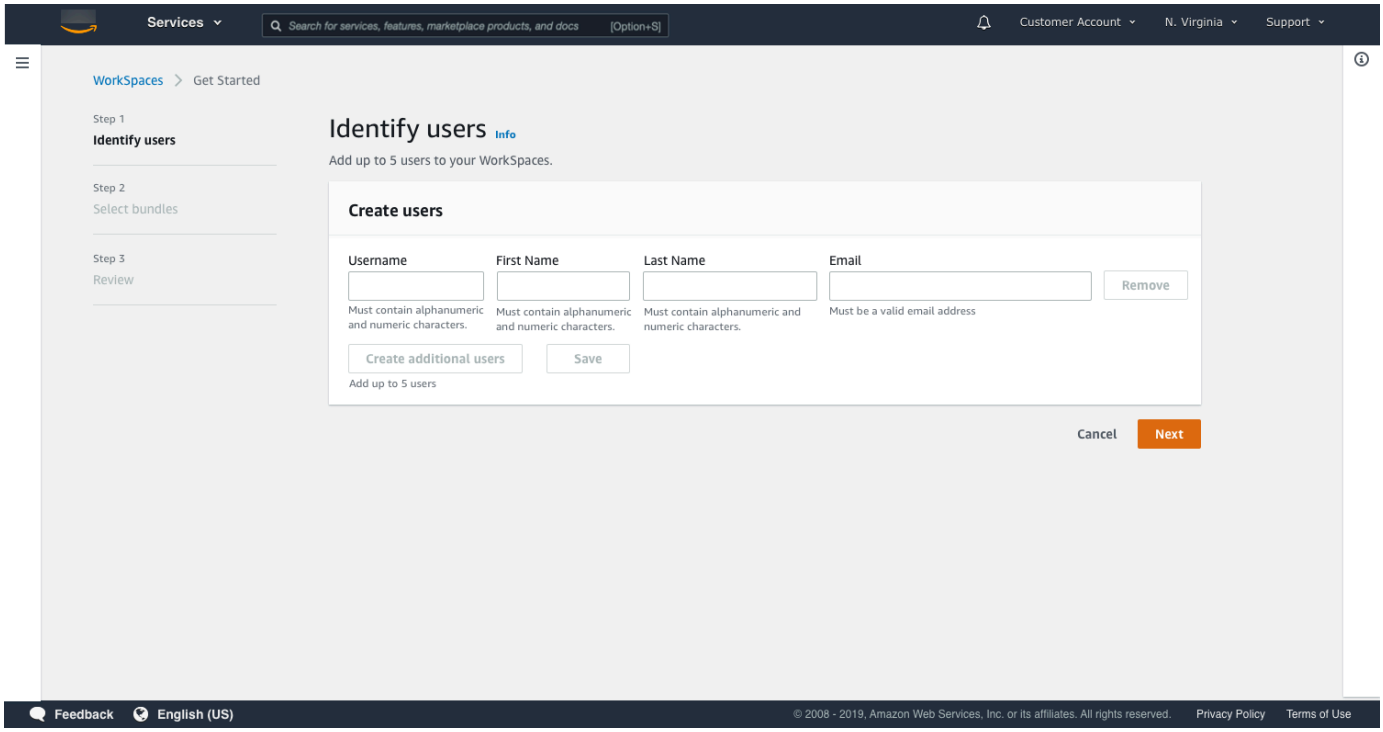
啟動 WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 選擇 Quick setup (快速設定)。如果沒看到此按鈕，表示您已在此區域中啟動 WorkSpace，或者您並未使用其中一個支援快速設定的區域。在這種情況下，請參閱 使用 WorkSpaces 啟動虛擬桌面。

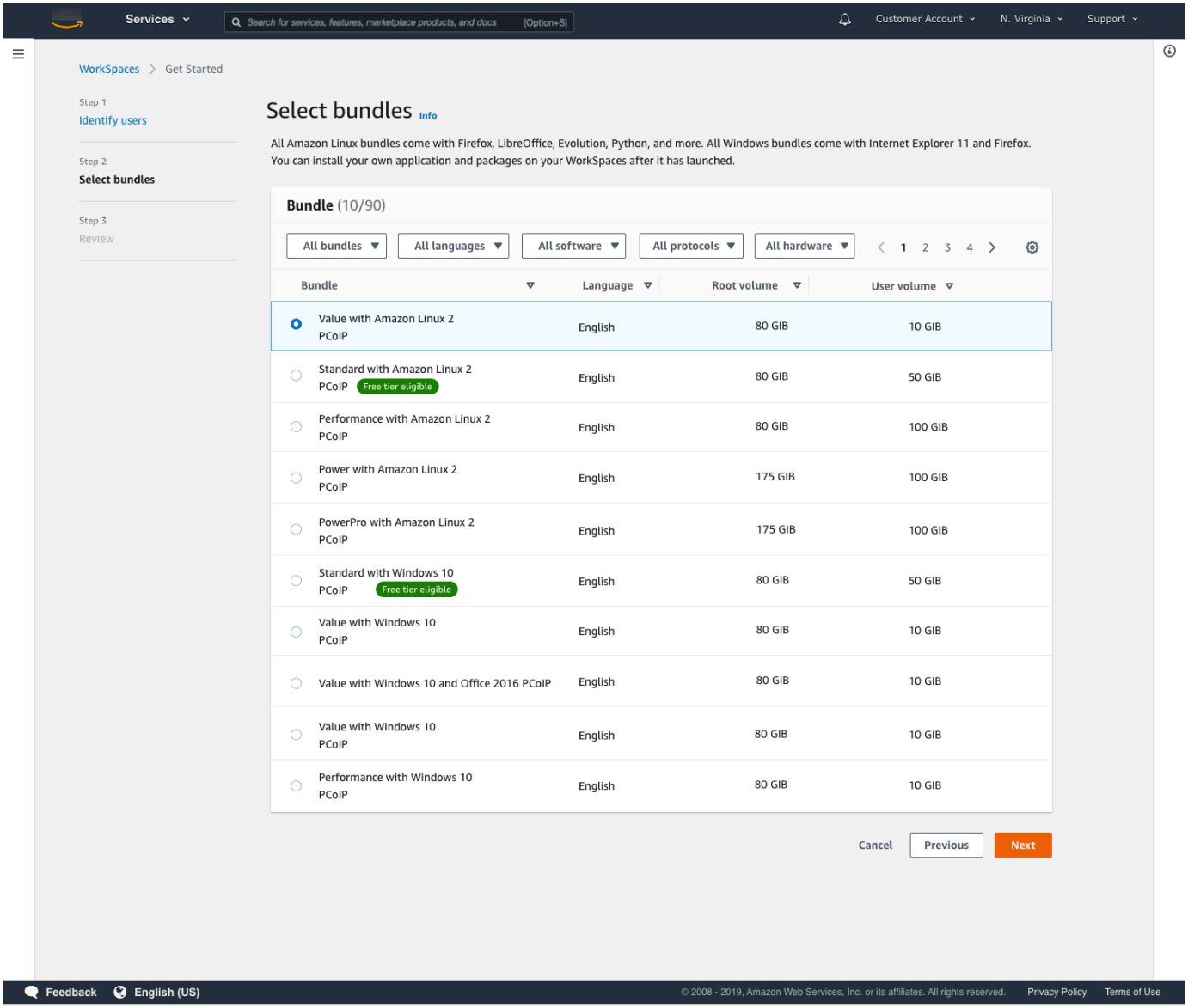


3. 針對識別使用者，輸入使用者名稱、名字、姓氏和電子郵件。然後選擇 Next (下一步)。

> **Note**
>
> 如果這是您第一次使用 WorkSpaces，我們建議您為自己建立使用者以進行測試。



4. 針對套件，請為具有適當通訊協定 (PCoIP 或 WSP) 的使用者選取套件 (硬體和軟體)。如需有關可用於 Amazon WorkSpaces 之各種公用套件的詳細資訊，請參閱 Amazon WorkSpaces 套件。



5. 檢閱您的資訊。然後選擇建立 WorkSpace。
6. 您的 WorkSpace 大約需要 20 分鐘的時間才能啟動。若要監控進度，請移至左側導覽窗格，然後選擇目錄。您將看到正在建立的目錄，其初始狀態為 REQUESTED，然後是 CREATING。

   建立目錄且狀態為 ACTIVE 之後，您可以在左側導覽窗格中選擇 WorkSpaces 來監控 WorkSpace 啟動程序的進度。WorkSpace 的初始狀態為 PENDING。啟動完成時，狀態為 AVAILABLE，而邀請會傳送至您為每個使用者指定的電子郵件地址。如果您的使用者沒有收到邀請電子郵件，請參閱傳送邀請電子郵件。

步驟 2：連線至 WorkSpace

收到邀請電子郵件後，您可以使用您選擇的用戶端來連線至 WorkSpace。登入後，用戶端會顯示 WorkSpace 桌面。

連線至 WorkSpace

1. 如果您尚未設定使用者的憑證，請開啟邀請電子郵件中的連結，並依照指示操作。請記住您指定的密碼，因為您需要密碼才能連線至 WorkSpace。

   > **Note**
   >
   > 密碼區分大小寫，長度須介於 8 至 64 個字元 (含) 之間。密碼必須至少包含下列每個類別中的一個字元：小寫字母 (a-z)、大寫字母 (A-Z)、數字 (0-9) 和組合 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 如需有關每個用戶端需求的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端，然後執行下列其中一項操作：

   - 出現提示時，請下載其中一個用戶端應用程式或啟動 Web Access。
   - 如果系統未提示您而且您尚未安裝用戶端應用程式，請開啟 https://clients.amazonworkspaces.com/ 並下載其中一個用戶端應用程式或啟動 Web Access。

   > **Note**
   >
   > 您無法使用 Web 瀏覽器 (Web Access) 來連線到 Amazon Linux WorkSpaces。

3. 啟動用戶端，輸入邀請電子郵件中的註冊碼，然後選擇註冊。
4. 當系統提示您登入時，請輸入登入憑證，然後選擇登入。
5. (選用) 當系統提示您儲存憑證時，請選擇是。

如需有關使用用戶端應用程式 (例如設定多個監視器或使用周邊裝置) 的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端和周邊裝置支援。

步驟 3：清除 (選用)

如果您已完成針對本教學課程建立的 WorkSpace，則可予以刪除。如需詳細資訊，請參閱 the section called “刪除 WorkSpace”。

> **Note**
>
> 您可以免費使用 Simple AD，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 Simple AD 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

後續步驟

您可以繼續自訂您剛建立的 WorkSpace。例如，您可以安裝軟體，然後從 WorkSpace 建立自訂套件。您也可以針對 WorkSpaces 和 WorkSpaces 目錄執行各種管理任務。如需詳細資訊，請參閱下列文件。

- 建立自訂 WorkSpaces 映像檔和套裝軟體
- 管理您的 WorkSpaces
- 管理 WorkSpaces 的目錄

若要建立額外 WorkSpaces，請執行下列其中一項操作：

- 如果您想要繼續使用由快速設定建立的 VPC 和 Simple AD 目錄，您可以依照「使用 Simple AD 啟動 WorkSpace」教學課程的 步驟 2：建立 WorkSpace 一節中的步驟，為其他使用者新增 WorkSpaces。
- 如果您需要使用其他目錄類型，或者您需要使用現有 Active Directory，請參閱 使用 WorkSpaces 啟動虛擬桌面 中適當的教學課程。

如需有關使用 WorkSpaces 用戶端應用程式 (例如設定多個監視器或使用周邊裝置) 的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端和周邊裝置支援。

開始使用 WorkSpaces 進階設定

在本教學課程中，您將了解如何使用 WorkSpaces 和 AWS Directory Service，佈建虛擬雲端式 Microsoft Windows 或 Amazon Linux 桌面 (也稱為 WorkSpace)。

本教學課程使用進階設定選項來啟動 WorkSpace。

> **Note**
>
> WorkSpaces 的所有區域都支援進階設定。

任務

- 開始之前
- 使用進階設定來啟動您的 WorkSpace

開始之前

開始之前，請先確定您具備可用來建立或管理 WorkSpace 的 AWS 帳戶。使用者不需要 AWS 帳戶即可連線到其 WorkSpaces 並加以使用。

繼續之前，請先檢閱並瞭解下列概念：

- 當您啟動 WorkSpace 時，您必須選取 WorkSpace 套件。如需詳細資訊，請參閱 Amazon WorkSpaces 套件。
- 當您啟動 WorkSpace 時，您必須選取要搭配套件使用的通訊協定 (PCoIP 或 WorkSpaces 串流協定 [WSP])。如需更多詳細資訊，請參閱 Amazon 協議 WorkSpaces。
- 啟動 WorkSpace 時，您必須指定使用者的設定檔資訊，包括使用者名稱和電子郵件地址。使用者藉由指定密碼來完成其設定檔。有關 WorkSpaces 和使用者的資訊儲存在目錄中。如需更多詳細資訊，請參閱 目錄。

使用進階設定來啟動您的 WorkSpace

若要使用進階設定來啟動您的 WorkSpace：

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。

2. 選擇下列其中一個目錄類型，然後選擇下一步。

   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector

3. 輸入目錄資訊。
4. 從兩個不同的可用區域中選擇 VPC 中的兩個子網路。如需詳細資訊，請參閱具有公用子網路的 VPC。
5. 檢閱目錄的資訊，然後選擇建立目錄。

WorkSpaces 的聯網和存取

身為 WorkSpace 管理員，您必須瞭解下列有關 WorkSpaces 聯網與存取的內容。

目錄

Amazon 協議 WorkSpaces

Amazon WorkSpaces 支持兩種協議：PCoIP 和 WorkSpaces 流協議（WSP）。您選擇的通訊協定取決於數個因素，例如使用者將 WorkSpaces 從哪種裝置存取裝置類型、您的作業系統上 WorkSpaces、使用者將面臨的網路狀況，以及您的使用者是否需要雙向視訊支援。

要求

WSP WorkSpaces 僅支援下列最低需求。

主機代理程式需求：

- Windows 主機代理程式 2.0.0.312 版或更高版本
- Ubuntu 主機代理程式 2.1.0.501 版或更高版本
- Amazon Linux 2 主機代理程式 2.0.0.596 版或更高版本

用戶端需求：

- Windows 原生用戶端 5.1.0.329 版或更高版本
- macOS 原生用戶端 5.5.0 版或更高版本
- Web 存取

如需如何檢查 WorkSpace 用戶端版本和主機代理程式版本的詳細資訊，請參閱常見問題集。

WSP 使用時機

- 如果您需要更高的損失/延遲容忍度來支援最終使用者的網路狀況。例如，您的用戶正在 WorkSpaces 跨全球距離訪問他們或使用不可靠的網絡。
- 如果您需要使用者使用智慧卡進行驗證，或在工作階段中使用智慧卡。
- 如果您在工作階段中需要網路攝影機支援功能。
- 如果您需要搭配 Windows 伺服器 2019 版 WorkSpaces 套件使用網頁存取。
- 如果你需要使用 Ubuntu 的 WorkSpaces。
- 如果您需要使用視窗 11 自攜 WorkSpaces.
- 如果您需要使用基於 GPU 的軟件包（圖形 .g4dn 和 .g4dn）。 GraphicsPro
- 如果您需要您的用戶使用 YubiKey 或 Windows Hello 等 WebAuthn 身份驗證器在會話中進行身份驗證。

PCoIP 使用時機

- 如果您想使用 iPad 或 Android Linux 用戶端。
- 如果您使用 Teradici 零客戶端裝置。
- 如果您需要使用基於 GPU 的服務包（圖形 .g4dn，.g4dn， GraphicsPro圖形或）。 GraphicsPro
- 如果您需要將 Linux 套件用於非智慧卡使用案例。
- 如果您需要 WorkSpaces 在中國 (寧夏) 區域使用。

Note

- 一個目錄中可以混合使用 PCoIP 和 WSP WorkSpaces 。
- 只要使用者位於 WorkSpaces 不同的目錄中，就可以 WorkSpace 同時擁有 PCoIP 和 WSP。相同的使用者不能在相同的目錄 WorkSpace 中擁有 PCoIP 和 WSP。如需為使用者建立多個項目 WorkSpaces 的更多資訊，請參閱為使用者建立多個 WorkSpaces。
- 您可以使用移轉功能在兩個通訊協定 WorkSpace 之間 WorkSpaces 移轉，此功能需要重建 WorkSpace. 如需詳細資訊，請參閱 遷移 WorkSpace。
- 如果您 WorkSpace 是使用 PCoIP 套裝軟體建立的，您可以修改串流通訊協定以在兩個通訊協定之間進行移轉，而不需要重建，同時保留根磁碟區。如需詳細資訊，請參閱修改通訊協定。
- 為了獲得最佳的視訊會議體驗，我們建議您僅使用 Power 或 PowerPro 套裝軟體。

設定虛 VPC WorkSpaces

WorkSpaces WorkSpaces 在虛擬私有雲（ VPC ）中啟動您的。

您可以為您的 WorkSpaces 和公用子網路中的 NAT 閘道建立具有兩個私有子網路的 VPC。或者，您可以為您建立具有兩個公用子網路的 VPC， WorkSpaces 並將公用 IP 位址或彈性 IP 位址與每個子網路建立關聯。 WorkSpace

如需 VPC 設計考量的詳細資訊，請參閱 Amazon WorkSpaces 部署中 VPC 和網路的最佳實務和部署的最佳實務 WorkSpaces -V PC 設計。

目錄

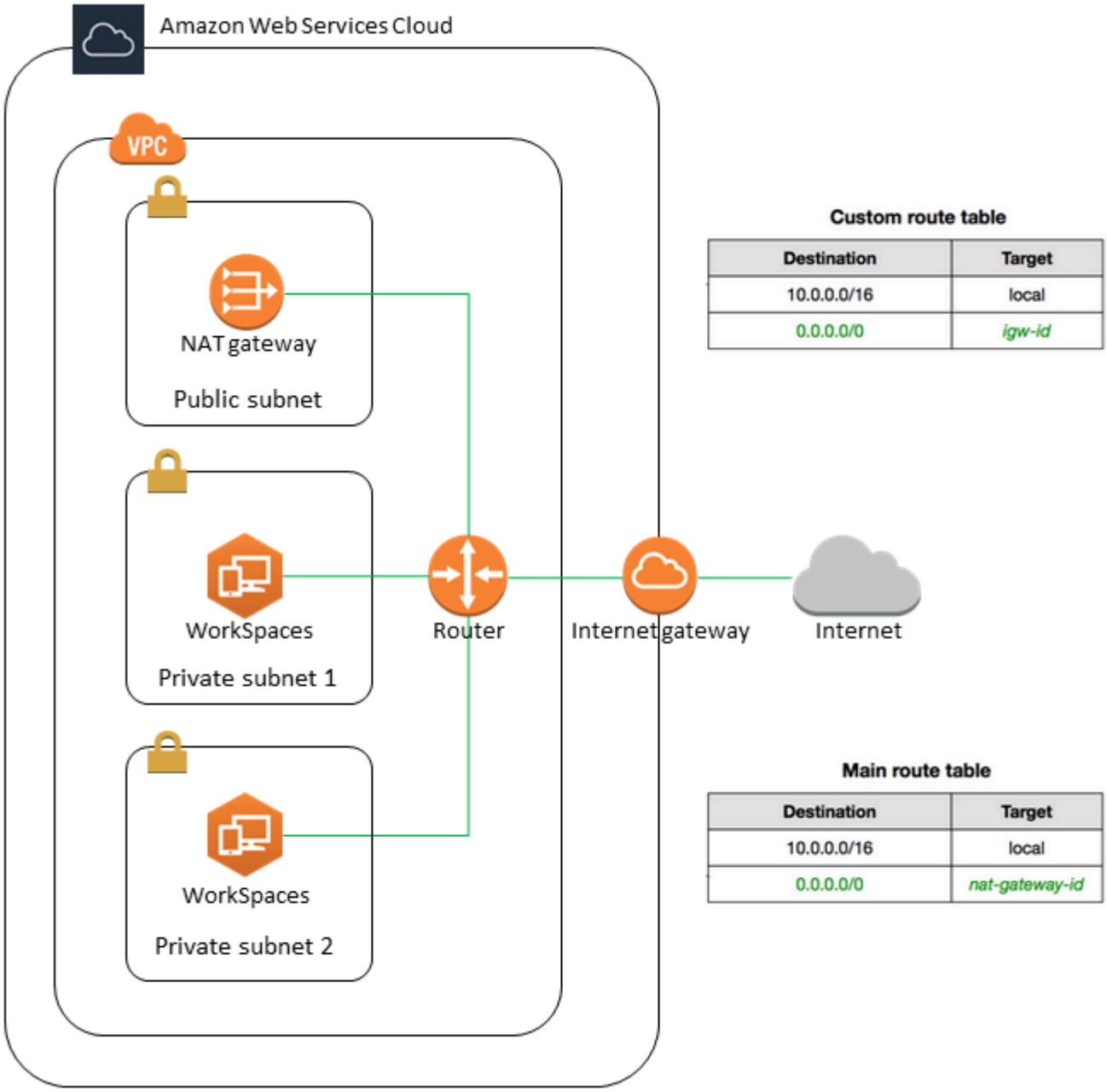
要求

您的 VPC 子網路必須位於您要啟動之區域中的不同可用區域。 WorkSpaces可用區域是代表不同的位置，旨在隔離其他可用區域的故障。藉由在個別的可用區域中啟動執行個體，您就可以保護應用程式免於發生單點故障。各個子網必須完全位於某一可用區域內，不得跨越多個區域。

> **Note**
>
> Amazon WorkSpaces 在每個支援的區域中提供可用區域的子集。若要判斷哪些可用區域可用於您正在使用的 VPC 的子網路 WorkSpaces，請參閱。Amazon 的可用區域 WorkSpaces

建立具有私有子網路與 NAT 閘道的 VPC

如果您使 AWS Directory Service 用建立 AWS 受管理的 Microsoft 或 Simple AD，建議您使用一個公用子網路和兩個私有子網路來設定 VPC。設定您的目錄以在私有子網路 WorkSpaces 中啟動您的。若要在私人子網路 WorkSpaces 中提供網際網路存取，請在公用子網路中設定 NAT 閘道。



若要建立具有一個公用子網路和兩個私有子網路的 VPC

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選擇建立 VPC。
3. 在要建立的資源之下，選擇 VPC 等。
4. 針對自動產生名稱標籤，輸入 VPC 的名稱。

5. 若要設定子網路，請執行下列動作：

   a. 針對可用區域數量，根據您的需求選擇 1 或 2。

   b. 展開自訂 AZ，然後選擇您的可用區域。否則，請為您 AWS 選擇它們。若要進行適當的選取，請參閱 Amazon 的可用區域 WorkSpaces。

   c. 針對 Number of public subnets (公用子網路數量)，請確定每個可用區域有一個公用子網路。

   d. 針對私有子網路數量，確定每個可用區域至少有一個私有子網路。

   e. 為每個子網路輸入 CIDR 區塊。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的子網路規模調整。

6. 針對 NAT 閘道，選擇每個可用區域 1 個。

7. 選擇建立 VPC。

IPv6 CIDR 區塊

您可以建立 IPv6 CIDR 區塊與您的 VPC 和子網路的關聯。不過，如果您將子網路設定為自動指派 IPv6 位址給子網路中啟動的執行個體，則無法使用 Graphics 套件。（但是，您可以使用圖形 .g4dn，GraphicsPro.g4dn 和捆綁包。）GraphicsPro 這項限制是由於不支援 IPv6 的前一代執行個體類型的硬體限制而產生。

若要解決此問題，您可以在啟動 Graphics 服務包之前，暫時停用 WorkSpaces 子網路上的自動指派 IPv6 位址設定，然後在啟動圖形服務包之後重新啟用此設定 (如果需要)，以便任何其他套裝軟體都能接收所需的 IP 位址。

根據預設，自動指派 IPv6 位址設定會停用。若要從 Amazon VPC 主控台檢查此設定，請在導覽窗格中選擇子網路。選取子網路，然後依序選擇動作、修改自動指派 IP 設定。

設定具有公用子網路的 VPC

如果您想要的話，可以建立具有兩個公用子網路的 VPC。若要 WorkSpaces 在公用子網路中提供網際網路存取，請將目錄設定為自動指派彈性 IP 位址，或手動為每個 WorkSpace子網路指派彈性 IP 位址。

任務

- 步驟 1：建立 VPC
- 步驟 2：將公共 IP 地址分配給您的 WorkSpaces

步驟 1：建立 VPC

如下所示，建立具有一個公用子網路的 VPC。

若要建立 VPC

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選擇建立 VPC。
3. 在要建立的資源之下，選擇 VPC 等。
4. 針對自動產生名稱標籤，輸入 VPC 的名稱。
5. 若要設定子網路，請執行下列動作：
   a. 針對可用區域數量，選擇 2。
   b. 展開自訂 AZ，然後選擇您的可用區域。否則，請為您 AWS 選擇它們。若要進行適當的選取，請參閱 Amazon 的可用區域 WorkSpaces。
   c. 針對公用子網路數量，選擇 2。
   d. 對於 Number of private subnet (私有子網的數量)，選擇 0。
   e. 輸入每個公用子網路的 CIDR 區塊。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的子網路規模調整。
6. 選擇建立 VPC。

IPv6 CIDR 區塊

您可以建立 IPv6 CIDR 區塊與您的 VPC 和子網路的關聯。不過，如果您將子網路設定為自動指派 IPv6 位址給子網路中啟動的執行個體，則無法使用 Graphics 套件。（但是，您可以使用 GraphicsPro 捆綁。）這項限制是由於不支援 IPv6 的前一代執行個體類型的硬體限制而產生。

若要解決此問題，您可以在啟動 Graphics 服務包之前，暫時停用 WorkSpaces 子網路上的自動指派 IPv6 位址設定，然後在啟動圖形服務包之後重新啟用此設定 (如果需要)，以便任何其他套裝軟體都能接收所需的 IP 位址。

根據預設，自動指派 IPv6 位址設定會停用。若要從 Amazon VPC 主控台檢查此設定，請在導覽窗格中選擇子網路。選取子網路，然後依序選擇動作、修改自動指派 IP 設定。

步驟 2：將公共 IP 地址分配給您的 WorkSpaces

您可以 WorkSpaces 自動或手動將公共 IP 地址分配給您。若要使用自動指派，請參閱 the section called “設定自動公用 IP 位址”。若要手動指派公用 IP 地址，請使用下列程序。

若要 WorkSpace 手動將公用 IP 位址指派給

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇 WorkSpaces。
3. 展開的列 (選擇箭頭圖示)， WorkSpace 並記下 WorkSpace IP 的值。這是的主要私人 IP 位址 WorkSpace。
4. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
5. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。如果您沒有可用的彈性 IP 地址，請選擇配置彈性 IP 地址，然後選擇 Amazon 的 IPv4 地址集區或客戶擁有的 IPv4 地址集區，然後選擇配置。記下新的 IP 地址。
6. 在導覽窗格中，選擇 Network Interfaces (網路介面)。
7. 選取您的網路介面 WorkSpace。若要尋找您的網路介面 WorkSpace，請在搜尋方塊中輸入 WorkSpace IP 值 (您先前所述)，然後按 Enter。WorkSpace IP 值與網路介面的主要私人 IPv4 位址相符。請注意，網路介面的虛擬私人雲端識別碼與 WorkSpaces VPC 的識別碼相符。
8. 選擇 Actions (動作)、Manage IP Addresses (管理 IP 地址)。選擇指派新的 IP，然後選擇是，更新。記下新的 IP 地址。
9. 選擇動作 > 建立與地址的關聯。
10. 在關聯彈性 IP 地址頁面上，從位址中選擇彈性 IP 地址。針對與私有 IP 地址建立關聯，請指定新的私有 IP 地址，然後選擇關聯位址。

Amazon 的可用區域 WorkSpaces

當您建立虛擬私有雲 (VPC) 以搭配 Amazon 使用時 WorkSpaces，VPC 的子網路必須位於您要啟動的區域中的不同可用區域。 WorkSpaces可用區域是代表不同的位置，旨在隔離其他可用區域的故障。藉由在個別的可用區域中啟動執行個體，您就可以保護應用程式免於發生單點故障。各個子網必須完全位於某一可用區域內，不得跨越多個區域。

可用區域以區域代碼加上字母識別符表示；例如 `us-east-1a`。為了確保資源分散到某個區域的可用區域，我們會將可用區域獨立對應至每個 AWS 帳戶的名稱。例如，您 AWS 帳戶的可`us-east-1a`用區域可能與其他 AWS 帳戶`us-east-1a`的位置不同。

為協調各帳戶的可用區域，您必須使用 AZ ID，這是可用區域唯一且一致的識別符。例如，`use1-az2`是`us-east-1`區域的 AZ ID，每個 AWS 帳戶都有相同的位置。

檢視 AZ ID 能讓您判斷某個帳戶資源在另一個帳戶中的相對位置。例如，如果您與另一個帳戶共享 AZ ID 為 use1-az2 的可用區域子網路，則 AZ ID 也是 use1-az2 之可用區域中的該帳戶就可以使用此子網路。Amazon VPC 主控台會顯示各 VPC 和子網路的 AZ ID。

Amazon WorkSpaces 僅適用於每個支援區域的可用區域子集。下表列出您可用於每個區域的 AZ ID。若要查看帳戶中 AZ ID 與可用區域的對應，請參閱《AWS RAM 使用者指南》中的資源適用的 AZ ID。

區域名稱	區域代碼	支援的 AZ ID
美國東部 (維吉尼亞北部)	us-east-1	use1-az2, use1-az4, use1-az6
美國西部 (奧勒岡)	us-west-2	usw2-az1, usw2-az2, usw2-az3
亞太區域 (孟買)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
亞太區域 (首爾)	ap-northeast-2	apne2-az1 , apne2-az3
亞太區域 (新加坡)	ap-southeast-1	apse1-az1 , apse1-az2
亞太區域 (雪梨)	ap-southeast-2	apse2-az1 , apse2-az3
亞太區域 (東京)	ap-northeast-1	apne1-az1 , apne1-az4
加拿大 (中部)	ca-central-1	cac1-az1, cac1-az2
歐洲 (法蘭克福)	eu-central-1	euc1-az2, euc1-az3
歐洲 (愛爾蘭)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
歐洲 (倫敦)	eu-west-2	euw2-az2, euw2-az3
南美洲 (聖保羅)	sa-east-1	sae1-az1, sae1-az3
非洲 (開普敦)	af-south-1	afs1-az1, afs1-az2, afs1-az3

區域名稱	區域代碼	支援的 AZ ID
以色列 (特拉維夫)	`il-central-1`	`ilc1-az1`, `ilc1-az2`, `ilc1-az3`
AWS GovCloud (美國西部)	`us-gov-west-1`	`usgw1-az1` , `usgw1-az2` , `usgw1-az3`
AWS GovCloud (美國東部)	`us-gov-east-1`	`usge1-az1` , `usge1-az2` , `usge1-az3`

如需有關可用區域和 AZ ID 的詳細資訊，請參閱 Amazon EC2 使用者指南中的區域、可用區域和 Local Zones。

的 IP 位址和連接埠需求 WorkSpaces

若要連線到您的 WorkSpaces，用 WorkSpaces 戶端所連線的網路必須有特定連接埠開啟到各種AWS 服務的 IP 位址範圍 (以子集分組)。這些位址範圍因 AWS 區域而異。這些相同的連接埠也必須在用戶端上執行的任何防火牆上開啟。如需不同區域的 AWS IP 位址範圍詳細資訊，請參閱《Amazon Web Services 一般參考》中的 AWS IP 位址範圍。

如需架構圖，請參閱WorkSpaces 架構。如需其他架構圖，請參閱部署 Amazon 的最佳實務 WorkSpaces。

用戶端應用程式的連接埠

用 WorkSpaces 戶端應用程式需要下列連接埠的輸出存取：

連接埠 53 (UDP)

此連接埠用於存取 DNS 伺服器。其必須開放給您的 DNS 伺服器 IP 位址，以便用戶端解析公用網域名稱。如果您未使用 DNS 伺服器進行網域名稱解析，則此連接埠需求為選用。

連接埠 443 (TCP)

此通訊埠用於用戶端應用程式更新、註冊和驗證。桌面用戶端應用程式支援使用代理伺服器處理連接埠 443 (HTTPS) 流量。若要啟用 Proxy 伺服器的使用，請開啟用戶端應用程式，選擇進階設定，選取使用 Proxy 伺服器，指定 Proxy 伺服器的位址和連接埠，然後選擇儲存。

此連接埠必須開放給下列 IP 位址範圍：

- GLOBAL 區域中的 AMAZON 子集。
- 所在「區域」中 WorkSpace 的AMAZON子集。
- us-east-1 區域中的 AMAZON 子集。
- us-west-2 區域中的 AMAZON 子集。
- us-west-2 區域中的 S3 子集。

連接埠 4172 (UDP 和 TCP)

此連接埠用於串流 WorkSpace 桌面和 PCoIP WorkSpaces 的健康狀態檢查。此連接埠必須開放給 PCoIP 閘道以及所在區域中的健全狀況檢查伺服器。 WorkSpace 如需詳細資訊，請參閱 運作狀態檢查伺服器 及 PCoIP 閘道伺服器。

對於 PCoIP WorkSpaces，桌面用戶端應用程式不支援使用 Proxy 伺服器，也不支援在 UDP 中使用 TLS 解密和檢查連接埠 4172 流量 (針對桌面流量)。它們需要直接連線至連接埠 4172。

連接埠 4195 (UDP 和 TCP)

此連接埠用於串流 WorkSpace 桌面和串 WorkSpaces 流通訊協定 (WSP) WorkSpaces 的健全狀況檢查。此連接埠必須開啟，才能使用 WSP 閘道 IP 位址範圍和所在區域中的健全狀況檢查伺服器。WorkSpace 如需詳細資訊，請參閱 運作狀態檢查伺服器 及 WSP 閘道伺服器。

對於 WSP WorkSpaces， WorkSpaces Windows 用戶端應用程式（5.1 及以上版本）和 macOS 用戶端應用程式（5.4 版及以上版本）支援使用 HTTP 代理伺服器進行連接埠 4195 TCP 流量，但不建議使用代理伺服器。不支援 TLS 解密和檢查。如需詳細資訊，請參閱針對視窗 WorkSpaces、Amazon Linux WorkSpaces 和 Ubuntu 的網際網路存取設定進行裝置代理伺服器設定 WorkSpaces。

> **Note**
>
> - 如果您的防火牆使用具狀態篩選，則會自動開放暫時連接埠 (也稱為動態連接埠) 以允許回傳通訊。如果您的防火牆使用無狀態篩選，您必須明確開放暫時連接埠，以允許傳回通訊。您必須開放的必要暫時連接埠範圍會根據您的組態而有所不同。
> - UDP 流量不支援 Proxy 伺服器功能。如果您選擇使用代理伺服器，用戶端應用程式對 Amazon WorkSpaces 服務進行的 API 呼叫也會被代理。API 呼叫和桌面流量都應該通過相同的 Proxy 伺服器。

適用於 Web Access 的連接埠

WorkSpaces Web 存取需要下列連接埠的輸出存取：

連接埠 53 (UDP)

此連接埠用於存取 DNS 伺服器。其必須開放給您的 DNS 伺服器 IP 位址，以便用戶端解析公用網域名稱。如果您未使用 DNS 伺服器進行網域名稱解析，則此連接埠需求為選用。

連接埠 80 (UDP 和 TCP)

此連接埠用於對 `https://clients.amazonworkspaces.com` 的初始連線，然後切換至 HTTPS。它必須開放給所在地區的EC2子集中的所有 IP 位址範圍。 WorkSpace

連接埠 443 (UDP 和 TCP)

此連接埠用於使用 HTTPS 進行註冊和驗證。它必須開放給所在地區的EC2子集中的所有 IP 位址範圍。 WorkSpace

連接埠 4195 (UDP 和 TCP)

針對 WorkSpaces 已設定為「 WorkSpaces 串流通訊協定」(WSP) 的連接埠，此連接埠會用於串流 WorkSpaces 桌面流量。此連接埠必須開放給 WSP 閘道 IP 位址範圍。如需詳細資訊，請參閱 WSP 閘道伺服器。

WSP Web 存取支援使用 Proxy 伺服器處理連接埠 4195 TCP 流量，但不建議這麼做。如需詳細資訊，請參閱針對視窗 WorkSpaces、Amazon Linux WorkSpaces 和 Ubuntu 的網際網路存取設定進行裝置代理伺服器設定 WorkSpaces。

> **Note**
>
> 如果您的防火牆使用具狀態篩選，則會自動開放暫時連接埠 (也稱為動態連接埠) 以允許回傳通訊。如果您的防火牆使用無狀態篩選，您必須明確開放暫時連接埠，以允許傳回通訊。您必須開放的必要暫時連接埠範圍會根據您的組態而有所不同。

一般而言，網頁瀏覽器會隨機選取高範圍內的來源連接埠，以用於串流流量。 WorkSpaces Web Access 無法控制瀏覽器選取的連接埠。您必須確保允許對此連接埠的傳回流量。

要新增至允許清單的網域和 IP 位址

若要讓用 WorkSpaces 戶端應用程式能夠存取 WorkSpaces 服務，您必須將下列網域和 IP 位址新增至用戶端嘗試存取服務之網路上的允許清單。

要新增至允許清單的網域和 IP 位址

類別	網域或 IP 位址
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	• https://d2td7dqidlhjx7.cloudfront.net/ • 在 AWS GovCloud (美國西部) 區域： https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ WorkSpacesAppCastx 64.xml
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： • 美國東部-1skylight-client-ds. 亞馬遜 • 美國西部-亞馬skylight-client-ds遜 • 阿帕-南方 1skylight-client-ds. 亞馬遜 • HTTPS://skylight-client-ds. 阿拉伯東北部-2. 亞馬遜 • HTTPS://skylight-client-ds.ap-東南部-1.亞馬遜 • HTTPS://skylight-client-ds.ap-東南部/亞馬遜 • HTTPS://skylight-client-ds. 阿拉伯東北部-1. 亞馬遜 • https://skylight-client-ds.ca-中央-1. 亞馬遜 • 亞馬遜網站://skylight-client-ds. 歐盟中央 • 歐盟西部 1skylight-client-ds. 亞馬遜 • 歐盟西部 2skylight-client-ds. 亞馬遜 • HTTPS://skylight-client-ds.sa-東部-1.亞馬遜 • 亞馬遜網站://skylight-client-ds. 南部

類別	網域或 IP 位址
	• HTTPS://skylight-client-ds. 中央-1. 亞馬遜 • 在 AWS GovCloud (美國西部) 區域： 網址：//skylight-client-ds。 us-gov-west-1. 亞馬遜 • 在 AWS GovCloud (美國東部) 區域： 網址：//skylight-client-ds。 us-gov-east-1. 亞馬遜

類別	網域或 IP 位址
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： • 美國東部-1ws-client-service. 亞馬遜 • 美國西部-亞馬ws-client-service遜 • 阿帕-南方 1ws-client-service. 亞馬遜 • HTTPS://ws-client-service. 阿拉伯東北部-2. 亞馬遜 • HTTPS://ws-client-service.ap-東南部-1.亞馬遜 • HTTPS://ws-client-service.ap-東南部/亞馬遜 • HTTPS://ws-client-service. 阿拉伯東北部-1. 亞馬遜 • https://ws-client-service.ca-中央-1. 亞馬遜 • 亞馬遜網站://ws-client-service. 歐盟中央 • 歐盟西部 1ws-client-service. 亞馬遜 • 歐盟西部 2ws-client-service. 亞馬遜 • HTTPS://ws-client-service.sa-東部-1.亞馬遜 • 亞馬遜網站://ws-client-service. 南部 • HTTPS://ws-client-service. 中央-1. 亞馬遜 • 在 AWS GovCloud (美國西部) 區域： 網址：//ws-client-service。 us-gov-west-1. 亞馬遜 • 在 AWS GovCloud (美國東部) 區域： 網址：//ws-client-service。 us-gov-east-1. 亞馬遜

類別	網域或 IP 位址
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/*<region>*/*<directory ID>* 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • 舊版—https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> • 美國東部 (維吉尼亞北部)—https://d2h1yryv1jxiq.cloudfront.net/ • 美國西部 (奧勒岡)—https://d1fq42e1gi7rtq.cloudfront.net/ • 亞太區域 (孟買)—https://d1ctsk4u02kky7.cloudfront.net/ • 亞太區域 (首爾)—https://dyoj3cw6iktvg.cloudfront.net • 亞太區域 (新加坡)—https://d1525ef92caquk.cloudfront.net/ • 亞太區域 (雪梨)—https://dodwxjr2amr8p.cloudfront.net/ • 亞太區域 (東京)—https://d3v7kcib8ir2e1.cloudfront.net/

類別	網域或 IP 位址
	• 加拿大 (中部)—https://d1ebdk07rro1qy.cloudfront.net/ • 歐洲 (法蘭克福)—https://d39q4y7cndearu.cloudfront.net/ • 歐洲 (愛爾蘭)—https://d2127w6wvrc6l3.cloudfront.net/ • 歐洲 (倫敦)—https://df4ahgpxbxqy2.cloudfront.net/ • 南美洲 (聖保羅)—https://d2nezqurrjvain.cloudfront.net/ • 非洲 (開普敦)—https://dr6ry0pwaoy23.cloudfront.net • 以色列 (特拉維夫) — https://d2kmf63k5sit88.cloudfront.net 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 美國東部 (維吉尼亞北部)—https://d32i4gd7pg4909.cloudfront.net/ • 美國西部 (奧勒岡)—https://d18af777lco7lp.cloudfront.net/ • 亞太區域 (孟買)—https://d78hovzzqqtsb.cloudfront.net/ • 亞太區域 (首爾)—https://dtyv4uwoh7ynt.cloudfront.net/ • 亞太區域 (新加坡)—https://d3qzmd7y07pz0i.cloudfront.net/

類別	網域或 IP 位址
	• 亞太區域 (雪梨)—https://dwcpoxuuza83q.cloudfront.net/ • 亞太區域 (東京)—https://d2c2t8mxjhq5z1.cloudfront.net/ • 加拿大 (中部)—https://d2wfbsypmqjmog.cloudfront.net/ • 歐洲 (法蘭克福)—https://d1whcm49570jjw.cloudfront.net/ • 歐洲 (愛爾蘭)—https://d3pgffbf39h4k4.cloudfront.net/ • 歐洲 (倫敦)—https://d16q6638mh01s7.cloudfront.net/ • 南美洲 (聖保羅)—https://d2lh2qc5bdoq4b.cloudfront.net/ • 非洲 (開普敦)—https://di5ygl2cs0mrh.cloudfront.net/ • 以色列 (特拉維夫) — https://d1a3pnge9on3sx.cloudfront.net 在 AWS GovCloud (美國西部) 區域： • 客戶目錄設定： https://s3.amazonaws.com/ workspaces-client-properties /品質/PDT/ <directory ID> • 客戶目錄層級合作品牌的登入頁面圖形： https://workspace-client-assets-pdt.s3--us-gov-west 一. 亞馬遜 • 用以設定登入頁面樣式的 CSS 檔案： https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript 文件的登錄頁面：

類別	網域或 IP 位址
	不適用 在 AWS GovCloud (美國東部) 區域： • 客戶目錄設定： https://s3.amazonaws.com/ workspaces-client-properties /品質/歐洲/ <directory ID> • 客戶目錄層級合作品牌的登入頁面圖形： https://workspace-client-assets-pdt.s3--us-gov-east 一. 亞馬遜 • 用以設定登入頁面樣式的 CSS 檔案： https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript 文件的登錄頁面： 不適用
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin. amazonaws-us-gov.com

類別	網域或 IP 位址
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域) 在 AWS GovCloud (美國西部) 和 AWS GovCloud (美國東部) 區域： https://login. us-gov-home<directory id>.awsapps.com /目錄/<directory id>/(客戶的網域名稱在哪裡)

類別	網域或 IP 位址
WS 中介裝置	網域： • 美國東部-1ws-broker-service. 亞馬遜 • 美國東部-1ws-broker-service-fips. 亞馬遜 • 美國西部-亞馬ws-broker-service遜 • 美國西部-亞馬ws-broker-service-fips遜 • 阿帕-南方 1ws-broker-service. 亞馬遜 • HTTPS://ws-broker-service. 阿拉伯東北部-2. 亞馬遜 • HTTPS://ws-broker-service.ap-東南部-1.亞馬遜 • HTTPS://ws-broker-service.ap-東南部/亞馬遜 • HTTPS://ws-broker-service. 阿拉伯東北部-1. 亞馬遜 • https://ws-broker-service.ca-中央-1. 亞馬遜 • 亞馬遜網站://ws-broker-service. 歐盟中央 • 歐盟西部 1ws-broker-service. 亞馬遜 • 歐盟西部 2ws-broker-service. 亞馬遜 • HTTPS://ws-broker-service.sa-東部-1.亞馬遜 • 亞馬遜網站://ws-broker-service. 南部 • HTTPS://ws-broker-service. 中央-1. 亞馬遜 • 網址：//ws-broker-service。 us-gov-west-1. 亞馬遜 • 網址：//ws-broker-service-fips。 us-gov-west-1. 亞馬遜 • 網址：//ws-broker-service。 us-gov-east-1. 亞馬遜 • 網址：//ws-broker-service-fips。 us-gov-east-1. 亞馬遜

類別	網域或 IP 位址
WorkSpaces API 端點	網域： • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

類別	網域或 IP 位址
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces. us-gov-west-1. 亞馬遜 • https://workspaces-fips. us-gov-west-1. 亞馬遜 • https://workspaces. us-gov-east-1. 亞馬遜 • https://workspaces-fips. us-gov-east-1. 亞馬遜

類別	網域或 IP 位址
WorkSpaces 適用於 SAML 單一登入 (SSO) 的端點	網域： • HTTPS://euc-sso-sm. 美國東部-1. 亞馬遜. COM /v1/ 報告心跳 • HTTPS://euc-sso-sm-fips. 美國東部-1. 亞馬遜. COM /v1/ 報告心跳 • 美國西部-亞馬遜公司 /V1 /報告euc-sso-sm心跳動 • 美國西部-亞馬遜公司 /V1 /報告euc-sso-sm-fips心跳動 • .ap-南 1. 亞馬遜公司 /v1/ 報告心euc-sso-sm跳 • HTTPS://euc-sso-sm. AP-東北部-2. 亞馬遜. COM /v1/ 報告心跳 • HTTPS://euc-sso-sm. AP-東南部-1. 亞馬遜. COM /v1/ 報告心跳 • HTTPS://euc-sso-sm. AP-東南部-2. 亞馬遜. COM /v1/ 報告心跳 • HTTPS://euc-sso-sm. AP-東北部-1. 亞馬遜. COM /v1/ 報告心跳 • 歐盟中心 1. 亞馬遜公司 /V1 /報告euc-sso-sm心跳動 • 歐盟西部 2. 亞馬遜公司 /V1 /報告euc-sso-sm心跳動 • 阿馬遜南 1. 亞馬遜公司 /v1/ 報告心euc-sso-sm跳 • 中心 1. 亞馬遜公司 /v1/ 報告心euc-sso-sm跳 • 網址：//euc-sso-sm。 us-gov-west-1. 亞馬遜. COM /v1/ 報告心跳 • 網址：//euc-sso-sm-fips。 us-gov-west-1. 亞馬遜. COM /v1/ 報告心跳

類別	網域或 IP 位址
	• 網址：//euc-sso-sm。 us-gov-east-1. 亞馬遜. COM /v1/ 報告心跳 • 網址：//euc-sso-sm-fips。 us-gov-east-1. 亞馬遜. COM /v1/ 報告心跳

要新增至 PCoIP 允許清單的網域和 IP 位址

類別	網域或 IP 位址
PCoIP 工作階段閘道 (PSG)	PCoIP 閘道伺服器
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.us-east-1.amazonaws.com • 美國東部-1skylight-cm-fips. 亞馬遜 • https://skylight-cm.us-west-2.amazonaws.com • 美國西部-亞馬skylight-cm-fips遜 • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com • https://skylight-cm.eu-central-1.amazonaws.com

類別	網域或 IP 位址
	• https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm. us-gov-west-1. 亞馬遜 • 網址：//skylight-cm-fips。 us-gov-west-1. 亞馬遜 • https://skylight-cm. us-gov-east-1. 亞馬遜 • 網址：//skylight-cm-fips。 us-gov-east-1. 亞馬遜

類別	網域或 IP 位址
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web Access 目前不適用於亞太 (孟買) 區域。 • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • 非洲 (開普敦) 地區目前不提供 Web 存取 • 以色列 (特拉維夫) 地區目前不提供 Web 存取。

要新增至 WorkSpaces 串流通訊協定 (WSP) 允許清單的網域和 IP 位址

類別	網域或 IP 位址
WSP 工作階段閘道 (WSG)	WSP 閘道伺服器
適用於 WSP 的 Web Access TURN 伺服器	WSP 閘道伺服器

運作狀態檢查伺服器

用 WorkSpaces 戶端應用程式會透過連接埠 4172 和 4195 執行健康狀態檢查。這些檢查會驗證 TCP 或 UDP 流量是否從 WorkSpaces 伺服器串流到用戶端應用程式。若要順利完成這些檢查，您的防火牆政策必須允許輸出流量至下列區域運作狀態檢查伺服器的 IP 位址。

區域	運作狀態檢查主機名稱	IP 位址
美國東部 (維吉尼亞北部)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
美國西部 (奧勒岡)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
亞太區域 (孟買)	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
亞太區域 (首爾)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105 52.78.44.253 52.79.54.102
亞太區域 (新加坡)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123

區域	運作狀態檢查主機名稱	IP 位址
		52.74.175.118
亞太區域 (雪梨)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
亞太區域 (東京)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
加拿大 (中部)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
歐洲 (法蘭克福)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227
歐洲 (愛爾蘭)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
歐洲 (倫敦)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36

區域	運作狀態檢查主機名稱	IP 位址
南美洲 (聖保羅)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
非洲 (開普敦)	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
以色列 (特拉維夫)	drp-tlv. 亞馬遜工作空間	51.17.52.90 51.17.109.231 51.16.190.43
AWS GovCloud (美國西部)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88
AWS GovCloud (美國東部)	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

PCoIP 閘道伺服器

WorkSpaces 使用 PCoIP 透過連接埠 4172 將桌面工作階段串流至用戶端。對於其 PCoIP 閘道伺服器， WorkSpaces 使用少量範圍的 Amazon EC2 公有 IPv4 地址。這可讓您針對存取的裝置設定更精細的防火牆原則 WorkSpaces。請注意，用 WorkSpaces 戶端目前不支援 IPv6 位址做為連線選項。

區域	公用 IP 位址範圍
美國東部 (維吉尼亞北部)	3.217.228.0-3.217.231.255 3.235.112.0-3.235.119.255 52.23.61.0-52.23.62.255
美國西部 (奧勒岡)	35.80.88.0-35.80.95.255 44.234.54.0-44.234.55.255 54.244.46.0-54.244.47.255
亞太區域 (孟買)	13.126.243.0-13.126.243.255
亞太區域 (首爾)	3.34.37.0-3.34.37.255 3.34.38.0-3.34.39.255 13.124.247.0-13.124.247.255
亞太區域 (新加坡)	18.141.152.0-18.141.152.255 18.141.154.0-18.141.155.255 52.76.127.0-52.76.127.255
亞太區域 (雪梨)	3.25.43.0-3.25.43.255 3.25.44.0-3.25.45.255 54.153.254.0-54.153.254.255
亞太區域 (東京)	18.180.178.0-18.180.178.255

區域	公用 IP 位址範圍
	18.180.180.0-18.180.181.255
	54.250.251.0-54.250.251.255
加拿大 (中部)	15.223.100.0-15.223.100.255
	15.223.102.0-15.223.103.255
	35.183.255.0-35.183.255.255
歐洲 (法蘭克福)	18.156.52.0-18.156.52.255
	18.156.54.0-18.156.55.255
	52.59.127.0-52.59.127.255
歐洲 (愛爾蘭)	3.249.28.0-3.249.29.255
	52.19.124.0-52.19.125.255
歐洲 (倫敦)	18.132.21.0-18.132.21.255
	18.132.22.0-18.132.23.255
	35.176.32.0-35.176.32.255
南美洲 (聖保羅)	18.230.103.0-18.230.103.255
	18.230.104.0-18.230.105.255
	54.233.204.0-54.233.204.255
非洲 (開普敦)	13.246.120.0-13.246.123.255
以色列 (特拉維夫)	51.17.28.0-51.17.31.255
AWS GovCloud (美國西部)	52.61.193.0-52.61.193.255
AWS GovCloud (美國東部)	18.254.140.0-18.254.143.255

WSP 閘道伺服器

> **Important**
>
> 從 2020 年 6 月開始， WorkSpaces將 WSP 的桌面工作階段透過連接埠 4195 (而非連接埠 4172) WorkSpaces 串流至用戶端。如果您要使用 WSP WorkSpaces，請確定連接埠 4195 已開放給流量使用。

WorkSpaces 為其 WSP 閘道伺服器使用少量範圍的 Amazon EC2 公有 IPv4 地址。這可讓您針對存取的裝置設定更精細的防火牆原則 WorkSpaces。請注意，用 WorkSpaces 戶端目前不支援 IPv6 位址做為連線選項。

區域	公用 IP 位址範圍
美國東部 (維吉尼亞北部)	• 3.227.4.0/22 • 44.209.84.0/22
美國西部 (奧勒岡)	34.223.96.0/22
亞太區域 (孟買)	65.1.156.0/22
亞太區域 (首爾)	3.35.160.0/22
亞太區域 (新加坡)	13.212.132.0/22
亞太區域 (雪梨)	3.25.248.0/22
亞太區域 (東京)	3.114.164.0/22
加拿大 (中部)	3.97.20.0/22
歐洲 (法蘭克福)	18.192.216.0/22
歐洲 (愛爾蘭)	3.248.176.0/22
歐洲 (倫敦)	18.134.68.0/22
南美洲 (聖保羅)	15.228.64.0/22

區域	公用 IP 位址範圍
非洲 (開普敦)	13.246.108.0/22
以色列 (特拉維夫)	51.17.72.0/22
AWS GovCloud (美國西部)	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud (美國東部)	18.254.148.0/22

WSP 閘道網域名稱

下表列出 WSP WorkSpace 閘道網域名稱。這些網域必須是可連絡的，用 WorkSpaces 戶端應用程式才能存取 WorkSpace WSP 服務。

區域	網域
美國東部 (維吉尼亞北部)	*. 上帝-东 1. 高地人.
美國西部 (奧勒岡)	*. 上帝美國西部 2. 高地德.
亞太區域 (孟買)	南部高地兰德
亞太區域 (首爾)	*. 东北部-高地人.
亞太區域 (新加坡)	*. 东南部-高地人 .aws.a2z.com
亞太區域 (雪梨)	*. 东南部-高地人 .aws.a2z.com
亞太區域 (東京)	*. 上帝国东北部-高地人.
加拿大 (中部)	*. 科罗卡-中部高地人
歐洲 (法蘭克福)	*. 普羅德歐洲中部高地人 .aws.a2z.com
歐洲 (愛爾蘭)	*. 上帝歐洲西部 1. 高地德.

區域	網域
歐洲 (倫敦)	*. 上帝欧洲西部 2. 高地代理
南美洲 (聖保羅)	*. 上帝-东 1. 高地人 .aws.a2z.com
非洲 (開普敦)	*. 上海地区南部高地兰德
以色列 (特拉維夫)	*. 上城市中心 1. 高地地区
AWS GovCloud (美國西部)	*.prod。 us-gov-west-1. 高地兰德. aw.a2z.com
AWS GovCloud (美國東部)	*.prod。 us-gov-east-1. 高地兰德. aw.a2z.com

網路介面

每個介面都 WorkSpace 有下列網路介面：

- 主要網路介面 (eth1) 提供連線到 VPC 內和網際網路上的資源，可用來加入 WorkSpace 目錄。
- 管理網路介面 (eth0) 連接到安全的 WorkSpaces管理網路。它用於 WorkSpace桌面到 WorkSpaces 客戶端的交互式流，並 WorkSpaces 允許管理 WorkSpace.

WorkSpaces 根據在中建立的區域，從不同的位址範圍選取管理網路介面的 IP 位址。 WorkSpaces 註冊目錄後，請 WorkSpaces 測試 VPC CIDR 和 VPC 中的路由表，以判斷這些位址範圍是否會產生衝突。如果在「區域」的所有可用位址範圍中發現衝突，則會顯示錯誤訊息，且不會註冊目錄。如果在註冊目錄後變更 VPC 中的路由表，則可能導致衝突。

> **Warning**
>
> 請勿修改或刪除任何附加到 WorkSpace. 這樣做可能會導致無 WorkSpace 法訪問或失去互聯網訪問。例如，如果您已在目錄層級啟用彈性 IP 地址的自動分配，則彈性 IP 地址（來自 Amazon 提供的集區）在啟動 WorkSpace時會分配給您。但是，如果您將擁有的彈性 IP 地址關聯到一個 WorkSpace，然後您稍後將該彈性 IP 地址與中斷關聯 WorkSpace，則會 WorkSpace 丟失其公共 IP 地址，並且不會自動從 Amazonon 提供的池中獲取新 IP 地址。若要將 Amazon 提供的集區中的新公用 IP 位址與相關聯 WorkSpace，您必須重建. WorkSpace 如果您不想重建 WorkSpace，則必須將您擁有的另一個彈性 IP 地址與 WorkSpace.

管理介面 IP 範圍

下表列出用於管理網路介面的 IP 位址範圍。

> **Note**
>
> - 如果您使用的是自攜授權 (BYOL) Windows WorkSpaces，則下表中的 IP 位址範圍不適用。PCoIP BYOL 會改為 WorkSpaces 使用 54.239.224.0/20 的 IP 位址範圍來處理所有區域中的管理介面流量。AWS對於 WSP 自攜裝置視窗 WorkSpaces，所有區域都會套用 54.239.224.0/20 和 10.0.0.0/8 的 IP 位址範圍。AWS(除了為 B WorkSpaces YOL 管理流量選取的 /16 CIDR 區塊之外，還會使用這些 IP 位址範圍。)
> - 如果您使用從公用套件組合 WorkSpaces 建立的 WSP，除了下表所示的 PCoIP/WSP 範圍外，IP 位址範圍 10.0.0.0/8 也適用於所有AWS區域的管理介面流量。

區域	IP 位址範圍
美國東部 (維吉尼亞北部)	PCoIP/WSP：172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 WSP：10.0.0.0/8
美國西部 (奧勒岡)	PCOIPP /WSP：172.31.0.0.0/16、192.168.0.0/16 及 198.19.0.0/16 WSP：10.0.0.0/8
亞太區域 (孟買)	PCoIP/WSP：192.168.0.0/16 WSP：10.0.0.0/8
亞太區域 (首爾)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
亞太區域 (新加坡)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8

區域	IP 位址範圍
亞太區域 (雪梨)	PCOIPP/WSP：172.31.0.0.0/16、192.168.0.0.0/16 及 198.19.0.0/16 WSP：10.0.0.0/8
亞太區域 (東京)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
加拿大 (中部)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
歐洲 (法蘭克福)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
歐洲 (愛爾蘭)	PCOIPP/WSP：172.31.0.0.0/16、192.168.0.0.0/16 及 198.19.0.0/16 WSP：10.0.0.0/8
歐洲 (倫敦)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
南美洲 (聖保羅)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
非洲 (開普敦)	PCoIP/WSP：172.31.0.0/16 和 198.19.0.0/16 WSP：10.0.0.0/8
以色列 (特拉維夫)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8

區域	IP 位址範圍
AWS GovCloud (美國西部)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8 和 192.169.0.0/16
AWS GovCloud (美國東部)	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8

管理介面連接埠

下列連接埠必須在所有的管理網路介面上開啟 WorkSpaces：

- 連接埠 4172 上的傳入 TCP。這用於在 PCoIP 通訊協定上建立串流連線。
- 連接埠 4172 上的傳入 UDP。這用於在 PCoIP 通訊協定上串流使用者輸入。
- 連接埠 4489 上的傳入 TCP。這用於使用 Web 客戶端進行存取。
- 連接埠 8200 上的傳入 TCP。這是用來管理和組態的 WorkSpace.
- 連接埠 8201-8250 上的傳入 TCP。這些連接埠用於建立串流連線，以及在 WSP 通訊協定上串流使用者輸入。
- 連接埠 8220 上的傳入 UDP。此連接埠用於建立串流連線，以及在 WSP 通訊協定上串流使用者輸入
- 連接埠 8443 和 9997 上的傳出 TCP。這用於使用 Web 客戶端進行存取。
- 連接埠 3478、4172 和 4195 上的傳出 UDP。這用於使用 Web 客戶端進行存取。
- 連接埠 50002 和 55002 上的傳出 UDP。這是用於串流。如果您的防火牆使用具狀態篩選，則會自動開放暫時連接埠 50002 和 55002 以允許回傳通訊。如果您的防火牆使用無狀態篩選，您必須開放暫時連接埠 49152 - 65535 以允許傳回通訊。
- 如管理介面 IP 範圍中所定義，連接埠 80 上的輸出 TCP 至 IP 位址 169.254.169.254，以便存取 EC2 中繼資料服務。指派給您的任何 HTTP 代理伺服器也 WorkSpaces 必須排除。
- 連接埠 1688 上對 IP 位址 169.254.169.250 和 169.254.169.251 的傳出 TCP，允許存取 Microsoft KMS，以便針對以公用套件為基礎的 Workspaces 進行 Windows 啟用。如果您使用的是自攜授權 (BYOL) 視窗 WorkSpaces，您必須允許存取您自己的 KMS 伺服器，才能啟用 Windows。
- 連接埠 1688 上的輸出 TCP 至 IP 位址 54.239.236.220，以允許存取 Microsoft KMS 以啟用自攜裝置的辦公室。 WorkSpaces

如果您透過其中一個公用服務包使用 Office，適用於辦 WorkSpaces 公室的 Microsoft KMS 啟用 IP 位址會有所不同。若要判斷 IP 位址，請尋找的管理介面的 IP 位址 WorkSpace，然後將最後兩個八位元組取代為。64.250例如，如果管理介面的 IP 位址是 192.168.3.5，則是用於 Microsoft KMS Office 啟用的 IP 位址為 192.168.64.250。

- 當主機設定為使用代理伺服器 WorkSpaces 時，WSP 的輸出 TCP 至 WorkSpace IP 位址 127.0.0.2。
- 源自迴路位址 127.0.01 的通訊。

在一般情況下， WorkSpaces 服務會為您的. WorkSpaces 如果在封鎖任何這些連接埠的安全性或防火牆軟體上安裝，則 WorkSpace 可能無法正常運作或無法連線。 WorkSpace

主要介面連接埠

無論您擁有哪種類型的目錄，都必須在所有主要網路介面上開啟下列連接埠 WorkSpaces：

- 對於網際網路連線，下列連接埠必須開放至所有目的地的出埠，以及從 WorkSpaces VPC 輸入的連接埠。如果您希望他們可以訪問 Internet， WorkSpaces 則需要手動將其添加到安全組中。
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- 若要與目錄控制器通訊，您的 WorkSpaces VPC 和目錄控制器之間必須開啟下列連接埠。對於 Simple AD 目錄，由 AWS Directory Service 建立的安全群組將會正確設定這些連接埠。對於 AD Connector 目錄，您可能需要調整 VPC 的預設安全群組，以開放這些連接埠。
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos 身分驗證
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - 網路通訊協定 636-LDAP (透過網路連接埠/SSL 的 LDAP)
  - TCP 1024-65535 - RPC 動態連接埠

如果在封鎖任何這些連接埠的安全性或防火牆軟體上安裝，則 WorkSpace 可能無法正常運作或無法連線。 WorkSpace

各區域的 IP 位址和連接埠需求

美國東部 (維吉尼亞北部)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 美國東部-1skylight-client-ds. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 美國東部-1ws-client-service. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

類別	詳細資訊
	客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 美國東部 (維吉尼亞北部)—https://d32i4gd7pg4909.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.us-east-1.signin.aws
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 美國東部-1ws-broker-service. 亞馬遜 • 美國東部-1ws-broker-service-fips. 亞馬遜
WorkSpaces API 端點	網域： https://workspaces.us-east-1.amazonaws.com

類別	詳細資訊
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.us-east-1.amazonaws.com • 美國東部-1skylight-cm-fips. 亞馬遜
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.us-east-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-iad.amazonworkspaces.com
運作狀態檢查 IP 位址	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
PCoIP 閘道伺服器公用 IP 位址範圍	• 3.217.228.0-3.217.231.255 • 3.235.112.0-3.235.119.255 • 52.23.61.0-52.23.62.255
WSP 閘道伺服器 IP 位址範圍	• 3.227.4.0/22 • 44.209.84.0/22
WSP 閘道網域名稱	*. 上帝-东 1. 高地人.
管理介面 IP 位址範圍	• PCoIP/WSP：172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 • WSP：10.0.0.0/8

美國西部 (奧勒岡)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 美國西部-亞馬skylight-client-ds遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 美國西部-亞馬ws-client-service遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID>

類別	詳細資訊
	用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 美國西部 (奧勒岡)—https://d18af777lco7lp.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.us-west-2.signin.aws
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 美國西部-亞馬ws-broker-service遜 • 美國西部-亞馬ws-broker-service-fips遜
WorkSpaces API 端點	網域： • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com

類別	詳細資訊
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.us-west-2.amazonaws.com • 美國西部-亞馬skylight-cm-fips遜
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.us-west-2.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-pdx.amazonworkspaces.com
運作狀態檢查 IP 位址	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
PCoIP 閘道伺服器公用 IP 位址範圍	• 35.80.88.0-35.80.95.255 • 44.234.54.0-44.234.55.255 • 54.244.46.0-54.244.47.255
WSP 閘道伺服器 IP 位址範圍	34.223.96.0/22
WSP 閘道網域名稱	*. 上帝美國西部 2. 高地德.
管理介面 IP 位址範圍	• PCoIP/WSP：172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 • WSP：10.0.0.0/8

亞太區域 (孟買)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 阿帕-南方 1skylight-client-ds. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 阿帕-南方 1ws-client-service. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID>

類別	詳細資訊
	用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 亞太區域 (孟買)—https://d78hovzzqqtsb.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 阿帕-南方 1ws-broker-service. 亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.ap-south-1.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.ap-south-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	Web Access 目前不適用於亞太 (孟買) 區域
運作狀態檢查主機名稱	drp-bom.amazonworkspaces.com

類別	詳細資訊
運作狀態檢查 IP 位址	• 13.127.57.82 • 13.234.250.73
PCoIP 閘道伺服器公用 IP 位址範圍	13.126.243.0-13.126.243.255
WSP 閘道伺服器 IP 位址範圍	65.1.156.0/22
WSP 閘道網域名稱	南部高地兰德
管理介面 IP 位址範圍	• PCoIP/WSP：192.168.0.0/16 • WSP：10.0.0.0/8

亞太區域 (首爾)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
裝置度量 (適用於 1.0 和 2.0 以上的 WorkSpaces 用戶端應用程式)	HTTPS://2. 亞馬device-metrics-us遜
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://skylight-client-ds. 阿拉伯東北部-2. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://ws-client-service. 阿拉伯東北部-2. 亞馬遜

類別	詳細資訊
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 亞太區域 (首爾)—https://dtyv4uwoh7ynt.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器

類別	詳細資訊
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • HTTPS://ws-broker-service. 阿拉伯東北部-2. 亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.ap-northeast-2.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.ap-northeast-2.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.ap-northeast-2.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-icn.amazonworkspaces.com
運作狀態檢查 IP 位址	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
PCoIP 閘道伺服器公用 IP 位址範圍	• 3.34.37.0-3.34.37.255 • 3.34.38.0-3.34.39.255 • 13.124.247.0-13.124.247.255
WSP 閘道伺服器 IP 位址範圍	3.35.160.0/22

類別	詳細資訊
WSP 閘道網域名稱	*. 东北部-高地人.
管理介面 IP 位址範圍	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

亞太區域 (新加坡)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://skylight-client-ds.ap-東南部-1.亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	域名:https://ws-client-service.ap-東南部-1. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定：

類別	詳細資訊
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 亞太區域 (新加坡)—https://d3qzmd7y07pz0i.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • HTTPS://ws-broker-service.ap-東南部-1.亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.ap-southeast-1.amazonaws.com

類別	詳細資訊
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.ap-southeast-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.ap-southeast-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-sin.amazonworkspaces.com
運作狀態檢查 IP 位址	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
PCoIP 閘道伺服器公用 IP 位址範圍	• 18.141.152.0-18.141.152.255 • 18.141.154.0-18.141.155.255 • 52.76.127.0-52.76.127.255
WSP 閘道伺服器 IP 位址範圍	13.212.132.0/22
WSP 閘道網域名稱	*. 东南部-高地人 .aws.a2z.com
管理介面 IP 位址範圍	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

亞太區域 (雪梨)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/

類別	詳細資訊
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://skylight-client-ds.ap-東南部/亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://ws-client-service.ap-東南部/亞馬遜

類別	詳細資訊
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 亞太區域 (雪梨)—https://dwcpoxuuza83q.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.ap-southeast-2.signin.aws

類別	詳細資訊
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • HTTPS://ws-broker-service.ap-東南部/亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.ap-southeast-2.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.ap-southeast-2.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.ap-southeast-2.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-syd.amazonworkspaces.com
運作狀態檢查 IP 位址	• 3.24.11.127 • 13.237.232.125
PCoIP 閘道伺服器公用 IP 位址範圍	• 3.25.43.0-3.25.43.255 • 3.25.44.0-3.25.45.255 • 54.153.254.0-54.153.254.255
WSP 閘道伺服器 IP 位址範圍	3.25.248.0/22
WSP 閘道網域名稱	*. 东南部-高地人 .aws.a2z.com

類別	詳細資訊
管理介面 IP 位址範圍	• PCOIPP/WSP：172.31.0.0.0/16、192.168.0.0.0/16 及 198.19.0.0/16 • WSP：10.0.0.0/8

亞太區域 (東京)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://skylight-client-ds. 阿拉伯東北部-1. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://ws-client-service. 阿拉伯東北部-1. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定：

類別	詳細資訊
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 亞太區域 (東京)—https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.ap-northeast-1.signin.aws
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • HTTPS://ws-broker-service. 阿拉伯東北部-1. 亞馬遜

類別	詳細資訊
WorkSpaces API 端點	網域： • https://workspaces.ap-northeast-1.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.ap-northeast-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.ap-northeast-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-nrt.amazonworkspaces.com
運作狀態檢查 IP 位址	• 18.178.102.247 • 54.64.174.128
PCoIP 閘道伺服器公用 IP 位址範圍	• 18.180.178.0-18.180.178.255 • 18.180.180.0-18.180.181.255 • 54.250.251.0-54.250.251.255
WSP 閘道伺服器 IP 位址範圍	3.114.164.0/22
WSP 閘道網域名稱	*. 上帝国东北部-高地人.
管理介面 IP 位址範圍	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

加拿大 (中部)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

類別	詳細資訊
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： https://skylight-client-ds.ca-中央-1. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： https://ws-client-service.ca-中央-1. 亞馬遜

類別	詳細資訊
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 加拿大 (中部)—https://d2wfbsypmqjmog.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器

類別	詳細資訊
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • https://ws-broker-service.ca-中央-1. 亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.ca-central-1.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.ca-central-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.ca-central-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-yul.amazonworkspaces.com
運作狀態檢查 IP 位址	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
PCoIP 閘道伺服器公用 IP 位址範圍	• 15.223.100.0-15.223.100.255 • 15.223.102.0-15.223.103.255 • 35.183.255.0-35.183.255.255
WSP 閘道伺服器 IP 位址範圍	3.97.20.0/22

類別	詳細資訊
WSP 閘道網域名稱	*. 科罗卡-中部高地人
管理介面 IP 位址範圍	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

歐洲 (法蘭克福)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 歐盟中央 1skylight-client-ds. 亞馬遜網站
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 歐盟中央 1ws-client-service. 亞馬遜網站
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定：

類別	詳細資訊
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 歐洲 (法蘭克福)—https://d1whcm49570jjw.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 歐盟中央 1ws-broker-service. 亞馬遜網站
WorkSpaces API 端點	網域： • https://workspaces.eu-central-1.amazonaws.com

類別	詳細資訊
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.eu-central-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.eu-central-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-fra.amazonworkspaces.com
運作狀態檢查 IP 位址	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
PCoIP 閘道伺服器公用 IP 位址範圍	• 18.156.52.0-18.156.52.255 • 18.156.54.0-18.156.55.255 • 52.59.127.0-52.59.127.255
WSP 閘道伺服器 IP 位址範圍	18.192.216.0/22
WSP 閘道網域名稱	*. 普羅德歐洲中部高地人 .aws.a2z.com
管理介面 IP 位址範圍	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

歐洲 (愛爾蘭)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/

類別	詳細資訊
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 歐盟西部-亞馬skylight-client-ds遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 歐盟西部-亞馬ws-client-service遜

類別	詳細資訊
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 歐洲 (愛爾蘭)—https://d3pgffbf39h4k4.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.eu-west-1.signin.aws

類別	詳細資訊
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 歐盟西部-亞馬ws-broker-service遜
WorkSpaces API 端點	網域： • https://workspaces.eu-west-1.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.eu-west-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.eu-west-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-dub.amazonworkspaces.com
運作狀態檢查 IP 位址	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
PCoIP 閘道伺服器公用 IP 位址範圍	• 3.249.28.0-3.249.29.255 • 52.19.124.0-52.19.125.255
WSP 閘道伺服器 IP 位址範圍	3.248.176.0/22
WSP 閘道網域名稱	*. 上帝歐洲西部 1. 高地德.

類別	詳細資訊
管理介面 IP 位址範圍	• PCOIPP/WSP：172.31.0.0.0/16、192.168.0.0.0/16 及 198.19.0.0/16 • WSP：10.0.0.0/8

歐洲 (倫敦)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 歐盟西部 2skylight-client-ds. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 歐盟西部 2ws-client-service. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定：

類別	詳細資訊
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 歐洲 (倫敦)—https://d16q6638mh01s7.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 歐盟西部 2ws-broker-service. 亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.eu-west-2.amazonaws.com

類別	詳細資訊
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.eu-west-2.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.eu-west-2.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-lhr.amazonworkspaces.com
運作狀態檢查 IP 位址	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
PCoIP 閘道伺服器公用 IP 位址範圍	• 18.132.21.0-18.132.21.255 • 18.132.22.0-18.132.23.255 • 35.176.32.0-35.176.32.255
WSP 閘道伺服器 IP 位址範圍	18.134.68.0/22
WSP 閘道網域名稱	*. 上帝欧洲西部 2. 高地代理
管理介面 IP 位址範圍	• 198.19.0.0/16 • WSP：10.0.0.0/8

南美洲 (聖保羅)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/

類別	詳細資訊
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://skylight-client-ds.sa-東部-1.亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： HTTPS://ws-client-service.sa-東部-1.亞馬遜

類別	詳細資訊
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 南美洲 (聖保羅)—https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器

類別	詳細資訊
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • HTTPS://ws-broker-service.sa-東部-1.亞馬遜
WorkSpaces API 端點	網域： • https://workspaces.sa-east-1.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.sa-east-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • turn:*.sa-east-1.rdn.amazonaws.com
運作狀態檢查主機名稱	drp-gru.amazonworkspaces.com
運作狀態檢查 IP 位址	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP 閘道伺服器公用 IP 位址範圍	• 18.230.103.0-18.230.103.255 • 18.230.104.0-18.230.105.255 • 54.233.204.0-54.233.204.255
WSP 閘道伺服器 IP 位址範圍	15.228.64.0/22

類別	詳細資訊
WSP 閘道網域名稱	*. 上帝-东 1. 高地人 .aws.a2z.com
管理介面 IP 位址範圍	• 198.19.0.0/16 • WSP：10.0.0.0/8

非洲 (開普敦)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 亞馬遜網站://skylight-client-ds. 南部
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 亞馬遜網站://ws-client-service. 南部
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定：

類別	詳細資訊
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 非洲 (開普敦)—https://di5ygl2cs0mrh.cloudfront.net/
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 亞馬遜網站://ws-broker-service. 南部
WorkSpaces API 端點	網域： • https://workspaces.af-south-1.amazonaws.com

類別	詳細資訊
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.af-south-1.amazonaws.com
運作狀態檢查主機名稱	drp-cpt.amazonworkspaces.com
運作狀態檢查 IP 位址	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP 閘道伺服器公用 IP 位址範圍	• 13.246.120.0-13.246.123.255
WSP 閘道伺服器 IP 位址範圍	15.228.64.0/22
WSP 閘道網域名稱	*. 上海地区南部高地兰德
管理介面 IP 位址範圍	• 172.31.0.0/16 和 198.19.0.0/16 • WSP：10.0.0.0/8

以色列 (特拉維夫)

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://d2td7dqidlhjx7.cloudfront.net/
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 阿馬遜網站://skylight-client-ds. 中央-阿馬遜

類別	詳細資訊
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 阿馬遜網站://ws-client-service. 中央-阿馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> 客戶目錄層級合作品牌的登入頁面圖形： • 用以設定登入頁面樣式的 CSS 檔案： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 文件的登錄頁面： • 以色列 (特拉維夫); —
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器

類別	詳細資訊
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://<directory id>.awsapps.com/ (其中 <directory id> 是客戶的網域)
WS 中介裝置	網域： • 阿馬遜網站://ws-broker-service. 中央-阿馬遜
WorkSpaces API 端點	網域： • https://workspaces.il-central-1.amazonaws.com
工作階段中介裝置 (PCM)	網域： • https://skylight-cm.il-central-1.amazonaws.com
適用於 PCoIP 的 Web Access TURN 伺服器	伺服器： • 轉:*. 中央-1.rdn.Amazonaws.com
運作狀態檢查主機名稱	drp-TLV. 亞馬遜工作空間
運作狀態檢查 IP 位址	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
PCoIP 閘道伺服器公用 IP 位址範圍	• 51.17.28.0-51.17.31.255
WSP 閘道伺服器 IP 位址範圍	51.17.72.0/22
WSP 閘道網域名稱	*. 上城市中心 1. 高地地区
管理介面 IP 位址範圍	• 198.19.0.0/16 • WSP：10.0.0.0/8

AWS GovCloud (美國西部) 區域

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://s3.amazonaws.com/ workspaces-client-updates /品質/PDT/窗口/ WorkSpacesAppCast
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 網址：//skylight-client-ds。 us-gov-west-1. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 網址：//ws-client-service。 us-gov-west-1. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://s3.amazonaws.com/ workspaces-client-properties /品質/PDT/ <directory ID> 客戶目錄層級合作品牌的登入頁面圖形：

類別	詳細資訊
	• https://s3.amazonaws.com/ workspaces-client-assets /品質/PDT/ <directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript 文件的登錄頁面： • 不適用
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.signin. amazonaws-us-gov.com
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://login. us-gov-home<directory id>.awsapps.com /目錄/<directory id>/(客戶的網域名稱在哪裡)
WS 中介裝置	網域： • 網址：//ws-broker-service。 us-gov-west-1. 亞馬遜 • 網址：//ws-broker-service-fips。 us-gov-west-1. 亞馬遜

類別	詳細資訊
WorkSpaces API 端點	網域： • https://workspaces. us-gov-west-1. 亞馬遜 • https://workspaces-fips. us-gov-west-1. 亞馬遜
工作階段中介裝置 (PCM)	網域： • https://skylight-cm. us-gov-west-1. 亞馬遜 • 網址：//skylight-cm-fips。 us-gov-west-1. 亞馬遜
運作狀態檢查主機名稱	drp-pdt.amazonworkspaces.com
運作狀態檢查 IP 位址	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoIP 閘道伺服器公用 IP 位址範圍	• 52.61.193.0-52.61.193.255
WSP 閘道伺服器 IP 位址範圍	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
WSP 閘道網域名稱	*.prod。 us-gov-west-1. 高地兰德. aw.a2z.com
管理介面 IP 位址範圍	• 198.19.0.0/16 • WSP：10.0.0.0/8 和 192.169.0.0/16

AWS GovCloud (美國東部) 區域

要新增至允許清單的網域和 IP 位址

類別	詳細資訊
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
用戶端自動更新	https://s3.amazonaws.com/ workspaces-client-updates /品質/奧洲/窗口/ WorkSpacesAppCast
連線能力檢查	https://connectivity.amazonworkspaces.com/
用戶端測量結果 (3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 網址：//skylight-client-ds。 us-gov-east-1. 亞馬遜
動態訊息服務 (適用於 3.0 個以上的 WorkSpaces 用戶端應用程式)	網域： 網址：//ws-client-service。 us-gov-east-1. 亞馬遜
目錄設定	從客戶端到客戶目錄的身份驗證，然後再登錄到 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> 來自 macOS 用戶端的連線： • https://d32i4gd7pg4909.cloudfront.net/ 客戶目錄設定： • https://s3.amazonaws.com/ workspaces-client-properties /品質/歐洲/ <directory ID> 客戶目錄層級合作品牌的登入頁面圖形：

類別	詳細資訊
	• https://s3.amazonaws.com/ workspaces-client-assets /品質/歐洲/ <directory ID> 用以設定登入頁面樣式的 CSS 檔案： • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript 文件的登錄頁面： • 不適用
Forrester 日誌服務	https://fls-na.amazon.com/
運作狀態檢查 (DRP) 伺服器	運作狀態檢查伺服器
工作階段前智慧卡驗證端點	https://smartcard.signin. amazonaws-us-gov.com
註冊相依性 (適用於 Web Access 和 Teradici PCoIP 零用戶端)	https://s3.amazonaws.com
使用者登入頁面	https://login. us-gov-home<directory id>.awsapps.com /目錄/<directory id>/(客戶的網域名稱在哪裡)
WS 中介裝置	網域： • 網址：//ws-broker-service。 us-gov-east-1. 亞馬遜 • 網址：//ws-broker-service-fips。 us-gov-east-1. 亞馬遜

類別	詳細資訊
WorkSpaces API 端點	網域： • https://workspaces. us-gov-east-1. 亞馬遜 • https://workspaces-fips. us-gov-east-1. 亞馬遜
工作階段中介裝置 (PCM)	網域： • https://skylight-cm. us-gov-east-1. 亞馬遜 • 網址：//skylight-cm-fips。 us-gov-east-1. 亞馬遜
運作狀態檢查主機名稱	drp-osu.amazonworkspaces.com
運作狀態檢查 IP 位址	• 18.253.251.70 • 18.254.0.118
PCoIP 閘道伺服器公用 IP 位址範圍	• 18.254.140.0-18.254.143.255
WSP 閘道伺服器 IP 位址範圍	18.254.148.0/22
WSP 閘道網域名稱	*.prod。 us-gov-east-1. 高地兰德. aw.a2z.com
管理介面 IP 位址範圍	• 198.19.0.0/16 • WSP：10.0.0.0/8

Amazon WorkSpaces 用戶端網路需求

WorkSpaces 使用者可以使用支援裝置的用戶端應用程式來連線至其 WorkSpaces。或者，他們也可使用 Web 瀏覽器來連線至支援此存取形式的 WorkSpaces。如需支援 Web 瀏覽器存取的 WorkSpaces 清單，請參閱「哪些 Amazon WorkSpaces 套件支援 Web 存取？」(出自用戶端存取、Web 存取和使用者體驗)。

> **Note**
>
> Web 瀏覽器無法用於連線至 Amazon Linux WorkSpaces。

> **Important**
>
> 自 2020 年 10 月 1 日起，客戶無法再使用 Amazon WorkSpaces Web Access 用戶端來連線到 Windows 7 自訂 WorkSpaces 或 Windows 7 自帶授權 (BYOL) WorkSpaces。

若要為使用者提供 WorkSpaces 的良好體驗，請確認其用戶端裝置符合下列網路需求：

- 用戶端裝置必須具有寬頻網際網路連線。我們建議您為同時觀看 480p 視訊視窗的每位使用者規劃至少 1 Mbps。視使用者對視訊解析度的品質需求而定，可能需要更多頻寬。
- 用戶端裝置所連線的網路，以及用戶端裝置上的任何防火牆，都必須對各種 AWS 服務的 IP 位址範圍開啟特定連接埠。如需詳細資訊，請參閱 的 IP 位址和連接埠需求 WorkSpaces。
- 為了獲得最佳的 PCoIP 效能，從用戶端網路到 WorkSpaces 所在區域的往返時間 (RTT) 應小於 100 毫秒。如果 RTT 介於 100 毫秒到 200 毫秒之間，則使用者可以存取 WorkSpace，但效能會受到影響。如果 RTT 介於 200 毫秒至 375 毫秒之間，則效能會降低。如果 RTT 超過 375 毫秒，則會終止 WorkSpaces 用戶端連線。

  為了獲得 WorkSpaces 串流協定 (WSP) 的最佳效能，從用戶端網路到 WorkSpaces 所在區域的 RTT 應小於 250 毫秒。如果 RTT 介於 250 毫秒到 400 毫秒之間，則使用者可以存取 WorkSpace，但效能會降低。

  若要檢查從您所在位置到各個 AWS 區域的 RTT，請使用 Amazon WorkSpaces 連線運作狀態檢查。
- 若要搭配 WSP 使用網路攝影機，我們建議上傳頻寬下限為每秒 1.7 MB。
- 如果使用者將透過虛擬私有網路 (VPN) 存取其 WorkSpaces，則連線必須支援至少 1200 個位元組的最大傳輸單元 (MTU)。

  > **Note**
  >
  > 您無法透過連線至您虛擬私有雲端 (VPC) 的 VPN 來存取 WorkSpaces。若要使用 VPN 存取 WorkSpaces，則需要網際網路連線 (透過 VPN 的公用 IP 位址)，如 的 IP 位址和連接埠需求 WorkSpaces 所述。

- 用戶端需要 HTTPS 存取由服務和 Amazon Simple Storage Service (Amazon S3) 託管的 WorkSpaces 資源。用戶端不支援應用程式層級的 Proxy 重新導向。需有 HTTPS 存取權，使用者才能成功完成註冊並存取其 WorkSpaces。

- 若要允許從 PCoIP 零用戶端裝置存取，您必須使用 WorkSpaces 的 PCoIP 通訊協定套件。您還必須在 Teradici 中啟用網路時間協定 (NTP)。如需詳細資訊，請參閱 為 WorkSpaces 設定 PCoIP 零用戶端。
- 對於 3.0+ 的用戶端，如果您使用 Amazon WorkDocs 的單一登入 (SSO)，則必須遵循《AWS Directory Service 管理指南》的單一登入中的指示。

您可以驗證用戶端裝置是否符合網路需求，如下所示。

驗證 3.0+ 用戶端的網路需求

1. 開啟您的 WorkSpaces 用戶端。如果這是您第一次開啟用戶端，系統會提示您輸入在邀請電子郵件中收到的註冊碼。
2. 視您使用的用戶端而定，執行下列其中一項操作。

如果您使用的是...	執行此作業
Windows 或 Linux 用戶端	在用戶端應用程式的右上角，選取網路圖示
macOS 用戶端	選擇連線、網路。

   用戶端應用程式會測試網路連線、連接埠和往返時間，並報告這些測試的結果。
3. 關閉網路對話方塊以返回登入頁面。

驗證 1.0+ 和 2.0+ 用戶端的網路需求

1. 開啟您的 WorkSpaces 用戶端。如果這是您第一次開啟用戶端，系統會提示您輸入在邀請電子郵件中收到的註冊碼。
2. 選擇用戶端應用程式右下角的網路。用戶端應用程式會測試網路連線、連接埠和往返時間，並報告這些測試的結果。
3. 選擇關閉以返回登入頁面。

限制對 WorkSpaces 受信任設備的訪問

默認情況下，用戶可以 WorkSpaces 從連接到互聯網的任何支持設備訪問他們的。如果貴公司限制對信任裝置 (也稱為受管理裝置) 的公司資料存取，您可以使用有效的憑證來限制對受信任裝置的 WorkSpaces 存取。

啟用此功能時， WorkSpaces 會使用憑證型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。

對於每個目錄，您最多可以匯入兩個根憑證。如果您匯入兩個根憑證，則會將它們同時 WorkSpaces 提供給用戶端，而用戶端會找到第一個鏈結到其中一個根憑證的有效相符憑證。

支援的用戶端

- Android，在 Android 或與 Android 系統相容的 Chrome 作業系統上執行
- macOS
- Windows

> **Important**
>
> 下列用戶端不支援此功能：
>
> - WorkSpaces 用戶端應用程 iPad
> - 第三方用戶端，包括但不限於 Terdici PCoIP、RDP 用戶端和遠端桌面應用程式。

> **Note**
>
> 當您啟用特定用戶端的存取權時，請確定您封鎖其他不需要裝置類型的存取。有關如何執行此操作的詳細資訊，請參閱下面的步驟 3.7。

步驟 1：建立憑證

此功能需要兩種類型的憑證：由內部憑證授權機構 (CA) 產生的根憑證，以及鏈結至根憑證的用戶端憑證。

要求

- 根憑證必須是 CRT、CERT 或 PEM 格式的 Base64 編碼憑證檔案。
- 根憑證必須符合下列規則運算式模式，也就是說，除了最後一行以外，每一個編碼行的長度都必須剛好是 64 個字元：`-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64}\u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`。
- 裝置憑證必須包含通用名稱。
- 裝置憑證必須包含下列副檔名：`Key Usage: Digital Signature` 和 `Enhanced Key Usage: Client Authentication`。
- 從裝置憑證到信任的根憑證授權機構的鏈結中的所有憑證都必須安裝在用戶端裝置上。
- 憑證鏈結支援的長度上限為 4。
- WorkSpaces 目前不支援用戶端憑證的裝置撤銷機制，例如憑證撤銷清單 (CRL) 或線上憑證狀態通訊協定 (OCSP)。
- 使用強大的加密演算法。我們建議使用 SHA256 結合 RSA、SHA256 結合 ECDSA、SHA384 結合 ECDSA 或 SHA512 結合 ECDSA。
- 對於 macOS，如果裝置憑證位於系統鑰匙圈中，建議您授權用 WorkSpaces 戶端應用程式存取這些憑證。否則，使用者必須在登入或重新連線時輸入鑰匙圈憑證。

步驟 2：將用戶端憑證部署到信任的裝置

在使用者的信任裝置上，您必須安裝憑證套件，其中包含從裝置憑證到信任的根憑證授權機構的鏈結中的所有憑證。您可以使用偏好的解決方案將憑證安裝到用戶端裝置機群；例如，系統中心組態管理員 (SCCM) 或行動裝置管理 (MDM)。請注意，SCCM 和 MDM 可以選擇性地執行安全狀態評估，以判斷裝置是否符合貴公司的存取政策。 WorkSpaces

用 WorkSpaces 戶端應用程式會搜尋憑證，如下所示：

- Android - 移至設定，選擇安全性和位置、憑證，然後選擇從 SD 卡安裝。
- Android 相容的 Chrome 作業系統 - 開啟 Android 設定，選擇安全性和位置、憑證，然後選擇從 SD 卡安裝。
- macOS - 在鑰匙圈中搜尋用戶端憑證。
- Windows - 在使用者和根憑證存放區中搜尋用戶端憑證。

步驟 3：設定限制

在信任的裝置上部署用戶端憑證之後，您可以在目錄層級啟用限制存取。這需要用 WorkSpaces 戶端應用程式先驗證裝置上的憑證，然後再允許使用者登入 WorkSpace.

若要設定限制

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選取目錄，然後依序選擇動作、更新詳細資訊。
4. 展開存取控制選項。
5. 在 [針對每個裝置類型] 下，指定可存取的裝置 WorkSpaces，選擇 [受信任的裝置]。
6. 匯入最多兩個根憑證。針對每個根憑證，執行下列操作：
   a. 選擇匯入。
   b. 將憑證主體複製到表單。
   c. 選擇匯入。
7. 指定其他類型的裝置是否可以存取 WorkSpaces。
   a. 向下捲動至其他平台區段。根據預設， WorkSpaces 系統會停用 Linux 用戶端，使用者可以 WorkSpaces 從他們的 iOS 裝置、安卓裝置、網頁存取、Chromebook 和 PCoIP 零用戶端裝置存取這些用戶端。
   b. 選取要啟用的裝置類型，並清除要停用的裝置類型。
   c. 若要封鎖來自所有所選裝置類型的存取，請選擇封鎖。
8. 選擇更新並結束。

WorkSpaces 與 SAML 2.0 整合

將 SAML 2.0 與您的 WorkSpaces 進行桌面工作階段驗證整合，可讓使用者透過其預設網頁瀏覽器使用其現有的 SAML 2.0 身分提供者 (IdP) 認證和驗證方法。藉由使用 IdP 來驗證 WorkSpaces 的使用者，您可運用 IdP 功能 (例如多因素驗證和關聯式存取政策) 來保護 WorkSpaces。

身分驗證工作流程

下列各節說明 WorkSpaces 用戶端應用程式、WorkSWorkSpaces Web Access 及 SAML 2.0 身分提供者 (IdP) 所起始的驗證工作流程：

- 由 IdP 初始化流程時。例如，當使用者在網頁瀏覽器的 IdP 使用者入口網站中選擇應用程式時。
- 由 WorkSpaces 用戶端起始流程時。例如，當使用者開啟用戶端應用程式並登入時。
- 由 WorkSpaces Web Access 起始流程時。例如，當使用者在瀏覽器中開啟 Web 存取並登入時。

在這些範例中，使用者輸入 `user@example.com` 以登入 IdP。IdP 具有針對 WorkSpaces 目錄設定的 SAML 2.0 服務提供者應用程式，而且使用者已獲得 WorkSpaces SAML 2.0 應用程式的授權。使用者會在啟用 SAML 2.0 驗證的目錄中，針對其使用者名稱建立 WorkSpace (`user`)。此外，使用者在其裝置上安裝 WorkSpaces 用戶端應用程式，或使用者在網頁瀏覽器中使用 Web Access。

身分提供者 (IdP) 起始的流程搭配用戶端應用程式

IdP 起始的流程可讓使用者在其裝置上自動註冊 WorkSpaces 用戶端應用程式，而不必輸入 WorkSpaces 註冊碼。使用者不會使用 IDP 起始的流程登入其 WorkSpaces。WorkSpaces 驗證必須源自用戶端應用程式。

1. 使用者可使用其網頁瀏覽器來登入 IdP。
2. 登入 IdP 後，使用者會從 IdP 使用者入口網站選擇 WorkSpaces 應用程式。
3. 使用者會在瀏覽器中重新導向至此頁面，且 WorkSpaces 用戶端應用程式會自動開啟。

4. WorkSpaces 用戶端應用程式現已註冊，使用者可按一下繼續登入 WorkSpaces 來繼續登入。

身分提供者 (IdP) 起始的流程搭配 Web Access

IdP 起始的 Web Access 流程可讓使用者透過網頁瀏覽器自動註冊其 WorkSpaces，而不必輸入 WorkSpaces 註冊碼。使用者不會使用 IDP 起始的流程登入其 WorkSpaces。WorkSpaces 驗證必須源自 Web Access。

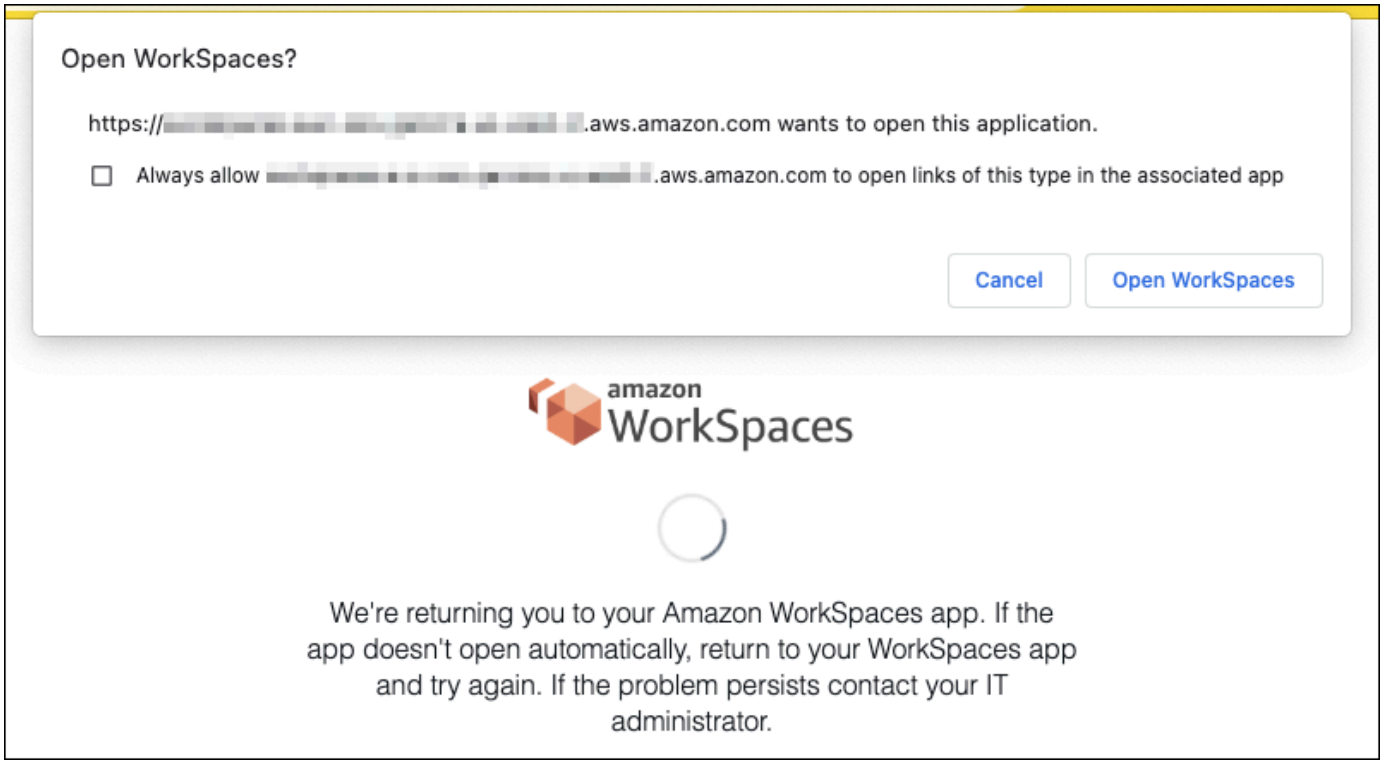
1. 使用者可使用其網頁瀏覽器來登入 IdP。
2. 登入 IdP 後，使用者會從 IdP 使用者入口網站按一下 WorkSpaces 應用程式。
3. 使用者會在瀏覽器中重新導向至此頁面。若要開啟 WorkSpaces，請在瀏覽器中選擇 Amazon WorkSpaces。

4. WorkSpaces 用戶端應用程式現已註冊，使用者可透過 WorkSpaces Web Access 繼續登入。

WorkSpaces 用戶端起始的流程

用戶端起始的流程可讓使用者在登入 IdP 後登入其 WorkSpaces。

1. 使用者啟動 WorkSpaces 用戶端應用程式 (如果尚未執行)，然後按一下繼續登入 WorkSpaces。
2. 系統會將使用者重新導向至其預設網頁瀏覽器，以登入 IdP。如果使用者已在其瀏覽器中登入 IdP，則不需要再次登入，而且會略過此步驟。
3. 登入 IdP 後，使用者會被重新導向至快顯視窗。遵循提示，允許您的網頁瀏覽器開啟用戶端應用程式。



4. 使用者已被重新導向至 WorkSpaces 用戶端應用程式，以完成其 WorkSpace 登入。WorkSpaces 使用者名稱會自動從 IdP SAML 2.0 聲明填入。當您使用憑證型驗證 (CBA) 時，使用者會自動登入。
5. 使用者已登入其 WorkSpace。

WorkSpaces Web 存取起始的流程

Web Access 起始的流程可讓使用者在登入 IdP 後登入其 WorkSpaces。

1. 使用者會啟動 WorkSpaces Web Access，然後選擇登入。
2. 在相同的瀏覽器索引標籤中，使用者會重新導向至 IdP 入口網站。如果使用者已在其瀏覽器中登入 IdP，則不需要再次登入，而且可略過此步驟。
3. 登入 IdP 後，使用者會在瀏覽器中重新導向至此頁面，然後按一下登入 WorkSpaces。
4. 使用者已被重新導向至 WorkSpaces 用戶端應用程式，以完成其 WorkSpace 登入。WorkSpaces 使用者名稱會自動從 IdP SAML 2.0 聲明填入。當您使用憑證型驗證 (CBA) 時，使用者會自動登入。
5. 使用者已登入其 WorkSpace。

設定 SAML 2.0

使用 SAML 2.0 身分識別提供者 (IdP) 認證和驗證方法，使用 SAML 2.0 身分識別提供者 (IdP) 認證和驗證方法， WorkSpaces 為您的使用者啟用用 WorkSpaces 戶端應用程式註冊和登入。若要使用 SAML 2.0 設定聯合身分，請使用 IAM 角色和轉送狀態 URL 來設定 IdP 並啟用 AWS。這會授予您的同盟使用者存取 WorkSpaces 目錄的權限。轉送狀態是 WorkSpaces指使用者成功登入後要轉送到的目錄端點 AWS。

目錄

要求

- SAML 2.0 驗證適用於下列區域：
  - 美國東部 (維吉尼亞北部) 區域
  - 美國西部 (奧勒岡) 區域
  - 非洲 (開普敦) 區域
  - 亞太 (孟買) 區域
  - 亞太 (首爾) 區域
  - 亞太區域 (新加坡) 區域
  - 亞太 (雪梨) 區域
  - 亞太 (東京) 區域
  - 加拿大 (中部) 區域
  - 歐洲 (法蘭克福) 區域
  - 歐洲 (愛爾蘭) 區域

  - 歐洲 (倫敦) 區域
  - 南美洲 (聖保羅) 區域
  - 以色列 (特拉維夫) 區域
  - AWS GovCloud (美國西部)
  - AWS GovCloud (美國東部)
- 若要搭配使用 SAML 2.0 驗證 WorkSpaces，IdP 必須支援具有深層連結目標資源或轉送狀態端點 URL 的來路不明的 IDP 起始 SSO。範例 IdPs 包括 ADFS、Azure AD、雙核單一登入、確認和. PingFederate PingOne 如需詳細資訊，請參閱 IdP 文件。
- SAML 2.0 驗證可在使用 Simple AD WorkSpaces 啟動時運作，但不建議這樣做，因為 Simple AD 未與 SAML 2.0 整合。 IdPs
- 下列 WorkSpaces 用戶端支援 SAML 2.0 驗證。其他用戶端版本不支援 SAML 2.0 驗證。開啟 Amazon WorkSpaces 用戶端下載以尋找最新版本：
  - Windows 用戶端應用程式 5.1.0.3029 版或更新版本
  - macOS 用戶端 5.x 版或更新版本
  - 適用於版本 2024.1 或更高版本的 Linux 用戶端
  - Web Access

  除非啟用後援，否則其他用戶端版本將無法連線到 WorkSpaces 已啟用的 SAML 2.0 驗證。如需詳細資訊，請參閱在 WorkSpaces 目錄上啟用 SAML 2.0 驗證。

step-by-step 如需將 SAML 2.0 與 WorkSpaces 使用 ADFS、Azure AD、雙核心單一登入、Okta 以 PingFederate 及企業版整合的指示 OneLogin，請 PingOne 參閱 Amazon WorkSpaces SAML 驗證實作指南。

必要條件

在設定目錄的 SAML 2.0 身分識別提供者 (IdP) 連線之前，請先完成下列先決條件 WorkSpaces 。

1. 將您的 IdP 設定為整合來自與目錄搭配使用的 Microsoft 作用中目錄中的使用者身分識別。WorkSpaces 對於具有的使用者 WorkSpace，Active Directory 使用者的 SAM AccountName 和電子郵件屬性和 SAML 宣告值必須相符，使用者才能 WorkSpaces 使用 IdP 登入。如需有關整合 Active Directory 與 IdP 的詳細資訊，請參閱您的 IdP 文件。
2. 設定 IdP 來與 AWS建立信任關係

- AWS如需設定聯合的詳細資訊，請參閱整合 AWS 協力廠商 SAML 解決方案提供者。相關範例包括與 AWS IAM 整合的 IdP，以存取 AWS 管理主控台。
- 使用 IdP 來產生並下載聯合中繼資料文件，以將您的組織描述為 IdP。這份簽章的 XML 文件是用來建立轉送方信任關係。請將這個檔案儲存到日後可從 IAM 主控台存取更新版本的位置。

3. 使用 WorkSpaces 管理主控台建立或註冊目錄。 WorkSpaces 如需詳細資訊，請參閱管理的目錄 WorkSpaces。下列目錄類型支援的 SAML 2.0 驗證： WorkSpaces

   - AD Connector
   - AWS 管理 Microsoft AD

4. WorkSpace 為可以使用支援的目錄類型登入 IdP 的使用者建立。您可以使 WorkSpace 用 WorkSpaces 管理主控台 AWS CLI或 WorkSpaces API 建立。如需詳細資訊，請參閱使用啟動虛擬桌面 WorkSpaces。

步驟 1：在 AWS IAM 中建立 SAML 身分識別提供者

首先，在 AWS IAM 中建立 SAML IdP。此 IdP 使用組織中的 IdP 軟體所產生的中繼資料文件，定義組織的 IdP 至AWS 信任關係。如需詳細資訊，請參閱建立和管理 SAML 身分提供者 (Amazon Web Services 管理主控台)。如需 IdPs 在 AWS GovCloud (美國西部) 和 AWS GovCloud (美國東部) 中使用 SAML 的相關資訊，請參閱 AWS Identity and Access Management。

步驟 2：建立 SAML 2.0 聯合 IAM 角色

接下來，建立 SAML 2.0 聯合 IAM 角色。此步驟會建立 IAM 與組織 IdP 之間的信任關係，以便將您的 IdP 識別為聯合信任的實體。

為 SAML IdP 建立 IAM 角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 角色、建立角色。
3. 針對 Role type (角色類型)，選擇 SAML 2.0 federation (SAML 2.0 聯合)。
4. 針對 SAML 提供者，選取您建立的 SAML IdP。

> **Important**
>
> 請勿選擇兩種 SAML 2.0 存取方法 (僅允許以程式設計的方式存取或允許以程式設計方式存取和 Amazon Web Services 管理主控台存取) 的任何一種。

5. 針對 Attribute (屬性)，選擇 SAML:sub_type。
6. 針對值輸入 `persistent`。此值會將角色存取限制為 SAML 使用者串流請求，其中包括 SAML 主旨類型聲明與持久值。如果 SAML:sub_type 為持久性，您的 IdP 就會針對來自特定使用者之所有 SAML 請求中的 NameID 元素，傳送相同的唯一值。如需有關 SAML: sub_type 宣告的詳細資訊，請參閱 < 使用 SAML 型聯合以 SAML 為基礎的聯合來存取 API 中的唯一識別使用者 > 一節。 AWS
7. 檢閱您的 SAML 2.0 信任資訊，確認信任實體和條件無誤，然後選擇 Next: Permissions (下一步：許可)。
8. 在 Attach permissions policies (連接許可政策) 頁面上，選擇 Next: Tags (下一步：標籤)。
9. (選用) 為您要新增的每個標籤輸入索引鍵和值。如需詳細資訊，請參閱標記 IAM 使用者和角色。
10. 完成後，請選擇 Next: Review (下一步：檢閱)。您稍後可為此角色建立並嵌入內嵌政策。
11. 針對角色名稱，輸入可識別此角色用途的名稱。因為有多個實體可能會參考此角色，所以建立角色後，您就無法編輯其名稱。
12. (選用) 在 Role description (角色說明) 中，輸入新角色的說明。
13. 檢閱角色詳細資訊，並選擇 Create role (建立角色)。
14. 將 sts: TagSession 權限新增至新 IAM 角色的信任政策。如需詳細資訊，請參閱在 AWS STS中傳入工作階段標籤。在新 IAM 角色的詳細資訊中，選擇信任關係索引標籤，然後選擇編輯信任關係。當編輯信任關係原則編輯器開啟時，新增 sts: TagSession * 權限，如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
```

```
    }]
}
```

以您在步驟 1 建立的 SAML IdP 名稱取代 `IDENTITY-PROVIDER`。然後選擇更新信任政策。

步驟 3：為 IAM 角色嵌入內嵌政策

接下來，為您建立的角色嵌入內嵌 IAM 政策。嵌入內嵌政策時，該政策中的許可不得意外附加至錯誤的主體實體。內嵌原則可讓聯合身分使用者存取目 WorkSpaces 錄。

> **Important**
>
> 此動作不支援 AWS 根據來源 IP 管理存取權的 IAM 政`workspaces:Stream`策。若要管理的 IP 存取控制 WorkSpaces，請使用 IP 存取控制群組。此外，使用 SAML 2.0 驗證時，您可以使用 IP 存取控制原則 (如果可從 SAML 2.0 IdP 取得)。

1. 在您建立的 IAM 角色的詳細資訊中，選擇許可索引標籤，然後將必要的許可新增至角色的許可政策。建立政策精靈將會啟動。
2. 在建立政策中，選擇 JSON 索引標籤。
3. 將下列 JSON 政策複製並貼入 JSON 視窗。然後，輸入您的 AWS 區域代碼、帳號 ID 和目錄 ID 來修改資源。在下列原則中，`"Action": "workspaces:Stream"`是為 WorkSpaces 使用者提供連線至 WorkSpaces 目錄中其桌面工作階段之權限的動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
```

```
        }
    ]
}
```

`REGION-CODE`以 WorkSpaces目錄所在的 AWS 區域取代。取代`DIRECTORY-ID`為可在 WorkSpaces 管理主控台中找到的 WorkSpaces 目錄 ID。對於 AWS GovCloud (美國西部) 或 AWS GovCloud (美國東部) 的資源，ARN 使用下列格式：`arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`

4. 完成時，請選擇 Review policy (檢閱政策)。政策檢查工具會回報任何語法錯誤。

步驟 4：設定 SAML 2.0 身分提供者

接下來，視您的 SAML 2.0 IdP 而定，您可能需要手動更新 IdP 以信任 AWS 身為服務提供者，方法是將此`saml-metadata.xml`檔案上傳至 https://signin.aws.amazon.com/static/saml-metadata.xml 至您的 IdP。此步驟會更新您的 IdP 中繼資料。對於某些人來說 IdPs，更新可能已經配置。如果是這種情況，請繼續下一個步驟。

如果您的 IdP 尚未設定這項更新，請檢閱 IdP 提供的文件以取得中繼資料更新方式的資訊。有些供應商會提供輸入 URL 的選項，由 IdP 為您取得並安裝檔案。另一些提供者則要求您從該 URL 處下載檔案，然後將其做為本機檔案提供。

> **Important**
>
> 此時，您也可以授權 IdP 中的使用者存取您在 IdP 中設定的 WorkSpaces應用程式。獲得授權存取您目錄之 WorkSpaces 應用程式的使用者不會自動為他們 WorkSpace 建立。同樣地，為其 WorkSpace 建立的使用者不會自動獲得存取應用 WorkSpaces 程式的授權。若要成功連線至 WorkSpace 使用 SAML 2.0 驗證，使用者必須獲得 IdP 的授權，且必須具有已建立 WorkSpace的驗證。

步驟 5：建立 SAML 身分驗證回應聲明

接下來，在 IdP 的驗證回應中設定 AWS 為 SAML 屬性傳送的資訊。根據您的 IdP，這已經設定完成，請略過此步驟並繼續進行步驟 6：設定聯合的轉送狀態。

如果您的 IdP 尚未設定這項資訊，請提供下列項目：

- SAML 主旨 NameID：進行登入之使用者的唯一識別碼。此值必須與 WorkSpaces 使用者名稱相符，而且通常是使用中目錄使用者的 SAM AccountName 屬性。
- SAML 主旨類型 (值設定為 `persistent`)：將值設定為 `persistent`，可確保您的 IdP 會針對來自特定使用者之所有 SAML 請求中的 `NameID` 元素，傳送相同的唯一值。確保 IAM 政策包含一個條件，僅允許 SAML sub_type 設為 `persistent` 的 SAML 請求，如步驟 2：建立 SAML 2.0 聯合 IAM 角色所述。
- **Name** 屬性設為 **`https://aws.amazon.com/SAML/Attributes/Role`** 的 **Attribute** 元素：此元素包含一或多個 `AttributeValue` 元素，其列出您 IdP 將使用者對應至的 IAM 角色和 SAML IdP。角色和 IdP 會指定為以逗號分隔的 ARN 對。預期值的範例是 `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`。
- **AttributeName**屬性設定為的元素 `https://aws.amazon.com/SAML/Attributes/RoleSessionName` — 此元素包含一個`AttributeValue`元素，可為針對 SSO 發出的 AWS 暫時認證提供識別碼。`AttributeValue` 元素中的值長度必須介於 2 到 64 個字元之間，只能包含字母數位字元、底線和以下字元：_ . : / = + - @。不可含有空格。此值通常是電子郵件地址或使用者主體名稱 (UPN)。該值不得包含空格，例如使用者的顯示名稱。
- **Name** 屬性設為 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** 的 **Attribute** 元素：此元素包含一個可提供使用者電子郵件地址的 `AttributeValue` 元素。此值必須符合 WorkSpaces 目錄中定義的 WorkSpaces 使用者電子郵件地址。標籤值可包含字母、數字、空格和 _ . : / = + - @ 字元的組合。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 和 AWS STS的標記規則。
- **Name** 屬性設為 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** 的 **Attribute** 元素 (選用)：此元素包含一個 `AttributeValue` 元素，該元素可為正在登入的使用者提供 Active Directory `userPrincipalName`。此值必須以 `username@domain.com` 格式提供。此參數與憑證型驗證搭配使用，做為終端使用者憑證中的主體替代名稱。如需詳細資訊，請參閱憑證型驗證。
- **Name** 屬性設為 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** 的 **Attribute** 元素 (選用)：此元素包含一個 `AttributeValue` 元素，該元素可為正在登入的使用者提供 Active Directory 安全識別碼 (SID)。此參數與憑證型驗證搭配使用，能夠強式對應至 Active Directory 使用者。如需詳細資訊，請參閱憑證型驗證。
- **Name** 屬性設為 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** 的 **Attribute**元素 (選用)：此元素包含一個可提供替代使用者名稱格式的 `AttributeValue` 元素。如果您有使用案例需要使用者名稱格式 (例如`corp\username`、或使用用 WorkSpaces 戶端登`username@corp.example.com`入)`corp.example.com\username`，請使用此屬性。標

鑰索引鍵和值可以包含字母、數字、空格和 _ : / . + = @ - 字元的任意組合。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 和 AWS STS的標記規則。若要宣告 corp\username 或 corp.example.com\username 格式，請在 SAML 聲明中以 / 取代 \。

- **AttributeName**屬性設定為 https://aws.amazon.com/SAML/Attributes/:Domain 的元素 PrincipalTag (選用) — 此元素包含一個元素，AttributeValue可為使用者登入提供作用中目錄 DNS 完整網域名稱 (FQDN)。當使用者的 Active Directory userPrincipalName 包含替代尾碼時，此參數會與憑證型驗證搭配使用。此值必須以 domain.com 提供，包括任何子網域。
- **AttributeName**屬性設定為 https://aws.amazon.com/SAML/Attributes/ 的元素 SessionDuration (選用) — 此元素包含一個**AttributeValue**元素，指定使用者的聯合串流工作階段在需要重新驗證之前可保持作用中的時間上限。預設值為 3600 秒 (60 分鐘)。如需詳細資訊，請參閱 SAML SessionDurationAttribute。

> **Note**
>
> 雖然 SessionDuration 是選用屬性，但我們建議您將它包含在 SAML 回應中。如果您未指定此屬性，工作階段持續時間會設定為預設值 3600 秒 (60 分鐘)。 WorkSpaces 桌面工作階段會在工作階段持續時間到期後中斷

如需有關如何設定這些元素的詳細資訊，請參閱《IAM 使用者指南》的針對身分驗證回應設定 SAML 聲明。如需 IdP 的特定組態需求相關資訊，請參閱您的 IdP 文件。

步驟 6：設定聯合的轉送狀態

接下來，使用 IdP 來設定同盟的轉送狀態，以指向 WorkSpaces 目錄轉送狀態 URL。成功驗證之後 AWS，使用者會被導向至 WorkSpaces 目錄端點，該端點定義為 SAML 驗證回應中的轉送狀態。

以下是轉送狀態 URL 格式：

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

從 WorkSpaces 目錄註冊碼以及與目錄所在區域相關聯的轉送狀態端點建構轉送狀態 URL。註冊碼可以在 WorkSpaces 管理主控台中找到。

或者，如果您要使用跨區域重新導向 WorkSpaces，您可以使用與主要區域和容錯移轉區域中目錄相關聯的完整網域名稱 (FQDN) 來取代註冊代碼。如需詳細資訊，請參閱 Amazon WorkSpaces 的跨區域重新導向。使用跨區域重新導向和 SAML 2.0 驗證時，必須使用與每個區域相關聯的轉送狀態端點，針

對 SAML 2.0 驗證啟用主要目錄和容錯移轉目錄並與 IdP 獨立設定。這將允許在使用者在登入前註冊其用 WorkSpaces 戶端應用程式時正確設定 FQDN，並允許使用者在容錯移轉事件期間進行驗證。

下表列出提供 WorkSpaces SAML 2.0 驗證之區域的轉送狀態端點。

可使用 WorkSpaces SAML 2.0 驗證的地區

區域	轉送狀態端點
美國東部 (維吉尼亞北部) 區域	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
美國西部 (奧勒岡) 區域	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-west-2.aws.amazon.com
非洲 (開普敦) 區域	workspaces.euc-sso.af-south-1.aws.amazon.com
亞太 (孟買) 區域	workspaces.euc-sso.ap-south-1.aws.amazon.com
亞太 (首爾) 區域	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
亞太 (新加坡) 區域	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
亞太 (雪梨) 區域	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
亞太 (東京) 區域	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
加拿大 (中部) 區域	workspaces.euc-sso.ca-central-1.aws.amazon.com

區域	轉送狀態端點
歐洲 (法蘭克福) 區域	workspaces.euc-sso.eu-central-1.aws.amazon.com
歐洲 (愛爾蘭) 區域	workspaces.euc-sso.eu-west-1.aws.amazon.com
歐洲 (倫敦) 區域	workspaces.euc-sso.eu-west-2.aws.amazon.com
南美洲 (聖保羅) 區域	workspaces.euc-sso.sa-east-1.aws.amazon.com
以色列 (特拉維夫) 區域	工作空間. 歐洲-中央 -1.aws.aws.az
AWS GovCloud (美國西部)	• workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** 如需詳細資訊，請參閱 AWS GovCloud (美國) 使用者指南 WorkSpaces中的 Amazon。

區域	轉送狀態端點
AWS GovCloud (美國東部)	• workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** 如需詳細資訊，請參閱 AWS GovCloud (美國) 使用者指南 WorkSpaces中的 Amazon。

步驟 7：在您的目錄上啟用與 SAML 2.0 的 WorkSpaces 整合

您可以使用主 WorkSpaces 控台在 WorkSpaces 目錄上啟用 SAML 2.0 驗證。

啟用與 SAML 2.0 的整合

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選擇您的目錄 ID WorkSpaces。
4. 在驗證之下選擇編輯。
5. 選擇編輯 SAML 2.0 身分提供者。
6. 核取啟用 SAML 2.0 身分驗證。
7. 對於使用者存取 URL 和 IdP 深層連結參數名稱，輸入適用於您的 IdP 和您在步驟 1 中設定之應用程式的值。如果省略此參數，IdP 深層連結參數名稱的預設值為 RelayState「"。下表列出的使用者存取 URL 和參數名稱對應用程式的各種身分提供者而言是唯一的。

   要新增至允許清單的網域和 IP 地址

身分提供者	參數	使用者存取 URL
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiateds`

身分提供者	參數	使用者存取 URL
		ignon.aspx?RelaySt ate=RPID=<relaying -party-uri>
Azure AD	RelayState	https://myapps.mic rosoft.com/signin/ <app_id>?tenantId= <tenant_id>
Duo 單一登入	RelayState	https://<sub-domai n>.sso.duosecurity .com/saml2/sp/<app _id>/sso
Okta	RelayState	https://<sub_domai n>.okta.com/app/<a pp_name>/<app_id>/ sso/saml
OneLogin	RelayState	https://<sub-domai n>.onelogin.com/tr ust/saml2/http-pos t/sso/<app-id>
JumpCloud	RelayState	https://sso.jumpcl oud.com/saml2/<app -id>
Auth0	RelayState	https://<DefaultTe natName>.us.auth0. com/samlp/<Client_ Id>
PingFederate	TargetResource	https://<host>/idp /startSSO.ping?Par tnerSpId=<sp_id>

身分提供者	參數	使用者存取 URL
PingOne 適用於企業	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

使用者存取 URL 通常是由未經要求 IdP 起始 SSO 的提供者所定義。使用者可以在 Web 瀏覽器中輸入此 URL，直接與 SAML 應用程式聯合。若要測試 IdP 的使用者存取 URL 和參數值，請選擇測試。將測試 URL 複製並貼到目前瀏覽器或其他瀏覽器中的私人視窗，以測試 SAML 2.0 登入，而不會中斷目前的 AWS 管理主控台工作階段。當 IDP 起始的 WorkSpaces 流程開啟時，您可以註冊用戶端。如需詳細資訊，請參閱身分提供者 (IdP) 起始的流程。

8. 核取或取消核取允許不支援 SAML 2.0 的用戶端登入來管理後援設定。啟用此設定可繼續為您的使用者提供 WorkSpaces 使用不支援 SAML 2.0 的用戶端類型或版本的存取權，或者使用者需要時間升級至最新的用戶端版本。

   > **Note**
   >
   > 此設定可讓使用者略過 SAML 2.0，並使用採用較舊用戶端版本的目錄驗證進行登入。

9. 若要搭配 Web 用戶端使用 SAML，請啟用 Web Access。如需詳細資訊，請參閱啟用和設定 Amazon WorkSpaces 網路存取。

   > **Note**
   >
   > Web Access 不支援採用 SAML 的 PCoIP。

10. 選擇儲存。您的 WorkSpaces 目錄現在已透過 SAML 2.0 整合啟用。您可以使用 IDP 起始和用戶端應用程式啟動的流程來註冊用 WorkSpaces 戶端應用程式並登入。 WorkSpaces

設定憑證型驗證

您可以使用憑證型驗證 WorkSpaces 來移除 Active Directory 網域密碼的使用者提示。使用憑證型身分驗證搭配 Active Directory 網域，您可以：

- 依賴 SAML 2.0 身分提供者來驗證使用者，並提供 SAML 聲明以比對 Active Directory 中的使用者。

- 賦予較少使用者提示的單一登入體驗。
- 使用 SAML 2.0 身分提供者啟用無密碼驗證流程。

憑證型驗證會使用您帳戶中的 AWS Private CA AWS 資源。 AWS Private CA 允許建立私有憑證授權單位 (CA) 階層，包括根 CA 和從屬 CA。使用時 AWS Private CA，您可以建立自己的 CA 階層，並發行憑證以驗證內部使用者。如需詳細資訊，請參閱 AWS Private Certificate Authority 使用者指南。

使用 AWS Private CA 憑證型驗證時， WorkSpaces 會在工作階段驗證期間自動為您的使用者要求憑證。使用者會使用隨著憑證佈建的虛擬智慧卡，對 Active Directory 進行驗證。

使用最新 WorkSpaces 網頁存取、Windows WorkSpaces 和 macOS 用戶端應用程式的 Windows WorkSpaces 串流通訊協定 (WSP) 服務包支援憑證型驗證。開啟 Amazon WorkSpaces 用戶端下載以尋找最新版本：

- Windows 用戶端 5.5.0 版或更新版本
- macOS 用戶端 5.6.0 版或更新版本

如需使用 Amazon 設定憑證型身份驗證的詳細資訊 WorkSpaces，請參閱如何為 Amazon 設定憑證型身份驗證和在具有 2.0 WorkSpaces 和的憑證型身份驗證的高度監管環境中設計考量事項。 AppStream WorkSpaces

必要條件

啟用憑證型驗證之前，請先完成下列步驟。

1. 使用 SAML 2.0 整合設定您的 WorkSpaces 目錄，以使用憑證型驗證。如需詳細資訊，請參閱與 SAML 2.0 WorkSpaces 整合。
2. 在您的 SAML 聲明中設定 `userPrincipalName` 屬性。如需詳細資訊，請參閱針對 SAML 驗證回應建立聲明。
3. 在您的 SAML 聲明中設定 `ObjectSid` 屬性。執行強式對應至 Active Directory 使用者時，這是選擇性操作。如果此屬性不符合 SAML_Subject `NameID` 中指定之使用者的 Active Directory 安全識別碼 (SID)，則憑證型驗證將會失敗。如需詳細資訊，請參閱針對 SAML 驗證回應建立聲明。
4. 如果您的 IAM 角色信任政策尚未存在，請將 sts: TagSession 權限新增至與 SAML 2.0 組態搭配使用的 IAM 角色信任政策。需有此許可才能使用憑證型驗證。如需詳細資訊，請參閱建立 SAML 2.0 聯合 IAM 角色。

5. 建立私人憑證授權單位 (CA)， AWS Private CA 如果您沒有使用您的 Active Directory 設定。 AWS Private CA 需要使用憑證型驗證。如需詳細資訊，請參閱規劃 AWS Private CA 部署，並遵循指引設定 CA 以進行憑證型驗證。以下是憑證型驗證使用案例最常見的 AWS Private CA 設定：

   a. CA 類型選項：

      i. 短期憑證 CA 使用模式 (如果您只使用 CA 來發行使用者憑證以進行憑證型驗證，則建議使用)

      ii. 具有根 CA 的單一層級階層 (或者，如果要與現有 CA 階層整合，請選擇次級 CA)

   b. 金鑰演算法選項：RSA 2048

   c. 主體辨別名稱選項：使用任何選項組合來識別 Active Directory 受信任的根憑證授權單位存放區中的 CA。

   d. 憑證撤銷選項：CRL 散發

   > **Note**
   >
   > 憑證型驗證需要可從桌面和網域控制站存取的線上 CRL 散發點。這需要未經驗證存取針對私有 CA CRL 項目設定的 Amazon S3 儲存貯體，或者如果封鎖公用存取，則可存取 S3 儲存貯體的 CloudFront散發。如需這些選項的詳細資訊，請參閱規劃憑證撤銷清單 (CRL)。

6. 使用標題為 `euc-private-ca` 的金鑰來標記您的私有 CA，以指定 CA 來搭配 EUC 憑證型驗證使用。此金鑰不需要值。如需詳細資訊，請參閱管理私有 CA 的標籤。

7. 憑證型驗證會利用虛擬智慧卡進行登入。遵循在 Active Directory 中啟用智慧卡登入第三方憑證授權單位的指導方針，執行下列步驟：

   - 使用網域控制站憑證設定網域控制站，以驗證智慧卡使用者。如果您在 Active Directory 中設定了 Active Directory Certificate Services 企業 CA，網域控制站會使用憑證自動註冊以啟用智慧卡登入。如果您沒有 Active Directory Certificate Services，請參閱來自第三方 CA 的網域控制站憑證需求。您可以使用 AWS Private CA建立網域控制站憑證。如果您這樣做，請勿使用為短期憑證設定的私有 CA。

   > **Note**
   >
   > 如果您正在使用 AWS Managed Microsoft AD，則可以在 EC2 執行個體上設定憑證服務，以滿足網域控制站憑證的需求。如AWS Launch Wizard需使用中目錄憑證服務 AWS Managed Microsoft AD 設定的範例部署，請參閱。 AWS 私有 CA 可以設定為使用中目錄憑證服務 CA 的從屬，也可以在使用 AWS Managed Microsoft AD時設定為其自己的根目錄。

使用 AWS Managed Microsoft AD 和 Active Directory 憑證服務的其他組態工作是建立輸出規則，從控制器 VPC 安全群組到執行憑證服務的 EC2 執行個體，允許 TCP 連接埠 135 和 49152-65535 啟用憑證自動註冊。此外，執行中的 EC2 執行個體必須允許來自網域執行個體 (包括網域控制站) 的相同連接埠上的輸入存取。如需尋找安全性群組的詳細資訊， AWS Managed Microsoft AD 請參閱設定您的 VPC 子網路和安全性群組。

- 在 AWS Private CA 主控台或使用 SDK 或 CLI，選取您的 CA，然後在 CA 憑證下匯出 CA 私有憑證。如需詳細資訊，請參閱匯出私有憑證。
- 將 CA 發佈至 Active Directory。登入網域控制站或已加入網域的電腦。將 CA 私有憑證複製到任何 `<path>\<file>` 並以網域管理員的身分執行下列命令。或者，您可使用群組政策和 Microsoft PKI Health 工具 (PKIView) 來發佈 CA。如需詳細資訊，請參閱設定指示。

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

確定命令已順利完成，然後移除私有憑證檔案。根據 Active Directory 複寫設定，CA 可能需要幾分鐘的時間才能發佈至您的網域控制站和桌面執行個體。

> **Note**
>
> - Active Directory 必須將 CA 散發給受信任的根憑證授權單位，而企業 NTAuth 會在 WorkSpaces 桌面加入網域時自動儲存桌面。
> - Active Directory 網域控制站必須處於相容性模式，憑證強式強制執行才能支援憑證型身分驗證。如需詳細資訊，請參閱 Microsoft Support 文件中的 KB5014754 — Windows 網域控制站上的憑證型驗證變更。如果您使用 AWS 受管理的 Microsoft AD，請參閱設定目錄安全性設定以取得詳細資訊。

啟用憑證型驗證

完成下列步驟，以啟用憑證型身分驗證。

1. 在開啟 WorkSpaces 主控台https://console.aws.amazon.com/workspaces。
2. 在導覽窗格中，選擇目錄。
3. 選擇您的目錄 ID WorkSpaces。
4. 在驗證之下，按一下編輯。

5. 按一下編輯憑證型驗證。
6. 核取啟用憑證型驗證。
7. 確認清單中已關聯您的私有 CA ARN。私有 CA 應位於同一 AWS 帳戶中 AWS 區域，且必須使用有權出現在清單中 euc-private-ca 的金鑰加上標記。
8. 按一下 Save Changes (儲存變更)。憑證型驗證現在已啟用。
9. WorkSpaces 在 WorkSpaces 串流通訊協定 (WSP) 服務包上重新啟動 Windows，以使變更生效。如需詳細資訊，請參閱重新開機 a WorkSpace.
10. 重新啟動之後，當使用者使用支援的用戶端透過 SAML 2.0 進行驗證時，他們不再收到輸入網域密碼的提示。

> **Note**
>
> 啟用憑證型驗證以登入時，即使在目錄上啟用 WorkSpaces，也不會提示使用者輸入多重要素驗證 (MFA)。使用憑證型驗證時，可以透過 SAML 2.0 身分提供者啟用 MFA。如需 AWS Directory Service MFA 的詳細資訊，請參閱多因素驗證 (AD Connector) 或啟用多重要素驗證。 AWS Managed Microsoft AD

管理憑證型驗證

CA 憑證

在一般組態中，私有 CA 憑證的有效期為 10 年。如需有關以過期憑證取代 CA 或以新的有效期重新發行 CA 的詳細資訊，請參閱管理私有 CA 生命週期。

最終使用者憑證

AWS Private CA 針對憑證型驗證而發行的使用者 WorkSpaces 憑證不需要續約或撤銷。這些證書是短暫的。 WorkSpaces每 24 小時自動發行一次新憑證。這些一般使用者憑證的有效期比一般 AWS Private CA CRL 散發短。因此，最終使用者憑證不需要撤銷，也不會出現在 CRL 中。

稽核報告

您可以建立稽核報告，以列出私有 CA 已發行或撤銷的所有憑證。如需詳細資訊，請參閱使用包含您私有 CA 的稽核報告。

記錄和監控

您可以使用AWS CloudTrail來記錄對 AWS Private CA 的 API 呼叫 WorkSpaces。如需詳細資訊，請參閱使用 CloudTrail。在CloudTrail事件歷史記錄中，您可以從WorkSpacesEcmAssumeRoleSession使用者名稱建立的acm-pca.amazonaws.com事件來源中檢視GetCertificate和IssueCertificate事件名稱。系統會為每個 EUC 憑證型驗證要求記錄這些事件。

啟用跨帳戶 PCA 共用

當您使用 Private CA 跨帳戶共用時，您可以授與其他帳戶使用集中式 CA 的權限，這樣就不需要每個帳戶中的 Private CA。CA 可以使用 AWS Resource Access Manager 來管理權限來產生和發行憑證。私有 CA 跨帳戶共用可與相同區域內的 WorkSpaces 憑證型驗證 (CBA) 搭配使用。 AWS

搭配 WorkSpaces CBA 使用共用私人 CA 資源

1. 在集中式 AWS 帳戶中設定 CBA 的私有 CA。如需詳細資訊，請參閱 設定憑證型驗證。
2. 依照如何使用 AWS RAM 共用 ACM 專用 CA 跨 AWS 帳戶中的步驟，與 WorkSpaces 資源利用 CBA 的資源帳號共用專用 CA。您不需要完成步驟 3 即可建立憑證。您可以與個別 AWS 帳戶共用 Private CA，也可以透過 Organ AWS izations 共用。若要與個別帳號共用，您必須使用 Resource Access Manager (RAM) 主控台或 API 接受資源帳號中的共用私有 CA。設定共用時，請確認資源帳號中私人 CA 的 RAM 資源共用正在使用AWS RAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority受管理的權限範本。此範本與發行 CBA 憑證時 WorkSpaces 服務角色所使用的 PCA 範本保持一致。
3. 成功共用之後，您應該可以使用資源帳號中的私人 CA 主控台來檢視共用的私有 CA。
4. 使用 API 或 CLI 將私有 CA ARN 與 WorkSpaces 目錄內容中的 CBA 產生關聯。目前，WorkSpaces 主控台不支援選取共用的私有 CA ARN。CLI 指令範例：

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

使用智慧卡進行驗證

Windows 和 Linux WorkSpaces WorkSpaces 串流通訊協定 (WSP) 套裝軟體允許使用通用存取卡 (CAC) 和個人身分驗證 (PIV) 智慧卡進行驗證。

Amazon WorkSpaces 支援使用智慧卡進行工作階段前身份驗證和工作階段內身份驗證。工作階段前驗證是指使用者登入時所執行的智慧卡驗證。 WorkSpaces工作階段內驗證是指在登入後執行的驗證。

例如，使用者可以在使用 Web 瀏覽器和應用程式時，使用智慧卡進行工作階段內驗證。他們也可以將智慧卡用於進行需要管理許可的動作。例如，如果使用者在 Linux 上具有系統管理權限 WorkSpace，則可以在執行`sudo`和`sudo -i`指令時使用智慧卡來驗證自己。

目錄

要求

- 工作階段前驗證需要 Active Directory Connector (AD Connector) 目錄。AD Connector 使用以憑證為基礎的交互式 Transport Layer Security (交互式 TLS) 驗證，透過硬體或軟體智慧卡憑證對 Active Directory 使用者進行身分驗證。如需如何設定 AD Connector 和內部部署目錄的詳細資訊，請參閱目錄組態。
- 若要搭配視窗或 Linux 使用智慧卡 WorkSpace，使用者必須使用 Amazon WorkSpaces 視窗用戶端 3.1.1 或更新版本或 WorkSpaces macOS 用戶端 3.1.5 或更新版本。如需將智慧卡與 Windows 和 macOS 用戶端搭配使用的詳細資訊，請參閱 Amazon 使用 WorkSpaces 者指南中的智慧卡 Support。
- 根 CA 和智慧卡憑證必須符合特定需求。如需詳細資訊，請參閱系統《AWS Directory Service 管理指南》中的在 AD Connector 中啟用 MTL 驗證以搭配智慧卡使用，以及 Microsoft 文件中的憑證需求。

  除了這些要求之外，Amazon 用於智慧卡身份驗證的使用者憑證還 WorkSpaces 必須包含下列屬性：

  - 憑證 userPrincipalName (SAN) 欄位中的 AD 使用者 subjectAltName (UPN)。我們建議為使用者的預設 UPN 核發智慧卡憑證。
  - 用戶端驗證 (1.3.6.1.5.5.7.3.2) 擴充金鑰使用 (EKU) 屬性。
  - 智慧卡登入 (1.3.6.1.4.1.311.20.2.2) EKU 屬性。

- 對於工作階段前驗證，憑證撤銷檢查需要線上憑證狀態協定 (OCSP)。對於工作階段內驗證，建議使用 OCSP，但非必要。

限制

- 智慧卡驗證目前僅支援 WorkSpaces Windows 用戶端應用程式 3.1.1 或更新版本，以及 macOS 用戶端應用程式 3.1.5 或更新版本。
- 僅當用戶端在 64 位元版本的 WorkSpaces Windows 上執行時，Windows 用戶端應用程式 3.1.1 或更新版本才支援智慧卡。
- Ubuntu 目前 WorkSpaces 不支援智慧卡驗證。
- 智慧卡驗證目前僅支援 AD Connector 目錄。
- 您可以在支援 WSP 的所有區域中使用工作階段內驗證。下列區域可以使用工作階段前驗證：
  - 亞太 (雪梨) 區域
  - 亞太 (東京) 區域
  - 歐洲 (愛爾蘭) 區域
  - AWS GovCloud (美國東部) 區域
  - AWS GovCloud (美國西部) 區域
  - 美國東部 (維吉尼亞北部) 區域
  - 美國西部 (奧勒岡) 區域
- 對於 Linux 或 Windows 上的工作階段內驗證和工作階段前驗證 WorkSpaces，目前一次只允許一張智慧卡。
- 對於工作階段前驗證，目前不支援在相同目錄上同時啟用智慧卡驗證和登入驗證。
- 目前僅支援 CAC 和 PIV 卡。其他類型的硬體或軟體型智慧卡也可以運作，但尚未針對搭配 WSP 使用進行完整測試。

目錄組態

若要啟用智慧卡驗證，您必須以下列方式設定 AD Connector 目錄和內部部署目錄。

AD Connector 目錄組態

在開始之前，確定您的 AD Connector 目錄已按照《AWS Directory Service 管理指南》中的 AD Connector 先決條件所述設定。尤其是，確定您已在防火牆中開啟必要的連接埠。

若要完成 AD Connector 目錄的設定，請依照《AWS Directory Service 管理指南》中的在 AD Connector 中啟用 MTL 驗證以搭配智慧卡使用的指示進行。

> **Note**
>
> 智慧卡驗證需要 Kerberos 限制委派 (KCD) 才能正常運作。KCD 要求 AD Connector 服務帳戶的使用者名稱部分與相同使用者AccountName 的 SAM 相符。一個 SAM 不AccountName 能超過 20 個字符。

內部部署目錄組態

除了設定 AD Connector 目錄之外，您也必須確定發行給內部部署目錄之網域控制站的憑證有「KDC 驗證」擴充金鑰使用 (EKU) 設定。若要這麼做，請使用 Active Directory Domain Services (AD DS) 預設 Kerberos 驗證憑證範本。請勿使用網域控制站憑證範本或網域控制站驗證憑證範本，因為這些範本不包含智慧卡驗證的必要設定。

啟用視窗的智慧卡 WorkSpaces

如需有關如何在 Windows 上啟用智慧卡驗證的一般指引，請參閱 Microsoft 文件中的讓智慧卡能透過第三方憑證授權單位登入的指導方針。

若要偵測 Windows 螢幕鎖定畫面並中斷工作階段的連線

若要允許使用者在螢幕鎖定時解除鎖定已啟用智慧卡工作階段前驗證的 Windows WorkSpaces ，您可以在使用者的工作階段中啟用 Windows 鎖定螢幕偵測。偵測到 Windows 鎖定畫面時， WorkSpace 工作階段會中斷連線，使用者可以使用其智慧卡與用 WorkSpaces 戶端重新連線。

您可以使用群組政策設定，在偵測到 Windows 螢幕鎖定畫面時，啟用中斷工作階段連線。如需詳細資訊，請參閱 針對 WSP 啟用或停用畫面鎖定時中斷工作階段連線。

啟用工作階段內或工作階段前驗證

依預設，Windows 不 WorkSpaces 會啟用以支援使用智慧卡進行工作階段前或工作階段中驗證。如果需要，您可以使用群組原則設定為 Windows WorkSpaces 啟用工作階段內和工作階段前驗證。如需詳細資訊，請參閱 啟用或停用 WSP 的智慧卡重新導向。

若要使用工作階段前驗證，除了更新群組政策設定之外，您還必須透過 AD Connector 目錄設定啟用工作階段前驗證。如需詳細資訊，請遵循《AWS Directory Service 管理指南》中在 AD Connector 中啟用 mTLS 驗證以用於智慧卡的指示。

讓使用者能夠在瀏覽器中使用智慧卡

如果使用者使用 Chrome 作為瀏覽器，則不需要特別設定即可使用智慧卡。

如果您的使用者使用 Firefox 作為他們的瀏覽器，您可以透過群組政策讓使用者能在 Firefox 中使用智慧卡。您可以在中使用這些 Firefox 群組原則範本 GitHub。

例如，您可以針對 Windows 安裝 64 位元版本的 OpenSC 以支援 PKCS #11，然後使用下列群組政策設定，其中 *NAME_OF_DEVICE* 是任何您要用來識別 PKCS #11 的值 (例如 OpenSC)，而 *PATH_TO_LIBRARY_FOR_DEVICE* 是 PKCS #11 模組的路徑。此路徑應指向副檔名為 .DLL 的程式庫，例如 `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`。

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

如果您使用 OpenSC，也可藉由執行 `pkcs11-register.exe` 程式，將 OpenSC `pkcs11` 模組載入 Firefox 瀏覽器。若要執行此程式，請按兩下位於 `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` 的檔案，或開啟命令提示視窗並執行下列命令：

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

若要驗證 OpenSc `pkcs11` 模組是否已載入 Firefox，請執行下列操作：

1. 如果 Firefox 已在執行中，請將它關閉。
2. 開啟 Firefox。選擇右上角的選單按鈕

   ，

   然後選擇選項。
3. 在 about:preferences 頁面上，選擇左側導覽窗格中的隱私權與安全性。
4. 在憑證之下，選擇安全裝置。
5. 在裝置管理員對話方塊中，您應會在左側導覽中看到 OpenSc 智慧卡架構 (0.21)，而當您加以選取時應該有下列值：

   模組：`OpenSC smartcard framework (0.21)`

路徑：C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll

故障診斷

如需智慧卡疑難排解的相關資訊，請參閱 Microsoft 文件中的憑證和設定問題。

可能導致問題的一些常見問題：

- 插槽與憑證的對應不正確。
- 智慧卡上有多個可比對使用者的憑證。使用下列條件比對憑證：
  - 憑證的根 CA。
  - 憑證的 <KU> 和 <EKU> 欄位。
  - 憑證主體中的 UPN。
- 擁有多個憑證在其金鑰使用中有 <EKU>msScLogin。

一般而言，最好只有一個對應至智慧卡中第一個插槽的憑證用於智慧卡驗證。

用於管理智慧卡上憑證和金鑰的工具 (例如移除或重新對應憑證和金鑰) 可能是製造商特有的工具。如需詳細資訊，請參閱智慧卡製造商提供的文件。

啟用適用於 Linux 的智慧卡 WorkSpaces

> **Note**
>
> WorkSpaces 在 WSP 上的 Linux 目前有以下限制：
>
> - 不支援剪貼簿、音訊輸入、視訊輸入和時區重新導向。
> - 不支援多個監視器。
> - 您必須使用 WorkSpaces 視窗用戶端應用程式 WorkSpaces 在 WSP 上連線到 Linux。

若要在 Linux 上啟用智慧卡的使用 WorkSpaces，您必須在 WorkSpace 映像中包含 PEM 格式的根 CA 憑證檔案。

若要取得根 CA 憑證

您可以透過多種方式取得根 CA 憑證：

- 您可以使用第三方憑證授權單位操作的根 CA 憑證。
- 您可以使用 Web 註冊網站匯出自己的根 CA 憑證，也就是 `http://ip_address/certsrv` 或 `http://fqdn/certsrv`，其中 *ip_address* 和 *fqdn* 是根憑證 CA 伺服器的 IP 地址和完整網域名稱 (FQDN)。如需使用 Web 註冊網站的相關資訊，請參閱 Microsoft 文件中的如何匯出根憑證授權單位憑證。
- 您可以使用下列程序，從執行 Active Directory Certificate Services (AD CS) 的根 CA 憑證伺服器匯出根 CA 憑證。如需安裝 AD CS 的相關資訊，請參閱 Microsoft 文件中的安裝憑證授權單位。

  1. 使用管理員帳戶登入根 CA 伺服器。
  2. 從 Windows 開始功能表，開啟命令提示視窗 (開始 > Windows 系統 > 命令提示)。
  3. 使用下列命令將根 CA 憑證匯出至新檔案，其中 *rootca*.cer 是新檔案的名稱：

     ```
     certutil -ca.cert rootca.cer
     ```

     如需執行 Certutil 的詳細資訊，請參閱 Microsoft 文件中的 Certutil。
  4. 使用下列 OpenSSL 命令，將匯出的根 CA 憑證從 DER 格式轉換為 PEM 格式，其中 *rootca* 是憑證的名稱。如需 openssl 的詳細資訊，請參閱 http://www.openssl.org/。

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

若要將根 CA 憑證新增至您的 Linux WorkSpaces

為了協助您啟用智慧卡，我們已將 `enable_smartcard` 指令碼新增至我們的 Amazon Linux WSP 套件。此指令碼會執行下列動作：

- 將根 CA 憑證匯入網路安全服務 (NSS) 資料庫。
- 安裝用於可插入式驗證模組 (PAM) 驗證的 `pam_pkcs11` 模組。
- 執行預設組態，包括`pkinit`在 WorkSpace 佈建期間啟用。

下列程序說明如何使用`enable_smartcard`指令碼將根 CA 憑證新增至 Linux，以 WorkSpaces 及如何為 Linux 啟用智慧卡 WorkSpaces。

1. 在啟用 WSP 通訊協定 WorkSpace 的情況下建立新的 Linux。在 Amazon WorkSpaces 主控台 WorkSpace 中啟動時，請務必在 [選取套裝軟體] 頁面上為通訊協定選取 WSP，然後選取其中一個 Amazon Linux 2 公用套裝軟體。
2. 在新版本上 WorkSpace，以 root 身分執行下列命令，其中*pem-path*是 PEM 格式的根 CA 憑證檔案的路徑。

```
/usr/lib/skylight/enable_smartcard --ca-cert pem-path
```

> **Note**
>
> Linux WorkSpaces 假設智慧卡上的憑證是針對使用者的預設使用者主體名稱 (UPN) 核發的，例如*sAMAccountName*@*domain*，其中*domain*是完整網域名稱 (FQDN)。若要使用替代 UPN 尾碼，`run /usr/lib/skylight/enable_smartcard --help` 以取得詳細資訊。對於每個使用者而言，替代 UPN 尾碼的對應都是唯一的。因此，必須對每個使用者個別執行該對應 WorkSpace。

3. (選擇性) 依預設，所有服務都會啟用在 Linux 上使用智慧卡驗證 WorkSpaces。若要將智慧卡驗證限制為僅限特定服務，您必須編輯 `/etc/pam.d/system-auth`。取消註解 `pam_succeed_if.so` 的 `auth` 行 並視需要編輯服務清單。

   取消註解 `auth` 行後，若要允許服務使用智慧卡驗證，您必須將其新增至清單。若要讓服務僅使用密碼驗證，則必須從清單中將其移除。
4. 執行任何其他自訂 WorkSpace。例如，您可能想要新增整個系統的政策，讓使用者能夠在 Firefox 中使用智慧卡。Chrome 使用者必須自行在其用戶端上啟用智慧卡。 如需詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的智慧卡 Support。)
5. 從中建立自訂 WorkSpace 映像並套裝軟體 WorkSpace。
6. 使用新的自訂套裝軟體 WorkSpaces 為您的使用者啟動。

讓使用者能夠在 Firefox 中使用智慧卡

您可以在 Linux WorkSpace 映像檔中新增 SecurityDevices 政策，讓您的使用者能夠在 Firefox 中使用智慧卡。如需更多有關新增全系統政策到 Firefox 的資訊，請參閱上 GitHub的 Mozilla 政策範本。

1. 在您用來建立 WorkSpace 映像檔的位置上，建立一個名為 `policies.json` in 的新檔案`/usr/lib64/firefox/distribution/`。 WorkSpace

2. 在 JSON 檔案中，新增下列 SecurityDevices 原則，其中*NAME_OF_DEVICE*是您要用來識別pkcs模組的任何值。例如，您可能想要使用 "0penSC" 之類的值：

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

故障診斷

針對疑難排解，我們建議新增 pkcs11-tools 公用程式。此公用程式可讓您執行下列動作：

- 列出每張智慧卡。
- 列出每張智慧卡上的插槽。
- 列出每張智慧卡上的憑證。

可能導致問題的一些常見問題：

- 插槽與憑證的對應不正確。
- 智慧卡上有多個可比對使用者的憑證。使用下列條件比對憑證：
  - 憑證的根 CA。
  - 憑證的 <KU> 和 <EKU> 欄位。
  - 憑證主體中的 UPN。
- 擁有多個憑證在其金鑰使用中有 <EKU>msScLogin。

一般而言，最好只有一個對應至智慧卡中第一個插槽的憑證用於智慧卡驗證。

用於管理智慧卡上憑證和金鑰的工具 (例如移除或重新對應憑證和金鑰) 可能是製造商特有的工具。您可用於處理智慧卡的其他工具包括：

- opensc-explorer
- opensc-tool
- pkcs11_inspect

- pkcs11_listcerts
- pkcs15-tool

若要啟用偵錯記錄功能

若要對 pam_pkcs11 和 pam-krb5 組態進行疑難排解，您可以啟用偵錯記錄。

1. 在 /etc/pam.d/system-auth-ac 檔案中，編輯 auth 動作並將 pam_pksc11.so 的 nodebug 參數變更為 debug。
2. 在 /etc/pam_pkcs11/pam_pkcs11.conf 檔案中，將 debug = false; 變更為 debug = true;。debug 選項會個別套用於每個對應器模組，因此您可能需要直接在 pam_pkcs11 區段下以及適當的對應器區段下進行變更 (根據預設，這是 mapper generic)。
3. 在 /etc/pam.d/system-auth-ac 檔案中，編輯 auth 動作並將 debug 或 debug_sensitive 參數新增至 pam_krb5.so。

啟用偵錯記錄之後，系統會直接在作用中終端機中列印 pam_pkcs11 偵錯訊息。pam_krb5 來自的訊息已記錄於 /var/log/secure。

若要檢查智慧卡憑證對應的使用者名稱，請使用下列 pklogin_finder 命令：

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

出現提示時，輸入智慧卡 PIN。pklogin_finder 在 stdout 上以 *NETBIOS**username* 形式輸出智慧卡憑證上的使用者名稱。此使用者名稱應符合 WorkSpace 使用者名稱。

在 Active Directory Domain Services (AD DS) 中，NetBIOS 網域名稱是 Windows 2000 前的網域名稱。一般而言 (但不一定)，NetBIOS 網域名稱通常是網域名稱系統 (DNS) 網域名稱的子網域。例如，如果 DNS 網域名稱為 example.com，則 NetBIOS 網域通常為 EXAMPLE。如果 DNS 網域名稱為 corp.example.com，則 NetBIOS 名稱通常為 CORP。

例如，對於 網域 corp.example.com 中的使用者 mmajor，來自 pklogin_finder 的輸出為 CORP\mmajor。

> **Note**
>
> 如果您收到訊息 "ERROR:pam_pkcs11.c:504: verify_certificate() failed"，此訊息指出 pam_pkcs11 在智慧卡上找到符合使用者名稱條件的憑證，但該憑證並未鏈結至機

器所辨識的根 CA 憑證。發生這種情況時，pam_pkcs11 會輸出上述訊息，然後嘗試下一個憑證。只有在找到符合使用者名稱並鏈結至已辨識根 CA 憑證的憑證時，才允許驗證。

若要對您的 pam_krb5 組態進行疑難排解，您可以使用下列命令在偵錯模式中手動調用 kinit：

```
KRB5_TRACE=/dev/stdout kinit -V
```

此命令應會成功取得 Kerberos 票證授予票證 (TGT)。如果失敗，請嘗試將正確的 Kerberos 主體名稱明確地新增至命令。例如，對於網域 corp.example.com 中的使用者 mmajor，請使用以下命令：

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

如果此命令成功，則問題很可能是從使用者名稱到 Kerberos 主要 WorkSpace 名稱的對應。檢查 /etc/krb5.conf 檔案中的 [appdefaults]/pam/mappings 區段。

如果此命令不成功，但密碼型 kinit 命令確實成功，請檢查 /etc/krb5.conf 檔案中的 pkinit_ 相關組態。例如，如果智慧卡包含多個憑證，您可能需要對 pkinit_cert_match 進行變更。

提供您的網際網路存取 WorkSpace

您 WorkSpaces 必須能夠存取網際網路，才能將更新安裝到作業系統並部署應用程式。您可以使用下列其中一個選項來允許您 WorkSpaces 在虛擬私有雲 (VPC) 中存取網際網路。

選項

- 啟動您 WorkSpaces 的私有子網路，並在 VPC 中的公有子網路中設定 NAT 閘道。
- 啟動您 WorkSpaces 的公用子網路，並自動或手動將公用 IP 位址指派給您的 WorkSpaces.

如需這些選項的詳細資訊，請參閱 設定虛 VPC WorkSpaces 中對應的章節。

使用這些選項中的任何一個，您必須確保您的安全性群組 WorkSpaces允許連接埠 80 (HTTP) 和 443 (HTTPS) 上的輸出流量傳輸至所有目的地 (0.0.0.0/0)。

Amazon Linux Extras Library

如果您使用的是 Amazon Linux 儲存庫，您的 Amazon Linux WorkSpaces 必須可以存取網際網路，或者您必須將 VPC 端點設定為此儲存庫和主要 Amazon Linux 儲存庫。如需詳細資訊，請參閱 Amazon

S3 的端點中的<範例：啟用 Amazon Linux AMI 儲存庫的存取>一節。Amazon Linux AMI 儲存庫是每個區域中的 Amazon S3 儲存貯體。如果您想要 VPC 中的執行個體透過端點存取儲存庫，請建立啟用存取這些儲存貯體的端點政策。下列政策允許存取 Amazon Linux 儲存庫。

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

適用於您的安全群組 WorkSpaces

當您向目錄註冊時 WorkSpaces，它會建立兩個安全性群組，一個用於目錄控制器，另一個用 WorkSpaces 於目錄控制器。目錄控制器的安全群組有一個名稱，該名稱包含後面接著 _controllers 的目錄識別碼 (例如 d-12345678e1_controllers)。的安全性群組 WorkSpaces 具有一個名稱，該名稱包含目錄識別碼，後跟 _ 工作空間成員 (例如，D-123456FC11_ 工作區成員)。

> **Warning**
>
> 避免修改、刪除或分離 _Console 和 _ 工作空間成員安全性群組。修改或刪除這些安全群組時務必小心，因為您將無法重新建立這些群組，並在修改或刪除這些群組之後將其重新加回。如需詳細資訊，請參閱適用於 Linux 執行個體的 Amazon EC2 安全群組和適用於 Windows 執行個體的 Amazon EC2 安全群組。

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 而不需要重建它們，如本主題稍後所說明。

當您將多個安全群組與一個 WorkSpaces 目錄產生關聯時，每個安全性群組中的規則都會有效彙總，以建立一組規則。建議盡可能緊縮您的安全群組規則。

如需安全群組的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 的安全群組。

若要將安全性群組新增至 WorkSpaces 目錄

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇目錄。
3. 選取目錄，然後選擇動作、更新詳細資訊。
4. 展開安全群組，然後選取安全群組。
5. 選擇更新並退出。

若要將安全性群組新增至現有群組 WorkSpace 而不重建它，您可以將新的安 elastic network interface 群組指派給. WorkSpace

若要將安全性群組新增至現有 WorkSpace

1. 找到每個 WorkSpace 需要更新的 IP 地址。
   a. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
   b. 展開每個項目 WorkSpace 並記錄其 WorkSpace IP 位址。
2. 找到每個 ENI， WorkSpace 並更新其安全群組指派。
   a. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
   b. 在網路與安全之下，選擇網路介面。
   c. 搜尋您在步驟 1 中記錄的第一個 IP 位址。
   d. 選取與 IP 位址相關聯的 ENI，選擇動作，然後選擇變更安全群組。
   e. 選取新的安全群組，然後選擇儲存。
   f. 根據需要對其他任何其他過程重複此過程 WorkSpaces。

WorkSpaces 的 IP 存取控制群組

Amazon WorkSpaces 可讓您控制可從哪些 IP 地址存取您的 WorkSpaces。使用以 IP 位址為基礎的控制群組，即可定義和管理受信任 IP 位址的群組，而且只允許使用者在連線到受信任的網路時存取其 WorkSpaces。

IP 存取控制群組可做為虛擬防火牆，以控制允許使用者存取其 WorkSpaces 的 IP 位址。若要指定 CIDR 位址範圍，請將規則新增至 IP 存取控制群組，然後將該群組與您的目錄建立關聯。您可以將每個 IP 存取控制群組與一或多個目錄建立關聯。您可以針對每個 AWS 帳戶的每個區域建立最多 100 個 IP 存取控制群組。不過，您最多只能將 25 個 IP 存取控制群組與單一目錄建立關聯。

預設 IP 存取控制群組與每個目錄相關聯。此預設群組包含允許使用者從任何地方存取其 WorkSpaces 的預設規則。您無法修改目錄的預設 IP 存取控制群組。如果您未將 IP 存取控制群組與您的目錄建立關聯，則會使用預設群組。如果您將 IP 存取控制群組與某個目錄建立關聯，則預設 IP 存取控制群組會取消關聯。

若要指定受信任網路的公用 IP 位址和 IP 位址範圍，請將規則新增至您的 IP 存取控制群組。如果使用者透過 NAT 閘道或 VPN 存取其 WorkSpaces，您必須建立規則，以允許來自 NAT 閘道或 VPN 之公用 IP 位址的流量。

> **Note**
>
> - IP 存取控制群組不允許對 NAT 使用動態 IP 位址。如果您使用 NAT，請將其設定為使用靜態 IP 位址，而非動態 IP 位址。確定 NAT 會在 WorkSpaces 工作階段期間透過相同的靜態 IP 位址路由傳送所有 UDP 流量。
> - IP 存取控制群組控制使用者可從中將其串流工作階段連線至 WorkSpaces 的 IP 位址。使用者仍然可以使用 Amazon WorkSpaces 公用 API，從任何 IP 位址執行諸如重新啟動、重新建置、關閉等功能。

您可以將此功能搭配 Web 存取、PCoIP 零用戶端及 macOS、iPad、Windows、Chromebook 和 Android 的用戶端應用程式使用。

建立 IP 存取控制群組

您可以建立 IP 存取控制群組，如下所示。每個 IP 存取控制群組最多可包含 10 個規則。

建立 IP 存取控制群組

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 IP 存取控制。
3. 選擇建立 IP 群組。
4. 在建立 IP 群組對話方塊中，輸入群組的名稱和描述，然後選擇建立。

5. 選取群組，然後選擇編輯。
6. 針對每個 IP 位址，選擇新增規則。在來源中，輸入 IP 地址或 IP 地址範圍。在描述中，輸入描述。當您完成規則新增時，選擇儲存。

將 IP 存取控制群組與目錄建立關聯

您可以將 IP 存取控制群組與目錄建立關聯，確保只能從受信任的網路存取 WorkSpaces。

如果您將沒有規則的 IP 存取控制群組與目錄建立關聯，則會封鎖對所有 WorkSpaces 的所有存取。

將 IP 存取控制群組與目錄建立關聯

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇目錄。
3. 選取目錄，然後選擇動作、更新詳細資訊。
4. 展開 IP 存取控制群組，然後選取一或多個 IP 存取控制群組。
5. 選擇更新並退出。

複製 IP 存取控制群組

您可使用現有的 IP 存取控制群組作為建立新 IP 存取控制群組的基礎。

從現有 IP 存取控制群組建立 IP 存取控制群組

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 IP 存取控制。
3. 選取群組，然後依序選擇動作、複製到新的。
4. 在複製 IP 群組對話方塊中，輸入新群組的名稱和描述，然後選擇複製群組。
5. (選用) 若要修改從原始群組複製的規則，請選取新群組並選擇編輯。視需要新增、更新或移除規則。選擇儲存。

建立 IP 存取控制群組。

您隨時可以從 IP 存取控制群組中刪除規則。如果您移除用來允許與 WorkSpace 連線的規則，使用者就會中斷與 WorkSpace 的連線。

您必須先取消 IP 存取控制群組與任何目錄的關聯，才能刪除該群組。

刪除 IP 存取控制群組

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇目錄。
3. 針對與 IP 存取控制群組相關聯的每個目錄，選取目錄，然後依序選擇動作、更新詳細資料。展開 IP 存取控制群組，清除 IP 存取控制群組的核取方塊，然後選擇更新並結束。
4. 在導覽窗格中，選擇 IP 存取控制。
5. 選取群組，然後依序選擇動作、刪除 IP 群組。

為 WorkSpaces 設定 PCoIP 零用戶端

PCoIP 零用戶端僅與使用 PCoIP 通訊協定的 WorkSpaces 套件相容。

如果零用戶端裝置的韌體版本為 6.0.0 版或更新版本，使用者即可直接連線至其 WorkSpaces。當使用者使用零用戶端裝置直接連線至其 WorkSpaces 時，建議您在 WorkSpaces 目錄使用多重要素驗證 (MFA)。如需在您的目錄使用 MFA 的詳細資訊，請參閱下列文件：

- AWS Managed Microsoft AD—《AWS Directory Service 管理指南》中的啟用 AWS Managed Microsoft AD 的多重要素驗證
- AD Connector—《AWS Directory Service 管理指南》中的啟用 AD Connector 的多重要素驗證和多重要素驗證 (AD Connector)
- 信任的網域—《AWS Directory Service 管理指南》中的啟用 AWS Managed Microsoft AD 的多重要素驗證
- Simple AD—多重要素驗證不適用於 Simple AD。

自 2021 年 4 月 13 日起，PCoIP Connection Manager 不再支援搭配 4.6.0 到 6.0.0 之間的零用戶端裝置韌體版本使用。如果零用戶端韌體不是 6.0.0 版或更新版本，您可以透過桌面存取訂閱 (網址為 https://www.teradici.com/desktop-access) 取得最新的韌體。

Important

- 在 Teradici PCoIP 管理 Web 介面 (AWI) 或 Teradici PCoIP 管理主控台 (MC) 中，確定啟用網路時間通訊協定 (NTP)。對於 NTP 主機 DNS 名稱，使用 **`pool.ntp.org`**，並將 NTP 主

機連接埠設定為 123。如果未啟用 NTP，PCoIP 零用戶端使用者可能會收到憑證失敗錯誤，例如「提供的憑證因時間戳記而無效」。

- 從 PCoIP 代理程式 20.10.4 版開始，Amazon WorkSpaces 預設會透過 Windows 登錄停用 USB 重新導向。當使用者使用 PCoIP 零用戶端裝置來連線至其 WorkSpaces 時，此登錄設定會影響 USB 周邊設備的行為。如需詳細資訊，請參閱 USB 印表機和其他 USB 周邊設備不適用於 PCoIP 零客戶端。

如需有關設定和連接 PCoIP 零用戶端裝置的資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 PCoIP 零用戶端。如需核准的 PCoIP 零用戶端裝置清單，請參閱 Terdici 網站上的 PCoIP 零用戶端。

針對 Chromebook 設定 Android

版本 2.4.13 是 Amazon WorkSpaces Chromebook 客戶端應用程序的最終版本。由於谷歌正逐步淘汰對 Chrome 應用程序的支持，因此 WorkSpaces Chromebook 客戶端應用程序不會進一步更新，並且不支持其使用。

對於支持安裝 Android 應用程序的 Chromebook，我們建議您改用 WorkSpaces Android 客戶端應用程序。

在 2019 年之前推出的某些 Chromebook 必須啟用才能安裝 Android 應用程序，用戶才能安裝 Amazon WorkSpaces Android 客戶端應用程序。如需詳細資訊，請參閱支援 Android 應用程式的 Chrome 作業系統。

若要遠端管理以便讓使用者的 Chromebook 安裝 Android 應用程式，請參閱在 Chrome 裝置上設定 Android。

啟用和設定 Amazon WorkSpaces 網路存取

大多數 WorkSpaces 捆綁包支持 Amazon WorkSpaces Web 訪問。有關支持 Web 瀏覽器訪問的 WorkSpaces 列表，請參閱「哪些 Amazon WorkSpaces 服務包支持 Web 訪問？」(出自用戶端存取、Web 存取和使用者體驗)。

> **Note**
>
> - 所有提供 WSP 的區域都支援使用 WSP WorkSpaces WorkSpaces 的網頁存取 (適用於 Windows 和 Ubuntu)。適用於 Amazon Linux 的 WSP WorkSpaces 僅適用於 AWS GovCloud （美國西部）。

- 我們強烈建議您將 Web Access 與 WSP 搭配使用，以 WorkSpaces 獲得最佳的串流品質和使用者體驗。以下是搭配 PCoIP WorkSpaces 使用網頁存取時的限制：
  - 亞太區域 (孟買) AWS GovCloud (US) Regions、非洲 (開普敦) 和以色列 (特拉維夫) 不支援使用 PCoIP 進行 Web 存取
  - 使用 PCoIP 的網頁存取僅支援視窗 WorkSpaces，而不支援 Amazon Linux。WorkSpaces
  - 某些使用 PCoIP 通訊協定 WorkSpaces 的視窗 10 無法使用網頁存取。如果您的 PCoIP WorkSpaces 是由視窗伺服器 2019 或 2022 供電，則無法使用網頁存取。
- 您無法使用網頁瀏覽器連線至啟用 GPU WorkSpaces。
- 如果您在 VPN 上使用 macOS 並使用 Firefox 的網頁瀏覽器，網頁瀏覽器將不支援透過網頁存取串流 PCoIP WorkSpaces 。 WorkSpaces 這是由於 WebRTC 協定的 Firefox 實作限制。

Important

自 2020 年 10 月 1 日起，客戶將無法再使用 Amazon WorkSpaces 網路存取用戶端連線到 Windows 7 自訂版 WorkSpaces 或 Windows 7 自攜授權 (BYOL)。 WorkSpaces

步驟 1：啟用對您的網頁存取 WorkSpaces

您可以 WorkSpaces 在目錄層級控制 Web 存取。針對您要允許使用者透過 Web Access 用戶端存取的每個目錄 WorkSpaces ，請執行下列步驟。

若要啟用網頁存取 WorkSpaces

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 在目錄 ID 欄下，選擇您要啟用 Web Access 之目錄的目錄 ID。
4. 在目錄詳細資訊頁面上，向下捲動至其他平台區段，然後選擇編輯。
5. 選擇 Web Access。
6. 選擇儲存。

> **Note**
>
> 啟用 Web 存取之後，請重新啟 WorkSpace 動以套用變更。

步驟 2：設定 Web Access 連接埠的輸入和輸出存取

Amazon WorkSpaces 網路存取需要特定連接埠的入站和出站存取權。如需詳細資訊，請參閱 適用於 Web Access 的連接埠。

步驟 3：設定群組政策和安全政策設定，讓使用者能夠登入

Amazon WorkSpaces 依賴特定的登入畫面組態，讓使用者能夠從其 Web 存取用戶端成功登入。

若要讓 Web Access 使用者登入其 WorkSpaces，您必須設定群組原則設定和三個安全性原則設定。如果未正確設定這些設定，使用者在嘗試登入時可能會遇到較長的登入時間或畫面變黑 WorkSpaces。若要進行這些設定，請使用下列程序。

您可以使用群組原則物件 (GPO) 來套用設定，以管理屬於 Windows WorkSpaces 目錄的 Windows WorkSpaces 或使用者。我們建議您為 WorkSpaces 電腦物件建立組織單位，並為您的 WorkSpaces 使用者物件建立組織單位。

如需有關使用 Active Directory 管理工具來處理 GPO 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的安裝 Active Directory 管理工具。

啟用 WorkSpaces 登入代理程式切換使用者

在大多數情況下，當使用者嘗試登入時 WorkSpace，使用者名稱欄位會預先填入該使用者的名稱。不過，如果管理員已建立與執行維護工作的 WorkSpace RDP 連線，則使用者名稱欄位會填入管理員的名稱。

若要避免此問題，請停用隱藏快速使用者切換的進入點群組政策設定。當您停用此設定時，WorkSpaces 登入代理程式可以使用切換使用者按鈕，將正確的名稱填入使用者名稱欄位。

1. 開啟群組原則管理工具 (gpmc.msc)，然後瀏覽至您 WorkSpaces使用的目錄的網域或網域控制站層級並選取 GPO。(如果您的網域中已安裝 WorkSpaces 群組原則系統管理範本，您可以將 WorkSpaces GPO 用於您的 WorkSpaces 電腦帳戶。)
2. 在主要功能表中依序選擇動作、編輯。
3. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、系統和登入。

4. 開啟隱藏快速使用者切換的進入點設定。
5. 在隱藏快速使用者切換的進入點對話方塊中，選擇停用，然後選擇確定。

隱藏上次登入的使用者名稱

預設會顯示上次登入的使用者清單，而不是切換使用者按鈕。視配置而定 WorkSpace，清單可能不會顯示「其他使用者」圖標。發生這種情況時，如果預先填入的使用者名稱不正確， WorkSpaces 登入代理程式就無法在欄位中填入正確的名稱。

若要避免此問題，請啟用安全政策設定互動式登入：不顯示上次登入或互動式登入：不要顯示最後一個使用者名稱 (視您使用的 Windows 版本而定)。

1. 開啟群組原則管理工具 (gpmc.msc)，然後瀏覽至您 WorkSpaces使用的目錄的網域或網域控制站層級並選取 GPO。(如果您的網域中已安裝 WorkSpaces 群組原則系統管理範本，您可以將 WorkSpaces GPO 用於您的 WorkSpaces 電腦帳戶。)
2. 在主要功能表中依序選擇動作、編輯。
3. 在群組政策管理編輯器中，選擇電腦設定、Windows 設定、安全設定、本機政策和安全選項。
4. 開啟下列其中一個設定：
   - 對於 Windows 7—互動式登入：不顯示上次登入
   - 對於 Windows 10—互動式登入：不顯示最後一個使用者名稱
5. 在設定的屬性對話方塊中，選擇啟用，然後選擇確定。

要求在使用者登入之前按 CTRL+ALT+DEL

對於 WorkSpaces 網頁存取，您必須要求使用者先按 CTRL+ALT+DEL 才能登入。要求使用者在登入前按 CTRL+ALT+DEL，可確保使用者在輸入密碼時使用信任的路徑。

1. 開啟群組原則管理工具 (gpmc.msc)，然後瀏覽至您 WorkSpaces使用的目錄的網域或網域控制站層級並選取 GPO。(如果您的網域中已安裝 WorkSpaces 群組原則系統管理範本，您可以將 WorkSpaces GPO 用於您的 WorkSpaces 電腦帳戶。)
2. 在主要功能表中依序選擇動作、編輯。
3. 在群組政策管理編輯器中，選擇電腦設定、Windows 設定、安全設定、本機政策和安全選項。
4. 開啟互動式登入：不需要 CTRL+ALT+DEL 設定。
5. 在本機安全設定索引標籤上，選擇停用，然後選擇確定。

在工作階段鎖定時顯示網域和使用者資訊

WorkSpaces 登入代理程式會尋找使用者的名稱和網域。設定此設定之後，螢幕鎖定畫面會顯示使用者的全名 (如果在 Active Directory 中指定)、其網域名稱及其使用者名稱。

1. 開啟群組原則管理工具 (gpmc.msc)，然後瀏覽至您 WorkSpaces使用的目錄的網域或網域控制站層級並選取 GPO。(如果您的網域中已安裝 WorkSpaces 群組原則系統管理範本，您可以將 WorkSpaces GPO 用於您的 WorkSpaces 電腦帳戶。)
2. 在主要功能表中依序選擇動作、編輯。
3. 在群組政策管理編輯器中，選擇電腦設定、Windows 設定、安全設定、本機政策和安全選項。
4. 開啟互動式登入：當工作階段鎖定時顯示使用者資訊設定。
5. 在本機安全設定索引標籤上，選擇使用者顯示名稱、網域和使用者名稱，然後選擇確定。

套用群組政策和安全政策設定變更

群組原則和安全性原則設定的變更會在下次群組原則更新後生效，以 WorkSpace 及 WorkSpace 工作階段重新啟動之後。若要在先前的程序中套用群組政策和安全政策變更，請執行下列其中一項操作：

- 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 ）。
- 在管理命令提示中輸入 gpupdate /force。

針對 FedRAMP 授權或 DoD SRG 合規設定 Amazon WorkSpaces

若要符合聯邦政府風險與授權管理計畫 (FedRAMP) 或國防部 (DoD) 雲端運算安全要求指南 (SRG)的規範，您必須設定 Amazon WorkSpaces，以在目錄層級使用聯邦政府資訊處理標準 (FIPS) 端點加密。您還必須使用具有 FedRAMP 授權或符合 DoD SRG 規範的美國 AWS 地區。

FedRAMP 授權層級 (中度或高) 或 DoD SRG 影響層級 (2、4 或 5) 取決於正在使用 Amazon WorkSpaces 的美國 AWS 區域。如需適用於每個區域的 FedRAMP 授權和 DoD SRG 合規層級，請參閱合規計畫範圍內的 AWS 服務。

> **Note**
>
> 除了使用 FIPS 端點加密之外，您也可以將您的 WorkSpaces 加密。如需詳細資訊，請參閱 加密 WorkSpaces。

需求

- 您必須在具有 FedRAMP 授權或符合 DoD SRG 規範的美國 AWS 地區中建立您的 WorkSpaces。
- WorkSpaces 目錄必須設定為使用 FIPS 140-2 驗證模式進行端點加密。

> **Note**
>
> 若要使用 FIPS 140-2 驗證模式設定，WorkSpaces 目錄必須是新的，或目錄中所有現有的 WorkSpaces 都必須使用 FIPS 140-2 驗證模式進行端點加密。否則，您無法使用此設定，因此您建立的 WorkSpaces 將不符合 FedRAMP 或 DoD 安全需求。

- 使用者必須從下列其中一個 WorkSpaces 用戶端應用程式存取其 WorkSpaces：
  - Windows：2.4.3 或更新版本
  - macOS：2.4.3 或更新版本
  - Linux：3.0.0 或更新版
  - iOS：2.4.1 或更新版本
  - Android：2.4.1 或更新版本
  - Fire 平板電腦：2.4.1 或更新版本
  - ChromeOS：2.4.1 或更新版本
  - Web Access

使用 FIPS 端點加密

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 確認您要在其中建立已獲 FedRAMP 授權且符合 DOD SRG 規範之 WorkSpaces 的目錄沒有任何與其相關聯的現有 WorkSpaces。如果有與此目錄相關聯的 WorkSpaces，且尚未啟用目錄以使用 FIPS 140-2 驗證模式，請終止 WorkSpaces 或建立新目錄。
4. 選擇符合上述條件的目錄，然後依序選擇動作、更新詳細資訊。
5. 在更新目錄詳細資訊頁面上，選擇箭號以展開存取控制選項區段。
6. 針對端點加密，選擇 FIPS 140-2 驗證模式，而不是 TLS 加密模式 (標準)。
7. 選擇更新並結束。

8. 您現在可以從這個目錄建立已獲 FedRAMP 授權且符合 DoD SRG 規範的 WorkSpaces。若要存取這些 WorkSpaces，使用者必須使用需求一節中先前所列的其中一個 WorkSpaces 用戶端應用程式。

為您的 Linux 啟用安全殼層連線 WorkSpaces

如果您或您的使用者想要使用命令列連線到 Amazon Linux WorkSpaces ，您可以啟用 SSH 連線。您可以啟用 SSH 連線至目錄 WorkSpaces 中的所有人或目錄 WorkSpaces 中的個別連線。

若要啟用 SSH 連線，您可以建立新的安全群組或更新現有安全群組，並為此目的新增規則來允許輸入流量。安全群組就像是防火牆，用於關聯的執行個體，可在執行個體層級控制傳入及傳出流量。建立或更新安全群組後，您的使用者和其他使用者可以使用 PuTTY 或其他終端機，從他們的裝置連接到 Amazon Linux WorkSpaces。如需詳細資訊，請參閱 the section called “安全群組”。

有關視頻教程，請參閱如何 WorkSpaces 使用 SSH 連接到我的 Linux Amazon？ 在 AWS 知識中心。

目錄

Amazon Linux 的 SSH 連接的先決條件 WorkSpaces

- 啟用傳入 SSH 流量至 WorkSpace — 若要新增規則以允許一個或多個 Amazon Linux 的輸入 SSH 流量 WorkSpaces，請確定您擁有需要 SSH 連線至您的裝置的公有或私有 IP 地址 WorkSpaces。例如，您可以指定虛擬私有雲 (VPC) 外部裝置的公有 IP 地址，或在與您的 VPC 相同的 VPC 中指定另一個 EC2 執行個體的私有 IP 地址。 WorkSpace

  如果您打算 WorkSpace 從本地設備連接到，則可以在互聯網瀏覽器中使用搜索短語「我的 IP 地址是什麼」或使用以下服務：檢查 IP。
- 連線到 WorkSpace — 若要啟動從裝置到 Amazon Linux 的安全殼層連線，需要下列資訊 WorkSpace。
  - 您所連線到的 Active Directory 網域的 NetBIOS 名稱。

- 您的 WorkSpace 使用者名稱。
- 您要連線到的公用 WorkSpace 或私人 IP 位址。

  私人：如果您的 VPC 私人雲端已連接至公司網路，而且您可以存取該網路，則可以指定. WorkSpace

  公用：如果您 WorkSpace 有公用 IP 位址，您可以使用 WorkSpaces 主控台尋找公用 IP 位址，如下列程序所述。

若要尋找您想要連線到的 Amazon Linux WorkSpace 的 IP 位址和您的使用者名稱

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇 WorkSpaces。
3. 在的清單中 WorkSpaces，選擇您 WorkSpace 要啟用 SSH 連線的目標。
4. 在「執行模式」欄中，確認狀 WorkSpace態為「可用」。
5. 按一下 WorkSpace 名稱左側的箭頭以顯示內嵌摘要，並注意下列資訊：
   - 該 WorkSpace IP。這是的私人 IP 位址 WorkSpace。

     取得與相關聯的 elastic network interface 需要私有 IP 位址 WorkSpace。需要網路介面才能擷取資訊，例如安全性群組或與相關聯的公用 IP 位址 WorkSpace。
   - WorkSpace 使用者名稱。這是您指定要連線到的使用者名稱 WorkSpace。
6. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
7. 在導覽窗格中，選擇 Network Interfaces (網路介面)。
8. 在搜尋方塊中，輸入您在步驟 5 中記下的 WorkSpace IP。
9. 選取與 WorkSpaceIP 相關聯的網路介面。
10. 如果您 WorkSpace 有公用 IP 位址，它會顯示在「IPv4 公用 IP」欄中。請記下此位址 (若適用)。

若要尋找您所連線到的 Active Directory 網域的 NetBIOS 名稱

1. 請在以下位置開啟 AWS Directory Service 主控台。 https://console.aws.amazon.com/directoryservicev2/
2. 在目錄清單中，按一下目錄的目錄 ID 連結 WorkSpace。
3. 在目錄詳細資料區段中，記下目錄 NetBIOS 名稱。

啟用 SSH 連線至目錄 WorkSpaces 中所有 Amazon Linux

若要啟用目錄中所有 Amazon Linux WorkSpaces 的 SSH 連線，請執行下列動作。

使用規則建立安全群組，以允許目錄 WorkSpaces 中所有 Amazon Linux 的輸入 SSH 流量

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇 Create Security Group (建立安全群組)。
4. 為您的安全群組輸入名稱和 (選擇) 描述。
5. 對於 VPC，請選擇包含您要啟用 SSH 連線的 VPC。 WorkSpaces
6. 在傳入索引標籤上，選擇新增規則，然後執行下列操作：
   - 針對 Type (類型)，選擇 SSH。
   - 針對通訊協定，當您選擇 SSH 時會自動指定 TCP。
   - 針對連接埠範圍，當您選擇 SSH 時會自動指定 22。
   - 對於來源，指定使用者將用來連線到其 WorkSpaces電腦的公用 IP 位址的 CIDR 範圍。例如，企業網路或家用網路。
   - (選用) 針對描述，輸入規則的描述。
7. 選擇建立。

Amazon Linux 2 中基於密碼的身份驗證 WorkSpaces

在 2023 年 11 月 10 日之前 WorkSpaces 推出的 Amazon Linux 2 預設會啟用 SSH 密碼驗證。對於 Amazon Linux 2 十一月後 WorkSpaces 推出 10. 預設會停用 SSH 密碼驗證。

在現有 Amazon Linux 2 WorkSpaces 執行個體中停用密碼身份驗證

1. 啟動 WorkSpaces 客戶端並登錄到您的 WorkSpace.
2. 開啟終端機視窗 (應用程式 > 系統工具 > MATE 終端機)。
3. 在 [終端機] 視窗中，執行下列命令。

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

在新建立的 Amazon Linux 2 WorkSpaces 執行個體中啟用密碼身份驗證

1. 啟動 WorkSpaces 客戶端並登錄到您的 WorkSpace.
2. 開啟終端機視窗 (應用程式 > 系統工具 > MATE 終端機)。
3. 在 [終端機] 視窗中，執行下列命令。

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

與 Ubuntu 不同 WorkSpaces，Amazon Linux 2 WorkSpaces 默認情況下不會在自定義映像中保留 SSH 密碼身份驗證設置。如果您想要在 Amazon Linux 2 中預設啟用 SSH 密碼身份驗證從自訂映像 WorkSpaces 佈建，除了啟用密碼身份驗證之外，還必須變更`/etc/cloud/cloud.cfg`檔案以移除建立自訂映像`ssh_pwauth`時包含的行。若要變更 `/etc/cloud/cloud.cfg` 檔案，請執行下列命令：

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

啟用 SSH 連線到特定的 Amazon Linux WorkSpace

若要啟用與特定 Amazon Linux 的 SSH 連線 WorkSpace，請執行下列動作。

將規則新增至現有安全群組，以允許對特定 Amazon Linux 的輸入安全殼層流量 WorkSpace

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 Network & Security (網路與安全) 中，選擇 Network Interfaces (網路界面)。
3. 在搜尋列中，輸入您要啟用 SSH 連線的私人 IP 位址。 WorkSpace
4. 在安全群組欄中，按一下安全群組的連結。
5. 在 Inbound (傳入) 標籤上，選擇 Edit (編輯)。
6. 選擇新增規則，然後執行下列操作：
   - 針對 Type (類型)，選擇 SSH。
   - 針對通訊協定，當您選擇 SSH 時會自動指定 TCP。
   - 針對連接埠範圍，當您選擇 SSH 時會自動指定 22。
   - 針對來源，選擇我的 IP 或自訂，然後以 CIDR 標記法指定單一 IP 地址或 IP 地址範圍。例如，若您的 IPv4 地址為 `203.0.113.25`，請指定 `203.0.113.25/32`，藉此以 CIDR 表示法列出此單一 IPv4 地址。如果您的公司會分配某個範圍的地址，請指定整個範圍 (例如 `203.0.113.0/24`)。

- (選用) 針對描述，輸入規則的描述。

7. 選擇儲存。

WorkSpace 使用 Linux 或 PuTTY Connect 到 Amazon Linux

在您建立或更新安全性群組並新增必要規則之後，您的使用者和其他使用者可以使用 Linux 或 PuTTY 將其裝置連線到您 WorkSpaces的裝置。

> **Note**
>
> 完成下列任一程序之前，請確定您有下列各項：
>
> - 您所連線到的 Active Directory 網域的 NetBIOS 名稱。
> - 您用來連線到的使用者名稱 WorkSpace。
> - 您要連線到的公用 WorkSpace 或私人 IP 位址。
>
> 如需有關如何取得此資訊的指示，請參閱本主題稍早的「SSH 連線至 Amazon Linux 的先決條件 WorkSpaces」。

若要 WorkSpace 使用 Linux 連線到 Amazon Linux

1. 以管理員身分開啟命令提示並輸入下列命令。針對 *NetBIOS ##*、*#用者名稱*和 *WorkSpace IP*，輸入適用的值。

```
ssh "NetBIOS_NAME\Username"@WorkSpaceIP
```

以下是 SSH 命令的範例，其中：

- *NetBIOS_NAME* 是任何公司
- *Username* 是 janedoe
- *WorkSpace IP ### 203.* 0.113.25

```
ssh "anycompany\janedoe"@203.0.113.25
```

2. 出現提示時，請輸入與用 WorkSpaces 戶端進行驗證時所使用的相同密碼 (您的 Active Directory 密碼)。

WorkSpace 使用 PuTTY 連接到 Amazon Linux

1. 開啟 PuTTY。
2. 在 PuTTY 組態對話方塊中，執行下列操作：

   - 針對主機名稱 (或 IP 地址)，輸入下列命令。將這些值取代為您連線到的使用中目錄網域的 NetBIOS 名稱、用來連線到的使用者名稱 WorkSpace，以及您要連線到的 IP 位址。WorkSpace

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

   - 針對連接埠，輸入 **22**。
   - 針對連線類型，選擇 SSH。

   如需 SSH 命令的範例，請參閱先前程序中的步驟 1。
3. 選擇 Open (開啟)。
4. 出現提示時，請輸入與用 WorkSpaces 戶端進行驗證時所使用的相同密碼 (您的 Active Directory 密碼)。

所需的組態和服務元件 WorkSpaces

WorkSpace 身為系統管理員，您必須瞭解下列必要組態與服務元件的相關資訊。

- the section called “路由表組態”
- the section called “Windows 的元件”
- the section called “Linux 的元件”
- the section called “Ubuntu 的元件”

所需的路由表組態

建議您不要修改的作業系統層次路由表格。 WorkSpace此 WorkSpaces 服務需要此表格中預先設定的路由，才能監視系統狀態並更新系統元件。如果您的組織需要變更路由表格，請在套用任何變更之前聯絡 Sup AWS port 部門或您的 AWS 客戶團隊。

Windows 所需的服務元件

在 Windows 上 WorkSpaces，服務元件會安裝在下列位置。請勿刪除、變更、封鎖或隔離這些物件。如果這樣做， WorkSpace 將無法正常運作。

如果已安裝防毒軟體 WorkSpace，請確定它不會干擾安裝在下列位置的服務元件。

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

32 位元 PCoIP 代理程式

截至 2021 年 3 月 29 日為止，我們已將 PCoIP 代理程式從 32 位元更新為 64 位元。對於使用 PCoIP 通訊協定的視窗 WorkSpaces ，這表示 Terdici 檔案的位置會從變更為。`C:\Program Files (x86)\Teradici` `C:\Program Files\Teradici`由於我們在定期維護期間更新了 PCoIP 代理程式，因此在轉換期間，有些使用 32 位元代理程式的時間 WorkSpaces 可能比其他代理程式長。

如果您已設定防火牆規則、防毒軟體排除項目 (在用戶端和主機端)、群組政策物件 (GPO) 設定或 Microsoft System Center Configuration Manager (SCCM)、Microsoft Endpoint Configuration Manager 或類似組態管理工具 (以 32 位元代理程式的完整路徑為基礎) 的設定，您也必須將 64 位元代理程式的完整路徑新增至這些設定。

如果您要篩選任何 32 位元 PCoIP 元件的路徑，務必將路徑新增至 64 位元版本的元件。由於您 WorkSpaces 可能不會同時更新所有內容，因此請勿將 32 位路徑替換為 64 位路徑，否則某些路徑 WorkSpaces 可能無法正常工作。例如，如果您是以 `C:\Program Files (x86)\Teradici \PCoIP Agent\bin\pcoip_server_win32.exe` 作為排除項目或通訊篩選條件的基礎，您也必須

新增 C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe。同樣地，如果您是以 C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe 作為排除項目或通訊篩選條件的基礎，您也必須新增 C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe。

PCoIP 仲裁者服務變更 — 請注意，當您 WorkSpaces 更新為使用 64 位元代理程式時，會移除 PCoIP 仲裁者服務 (C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe)。

PCoIP 零用戶端和 USB 裝置 — 從 PCoIP 代理程式 20.10.4 版開始，Amazon 預設會透過 Windows 登錄 WorkSpaces 停用 USB 重新導向。當您的使用者使用 PCoIP 零用戶端裝置連線至 USB 周邊裝置時，此登錄設定會影響 USB 周邊設備的行為。 WorkSpaces如需詳細資訊，請參閱 USB 印表機和其他 USB 周邊設備不適用於 PCoIP 零客戶端。

Linux 所需的服務元件

在 Amazon Linux 上 WorkSpaces，服務元件安裝在下列位置。請勿刪除、變更、封鎖或隔離這些物件。如果這樣做， WorkSpace將無法正常運作。

> **Note**
>
> 對其他檔案進行變更/etc/pcoip-agent/pcoip-agent.conf可能會導 WorkSpaces 致您停止運作，並可能需要您重新建置它們。如需修改 /etc/pcoip-agent/pcoip-agent.conf 的詳細資訊，請參閱 管理您的 Amazon Linux WorkSpaces。

- /etc/dhcp/dhclient.conf
- /etc/logrotate.d/pcoip-agent
- /etc/logrotate.d/pcoip-server
- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf

- /etc/systemd/system/euc-analytic-agent.service
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp

- /var/log/eucanalytics

Ubuntu 所需的服務元件

在 Ubuntu 上 WorkSpaces，服務元件安裝在下列位置。請勿刪除、變更、封鎖或隔離這些物件。如果這樣做， WorkSpace將無法正常運作。

- /etc/X11/default-display-manager
- /etc/X11/xorg.conf
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /etc/systemd/system/euc-analytic-agent.service
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

管理 WorkSpaces 的目錄

WorkSpaces 會使用目錄來儲存和管理 WorkSpaces 和使用者的資訊。您可以使用下列其中一個選項：

- AD Connector—使用現有的內部部署 Microsoft Active Directory。使用者可以使用其內部部署憑證來登入其 WorkSpaces，並從其 WorkSpaces 存取內部部署資源。
- AWS Managed Microsoft AD—建立在 AWS 上託管的 Microsoft Active Directory。
- Simple AD—建立與 Microsoft Active Directory 相容並在 AWS 上託管的目錄 (由 Samba 4 提供支援)。
- 交叉信任—建立 AWS Managed Microsoft AD 與內部部署網域之間的信任關係。

如需示範如何設定這些目錄和啟動 WorkSpaces 的教學課程，請參閱 使用 WorkSpaces 啟動虛擬桌面。

> **Tip**
>
> 如需各種部署案例的目錄和虛擬私有雲端 (VPC) 設計考量的詳細探索，請參閱部署 Amazon WorkSpaces 的最佳實務。

建立目錄之後，您會使用 Active Directory 管理工具等工具來執行大部分的目錄管理工作。您可使用 WorkSpaces 主控台來執行某些目錄管理任務，並使用群組原則來執行其他任務。如需管理使用者和群組的詳細資訊，請參閱 管理 WorkSpaces 使用者 和 設定 WorkSpaces 的 Active Directory 管理工具。

> **Note**
>
> - 共用目錄目前不支援搭配 Amazon WorkSpaces 使用。
> - 如果您針對多區域複寫設定 AWS Managed Microsoft AD 目錄，則只能註冊主要區域中的目錄以便與 Amazon WorkSpaces 搭配使用。嘗試在複寫的區域中註冊目錄以搭配 Amazon WorkSpaces 使用將會失敗。AWS Managed Microsoft AD 的多區域複寫不支援搭配複寫區域內的 Amazon WorkSpaces 使用。
> - 您可以免費使用 Simple AD 和 AD Connector，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 或 AD Connector 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。

若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 Simple AD 或 AD Connector 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

目錄

向 WorkSpaces 註冊目錄

若要允許 WorkSpaces 使用現有的 AWS Directory Service 目錄，您必須向 WorkSpaces 註冊該目錄。註冊目錄之後，您可以在目錄中啟動 WorkSpaces。

需求

若要註冊目錄以便搭配 WorkSpaces 使用，必須滿足下列需求：

- 如果您使用 AWS Managed Microsoft AD 或 Simple AD，只要目錄可存取 WorkSpaces 所在的 VPC，您的目錄即可位於專用的私有子網路中。

如需目錄和 VPC 設計的詳細資訊，請參閱部署 Amazon WorkSpaces 的最佳實務白皮書。

> **Note**
>
> 您可以免費使用 Simple AD 和 AD Connector，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 或 AD Connector 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。
>
> 若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 Simple AD 或 AD Connector 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

註冊目錄

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選取目錄。
4. 選擇動作、註冊。

> **Note**
>
> - 共用目錄目前不支援搭配 Amazon WorkSpaces 使用。
> - 如果已針對多區域複寫設定 AWS Managed Microsoft AD 目錄，則只能註冊主要區域中的目錄，以便搭配 Amazon WorkSpaces 使用。嘗試在複寫的區域中註冊目錄以搭配 Amazon WorkSpaces 使用將會失敗。AWS Managed Microsoft AD 的多區域複寫不支援搭配複寫區域內的 Amazon WorkSpaces 使用。

5. 為您的 VPC 選取並非來自相同可用區域的兩個子網路。這些子網路將用來啟動您的 WorkSpaces。如需詳細資訊，請參閱 Amazon 的可用區域 WorkSpaces。

> **Note**
>
> 如果您不知道要選擇哪些子網路，請選取無偏好設定。

6. 針對啟用自助服務許可，選擇是可讓使用者重新建置其 WorkSpaces、變更磁碟區大小、運算類型和執行模式。啟用可能會影響您針對 Amazon WorkSpaces 支付的費用。否則選擇否。
7. 針對啟用 Amazon WorkDocs，選擇是來註冊目錄，以便搭配 Amazon WorkDocs 搭配，否則選擇否。

> **Note**
>
> 只有在 Amazon WorkDocs 適用於區域，而且您並未使用 AWS Managed Microsoft AD 時，才會顯示此選項。如果您正在使用 AWS Managed Microsoft AD，請完成您的目錄註冊，然後查看 為 AWS Managed Microsoft AD 啟用 Amazon WorkDocs。

8. 選擇 Register (註冊)。最初已註冊的值為 `REGISTERING`。註冊完成後，此值為 `Yes`。

當您完成搭配 WorkSpaces 使用目錄之後，即可將其取消註冊。請注意，您必須先取消註冊目錄，才能加以刪除。如果您想要取消註冊並刪除目錄，您必須先尋找並移除註冊到目錄的所有應用程式和服務。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的刪除目錄。

取消註冊目錄

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選取目錄。
4. 選擇 Actions (動作)、Deregister (取消註冊)。
5. 出現確認的提示時，請選擇 Deregister (取消註冊)。取消註冊完成後，已註冊的值為 No。

更新您的目錄詳細資料 WorkSpaces

您可以使用 WorkSpaces 主控台完成下列目錄管理工作。

任務

- 選取組織單位
- 設定自動公用 IP 位址
- 控制裝置存取
- 管理本機管理員許可
- 更新 AD Connector 帳戶 (AD Connector)
- 多重要素驗證 (AD Connector)

選取組織單位

WorkSpace 機器帳戶會放置在 WorkSpaces 目錄的預設組織單位 (OU) 中。一開始，機器帳戶會放置於您目錄的電腦 OU 或 AD Connector 連線至的目錄中。您可以從目錄或連線的目錄中選取不同的 OU，或在不同的目標網域中指定 OU。請注意，您只能為每個目錄選取一個 OU。

選取新 OU 之後，所有 WorkSpaces 已建立或重建的機器帳戶都會放置在新選取的 OU 中。

選取組織單位

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。

3. 選擇您的目錄。
4. 在 [目標網域和組織單位] 下，選擇 [編輯]。
5. 若要尋找 OU，您可以在 [目標和組織單位] 底下開始輸入全部或部分 OU 名稱，然後選擇要使用的 OU。
6. (選擇性) 選擇 OU 偽裝名稱，以自訂 OU 覆寫您選取的 OU。
7. 選擇儲存。
8. (選擇性) 重建現有的， WorkSpaces 以更新 OU。如需詳細資訊，請參閱 重建 WorkSpace。

設定自動公用 IP 位址

啟用自動分配公共 IP 地址後，您啟動的每 WorkSpace 個 IP 地址都會從 Amazonon 提供的公共地址池中分配一個公共 IP 地址。公共子網 WorkSpace 中的 A 可以通過互聯網網關訪問互聯網，如果它有一個公共 IP 地址。 WorkSpaces 在啟用自動指派之前已存在的項目，除非您重建公用位址，否則不會接收公用位址。

請注意，如果您 WorkSpaces 位於私有子網路中，並且已為虛擬私人雲端 (VPC) 設定 NAT 閘道，或者您位於公用子網路中且已為其指派彈性 IP 位址，則不需要啟用自動指派公用位址。 WorkSpaces 如需詳細資訊，請參閱 設定虛 VPC WorkSpaces。

> **Warning**
>
> 如果您將擁有的彈性 IP 地址關聯到一個 WorkSpace，然後您稍後將該彈性 IP 地址與中斷關聯 WorkSpace，則會 WorkSpace 丟失其公共 IP 地址，並且不會自動從 Amazonon 提供的池中獲取新 IP 地址。若要將 Amazon 提供的集區中的新公用 IP 位址與相關聯 WorkSpace，您必須重建. WorkSpace 如果您不想重建 WorkSpace，則必須將您擁有的另一個彈性 IP 地址與 WorkSpace.

設定彈性 IP 位址

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選取您的目錄 WorkSpaces。
4. 選擇動作、更新詳細資訊。
5. 展開存取網際網路，然後選取啟用或停用。
6. 選擇更新。

控制裝置存取

您可以指定具有存取權限的裝置類型 WorkSpaces。此外，您可以限制對 WorkSpaces 受信任裝置 (也稱為受管理裝置) 的存取。

若要控制裝置存取 WorkSpaces

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選擇您的目錄。
4. 在存取控制選項下，選擇編輯。
5. 在 [信任的裝置] 下，選取 WorkSpaces [允許所有裝置]、[信任的裝置] 或 [全部拒絕]，以指定可存取的裝置類型 如需詳細資訊，請參閱 限制對 WorkSpaces 受信任設備的訪問。
6. 選擇 Save (儲存)。

管理本機管理員許可

您可以指定使用者是否為其上的本機管理員 WorkSpaces，這樣他們就可以在其上安裝應用程式和修改設定 WorkSpaces。依預設，使用者是本機管理員。如果您修改此設定，變更會套用至您建立的所有新項目 WorkSpaces 以及您重新建立 WorkSpaces 的任何項目。

修改本機管理員許可

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選擇您的目錄。
4. 在 [本機管理員設定] 下，選擇 [編輯
5. 若要確保使用者是本機管理員，請選擇 [啟用本機管理員設定]。
6. 選擇儲存。

更新 AD Connector 帳戶 (AD Connector)

您可以更新用來讀取使用者和群組，以及將 WorkSpaces 機 AD Connector 帳戶加入 AD 連接器目錄的 AD 連接器帳戶。

更新 AD Connector 帳戶

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選取目錄，然後選擇 [檢視詳細資料]。
4. 在 AD 連接器帳戶下，選擇 [編輯]。
5. 輸入新帳戶的登入憑證。
6. 選擇儲存。

多重要素驗證 (AD Connector)

您可為 AD Connector 目錄啟用多重要素驗證 (MFA)。如需搭配 AWS Directory Service 使用多重要素驗證的詳細資訊，請參閱為 AD Connector 啟用多重要素驗證和 AD Connector 先決條件。

> **Note**
>
> - 您的 RADIUS 伺服器可以由 AWS 託管，也可以內部部署。
> - 使用者名稱必須在 Active Directory 與 RADIUS 伺服器之間相符。

啟用多重要素驗證

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選取您的目錄，然後依序選擇動作、更新詳細資訊。
4. 展開多重要素驗證，然後選取啟用多重要素驗證。
5. 對於 RADIUS 伺服器 IP 位址，輸入 RADIUS 伺服器端點的 IP 位址 (以逗號分隔)，或輸入 RADIUS 伺服器負載平衡器的 IP 位址。
6. 針對連接埠，輸入 RADIUS 伺服器用於通訊的連接埠。您的內部部署網路必須允許 AD Connector 透過預設 RADIUS 伺服器連接埠 (UDP:1812) 傳入流量。
7. 針對共用秘密代碼和確認共用秘密代碼，輸入 RADIUS 伺服器的共用秘密代碼。
8. 針對通訊協定，選擇 RADIUS 伺服器的通訊協定。
9. 針對伺服器逾時，輸入等待 RADIUS 伺服器回應的時間 (以秒為單位)。此值必須介於 1 到 50。
10. 針對最大重試次數，輸入嘗試與 RADIUS 伺服器通訊的次數。此值必須介於 0 到 10。

11. 選擇更新並結束。

當 RADIUS 狀態 為啟用時，即可使用多重要素驗證。在設置多因素身份驗證時，用戶無法登錄到他們WorkSpaces的.

更新 Amazon WorkSpaces 的 DNS 伺服器

如果您需要在啟動 WorkSpaces 之後更新 Active Directory 的 DNS 伺服器 IP 位址，您也必須使用新的 DNS 伺服器設定來更新您的 WorkSpaces。

您可使用下列其中一種方式，使用新的 DNS 設定來更新 WorkSpaces：

- 在更新 Active Directory 的 DNS 設定之前，請先更新 WorkSpaces 上的 DNS 設定。
- 更新 Active Directory 的 DNS 設定之後，請重新建置 WorkSpaces。

我們建議在更新 Active Directory 中的 DNS 設定之前，先更新 WorkSpaces 上的 DNS 設定 (如下列程序的步驟 1 所述)。

如果您想要改為重新建置 WorkSpaces，請更新 Active Directory 中的其中一個 DNS 伺服器 IP 位址 (步驟 2)，然後依照 重建 WorkSpace 中的程序重新建置 WorkSpaces。重新建置 WorkSpaces 之後，請依照步驟 3 中的程序來測試 DNS 伺服器更新。完成該步驟之後，請在 Active Directory 中更新第二個 DNS 伺服器的 IP 位址，然後再次重新建置 WorkSpaces。務必遵循步驟 3 中的程序來測試您的第二個 DNS 伺服器更新。如最佳實務一節所述，建議您一次更新一個 DNS 伺服器 IP 位址。

最佳實務

當您更新 DNS 伺服器設定時，建議您採用下列最佳實務：

- 為了避免網域資源中斷連線和無法存取，我們強烈建議您在離峰時間或在計劃的維護期間執行 DNS 伺服器更新。
- 請勿在變更 DNS 伺服器設定的前 15 分鐘和後 15 分鐘內啟動任何新的 WorkSpaces。
- 更新 DNS 伺服器設定時，請一次變更一個 DNS 伺服器 IP 位址。在更新第二個 IP 位址之前，請先確認第一次更新正確無誤。我們建議您執行下列程序兩次 (步驟 1、步驟 2 和步驟 3)，以便一次更新一個 IP 位址。

步驟 1：更新 WorkSpaces 上的 DNS 伺服器設定

在下列程序中，目前和新的 DNS 伺服器 IP 位址值參考如下：

- 目前的 DNS IP 位址：*OldIP1*、*OldIP2*
- 新的 DNS IP 位址：*NewIP1*、*NewIP2*

> **Note**
>
> 如果這是您第二次執行此程序，請以 *OldIP2* 取代 *OldIP1* 和以 *NewIP2* 取代 *NewIP1*。

更新 Windows WorkSpaces 的 DNS 伺服器設定

如果您有多個 WorkSpaces，您可以在 WorkSpaces 的 Active Directory OU 上套用群組政策物件 (GPO)，將下列登錄更新部署至 WorkSpaces。如需使用 GPO 的詳細資訊，請參閱 管理您的視窗 WorkSpaces。

您可以使用登錄編輯程式或使用 Windows PowerShell 進行這些更新。本節將說明這兩個程序。

使用登錄編輯程式更新 DNS 登錄設定

1. 在 Windows WorkSpace 上，開啟 Windows 搜尋方塊，然後輸入 **`registry editor`** 以開啟登錄編輯程式 (regedit.exe)。
2. 當系統詢問「您要允許此應用程式對裝置進行變更嗎？」時，請選擇是。
3. 在登錄編輯程式中，導覽至下列登錄項目：

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight
4. 開啟 DomainJoinDns 登錄機碼。使用 *NewIP1* 更新 *OldIP1*，然後選擇確定。
5. 關閉登錄編輯程式。
6. 重新啟動 WorkSpace，或重新啟動 SkyLightWorkspaceConfigService 服務。

   > **Note**
   >
   > 重新啟動 SkyLightWorkspaceConfigService 服務之後，網路介面卡最多可能需要 1 分鐘才會反映變更。
7. 繼續進行步驟 2，並在 Active Directory 中更新 DNS 伺服器設定以使用 *NewIP1* 取代 *OldIP1*。

使用 PowerShell 更新 DNS 登錄設定

下列程序會使用 PowerShell 命令來更新您的登錄，並重新啟動 SkyLightWorkspaceConfigService 服務。

1. 在 Windows WorkSpace 上，開啟 Windows 搜尋方塊，然後輸入 **powershell**。選擇以管理員身分執行。
2. 當系統詢問「您要允許此應用程式對裝置進行變更嗎？」時，請選擇是。
3. 在 PowerShell 視窗中，執行下列命令以擷取目前的 DNS 伺服器 IP 位址。

```
Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
```

您應該會收到以下輸出。

```
DomainJoinDns : OldIP1,OldIP2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon\SkyLight
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon
PSChildName   : SkyLight
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

4. 在 PowerShell 視窗中，執行下列命令，將 *OldIP1* 變更為 *NewIP1*。務必暫時將 *OldIP2* 保持原樣。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
 "NewIP1,OldIP2"
```

5. 執行下列命令以重新啟動 SkyLightWorkspaceConfigService 服務。

```
restart-service -Name SkyLightWorkspaceConfigService
```

> **Note**
>
> 重新啟動 SkyLightWorkspaceConfigService 服務之後，網路介面卡最多可能需要 1 分鐘才會反映變更。

6. 繼續進行步驟 2，並在 Active Directory 中更新 DNS 伺服器設定以使用 *NewIP1* 取代 *OldIP1*。

更新 Linux WorkSpaces 的 DNS 伺服器設定

如果您有多個 Linux WorkSpace，建議您使用組態管理解決方案來散發和強制執行政策。例如，您可以使用 AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise 或 Ansible。

在 Linux WorkSpace 上更新 DNS 伺服器設定

1. 在 Linux WorkSpace 上，開啟終端視窗 (應用程式 > 系統工具 > MATE 終端)。
2. 使用以下 Linux 命令來編輯 `/etc/dhcp/dhclient.conf` 檔案。您必須擁有 root 使用者權限才能編輯此檔案。使用 `sudo -i` 命令以成為 root，或者如下所示使用 `sudo` 執行所有命令。

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   在 `/etc/dhcp/dhclient.conf` 檔案中，您將看到以下 `prepend` 命令，其中 *`OldIP1`* 和 *`OldIP2`* 是 DNS 伺服器的 IP 位址。

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```
3. 以 *`NewIP1`* 取代 *`OldIP1`*，並且暫時將 *`OldIP2`* 保持原樣。
4. 將您的變更儲存至 `/etc/dhcp/dhclient.conf`。
5. 重新啟動 WorkSpace。
6. 繼續進行步驟 2，並在 Active Directory 中更新 DNS 伺服器設定以使用 *`NewIP1`* 取代 *`OldIP1`*。

步驟 2：更新 Active Directory 的 DNS 伺服器設定

在此步驟中，您會更新 Active Directory 的 DNS 伺服器設定。如最佳實務一節所述，建議您一次更新一個 DNS 伺服器 IP 位址。

若要更新 Active Directory 的 DNS 伺服器設定，請參閱《AWS Directory Service 管理指南》中的下列文件：

- AD Connector：更新 AD Connector 的 DNS 位址
- AWS Managed Microsoft AD：為內部部署網域設定 DNS 條件式轉寄站
- Simple AD：設定 DNS

更新 DNS 伺服器設定之後，請繼續執行步驟 3。

步驟 3：測試已更新的 DNS 伺服器設定

完成步驟 1 和步驟 2 之後，請使用下列程序來確認已更新的 DNS 伺服器設定是否如預期般運作。

在下列程序中，目前和新的 DNS 伺服器 IP 位址值參考如下：

- 目前的 DNS IP 位址：*OldIP1*、*OldIP2*
- 新的 DNS IP 位址：*NewIP1*、*NewIP2*

> **Note**
>
> 如果這是您第二次執行此程序，請以 *OldIP2* 取代 *OldIP1* 和以 *NewIP2* 取代 *NewIP1*。

測試 Windows WorkSpaces 的已更新 DNS 伺服器設定

1. 關閉 *OldIP1* DNS 伺服器。
2. 登入 Windows WorkSpace。
3. 在 Windows Start (開始) 功能表，選擇 Windows System (Windows 系統)，然後選擇 Command Prompt (命令提示字元)。
4. 執行下列命令，其中 *AD_Name* 是 Active Directory 的名稱 (例如，`corp.example.com`)。

   ```
   nslookup AD_Name
   ```

   nslookup 命令應該會傳回下列輸出。(如果這是您第二次執行此程序，您應該會看到 *NewIP2* 代替 *OldIP2*。)

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```
5. 如果輸出不是您預期的輸出，或者您收到任何錯誤，請重複步驟 1。
6. 請等待一個小時，確認沒有回報任何使用者問題。確認 *NewIP1* 正在取得 DNS 查詢並回應答案。
7. 確認第一個 DNS 伺服器運作正常之後，請重複步驟 1 來更新第二個 DNS 伺服器，這次會以 *NewIP2* 取代 *OldIP2*。然後重複步驟 2 和步驟 3。

測試 Linux WorkSpaces 的已更新 DNS 伺服器設定

1. 關閉 *OldIP1* DNS 伺服器。
2. 登入 Linux WorkSpace。
3. 在 Linux WorkSpace 上，開啟終端視窗 (應用程式 > 系統工具 > MATE 終端)。
4. DHCP 回應中傳回的 DNS 伺服器 IP 位址會寫入 WorkSpace 上的本機 `/etc/resolv.conf` 檔案。執行下列命令以檢視 `/etc/resolv.conf` 檔案的內容。

```
cat /etc/resolv.conf
```

您應該會看到下列輸出。(如果這是您第二次執行此程序，您應該會看到 *NewIP2* 代替 *OldIP2*。)

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> 如果您手動修改 `/etc/resolv.conf` 檔案，則當 WorkSpace 重新啟動時，這些變更就會遺失。

5. 如果輸出不是您預期的輸出，或者您收到任何錯誤，請重複步驟 1。
6. 實際的 DNS 伺服器 IP 位址會儲存在 `/etc/dhcp/dhclient.conf` 檔案中。若要查看此檔案的內容，請執行以下命令。

```
sudo cat /etc/dhcp/dhclient.conf
```

您應該會看到下列輸出。(如果這是您第二次執行此程序，您應該會看到 *NewIP2* 代替 *OldIP2*。)

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. 請等待一個小時，確認沒有回報任何使用者問題。確認 *NewIP1* 正在取得 DNS 查詢並回應答案。
8. 確認第一個 DNS 伺服器運作正常之後，請重複步驟 1 來更新第二個 DNS 伺服器，這次會以 *NewIP2* 取代 *OldIP2*。然後重複步驟 2 和步驟 3。

刪除 WorkSpaces 的目錄

如果 WorkSpaces 目錄不再由其他 WorkSpaces 或其他應用程式 (例如 Amazon WorkDocs、Amazon WorkMail 或 Amazon Chime) 使用，即可加以刪除。請注意，您必須先取消註冊目錄，才能加以刪除。

> **Note**
>
> 您可以免費使用 Simple AD 和 AD Connector，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 或 AD Connector 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。
> 如果您刪除 Simple AD 或 AD Connector 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

刪除目錄時會發生什麼狀況

刪除 Simple AD 或 AWS Directory Service for Microsoft Active Directory 目錄時，所有的目錄資料和快照都會遭到刪除，而且無法復原。刪除目錄之後，任何加入目錄的 Amazon EC2 執行個體都會保持不變。不過，您無法使用目錄憑證來登入這些執行個體。您需要使用執行個體的本機 AWS 帳戶 來登入這些執行個體。

刪除 AD Connector 目錄時，您的內部部署目錄會保持不變。任何加入目錄的 Amazon EC2 執行個體也會保持不變，並保持在已加入您內部部署目錄的狀態。您仍然可以使用目錄登入資料來登入這些執行個體。

刪除目錄

1. 刪除目錄中的所有 WorkSpaces。如需詳細資訊，請參閱 刪除 WorkSpace。
2. 尋找並移除目錄中註冊的所有應用程式和服務。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的刪除目錄。
3. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。

4. 在導覽窗格中，選擇 Directories (目錄)。
5. 選取目錄，然後依序選擇動作、取消註冊。
6. 出現確認的提示時，請選擇 Deregister (取消註冊)。
7. 再次選取目錄，然後依序選擇動作、刪除。
8. 出現確認提示時，請選擇 Delete (刪除)。

> **Note**
>
> 移除應用程式指派有時會比預期花費更多的時間。如果您收到下列錯誤訊息，請確認您已移除所有應用程式指派，然後等待 30 到 60 分鐘，再次嘗試刪除目錄：
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (選用) 刪除目錄的虛擬私有雲端 (VPC) 中的所有資源後，您可以刪除 VPC 並釋放用於 NAT 閘道的彈性 IP 位址。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的刪除 VPC和使用彈性 IP 位址。
10. (選用) 若要刪除您已完成的任何自訂套件和映像，請參閱 刪除自訂 WorkSpaces 套裝軟體或影像。

為 AWS Managed Microsoft AD 啟用 Amazon WorkDocs

如果您使用 AWS Managed Microsoft AD 搭配 Amazon WorkSpaces，您可以透過 Amazon WorkDocs 主控台或 AWS Directory Service 主控台為您的目錄啟用 Amazon WorkDocs。

> **Note**
>
> Amazon WorkDocs 不適用於可使用 Amazon WorkSpaces 的所有 AWS 區域中。如需詳細資訊，請參閱 Amazon WorkDocs 定價。

若要透過 Amazon WorkDocs 主控台啟用 WorkDocs

1. 開啟 Amazon WorkDocs 主控台，網址為 https://console.aws.amazon.com/zocalo/。
2. 選擇建立新的 WorkDocs 網站。

3. 在標準設定之下，選擇啟動。
4. 選擇目錄並建立您的網站名稱。
5. 指定將管理 WorkDocs 網站的使用者。您可以使用管理員或在目錄中建立的任何使用者。

如需詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的 AWS Managed Microsoft AD 入門。

若要透過 AWS Directory Service 主控台啟用 WorkDocs

1. 開啟 AWS Directory Service 主控台，網址為 https://console.aws.amazon.com/directoryservicev2/。
2. 在導覽窗格中，選擇目錄。
3. 在目錄頁面上，選擇您的目錄。
4. 在目錄詳細資訊頁面上，選取應用程式管理索引標籤。
5. 在應用程式存取 URL 區段中，如果尚未將存取 URL 指派給目錄，則會顯示建立按鈕。輸入目錄別名，然後選擇建立。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立存取 URL。
6. 在應用程式存取 URL 區段中，選擇啟用以啟用 Amazon WorkDocs 的單一登入。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的單一登入。

設定 WorkSpaces 的 Active Directory 管理工具

您將使用目錄管理工具 (例如 Active Directory 系統管理工具) 為 WorkSpaces 目錄執行大部分的管理工作。不過，您將使用 WorkSpaces 主控台來執行一些目錄相關任務。如需詳細資訊，請參閱 管理 WorkSpaces 的目錄。

如果您使用包含五個以上 WorkSpaces 的 AWS Managed Microsoft AD 或 Simple AD 建立目錄，建議您在 Amazon EC2 執行個體上集中管理。雖然您可以在 WorkSpace 上安裝目錄管理工具，但是使用 Amazon EC2 執行個體是更強大的解決方式。

若要安裝 Active Directory 管理工具

1. 啟動 Amazon EC2 Windows 執行個體，並使用下列其中一個選項將其加入您的 WorkSpaces 目錄：

   - 如果您還沒有現有的 Amazon EC2 Windows 執行個體，則可以在啟動執行個體時將執行個體加入目錄網域。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的無縫加入 Windows EC2 執行個體。

- 如果您已經有一個現有的 Amazon EC2 Windows 執行個體，則可以手動將其加入您的目錄。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的手動新增 Windows 執行個體。

2. 在 Amazon EC2 Windows 執行個體上安裝 Active Directory 管理工具。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的安裝 Active Directory 管理工具。

> **Note**
>
> 當您安裝 Active Directory 管理工具時，務必也選取群組政策管理來安裝群組政策管理編輯器 (gpmc.msc) 工具。

當功能安裝完成時，可以在 Windows 系統管理工具下的 Windows 開始功能表上取得 Active Directory 工具。

3. 以目錄管理員身分執行工具，如下所示：

   a. 在 Windows 開始功能表上，開啟 Windows 系統管理工具。

   b. 按住 Shift 鍵，以滑鼠右鍵按一下您要使用之工具的快速鍵，然後選擇以不同的使用者身分執行。

   c. 輸入管理員的登入認證。使用 Simple AD，使用者名稱是 **`Administrator`**，而使用 AWS Managed Microsoft AD，管理員是 **`Admin`**。

您現在可以使用您熟悉的 Active Directory 工具來執行目錄管理工作。例如，您可以使用 Active Directory 使用者和電腦工具來新增使用者、移除使用者、將使用者升級為目錄管理員，或重設使用者密碼。請注意，您必須以具有管理目錄中使用者之許可的使用者身分登入 Windows 執行個體。

若要將使用者升級為目錄管理員

> **Note**
>
> 此程序僅適用於使用 Simple AD 建立的目錄，不適用於使用 AWS Managed AD 建立的目錄。對於使用 AWS Managed AD 建立的目錄，請參閱《AWS Directory Service 管理指南》中的在 AWS Managed Microsoft AD 中管理使用者和群組。

1. 開啟 Active Directory 使用者和電腦工具。
2. 瀏覽至您網域之下的使用者資料夾，然後選取要升級的使用者。

3. 選擇動作、內容。
4. 在#####內容對話方塊中，選擇成員群組。
5. 將使用者新增至下列群組，然後選擇確定。

   - 管理員
   - 網域管理員
   - 企業管理員
   - 群組政策建立者擁有者
   - 結構描述管理員

若要新增或移除使用者

您只能在啟動 WorkSpace 的過程中從 Amazon WorkSpaces 主控台建立新使用者，而且無法透過 Amazon WorkSpaces 主控台刪除使用者。大多數使用者管理工作 (包括管理使用者群組) 都必須透過您的目錄執行。

> **Important**
>
> 您必須先刪除指派給使用者的 WorkSpace，才能移除該使用者。如需詳細資訊，請參閱 刪除 WorkSpace。

您用於管理使用者和群組的程序取決於您所使用的目錄類型。

- 如果您使用 AWS Managed Microsoft AD，請參閱《AWS Directory Service 管理指南》中的在 AWS Managed Microsoft AD 中管理使用者和群組。
- 如果您使用 Simple AD，請參閱《AWS Directory Service 管理指南》中的在 Simple AD 中管理使用者和群組。
- 如果您透過 AD Connector 或信任關係使用 Microsoft Active Directory，您可以使用 Active Directory 模組來管理使用者和群組。

若要重設使用者密碼

當您為現有使用者重設密碼時，請勿設定使用者必須在下次登入時變更密碼。否則，使用者無法連線至其 WorkSpaces。改為針對每個使用者指定安全的臨時密碼，然後要求使用者在下次登入時從 WorkSpace 內手動變更其密碼。

> **Note**
>
> 如果您使用 AD Connector，或者您的使用者位於 AWS GovCloud (美國西部) 區域，您的使用者將無法重設自己的密碼。(WorkSpaces 用戶端應用程式登入畫面上的忘記密碼？選項將無法使用。)

使用 WorkSpaces 啟動虛擬桌面

透過 WorkSpaces，您可使用者佈建虛擬、雲端式 Microsoft Windows、Amazon Linux 或 Ubuntu Linux 桌面。

> **Note**
>
> 在 Amazon WorkSpaces 主控台中針對 WorkSpace 顯示的電腦名稱值會有所不同，這取決於您啟動的 WorkSpace 類型 (Amazon Linux、Ubuntu 或 Windows)。WorkSpace 的電腦名稱應是以下列其中一種格式：
>
> - Amazon Linux：A-*xxxxxxxxxxxxx*
> - Ubuntu：U-*xxxxxxxxxxxxx*
> - Windows：IP-C*xxxxxx* 或 WSAMZN-*xxxxxxx* 或 EC2AMAZ-*xxxxxxx*
>
> 對於 Windows WorkSpaces，電腦名稱格式是由套件類型決定，如果 WorkSpaces 是從公用套件或從以公用映像為基礎的自訂套件建立，則是由建立公用映像的時間決定。
> 自 2020 年 6 月 22 日起，從公用套件啟動的 Windows WorkSpaces 的電腦名稱使用 WSAMZN-*xxxxxxx* 格式，而不是 IP-C*xxxxxx* 格式。
> 對於以公用映像為基礎的自訂套件，如果公用映像是在 2020 年 6 月 22 日之前建立，則電腦名稱的格式為 EC2AMAZ-*xxxxxxx*。如果公用映像是在 2020 年 6 月 22 日當天或之後建立，則電腦名稱的格式為 WSAMZN-*xxxxxxx*。
> 若為自帶授權 (BYOL) 套件，電腦名稱預設會使用 DESKTOP-*xxxxxxx* 或 EC2AMAZ-*xxxxxxx* 格式。
> 如果您已為自訂或 BYOL 套件中的電腦名稱指定自訂格式，則自訂格式會覆寫這些預設值。若要指定自訂格式，請參閱 建立自訂 WorkSpaces 映像檔和套裝軟體。
> 重要—如果您透過 Windows 系統設定變更 WorkSpace 的電腦名稱，您將無法再存取 WorkSpace。

WorkSpaces 會使用目錄來儲存和管理 WorkSpaces 和使用者的資訊。您可以執行下列任何操作：

- 建立 Simple AD 目錄。
- 為 Microsoft Active Directory 建立 AWS Directory Service，也稱為 AWS Managed Microsoft AD。
- 使用 Active Directory 連接器連線到現有的 Microsoft Active Directory。
- 建立 AWS Managed Microsoft AD 目錄與內部部署網域之間的信任關係。

> **Note**
>
> - 共用目錄目前不支援搭配 Amazon WorkSpaces 使用。
> - 如果您針對多區域複寫設定 AWS Managed Microsoft AD 目錄，則只能註冊主要區域中的目錄以便與 Amazon WorkSpaces 搭配使用。嘗試在複寫的區域中註冊目錄以搭配 Amazon WorkSpaces 使用將會失敗。AWS Managed Microsoft AD 的多區域複寫不支援搭配複寫區域內的 Amazon WorkSpaces 使用。
> - 您可以免費使用 Simple AD 和 AD Connector，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 或 AD Connector 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。
>
> 若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 Simple AD 或 AD Connector 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

下列教學課程說明如何使用支援的目錄服務選項來啟動 WorkSpace。

教學課程

- 使用 AWS Managed Microsoft AD 啟動 WorkSpace
- 使用 Simple AD 啟動 WorkSpace
- 使用 AD Connector 啟動 WorkSpace
- 使用信任的網域啟動 WorkSpace

使用 AWS Managed Microsoft AD 啟動 WorkSpace

WorkSpaces 可讓您為使用者佈建虛擬、雲端式 Windows 和 Linux 桌面 (也稱為 WorkSpaces)。

WorkSpaces 會使用目錄來儲存和管理 WorkSpaces 和使用者的資訊。對於您的目錄，您可以從 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory (也稱為 AWS Managed Microsoft AD) 中選擇。此外，您可以在 AWS Managed Microsoft AD 目錄與內部部署網域之間建立信任關係。

在本教學課程中，我們會啟動使用 AWS Managed Microsoft AD 的 WorkSpace。如需使用其他選項的教學課程，請參閱 使用 WorkSpaces 啟動虛擬桌面。

任務

開始之前

- 並非每個區域都可以使用 WorkSpaces。確認支援的區域，然後為您的 WorkSpaces 選取一個區域。如需支援區域的詳細資訊，請參閱各個 AWS 區域的 WorkSpaces 定價。
- 當您啟動 WorkSpace 時，您必須選取 WorkSpace 套件。套件是作業系統、儲存、運算和軟體資源的組合。如需詳細資訊，請參閱 Amazon WorkSpaces 套件。
- 當您使用 AWS Directory Service 或啟動 WorkSpace 建立目錄時，您必須建立或選取以一個公用子網路和兩個私有子網路設定的虛擬私有雲端。如需詳細資訊，請參閱 設定虛 VPC WorkSpaces。

步驟 1：建立 AWS Managed Microsoft AD 目錄

首先，建立 AWS Managed Microsoft AD 目錄。AWS Directory Service 會建立兩個目錄伺服器，您 VPC 的每個私有子網路中各有一個目錄伺服器。請注意，目錄最初沒有任何使用者。當您啟動 WorkSpace 時，您會在下一個步驟中新增使用者。

> **Note**
>
> - 共用目錄目前不支援搭配 Amazon WorkSpaces 使用。
> - 如果已針對多區域複寫設定 AWS Managed Microsoft AD 目錄，則只能註冊主要區域中的目錄，以便搭配 Amazon WorkSpaces 使用。嘗試在複寫的區域中註冊目錄以搭配 Amazon WorkSpaces 使用將會失敗。AWS Managed Microsoft AD 的多區域複寫不支援搭配複寫區域內的 Amazon WorkSpaces 使用。

建立 AWS Managed Microsoft AD 目錄

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選擇設定目錄，建立 Microsoft AD。

4. 設定目錄，如下所示：

   a. 在組織名稱中，為您的目錄輸入唯一組織名稱 (例如，my-demo-directory)。此名稱的長度至少必須有 4 個字元，只能包含英數字元和連字號 (-)，而且以非連字號的字元開頭或結尾。

   b. 針對目錄 DNS，輸入目錄的完整名稱 (例如，workspaces.demo.com)。

   > **Important**
   >
   > 如果您需要在啟動 WorkSpaces 之後更新 DNS 伺服器，請遵循 更新 Amazon WorkSpaces 的 DNS 伺服器 中的程序，確保您的 WorkSpaces 能正確更新。

   c. 針對 NetBIOS 名稱，輸入目錄的簡短名稱 (例如，workspaces)。

   d. 針對管理員密碼和確認密碼，輸入目錄管理員帳戶的密碼。如需有關密碼需求的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立 AWS Managed Microsoft AD 目錄。

   e. (選用) 針對描述，輸入目錄的描述。

   f. 針對 VPC，選取您建立的 VPC。

   g. 針對子網路，選取兩個私用子網路 (具有 CIDR 區塊 `10.0.1.0/24` 和 `10.0.2.0/24`)。

   h. 選擇 Next Step (後續步驟)。

5. 選擇建立 Microsoft AD。

6. 選擇 Done (完成)。目錄的初始狀態為 `Creating`。目錄建立完成時，狀態為 `Active`。

步驟 2：建立 WorkSpace

現已建立 AWS Managed Microsoft AD 目錄，您就可以建立 WorkSpace。

若要建立 WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選擇啟動 WorkSpaces。
4. 在變更目錄頁面上，選取您所建立的目錄，然後選擇後續步驟。WorkSpaces 會註冊您的目錄。
5. 在識別使用者頁面上，將新使用者新增至您的目錄，如下所示：

   a. 完成使用者名稱、名字、姓氏和電子郵件。使用您有權存取的電子郵件地址。

   b. 選擇建立使用者。

c. 選擇 Next Step (後續步驟)。

6. 在選取套件頁面上，選取套件，然後選擇後續步驟。

> **Note**
>
> 檢閱每個套件的建議用途和規格，協助確保您選取最適合使用者的套件。如需每個使用案例的詳細資訊，請參閱 Amazon WorkSpaces 套件。如需套件規格、建議用途和定價的詳細資訊，請參閱 Amazon WorkSpaces 定價。

7. 在 WorkSpaces 組態頁面上，選擇執行模式，然後選擇後續步驟。

8. 在檢閱和啟動 WorkSpaces 頁面上，選擇 啟動 WorkSpaces。WorkSpace 的初始狀態為 `PENDING`。啟動完成時，狀態為 `AVAILABLE`，而邀請會傳送至您為使用者指定的電子郵件地址。

> **Note**
>
> 如果使用者已經存在於 Active Directory 中，則不會傳送邀請電子郵件。反而，確保手動向用戶傳送邀請電子郵件。如需詳細資訊，請參閱 傳送邀請電子郵件。

9. (選用) 如果區域支援 Amazon WorkDocs，您可以為目錄中的所有使用者啟用 Amazon WorkDocs。如需詳細資訊，請參閱 為 AWS Managed Microsoft AD 啟用 Amazon WorkDocs。如需 Amazon WorkDocs 的詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的 Amazon WorkDocs 磁碟機。

步驟 3：連線至 WorkSpace

收到邀請電子郵件後，您可以使用您選擇的用戶端來連線至 WorkSpace。登入後，用戶端會顯示 WorkSpace 桌面。

連線至 WorkSpace

1. 開啟邀請電子郵件中的連結。出現提示時，指定密碼並啟用使用者。請記住此密碼，因為您需有密碼才能登入 WorkSpace。

> **Note**
>
> 密碼區分大小寫，長度須介於 8 至 64 個字元 (含) 之間。密碼必須至少包含下列每個類別中的一個字元：小寫字母 (a-z)、大寫字母 (A-Z)、數字 (0-9) 和 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 如需有關每個用戶端需求的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端，然後執行下列其中一項操作：
   - 出現提示時，請下載其中一個用戶端應用程式或啟動 Web Access。
   - 如果系統未提示您而且您尚未安裝用戶端應用程式，請開啟 https://clients.amazonworkspaces.com/ 並下載其中一個用戶端應用程式或啟動 Web Access。

> **Note**
>
> 您無法使用 Web 瀏覽器 (Web Access) 來連線到 Amazon Linux WorkSpaces。

3. 啟動用戶端，輸入邀請電子郵件中的註冊碼，然後選擇註冊。
4. 當系統提示您登入時，請輸入使用者的登入認證，然後選擇登入。
5. (選用) 當系統提示您儲存憑證時，請選擇是。

後續步驟

您可以繼續自訂您剛建立的 WorkSpace。例如，您可以安裝軟體，然後從 WorkSpace 建立自訂套件。您也可以針對 WorkSpaces 和 WorkSpaces 目錄執行各種管理任務。如果您結束使用 WorkSpace，即可予以刪除。如需詳細資訊，請參閱下列文件。

- 建立自訂 WorkSpaces 映像檔和套裝軟體
- 管理您的 WorkSpaces
- 管理 WorkSpaces 的目錄
- 刪除 WorkSpace

如需有關使用 WorkSpaces 用戶端應用程式 (例如設定多個監視器或使用周邊裝置) 的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端和周邊裝置支援。

使用 Simple AD 啟動 WorkSpace

WorkSpaces 可讓您為使用者佈建虛擬、雲端式 Microsoft Windows 和 Linux 桌面 (也稱為 WorkSpaces)。

WorkSpaces 會使用目錄來儲存和管理 WorkSpaces 和使用者的資訊。對於您的目錄，您可以從 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory (也稱為 AWS Managed Microsoft AD) 中選擇。此外，您可以在 AWS Managed Microsoft AD 目錄與內部部署網域之間建立信任關係。

在本教學課程中，我們會啟動使用 Simple AD 的 WorkSpace。如需使用其他選項的教學課程，請參閱使用 WorkSpaces 啟動虛擬桌面。

任務

開始之前

- 並非每個區域都可以使用 Simple AD。確認支援的區域，然後為您的 Simple AD 目錄選取一個區域。如需有關 Simple AD 支援的區域資訊，請參閱 AWS Directory Service 的區域可用性。
- 並非每個區域都可以使用 WorkSpaces。確認支援的區域，然後為您的 WorkSpaces 選取一個區域。如需支援區域的詳細資訊，請參閱各個 AWS 區域的 WorkSpaces 定價。
- 當您啟動 WorkSpace 時，您必須選取 WorkSpace 套件。套件是作業系統、儲存、運算和軟體資源的組合。如需詳細資訊，請參閱 Amazon WorkSpaces 套件。
- 當您使用 AWS Directory Service 或啟動 WorkSpace 建立目錄時，您必須建立或選取以一個公用子網路和兩個私有子網路設定的虛擬私有雲端。如需詳細資訊，請參閱 設定虛 VPC WorkSpaces。

步驟 1：建立 Simple AD 目錄

建立 Simple AD 目錄。AWS Directory Service 會建立兩個目錄伺服器，每個 VPC 的私有子網路中各有一個目錄伺服器。請注意，目錄最初沒有任何使用者。當您建立 WorkSpace 時，您會在下一個步驟中新增使用者。

> **Note**
>
> 您可以免費使用 Simple AD，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 Simple AD 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

建立 Simple AD 目錄

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選擇設定目錄、Simple AD 和下一步。
4. 設定目錄，如下所示：
   a. 在組織名稱中，為您的目錄輸入唯一組織名稱 (例如，my-example-directory)。此名稱的長度至少必須有 4 個字元，只能包含英數字元和連字號 (-)，而且以非連字號的字元開頭或結尾。
   b. 針對目錄 DNS 名稱，輸入目錄的完整名稱 (例如，example.com)。

      > **Important**
      >
      > 如果您需要在啟動 WorkSpaces 之後更新 DNS 伺服器，請遵循 更新 Amazon WorkSpaces 的 DNS 伺服器 中的程序，確保您的 WorkSpaces 能正確更新。

   c. 針對 NetBIOS 名稱，輸入目錄的簡短名稱 (例如，example)。
   d. 針對管理員密碼和確認密碼，輸入目錄管理員帳戶的密碼。如需密碼需求的相關資訊，請參閱《AWS Directory Service 管理指南》中的如何建立 Microsoft AD 目錄。
   e. (選用) 針對描述，輸入目錄的描述。
   f. 針對目錄大小，選擇小型。
   g. 對於 VPC (VPC)，選取您建立的 VPC。
   h. 針對子網路，選取兩個私用子網路 (具有 CIDR 區塊 `10.0.1.0/24` 和 `10.0.2.0/24`)。
   i. 選擇下一步。
5. 選擇建立目錄。

6. 目錄的初始狀態為 Requested，然後是 Creating。目錄建立完成時 (這可能需要幾分鐘)，狀態為 Active。

建立目錄期間發生的事

WorkSpaces 會代表您完成下列任務：

- 建立 IAM 角色，以允許 WorkSpaces 服務建立彈性網路介面並列出您的 WorkSpaces 目錄。此角色具有名稱 workspaces_DefaultRole。
- 在用於儲存使用者與 WorkSpace 資訊的 VPC 中設定 Simple AD 目錄。此目錄有一個具使用者名稱 Administrator 與指定密碼的管理員帳戶。
- 建立兩個安全群組，一個用於目錄控制器，另一個用於目錄中的 WorkSpaces。

步驟 2：建立 WorkSpace

您現在可以隨時啟動 WorkSpace。

若要為使用者建立 WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選擇啟動 WorkSpaces。
4. 在選取目錄頁面上，執行下列操作：
   a. 針對目錄，選擇您建立的目錄。
   b. 針對啟用自助服務許可，選擇是或否，然後輸入描述。
   c. 針對啟用 Amazon WorkDocs，選擇是。

      > **Note**
      >
      > 只有在 Amazon WorkDocs 適用於所選的區域時，才可使用此選項。

   d. 選擇 Next Step (後續步驟)。WorkSpaces 會註冊您的 Simple AD 目錄。
5. 在識別使用者頁面上，將新使用者新增至您的目錄，如下所示：
   a. 完成使用者名稱、名字、姓氏和電子郵件。使用您有權存取的電子郵件地址。
   b. 選擇建立使用者。

c. 選擇 Next Step (後續步驟)。

6. 在選取套件頁面上，選取套件，然後選擇後續步驟。

> **Note**
>
> 檢閱每個套件的建議用途和規格，協助確保您選取最適合使用者的套件。如需每個使用案例的詳細資訊，請參閱 Amazon WorkSpaces 套件。如需套件規格、建議用途和定價的詳細資訊，請參閱 Amazon WorkSpaces 定價。

7. 在 WorkSpaces 組態頁面上，選擇執行模式，然後選擇後續步驟。

8. 在檢閱和啟動 WorkSpaces 頁面上，選擇 啟動 WorkSpaces。WorkSpace 的初始狀態為 `PENDING`。啟動完成時 (最多可能需要 20 分鐘)，狀態為 `AVAILABLE`，而邀請會傳送至您為使用者指定的電子郵件地址。

> **Note**
>
> 如果使用者已經存在於 Active Directory 中，則不會傳送邀請電子郵件。反而，確保手動向用戶傳送邀請電子郵件。如需詳細資訊，請參閱 傳送邀請電子郵件。

步驟 3：連線至 WorkSpace

收到邀請電子郵件後，您可以使用您選擇的用戶端來連線至 WorkSpace。登入後，用戶端會顯示 WorkSpace 桌面。

連線至 WorkSpace

1. 開啟邀請電子郵件中的連結。出現提示時，輸入密碼並啟用使用者。請記住此密碼，因為您需有密碼才能登入 WorkSpace。

> **Note**
>
> 密碼區分大小寫，長度須介於 8 至 64 個字元 (含) 之間。密碼必須至少包含下列每個類別中的一個字元：小寫字母 (a-z)、大寫字母 (A-Z)、數字 (0-9) 和 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 如需有關每個用戶端需求的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端，然後執行下列其中一項操作：

- 出現提示時，請下載其中一個用戶端應用程式或啟動 Web Access。
- 如果系統未提示您而且您尚未安裝用戶端應用程式，請開啟 https://clients.amazonworkspaces.com/ 並下載其中一個用戶端應用程式或啟動 Web Access。

> **Note**
>
> 您無法使用 Web 瀏覽器 (Web Access) 來連線到 Amazon Linux WorkSpaces。

3. 啟動用戶端，輸入邀請電子郵件中的註冊碼，然後選擇註冊。
4. 當系統提示您登入時，請輸入使用者的登入認證，然後選擇登入。
5. (選用) 當系統提示您儲存憑證時，請選擇是。

後續步驟

您可以繼續自訂您剛建立的 WorkSpace。例如，您可以安裝軟體，然後從 WorkSpace 建立自訂套件。您也可以針對 WorkSpaces 和 WorkSpaces 目錄執行各種管理任務。如果您結束使用 WorkSpace，即可予以刪除。如需詳細資訊，請參閱下列文件。

- 建立自訂 WorkSpaces 映像檔和套裝軟體
- 管理您的 WorkSpaces
- 管理 WorkSpaces 的目錄
- 刪除 WorkSpace

如需有關使用 WorkSpaces 用戶端應用程式 (例如設定多個監視器或使用周邊裝置) 的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端和周邊裝置支援。

使用 AD Connector 啟動 WorkSpace

WorkSpaces 可讓您為使用者佈建虛擬、雲端式 Microsoft Windows 和 Linux 桌面 (也稱為 WorkSpaces)。

WorkSpaces 會使用目錄來儲存和管理 WorkSpaces 和使用者的資訊。對於您的目錄，您可以從 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory (也稱為 AWS Managed Microsoft AD) 中選擇。此外，您可以在 AWS Managed Microsoft AD 目錄與內部部署網域之間建立信任關係。

在本教學課程中，我們會啟動使用 AD Connector 的 WorkSpace。如需使用其他選項的教學課程，請參閱 使用 WorkSpaces 啟動虛擬桌面。

任務

開始之前

- 並非每個區域都可以使用 WorkSpaces。確認支援的區域，然後為您的 WorkSpaces 選取一個區域。如需支援區域的詳細資訊，請參閱各個 AWS 區域的 WorkSpaces 定價。
- 當您啟動 WorkSpace 時，您必須選取一個 WorkSpace 套件。套件是作業系統、儲存、運算和軟體資源的組合。如需詳細資訊，請參閱 Amazon WorkSpaces 套件。
- 建立至少有兩個私有子網路的虛擬私有雲端。如需詳細資訊，請參閱 設定虛 VPC WorkSpaces。VPC 必須透過虛擬私有網路 (VPN) 連線或 AWS Direct Connect 連線到您的現場部署網路。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的 AD Connector 先決條件。
- 提供從 WorkSpace 對網際網路的存取。如需詳細資訊，請參閱 提供您的網際網路存取 WorkSpace。

步驟 1：建立 AD Connector

> **Note**
>
> 您可以免費使用 AD Connector，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 AD Connector 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 AD Connector 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

建立 AD Connector

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選擇設定目錄、建立 AD Connector。
4. 在組織名稱中，為您的目錄輸入唯一組織名稱 (例如，my-example-directory)。此名稱的長度至少必須有 4 個字元，只能包含英數字元和連字號 (-)，而且以非連字號的字元開頭或結尾。
5. 針對連線的目錄 DNS，輸入內部部署目錄的完整名稱 (例如，example.com)。
6. 針對連線的目錄 NetBIOS 名稱，輸入內部部署目錄的簡短名稱 (例如，example)。
7. 針對連接器帳戶使用者名稱，輸入內部部署目錄中使用者的使用者名稱。使用者必須具有讀取使用者和群組、建立電腦物件以及將電腦加入網域的許可。
8. 針對連接器帳戶密碼和確認密碼，輸入內部部署使用者的密碼。
9. 針對 DNS 位址，輸入內部部署目錄中至少一個 DNS 伺服器的 IP 位址。

   > **Important**
   >
   > 如果您需要在啟動 WorkSpaces 之後更新 DNS 伺服器 IP 位址，請遵循 更新 Amazon WorkSpaces 的 DNS 伺服器 中的程序，確保您的 WorkSpaces 能正確更新。

10. (選用) 針對描述，輸入目錄的描述。
11. 將大小保持為小。
12. 針對 VPC，選取您的 VPC。
13. 針對子網路，選取您的子網路。您指定的 DNS 伺服器必須可從每個子網路存取。
14. 選擇 Next Step (後續步驟)。
15. 選擇建立 AD Connector。連線您的目錄需要幾分鐘的時間。目錄的初始狀態為 `Requested`，然後是 `Creating`。目錄建立完成時，狀態為 `Active`。

步驟 2：建立 WorkSpace

現在，您已準備好為內部部署目錄中的一或多個使用者啟動 WorkSpaces。

為現有使用者啟動 WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。

3. 選擇啟動 WorkSpaces。
4. 針對目錄，選擇您建立的目錄。
5. (選用) 如果這是您第一次在此目錄中啟動 WorkSpace，且區域中支援 Amazon WorkDocs，您可以為目錄中的所有使用者啟用或停用 Amazon WorkDocs。如需 Amazon WorkDocs 的詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的 Amazon WorkDocs 磁碟機。
6. 選擇 Next (下一步)。WorkSpaces 會註冊您的 AD Connector。
7. 從內部部署目錄中選取一或多個現有使用者。請勿透過 WorkSpaces 主控台將新使用者新增至內部部署目錄。

   若要尋找要選取的使用者，您可以輸入全部或部分使用者的名稱，然後選擇搜尋或選擇顯示所有使用者。請注意，您無法選取沒有電子郵件地址的使用者。

   選取使用者之後，請選擇新增所選，然後選擇下一步。
8. 在選取套件下，選擇要用於 WorkSpaces 的預設 WorkSpace 套件。在指派 WorkSpace 套件下，您可以視需要為個別 WorkSpace 選擇不同的套件。完成時，選擇後續步驟。

   > **Note**
   >
   > 檢閱每個套件的建議用途和規格，協助確保您選取最適合使用者的套件。如需每個使用案例的詳細資訊，請參閱 Amazon WorkSpaces 套件。如需套件規格、建議用途和定價的詳細資訊，請參閱 Amazon WorkSpaces 定價。
9. 為您的 WorkSpaces 選擇執行模式，然後選擇後續步驟。如需詳細資訊，請參閱 管理 WorkSpace 執行模式。
10. 選擇啟動 WorkSpaces。WorkSpace 的初始狀態為 `PENDING`。啟動完成時，狀態為 `AVAILABLE`。
11. 傳送邀請至每位使用者的電子郵件地址。(如果您使用 AD Connector，則不會自動傳送這些邀請。) 如需詳細資訊，請參閱 傳送邀請電子郵件。

步驟 3：連線至 WorkSpace

您可以使用您選擇的用戶端連線至 WorkSpace。登入後，用戶端會顯示 WorkSpace 桌面。

連線至 WorkSpace

1. 開啟邀請電子郵件中的連結。

2. 如需有關每個用戶端需求的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端，然後執行下列其中一項操作：

   - 出現提示時，請下載其中一個用戶端應用程式或啟動 Web Access。
   - 如果系統未提示您而且您尚未安裝用戶端應用程式，請開啟 https://clients.amazonworkspaces.com/ 並下載其中一個用戶端應用程式或啟動 Web Access。

   > **Note**
   >
   > 您無法使用 Web 瀏覽器 (Web Access) 來連線到 Amazon Linux WorkSpaces。

3. 啟動用戶端，輸入邀請電子郵件中的註冊碼，然後選擇註冊。
4. 當系統提示您登入時，請輸入使用者的登入認證，然後選擇登入。
5. (選用) 當系統提示您儲存憑證時，請選擇是。

> **Note**
>
> 因為您使用 AD Connector，您的使用者將無法重設自己的密碼。(WorkSpaces 用戶端應用程式登入畫面上的忘記密碼？選項將無法使用。) 如需重設使用者密碼的詳細資訊，請參閱 設定 WorkSpaces 的 Active Directory 管理工具。

後續步驟

您可以繼續自訂您剛建立的 WorkSpace。例如，您可以安裝軟體，然後從 WorkSpace 建立自訂套件。您也可以針對 WorkSpaces 和 WorkSpaces 目錄執行各種管理任務。如果您結束使用 WorkSpace，即可予以刪除。如需詳細資訊，請參閱下列文件。

- 建立自訂 WorkSpaces 映像檔和套裝軟體
- 管理您的 WorkSpaces
- 管理 WorkSpaces 的目錄
- 刪除 WorkSpace

如需有關使用 WorkSpaces 用戶端應用程式 (例如設定多個監視器或使用周邊裝置) 的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端和周邊裝置支援。

使用信任的網域啟動 WorkSpace

WorkSpaces 可讓您為您的使用者佈建虛擬、雲端式 Microsoft Windows、Amazon Linux 或 Ubuntu Linux 桌面，也稱為 WorkSpaces。

WorkSpaces 會使用目錄來儲存和管理 WorkSpaces 和使用者的資訊。對於您的目錄，您可以從 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory (也稱為 AWS Managed Microsoft AD) 中選擇。此外，您可以在 AWS Managed Microsoft AD 目錄與內部部署網域之間建立信任關係。

在本教學課程中，我們會啟動使用信任關係的 WorkSpace。如需使用其他選項的教學課程，請參閱 使用 WorkSpaces 啟動虛擬桌面。

任務

開始之前

- 當 WorkSpaces 設定了與您的內部部署目錄的信任關係時，在個別信任的網域中使用 AWS 帳戶啟動 WorkSpaces 會與 AWS Managed Microsoft AD 搭配運作。但是，使用 Simple AD 或 AD Connector 的 WorkSpaces 無法為來自信任網域的使用者啟動 WorkSpaces。
- 並非每個區域都可以使用 WorkSpaces。確認支援的區域，然後為您的 WorkSpaces 選取一個區域。如需支援區域的詳細資訊，請參閱各個 AWS 區域的 WorkSpaces 定價。
- 當您啟動 WorkSpace 時，您必須選取 WorkSpace 套件。套件是儲存、運算和軟體資源的組合。如需詳細資訊，請參閱 Amazon WorkSpaces 套件。
- 當您使用 AWS Directory Service 或啟動 WorkSpace 建立目錄時，您必須建立或選取以一個公用子網路和兩個私有子網路設定的虛擬私有雲端。如需詳細資訊，請參閱 設定虛 VPC WorkSpaces。

步驟 1：建立信任關係

設定信任關係

1. 在您的虛擬私有雲端 (VPC) 中設定 AWS Managed Microsoft AD。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立 AWS Managed Microsoft AD 目錄。

   > **Note**
   >
   > - 共用目錄目前不支援搭配 Amazon WorkSpaces 使用。
   > - 如果已針對多區域複寫設定 AWS Managed Microsoft AD 目錄，則只能註冊主要區域中的目錄，以便搭配 Amazon WorkSpaces 使用。嘗試在複寫的區域中註冊目錄以搭配 Amazon WorkSpaces 使用將會失敗。AWS Managed Microsoft AD 的多區域複寫不支援搭配複寫區域內的 Amazon WorkSpaces 使用。

2. 建立 AWS Managed Microsoft AD 與內部部署網域之間的信任關係。確定信任已設定為雙向信任。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的教學課程：在 AWS Managed Microsoft AD 與內部部署網域之間建立信任關係。

單向或雙向信任可用於管理和驗證 WorkSpaces，以便將 WorkSpaces 佈建給內部部署使用者和群組。如需詳細資訊，請參閱使用與 AWS Directory Service 的單向信任資源網域部署 Amazon WorkSpaces。

> **Note**
>
> Ubuntu WorkSpaces 使用系統安全服務常駐程式（SSSD）進行 Active Directory 整合，而 SSSD 不支援樹系信任。請改為設定外部信任。建議對 Amazon Linux 和 Ubuntu WorkSpace 使用雙向信任。

步驟 2：建立 WorkSpace

在 AWS Managed Microsoft AD 與內部部署 Microsoft Active Directory 網域之間建立信任關係之後，您可以為內部部署網域中的使用者佈建 WorkSpaces。

請注意，您必須先確定 GPO 設定已跨網域複寫，才能將其套用至 WorkSpaces。

為信任的內部部署網域中的使用者啟動工作區

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選擇啟動 WorkSpaces。
4. 在選取目錄頁面上，選擇您剛註冊的目錄，然後選擇後續步驟。
5. 在識別使用者頁面上，執行下列操作：
   a. 針對從樹系選取信任，選取您建立的信任關係。
   b. 從內部部署網域選取使用者，然後選擇新增所選項目。
   c. 選擇 Next Step (後續步驟)。
6. 選取要用於 WorkSpaces 的套件，然後選擇後續步驟。

> **Note**
>
> 檢閱每個套件的建議用途和規格，協助確保您選取最適合使用者的套件。如需每個使用案例的詳細資訊，請參閱 Amazon WorkSpaces 套件。如需套件規格、建議用途和定價的詳細資訊，請參閱 Amazon WorkSpaces 定價。

7. 選擇執行模式，選擇加密設定，以及設定任何標籤。完成時，選擇後續步驟下一步。
8. 選擇啟動 WorkSpaces。請注意，最多需要 20 分鐘讓 WorkSpaces 變得可用，若已啟用加密，最多則需要 40 分鐘才可使用。WorkSpace 的初始狀態為 PENDING。啟動完成時，狀態為 AVAILABLE。
9. 傳送邀請至每位使用者的電子郵件地址。(如果您使用信任關係，則不會自動傳送這些邀請。) 如需詳細資訊，請參閱 傳送邀請電子郵件。

步驟 3：連線至 WorkSpace

收到邀請電子郵件之後，您便可以連線至 WorkSpace。使用者可以輸入其使用者名稱作為 username、corp\username 或 corp.example.com\username)。

連線至 WorkSpace

1. 開啟邀請電子郵件中的連結。出現提示時，輸入密碼並啟用使用者。請記住此密碼，因為您需有密碼才能登入 WorkSpace。

> **Note**
>
> 密碼區分大小寫，長度須介於 8 至 64 個字元 (含) 之間。密碼必須至少包含下列每個類別中的一個字元：小寫字母 (a-z)、大寫字母 (A-Z)、數字 (0-9) 和 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 如需有關每個用戶端需求的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端，然後執行下列其中一項操作：

   - 出現提示時，請下載其中一個用戶端應用程式或啟動 Web Access。
   - 如果系統未提示您而且您尚未安裝用戶端應用程式，請開啟 https://clients.amazonworkspaces.com/ 並下載其中一個用戶端應用程式或啟動 Web Access。

   > **Note**
   >
   > 您無法使用 Web 瀏覽器 (Web Access) 來連線到 Amazon Linux WorkSpaces。

3. 啟動用戶端，輸入邀請電子郵件中的註冊碼，然後選擇註冊。
4. 當系統提示您登入時，請輸入使用者的登入認證，然後選擇登入。
5. (選用) 當系統提示您儲存憑證時，請選擇是。

後續步驟

您可以繼續自訂您剛建立的 WorkSpace。例如，您可以安裝軟體，然後從 WorkSpace 建立自訂套件。您也可以針對 WorkSpaces 和 WorkSpaces 目錄執行各種管理任務。如果您結束使用 WorkSpace，即可予以刪除。如需詳細資訊，請參閱下列文件。

- 建立自訂 WorkSpaces 映像檔和套裝軟體
- 管理您的 WorkSpaces
- 管理 WorkSpaces 的目錄
- 刪除 WorkSpace

如需有關使用 WorkSpaces 用戶端應用程式 (例如設定多個監視器或使用周邊裝置) 的詳細資訊，請參閱《Amazon WorkSpaces 使用者指南》中的 WorkSpaces 用戶端和周邊裝置支援。

管理 WorkSpace 使用者

每個 WorkSpace 都會指派給單一使用者，且不能由多個使用者共用。依預設，允許每個使用者在每個目錄中只有一個 WorkSpace。

目錄

管理 WorkSpaces 使用者

身為 WorkSpaces 的管理員，您可以執行下列任務來管理 WorkSpaces 使用者。

編輯使用者資訊

您可以使用 WorkSpaces 主控台來編輯 WorkSpace 的使用者資訊。

> **Note**
>
> 只有當您使用 AWS Managed Microsoft AD 或 Simple AD 時，才能使用這項功能。如果您透過 AD Connector 或信任關係來使用 Microsoft Active Directory，您可使用 Active Directory 模組來管理使用者和群組。

若要編輯使用者資訊

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取使用者，然後依序選擇動作、編輯使用者。
4. 視需要更新名字、姓氏和電子郵件。
5. 選擇更新。

新增或刪除使用者

您只能在啟動 WorkSpace 的過程中從 Amazon WorkSpaces 主控台建立使用者，而且無法透過 Amazon WorkSpaces 主控台刪除使用者。大多數使用者管理工作 (包括管理使用者群組) 都必須透過您的目錄執行。

若要新增或刪除使用者和群組

若要新增、刪除或以其他方式管理使用者和群組，您必須透過目錄執行此操作。您將使用目錄管理工具 (例如 Active Directory 管理工具) 為 WorkSpaces 目錄執行大部分的管理任務。如需詳細資訊，請參閱設定 WorkSpaces 的 Active Directory 管理工具。

> **Important**
>
> 您必須先刪除指派給使用者的 WorkSpace，才能移除該使用者。如需詳細資訊，請參閱 刪除 WorkSpace。

您用於管理使用者和群組的程序取決於您所使用的目錄類型。

- 如果您使用 AWS Managed Microsoft AD，請參閱《AWS Directory Service 管理指南》中的在 AWS Managed Microsoft AD 中管理使用者和群組。
- 如果您使用 Simple AD，請參閱《AWS Directory Service 管理指南》中的在 Simple AD 中管理使用者和群組。
- 如果您透過 AD Connector 或信任關係來使用 Microsoft Active Directory，您可使用 Active Directory 模組來管理使用者和群組。

傳送邀請電子郵件

如有需要，您可以手動傳送邀請電子郵件給使用者。

> **Note**
>
> 如果您使用 AD Connector 或受信任的網域，邀請電子郵件就不會自動傳送給使用者，因此您必須手動傳送。如果使用者已經存在於 Active Directory 中，也不會自動傳送邀請電子郵件。

若要重新傳送邀請電子郵件

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 在 WorkSpaces 頁面上，使用搜尋方塊來搜尋您要傳送邀請的使用者，然後從搜尋結果中選取對應的 WorkSpace。您一次只能選取一個 WorkSpace。
4. 選擇動作、邀請使用者。
5. 在邀請使用者存取 WorkSpace 頁面上，選擇傳送邀請。

為使用者建立多個 WorkSpaces

預設情況下，只能在每個目錄中為每個使用者建立一個 WorkSpace。但是，如有需要，您可以根據您的目錄設定，為一個使用者建立多個 WorkSpace。

- 如果您的 WorkSpaces 只有一個目錄，請為該使用者建立多個使用者名稱。例如，名為 Mary Major 的使用者可以將 mmajor1、mmajor2 等作為使用者名稱。每個使用者名稱都與相同目錄中的不同 WorkSpace 相關聯，但是只要 WorkSpaces 都在相同 AWS 區域的相同目錄中建立，WorkSpaces 就會有相同的註冊碼。
- 如果您的 WorkSpaces 有多個目錄，請在不同的目錄中為使用者建立 WorkSpaces。您可以在目錄中使用相同的使用者名稱，也可以在目錄中使用不同的使用者名稱。WorkSpaces 將有不同的註冊碼。

> **Tip**
>
> 所以為了讓您可輕鬆找到您為使用者建立的所有 WorkSpaces，請對每個 WorkSpace 使用相同的基礎使用者名稱。
>
> 例如，如果您有名為 Mary Major 的使用者具有 Active Directory 使用者名稱 mmajor，請使用 mmajor、mmajor1、mmajor2、mmajor3 或其他變體 (如 mmajor_windows 或 mmajor_linux) 等使用者名稱為她建立 WorkSpaces。只要所有 WorkSpaces 具有相同的開頭基礎使用者名稱 (mmajor)，您就可以在 WorkSpaces 主控台中依照使用者名稱排序，以將該使用者的所有 WorkSpaces 分組在一起。

Important

- 只要兩個 WorkSpace 位於不同的目錄中，使用者就可以同時有 PCoIP 和 WSP WorkSpaces。相同的使用者不能在相同的目錄中有 PCoIP 和 WSP WorkSpace。
- 如果您要設定多個 WorkSpaces 以搭配跨區域重新導向使用，則必須在不同 AWS 區域的不同目錄中設定 WorkSpaces，而且您必須在每個目錄中使用相同的使用者名稱。如需跨區域重新導向的詳細資訊，請參閱 Amazon 的跨區域重新導向 WorkSpaces。

為了在 WorkSpaces 之間切換，使用者會使用與特定 Workspace 相關聯的使用者名稱和註冊碼進行登入。如果使用者使用適用於 Windows、macOS 或 Linux 的 3.0+ 版 WorkSpaces 用戶端應用程式，則使用者可以前往用戶端應用程式中的設定、管理登入資訊，將不同的名稱指派給 WorkSpaces。

自訂使用者登入他們的方式 WorkSpaces

使用統一資源識別碼 (URI) WorkSpaces 來自訂使用者的存取權，以提供與組織中現有工作流程整合的簡化登入體驗。例如，您可以自動產生登入 URI，以使用其註冊碼來註冊您的 WorkSpaces 使用者。因此：

- 使用者可以略過手動註冊程序。
- 他們的用戶名會自動輸入到他們的 WorkSpaces 客戶登錄頁面上。
- 如果您的組織中使用了多重要素驗證 (MFA)，其使用者名稱和 MFA 驗證碼會在其用戶端登入頁面上自動輸入。

URI 存取可搭配區域型註冊碼 (例如 `WSpdx+ABC12D`) 和完整網域名稱 (FQDN) 型註冊碼 (例如 `desktop.example.com`) 運作。如需建立和使用 FQDN 型註冊碼的詳細資訊，請參閱 Amazon 的跨區域重新導向 WorkSpaces。

您可以在下列支援的裝置上 WorkSpaces 為用戶端應用程式設定 URI 存取權：

- Windows 電腦
- macOS 電腦
- UBUNTU 系統電腦
- iPad
- Android 裝置

要使用 URI 來訪問他們的 WorkSpaces，用戶必須首先通過打開 https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

URI 訪問支持在火狐和鉻瀏覽器上的視窗和 macOS 的計算機上，在火狐瀏覽器上的 Ubuntu Linux 18.04，20.04 和 22.04 計算機，並在互聯網瀏覽器和 Microsoft 邊緣瀏覽器在 Windows 計算機上。如需有關用 WorkSpaces 戶端的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的用WorkSpaces 戶端。

> **Note**
>
> 在 Android 裝置上，URI 存取僅適用於 Firefox 瀏覽器，而不適用於 Google Chrome 瀏覽器。

若要設定的 URI 存取權 WorkSpaces，請使用下表所述的任何 URI 格式。

> **Note**
>
> 如果 URI 的資料元件包含下列任何保留字元，建議您在資料元件中使用百分比編碼，以避免模棱兩可：
> `@ : / ? & =`
> 例如，如果您的使用者名稱包含任何這些字元，您應該對 URI 中的這些使用者名稱進行百分比編碼。如需詳細資訊，請參閱統一資源識別符 (URI)：通用語法。

支援的語法	描述
workspaces://	開啟用戶 WorkSpaces 端應用程式。(注意：Linux 用戶端應用程式目前不支援單獨使用 workspaces://。)
workspaces://@registrationcode	使用其 WorkSpaces 註冊碼註冊使用者。也會顯示用戶端登入頁面。
workspaces://username@registrationcode	使用其 WorkSpaces 註冊碼註冊使用者。也會在用戶端登入頁面的使用者名稱欄位中自動輸入使用者名稱。
workspaces://username@registrationcode?MFACode=mfa	使用其 WorkSpaces 註冊碼註冊使用者。也會在使用者名稱欄位中自動輸入使用者名稱，並在用戶端登入頁面的 MFA 代碼欄位中輸入多重要素驗證 (MFA) 驗證碼。

支援的語法	描述
workspaces://@registrationcode?MFACode=mfa	使用其 WorkSpaces 註冊碼註冊使用者。也會在用戶端登入頁面的 MFA 代碼欄位中自動輸入多重要素驗證 (MFA) 驗證碼。

> **Note**
>
> 如果使用者在已 WorkSpace 從 Windows 用戶端連線至 URI 連結時開啟 URI 連結，則會開啟新 WorkSpaces 工作階段，而其原始工作 WorkSpaces 階段仍保持開啟狀態。如果使用者在 WorkSpace 從 macOS、iPad 或 Android 用戶端連線至 URI 連結時開啟 URI 連結，則不會開啟任何新工作階段；只有其原始工 WorkSpaces 作階段會保持開啟狀態。

為您的使用者啟用自助式 WorkSpace管理功能

在中 WorkSpaces，您可以為使用者啟用自助式 WorkSpace 管理功能，讓他們能夠更好地控制自己的體驗。它還可以減少您的 IT 支持人員的工作量 WorkSpaces。當您啟用自助功能時，使用者可以直接從其用 WorkSpaces 戶端執行下列一或多項工作：

- 在他們的客戶端上快取其憑證。這使他們可以重新連接到他們， WorkSpace 而無需重新輸入其憑據。
- 重新啟動（重啟）他們的 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.

支援的用戶端

- Android，在 Android 或與 Android 系統相容的 Chrome 作業系統上執行
- Linux
- macOS
- Windows

為使用者啟用自助式管理功能

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選擇您要啟用自助式管理功能的目錄。
4. 向下捲動至自助服務權限，然後選擇編輯。視需要啟用或停用下列選項，以決定使用者可從其用戶端執行的 WorkSpace 管理工作：

   - 記住我—使用者可以選取登入畫面上的記住我或讓我保持登入狀態核取方塊，選擇是否要在用戶端上快取其憑證。憑證只會在 RAM 中快取。當使用者選擇快取其身份證明時，他們可以重新連線至他們的身份證明， WorkSpaces 而無需重新輸入 若要控制使用者可快取其憑證的時間長度，請參閱 設定 Kerberos 票證的生命週期上限。
   - WorkSpace 從用戶端重新啟動 — 使用者可以重新啟動 (重新開機) 其 WorkSpace 重新啟動會中斷使用者與他們的連線 WorkSpace、將其關閉，然後重新啟動。使用者資料、作業系統和系統設定均不受影響。
   - 增加磁碟區大小 — 使用者可以將其根磁碟區和使用者磁碟區擴充 WorkSpace 到指定的大小，而無需聯絡 IT 支援人員。使用者可以將根磁碟區的大小 (對於 Windows 而言，C: 磁碟機；對於 Linux，/) 和使用者磁碟區的大小 (對於視窗而言，D: 磁碟機；對於 Linux，/home) 最大可增加 100 GB。 WorkSpace 根磁碟區和使用者磁碟區位於無法變更的設定群組中。可用的群組為 [[根磁碟區(GB)，使用者磁碟區(GB)]：[80，10]、[80，50]、[80，100]、[175 至 2000，100 至 2000]。如需詳細資訊，請參閱 修改一個 WorkSpace。

     對於新創建的 WorkSpace，用戶必須等待 6 小時才能增加這些驅動器的大小。此後，他們每 6 小時只能這樣做一次。雖然磁碟區大小增加正在進行中，使用者可以在其上執行大多數工作 WorkSpace。他們無法執行的工作包括：變更其 WorkSpace 運 WorkSpace 算類型、切換執行模式、重新啟動或重新建置。 WorkSpace WorkSpace程序完成時， WorkSpace 必須重新開機，變更才會生效。此程序最多需要 1 小時的時間。

     > **Note**
     >
     > 如果使用者增加他們的磁碟區大小 WorkSpace，這會增加他們的計費率 WorkSpace。

   - 變更運算類型 — 使用者可以在運算類型 (套裝軟體) WorkSpace 之間切換。對於新建立的使用者必須等待 6 小時 WorkSpace，才能切換至不同的套裝軟體。此後，他們只能在 6 小時內切換到較大的套件一次，或在 30 天內切換到較小的套件一次。當 WorkSpace 運算類型變更進行中時，使用者會與其中斷連線 WorkSpace，而且他們無法使用或變更 WorkSpace. 會在 WorkSpace 計算類型變更程序期間自動重新啟動。此程序最多需要 1 小時的時間。

> **Note**
>
> 如果使用者變更其 WorkSpace 運算類型，這會變更他們的計費費率 WorkSpace。

- 切換運行模式 — 用戶可以在AlwaysOn和AutoStop運行模式 WorkSpace 之間切換。如需詳細資訊，請參閱 管理 WorkSpace 執行模式。

> **Note**
>
> 如果使用者切換他們的執行模式 WorkSpace，這會變更他們的計費費率 WorkSpace。

- WorkSpace 從用戶端重建 — 使用者可以 WorkSpace 將 a 的作業系統重建為其原始狀態。重建 WorkSpace 時，會從最新備份重新建立使用者磁碟區 (D: 磁碟機)。由於備份會每 12 小時完成一次，因此使用者的資料最多可能存在 12 小時。對於新創建的 WorkSpace，用戶必須等待 12 小時才能重建他們的 WorkSpace。當 WorkSpace重建正在進行時，使用者會與其中斷連線 WorkSpace，而且他們無法使用或變更它們的 WorkSpace. 此程序最多需要 1 小時的時間。
- 診斷防護記錄檔上傳 — 使用者可以將用 WorkSpaces 戶端記錄檔直接上傳 WorkSpaces 至以疑難排解問題，而不會中斷用 WorkSpaces 戶端的使用。如果您為使用者啟用診斷記錄上傳，或讓您的使用者自行啟用，記錄檔會 WorkSpaces 自動傳送到。您可以在 WorkSpaces 串流工作階段之前或期間啟用診斷記錄上傳。

5. 選擇 Save (儲存)。

為使用者啟用 Amazon Connect 音訊最佳化

在 WorkSpaces 管理主控台中，您可以為 WorkSpaces 機群啟用 Amazon Connect 聯絡控制面板 (CCP) 音訊最佳化，以增強安全性並啟用原生品質的音訊。啟用 CCP 音訊最佳化後，用戶端端點會處理 CCP 音訊，而 WorkSpaces 使用者即可從其 WorkSpaces 與 CCP 互動。

Amazon Connect 聯絡控制面板 (CCP) 音訊最佳化適用於：

- WorkSpaces Windows 用戶端。
- Amazon Linux 與 Windows WorkSpaces。
- 使用 PCoIP 或 WSP 的 WorkSpaces。

需求

- 您必須使用 Amazon Connect 進行設定。
- 您必須建立沒有通話發訊媒體的 CCP，以使用 Amazon Connect Stream API 建置自訂 CCP。如此，媒體就會在本機桌面上以標準 CCP 處理，而發訊和通話控制則會在遠端連線上以無媒體的 CCP 處理。如需有關 Amazon Connect Stream API 的詳細資訊，請參閱 GitHub 儲存庫 (網址為 https://github.com/aws/amazon-connect-streams)。您建置的自訂 CCP 是您的 Amazon Connect 客服人員將在其 WorkSpaces 中使用的 CCP。
- 您必須在 Amazon Connect 支援的 WorkSpaces 用戶端端點上安裝網頁瀏覽器。如需支援的瀏覽器清單，請參閱 Amazon Connect 支援的瀏覽器。

> **Note**
>
> 如果使用者使用不受支援的瀏覽器，當他們嘗試登入 CCP 時，系統會要求他們下載支援的瀏覽器。

啟用 Amazon Connect 音訊最佳化

若要為使用者啟用 Amazon Connect 音訊最佳化：

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選取您的目錄，然後依序選擇動作、更新詳細資訊。
4. 展開 Amazon Connect 音訊最佳化。

> **Note**
>
> 使用 Amazon Connect 進行設定之前，請選擇更新以儲存先前在管理主控台中所做的任何未儲存變更。

5. 選擇設定 Amazon Connect。
6. 輸入 Amazon Connect 聯絡控制面板 (CCP) 名稱。

> **Note**
>
> 您為 CCP 提供的名稱將使用於使用者增益集功能表中。選擇對您的使用者有意義的名稱。

7. 輸入由 Amazon Connect 產生的 Amazon Connect 聯絡控制面板 URL。如需取得 URL 的詳細資訊，請參閱提供聯絡控制面板的存取權。
8. 選擇建立 Amazon Connect。

更新目錄的 Amazon Connect 音訊最佳化詳細資訊

若要更新目錄的 Amazon Connect 音訊最佳化詳細資訊：

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選取您的目錄，然後依序選擇動作、更新詳細資訊。
4. 展開 Amazon Connect 音訊最佳化。

> **Note**
>
> 使用 Amazon Connect 進行設定之前，請選擇更新以儲存先前在管理主控台中所做的任何未儲存變更。

5. 選擇設定 Amazon Connect。
6. 選擇編輯。
7. 選取您的目錄，然後依序選擇動作、更新詳細資訊。
8. 更新 Amazon Connect 聯絡控制面板名稱和 URL。
9. 選擇 Save (儲存)。

刪除目錄的 Amazon Connect 音訊最佳化

若要刪除目錄的 Amazon Connect 音訊最佳化：

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。

3. 選取您的目錄，然後依序選擇動作、更新詳細資訊。
4. 展開 Amazon Connect 音訊最佳化。

> **Note**
>
> 使用 Amazon Connect 進行設定之前，請選擇更新以儲存先前在管理主控台中所做的任何未儲存變更。

5. 選擇設定 Amazon Connect。
6. 選擇刪除 Amazon Connect。

如需詳細資訊，請參閱客服人員訓練指南。

啟用診斷日誌上傳

如果要疑難排解用 WorkSpaces 戶端問題，請啟動自動診斷記錄檔 視窗、macOS、Linux 和網頁存取用戶端目前支援此功能。

> **Note**
>
> AWS GovCloud (美國西部) 區域目前無法使用用 WorkSpaces 戶端診斷記錄上傳功能。

診斷日誌上傳

使用診斷記錄檔上傳，您可以將用 WorkSpaces 戶端記錄檔直接上傳 WorkSpaces 至疑難排解問題，而不會中斷用 WorkSpaces 戶端的使用。如果您為使用者啟用診斷記錄上傳，或讓您的使用者自行啟用，記錄檔會 WorkSpaces 自動傳送到。您可以在 WorkSpaces 串流工作階段之前或期間啟用診斷記錄上傳。

如果要從受管理設備自動上傳診斷記錄檔，請安裝支援診斷上傳的 WorkSpaces用戶端。預設會啟用日誌上傳功能。您可使用下列任何一種方式修改設定：

選項 1：使用主 AWS 控台

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。

3. 選擇要啟用診斷記錄的目錄名稱。
4. 向下捲動至自助服務許可。
5. 選擇「查看詳情
6. 選擇編輯。
7. 選擇診斷日誌上傳。
8. 選擇儲存。

選項 2：使用 API 呼叫

您可以編輯目錄設定，以啟用或停用 WorkSpaces Windows、macOS 和 Linux 用戶端，以便使用 API 呼叫自動上傳診斷記錄。如果啟用，當發生用戶端問題時，會將記錄檔傳送至， WorkSpaces 而不需要使用者互動。如需詳細資訊，請參閱 WorkSpaces API 參考資料。

您也可以讓使用者選擇是否要在安裝用戶端後啟用自動診斷日誌上傳。如需詳細資訊，請參閱 WorkSpacesWindows 用戶端應用程式、WorkSpaces macOS 用戶端應用程式和 WorkSpacesLinux 用戶端應用程式。

> **Note**
>
> - 診斷日誌不包含敏感資訊。您可以在目錄層級為使用者停用自動診斷日誌上傳，或允許使用者自行停用這些功能。
> - 若要存取診斷記錄檔上傳功能，您必須安裝下列版本的 WorkSpaces 用戶端：
>   - 5.4.0 或更新版本的視窗用戶端
>   - 5.8.0 或更新版本的 macOS 用戶端
>   - 用戶端的
>   - 二零四客戶端
>   - 您也可以使用 Web Access 用戶端存取診斷記錄檔上傳功能

管理您的 WorkSpaces

您可以 WorkSpaces 使用 WorkSpaces 控制台管理您的。

若要執行目錄管理工作，請參閱 the section called “設定目錄管理”。

> **Note**
>
> - 請務必更新網路相依性驅動程式，例如 ENA、NVMe 和 PV 驅動程式。 WorkSpaces您應該至少每 6 個月執行一次。如需詳細資訊，請參閱針對 Windows 執行個體安裝或升級彈性網路介面卡 (ENA) 驅動程式和升級 Windows 執行個體上的 PV 驅動程式。AWS NVMe 驅動程式
> - 請務必定期將 EC2Config、EC2Launch 和 EC2Launch V2 代理程式更新為最新版本。您應該至少每 6 個月執行一次。如需詳細資訊，請參閱更新 EC2Config 和 EC2 啟動。

目錄

- Microsoft 365 自帶授權 (BYOL)
- 升級視窗自攜裝置 WorkSpaces
- 遷移 WorkSpace
- 刪除 WorkSpace

管理您的視窗 WorkSpaces

您可以使用群組原則物件 (GPO) 來套用設定，以管理屬於 Windows WorkSpaces 目錄的 Windows WorkSpaces 或使用者。

> **Note**
>
> Linux 執行個體不會遵守群組政策。如需管理 Amazon Linux 的相關資訊 WorkSpaces，請參閱管理您的 Amazon Linux WorkSpaces。

我們建議您為 WorkSpaces 電腦物件建立組織單位，並為您的 WorkSpaces 使用者物件建立組織單位。

若要使用 Amazon 專屬的群組原則設定 WorkSpaces，您必須為正在使用的一或多個通訊協定 (PCoIP 或 WorkSpaces 串流通訊協定 (WSP) 安裝群組原則管理範本。

> **Warning**
>
> 群組原則設定可能會影響 WorkSpace 使用者的體驗，如下所示：
>
> - 實作互動式登入訊息以顯示登入橫幅，可防止使用者存取其 WorkSpaces。PCo WorkSpaces IP 目前不支援互動式登入訊息群組原則設定。WSP 支援登入訊息 WorkSpaces，使用者必須在接受登入橫幅後再次登入。
> - 透過群組政策設定停用卸除式儲存裝置會導致登入失敗，這會導致使用者登入無法存取磁碟機 D 的暫時使用者設定檔。
> - 透過群組原則設定從「遠端桌面使用者」本機群組移除使用者，可防止這些使用者透過用 WorkSpaces 戶端應用程式進行驗證。如需有關此群組政策設定的詳細資訊，請參閱 Microsoft 文件中的允許透過遠端桌面服務登入。
> - 如果您從允許本機登入安全性原則中移除內建的使用者群組，您的 PCoIP WorkSpaces 使用者將無法 WorkSpaces 透過用 WorkSpaces 戶端應用程式連線到他們的使用者。您的

PCoIP WorkSpaces 也不會收到 PCoIP 代理程式軟體的更新。PCoIP 代理程式更新可能包含安全性和其他修正程式，或者可能會為您的. WorkSpaces 如需有關使用此安全政策的詳細資訊，請參閱 Microsoft 文件中的允許本機登入。

- 群組政策設定可用於限制磁碟機存取。如果您將群組原則設定設定為限制對磁碟機 C 或磁碟機 D 的存取，則使用者將無法存取磁碟機 D WorkSpaces。若要避免發生此問題，請確定使用者可以存取磁碟機 C 和磁碟機 D。
- WorkSpaces 音訊輸入功能需要在. WorkSpace 視窗 WorkSpaces預設會啟用音訊輸入功能。不過，如果您的群組原則設定會限制使用者的本機登入 WorkSpaces，則音訊輸入將無法在您的. WorkSpaces 如果您移除該群組原則設定，則會在下次重新開機後啟用音訊輸入功能。 WorkSpace如需此群組政策設定的詳細資訊，請參閱 Microsoft 文件中的允許在本機登入。

  如需啟用或停用音訊輸入重新導向的詳細資訊，請參閱 啟用或停用 PCoIP 的音訊輸入重新導向 或 啟用或停用 WSP 的音訊輸入重新導向。
- 使用群組原則將 Windows 電源計劃設定為「平衡」或「省電模式」可能會導 WorkSpaces 致您在閒置時進入睡眠狀態。我們強烈建議使用群組政策將 Windows 電源計畫設定為高效能。如需詳細資訊，請參閱 我的窗戶 WorkSpace 在閒置時進入睡眠狀態。
- 某些群組政策設定會強制使用者在中斷與工作階段的連線時登出。使用者在其上開啟的任何應用程式 WorkSpaces 都會關閉。
- WSP WorkSpaces 目前不支援「為使用中但閒置的遠端桌面服務工作階段設定時間限制」。避免在 WSP 工作階段期間使用它，因為即使有活動且工作階段並未閒置，也會導致連線中斷。

如需使用 Active Directory 管理工具來處理 GPO 的相關資訊，請參閱 設定 WorkSpaces 的 Active Directory 管理工具。

目錄

安裝 WorkSpaces 串流通訊協定 (WSP) 的群組原則系統管理範本檔案

若要使用使用 WorkSpaces 串流通訊協定 (WSP) WorkSpaces 時特定的群組原則設定，您必須將 WSP 的群組原則系統管理範本`wsp.admx`和`wsp.adml`檔案新增至您 WorkSpaces 目錄的網域控制站的中央存放區。如需有關 `.admx` 和 `.adml` 檔案的詳細資訊，請參閱如何在 Windows 中建立和管理群組政策管理範本的中央存放區。

下列程序說明如何建立中央存放區並將管理範本檔案新增到中央存放區。對加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體執行下 WorkSpaces列程序。

若要安裝 WSP 的群組政策管理範本檔案

1. 在執行中的 Windows 中 WorkSpace，複製目`C:\Program Files\Amazon\WSP`錄中的`wsp.admx`和`wsp.adml`檔案。
2. 在加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體上，開啟 Windows 檔案總管，然後在網址列中輸入組織的完整網域名稱 (FQDN)，例如。 WorkSpaces `\\example.com`
3. 開啟 `sysvol` 資料夾。
4. 開啟具有 *FQDN* 名稱的資料夾。
5. 開啟 `Policies` 資料夾。您現在應該在 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies` 中。
6. 如果它不存在，請建立名為 `PolicyDefinitions` 的資料夾。
7. 開啟 `PolicyDefinitions` 資料夾。
8. 將 `wsp.admx` 檔案複製到 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions` 資料夾中。

9. 在 PolicyDefinitions 資料夾中建立名為 en-US 的檔案。
10. 開啟 en-US 資料夾。
11. 將 wsp.adml 檔案複製到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US 資料夾中。

若要確認已正確安裝管理範本檔案

1. 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)。
2. 展開樹系 (樹系：***FQDN***)。
3. 展開網域。
4. 展開您的 FQDN (例如，example.com)。
5. 展開群組政策物件。
6. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。相反地，您必須在具有委派權限的網域容器之下建立並連結 GPO。使用建立目錄時 AWS Managed Microsoft AD， AWS Directory Service 會在網域根目錄下建立######組織單位 (OU)。此 OU 的名稱是以您建立目錄時所輸入的 NetBIOS 名稱為基礎。如未指定 NetBIOS 名稱，預設名稱會是您的目錄 DNS 名稱的第一個部分 (以 corp.example.com 為例，NetBIOS 名稱是 corp)。
> 若要建立 GPO，請不要選取預設網域政策，而是選取 *yourdomainname* OU (或該 OU 下的任何 OU)、開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。
> 如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

7. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
8. 您現在可以使用此 WSP 群組原則物件來修改使用 WSP WorkSpaces 時特定的群組原則設定。

管理 WorkSpaces 串流通訊協定 (WSP) 的群組原則設定

您可以使用群組原則設定來管理使 WorkSpaces 用 WSP 的視窗。

設定 WSP 的印表機支援

預設情況下， WorkSpaces 啟用 Basic 遠端列印，因為它在主機端使用一般印表機驅動程式來確保相容列印，因此提供有限的列印功能。

Windows 用戶端的進階遠端列印 (不適用於 WSP) 可讓您使用印表機的特定功能 (例如雙面列印)，但需要在主機端安裝相符的印表機驅動程式。

遠端列印會以虛擬通道的形式實作。如果停用虛擬通道，遠端列印無法運作。

對於 Windows WorkSpaces，您可以視需要使用群組原則設定來設定印表機支援。

設定印表機支援

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

   > **Note**
   >
   > 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟設定遠端列印設定。
10. 在設定遠端列印對話方塊中，執行下列其中一項操作：
    - 若要啟用本機印表機重新導向，請選擇啟用，然後針對列印選項，選擇基本。若要自動使用用戶端電腦目前的預設印表機，請選取將本機預設印表機對應至遠端主機。

- 若要停用列印，請選擇停用。

11. 選擇確定。
12. 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：

    - 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 ）。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

設定 WSP 的剪貼簿重新導向 (複製/貼上)

根據預設， WorkSpaces 支援雙向 (複製/貼上) 剪貼簿重新導向。對於 Windows WorkSpaces，您可以使用群組原則設定來停用此功能，或設定允許剪貼簿重新導向的方向。

若要設定 Windows 的剪貼簿重新導向 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *`yourdomainname`* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *`yourdomainname`* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟設定剪貼簿重新導向設定。

10. 在設定剪貼簿重新導向對話方塊中，選擇啟用或停用。

    當設定剪貼簿重新導向為啟用時，即可使用下列剪貼簿重新導向選項：

    - 選擇複製並貼上，允許雙向剪貼簿複製並貼上重新導向。
    - 選擇僅限複製，只允許將伺服器剪貼簿中的資料複製到用戶端剪貼簿。
    - 選擇僅限貼上，只允許將用戶端剪貼簿中的資料貼到伺服器剪貼簿。
11. 選擇確定。
12. 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：

    - 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）。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

已知限制

在上啟用剪貼簿重新導向後 WorkSpace，如果您從 Microsoft Office 應用程式複製大於 890 KB 的內容，應用程式可能會變得緩慢或沒有回應，最多 5 秒鐘。

設定 WSP 的工作階段繼續逾時

當您失去網路連線時，作用中的 WorkSpaces 用戶端工作階段會中斷連線。 WorkSpaces 如果在特定時間內還原網路連線，Windows 和 macOS 的用戶端應用程式會嘗試自動重新連線工作階段。預設的工作階段繼續逾時為 20 分鐘 (1200 秒)，但您可以修改該值，由網域的群組原則設定所控制。WorkSpaces

若要設定自動工作階段繼續逾時值

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。

7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用自動重新連線設定。
10. 在啟用/停用自動重新連線對話方塊中，選擇啟用，然後將重新連線逾時 (秒數) 設定為所需的逾時 (秒數)。
11. 選擇確定。
12. 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：

    - 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）。
    - 在管理命令提示中輸入 **gpupdate /force**。

啟用或停用 WSP 的視訊輸入重新導向

默認情況下， WorkSpaces 支持從本地攝像機重定向數據。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

啟用或停用 Windows 的視訊輸入重新導向 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。

6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用視訊輸入重新導向設定。
10. 在啟用/停用視訊輸入重新導向對話方塊中，選擇啟用或停用。
11. 選擇確定。
12. 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：
    - 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）。
    - 在管理命令提示中輸入 **gpupdate /force**。

啟用或停用 WSP 的音訊輸入重新導向

根據預設， WorkSpaces 支援從本機麥克風重新導向資料。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

啟用或停用 Windows 的音訊輸入重新導向 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。

6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用音訊輸入重新導向設定。
10. 在啟用/停用音訊輸入重新導向對話方塊中，選擇啟用或停用。
11. 選擇確定。
12. 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：
    - 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）。
    - 在管理命令提示中輸入 **gpupdate /force**。

啟用或停用 WSP 的音訊輸出重新導向

根據預設，會將資料 WorkSpaces 重新導向至本機喇叭。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

啟用或停用 Windows 的音訊輸出重新導向 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN。例如 `example.com`。

6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，則無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用音訊輸出重新導向設定。
10. 在啟用/停用音訊輸出重新導向對話方塊中，選擇啟用或停用。
11. 選擇確定。
12. 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：
    - 重新啟動 WorkSpace. 在 Amazon 主 WorkSpaces 控台中，選取 WorkSpace，然後選擇「動作」>「重新開機」 WorkSpaces。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

停用 WSP 的時區重新導向

依預設，Workspace 中的時間設定為鏡像用來連線到的用戶端的時區 WorkSpace。此行為透過時區重新導向控制。您可能會基於各種原因而想要關閉時區方向：例如：

- 貴公司希望所有員工都能在特定時區工作 (即使部分員工位於其他時區)。
- 您已排程的工作 WorkSpace ，其目的是要在特定時區的特定時間執行。
- 您經常旅行的用戶希望將其保留 WorkSpaces 在一個時區，以確保一致性和個人偏好。

如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

若要停用 Windows 的時區重新導向 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，則無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用時區重新導向設定。
10. 在啟用/停用時區重新導向對話方塊中，選擇停用。
11. 選擇確定。
12. 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：
    - 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 ）。
    - 在管理命令提示中輸入 **`gpupdate /force`**。
13. 將時區設定 WorkSpaces 為所需的時區。

的時區現在 WorkSpaces 是靜態的，不再鏡像用戶端電腦的時區。

設定 WSP 安全設定

對於 WSP，傳輸中的資料會使用 TLS 1.2 加密進行加密。根據預設，允許下列所有密碼用於加密，而用戶端和伺服器會交涉要使用哪個密碼：

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

對於 Windows WorkSpaces，您可以使用群組原則設定來修改 TLS 安全性模式，以及新增新的或封鎖特定的加密套件。設定安全設定群組政策對話方塊中提供了這些設定和支援密碼套件的詳細說明。

若要設定 WSP 安全設定

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN。例如 `example.com`。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，則無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟設定安全設定。
10. 在設定安全設定對話方塊中，選擇啟用。新增您要允許的密碼套件，並移除您要封鎖的密碼套件。如需有關這些設定的詳細資訊，請參閱設定安全設定對話方塊中提供的描述。
11. 選擇確定。
12. 群組原則設定變更會在下一次群組原則更新之後 WorkSpace，以及重新啟動 WorkSpace工作階段之後生效。若要套用群組政策變更，請執行下列其中一項：

    - 若要重新啟動 WorkSpace，請在 Amazon WorkSpaces 主控台中選取 WorkSpace，然後選擇動作，重新開機 WorkSpaces。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

設定 WSP 的延伸模組

根據預設，會停用 WorkSpaces 擴充功能的支援。如果需要，您可以通過以下方式配置 WorkSpace 為使用擴展程序：

- 伺服器和用戶端 – 啟用伺服器和用戶端的延伸模組
- 僅限伺服器 – 僅啟用伺服器的延伸模組
- 僅限用戶端 – 僅啟用用戶端的延伸模組

對於 Windows WorkSpaces，您可以使用群組原則設定來設定擴充功能的使用。

若要設定 WSP 的延伸模組

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN。例如：`example.com`
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，則無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟設定延伸模組設定。
10. 在設定延伸模組對話方塊中，選擇啟用，然後設定所需的支援選項。選擇僅限用戶端、伺服器和用戶端或僅限伺服器。
11. 選擇確定。
12. 群組原則設定變更會在下次群組原則更新之後生效，以 WorkSpace 及重新啟動 WorkSpace工作階段之後。若要套用群組政策變更，請執行下列其中一項：

    - 重新啟動 WorkSpace. 在 Amazon 主 WorkSpaces 控台中，選取 WorkSpace，然後選擇動作，重新開機 WorkSpaces。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

啟用或停用 WSP 的智慧卡重新導向

依預設，Amazon WorkSpaces 無法支援使用智慧卡進行工作階段前身份驗證或工作階段內身份驗證。工作階段前驗證是指使用者登入時所執行的智慧卡驗證。 WorkSpaces工作階段內驗證是指在登入後執行的驗證。

如果需要，您可以使用群組原則設定為 Windows 啟用工作階段前和工 WorkSpaces 作階段內驗證。您也必須使用 EnableClientAuthentication API 動作或enable-client-authentication AWS CLI 命令，透過 AD Connector 目錄設定來啟用工作階段前驗證。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的啟用 AD Connector 的智慧卡驗證。

> **Note**
>
> 若要在 Windows 中啟用使用智慧卡 WorkSpaces，則需要執行其他步驟。如需詳細資訊，請參閱 使用智慧卡進行驗證。

啟用或停用 Windows 的智慧卡重新導向 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用智慧卡重新導向設定。
10. 在啟用/停用智慧卡重新導向對話方塊中，選擇啟用或停用。
11. 選擇確定。
12. 群組原則設定變更會在 WorkSpace工作階段重新啟動後生效。要應用組策略更改，請重新啟動 WorkSpace （ 在 Amazon WorkSpaces 控制台中，選擇 WorkSpace，然後選擇操作，重新啟動 WorkSpaces ）。

啟用或停用 WSP 的重新導向 WebAuthn (FIDO2)

根據預設，Amazon WorkSpaces 允許使用 WebAuthn 驗證器進行工作階段內身份驗證。會話中身份驗證是指在登錄後執行並由會話中運行的 Web 應用程序請求後執行的 WebAuthn 身份驗證。

要求

WebAuthn (FIDO2) WSP 的重新導向需要下列條件：

- WSP 主機代理程式版本 2.0.0.1425 或更新版本
- WorkSpaces 客戶端：
  - 系統版本
  - 視窗 5.19.0 或更高版本
  - Mac 用戶端 5.19.0 或更高版本
- 在 WorkSpaces 執行 Amazon DCV WebAuthn 重新導向延伸模組上安裝的網頁瀏覽器：
  - 谷歌瀏覽器
  - Microsoft 邊緣

啟用或停用視窗的重新導向 WebAuthn (FIDO2) WorkSpaces

如果需要，您可以使用群組原則設定啟用或停用 Windows WebAuthn WorkSpaces 驗證器的工作階段內驗證支援。如果啟用或未設定此設定，將啟用 WebAuthn 重新導向，且使用者可以在遠端 WorkSpace使用本機驗證器。

啟用功能後，工作階段中來自瀏覽器的所有 WebAuthn 要求都會重新導向至本機用戶端。用戶可以使用 Windows Hello 或本地連接的安全設備（如 YubiKey 或其他 FIDO2 兼容的身份驗證器）來完成身份驗證過程。

啟用或停用視窗的重新導向 WebAuthn (FIDO2) WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *`yourdomainname`* OU (或該 OU 下的任何 OU)，

開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用 WebAuthn 重定向設定。
10. 在 [啟用/停用 WebAuthn 重新導向] 對話方塊中，選擇 [啟用] 或
11. 選擇確定。
12. 群組原則設定變更會在 WorkSpace 工作階段重新啟動後生效。要應用組策略更改，請轉 WorkSpace 到 Amazon WorkSpaces 控制台並選擇重新啟動 WorkSpace。然後，選擇操作，重新啟動 WorkSpaces ）。

安裝 Amazon DCV WebAuthn 重定向擴展

使用者需要安裝 Amazon DCV WebAuthn 重新導向延伸模組，才能在啟用此功能 WebAuthn 之後使用，方法是執行下列任一動作：

- 系統會提示您的使用者在瀏覽器中啟用瀏覽器擴充功能。

> **Note**
>
> 這是一次性的瀏覽器提示。當您將 WSP 代理程式版本更新為 2.0.0.1425 或更新版本時，您的使用者會收到通知。如果您的最終使用者不需要 WebAuthn 重新導向，他們只需從瀏覽器中移除擴充功能即可。您也可以使用下面的 GPO 原則封鎖 WebAuthn 重新導向延伸模組安裝提示。

- 您可以使用以下 GPO 原則強制安裝使用者的重新導向延伸模組。如果您啟用 GPO 原則，當您的使用者啟動具有網際網路存取功能的受支援瀏覽器時，就會自動安裝擴充功能。
- 您的用戶可以使用 Microsoft 邊緣附加組件或 Chrome 網上應用店手動安裝擴展程序。

使用群組原則管理和安裝瀏覽器擴充功能

您可以使用群組原則從您的網域集中安裝 Amazon DCV WebAuthn 重新導向延伸模組，適用於加入 Active Directory (AD) 網域的工作階段主機，或針對每個工作階段主機使用本機群組原則編輯器。此過程將根據您使用的瀏覽器而改變。

對於 Microsoft 邊緣

1. 下載並安裝 Microsoft 邊緣管理範本。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。
8. 選擇電腦設定、系統管理範本、Microsoft 邊緣和擴充功能
9. 開啟 [設定擴充功能管理設定] 並將其設定為 [啟用
10. 在 [設定擴充功能管理設定] 下，輸入下列內容

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. 選擇確定。
12. 群組原則設定變更會在 WorkSpace 工作階段重新啟動後生效。要應用組策略更改，請轉 WorkSpace 到 Amazon WorkSpaces 控制台並選擇重新啟動 WorkSpace。然後，選擇操作，重新啟動 WorkSpaces ）。

> **Note**
>
> 您可以套用下列組態管理設定來封鎖擴充功能的安裝：
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

對於谷歌瀏覽器

1. 下載並安裝谷歌瀏覽器管理模板。如需詳細資訊，請參閱在受管理的電腦上設定 Chrome 瀏覽器政策。

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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。
8. 選擇計算機配置，管理模板，谷歌瀏覽器和擴展
9. 開啟 [設定擴充功能管理設定] 並將其設定為 [啟用
10. 在 [設定擴充功能管理設定] 下，輸入下列內容

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. 選擇確定。
12. 群組原則設定變更會在 WorkSpace 工作階段重新啟動後生效。要應用組策略更改，請轉 WorkSpace 到 Amazon WorkSpaces 控制台並選擇重新啟動 WorkSpace。然後，選擇操作，重新啟動 WorkSpaces ）。

> **Note**
>
> 您可以套用下列組態管理設定來封鎖擴充功能的安裝：
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

針對 WSP 啟用或停用畫面鎖定時中斷工作階段連線

如果需要，您可以在偵測到 Windows 鎖定螢幕時中斷使用者 WorkSpaces 工作階段的連線。若要從用 WorkSpaces 戶端重新連線，使用者可以使用其密碼或智慧卡來驗證自己，這取決於已為其啟用的驗證類型而定 WorkSpaces。

預設會停用群組政策設定。如果需要，您可以使用「群組原則」設定，在偵測到 Windows 的 Windows 鎖定螢幕時啟用中斷工作階段的連線。 WorkSpaces

> **Note**
>
> - 此群組政策設定適用於經過密碼驗證和智慧卡驗證的工作階段。
> - 若要在 Windows 中啟用使用智慧卡 WorkSpaces，則需要執行其他步驟。如需詳細資訊，請參閱 使用智慧卡進行驗證。

啟用或停用 Windows 螢幕鎖定上的中斷連線工作階段 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

   > **Note**
   >
   > 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟啟用/停用畫面鎖定時中斷工作階段連線設定。
10. 在啟用/停用畫面鎖定時中斷工作階段連線對話方塊中，選擇啟用或停用。
11. 選擇確定。

12. 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：

    - 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）。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

啟用或停用 WSP 的間接顯示驅動程式 (IDD)

依預設， WorkSpaces 支援使用間接顯示驅動程式 (IDD) 的支援。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

啟用或停用視窗的間接顯示驅動程式 (IDD) WorkSpaces

1. 請確定 WSP 的最新 WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces 目錄的網域控制站的中央存放區中。
2. 在加入目錄的目 WorkSpaces 錄管理 WorkSpace 或 Amazon 彈性運算雲端執行個體上，開啟群組原則管理工具 (gpmc .msc)。
3. 展開樹系 (樹系:FQDN)。
4. 展開網域。
5. 展開您的 FQDN (例如，`example.com`)。
6. 展開群組政策物件。
7. 選取「預設網域原則」，在功能表上按一下滑鼠右鍵開啟內容，然後選擇「編輯

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS 受管理的 Microsoft AD 目錄，您就無法使用預設網域原則來建立您的 GPO。請改為選取該網域名稱下的`yourdomainname`組織單位 (OU) 或任何 OU，在功能表上按一下滑鼠右鍵開啟前後關聯，然後選擇 [在此網域中建立 GPO]，然後在此處連結。如需 `yourdomainname` OU 的相關資訊，請參閱《 AWS Directory Service 管理指南》中的建立項目。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟「啟用 AWS 間接顯示驅動程式」設定。
10. 在「啟用 AWS 間接顯示驅動程式」對話方塊中，選擇「啟用」或「停用」。
11. 選擇確定。

12. 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 WorkSpaces 控制台中，選擇 WorkSpace，然後選擇操作，重新啟動 WorkSpaces）。

    b. 在管理命令提示中輸入 `gpupdate /force`。

設定 WSP 的顯示設定

WorkSpaces 可讓您設定數種不同的顯示設定，包括最大畫面播放速率、最低影像品質、最大影像品質和 YUV 編碼。根據您需要的影像品質、回應能力和色彩準確度來調整這些設定。

依預設，最大影格率值為 25。最大影格率值可指定每秒允許的最大影格數 (fps)。值為 0 表示沒有限制。

依預設，最低影像品質值為 30。最低影像品質可進行最佳化，以獲得最佳影像回應能力或最佳影像品質。為了獲得最佳回應能力，請降低最低品質。為了獲得最佳品質，請提高最低品質。

- 最佳回應能力的理想值在 30 到 90 之間。
- 最佳品質的理想值在 60 到 90 之間。

依預設，最高影像品質值為 80。最高影像品質不會影響影像回應能力或品質，但會設定最大值以限制網路使用量。

依預設，影像編碼設定為 YUV420。選取啟用 YUV444 編碼可啟用 YUV444 編碼以達到高色彩準確度。

對於 Windows WorkSpaces，您可以使用群組原則設定來設定最大畫面速率、最低影像品質和最大影像品質值。

若要設定視窗的顯示設定 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。

5. 展開您的 FQDNN，例如 `example.com`。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，則無法使用預設網域原則來建立 GPO。請改為選取 *yourdomainname* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟設定顯示設定設定。
10. 在設定顯示設定對話方塊中，選擇啟用，然後將最大影格率 (fps)、最低影像品質和最高影像品質值設定為所需的等級。
11. 選擇確定。
12. 群組原則設定變更會在下次群組原則更新之後生效，以 WorkSpace 及重新啟動 WorkSpace工作階段之後。若要套用群組政策變更，請執行下列其中一項：
    - 重新啟動 WorkSpace Amazon WorkSpaces 控制台，選擇 WorkSpace，然後選擇操作，重新啟動 WorkSpaces
    - 在管理命令提示中輸入 **`gpupdate /force`**。

針對 WSP 的僅限 AWS 虛擬顯示驅動程式啟用或停用 vSync

依預設， WorkSpaces 支援將 vSync 功能用於僅限 AWS 虛擬顯示驅動程式。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

啟用或停用視窗同步 WorkSpaces

1. 請確定 WSP 的最新 WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces 目錄的網域控制站的中央存放區中。
2. 在加入目錄的目 WorkSpaces 錄管理 WorkSpace 或 Amazon 彈性運算雲端執行個體上，開啟群組原則管理工具 (gpmc .msc)。
3. 展開樹系 (樹系:FQDN)。

4. 展開網域。
5. 展開您的 FQDN (例如，example.com)。
6. 展開群組政策物件。
7. 選取「預設網域原則」，在功能表上按一下滑鼠右鍵開啟內容，然後選擇「編輯

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS 受管理的 Microsoft AD 目錄，您就無法使用預設網域原則來建立您的 GPO。請改為選擇yourdomainname組織單位 (OU) 或該網域名稱下的任何 OU，重新按一下功能表以開啟內容，然後選擇 [在此網域中建立 GPO]，然後在此處連結。如需 yourdomainname OU 的相關資訊，請參閱《AWS Directory Service 管理指南》中的建立項目。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟僅限 AWS 虛擬顯示驅動程式設定的啟用 vSync 功能。
10. 在 [僅限 AWS 虛擬顯示驅動程式] 對話方塊的 [啟用 vSync] 功能中，選擇 [啟用] 或 [停用]。
11. 選擇確定。
12. 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。若要套用群組原則變更，請執行下列動作：

    a. 執行下 WorkSpace 列其中一項作業以重新啟動：

       i. 選項 1 — 在 WorkSpaces 控制台中，選擇 WorkSpace 要重新啟動的。然後，選擇操作，重新啟動 WorkSpaces。

       ii. 選項 2 — 在系統管理命令提示字元中，輸入gpupdate /force。

    b. 重新連線至以套用設定。 WorkSpace

    c. 再次重新啟動工作區。

設定 WSP 的日誌詳細程度

根據預設，WSP 的記錄詳細程度層級會設定 WorkSpaces 為 [資訊]。您可以將日誌層級設定為從最不詳細到最詳細的詳細層級，如下所述：

- 錯誤 - 最不詳細
- 警告
- 資訊 - 預設

- 除錯 - 最詳細

對於 Windows WorkSpaces，您可以使用群組原則設定來設定記錄詳細程度等級。

若要設定 Windows 的記錄詳細資訊層級 WorkSpaces

1. 請確定 WSP 的最新WorkSpaces 群組原則系統管理範本已安裝在您 WorkSpaces目錄的網域控制站的中央存放區中。
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)。
3. 展開樹系 (樹系：***FQDN***)。
4. 展開網域。
5. 展開您的 FQDN。例如 `example.com`。
6. 展開群組政策物件。
7. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，則無法使用預設網域原則來建立 GPO。請改為選取 *`yourdomainname`* OU (或該 OU 下的任何 OU)，開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。如需有關 *`yourdomainname`* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

8. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、Amazon 和 WSP。
9. 開啟設定日誌詳細程度設定。
10. 在設定日誌詳細程度對話方塊中，選擇啟用，然後將日誌詳細層級設定為偵錯、錯誤、資訊或警告。
11. 選擇確定。
12. 群組原則設定變更會在下次群組原則更新之後生效，以 WorkSpace 及重新啟動 WorkSpace工作階段之後。若要套用群組政策變更，請執行下列其中一項：
    - 重新啟動 WorkSpace. 在 Amazon 主 WorkSpaces 控台中，選取 WorkSpace，然後選擇動作，重新開機 WorkSpaces。
    - 在管理命令提示中輸入 **`gpupdate /force`**。

安裝 PCoIP 的群組政策管理範本

若要在使用 PCoIP 通訊協定 WorkSpaces 時使用 Amazon 專屬的群組原則設定，您必須新增適用於您的 PCoIP 代理程式版本 (32 位元或 64 位元) 的群組原則管理範本。 WorkSpaces

> **Note**
>
> 如果您混合使 WorkSpaces 用 32 位元和 64 位元代理程式，則可以使用 32 位元代理程式的群組原則系統管理範本，而且您的群組原則設定會套用至 32 位元和 64 位元代理程式。當所有使用 64 位元代理程式時，您 WorkSpaces 可以切換至使用 64 位元代理程式的系統管理範本。

判斷您 WorkSpaces 擁有 32 位元代理程式還是 64 位元代理程式

1. 登入 a WorkSpace，然後選擇 [檢視]、[傳送 Ctrl + Alt + 刪除]，或在工作列上按一下滑鼠右鍵並選擇 [工作管理員] 來開啟 [工作管理員]。
2. 在任務管理員中，移至詳細資訊索引標籤，在欄標題上按一下滑鼠右鍵，然後選擇選取欄。
3. 在選取欄對話方塊中，選取平台，然後選擇確定。
4. 在詳細資訊索引標籤上找到 `pcoip_agent.exe`，然後檢查其平台欄中的值，以判斷 PCoIP 代理程式是 32 位元還是 64 位元。(您可能會看到 32 位元和 64 位 WorkSpaces 元元件的混合，這是正常的。)

安裝 PCoIP 的群組政策管理範本 (32 位元)

若要使用 PCoIP 通訊協定搭配 32 位元 PCoIP 代理程式 WorkSpaces 使用特定的群組原則設定，您必須安裝 PCoIP 的群組原則管理範本。對加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體執行下列程序。

如需使用 .adm 檔案的詳細資訊，請參閱 Microsoft 文件中的管理群組政策管理範本 (.adm) 檔案的建議。

若要安裝 PCoIP 的群組政策管理範本

1. 從正在運行的 Windows 中 WorkSpace，在`C:\Program Files (x86)\Teradici\PCoIP Agent\configuration`目錄中製作`pcoip.adm`文件的副本。
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)，然後導覽至網域中包含 WorkSpaces 機器帳戶的組織單位。

3. 開啟機器帳戶組織單位的內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。
4. 在 [新增 GPO] 對話方塊中，輸入 GPO 的描述性名稱 (例如WorkSpaces 電腦原則)，並將 [來源起始程式 GPO] 設定為 [無]。選擇確定。
5. 開啟新 GPO 的內容 (滑鼠右鍵) 功能表，然後選擇編輯。
6. 在群組政策管理編輯器中，選擇電腦設定、政策和管理範本。從主功能表中依序選擇動作、新增/移除範本。
7. 在新增/移除範本對話方塊中，選擇新增，選取先前複製的 `pcoip.adm` 檔案，然後選擇開啟、關閉。
8. 關閉群組政策管理編輯器。您現在可以使用這個 GPO 來修改特定的群組原則設定 WorkSpaces。

若要確認已正確安裝管理範本檔案

1. 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)，然後瀏覽並選取 WorkSpaces 機器帳戶的 WorkSpaces GPO。在功能表中依序選擇動作、編輯。
2. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、傳統管理範本和 PCoIP 工作階段變數。
3. 您現在可以使用此 PCoIP 工作階段變數群組原則物件來修改 Amazon 在使用 PCoIP WorkSpaces 時特定的群組原則設定。

> **Note**
>
> 若要允許使用者覆寫您的設定，請選擇可覆寫的管理員設定；否則，選擇不可覆寫的管理員設定。

安裝 PCoIP 的群組政策管理範本 (64 位元)

若要使用 PCoIP 通訊協定 WorkSpaces 時特定的群組原則設定，您必須將群組原則系統管理範本`PCoIP.admx`和 PCoIP 的`PCoIP.adml`檔案新增至您目錄的網域控制站的中央存放區。WorkSpaces如需有關 `.admx` 和 `.adml` 檔案的詳細資訊，請參閱如何在 Windows 中建立和管理群組政策管理範本的中央存放區。

下列程序說明如何建立中央存放區並將管理範本檔案新增到中央存放區。對加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體執行下 WorkSpaces 列程序。

若要安裝 PCoIP 的群組政策管理範本檔案

1. 在執行中的 Windows 中 WorkSpace，複製目C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions錄中的PCoIP.admx和PCoIP.adml檔案。PCoIP.adml 檔案位於該目錄的 en-US 子資料夾中。
2. 在加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體上，開啟 Windows 檔案總管，然後在網址列中輸入組織的完整網域名稱 (FQDN)，例如。 WorkSpaces \\example.com
3. 開啟 sysvol 資料夾。
4. 開啟具有 *FQDN* 名稱的資料夾。
5. 開啟 Policies 資料夾。您現在應該在 *FQDN*\sysvol*FQDN*\Policies 中。
6. 如果它不存在，請建立名為 PolicyDefinitions 的資料夾。
7. 開啟 PolicyDefinitions 資料夾。
8. 將 PCoIP.admx 檔案複製到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions 資料夾中。
9. 在 PolicyDefinitions 資料夾中建立名為 en-US 的檔案。
10. 開啟 en-US 資料夾。
11. 將 PCoIP.adml 檔案複製到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US 資料夾中。

若要確認已正確安裝管理範本檔案

1. 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)。
2. 展開樹系 (樹系：***FQDN***)。
3. 展開網域。
4. 展開您的 FQDN (例如，example.com)。
5. 展開群組政策物件。
6. 選取預設網域政策，開啟內容 (滑鼠右鍵) 功能表，然後選擇編輯。

> **Note**
>
> 如果支援的網域 WorkSpaces 是 AWS Managed Microsoft AD 目錄，您就無法使用預設網域原則來建立 GPO。相反地，您必須在具有委派權限的網域容器之下建立並連結 GPO。

使用建立目錄時 AWS Managed Microsoft AD， AWS Directory Service 會在網域根目錄下建立######組織單位 (OU)。此 OU 的名稱是以您建立目錄時所輸入的 NetBIOS 名稱為基礎。如未指定 NetBIOS 名稱，預設名稱會是您的目錄 DNS 名稱的第一個部分 (以 corp.example.com 為例，NetBIOS 名稱是 corp)。
若要建立 GPO，請不要選取預設網域政策，而是選取 *yourdomainname* OU (或該 OU 下的任何 OU)、開啟內容 (滑鼠右鍵) 功能表，然後選擇在此網域中建立 GPO 並連結到此處。
如需有關 *yourdomainname* OU 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立內容。

7. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本和 PCoIP 工作階段變數。
8. 您現在可以使用此 PCoIP 工作階段變數群組原則物件來修改使用 PCoIP WorkSpaces 時特定的群組原則設定。

> **Note**
>
> 若要允許使用者覆寫您的設定，請選擇可覆寫的管理員設定；否則，選擇不可覆寫的管理員設定。

管理 PCoIP 的群組原則設定

使用群組原則設定來管理使用 PCoIP WorkSpaces 的視窗。

設定 PCoIP 的印表機支援

預設情況下， WorkSpaces 啟用 Basic 遠端列印，因為它在主機端使用一般印表機驅動程式來確保相容列印，因此提供有限的列印功能。

Windows 用戶端的進階遠端列印可讓您使用印表機的特定功能 (例如雙面列印)，但需要在主機端安裝相符的印表機驅動程式。

遠端列印會以虛擬通道的形式實作。如果停用虛擬通道，遠端列印無法運作。

對於 Windows WorkSpaces，您可以視需要使用群組原則設定來設定印表機支援。

設定印表機支援

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟設定遠端列印設定。
4. 在設定遠端列印對話方塊中，執行下列其中一項操作：
   - 若要啟用進階遠端列印，請選擇啟用，然後針對選項之下的設定遠端列印，選擇 Windows 用戶端的基本和進階列印。若要自動使用用戶端電腦目前的預設印表機，請選取自動設定預設印表機。
   - 若要停用列印，請選擇啟用，然後在選項、設定遠端列印之下選擇 停用列印。
5. 選擇確定。
6. 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：
   - 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）。
   - 在管理命令提示中輸入 **`gpupdate /force`**。

預設會停用本機印表機自動重新導向。您可以使用群組原則設定來啟用此功能，以便每次連線到您的本機印表機時，都會將本機印表機設定為預設印表機 WorkSpace。

> **Note**
>
> 本機印表機重新導向不適用於 Amazon Linux WorkSpaces。

若要啟用本機印表機自動重新導向

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟設定遠端列印設定。
4. 選擇啟用，然後在選項、設定遠端列印之下，選擇下列其中一項：
   - Windows 用戶端的基本和進階列印
   - 基本列印

5. 選取自動設定預設印表機，然後選擇確定。
6. 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：
   - 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）。
   - 在管理命令提示中輸入 **gpupdate /force**。

啟用或停用 PCoIP 的剪貼簿重新導向 (複製/貼上)

默認情況下， WorkSpaces 支持剪貼板重定向。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

若要啟用或停用剪貼簿重新導向

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟設定剪貼簿重新導向設定。
4. 在設定剪貼簿重新導向對話方塊中，選擇啟用，然後選擇下列其中一個設定來決定允許剪貼簿重新導向的方向。完成時，選擇確定。
   - 兩個方向都停用
   - 僅啟用代理程式至用戶端 (WorkSpace 至本機電腦)
   - 僅啟用用戶端至代理程式 (本機電腦至 WorkSpace)
   - 兩個方向都啟用
5. 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：
   - 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）。
   - 在管理命令提示中輸入 **gpupdate /force**。

已知限制

在上啟用剪貼簿重新導向後 WorkSpace，如果您從 Microsoft Office 應用程式複製大於 890 KB 的內容，應用程式可能會變得緩慢或沒有回應，最多 5 秒鐘。

設定 PCoIP 的工作階段繼續逾時

當您失去網路連線時，作用中的 WorkSpaces 用戶端工作階段會中斷連線。 WorkSpaces 如果在特定時間內還原網路連線，Windows 和 macOS 的用戶端應用程式會嘗試自動重新連線工作階段。預設的工作階段繼續逾時為 20 分鐘，但您可以修改由網域的群組原則設定所控制的值。 WorkSpaces

若要設定自動工作階段繼續逾時值

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟設定工作階段自動重新連線政策設定。
4. 在設定工作階段自動重新連線政策對話方塊中，選擇啟用，將設定工作階段自動重新連線政策選項設定為所需的逾時 (分鐘)，然後選擇確定。
5. 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：

   - 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 ）。
   - 在管理命令提示中輸入 **`gpupdate /force`**。

啟用或停用 PCoIP 的音訊輸入重新導向

根據預設，Amazon WorkSpaces 支援從本機麥克風重新導向資料。如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

> **Note**
>
> 如果您的群組原則設定會限制使用者的本機登入 WorkSpaces，音訊輸入將無法在您的. WorkSpaces 如果您移除該群組原則設定，則會在下次重新開機後啟用音訊輸入功能。 WorkSpace如需此群組政策設定的詳細資訊，請參閱 Microsoft 文件中的允許在本機登入。

若要啟用或停用音訊輸入重新導向

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟在 PCoIP 工作階段中啟用/停用音訊設定。
4. 在在 PCoIP 工作階段中啟用/停用音訊對話方塊中，選擇啟用或停用。
5. 選擇確定。
6. 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：

   - 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 ）。
   - 在管理命令提示中輸入 **`gpupdate /force`**。

停用 PCoIP 的時區重新導向

依預設，Workspace 中的時間設定為鏡像用來連線到的用戶端的時區 WorkSpace。此行為透過時區重新導向控制。您可能會基於各種原因而想要關閉時區方向：

- 貴公司希望所有員工都能在特定時區工作 (即使部分員工位於其他時區)。
- 您已排程的工作 WorkSpace ，其目的是要在特定時區的特定時間執行。
- 您經常旅行的用戶希望將其保留 WorkSpaces 在一個時區，以確保一致性和個人偏好。

如果 Windows 需要 WorkSpaces，您可以使用群組原則設定來停用此功能。

若要停用時區重新導向

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟設定時區重新導向設定。
4. 在設定時區重新導向對話方塊中，選擇停用。
5. 選擇確定。

6. 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：

   - 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）。
   - 在管理命令提示中輸入 **`gpupdate /force`**。
7. 將時區設定 WorkSpaces 為所需的時區。

的時區現在 WorkSpaces 是靜態的，不再鏡像用戶端電腦的時區。

設定 PCoIP 安全設定

對於 PCoIP，傳輸中的資料會使用 TLS 1.2 加密和 SigV4 要求簽署加密。PCoIP 通訊協定會針對串流像素，使用加密的 UDP 流量搭配 AES 加密。使用連接埠 4172 (TCP 和 UDP) 的串流連線會使用 AES-128 和 AES-256 密碼加密，但是加密預設為 128 位元。您可使用設定 PCoIP 安全設定群組政策設定，將此預設值變更為 256 位元。

您也可使用此群組政策設定來修改 TLS 安全模式，以及封鎖特定密碼套件。設定 PCoIP 安全設定群組政策對話方塊中提供了這些設定和支援密碼套件的詳細說明。

若要設定 PCoIP 安全設定

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟設定 PCoIP 保全設定設定。
4. 在設定 PCoIP 保全設定對話方塊中，選擇啟用。若要將串流流量的預設加密設為 256 位元，請前往 PCoIP 資料加密密碼選項，然後選取僅限 AES-256-GCM。
5. (選用) 調整 TLS 安全模式設定，然後列出您要封鎖的任何密碼套件。如需有關這些設定的詳細資訊，請參閱設定 PCoIP 保全設定對話方塊中提供的描述。
6. 選擇確定。
7. 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：

   - 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）。

- 在管理命令提示中輸入 **gpupdate /force**。

啟用 YubiKey U2F 的 USB 重新導向

> **Note**
>
> Amazon WorkSpaces 目前僅支持 YubiKey U2F 的 USB 重定向。其他類型的 USB 裝置可能會被重新導向，但不受支援，可能無法正常運作。

若要啟用 YubiKey U2F 的 USB 重新導向

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) 並導覽至 PCoIP 工作階段變數。
3. 開啟在 PCOIP 工作階段中啟用/停用 USB 設定。
4. 選擇啟用，然後選擇確定。
5. 開啟設定 PCoIP USB 允許和不允許的裝置規則設定。
6. 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。
   - 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，其中 xxxx 是十六進位格式的 VID，而 yyyy 則是十六進位格式的 PID。在這個範例中，1050 是 VID，而 0407 是 PID。如需更多 YubiKey USB 值，請參閱 YubiKey USB 識別碼值。
7. 在輸入 USB 授權表格 (最多十個規則) 之下，設定您的 USB 裝置封鎖清單規則。
   - 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。
8. 選擇確定。

9. 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：

   - 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）。
   - 在管理命令提示中輸入 **`gpupdate /force`**。

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。

設定 Kerberos 票證的生命週期上限

如果您尚未停用 Windows 的 [記住我] 功能 WorkSpaces，您的使用 WorkSpace 者可以使用用 WorkSpaces 戶端應用程式中的 [記住我] 或 [讓我保持登入狀態] 核取方塊來儲存其認證。此功能可讓使用者在用戶端應用程式維持執行 WorkSpaces時輕鬆連線至其。他們的憑證會安全地進行快取，直到其 Kerberos 票證的生命週期上限為止。

如果您 WorkSpace 使用 AD Connector 目錄，您可以透過群組原則修改使用 WorkSpaces 者 Kerberos 票證的最長存留期限，方法是遵循 Microsoft Windows 說明文件中的使用者票證中的步驟。

若要啟用或停用記住我功能，請參閱 為您的使用者啟用自助式 WorkSpace管理功能。

設定裝置 Proxy 伺服器設定以存取網際網路

根據預設，用 WorkSpaces 戶端應用程式會使用 HTTPS (連接埠 443) 流量裝置作業系統設定中指定的 Proxy 伺服器。Amazon 用 WorkSpaces 戶端應用程式使用 HTTPS 連接埠進行更新、註冊和身份驗證。

> **Note**
>
> 不支援需要使用登入憑證進行驗證的 Proxy 伺服器。

您可以依照 Microsoft 說明文件中設定裝置 Proxy 和網際網路連線設定中的步驟， WorkSpaces 透過群組原則為您的 Windows 設定裝置代理伺服器設定。

如需有關在 WorkSpaces Windows 用戶端應用程式中設定代理伺服器的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

如需有關在 WorkSpaces macOS 用戶端應用程式中設定代理伺服器的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

如需有關在 WorkSpaces Web 存取用戶端應用程式中設定代理伺服器設定的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

代理桌面流量

對於 PCoIP WorkSpaces，桌面用戶端應用程式不支援使用 Proxy 伺服器，也不支援在 UDP 中使用 TLS 解密和檢查連接埠 4172 流量 (針對桌面流量)。它們需要直接連線至連接埠 4172。

對於 WSP WorkSpaces， WorkSpaces 視窗用戶端應用程式（5.1 及以上版本）和 macOS 用戶端應用程式（5.4 版及以上版本）支援使用 HTTP 代理伺服器進行連接埠 4195 TCP 流量。不支援 TLS 解密和檢查。

WSP 不支援透過 UDP 將 Proxy 用於桌面流量。只有 WorkSpaces Windows 和 macOS 桌面用戶端應用程式和 WSP 網頁存取支援使用代理伺服器，用於 TCP 流量。

> **Note**
>
> 如果您選擇使用 Proxy 伺服器，用戶端應用程式對 WorkSpaces 服務進行的 API 呼叫也會被代理。API 呼叫和桌面流量都應該通過相同的 Proxy 伺服器。

Proxy 伺服器的使用建議

我們不建議使用代理服務器與您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已經加密，因此 Proxy 無法改善安全性。Proxy 代表網路路徑中的額外躍點，可能會藉由引入延遲來影響串流品質。如果 Proxy 未適當調整大小以處理桌面串流流量，Proxy 也可能降低輸送量。此外，大多數代理不是為支持長時間運行 WebSocket（TCP）連接而設計的，可能會影響流的質量和穩定性。

如果您必須使用代理伺服器，請將 Proxy 伺服器盡可能靠近用 WorkSpace戶端 (最好位於同一個網路中)，以避免增加網路延遲，這可能會對串流品質和回應能力造成負面影響。

啟用 Amazon WorkSpaces 的 Zoom 會議媒體插件支持

縮放支持基於 WSP 和 PCoIP 視窗的優化實時通信 WorkSpaces，與縮放 VDI 插件。直接用戶端通訊可讓視訊通話略過雲端虛擬桌面，並在會議在使用者內部執行時提供類似本機的 Zoom 體驗。WorkSpace

為 WSP 啟用縮放會議媒體插件

在安裝 Zoom VDI 元件之前，請先更新您的 WorkSpaces 組態以支援 Zoom 最佳化。

必要條件

在使用插件之前，請確保滿足以下要求。

- 視窗 WorkSpaces 用戶端版本 5.10.0+ 與縮放 V DI 外掛程式版本 5.17.10 以上
- 在您的 WorkSpaces — 縮放 VDI 會議用戶端版本 5.17.10 以上

開始之前

1. 啟用「擴充功能群組原則」設定。如需詳細資訊，請參閱 設定 WSP 的延伸模組。
2. 停用 [自動重新連線群組原則] 設定。如需詳細資訊，請參閱 設定 WSP 的工作階段繼續逾時。

安裝縮放組件

若要啟用縮放最佳化，請在您的視窗上安裝 Zoom 提供的兩個元件 WorkSpaces。如需詳細資訊，請參閱針對 Amazon Web Services 使用 Zoom。

1. 安裝縮放 VDI 會議客戶端版本 5.12.6+ 在您的. WorkSpace
2. 在安裝您的用戶端上安裝縮放 VDI 外掛程式 (視窗通用安裝程式) 5.12.6+ 版 WorkSpace
3. 通過確認您的 VDI 插件狀態在 Zoom VDI 客戶端中顯示為「已連接」，驗證插件是否正在優化 Zoom 流量。如需詳細資訊，請參閱如何確認 Amazon WorkSpaces 最佳化。

為 PCoIP 啟用縮放會議媒體外掛程式

具有 Active Directory 系統管理權限的使用者可以使用其群組原則物件 (GPO) 產生登錄機碼。這可讓使用者使用強制更新，將登錄機碼傳送至網域 WorkSpaces 內的所有 Windows。或者，具有系統管理權限的使用者也可以在其 WorkSpaces 主機上個別安裝登錄機碼。

必要條件

在使用插件之前，請確保滿足以下要求。

- 視窗 WorkSpaces 客戶端版本 5.4.0 + 與縮放 VDI 插件版本 5.12.6+。
- 在您的 WorkSpaces — 縮放 VDI 會議客戶端版本 5.12.6+.

在 Windows WorkSpaces 主機上建立登錄機碼

請完成下列程序，在 Windows WorkSpaces 主機上建立登錄機碼。需要登錄機碼才能在視窗上使用縮放功能 WorkSpaces。

1. 以管理員身分開啟 Windows 登錄編輯程式。
2. 前往 `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`。
3. 如果延伸模組金鑰不存在，請按一下滑鼠右鍵並選擇新增 > 金鑰，然後將其命名為延伸模組。
4. 在新的延伸模組金鑰中，按一下滑鼠右鍵並選擇新增 > DWORD，然後將其命名為啟用。名稱必須是小寫。
5. 選擇新的 DWORD 並將「值」變更為 1。
6. 重新啟動電腦以完成此程序。
7. 在您的 WorkSpaces 主機上下載並安裝最新的 Zoom VDI 用戶端。在您的 WorkSpaces 客戶端（5.4 或更高版本）上，下載並安裝 Amazon WorkSpaces 最新的 Zoom VDI 客戶端插件。如需詳細資訊，請參閱 Zoom 支援網站上的 VDI 版本和下載。

啟動 Zoom 以開始進行視訊通話。

故障診斷

完成下列動作以疑難排解「視窗上的縮放」問 WorkSpaces題

- 確認登錄機碼啟用並正確套用。
- 前往 `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`。您應該看見 `wse_core_dll`。
- 請確定主機和用戶端上的版本正確且相同。

如果您仍然遇到困難，請 AWS Support 使用中AWS Support 心聯繫。

您可以使用下列範例，以目錄的管理員身分套用 GPO。

- WSE.ADML

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
```

```
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
```

```
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

管理您的 Amazon Linux WorkSpaces

與 Windows 一樣 WorkSpaces，Amazon Linux WorkSpaces 已加入網域，因此您可以使用活動目錄使用者和群組來：

- 管理您的 Amazon Linux WorkSpaces
- WorkSpaces 為使用者提供存取權限

由於 Linux 執行個體不遵守群組政策，因此建議您使用組態管理解決方案來散發和強制執行政策。例如，您可以使用 AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise 或 Ansible。

> **Note**
>
> 本機印表機重新導向不適用於 Amazon Linux WorkSpaces。

在 Amazon Linux 上控制 WorkSpaces 流協議（WSP）行為 WorkSpaces

WSP 的行為是由位於 `/etc/wsp/` 目錄中的 `wsp.conf` 檔案中的組態設定所控制。若要部署和強制執行政策變更，請使用支援 Amazon Linux 的組態管理解決方案。任何變更都會在代理程式啟動時生效。

> **Note**
>
> - 如果您對`wsp.conf`檔案進行了不正確或不支援的變更，原則變更可能不會套用至您的上新建立的連線 WorkSpace。
> - WSP WorkSpaces 上的 Amazon Linux 服務包目前有以下限制：
>   - 目前僅適用於 AWS GovCloud （美國西部）和 AWS GovCloud （美國東部）。
>   - 不支援視訊輸入。
>   - 不支援在螢幕鎖定時中斷工作階段連線。

下列各節描述如何啟用或停用某些功能。

設定 WSP Amazon Linux 的剪貼簿重新導向 WorkSpaces

默認情況下， WorkSpaces 支持剪貼板重定向。如有需要，使用 WSP 組態檔來設定此功能。當您中斷連接並重新連接時，此設定生效 WorkSpace。

若要設定 WSP Amazon Linux 的剪貼簿重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. ```
   clipboard = X
   ```

   其中 *X* 的可能值為：

   `enabled`—雙向啟用剪貼簿重新導向 (預設值)
   ```

disabled—雙向停用剪貼簿重新導向

paste-only—已啟用剪貼簿重新導向，但僅允許您從本機用戶端裝置複製內容並將其貼到遠端主機桌面

copy-only—已啟用剪貼簿重新導向，但僅允許您從遠端主機桌面複製內容並將其貼到本機用戶端裝置

啟用或停用 WSP Amazon Linux 的音訊輸入重新導向 WorkSpaces

依預設， WorkSpaces 支援音訊輸入重新導向。如有需要，使用 WSP 組態檔來停用此功能。當您中斷連接並重新連接到時，此設定生效 WorkSpace。

啟用或停用 WSP Amazon Linux 的音訊輸入重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 wsp.conf 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 在檔案的結尾新增此行：

```
audio-in = X
```

其中 *X* 的可能值為：

enabled—已啟用音訊輸入重新導向 (預設值)

disabled—已停用音訊輸入重新導向

啟用或停用 WSP Amazon Linux 的時區重新導向 WorkSpaces

依預設，Workspace 中的時間設定為鏡像用來連線到的用戶端的時區 WorkSpace。此行為透過時區重新導向控制。您可能會基於下列之類的原因而想要關閉時區方向：

- 貴公司希望所有員工都能在特定時區工作 (即使部分員工位於其他時區)。
- 您已排程的工作 WorkSpace ，其目的是要在特定時區的特定時間執行。
- 您經常旅行的用戶希望將其保留 WorkSpaces 在一個時區，以確保一致性和個人偏好。

如有需要，使用 WSP 組態檔來設定此功能。在您中斷連接並重新連接到之後，此設定生效 WorkSpace。

啟用或停用 WSP Amazon Linux 的時區重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. 在檔案的結尾新增此行：

```
timezone_redirect= X
```

其中 *X* 的可能值為：

enabled—已啟用時區重新導向 (預設值)

disabled—已停用時區重新導向

控制 Amazon 伺服器上的 PCoIP 代理程式行為 WorkSpaces

PCoIP 代理程式的行為是由位於 `/etc/pcoip-agent/` 目錄中的 `pcoip-agent.conf` 檔案中的組態設定所控制。若要部署和強制執行政策變更，請使用支援 Amazon Linux 的組態管理解決方案。任何變更都會在代理程式啟動時生效。重新啟動代理程式會結束任何開啟的連線並重新啟動視窗管理員。若要套用任何變更，建議您重新啟動 WorkSpace.

> **Note**
>
> 如果您對`pcoip-agent.conf`檔案進行了不正確或不支援的變更，可能會導 WorkSpace 致您停止運作。如果您 WorkSpace 停止運作，您可能需要 WorkSpace 使用 SSH 連線以復原變更，或者您可能必須重建 WorkSpace.

下列各節描述如何啟用或停用某些功能。如需可用設定的完整清單，請`man pcoip-agent.conf`從任何 Amazon Linux 上的終端機執行 WorkSpace。

為 PCoIP Amazon Linux 設定剪貼簿重新導向 WorkSpaces

默認情況下， WorkSpaces 支持剪貼板重定向。如有需要，使用 PCoIP 代理程式組態來停用此功能。當您重新開機時，此設定會生效 WorkSpace。

若要設定 PCoIP Amazon Linux 的剪貼簿重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `pcoip-agent.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 在檔案的結尾新增此行：

```
pcoip.server_clipboard_state = X
```

其中 *X* 的可能值為：

0—雙向停用剪貼簿重新導向

1—雙向啟用剪貼簿重新導向

2—僅啟用用戶端至代理程式的剪貼簿重新導向 (僅允許從本機用戶端裝置複製並貼到遠端主機桌面)

3—僅啟用代理程式至用戶端的剪貼簿重新導向 (僅允許從遠端主機桌面複製並貼到本機用戶端裝置)

> **Note**
>
> 剪貼簿重新導向會以虛擬通道的形式實作。如果停用虛擬通道，剪貼簿重新導向無法運作。若要啟用虛擬通道，請參閱 Teradici 文件中的 PCoIP 虛擬通道。

啟用或停用 PCoIP Amazon Linux 的音訊輸入重新導向 WorkSpaces

依預設， WorkSpaces 支援音訊輸入重新導向。如有需要，使用 PCoIP 代理程式組態來停用此功能。當您重新開機時，此設定會生效 WorkSpace。

啟用或停用 PCoIP Amazon Linux 的音訊輸入重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `pcoip-agent.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 在檔案的結尾新增此行：

```
pcoip.enable_audio = X
```

其中 *X* 的可能值為：

0—已停用音訊輸入重新導向

1—已啟用音訊輸入重新導向

啟用或停用時區重新導向 WorkSpaces

依預設，Workspace 中的時間設定為鏡像用來連線到的用戶端的時區 WorkSpace。此行為透過時區重新導向控制。您可能會基於下列之類的原因而想要關閉時區方向：

- 貴公司希望所有員工都能在特定時區工作 (即使部分員工位於其他時區)。
- 您已排程的工作 WorkSpace ，其目的是要在特定時區的特定時間執行。
- 您經常旅行的用戶希望將其保留 WorkSpaces 在一個時區，以確保一致性和個人偏好。

如果 Linux 有需要 WorkSpaces，您可以使用 PCoIP 代理程式連接來停用這項功能。當您重新開機時，此設定會生效 WorkSpace。

若要啟用或停用 PCoIP Amazon Linux 的時區重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `pcoip-agent.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 在檔案的結尾新增此行：

```
pcoip.enable_timezone_redirect= X
```

其中 *X* 的可能值為：

0—已停用時區重新導向

1—已啟用時區重新導向

將 SSH 存取權授予 Amazon Linux WorkSpaces 管理員

根據預設，只有網域管理員群組中指派的使用者和帳戶可以使用 SSH 連線到 Amazon Linux WorkSpaces 。

我們建議您在活動目錄中為您的 Amazon Linux 管理員創建一個專用的 WorkSpaces管理員組。

若要啟用 Linux_Workspaces_Admins Active Directory 群組成員的 sudo 存取權

1. 使用 `visudo` 來編輯 `sudoers` 檔案，如下列範例所示。

```
[example\username@workspace-id ~]$ sudo visudo
```

2. 新增以下這一行。

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

建立專用管理員群組後，請依照下列步驟來啟用群組成員的登入功能。

啟用登入 Linux WorkSpaces _ 管理員作用中目錄群組的成員

1. 使用提升的權限編輯 `/etc/security/access.conf`。

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 新增以下這一行。

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

如需有關啟用 SSH 連線的詳細資訊，請參閱 為您的 Linux 啟用安全殼層連線 WorkSpaces。

覆蓋 Amazon Linux 的默認外殼 WorkSpaces

若要覆寫 Linux 的預設殼層 WorkSpaces，建議您編輯使用者的~/.bashrc檔案。例如，若要使用 Z shell 而不是 Bash Shell，請將下列幾行加入至 /home/*username*/.bashrc。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 進行此變更之後，您必須重新啟動 WorkSpace 或登出 WorkSpace (不只是中斷連線)，然後重新登入，變更才會生效。

保護自訂儲存庫免於未經授權的存取

若要控制對自訂儲存庫的存取，建議您使用 Amazon Virtual Private Cloud (Amazon VPC) 內建的安全功能，而非使用密碼。例如，使用網路存取控制清單 (ACL) 和安全群組。如需這些功能的詳細資訊，請參閱《Amazon VPC 使用者指南》中的安全性。

如果您必須使用密碼來保護儲存庫，務必建立 yum 儲存庫定義檔案，如 Fedora 文件中的儲存庫定義檔所示。

使用 Amazon Linux Extras Library 儲存庫

使用 Amazon Linux 時，您可用 Extras Library 將應用程式和軟體更新安裝至執行個體。如需使用 Extras Library 的詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的 Extras Library (Amazon Linux)。

> **Note**
>
> 如果您使用的是 Amazon Linux 儲存庫，您的 Amazon Linux WorkSpaces 必須能夠存取網際網路，或者您必須將虛擬私有雲端 (VPC) 端點設定為此儲存庫和主要 Amazon Linux 儲存庫。如需詳細資訊，請參閱 提供您的網際網路存取 WorkSpace。

在 Linux 上使用智慧卡進行驗證 WorkSpaces

Linux WorkSpaces on WorkSpaces 串流通訊協定 (WSP) 套件允許使用通用存取卡 (CAC) 和個人身分驗證 (PIV) 智慧卡進行驗證。如需詳細資訊，請參閱 使用智慧卡進行驗證。

設定裝置 Proxy 伺服器設定以存取網際網路

根據預設，用 WorkSpaces 戶端應用程式會使用 HTTPS (連接埠 443) 流量裝置作業系統設定中指定的 Proxy 伺服器。Amazon 用 WorkSpaces 戶端應用程式使用 HTTPS 連接埠進行更新、註冊和身份驗證。

> **Note**
>
> 不支援需要使用登入憑證進行驗證的 Proxy 伺服器。

您可以依照 Microsoft 說明文件中設定裝置 Proxy 和網際網路連線設定中的步驟， WorkSpaces 透過群組原則為 Linux 設定裝置 Proxy 伺服器設定。

如需有關在 WorkSpaces Windows 用戶端應用程式中設定代理伺服器的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

如需有關在 WorkSpaces macOS 用戶端應用程式中設定代理伺服器的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

如需有關在 WorkSpaces Web 存取用戶端應用程式中設定代理伺服器設定的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

代理桌面流量

對於 PCoIP WorkSpaces，桌面用戶端應用程式不支援使用 Proxy 伺服器，也不支援在 UDP 中使用 TLS 解密和檢查連接埠 4172 流量 (針對桌面流量)。它們需要直接連線至連接埠 4172。

對於 WSP WorkSpaces， WorkSpaces 視窗用戶端應用程式（5.1 及以上版本）和 macOS 用戶端應用程式（5.4 版及以上版本）支援使用 HTTP 代理伺服器進行連接埠 4195 TCP 流量。不支援 TLS 解密和檢查。

WSP 不支援透過 UDP 將 Proxy 用於桌面流量。只有 WorkSpaces Windows 和 macOS 桌面用戶端應用程式和 WSP 網頁存取支援使用代理伺服器，用於 TCP 流量。

> **Note**
>
> 如果您選擇使用 Proxy 伺服器，用戶端應用程式對 WorkSpaces 服務進行的 API 呼叫也會被代理。API 呼叫和桌面流量都應該通過相同的 Proxy 伺服器。

Proxy 伺服器的使用建議

我們不建議使用代理服務器與您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已經加密，因此 Proxy 無法改善安全性。Proxy 代表網路路徑中的額外躍點，可能會藉由引入延遲來影響串流品質。如果 Proxy 未適當調整大小以處理桌面串流流量，Proxy 也可能降低輸送量。此外，大多數代理不是為支持長時間運行 WebSocket （ TCP ）連接而設計的，可能會影響流的質量和穩定性。

如果您必須使用代理伺服器，請將 Proxy 伺服器盡可能靠近用 WorkSpace 戶端 (最好位於同一個網路中)，以避免增加網路延遲，這可能會對串流品質和回應能力造成負面影響。

管理您的 WorkSpaces

與視窗和 Amazon Linux 一樣 WorkSpaces，Ubuntu WorkSpaces 是域加入的，因此您可以使用活動目錄用戶和組來：

- 管理你的 WorkSpaces
- WorkSpaces 為使用者提供存取權

您可以通過使用 ADSys 管理 Ubuntu WorkSpaces 與組策略。如需詳細資訊，請參閱 Ubuntu Active Directory 整合常見問答集。您也可以使用其他配置和管理解決方案，例如 Landscape 和 Ansible。

控制 Ubuntu 上的 WorkSpaces 串流通訊協定 (WSP) 行為 WorkSpaces

WSP 的行為是由位於 `/etc/wsp/` 目錄中的 `wsp.conf` 檔案中的組態設定所控制。若要部署和強制執行政策變更，請使用支援 Ubuntu 的組態管理解決方案。任何變更都會在代理程式啟動時生效。

> **Note**
>
> 如果您對`wsp.conf`原則進行不正確或不支援的變更，可能不會套用至您的新建立的連線 WorkSpace。

下列各節描述如何啟用或停用某些功能。

啟用或停用 Ubuntu 的剪貼簿重新導向 WorkSpaces

默認情況下， WorkSpaces 支持剪貼板重定向。如有需要，使用 WSP 組態檔來停用此功能。

若要啟用或停用 Ubuntu 的剪貼簿重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 在 `[policies]` 群組的結尾新增此行：

```
clipboard = X
```

其中 *X* 的可能值為：

enabled—雙向啟用剪貼簿重新導向 (預設值)

disabled—雙向停用剪貼簿重新導向

paste-only—已啟用剪貼簿重新導向，且僅允許您從本機用戶端裝置複製內容並將其貼到遠端主機桌面

copy-only—已啟用剪貼簿重新導向，且僅允許您從遠端主機桌面複製內容並將其貼到本機用戶端裝置

啟用或停用 Ubuntu 的音訊輸入重新導向 WorkSpaces

依預設， WorkSpaces 支援音訊輸入重新導向。如有需要，使用 WSP 組態檔來停用此功能。

若要啟用或停用 Ubuntu 的音訊輸入重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 在 `[policies]` 群組的結尾新增此行：

```
audio-in = X
```

其中 *X* 的可能值為：

enabled—已啟用音訊輸入重新導向 (預設值)

disabled—已停用音訊輸入重新導向

啟用或停用 Ubuntu 的視訊輸入重新導向 WorkSpaces

依預設， WorkSpaces 支援視訊輸入重新導向。如有需要，使用 WSP 組態檔來停用此功能。

若要啟用或停用 Ubuntu 的視訊輸入重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 在 `[policies]` 群組的結尾新增此行：

```
video-in = X
```

其中 *X* 的可能值為：

enabled—已啟用視訊輸入重新導向 (預設值)

disabled—已停用視訊輸入重新導向

啟用或停用 Ubuntu 的時區重新導向 WorkSpaces

依預設，Workspace 中的時間設定為鏡像用來連線到的用戶端的時區 WorkSpace。此行為透過時區重新導向控制。您可能會基於下列之類的原因而想要關閉時區方向：

- 貴公司希望所有員工都能在特定時區工作 (即使部分員工位於其他時區)。
- 您已排程的工作 WorkSpace ，其目的是要在特定時區的特定時間執行。
- 您的用戶經常旅行，並希望將其保持 WorkSpaces 在一個時區，以確保一致性和個人偏好。

如有需要，使用 WSP 組態檔來設定此功能。

若要啟用或停用 Ubuntu 的時區重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 在 `[policies]` 群組的結尾新增此行：

```
timezone-redirection = X
```

其中 *X* 的可能值為：

enabled—已啟用時區重新導向 (預設值)

disabled—已停用時區重新導向

啟用或停用 Ubuntu 的印表機重新導向 WorkSpaces

依預設， WorkSpaces 支援印表機重新導向。如有需要，使用 WSP 組態檔來停用此功能。

若要啟用或停用 Ubuntu 的印表機重新導向 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 在 `[policies]` 群組的結尾新增此行：

```
remote-printing = X
```

其中 *X* 的可能值為：

enabled—已啟用印表機重新導向 (預設值)

disabled—已停用印表機重新導向

針對 WSP 啟用或停用畫面鎖定時中斷工作階段連線

啟用螢幕鎖定時中斷連線工作階段，以允許使用者在偵測到鎖定螢幕時結束 WorkSpaces 工作階段。若要從用 WorkSpaces 戶端重新連線，使用者可以使用其密碼或智慧卡來驗證自己，具體取決於已為其啟用的驗證類型而定 WorkSpaces。

默認情況下， WorkSpaces 不支持在屏幕鎖定上斷開會話。如有需要，使用 WSP 組態檔來啟用此功能。

若要啟用或停用 Ubuntu 螢幕鎖定上的中斷連線工作階段 WorkSpaces

1. 使用以下命令在具有提升權限的編輯器中開啟 `wsp.conf` 檔案。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. 在 `[policies]` 群組的結尾新增此行：

   ```
   disconnect-on-lock = X
   ```

   其中 *X* 的可能值為：

   enabled—已啟用螢幕鎖定時中斷連線

   disabled—已停用螢幕鎖定時中斷連線 (預設值)

授予安全殼層存取權給 Ubuntu WorkSpaces 管

根據預設，只有「網域管理員」群組中指派的使用者和帳戶才能使 WorkSpaces 用 SSH 連線到 Ubuntu。要使其他用戶和帳戶 WorkSpaces 使用 SSH 連接到 Ubuntu，我們建議您在活動目錄中為您的 Ubuntu 管理員創建一個專用的 WorkSpaces 管理員組。

若要啟用 **`Linux_WorkSpaces_Admins`** Active Directory 群組成員的 sudo 存取權

1. 使用 `visudo` 來編輯 `sudoers` 檔案，如下列範例所示。

   ```
   [username@workspace-id ~]$ sudo visudo
   ```

2. 新增以下這一行。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

建立專用管理員群組後，請依照下列步驟來啟用群組成員的登入功能。

若要啟用 **Linux_WorkSpaces_Admins** Active Directory 群組成員的登入功能

1. 使用提升的權限編輯 /etc/security/access.conf。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 新增以下這一行。

```
+:(Linux_WorkSpaces_Admins):ALL
```

使用 Ubuntu 時， WorkSpaces 您不需要在為 SSH 連接指定用戶名時添加域名，默認情況下，密碼身份驗證處於禁用狀態。要通過 SSH 連接，您需要將 SSH 公鑰添加到 Ubuntu $HOME/.ssh/authorized_keys 上 WorkSpace，或編輯/etc/ssh/sshd_config以設置 PasswordAuthentication 為yes。如需有關啟用 SSH 連線的詳細資訊，請參閱啟用 Linux 的 SSH 連線 WorkSpaces。

覆蓋 Ubuntu 的默認外殼 WorkSpaces

若要覆寫 Ubuntu 的預設外殼 WorkSpaces，我們建議您編輯使用者的~/.bashrc檔案。例如，若要使用 Z shell 而不是 Bash Shell，請將下列幾行加入至 /home/username/.bashrc。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 進行此變更之後，您必須重新啟動 WorkSpace 或登出 WorkSpace (不只是中斷連線)，然後重新登入，變更才會生效。

設定裝置 Proxy 伺服器設定以存取網際網路

根據預設，用 WorkSpaces 戶端應用程式會使用 HTTPS (連接埠 443) 流量裝置作業系統設定中指定的 Proxy 伺服器。Amazon 用 WorkSpaces 戶端應用程式使用 HTTPS 連接埠進行更新、註冊和身份驗證。

> **Note**
>
> 不支援需要使用登入憑證進行驗證的 Proxy 伺服器。

您可以依照 Microsoft 說明文件中的設定裝置 Proxy 和網際網路連線設定中的步驟， WorkSpaces 透過群組原則為 Ubuntu 設定裝置代理伺服器設定。

如需有關在 WorkSpaces Windows 用戶端應用程式中設定代理伺服器的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

如需有關在 WorkSpaces macOS 用戶端應用程式中設定代理伺服器的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

如需有關在 WorkSpaces Web 存取用戶端應用程式中設定代理伺服器設定的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南中的代理伺服器。

代理桌面流量

對於 PCoIP WorkSpaces，桌面用戶端應用程式不支援使用 Proxy 伺服器，也不支援在 UDP 中使用 TLS 解密和檢查連接埠 4172 流量 (針對桌面流量)。它們需要直接連線至連接埠 4172。

對於 WSP WorkSpaces， WorkSpaces 視窗用戶端應用程式（5.1 及以上版本）和 macOS 用戶端應用程式（5.4 版及以上版本）支援使用 HTTP 代理伺服器進行連接埠 4195 TCP 流量。不支援 TLS 解密和檢查。

WSP 不支援透過 UDP 將 Proxy 用於桌面流量。只有 WorkSpaces Windows 和 macOS 桌面用戶端應用程式和 WSP 網頁存取支援使用代理伺服器，用於 TCP 流量。

> **Note**
>
> 如果您選擇使用 Proxy 伺服器，用戶端應用程式對 WorkSpaces 服務進行的 API 呼叫也會被代理。API 呼叫和桌面流量都應該通過相同的 Proxy 伺服器。

Proxy 伺服器的使用建議

我們不建議使用代理服務器與您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已經加密，因此 Proxy 無法改善安全性。Proxy 代表網路路徑中的額外躍點，可能會藉由引入延遲來影響串流品質。如果 Proxy 未適當調整大小以處理桌面串流流量，Proxy 也可能降低輸送量。此外，大多數代理不是為支持長時間運行 WebSocket （TCP）連接而設計的，可能會影響流的質量和穩定性。

如果您必須使用代理伺服器，請將 Proxy 伺服器盡可能靠近用 WorkSpace 戶端 (最好位於同一個網路中)，以避免增加網路延遲，這可能會對串流品質和回應能力造成負面影響。

優化 Amazon WorkSpaces 實現實時通信

Amazon WorkSpaces 提供了多種技術來促進 Microsoft 團隊，Zoom，Webex 等統一通信（UC）應用程序的部署。在當代應用領域中，大多數 UC 應用程序都包含各種功能，包括一對一聊天室、協作群組聊天通道、無縫檔案儲存和交換，即時活動、網路研討會、廣播、互動式畫面共用和控制、白板功能和離線音訊/視訊傳訊功能。這些功能大部分都可以無縫地 WorkSpaces 作為標準功能使用，而無需進行額外的微調或增強。但是，值得注意的是，即時通訊元素，特別是 one-on-one 呼叫和集體小組會議，代表此規則的例外狀況。在 WorkSpaces 部署過程中，成功納入此類功能通常需要專門的重點和規劃。

在 Amazon 上規劃 UC 應用程式的即時通訊功能實作時 WorkSpaces，您有三種不同的即時通訊 (RTC) 組態模式可供選擇。其選擇取決於您打算提供給使用者和您計劃使用的用戶端裝置的特定應用程式。

本文件著重於最佳化 Amazon 中最常見的 UC 應用程式的使用者體驗 WorkSpaces。如需特定於 WorkSpaces 核心的最佳化，請參閱合作夥伴特定文件。

主題

- 媒體最佳化模式概觀
- 要使用哪個 RTC 最佳化模式？

- RTC 最佳化指引

媒體最佳化模式概觀

以下是可用的媒體最佳化選項。

選項 1：媒體最佳化即時通訊 (媒體最佳化 RTC)

在此模式下，協力廠商 UC 和 VoIP 應用程式會在遠端執行 WorkSpace，而其媒體架構則卸載到支援的用戶端以進行直接通訊。下列 UC 應用程式在 Amazon 上使用此方法 WorkSpaces：

- Zoom 會議
- Cisco 會議

若要讓媒體最佳化 RTC 模式運作，UC 應用程式廠商應 WorkSpaces 使用其中一個可用的軟體開發套件 (SDK) (例如 DCV 延伸 SDK) 來開發整合。此模式需要在用戶端裝置上安裝 UC 元件。

如需設定此模式的詳細資訊，請參閱 設定媒體最佳化 RTC。

選項 2：工作階段內最佳化即時通訊 (工作階段內最佳化 RTC)

在此模式下，未變更的 UC 應用程式會在上執行 WorkSpace，透過串流通訊協定將音訊和視訊 WorkSpaces 流量引導至用戶端裝置。來自網路攝影機的麥克風和視訊串流的本機音訊會重新導向至 UC 應用程式所使用的位置。 WorkSpace此模式提供廣泛的應用程式相容性，並有效地將 UC 應用程式從遠端傳送 WorkSpace到各種用戶端平台。您不需要將 UC 應用程式元件部署到用戶端裝置。

如需設定此模式的詳細資訊，請參閱 設定工作階段內最佳化 RTC。

選項 3：直接即時通訊 (直接 RTC)

在此模式中，在中操作的應用程式會 WorkSpace 接管位於使用者桌面或用戶端作業系統上的實體或虛擬電話組的控制權。這會導致音訊流量直接從使用者工作站的實體電話或在用戶端裝置上運作的虛擬電話周遊到遠端通話對等端。在此模式下運行的應用程序值得注意的執行個體包括：

- Amazon Amazon Connect 優化 WorkSpaces
- Genesys Cloud WebRTC 媒體協助程式
- Microsoft Teams SIP 閘道

- Microsoft Teams 桌上電話和 Teams 顯示器
- 透過 UC 應用程式的撥入或「撥打我的電話」功能參與音訊會議。

如需設定此模式的詳細資訊，請參閱 設定直接 RTC。

要使用哪個 RTC 最佳化模式？

您可同時使用不同的 RTC 最佳化模式，也可設定為彼此互補作為備用。例如，考慮為 Cisco Webex 會議啟用媒體最佳化 RTC。此組態可確保使用者 WorkSpace 透過桌面用戶端存取時，體驗最佳化的通訊體驗。但是，在從缺少 UC 最佳化元件的共用網際網路資訊站存取 Webex 的情況下，Webex 將無縫轉換為工作階段內最佳化 RTC 模式來維持功能。當使用者使用多個 UC 應用程式時，RTC 設定模式可能會因其獨特的需求而有所不同。

下表說明常見的 UC 應用程式功能並定義哪種 RTC 設定模式可提供最佳結果。

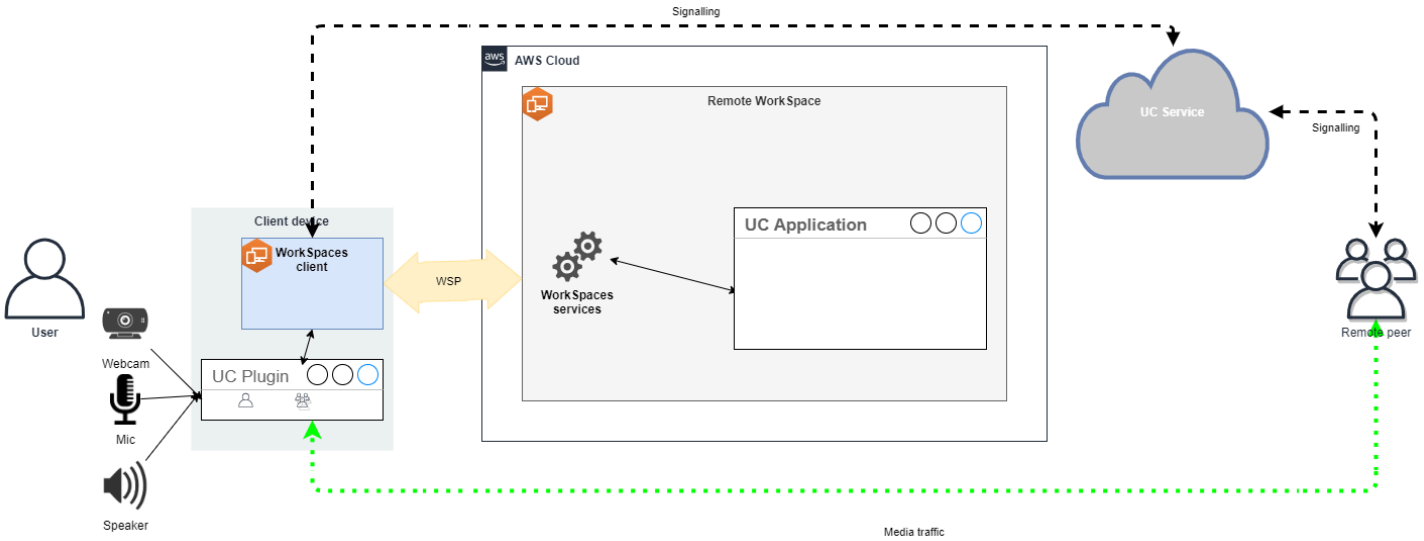
功能	直接 RTC	媒體最佳化 RTC	工作階段內 最佳化 RTC
一對一聊天	不需要 RTC 設定		
群組聊天室	不需要 RTC 設定		
群組音訊會議	最佳	最佳	好
群組視訊會議	好	最佳	好
一對一音訊通話	最佳	最佳	好
一對一視訊通話	好	最佳	好
白板功能	不需要 RTC 設定		
音訊/音訊片段/傳訊	不適用	好	最佳
檔案共用	不適用	取決於 UC 應用程式	最佳
畫面共用與控制	不適用	取決於 UC 應用程式	最佳
網路研討會/廣播活動	不適用	好	最佳

RTC 最佳化指引

設定媒體最佳化 RTC

媒體最佳化 RTC 模式可由 UC 應用程式廠商使用 Amazon 所提供的 SDK 來實現。該架構要求 UC 廠商開發 UC 特定外掛程式或延伸模組，並將其部署到用戶端。

SDK 包括公開可用的選項，例如 DCV 擴充功能 SDK 和自訂的私有版本，會在操作的 UC 應用程式模組 WorkSpace 與用戶端的外掛程式之間建立控制通道。通常，此控制通道會指示用戶端延伸模組起始或加入通話。一旦透過用戶端延伸模組建立通話，UC 外掛程式會擷取來自麥克風的音訊和來自網路攝影機的視訊，然後將其直接傳輸到 UC 雲端或通話對等端。傳入的音訊會在本機播放，而且視訊覆蓋在遠端用戶端 UI 上。控制通道負責傳達通話的狀態。



Amazon WorkSpaces 目前透過媒體優化 RTC 模式支援下列應用程式：

- 縮放會議 (適用於 PCoIP 和 WSP) WorkSpaces
- 思科會議 (WorkSpaces 僅適用於 WSP)

如果您使用的應用程式不在清單上，建議您洽詢應用程式廠商，並要求 WorkSpaces 媒體最佳化 RTC 的支援。若要加快此程序，請鼓勵他們聯絡 aws-av-offloading@amazon .com。

雖然媒體最佳化 RTC 模式可增強通話效能並將 WorkSpace資源使用率降至最低，但確實具有某些限制：

- UC 用戶端延伸模組必須安裝在用戶端裝置上。
- UC 用戶端延伸模組需要獨立管理和更新。

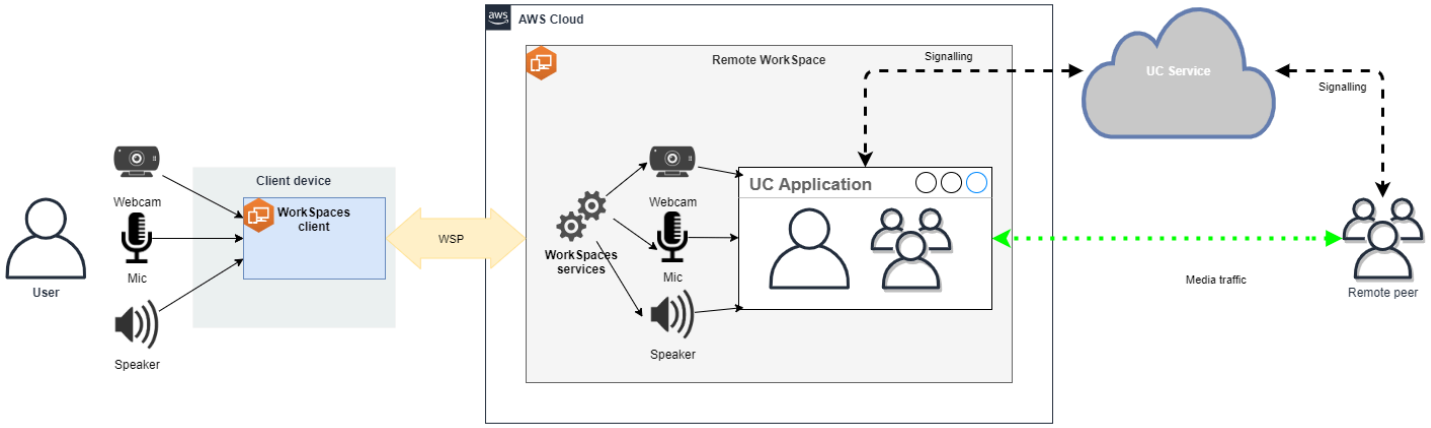
- UC 用戶端延伸模組可能無法在某些用戶端平台 (例如行動平台或 Web 用戶端) 上使用。
- 在此模式下，某些 UC 應用程式功能可能會受到限制；例如，畫面共用行為可能有所不同。
- 使用用戶端延伸模組可能不適合自攜裝置 (BYOD) 或共用資訊站等案例。

如果媒體最佳化 RTC 模式證明不適合您的環境，或是某些使用者無法安裝用戶端延伸模組，則建議將工作階段內最佳化 RTC 模式設定為備用選項。

設定工作階段內最佳化 RTC

在工作階段中最佳化 RTC 模式中，UC 應用程式在不進行任何修改的 WorkSpace情況下運作，提供類似於本機的體驗。應用程序生成的音頻和視頻流由 WorkSpaces 流協議（WSP）捕獲並傳輸到客戶端。在用戶端上，麥克風 (在 WSP 和 PCoIP 上 WorkSpaces) 和網路攝影機 (僅在 WSP 上 WorkSpaces) 訊號會擷取、重新導向回，然後順暢地傳送至 UC 應用程式。 WorkSpace

值得注意的是，此選項可確保卓越的相容性 (即使是舊版應用程式)，無論應用程式的來源為何，都能提供一致的使用者體驗。工作階段內最佳化也適用於 Web 用戶端。



WorkSpaces 串流通訊協定 (WSP) 經過精心最佳化，可增強遠端 RTC 模式的效能。最佳化措施包括：

- 利用自適應 UDP 型 QUIC 傳輸，確保高效率的資源傳輸。
- 建立低延遲音訊路徑，促進快速音訊輸入和輸出。
- 實作語音最佳化的音訊轉碼器，以保持音訊品質，同時降低 CPU 和網路使用率。
- 網路攝影機重新導向，能夠整合網路攝影機功能。
- 設定網路攝影機解析度以最佳化效能。
- 整合自適應顯示轉碼器，以平衡速度和視覺品質。
- 音訊抖動校正，保證流暢的音訊傳輸。

這些最佳化共同為遠端 RTC 模式提供穩健且流暢的體驗。

大小建議

為了有效支持遠程 RTC 模式，確保適當的 Amazon WorkSpaces 尺寸至關重要。遙控器 WorkSpace 必須符合或超過個別整合通訊 (UC) 應用程式的系統需求。下表列出用於視訊和音訊通話時，常用 UC 應用程式的最低支援與建議 WorkSpaces 組態：

			視訊通話		音訊通話		
應用程式	RTC 應用程式的 CPU 需求	RTC 應用程式的 RAM 需求	最低限度支持 WorkSpace	推薦 WorkSpace	最低限度支持 WorkSpace	推薦 WorkSpace	參考資料
Microsoft Teams	需要 2 個核心，建議使用 4 個核心	4.0 GB RAM	電源 (4 個 vCPU、16 GB 記憶體)	PowerPro (8 個 vCPU，32 GB 記憶體)	效能 (2 個 vCPU、8 GB 記憶體)	電源 (4 個 vCPU、16 GB 記憶體)	Microsoft Teams 的硬體需求
Zoom	需要 2 個核心，建議使用 4 個核心	4.0 GB RAM	電源 (4 個 vCPU、16 GB 記憶體)	PowerPro (8 個 vCPU，32 GB 記憶體)	效能 (2 個 vCPU、8 GB 記憶體)	電源 (4 個 vCPU、16 GB 記憶體)	Zoom 系統需求：Windows、macOS、Linux
Webex	需要 2 個核心	4.0 GB RAM	電源 (4 個 vCPU、16 GB 記憶體)	PowerPro (8 個 vCPU，32 GB 記憶體)	效能 (2 個 vCPU、8 GB 記憶體)	電源 (4 個 vCPU、16 GB 記憶體)	適用於 Webex 服務的系統需求

重要的是要注意，視訊會議牽涉到視訊編碼和解碼的大量資源使用。在實體機器案例中，這些任務會卸載至 GPU。在非 GPU 中 WorkSpaces，這些工作會與遠端通訊協定編碼 parallel 在 CPU 上執行。因此，對於定期進行視頻流或視頻通話的用戶，強烈建議選擇 PowerPro配置。

畫面共用也會顯著消耗資源，資源消耗會隨著更高的解析度而增加。因此，在非 GPU 上 WorkSpaces，螢幕共用通常會限制在較低的畫面播放速率。

透過 WorkSpaces 串流通訊協定 (WSP) 運用以 UDP 為基礎的 QUIC 傳輸

UDP 傳輸特別適合傳輸 RTC 應用程式。為了提高效率，確保您的網路已設為針對 WSP 使用 QUIC 傳輸。請注意，UDP 型傳輸僅適用於原生用戶端。

設定 UC 應用程式 WorkSpaces

對於增強的視頻處理功能，例如背景模糊，虛擬背景，反應或託管現場活動，選擇啟用 GPU WorkSpace 對於實現最佳性能至關重要。

大部分的 UC 應用程式都會提供停用進階視訊處理的指引，以降低非 GPU WorkSpaces 上的 CPU 使用率。

如需詳細資訊，請參閱下列資源：

- Microsoft Teams：適用於虛擬化桌面基礎架構的 Teams
- Zoom 會議：管理不相容 VDI 外掛程式的使用者體驗
- Webex：適用於虛擬桌面基礎架構 (VDI) 的 Webex 應用程式部署指南 - 管理和疑難排解適用於 VDI 的 Webex 應用程式 [Webex 應用程式]
- Google Meet:使用 VDI

啟用雙向音訊和網路攝影機重新導向

預設情況下，Amazon WorkSpaces 本質上透過視訊輸入支援音訊輸入、音訊輸出和攝影機重新導向。不過，如果因任何特定原因而停用這些功能，您可以依照所提供的指引重新啟用重新導向。如需詳細資訊，請參閱 Amazon WorkSpaces 管理指南中的啟用或停用 WSP 的視訊輸入重新導向。使用者需要在連線之後選取要在工作階段中使用的攝影機。有關更多信息，用戶應參閱 Amazon 用 WorkSpaces 戶指南中的網絡攝像頭和其他視頻設備。

限制最大網路攝影機解析度

對於使用 Power 或 PowerPro WorkSpaces 進行視頻會議的用戶，強烈建議限制重定向網絡攝像頭的最大分辨率。在的情況下 PowerPro，建議的最大解析度是寬度 640 像素乘高 480 像素。對於 Power，建議的最大解析度為 320 像素的寬度搭配 240 像素的高度。

完成下列步驟，以設定最大網路攝影機解析度。

1. 開啟 Windows 登錄編輯程式。
2. 前往以下登錄檔路徑：

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. 建立名為 `max-resolution` 的字串值並在 `(X,Y)` 格式中將其設為所需的解析度，其中 X 表示水平像素計數 (寬度)，而 Y 表示垂直像素計數 (高度)。例如，指定 `(640,480)` 表示寬度為 640 像素和高度為 480 像素的解析度。

啟用語音最佳化的音訊設定

默認情況下，設 WorkSpaces 置為從客戶端提供 7.1 高保真音頻， WorkSpaces 以確保卓越的音樂播放質量。不過，如果您的主要使用案例涉及音訊或視訊會議，則將音訊轉碼器設定檔修改為語音最佳化設定可節省 CPU 和網路資源。

完成下列步驟，將音訊設定檔設為語音最佳化。

1. 開啟 Windows 登錄編輯程式。
2. 前往以下登錄檔路徑：

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

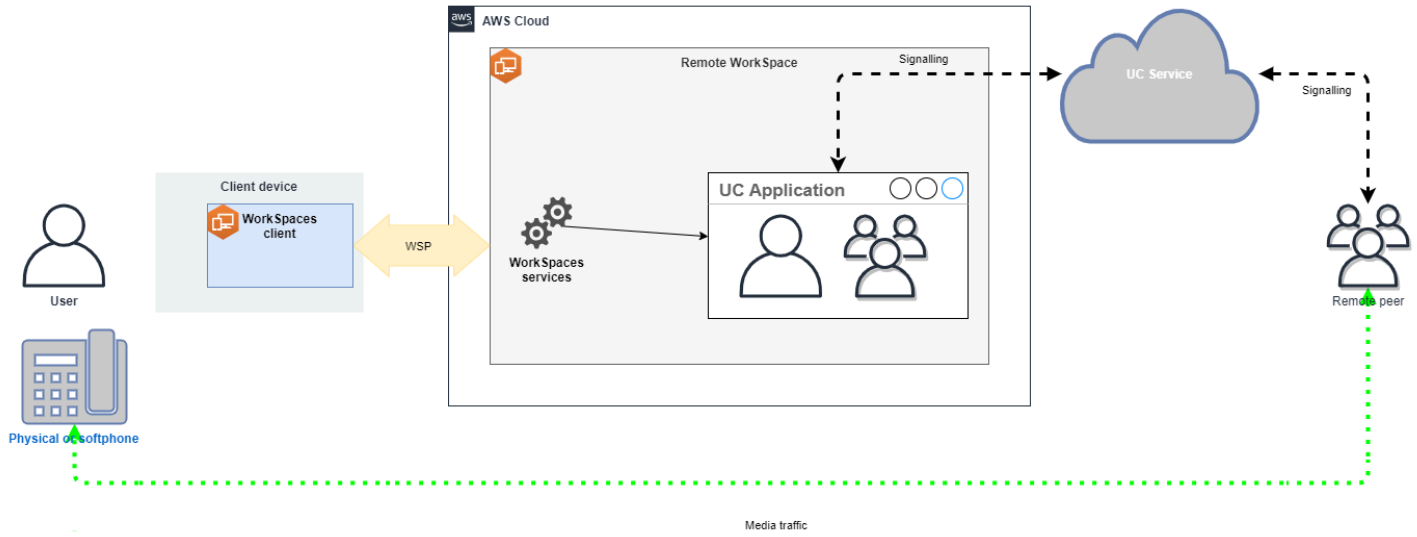
3. 建立字串值名稱 `default-profile` 並將其設定為 `voice`。

使用高品質耳機進行音訊和視訊通話

為了增強音訊體驗並防止回音，使用高品質耳機至關重要。利用桌面揚聲器可能導致通話的遠端發生回音問題。

設定直接 RTC

直接 RTC 模式的組態取決於特定的整合通訊 (UC) 應用程式，不需要在組態中進行任何變更。WorkSpaces 下列清單提供各種 UC 應用程式最佳化的非詳盡編譯。



- Microsoft Teams:
  - SIP 閘道規劃
  - 在 Microsoft 365 中進行音訊會議
  - 規劃 Teams 語音解決方案
- Zoom 會議：
  - 啟用或停用付費電話撥入號碼
  - 使用桌上電話通話控制
  - 桌上電話夥伴模式
- Webex：
  - Webex 應用程式 | 使用桌上電話撥打電話
  - Webex 應用程式 | 支援的通話選項
- BlueJeans:
  - 從桌上電話撥入會議
- Genesys：
  - Genesys Cloud WebRTC 媒體協助程式
- Amazon Connect：
  - Amazon Amazon Connect 優化 WorkSpaces
- Google Meet:
  - 在視訊會議中使用電話收發音訊

管理 WorkSpace 執行模式

WorkSpace 的執行模式會決定其立即可用性以及付費方式 (每月或每小時)。您可以在建立 WorkSpace 時選擇下列執行模式：

- AlwaysOn—在支付固定月費以便無限使用 WorkSpaces 時使用此功能。此模式最適合使用其 WorkSpace 完整時間作為其主要桌面的使用者。
- AutoStop—按小時支付 WorkSpaces 費用時使用。使用此模式時，WorkSpaces 會在指定的中斷連線期間後停止，並儲存應用程式和資料的狀態。

如需詳細資訊，請參閱 WorkSpaces 定價。

AutoStop WorkSpaces

若要設定自動停止時間，請在 Amazon WorkSpaces 主控台中選取 WorkSpace，選擇動作、修改執行模式屬性，然後設定AutoStop 時間 (小時)。依預設，AutoStop 時間 (小時) 設定為 1 小時，這表示 WorkSpace 會在中斷連線後 1 小時自動停止。

在 WorkSpace 中斷連線且 AutoStop 時間期間到期之後，WorkSpace 可能需要額外幾分鐘的時間才會自動停止。不過，一旦 AutoStop 時間期間到期，計費就會停止，且不會對您收取額外時間的費用。

如果可能，桌面的狀態會儲存至 WorkSpace 的根磁碟區。WorkSpace 會在使用者登入時繼續執行，且所有開啟的文件和執行中的程式都會回到其儲存的狀態。

AutoStop Graphics.g4dn、GraphicsPro.g4dn、Graphics 和 GraphicsPro WorkSpaces 不會保留資料的狀態和程式停止時的狀態。對於這些 Autostop WorkSpaces，我們建議您在每次使用完之後儲存您的工作。

對於自帶授權 (BYOL) AutoStop WorkSpaces，大量並行登入可能會大幅增加可取得 WorkSpaces 的時間。如果您期望許多使用者同時登入您的 BYOL AutoStop WorkSpaces，請洽詢您的客戶經理以取得建議。

> **Important**
>
> 只有在 WorkSpaces 中斷連線時，AutoStop WorkSpaces 才會自動停止。

只有在下列情況，WorkSpace 才會中斷連線：

- 如果使用者手動中斷與 WorkSpace 的連線，或結束 Amazon WorkSpaces 用戶端應用程式。
- 如果用戶端裝置已關閉。
- 如果用戶端裝置與 WorkSpace 之間沒有任何連線超過 20 分鐘。

最佳實務是，AutoStop WorkSpace 使用者應在每天使用完時手動中斷與其 WorkSpaces 的連線。若要手動中斷連線，請從適用於 Linux、macOS 或 Windows 的 WorkSpace 用戶端應用程式中的 Amazon WorkSpaces 功能表，選擇中斷 WorkSpace 的連線或結束 Amazon WorkSpaces。對於 Android 或 iPad，從側邊欄選單中選擇中斷連線。

在下列情況下，AutoStop WorkSpaces 可能不會自動停止：

- 如果用戶端裝置僅只鎖定、休眠中或非作用中 (例如，筆記型電腦上蓋已關閉) 而非關閉，WorkSpaces 應用程式可能仍在背景中執行。只要 WorkSpaces 應用程式仍在執行中，WorkSpace 可能不會中斷連線，因此 WorkSpace 可能不會自動停止。
- 只有在使用者使用 WorkSpaces 用戶端時，WorkSpaces 才能偵測中斷連線。如果使用者正在使用第三方用戶端，WorkSpaces 可能無法偵測中斷連線，因此 WorkSpaces 可能不會自動停止，且計費可能不會暫停。

修改執行模式

您可以隨時在執行模式之間切換。

若要修改 WorkSpace 的執行模式

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取要修改的 WorkSpace，然後選擇動作、修改執行模式。
4. 選取新的執行模式 (AlwaysOn 或 AutoStop)，然後選擇儲存。

若要使用 AWS CLI 修改 WorkSpace 的執行模式

使用 modify-workspace-properties 命令。

停止和啟動 AutoStop WorkSpace

當 AutoStop WorkSpaces 中斷連線時，它們會在指定的中斷連線期間之後自動停止，且暫停每小時計費。若要進一步最佳化成本，您可以手動暫停與 AutoStop WorkSpaces 相關聯的每小時費

用。WorkSpace 會停止，而所有應用程式和資料都會儲存，以供使用者下次登入 WorkSpace 時使用。

當使用者重新連線至已停止的 WorkSpace 時，它會從停止的地方繼續執行，通常在 90 秒以下。

您可以重新啟動可用或處於錯誤狀態的 AutoStop WorkSpaces。

若要停止 AutoStop WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取要停止的 WorkSpace，然後選擇動作、停止 WorkSpaces。
4. 出現確認提示時，請選擇停止 WorkSpace。

若要啟動 AutoStop WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取要啟動的 WorkSpaces，然後選擇動作、啟動 WorkSpaces。
4. 出現確認提示時，請選擇啟動 WorkSpace。

若要移除與 AutoStop WorkSpaces 相關聯的固定基礎結構成本，請從您的帳戶中移除 WorkSpace。如需詳細資訊，請參閱 刪除 WorkSpace。

若要使用 AWS CLI 來停止和啟動 AutoStop WorkSpace

使用 stop-WorkSpaces 和 start-WorkSpaces 命令。

管理應用程式

啟動之後 WorkSpace，您可以 WorkSpace 在 WorkSpaces 主控台上看到與您相關聯的所有應用程式套裝軟體的清單。

若要查看與您相關聯的所有應用程式套裝軟體的清單 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在左側導覽窗格中，選擇WorkSpaces。

3. 選取 WorkSpace 並選擇「檢視詳細資訊」。
4. 在「應用程式」下，尋找與此 WorkSpace相關聯的應用程式清單及其安裝狀態。

您可以透過下列方式更新您 WorkSpace 的應用程式套裝軟體：

- 將應用程式套件安裝在您 WorkSpace
- 解除安裝應用程式套件 WorkSpace
- 安裝應用程式套裝軟體並解除安裝不同的應用程式套裝軟體 WorkSpace

> **Note**
>
> - 若要更新應用程式套裝軟體，狀態 WorkSpace 必須為`AVAILABLE`或`STOPPED`。
> - 管理應用程式僅適用於 Windows WorkSpaces。
> - 「管理應用程式」僅適用於透過 AWS訂閱的應用程式套件。

管理應用程式支援的套件

管理應用程式可讓您在 WorkSpaces. 對於 Microsoft Office 2016 套件和 Microsoft Office 2019，您只能解除安裝。

- Microsoft Office LTSC 專業增強版 2021
- Microsoft Visio LTSC 專業版 2021
- Microsoft Project 專業版 2021
- Microsoft Office LTSC 標準版 2021
- Microsoft Visio LTSC 標準版 2021
- Microsoft Project 標準版 2021

下表顯示支援及不支援的應用程式和作業系統組合清單：

	Microsoft Office 專業增強版 2016 (32 位元)	Microsoft Office 專業增強版 2019 (64 位元)	Microsoft LTSC Office 專業增強版/標準版 2021 (64 位元)	Microsoft Project 專業版/標準版 2021 (64 位元)	Microsoft LTSC Visio 專業版/標準版 2021 (64 位元)
Windows Server 2016	解除安裝	不支援	不支援	不支援	不支援
Windows Server 2019	不支援	解除安裝	安裝/解除安裝	安裝/解除安裝	安裝/解除安裝
Windows Server 2022	不支援	解除安裝	安裝/解除安裝	安裝/解除安裝	安裝/解除安裝
Windows 10	解除安裝	解除安裝	安裝/解除安裝	安裝/解除安裝	安裝/解除安裝
Windows 11	解除安裝	解除安裝	安裝/解除安裝	安裝/解除安裝	安裝/解除安裝

Important

- 這些應用程式必須使用相同的版本。例如，您無法將標準版應用程式與專業版應用程式混合使用。
- 這些應用程式必須使用相同的版本。例如，您不能將 2019 年應用程序與 2021 版應用程序混合使用。
- Microsoft 辦公室/視覺/專案 2021 標準版/專業版不支援價值、圖形和組合包。 GraphicsPro WorkSpaces
- 當您從您的移除 Microsoft Office 2016 的 Plus 應用程式套裝軟體時 WorkSpaces，您將無法存取任何趨勢科技解決方案，這些解決方案包含在該 Amazon WorkSpaces 服務包中。如

果您想繼續在 Amazon 上使用趨勢科技解決方案 WorkSpaces，可以在AWS 市集上另行購買。

- 為了安裝/解除安裝 Microsoft 365 應用程式，您需要自備工具和安裝程式，「管理應用程式」工作流程無法安裝/解除安裝 Microsoft 365 應用程式。
- 您無法建立透過「管理應用程式」安裝之應 WorkSpaces 用程式的自訂影像，但您可以建立自訂影像，使用「管理應用程式」 WorkSpaces 從中解除安裝應用程式服務包。
- 必須啟用 DNS 解析才能使用「管理應用程式」。
- 對於選擇加入區域，例如非洲 (開普敦)，必須在目錄層級啟用 WorkSpaces 網際網路連線。

若要更新應用程式套裝軟體 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取 WorkSpace 並選擇 [動作]、[管理應用程式]。
4. 在 [目前的應用程式] 下，您會看到已安裝在此應用程式 WorkSpace 和 [選擇應用程式] 下方的應用程式套裝軟體清單，其中包含可安裝的應用程式套裝軟體清單 WorkSpace。
5. 若要在此上安裝應用程式套件 WorkSpace：
   a. 選取您要在其上安裝的應用程式套裝軟體 WorkSpace，然後選擇「關聯」。
   b. 重複前一個步驟以安裝其他應用程式套件。
   c. 安裝應用程式套件時，您會在目前的應用程式之下看到其具有 `Pending install deployment` 狀態。
6. 若要從此解除安裝應用程式套件 WorkSpace：
   a. 在選擇應用程式之下，選取要解除安裝的應用程式套件，然後選擇取消關聯。
   b. 重複前一個步驟以解除安裝其他應用程式套件。
   c. 解除安裝應用程式套件時，您會在目前的應用程式之下看到其具有 `Pending uninstall deployment` 狀態。
7. 若要回復套件安裝或安裝狀態，請執行下列其中一項操作。
   - 如果您要將套件從 `Pending uninstall deployment` 狀態回復，請選取要回復的應用程式，然後選擇關聯。

- 如果您要將套件從 Pending install deployment 狀態回復，請選取要回復的應用程式，然後選擇取消關聯。

8. 在您選擇要安裝或解除安裝的應用程式套件處於擱置狀態之後，請選擇部署應用程式。

> **Important**
>
> 選取 [部署應用程式] 之後，一般使用者工作階段將 WorkSpaces 會終止，而且在安裝或解除安裝應用程式時將無法存取。

9. 若要確認您的動作，請輸入確認。選擇強制來安裝或解除安裝處於錯誤狀態的應用程式套件。
10. 若要監控應用程式套件的進度：

    a. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/

    b. 在導覽窗格中，選擇 WorkSpaces。您可以在狀態之下看到狀態，包括下列各項。

    - 更新中 - 應用程式套件更新仍在進行中。
    - 可用/已停止-應用程式套裝軟體更新已完成， WorkSpace 且回到其原始狀態。

    c. 若要監視應用程式套裝軟體的安裝或解除安裝狀態，請選取 WorkSpace 並選擇「檢視詳細資訊」。在應用程式之下，您可以在狀態下看到狀態，包括 Pending install、Pending uninstall 和 Installed。

> **Note**
>
> 如果您的使用者發現透過受管理的應用程式新安裝的應用程式套裝軟體未啟動授權，您可以手動 WorkSpace 重新啟動。您的使用者可以在重新啟動後開始使用這些應用程序。如需其他支援，請聯絡 AWS 支援。

使用管理 WorkSpaces 應用程式來管理

在您的上安裝或解除安裝應用程式套裝軟體後 WorkSpaces，下列動作可能會影響現有的組態

- Re@@ store a WorkSpace-還原根據狀況良好時建立的這些磁碟區的最 WorkSpace 新快照會重新建立根磁碟區和使用者磁碟區。 WorkSpace 每 12 小時會 WorkSpace 拍攝一次完整快照。如需詳細資訊，請參閱還原 WorkSpace. 請務必等待至少 12 WorkSpaces 個小時，然後再使用管理應用程式還原已修改的檔案。在使用管理應用程式修改的下一個完整快照 WorkSpaces 之前還原的下一個完整快照會產生以下情況：

  - 您使用「管理應用程式」工作流程安裝的應 WorkSpaces 用程式套裝軟體將會從您的帳戶中移除， WorkSpaces 但授權仍會啟用，且您 WorkSpaces 需要支付這些應用程式的費用。若要讓這些應用程式套裝軟體重新開始， WorkSpaces 您需要再次執行管理應用程式工作流程，解除安裝應用程式以重新開始，然後重新安裝。
  - 使用「管理應用程式」工作流程從您移除的應 WorkSpaces 用程式套裝軟體將會回到您的 WorkSpaces. 但是，這些應用程式套件將無法正常運作，因為授權啟用將會遺失。若要移除這些應用程式套裝軟體，請從您的 WorkSpaces.
- 重建一個 WorkSpace-重建一個 WorkSpace 重新創建根卷。如需詳細資訊，請參閱重建 WorkSpace. 使用「管理」應用程式重建已修改的 WorkSpaces 項目將會產生以下情況：
  - 您使用「管理應用程式」工作流程安裝的應 WorkSpaces 用程式套裝軟體將會從中移除並停用 WorkSpaces。若要讓這些應用程式重新開啟， WorkSpaces 您需要再次執行「管理應用程式」工作流程。
  - WorkSpaces 透過管理應用程式工作流程從您移除的應用程式套裝軟體將會安裝並啟用於您的 WorkSpaces。若要從您的應用程式套裝軟體中移除 WorkSpaces，您需要再次執行「管理應用程式」工作流程。
- Migrate a WorkSpace-移轉程序會使用目標套裝軟體映像中的新根磁碟區和原始 WorkSpace檔案的最後一個可用快照中的使用者磁碟區來重新建立。 WorkSpace 會建立 WorkSpace 具有新 WorkSpace ID 的新 ID。如需詳細資訊，請參閱 WorkSpace移轉使用管理應用程式修改的移轉會產生以下情況： WorkSpaces
  - WorkSpaces 將移除並停用來源中的所有應用程式套裝軟體。新目的地 WorkSpaces 將繼承目標 WorkSpaces 套裝軟體的應用程式。來源 WorkSpaces 應用程式套裝軟體將按整個月計費，但目的地服務包上的應用程式套裝軟體會有按比例計費。

修改一個 WorkSpace

啟動之後 WorkSpace，您可以透過三種方式修改其組態：

- 您可以變更其根磁碟區的大小 (Windows 為磁碟機 C；Linux 為 /) 及其使用者磁碟區 (Windows 為磁碟機 D；Linux 為 /home)。
- 您可以變更其運算類型以選取新的套件。
- 如果您 WorkSpace 是使用 PCoIP 服務包建立的，您可以使用 AWS CLI 或 Amazon WorkSpaces API 修改串流通訊協定。

若要查看的目前修改狀態 WorkSpace，請選取箭頭以顯示有關該修改狀態的更多詳細資訊 WorkSpace。狀態的可能值為修改運算、修改儲存體和無。

如果要修改 WorkSpace，它的狀態必須為AVAILABLE或STOPPED。您無法同時變更磁碟區大小和運算類型。

變更磁碟區大小或計算類型 WorkSpace 將會變更的計費費率 WorkSpace。

若要允許使用者自行修改其磁碟區和運算類型，請參閱 為您的使用者啟用自助式 WorkSpace管理功能。

修改磁碟區大小

您可以增加根磁碟區和使用者磁碟區的大小 WorkSpace，每個磁碟區最多可增加 2000 GB。WorkSpace 根磁碟區和使用者磁碟區位於無法變更的設定群組中。可用的群組如下：

[根目錄 (GB)，使用者 (GB)]
[80，10]
[80，50]
[80，100]
[175 至 2000，100 至 2000]

您可以擴充根磁碟區和使用者磁碟區 (無論已加密或未加密)，並且可以在 6 小時內擴充一次這兩個磁碟區。但是，您無法同時增加根磁碟區和使用者磁碟區的大小。如需詳細資訊，請參閱增加磁碟區的限制。

> **Note**
>
> 當您擴充磁碟區時 WorkSpace，會在 Windows 或 Linux 中 WorkSpaces 自動擴充磁碟區的分割區。程序完成後，您必須重新啟 WorkSpace 動，變更才會生效。

若要確保您的資料得以保留，您無法在啟動之後減少根磁碟區或使用者磁碟區的大小 WorkSpace。相反地，請務必在啟動時指定這些磁碟區的最小大小 WorkSpace。您可以啟動「值」、「標準」、「效

能」、「電源」，或 PowerPro WorkSpace 啟動根磁碟區至少為 80 GB，使用者磁碟區啟動 10 GB。您可以啟動圖形 .g4dn、 GraphicsPro .g4dn、圖形，或者根磁碟區至少為 100 GB， GraphicsPro WorkSpace 使用者磁碟區的使用者磁碟區至少為 100 GB。

當 WorkSpace 磁碟大小增加正在進行中時，使用者可以在其上執行大多數工作 WorkSpace。但是，他們無法更改其 WorkSpace 計算類型，切換 WorkSpace 運行模式，重建它們 WorkSpace或重新啟動（重新啟動）它們的 WorkSpace。

> **Note**
>
> 如果您希望使用者能夠 WorkSpaces 在磁碟大小增加的過程中使用它們，請在調整磁碟區大小的大小之`STOPPED`前，請確定其狀態為，`AVAILABLE`而不是 WorkSpaces。 WorkSpaces 如果 WorkSpaces 是`STOPPED`，則無法在磁盤大小增加時啟動它們。

在大多數情況下，磁碟大小增加程序最多可能需要兩個小時。但是，如果您要修改大量的磁碟區大小 WorkSpaces，則處理程序可能需要更長的時間。如果您有大量的修 WorkSpaces 改，我們建議您聯繫 AWS Support尋求幫助。

增加磁碟區的限制

- 您只能調整 SSD 磁碟區的大小。
- 啟動時 WorkSpace，您必須等待 6 小時才能修改其磁碟區的大小。
- 您無法同時增加根磁碟區和使用者磁碟區的大小。若要增加根磁碟區，您必須先將使用者磁碟區變更為 100 GB。進行該變更之後，您就可以將根磁碟區更新為 175 到 2000 GB 之間的任何值。在根磁碟區變更為 175 到 2000 GB 之間的任何值之後，您就可以進一步將使用者磁碟區更新為 100 到 2000 GB 之間的任何值。

  > **Note**
  >
  > 如果要同時增加兩個磁碟區，則必須先等待 20-30 分鐘讓第一項操作完成，才能開始第二項操作。

- 除非 WorkSpace 是圖形 .g4dn、 GraphicsPro .g4dn、圖形，或者，當使用者磁碟區為 100 GB 時 GraphicsPro WorkSpace，根磁碟區不能小於 175 GB。圖形 .g4dn、 GraphicsPro .g4dn、圖形，並且 GraphicsPro WorkSpaces可以將根磁碟區和使用者磁碟區都設定為最小 100 GB。
- 如果使用者磁碟區為 50 GB，則無法將根磁碟區更新為 80 GB 以外的任何值。如果根磁碟區為 80 GB，則使用者磁碟區只能是 10、50 或 100 GB。

若要修改根磁碟區 WorkSpace

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取 WorkSpace 並選擇動作、修改根磁碟區。 。
4. 在根磁碟區大小之下，選擇磁碟區大小或選擇自訂以輸入自訂磁碟區大小。
5. 選擇儲存變更。
6. 當磁碟大小增加完成時，您必須重新啟動，變更才會生效。 WorkSpace為避免數據丟失，請確保用戶在重新啟動之前保存任何打開的文件 WorkSpace。

若要修改的使用者磁碟區 WorkSpace

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取 WorkSpace 並選擇 [動作]、[修改使用者磁碟區]。 。
4. 在使用者磁碟區大小之下，選擇磁碟區大小或選擇自訂以輸入自訂磁碟區大小。
5. 選擇儲存變更。
6. 當磁碟大小增加完成時，您必須重新啟動，變更才會生效。 WorkSpace為避免數據丟失，請確保用戶在重新啟動之前保存任何打開的文件 WorkSpace。

變更磁碟區大小的步驟 WorkSpace

將modify-workspace-properties指令與 `RootVolumeSizeGib` or `UserVolumeSizeGib` 屬性搭配使用。

修改運算類型

您可以在標準、電源、效能和 PowerPro 運算類型 WorkSpace 之間切換。如需這些運算類型的詳細資訊，請參閱 Amazon WorkSpaces 套裝軟體。

> **Note**
>
> - 您可以將計算類型從圖形 .g4dn 更改為 .g4dn，或從 .g4dn 更改為圖形 GraphicsPro .g4dn。GraphicsPro您無法將圖形 GraphicsPro .g4dn 和 .g4dn 的計算類型變更為任何其他值。

- 在 2023 年 11 月 30 日之後，不再支援 Graphics 套件。我們建議您移轉 WorkSpaces 至圖形 .g4dn 套裝軟體。如需詳細資訊，請參閱 遷移 WorkSpace。
- 您無法變更圖形的運算類型和任 GraphicsPro 何其他值。

當您要求計算變更時，請 WorkSpace 使用新的運算類型 WorkSpaces 重新啟動。 WorkSpaces 會保留的作業系統、應用程式、資料和儲存設定 WorkSpace。

您可以在 6 小時內請求一次較大的運算類型，或是每 30 天請求一次較小的運算類型。對於新啟動的 WorkSpace，您必須等待 6 小時才能要求較大的運算類型。

當 WorkSpace 運算類型變更進行中時，使用者會與其中斷連線 WorkSpace，而且他們無法使用或變更 WorkSpace. 會在 WorkSpace 計算類型變更程序期間自動重新啟動。

Important

若要避免資料遺失，請確定使用者在變更 WorkSpace 運算類型之前，先儲存任何開啟的文件和其他應用程式檔案。

運算類型變更程序最多可能需要一小時。

若要變更的運算類型 WorkSpace

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取 WorkSpace 並選擇動作、修改運算類型。
4. 在運算類型之下，選擇運算類型。
5. 選擇儲存變更。

若要變更的運算類型 WorkSpace

使用指modify-workspace-properties令搭配`ComputeTypeName`屬性。

修改通訊協定

如果您 WorkSpace 是使用 PCoIP 服務包建立的，您可以使用 AWS CLI 或 Amazon WorkSpaces API 修改其串流通訊協定。這可讓您在不使用移轉功能的 WorkSpace 情況下使用現有通訊協定來

WorkSpace 移轉通訊協定。這也可讓您使用 WorkSpaces 串流通訊協定 (WSP) 並維護根磁碟區，而無需在移轉 WorkSpaces 過程中重新建立現有的 PCoIP。

- 只有在您使用 PCoIP 套裝軟體建立的通訊協定 WorkSpace 時，才能修改您的通訊協定。
- 將通訊協定修改為 WSP 之前，請確定您 WorkSpace 符合 W WorkSpace SP 的下列需求。
  - 您的 WorkSpaces 客戶端支援 WSP
  - 您的部署地 WorkSpace 區支援 WSP
  - WSP 的 IP 位址和連接埠需求已開啟。如需詳細資訊，請參閱的 IP 位址和連接埠需求 WorkSpaces。
  - 確保您目前的套件可與 WSP 一起使用。
  - 為了獲得最佳的視訊會議體驗，我們建議您僅使用 Power 或 PowerPro 套裝軟體。

> **Note**
>
> - 我們強烈建議您在開始變更通訊協定 WorkSpaces 之前，先對非生產環境進行測試。
> - 如果您將通訊協定從 PCoIP 修改為 WSP，然後將通訊協定修改回 PCoIP，您將無法透過網頁存取連線到。 WorkSpaces

若要變更的通訊協定 WorkSpace

1. [選擇性] 重新啟動 WorkSpace 並等待它進入AVAILABLE狀態，然後再修改通訊協定。
2. [選擇性] 使用describe-workspaces指令列出 WorkSpace 屬性。確保其處於 AVAILABLE 狀態而且其目前 Protocol 是準確的。
3. 使用 modify-workspace-properties 命令並將 Protocols 屬性從 PCOIP 修改為 WSP，或以其他方式修改。

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> Protocols 屬性區分大小寫。確定您使用 PCOIP 或 WSP。

4. 執行命令之後，最多可能需要 20 分鐘才能重新 WorkSpace 開機並完成必要的設定。
5. 再次使用`describe-workspaces`命令列出 WorkSpace屬性，並確認它處於`AVAILABLE`狀態，並且目前的`Protocols`屬性已變更為正確的通訊協定。

> **Note**
>
> - 修改 WorkSpace的通訊協定不會更新主控台中的套裝軟體說明。啟動套件描述不會變更。
> - 如果 20 分鐘後 WorkSpace 仍處於`UNHEALTHY`狀態，請在主控台 WorkSpace 中重新啟動。

6. 您現在可以連接到 WorkSpace.

自訂 WorkSpace 品牌

Amazon WorkSpaces 可讓您使用 API 使用自己的品牌標誌、IT 支援資訊、忘記密碼連結和登入訊息自訂登入頁面的外觀，為使用者建立熟悉的 WorkSpaces 體驗。 WorkSpace您的品牌會在使用者的 WorkSpace 登入頁面中顯示，而非預設 WorkSpaces 品牌。

支援的用戶端如下：

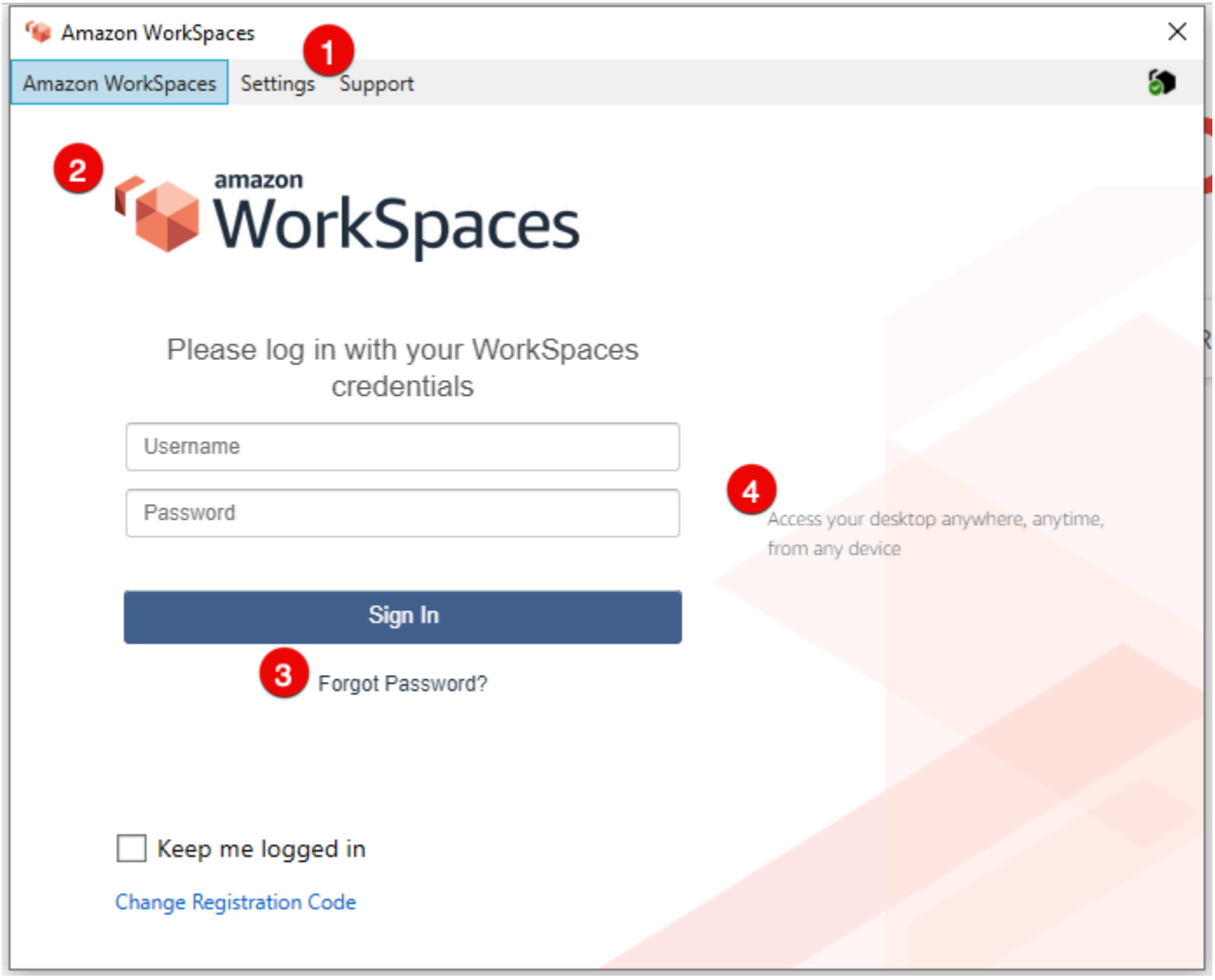
- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

> **Note**
>
> 若要使用中的 ClientBranding API 修改品牌元素AWS GovCloud (US) Region，請使用 5.10.0 的用 WorkSpaces 戶端版本。

匯入自訂品牌

若要匯入您的用戶端品牌自訂，請使用動作 `ImportClientBranding`，其中包含下列元素。如需詳細資訊，請參閱 ImportClientBranding API 參考。

> **Important**
>
> 用戶端品牌屬性為公眾面向。確保您不包含敏感資訊。



1. 支援連結
2. 標誌

3. 忘記密碼連結

4. 登入訊息

自訂品牌元素

品牌元素	描述	要求和建議
支援連結	可讓您指定支援電子郵件連結，供使用者聯絡以尋求協助 WorkSpaces。您可以使用 `SupportEmail` 屬性，或使用 `SupportLink` 屬性提供支援頁面的連結。	• 對於每個平台類型，`SupportEmail` 和 `SupportLink` 參數都是互斥的。您可以為每個平台類型指定單一參數，但不能同時指定兩者。 • 預設電子郵件為 `workspaces-feedback@amazon.com` 。 • 長度限制：長度下限為 1。長度上限為 200。

標誌	可讓您使用 Logo 屬性來自訂貴組織的標誌。	• 唯一接受的影像格式是從 `.png` 檔案轉換而來的二進位資料物件。
		• 建議的解析度：
		  • Android：978 x 190
		  • 桌上型電腦：319 x 55
		  • iOS@2x：110 x 200
		  • iOS@3x：1650 x 300

忘記密碼連結	可讓您使用 ForgotPasswordLink 屬性來新增網址，如果使用者忘記密碼，就可以前往該屬性 WorkSpace。	長度限制：長度下限為 1。長度上限為 200。
登入訊息	可讓您使用登入畫面上的 `LoginMessage` 屬性來自訂訊息。	• 長度限制：長度下限為 0。與 HTML 標籤和不同字型大小整合的長度上限為 2000

品牌元素	描述	要求和建議
		個字元。對於沒有 HTML 標籤的預設情況，建議將登入訊息保持在 600 個字元以下。 • 支援的 HTML 標籤：a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul

以下是使用的範例程式碼片段 ImportClientBranding。

AWS CLI 第 2 版

> **Warning**
>
> 匯入自訂商標會覆寫該平台內您使用自訂資料指定的屬性。也會覆寫您未使用預設自訂品牌屬性值指定的屬性。您必須包含您不想覆寫之任何屬性的資料。

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

匯入 JSON 檔案看起來應該如下列範例程式碼所示：

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
```

```
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

下列範例 Java 程式碼片段會將標誌影像轉換為 base64 編碼字串：

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

下列範例 Python 程式碼片段會將標誌影像轉換為 base64 編碼的字串：

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> 匯入自訂商標會覆寫該平台內您使用自訂資料指定的屬性。也會覆寫您未使用預設自訂品牌屬性值指定的屬性。您必須包含您不想覆寫之任何屬性的資料。

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));
```

```
// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> 匯入自訂商標會覆寫該平台內您使用自訂資料指定的屬性。也會覆寫您未使用預設自訂品牌屬性值指定的屬性。您必須包含您不想覆寫之任何屬性的資料。

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')
```

```
# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

若要預覽登入頁面，請啟動 WorkSpaces 應用程式或網頁登入頁面。

> **Note**
>
> 變更可能需要多達 1 分鐘的時間才會出現。

描述自訂品牌

若要查看您目前擁有之用戶端品牌自訂的詳細資料，請使用動作 `DescribeCustomBranding`。以下是使用的範例指令碼 DescribeClientBranding。如需詳細資訊，請參閱 DescribeClientBranding API 參考。

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

刪除自訂品牌

若要刪除您的用戶端品牌自訂，請使用動作 `DeleteCustomBranding`。以下是使用的範例指令碼 DeleteClientBranding。如需詳細資訊，請參閱 DeleteClientBranding API 參考。

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> 變更可能需要多達 1 分鐘的時間才會出現。

標記 WorkSpaces 資源

您可以透過標籤形式將自己的中繼資料指派給每個資源，以組織和管理 WorkSpaces 的資源。您可以指定每一個標籤的金鑰和值。索引鍵可以是一般類別，例如「專案」、「擁有者」或「環境」，與特定相關的值。標籤是個簡單的工具，但功能強大，可管理 AWS 資源並整理資料，包括帳單資料。

當您將標籤新增至現有資源時，這些標籤不會出現在成本配置報告中，直到下個月的第一天為止。例如，如果您在 7 月 15 日將標籤新增至現有 WorkSpace，則這些標籤會在 8 月 1 日之前出現在成本配置報告中。如需詳細資訊，請參閱 AWS Billing 使用者指南中的使用成本分配標籤。

> **Note**
>
> 若要在 Cost Explorer 中檢視 WorkSpaces 資源標籤，您必須遵循《AWS Billing 使用者指南》中啟用使用者定義的成本配置標籤中的指示，啟用您已套用至 WorkSpaces 資源的標籤。

雖然標籤會在啟用後 24 小時出現，但與這些標籤相關聯的值可能需要 4 到 5 天才會顯示在 Cost Explorer 中。此外，若要在 Cost Explorer 中顯示並提供成本資料，已標記的 WorkSpaces 資源必須在該期間產生費用。Cost Explorer 只會顯示標籤啟用時和之後的成本資料。目前沒有可用的歷史資料。

您可以標記的資源

- 建立下列資源時，您可以對其新增標籤：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、註冊的目錄、自訂套件、映像和 IP 存取控制群組。

標籤限制

- 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。
- 標籤名稱或值不可使用 `aws:` 或 `aws:workspaces:` 字首，因為其保留給 AWS 使用。您不可編輯或刪除具有這些字首的標籤名稱或值。

使用主控台來更新現有資源的標籤 (目錄、WorkSpaces 或 IP 存取控制群組)

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在瀏覽窗格中，選擇下列其中一種資源類型：目錄、WorkSpaces 或 IP 存取控制。
3. 選取資源以開啟其詳細資訊頁面。
4. 執行下列其中一項或多項：
   - 若要更新標籤，請編輯 Key (索引鍵) 和 Value (值) 的值。
   - 若要新增標籤，請選擇新增標籤，然後編輯索引鍵和值的值。
   - 若要刪除標籤，請選擇標籤旁的刪除圖示 (X)。
5. 完成標籤更新時，請選擇儲存。

使用主控台來更新現有資源的標籤 (映像或套件)

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇下列其中一種資源類型：套件或映像。
3. 選擇資源以開啟其詳細資訊頁面。
4. 在 Tags (標籤) 下，選擇 Manage tags (管理標籤)。
5. 執行下列其中一項或多項：
   - 若要更新標籤，請編輯 Key (索引鍵) 和 Value (值) 的值。
   - 若要新增標籤，請選擇新增標籤，然後編輯索引鍵和值的值。
   - 若要刪除標籤，請選擇標籤旁的移除。
6. 完成標籤更新後，請選擇儲存變更。

使用 AWS CLI 來更新現有資源的標籤

使用 create-tags 和 delete-tags 命令。

WorkSpace 維護

建議您定期維護 WorkSpaces。WorkSpaces 會為您的 WorkSpaces 安排預設維護時段。在維護期間，WorkSpace 會安裝來自 Amazon WorkSpaces 的重要更新，並視需要重新啟動。如果可用，也會從 WorkSpace 設定要使用的作業系統更新伺服器安裝作業系統更新。在維護期間，您的 WorkSpaces 可能無法使用。

根據預設，Windows WorkSpaces 會設定為接收來自 Windows Update 的更新。若要設定您自己的 Windows 自動更新機制，請參閱 Windows Server Update Services (WSUS) 和 Configuration Manager 文件。

需求

WorkSpaces 必須能夠存取網際網路，才能將更新安裝到作業系統及部署應用程式。如需詳細資訊，請參閱 the section called “網際網路存取”。

AlwaysOn WorkSpaces 的維護時段

對於 AlwaysOn WorkSpaces，維護時段由作業系統設定決定。預設值為每個星期日早上 00 點到 04 點 (WorkSpace 時區) 之間的四小時期間。根據預設，AlwaysOn WorkSpace 的時區是 WorkSpace

的 AWS 區域時區。不過，如果您從另一個區域連線並已啟用時區重新導向，然後您中斷連線，則 WorkSpace 的時區會更新為您所連線來源區域的時區。

您可使用群組政策來停用 Windows WorkSpaces 的時區重新導向。您可使用 PCoIP 代理程式組態來停用 Linux WorkSpaces 的時區重新導向。

對於 Windows WorkSpaces，您可使用群組政策設定來設定維護時段；請參閱設定自動更新的群組政策設定。您無法設定 Linux WorkSpaces 的維護時段。

AutoStop WorkSpaces 的維護時段

AutoStop WorkSpaces 會每月自動啟動一次，以便安裝重要更新。從當月的第三個星期一開始 (最多兩週)，維護時段是在 WorkSpace 的 AWS 區域時區中，每天約從 00 點開始到 05 點。WorkSpace 可以在維護時段中的任何一天進行維護。在此時段內，只會維護超過 7 天的 WorkSpaces。

在 WorkSpace 進行維護的期間內，WorkSpace 的狀態會設定為 `MAINTENANCE`。

雖然您無法修改用於維護 AutoStop WorkSpaces 的時區，但您可以依照下列方式停用 AutoStop WorkSpaces 的維護時段。如果停用維護模式，WorkSpaces 不會重新啟動，也不會進入 `MAINTENANCE` 狀態。

停用維護模式

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 Directories (目錄)。
3. 選取您的目錄，然後依序選擇動作、更新詳細資訊。
4. 展開維護模式。
5. 若要啟用自動更新，請選擇啟用。如果您想手動管理更新，請選擇停用。
6. 選擇更新並結束。

手動維護

如果您想要的話，可以按照自己的排程維護 WorkSpaces。當您執行維護任務時，建議您將 WorkSpace 的狀態變更為維護。完成時，將 WorkSpace 的狀態變更為可用。

當 WorkSpace 處於維護狀態時，會發生下列行為：

- WorkSpace 不會回應重新啟動、停止、啟動或重新建置的請求。
- 使用者無法登入 WorkSpace。

- AutoStop WorkSpace 未進入休眠狀態。

使用主控台變更 WorkSpace 的狀態

> **Note**
>
> 若要變更 WorkSpace 的狀態，WorkSpace 必須處於可用狀態。當 WorkSpace 不在可用狀態時，無法使用修改狀態設定。

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取您的 WorkSpace，然後選擇動作、修改狀態。
4. 在修改狀態之下，選擇可用或維護。
5. 選擇 Save (儲存)。

使用 AWS CLI 變更 WorkSpace 的狀態

使用 modify-workspace-state 命令。

加密 WorkSpaces

WorkSpaces 與 AWS Key Management Service （AWS KMS）集成。這可讓您 WorkSpaces 使用 AWS KMS Key 加密的儲存磁碟區。當您啟動時 WorkSpace，您可以加密根磁碟區（適用於 Microsoft 視窗，C 磁碟機；對於 Linux，/）和使用者磁碟區（適用於視窗，D 磁碟機；對於 Linux，/home）。這麼做可確保靜態儲存的資料、磁碟區的磁碟 I/O，以及從磁碟區建立的快照全都加密。

> **Note**
>
> 除了對您的進行加密之外 WorkSpaces，您還可以在某些 AWS 美國地區使用 FIPS 端點加密。如需詳細資訊，請參閱 針對 FedRAMP 授權或 DoD SRG 合規設定 Amazon WorkSpaces。

目錄

- 限制
- 使用的 WorkSpaces 加密概述 AWS KMS
- WorkSpaces 加密上下文
- WorkSpaces 授與代表您使用 KMS 金鑰的權限
- 加密一個 WorkSpace
- 檢視已加密 WorkSpaces

必要條件

在開始加密過程之前，您需要一個密 AWS KMS 鑰。此 KMS 金鑰可以是 Amazon 的AWS 受管 KMS 金鑰 WorkSpaces (aw/ 工作區)，也可以是對稱的客戶受管 KMS 金鑰。

- AWS 受管 KMS 金鑰 — 當您第一次 WorkSpace 從區域中的 WorkSpaces 主控台啟動未加密的金鑰時，Amazon WorkSpaces 會在您的帳戶中自動建立 AWS 受管 KMS 金鑰 (aw/ 工作區)。您可以選取此 AWS 受管 KMS 金鑰來加密您的使用者和根磁碟區 WorkSpace。如需詳細資訊，請參閱 使用的 WorkSpaces 加密概述 AWS KMS。

  您可以檢視此 AWS 受管理的 KMS 金鑰 (包括其原則和授權)，並可追蹤其在 AWS CloudTrail 記錄中的使用情況，但無法使用或管理此 KMS 金鑰。Amazon WorkSpaces 創建和管理這個 KMS 密鑰。只有 Amazon WorkSpaces 可以使用此 KMS 金鑰，而且只 WorkSpaces 能用來加密您帳戶中的 WorkSpaces 資源。

  AWS 受管 KMS 金鑰 (包括 Amazon WorkSpaces 支援的金鑰) 每三年輪換一次。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南中的旋轉 AWS KMS 金鑰。
- 客戶受管 KMS 金鑰 — 或者，您也可以選取您使用 AWS KMS建立的對稱客戶受管 KMS 金鑰。您可以檢視、使用和管理此 KMS 金鑰，包括設定其政策。如需有關建立 KMS 金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的建立金鑰。如需使用 AWS KMS API 建立 KMS 金鑰的詳細資訊，請參閱開AWS Key Management Service 發人員指南中的使用金鑰。

  除非您決定啟用自動金鑰輪換，否則不會自動輪換客戶受管 KMS 金鑰。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南中的旋轉 AWS KMS 按鍵。

> **Important**
>
> 手動輪換 KMS 金鑰時，您必須同時保持啟用原始 KMS 金鑰和新 KMS 金鑰，才 AWS KMS 能將 WorkSpaces 原始 KMS 金鑰加密的解密。如果您不想讓原始 KMS 金鑰保持啟用狀態，則必須使用新的 KMS 金鑰重新建立 WorkSpaces並加密它們。

您必須符合以下要求才能使用 AWS KMS 金鑰來加密您的 WorkSpaces：

- KMS 金鑰必須為對稱金鑰。Amazon WorkSpaces 不支持非對稱的 KMS 密鑰。如需區分對稱與非對稱 KMS 金鑰的相關資訊，請參閱《AWS Key Management Service 開發人員指南》中的識別對稱與非對稱 KMS 金鑰。
- 必須啟用 KMS 金鑰。若要判斷 KMS 金鑰是否已啟用，請參閱《AWS Key Management Service 開發人員指南》中的顯示 KMS 金鑰詳細資訊。
- 您必須擁有與 KMS 金鑰相關聯的正確許可和政策。如需詳細資訊，請參閱 第 2 部分：使用 IAM 政策授予 WorkSpaces 管理員其他許可。

限制

- 您無法加密現有的 WorkSpace. 您必須在啟動 WorkSpace 時加密它。
- 不支援從加密 WorkSpace 建立自訂映像檔。
- 目前不支援停用加密 WorkSpace 的加密功能。
- WorkSpaces 在啟用根磁碟區加密的情況下啟動可能需要長達一小時的時間來佈建。
- 若要重新開機或重建加密 WorkSpace，請先確定 AWS KMS 金鑰已啟用；否則，將 WorkSpace 無法使用。若要判斷 KMS 金鑰是否已啟用，請參閱《AWS Key Management Service 開發人員指南》中的顯示 KMS 金鑰詳細資訊。

使用的 WorkSpaces 加密概述 AWS KMS

使 WorkSpaces 用加密磁碟區建立時，請 WorkSpaces 使用 Amazon Elastic Block Store (Amazon EBS) 來建立和管理這些磁碟區。Amazon EBS 會使用業界標準的 AES-256 演算法資料金鑰加密您的磁碟區。Amazon EBS 和 Amazon 都 WorkSpaces 使用您的 KMS 金鑰來處理加密的磁碟區。如需有關 EBS 磁碟區加密的詳細資訊，請參閱 Amazon EC2 使用者指南中的亞馬遜 EBS 加密。

當您 WorkSpaces 使用加密磁碟區啟動時， end-to-end 程序的運作方式如下：

1. 您可以指定用於加密的 KMS 金鑰，以及的使用者和目錄 WorkSpace。此動作會建立僅允許針對此使 WorkSpaces 用 KMS 金鑰的授權，也就是 WorkSpace說，僅適用於與指定的使用者和目錄 WorkSpace相關聯的 KMS 金鑰。
2. WorkSpaces 會建立加密的 EBS 磁碟區， WorkSpace 並指定要使用的 KMS 金鑰以及磁碟區的使用者和目錄。此動作會建立授權，讓 Amazon EBS 僅針對此 WorkSpace 和磁碟區使用您的 KMS 金鑰 — 也就是說，僅針對與指定的使用者和目錄 WorkSpace 相關聯的使用者和目錄，而且僅針對指定的磁碟區使用您的 KMS 金鑰。
3. Amazon EBS 請求根據您的 KMS 金鑰加密的磁碟區資料金鑰，並指定 WorkSpace 使用者的作用中目錄安全識別碼 (SID) 和 AWS Directory Service 目錄識別碼，以及 Amazon EBS 磁碟區識別碼做為加密內容。
4. AWS KMS 建立新的資料金鑰，在您的 KMS 金鑰下加密該金鑰，然後將加密的資料金鑰傳送到 Amazon EBS。
5. WorkSpaces 使用 Amazon EBS 將加密磁碟區附加到您的 WorkSpace. Amazon EBS 會將加密的資料金鑰 AWS KMS 與`Decrypt`請求一起傳送給，並指定使用 WorkSpace 者的 SID、目錄 ID 和磁碟區 ID (用作加密內容)。
6. AWS KMS 使用您的 KMS 金鑰解密資料金鑰，然後將純文字資料金鑰傳送至 Amazon EBS。
7. Amazon EBS 使用純文字資料金鑰來加密進出已加密磁碟區的所有資料。Amazon EBS 會將純文字資料金鑰保留在記憶體中，只要磁碟區已連接到 WorkSpace.
8. Amazon EBS 會將加密的資料金鑰 (接收於Step 4) 與磁碟區中繼資料一起儲存，以備 future 在重新啟動或重建時使用。 WorkSpace
9. 當您使用移 AWS Management Console 除 WorkSpace (或使用 WorkSpaces API 中的`TerminateWorkspaces`動作) 時， WorkSpaces Amazon EBS 會淘汰允許他們為此使用您的 KMS 金鑰的授權。 WorkSpace

WorkSpaces 加密上下文

WorkSpaces 不會直接將 KMS 金鑰用於密碼編譯作業 (例如`EncryptDecrypt`、等) `GenerateDataKey`，這表示 WorkSpaces 不會將要求傳送至包 AWS KMS 含加密內容的要求。但是，當 Amazon EBS 為 WorkSpaces (Step 3在中使用的 WorkSpaces 加密概述 AWS KMS) 的加密磁碟區請求加密的資料金鑰時，當它要求該資料金鑰的純文字複本 (Step 5) 時，它會在請求中包含加密內容。

加密內容提供額外的驗證資料 (AAD)，可 AWS KMS 用來確保資料完整性。加密內容也會寫入您的 AWS CloudTrail 記錄檔，以協助您瞭解使用指定 KMS 金鑰的原因。Amazon EBS 將以下項目用於加密內容：

- 與 WorkSpace
- AWS Directory Service 與 WorkSpace
- 已加密磁碟區的 Amazon EBS 磁碟區 ID

以下範例顯示 Amazon EBS 所用加密內容的 JSON 顯示方式：

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

WorkSpaces 授與代表您使用 KMS 金鑰的權限

您可以使用 AWS 受管理的 KMS 金鑰 WorkSpaces (aw/ 工作區) 或客戶管理的 KMS 金鑰來保護您的 WorkSpace 資料。如果您使用客戶管理的 KMS 金鑰，則需要授與 WorkSpaces 權限，才能代表帳戶中的管理 WorkSpaces 員使用 KMS 金鑰。根據預設，的 AWS 受管理 KMS 金鑰 WorkSpaces具有必要的權限。

若要準備客戶受管 KMS 金鑰以供搭配使用 WorkSpaces，請遵循下列程序。

1. 將您的 WorkSpaces 管理員新增至 KMS 金鑰金鑰原則中的金鑰使用者清單
2. 使用 IAM 政策為您的 WorkSpaces 管理員提供其他許可

您的 WorkSpaces 管理員也需要使用權限 WorkSpaces。如需這些許可的詳細資訊，請前往 適用於 WorkSpaces 的身分和存取管理。

第 1 部分：將 WorkSpaces 管理員新增為金鑰使用者

若要提供 WorkSpaces 管理員所需的權限，您可以使用 AWS Management Console 或 AWS KMS API。

將 WorkSpaces 管理員新增為 KMS 金鑰 (主控台) 的金鑰使用者

1. 登入 AWS Management Console 並開啟 AWS Key Management Service (AWS KMS) 主控台，網址為 https://console.aws.amazon.com/kms。
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 Customer managed keys (客戶受管金鑰)。

4. 選擇您偏好的客戶受管 KMS 金鑰的金鑰 ID 或別名。
5. 選擇 Key policy (金鑰政策) 標籤。在 Key users (金鑰使用者) 中，選擇 Add (新增)。
6. 在 IAM 使用者和角色清單中，選取對應至 WorkSpaces 管理員的使用者和角色，然後選擇 [新增]。

將 WorkSpaces 管理員新增為 KMS 金鑰 (API) 的金鑰使用者

1. 使用 [GetKey原則] 作業取得現有的金鑰原則，然後將原則文件儲存至檔案。
2. 在您偏好的文字編輯器中開啟政策文件。將與您的 WorkSpaces 管理員對應的 IAM 使用者和角色新增至授予關鍵使用者權限的政策陳述式。接著儲存檔案。
3. 使用PutKey原則作業將金鑰原則套用至 KMS 金鑰。

第 2 部分：使用 IAM 政策授予 WorkSpaces 管理員其他許可

如果您選取用於加密的客戶受管 KMS 金鑰，則必須建立 IAM 政策， WorkSpaces 以允許 Amazon 代表您帳戶中啟動加密的 IAM 使用者使用 KMS 金鑰 WorkSpaces。該用戶還需要使用 Amazon 的許可 WorkSpaces。如需建立和編輯 IAM 使用者政策的詳細資訊，請參閱《IAM 使用者指南》中的受管 IAM 政策和適用於 WorkSpaces 的身分和存取管理。

WorkSpaces 加密需要有限的 KMS 金鑰存取權。下列是您可以使用的範例金鑰政策。此政策會將可管理 AWS KMS 金鑰的主體與可使用該金鑰的主體分開。在您使用本範例金鑰政策之前，請將範例帳戶 ID 和 IAM 使用者名稱取代為您帳戶的實際值。

第一個陳述式符合預設 AWS KMS 金鑰原則。它提供您的帳戶使用 IAM 政策來控制 KMS 金鑰存取的許可。第二個和第三個陳述式會分別定義哪些 AWS 主參與者可以管理和使用索引鍵。第四個陳述式可讓與整合 AWS KMS 的 AWS 服務代表指定的主體使用金鑰。此陳述式使 AWS 服務能夠建立和管理授與。陳述式會使用條件元素，將 KMS 金鑰授與限制為 AWS 服務代表您帳戶中的使用者所做的授與。

> **Note**
>
> 如果您的 WorkSpaces 管理員使 WorkSpaces 用建立加密磁碟區，管理員需要列出別名和金鑰 (`"kms:ListAliases"`和`"kms:ListKeys"`權限) 的權限。 AWS Management Console 如果您的 WorkSpaces 管理員僅使用 Amazon WorkSpaces API (而非主控台)，則可以省略`"kms:ListAliases"`和`"kms:ListKeys"`許可。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
```

```
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

正在加密的使用者或角色的 IAM 政策 WorkSpace 必須包含客戶受管 KMS 金鑰的使用許可，以及對的存取 WorkSpaces。若要授與 IAM 使用者或角色 WorkSpaces 許可，您可以將下列範例政策附加至 IAM 使用者或角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

使用者需要下列 IAM 政策才能使用 AWS KMS。其將對 KMS 金鑰的唯讀存取權以及建立授與的能力提供給使用者。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

如果您想要在政策中指定 KMS 金鑰，請使用類似以下的 IAM 政策。以有效的 KMS 金鑰 ARN 取代範例 KMS 金鑰 ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

加密一個 WorkSpace

若要加密 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 選擇啟動 WorkSpaces並完成前三個步驟。
3. 對於「WorkSpaces 組態」步驟，請執行下列操作：

    a. 選取要加密的磁碟區：根磁碟區、使用者磁碟區或兩個磁碟區。

b. 對於加密金鑰，請選取金 AWS KMS 鑰 (Amazon 建立的 AWS 受管 KMS 金鑰 WorkSpaces 或您建立的 KMS 金鑰)。您選取的 KMS 金鑰必須是對稱金鑰。Amazon WorkSpaces 不支持非對稱的 KMS 密鑰。

c. 選擇 Next Step (後續步驟)。

4. 選擇 [啟動] WorkSpaces。

檢視已加密 WorkSpaces

若要查看已從 WorkSpaces 主控台加密的磁碟區 WorkSpaces 和磁碟區，請WorkSpaces從左側的導覽列中選擇。[磁碟區加密] 欄會顯示每個加密是否 WorkSpace 已啟用或停用。若要查看已加密的特定磁碟區，請展開 WorkSpace 項目以查看 [加密磁碟區] 欄位。

重新啟動 a WorkSpace

有時，您可能需要手動重新啟動（ 重新啟 WorkSpace 動 ）a。重新啟動會中 WorkSpace 斷使用者的連線，然後執行關閉和重新啟動 WorkSpace. 若要避免資料遺失，請確定使用者在重新開機之前儲存任何開啟的文件和其他應用程式檔案 WorkSpace。使用者資料、作業系統和系統設定均不受影響。

> **Warning**
>
> 若要重新啟動加密 WorkSpace，請先確定AWS KMS金鑰已啟用；否則，將 WorkSpace 無法使用。若要判斷 KMS 金鑰是否已啟用，請參閱《AWS Key Management Service 開發人員指南》中的顯示 KMS 金鑰詳細資訊。

若要重新啟動 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選擇重新啟 WorkSpaces 動，然後選擇操作，重新啟動 WorkSpaces。
4. 出現確認提示時，請選擇「重新開機 WorkSpaces」

要 WorkSpace 使用重新啟動 AWS CLI

使用 reboot-workspaces 命令。

批量重新啟動 WorkSpaces

使用 amazon-workspaces-admin-module.

重建 WorkSpace

重建 WorkSpace 會重新建立從中啟動的套裝軟體之最新映像的根磁碟區、其使用者磁碟區及其主要 elastic network interface。 WorkSpace 重建 WorkSpace 刪除的資料比還原還原還多 WorkSpace，但只需要您擁有使用者磁碟區的快照即可。若要還原 WorkSpace，請參閱還原 WorkSpace。

重建 a 會 WorkSpace 導致發生以下情況：

- 根磁碟區 (針對 Microsoft 視窗，磁碟機 C；若為 Linux，/) 會以建立的套裝軟體的最新影像重新整理。 WorkSpace 所有已安裝的應用程式或在建立之後變更的 WorkSpace 系統設定都會遺失。
- 使用者磁碟區 (Microsoft Windows 為磁碟機 D；Linux 為 /home) 會從最新的快照重新建立。使用者磁碟區的目前內容會遭到覆寫。

  每 12 小時排定一次重建 WorkSpace 時使用的自動快照。無論健康狀態為何，都會擷取這些使用者磁碟區的快照 WorkSpace。當您選擇「動作」、「重建/還原 WorkSpace」時，會顯示最新快照的日期和時間。

  當您重建時 WorkSpace，也會在重建完成後不久 (通常在 30 分鐘內) 拍攝新的快照。
- 主要彈性網路介面已重新建立。會 WorkSpace 接收新的私有 IP 位址。

> **Important**
>
> 在 2020 年 1 月 14 日之後，從公用視窗 7 套裝軟體建 WorkSpaces 立，便無法再重建。您可能需要考慮將視窗 7 遷移 WorkSpaces 到視窗 10。如需詳細資訊，請參閱 遷移 WorkSpace。

WorkSpace 只有在符合下列條件時，才能重新計算：

- 必 WorkSpace 須具有`AVAILABLE`、、`ERROR`或`UNHEALTHY`的狀態`STOPPED`、或`REBOOTING`。若要 WorkSpace 在`REBOOTING`狀態下重建，您必須使用 RebuildWorkspacesAPI 作業或重建工作區命令 AWS CLI 。
- 使用者磁碟區的快照必須存在。

若要重新建置 WorkSpace

> **Warning**
>
> 若要重建加密 WorkSpace，請先確定 AWS KMS 金鑰已啟用；否則，將 WorkSpace 無法使用。若要判斷 KMS 金鑰是否已啟用，請參閱《AWS Key Management Service 開發人員指南》中的顯示 KMS 金鑰詳細資訊。

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取 WorkSpace 要重新計算，然後選擇「動作」、「重建/還原」 WorkSpace。
4. 在快照之下，選取快照的時間戳記。
5. 選擇 Rebuild (重建)。

若要 WorkSpace 使用重新建置 AWS CLI

使用 rebuild-workspaces 命令。

故障診斷

如果您在變更使用中目錄中的使用者的 SAM AccountName 使用者命名屬性 WorkSpace 之後重建，您可能會收到下列錯誤訊息：

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

若要解決此問題，請回復為原始使用者命名屬性，然後重新起始重建，或 WorkSpace 為該使用者建立新的屬性。

還原 WorkSpace

還原 WorkSpace 會根據 WorkSpace 狀態良好時所建立的這些磁碟區的最新快照，重新建立根磁碟區和使用者磁碟區。還原 WorkSpace 刪除的資料比重新建置 WorkSpace 還要少。但是，其要求您同時擁有根磁碟區和使用者磁碟區的快照，而重新建置 WorkSpace 只需要使用者磁碟區的快照。若要重新建置 WorkSpace，請參閱 重建 WorkSpace。

還原 WorkSpace 會導致下列情況發生：

- 根磁碟區 (Microsoft Windows 為磁碟機 C；Linux 則為 /) 會還原為最新的快照。任何已安裝的應用程式，或在建立最新快照之後變更的系統設定都會遺失。
- 使用者磁碟區 (Microsoft Windows 為磁碟機 D；Linux 為 /home) 會從最新的快照重新建立。使用者磁碟區的目前內容會遭到覆寫。

製作快照時

根磁碟區和使用者磁碟區的快照會依照下列基礎製作。當您選擇動作、重新建置/還原 WorkSpace時，會顯示最新快照的日期和時間。

- 第一次建立 WorkSpace 之後—通常會在建立 WorkSpace 之後，立即製作根磁碟區和使用者磁碟區的初始快照 (通常在 30 分鐘內)。在某些 AWS 區域中，建立 WorkSpace 之後可能需要數小時才能製作初始快照。

  如果在製作初始快照之前，WorkSpace 變得狀態不佳，則無法還原 WorkSpace。在這種情況下，您可以嘗試重新建置 WorkSpace 或聯絡 AWS 支援尋求協助。
- 一般使用期間—用於還原 WorkSpace 時使用的自動快照會每 12 小時排程一次。如果 WorkSpace 狀態良好，則大約會在同一時間建立根磁碟區和使用者磁碟區的快照。如果 WorkSpace 狀態不佳，則只會為使用者磁碟區建立快照。
- 還原 WorkSpace 之後—當您還原 WorkSpace 時，會在還原完成後立即製作新的快照 (通常在 30 分鐘內)。在某些 AWS 區域中，還原 WorkSpace 之後可能需要數小時才能製作這些快照。

  還原 WorkSpace 之後，如果 WorkSpace 在可以製作新快照之前變成狀態不佳，則無法再次還原 WorkSpace。在這種情況下，您可以嘗試重新建置 WorkSpace 或聯絡 AWS 支援尋求協助。

只有在符合下列條件時，才可還原 WorkSpace：

- WorkSpace 的狀態必須為 `AVAILABLE`、`ERROR`、`UNHEALTHY` 或 `STOPPED`。
- 根磁碟區和使用者磁碟區的快照必須存在。

若要還原 WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取要還原的 WorkSpace，然後選擇動作、重新建置/還原 WorkSpace。

4. 在快照之下，選取快照的時間戳記。
5. 選擇 Restore (還原)。

若要使用 AWS CLI 還原 WorkSpace

使用 restore-workspace 命令。

Microsoft 365 自帶授權 (BYOL)

Amazon WorkSpaces 允許您攜帶自己的 Microsoft 365 許可證，如果他們滿足微軟的許可要求。這些授權可讓您安裝並啟動 Microsoft 365 應用程式適用於企業軟體，且 WorkSpaces 這些應用程式由下列作業系統提供支援：

- Windows 10 (自帶授權)
- Windows 11 (自帶授權)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

要使用適用於企業的 Microsoft 365 應用程序 WorkSpaces，您必須訂閱 Microsoft 365 E3/E5，Microsoft 365 A3/A5 或 Microsoft 365 商務高級版。

在您的 Amazon 上， WorkSpaces 您可以使用您的 Microsoft 365 許可證來安裝和激活 Microsoft 365 企業應用程序，包括以下內容：

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

如需詳細資訊，請參閱 Microsoft 365 Apps 企業版完整清單。

您還可以安裝 Microsoft 應用程序不包括在 Microsoft 365，如 Microsoft 項目，Microsoft Visio 和 Microsoft 電源自動化， WorkSpaces 但你需要帶在自己的額外許可證。

您可以使用多區域復原，在主要應用程式和容錯移轉上安裝及 WorkSpaces 使用 Microsoft 365 WorkSpaces 和其他 Microsoft 應用程式。

目錄

WorkSpaces 使用適用於企業的 Microsoft 365 應用程式

若要使用適 WorkSpaces 用於企業的 Microsoft 365 應用程式建立，您必須建立已安裝應用程式的自訂映像，並使用它來建立自訂套裝軟體。您可以使用套裝軟體啟動已安裝應用程式的新功 WorkSpaces 能。 WorkSpaces 不提供適用於企業的 Microsoft 365 應用程式的公用服務包。

WorkSpaces 使用適用於企業的 Microsoft 365 應用程式建立：

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 啟動您 WorkSpace 要用作其他 Microsoft 應用程序的圖像 WorkSpaces。這是您將安裝 Microsoft 應用程式的地方。如需有關啟動的詳細資訊 WorkSpace，請參閱使用啟動虛擬桌面 WorkSpaces。
3. 從 https://clients.amazonworkspaces.com/ 啟動用戶端應用程式，輸入邀請電子郵件中的註冊碼，然後選擇註冊。
4. 當系統提示您登入時，請輸入使用者的登入認證，然後選擇登入。
5. 安裝和設定 Microsoft 365 Apps 企業版。
6. 從建立自訂映像 WorkSpace，並使用它來建立自訂套裝軟體。如需有關建立自訂映像和套裝軟體的詳細資訊，請參閱建立自訂 WorkSpaces 映像和套裝軟體。
7. WorkSpaces 使用您建立的自訂套裝軟體啟動。這些 WorkSpaces 都安裝了 Microsoft 365 企業應用程序。

遷移您現有 WorkSpaces 的企業使用 Microsoft 365 應用程式

如果您 WorkSpaces 沒有通過 Microsoft Office 許可證AWS，您可以在您的 WorkSpaces.

如果您 WorkSpaces 確實擁有 Microsoft Office 許可證AWS，則必須先取消註冊您的 Microsoft Office 許可證，然後才能安裝適用於企業的 Microsoft 365 應用程序。

> **Important**
>
> 從您卸載 Microsoft Office 應用程序 WorkSpaces 不會取消註冊許可證。若要避免收取 Microsoft Office 授權費用，請透過AWS執行下列其中一項作業， WorkSpaces 從 Microsoft Office 應用程式中取消註冊：
>
> - 管理應用程式 (推薦) — 您可以卸載 Microsoft 辦公室 2016 和 2019 從您的 WorkSpaces. 如需詳細資訊，請參閱管理應用程式。解除安裝之後，您可以在您的 WorkSpaces.
> - 移轉 WorkSpace — 您可以將一個 WorkSpace 套裝軟體移轉至另一個套裝軟體，同時將資料保留在使用者磁碟區上。
>   - 將您的套件移轉 WorkSpaces 至包含沒有 Microsoft Office 訂閱的映像檔。遷移完成後，您可以在您的 WorkSpaces.
>   - 或者，建立已在 WorkSpaces 映像上安裝 Microsoft 365 企業用應用程式的自訂映像和套裝軟體，然後將您的影像移轉 WorkSpaces 至此新的自訂服務包。移轉完成後，您的使用 WorkSpaces 者可以開始使用適用於企業的 Microsoft 365 應用程式。
>   - 如需如何移轉的詳細資訊 WorkSpaces，請參閱移轉 WorkSpace.

更新適用於企業的 Microsoft 365 應用程式 WorkSpaces

默認情況下，您在 Microsoft Windows 操作系統上 WorkSpaces 運行的配置為接收來自 Windows 更新的更新。但是，Microsoft 365 Apps 企業版的更新無法透過 Windows Update 取得。設置更新以從 Office CDN 自動執行，或使用 Windows Server Update Services (WSUS) 搭配 Microsoft Configuration Manager 來更新 Microsoft 365 Apps 企業版。如需詳細資訊，請參閱使用 Microsoft Configuration Manager 管理 Microsoft 365 Apps 的更新。若要設定 Microsoft 365 應用程式更新的頻率，請指定更新通道並將其設定為目前或每月企業版，以符合 Microsoft 365 WorkSpaces 授權原則。

升級視窗自攜裝置 WorkSpaces

在您的 Windows 自攜授權 (BYOL) 上 WorkSpaces，您可以使用就地升級程序升級至較新版本的 Windows。若要這麼做，請遵循本主題中的指示。

就地升級程序僅適用於視窗 10 和自攜 WorkSpaces裝置。

> **Important**
>
> 請勿在升級版本上執行系統表示。 WorkSpace如果您這麼做，可能會發生阻止 Sysprep 完成的錯誤。如果您打算執行 Sysprep，請僅在尚未升級的版本上執行此操作。 WorkSpace

> **Note**
>
> 您可以使用此過程將 Windows 10 和 11 升級 WorkSpaces 到較新的版本。但是，此過程無法用於將窗戶 10 升級 WorkSpaces 到窗戶 11。

目錄

必要條件

- 如果您使用群組原則或系統中心組態管理員 (SCCM) 延遲或暫停 Windows 10 和 11 升級，請啟用 Windows 10 和 11 的作業系統升級。 WorkSpaces
- 如果 WorkSpace 是 AutoStop WorkSpace，請在就地升級程序 AlwaysOn WorkSpace之前將其變更為，以便在套用更新時不會自動停止。如需詳細資訊，請參閱 修改執行模式。如果您希望將 WorkSpace 設定保留為 AutoStop，請在升級 AutoStop 期間將時間變更為三小時或更長時間。
- 就地升級程序會藉由複製名為預設使用者 (`C:\Users\Default`) 的特殊設定檔來重新建立使用者設定檔。請勿使用此預設使用者設定檔進行自訂。建議改為透過群組政策物件 (GPO) 對使用者設定檔進行任何自訂。透過 GPO 進行的自訂可輕鬆地修改或復原，而且不易發生錯誤。
- 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。

考量事項

就地升級程序會使用兩個登錄指令碼 (enable-inplace-upgrade.ps1和update-pvdrivers.ps1) 來對您的進行必要 WorkSpaces 的變更，以便執行 Windows Update 程序。這些變更涉及在磁碟機 C (而非磁碟機 D) 上建立 (暫時) 使用者設定檔。如果磁碟機 D 上已存在使用者設定檔，則該原始使用者設定檔中的資料會保留在磁碟機 D 上。

依預設， WorkSpaces 會在中建立使用者紀要D:\Users\%USERNAME%。enable-inplace-upgrade.ps1 指令碼會將 Windows 設為在 C:\Users\%USERNAME% 中建立新的使用者設定檔，並將使用者 Shell 資料夾重新導向至 D:\Users\%USERNAME%。這個新的使用者設定檔會在使用者第一次登入時建立。

就地升級之後，您可選擇將使用者設定檔保留在磁碟機 C 上，讓使用者未來使用 Windows Update 程序來升級其電腦。但是請注意 WorkSpaces ，除非您自己備份並還原該資料，否則儲存在磁碟機 C 上的設定檔無法重建或移轉，而不會遺失使用者設定檔中的所有資料。如果您決定將設定檔保留在磁碟機 C 上，您可以使用UserShellFoldersRedirection登錄機碼將使用者 shell 資料夾重新導向至磁碟機 D，如本主題稍後所述。

為了確保您可以重建或移轉您的， WorkSpaces 並避免任何潛在的使用者 shell 資料夾重新導向問題，我們建議您選擇在就地升級之後將使用者設定檔還原至磁碟機 D。您可以使用 PostUpgradeRestoreProfileOnD 登錄機碼來執行此操作，如本主題稍後所述。

已知限制

- 在 WorkSpace 重建或移轉期間，不會發生使用者設定檔位置從磁碟機 D 變更為磁碟機 C。如果您在 Windows 10 或 11 BYOL 上執行就地升級， WorkSpace 然後重建或移轉它，則新的磁碟機 D 上 WorkSpace 會有使用者設定檔。

  > **Warning**
  >
  > 如果您在就地升級後將使用者設定檔保留在磁碟機 C 上，則儲存在磁碟機 C 上的使用者設定檔資料將會在重新建置或遷移期間遺失，除非您在重新建置或遷移前手動備份使用者設定檔資料，然後在執行重新建置或遷移程序後手動還原使用者設定檔資料。

- 如果您的預設 BYOL 套裝軟體包含以舊版 Windows 10 和 11 為基礎的映像，您必須在重建或移轉之後再次執行就地升級。 WorkSpace

登錄機碼設定摘要

若要啟用就地升級程序，並指定升級後的使用者設定檔位置，您必須設定數個登錄機碼。

登錄路徑：港島線 M:\Software\AmazonWorkSpacesConfig\ .ps1 enable-inplace-upgrade

登錄機碼	Type	值
已啟用	DWORD	0 - (預設值) 停用就地升級 1 - 啟用就地升級
PostUpgradeRestoreProfileOnD	DWORD	0 - (預設值) 在就地升級後不嘗試還原使用者設定檔路徑 1 — 在就地升級後還原使用者紀要路徑 (ProfileImagePath)
UserShellFoldersRedirection	DWORD	0 - 不啟用使用者 Shell 資料夾的重新導向 1 - (預設值) 在 C:\Users\%USERNAME% 上重新產生使用者設定檔後，啟用使用者 shell 資料夾的重新導向至 D:\Users\%USERNAME%
NoReboot	DWORD	0 - (預設值) 允許您在修改使用者設定檔的登錄後，控制重新啟動的時間 1 — 修改使用者設定檔的登錄 WorkSpace 後，不允許指令碼重新開機

登錄路徑：港島線 M:\Software\Amazon\WorkSpacesConfig\ 更新程式驅動程式 .ps1

登錄機碼	Type	值
已啟用	DWORD	0 — (預設值) 停用 AWS PV 驅動程式更新 1 — 啟用 AWS PV 驅動程式更新

執行就地升級

若要在 BYOL 上啟用就地 Windows 升級 WorkSpaces，您必須設定特定登錄機碼，如下列程序所述。您也必須設定某些登錄機碼，以指出在就地升級完成後，您希望使用者設定檔所在的磁碟機 (C 或 D)。

您可以手動進行這些登錄變更。如果您有多個 WorkSpaces 要更新的項目，您可以使用群組原則或 SCCM 來推送 PowerShell 指令碼。如需範例 PowerShell指令集，請參閱使用 PowerShell 指令碼更新您的 WorkSpace 登錄。

若要執行視窗 10 和 11 的就地升級

1. 請記下您正在更新的 Windows 10 和 11 BYOL WorkSpaces 上目前執行的 Windows 版本，然後將它們重新開機。
2. 更新下列 Windows 系統登錄機碼，將已啟用的值資料從 0 變更為 1。這些登錄變更會啟用 WorkSpace.

   - HKEY 本地機器\ 軟體\ Amazon\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY 本地機器\ 軟件\ Amazon\\ 更新 PV驅動程序 .ps1 WorkSpacesConfig

   > **Note**
   >
   > 如果這些金鑰不存在，請重新啟動 WorkSpace. 當系統重新啟動時，應該新增這些機碼。

   (選用) 如果您使用受管的工作流程 (例如 SCCM 任務序列) 來執行升級，請將下列機碼值設定為 1，以防止電腦重新開機：

   HKEY 本地機器\ 軟體\ Amazon\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. 決定使用者設定檔在就地升級程序後所在的磁碟機 (如需詳細資訊，請參閱 考量事項)，並依下列方式設定登錄機碼：

   - 如果您希望使用者設定檔在升級後位於磁碟機 C 上，則設定如下：

     HKEY 本地機器\ 軟體\ Amazon\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     金鑰名稱：PostUpgradeRestoreProfileOnD

     機碼值：0

     金鑰名稱：UserShellFoldersRedirection

     機碼值：1

   - 如果您希望使用者設定檔在升級後位於磁碟機 D 上，則設定如下：

     HKEY 本地機器\ 軟體\ Amazon\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     金鑰名稱：PostUpgradeRestoreProfileOnD

     機碼值：1

     金鑰名稱：UserShellFoldersRedirection

     機碼值：0

4. 將更改保存到註冊表後， WorkSpace 再次重新啟動以便應用更改。

   > **Note**
   >
   > - 重新啟動後，登錄到 WorkSpace 創建一個新的用戶配置文件。您可能會在開始功能表中看到預留位置圖示。此行為會在就地升級完成後自動解決。
   > - 允許 10 分鐘以確保解除阻止。 WorkSpace

   (選擇性) 確認下列索引鍵值設定為 1，以解除封鎖以 WorkSpace 進行更新：

   HKEY 本地機器\ 軟體\ Amazon\ .ps1\ 已刪除 WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. 執行就地升級。您可以使用任何您喜歡的方法，例如 SCCM、ISO 或 Windows 更新 (WU)。根據您的原始 Windows 10 和 11 版本以及安裝了多少應用程式，此過程可能需要 40 到 120 分鐘。

   > **Note**
   >
   > 就地升級程序可能需要至少一個小時。 WorkSpace 執行個體狀態可能會顯示為升級UNHEALTHY期間。

6. 更新程序完成後，請確認 Windows 版本已更新。

   > **Note**
   >
   > 如果就地升級失敗，Windows 會自動復原以使用在您開始升級之前就地存在的 Windows 10 和 11 版本。如需詳細資訊，請參閱 Microsoft 文件。

   (選用) 若要確認更新指令碼已成功執行，請確認下列機碼值設定為 1：

   HKEY 本地機器\ 軟體\ Amazon\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. 如果您 WorkSpace 透過將其設定為 AlwaysOn 或變更期 AutoStop 間來修改的執行模式，以便就地升級程序可以在不中斷的情況下執行，請將執行模式設回原始設定。如需詳細資訊，請參閱 修改執行模式。

如果您尚未將 PostUpgradeRestoreProfileOnD 登錄機碼設定為 1，則 Windows 會重新產生使用者設定檔，並在就地升級`C:\Users\%USERNAME%`之後放置在其中，如此一 future 您就地升級就地不必再執行上述步驟。根據預設，`enable-inplace-upgrade.ps1` 指令碼會將下列 Shell 資料夾重新導向至磁碟機 D：

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`
- `D:\Users\%USERNAME%\Documents`

- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

如果您將 shell 資料夾重新導向至上的其他位置 WorkSpaces，請在就地升級 WorkSpaces 之後對中執行必要的作業。

故障診斷

如果您在更新時遇到任何問題，可以檢查下列項目協助進行疑難排解：

- Windows 日誌預設位於下列位置：

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`

- Windows 事件檢視器

  視窗日誌 > 應用程式 > 來源：Amazon WorkSpaces

> **Tip**
>
> 在就地升級過程中，如果您看到桌面上的某些圖示捷徑不再起作用，這是因為 WorkSpaces 將位於磁碟機 D 上的任何使用者設定檔移至磁碟機 C 以準備升級。升級完成後，捷徑就會如預期般運作。

使用 PowerShell 指令碼更新您的 WorkSpace 登錄

您可以使用下列範例 PowerShell 指令碼來更新您的登錄， WorkSpaces 以啟用就地升級。按照執行就地升級，但使用此腳本更新每個註冊表 WorkSpace。

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
```

```
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

遷移 WorkSpace

> **Note**
>
> 如果您想要透過AWS您的取消訂閱或解除安裝 Microsoft Office 版本授權 WorkSpace，我們建議您使用管理應用程式。

您可以將一個 WorkSpace 套裝軟體移轉至另一個套裝軟體，同時將資料保留在使用者磁碟區上。範例案例如下：

- 您可以 WorkSpaces 從 Windows 7 桌面體驗遷移到 Windows 10 桌面體驗。
- 您可以 WorkSpaces 從 PCoIP 通訊協定移轉至 WorkSpaces 串流通訊協定 (WSP)。
- 您可以 WorkSpaces 從 32 位 Microsoft 辦公軟件包遷移到 64 位 Microsoft 辦公軟 WorkSpaces 件包 Windows 服務器 2019 和 Windows 服務器 2022 WorkSpaces 驅動的捆綁包。
- 您可以 WorkSpaces 從一個公用套裝軟體或自訂套裝軟體移轉至另一個 例如，您可以從啟用 GPU (圖形 .g4dn) 移轉。 GraphicsPro.g4dn、圖形和 GraphicsPro) 會套裝至未啟用 GPU 的套裝軟體，以及其他方向。
- 您可以 WorkSpaces 從視窗 10 BYOL 遷移到視窗 11 自攜裝置，但從視窗 11 遷移到視窗 10 不支援。
- Windows 11 不支援超值套件。若要將您的 Windows 7 或 10 超值套裝軟體遷移 WorkSpaces 至 Windows 11，您需要先將您的價值切 WorkSpaces 換為更大的套裝產品。
- WorkSpaces 從窗戶 7 遷移到窗戶 11 之前，您需要將其遷移到窗戶 10。請至少登入一次 WorkSpace ，然後再將其移轉至視窗 11。不支援從視窗 7 WorkSpaces 直接移轉至視窗 11。
- 您可以將使用 Microsoft 辦公室 WorkSpaces 的視窗移轉AWS至具有 Microsoft 365 應用程式的自訂 WorkSpaces 服務包。移轉之後，您 WorkSpaces 將取消訂閱 Microsoft Office。
- 您可以將使 WorkSpaces 用 Microsoft 辦公軟件的視窗遷移AWS到沒有辦公室 2016/2019 訂閱的 WorkSpaces捆綁。移轉之後，您 WorkSpaces 將取消訂閱 Microsoft Office。

如需 Amazon WorkSpaces 套裝軟體的詳細資訊，請參閱WorkSpace 捆綁和圖像。

移轉程序會使用目標套裝軟體映像中的新根磁碟區和原始 WorkSpace檔案的上一個可用快照中的使用者磁碟區來重新建立。 WorkSpace 遷移期間會產生新的使用者設定檔，以提高相容性。舊的使用者設定檔會重新命名，然後舊使用者設定檔中的某些檔案會移至新的使用者設定檔。(如需移動內容的詳細資訊，請參閱 遷移期間發生的事。)

每個遷移程序最多需要一個小時 WorkSpace。當您啟動移轉程序時，會建立新 WorkSpace 的程序。如果發生阻止成功移轉的錯誤，原始 WorkSpace 檔案會復原並返回其原始狀態，並終止新 WorkSpace 的狀態。

內容

遷移限制

- 您無法遷移至公用或自訂 Windows 7 桌面體驗套件。您也無法遷移至自帶授權 (BYOL) Windows 7 套件。
- 您 WorkSpaces 只能將 BYOL 移轉至其他 BYOL 服務包。若要將 BYOL WorkSpace 從 PCoIP 移轉至 WSP，您必須先使用 WSP 通訊協定建立 BYOL 服務包。然後，您可以將您的 PCoIP BYOL 移轉 WorkSpaces 至該 WSP 自攜服務包。
- 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。
- 圖形 .g4dn、 GraphicsPro .g4dn、圖形和 GraphicsPro 套裝軟體目前僅適用於 PCoIP 通訊協定，因此圖形 .g4dn、.g4dn、圖形，而且還無法移轉至 WSP。 GraphicsPro GraphicsPro WorkSpaces
- 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，在支援多種語言的區域中，只要語言不同，您就可以遷移至相同的 Windows 10 套件。) 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。
- 在某些情況下，如果遷移無法順利完成，您可能不會收到錯誤訊息，而且可能遷移程序似乎尚未開始。如果 WorkSpace 套裝軟體在嘗試移轉一小時後維持不變，則移轉不會成功。聯絡 AWS Support 中心尋求協助。

遷移案例

下表顯示可用的遷移案例：

來源作業系統	目標作業系統	可用？
公用或自訂套件 Windows 7	公用或自訂套件 Windows 10	是
自訂套件 Windows 7	公用套件 Windows 7	否
自訂套件 Windows 7	自訂套件 Windows 7	否
公用套件 Windows 7	自訂套件 Windows 7	否
公用或自訂套件 Windows 10	公用或自訂套件 Windows 7	否
公用或自訂套件 Windows 10	自訂套件 Windows 10	是
Windows 7 BYOL 套件	Windows 7 BYOL 套件	否
Windows 7 BYOL 套件	Windows 10 BYOL 套件	是
Windows 10 BYOL 套件	Windows 7 BYOL 套件	否
Windows 10 BYOL 套件	Windows 10 BYOL 套件	是
Windows Server 2016 支援的公用 Windows 10 套件	Windows Server 2019 支援的公用 Windows 10 套件 	是

來源作業系統	目標作業系統	可用？
Windows Server 2019 支援的公用 Windows 10 套件 	Windows Server 2016 支援的公用 Windows 10 套件	是
Windows 10 BYOL 套件	Windows 11 BYOL 套件	是
Windows 11 BYOL 套件	Windows 10 BYOL 套件	否
Windows Server 2016 支援的自訂 Windows 10 套件	Windows Server 2019 支援的公用 Windows 10 套件	是
Windows Server 2016 支援的自訂 Windows 10 套件	Windows Server 2022 支援的公用 Windows 10 套件	是
Windows Server 2019 支援的自訂 Windows 10 套件	Windows Server 2022 支援的公用 Windows 10 套件	是

Note

Web 存取不適用於 Windows Server 2019 支援的公用 Windows 10 套件 PCoIP 分支。

Important

Windows Server 2016 支援的公用 Windows 10 增強套件包含 Microsoft Office 2016 和 Trend Micro Worry-Free Business Security Services。Windows Server 2019 支援的公用 Windows 10 增強套件僅包含 Microsoft Office 2019，而不包含 Trend Micro Services。

遷移期間發生的事

在遷移期間，會保留使用者磁碟區 (磁碟機 D) 上的資料，但是根磁碟區 (磁碟機 C) 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 .NotMigrated 字尾重新命名，並建立新的使用者設定檔。

遷移程序會根據原始使用者磁碟區的最後一個快照重新建立磁碟機 D。在新資料夾的第一次開機期間 WorkSpace，移轉程序會將原始D:\Users\%USERNAME%資料夾移至名為的資料夾D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated。新的作業系統會產生新的 D:\Users\%USERNAME%\ 資料夾。

建立新的使用者設定檔之後，下列使用者 shell 資料夾中的檔案會從舊的 .NotMigrated 設定檔移至新設定檔：

- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos

> **Important**
>
> 遷移程序會嘗試將檔案從舊使用者設定檔移至新設定檔。遷移期間內任何未移動的檔案都會保留在 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 資料夾中。如果遷移成功，您可以查看哪些檔案移入 C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs。您可以手動移動任何未自動移動的檔案。
> 依預設，公用套件會停用本機搜尋檢索。若要加以啟用，則預設會搜尋 C:\Users 而不是 D:\Users，因此您也需要進行調整。如果您已將本機搜尋檢索特別設定為 D:\Users*username* 而非 D:\Users，則本機搜尋檢索可能無法在遷移後對 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 資料夾中的任何使用者檔案運作。

移轉期間，指派給原始標籤的 WorkSpace 所有標籤都會繼續進行，並保留的 WorkSpace 執行模式。不過，新的 WorkSpace 會取得新的 WorkSpace ID、電腦名稱和 IP 位址。

最佳實務

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「遷移 WorkSpaces」頁面上，您可以查看上次快照的時間。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，請確定您的使用者登出他們的使用者， WorkSpaces而且在遷移程序完成之前不要重新登入。請注意，當它們處於ADMIN_MAINTENANCE模式時， WorkSpaces 無法進行遷移。
- 請確定 WorkSpaces 您要移轉的狀態為AVAILABLESTOPPED、或ERROR。
- 請確定您有足夠的 IP 位址供 WorkSpaces 您移轉的使用者使用。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。

故障診斷

- 如果使用者在遷移之後回報遺失檔案，請查看其使用者設定檔是否未在遷移過程中移動。您可以查看哪些檔案移入 C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs。未移動的檔案將位於 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 資料夾中。您可以手動移動任何未自動移動的檔案。
- 如果您使用 API 進行遷移 WorkSpaces ，但遷移未成功，則不會使用 API 傳回的目標 WorkSpace ID，而且仍 WorkSpace會擁有原始 WorkSpace ID。
- 如果遷移未成功完成，請檢查 Active Directory 以查看其是否已相應地清除。您可能需要手動移除 WorkSpaces 不再需要的項目。

計費影響

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。

> **Note**
>
> 如果您要移轉 WorkSpace 至不同的套裝軟體類型 (例如，從「效能」移轉至「電源」或「值」移轉至「標準」)，則在移轉過程中，根磁碟區 (磁碟機 C) 和使用者磁碟區 (磁碟機 D) 的大小可能會增加。如有必要，根磁碟區會增加以符合新套件的預設根磁碟區大小。但是，如果您已經為使用者磁碟區指定的大小與原始套件的預設值不同 (更大或更小)，則在遷移過程中會保留相同的使用者磁碟區大小。否則，移轉程序會使用較大的來源使用 WorkSpace 者磁碟區大小和新套裝軟體的預設使用者磁碟區大小。

遷移 WorkSpace

您可以 WorkSpaces 透過 Amazon WorkSpaces 主控台AWS CLI或 Amazon WorkSpaces API 進行遷移。

若要移轉 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取您的 WorkSpace 並選擇 [動作]、[移轉] WorkSpaces。
4. 在「組合包」下，選取您要移轉 WorkSpace 至的套裝軟體。

   > **Note**
   >
   > 若要將 BYOL WorkSpace 從 PCoIP 移轉至 WSP，您必須先使用 WSP 通訊協定建立 BYOL 服務包。然後，您可以將您的 PCoIP BYOL 移轉 WorkSpaces 至該 WSP 自攜服務包。

5. 選擇「移轉」 WorkSpaces。

   Amazon WorkSpaces 控制台中`PENDING`會出現一個狀態為的新 WorkSpace 功能。移轉完成時，原始檔 WorkSpace 案會終止，且新的狀態會設定 WorkSpace 為`AVAILABLE`。
6. (選用) 若要刪除您不再需要的任何自訂套件和映像，請參閱 刪除自訂 WorkSpaces 套裝軟體或影像。

若要 WorkSpaces 透過移轉AWS CLI，請使用移轉工作區指令。若要 WorkSpaces 透過 Amazon WorkSpaces API 進行遷移，請參閱 Amazon WorkSpaces API 參考MigrateWorkSpace中的。

刪除 WorkSpace

WorkSpace 結束使用後即可刪除。您也可以刪除相關資源。

> **Warning**
>
> 刪除 WorkSpace 是永久動作，無法復原。WorkSpace 使用者的資料不會持續存在，而且會被銷毀。如需備份使用者資料的協助，請聯絡 AWS 支援。

> **Note**
>
> 您可以免費使用 Simple AD 和 AD Connector，以便與 WorkSpaces 搭配使用。如果連續 30 天沒有任何 WorkSpaces 搭配您的 Simple AD 或 AD Connector 目錄使用，則此目錄會自動取消註冊以便搭配 Amazon WorkSpaces 使用，而且您需依據 AWS Directory Service 定價條款支付此目錄的費用。
> 若要刪除空目錄，請參閱 刪除 WorkSpaces 的目錄。如果您刪除 Simple AD 或 AD Connector 目錄，當您想要再次開始使用 WorkSpaces 時，隨時都可以建立新的目錄。

如要刪除 WorkSpace

您可以刪除處於暫停以外任何狀態的 WorkSpace。

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取您的 WorkSpace，然後選擇刪除。
4. 出現確認提示時，請選擇刪除 WorkSpace。刪除 WorkSpace 大約需要 5 分鐘。在刪除期間，WorkSpace 的狀態會設定為終止中。刪除完成時，WorkSpace 會從主控台中消失。
5. (選用) 若要刪除您已完成的任何自訂套件和映像，請參閱 刪除自訂 WorkSpaces 套裝軟體或影像。
6. (選用) 刪除目錄中的所有 WorkSpaces 之後，您可以刪除該目錄。如需詳細資訊，請參閱 刪除 WorkSpaces 的目錄。
7. (選用) 刪除目錄的虛擬私有雲端 (VPC) 中的所有資源後，您可以刪除 VPC 並釋放用於 NAT 閘道的彈性 IP 位址。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的刪除 VPC和使用彈性 IP 位址。

若要使用 AWS CLI 刪除 WorkSpace

使用 terminate-workspaces 命令。

WorkSpace 捆綁和圖像

WorkSpace 服務包是作業系統、儲存、運算和軟體資源的組合。啟動時 WorkSpace，請選取符合您需求的套裝軟體。可用的預設套裝軟體稱 WorkSpaces 為公用套裝軟體。如需有關各種可用公用套件的詳細資訊 WorkSpaces，請參閱 Amazon WorkSpaces 組合包。

如果您已經啟動了 Windows 或 Linux WorkSpace 並進行了自定義，則可以從中創建自定義映像 WorkSpace。

自訂映像僅包含的作業系統、軟體和設定 WorkSpace。自訂套裝軟體是該自訂映像檔和 WorkSpace 可從中啟動的硬體的組合。

建立自訂映像後，您可以建置自訂服務包，結合自訂 WorkSpace 映像以及您選取的基礎運算和儲存區組態。然後，您可以在啟動新的時候指定此自訂套裝軟體， WorkSpaces 以確保新配置 WorkSpaces 具有相同的一致組態 (硬體和軟體)。

如果您需要執行軟體更新或在您的上安裝其他軟體 WorkSpaces，您可以更新自訂套裝軟體並使用它來重建 WorkSpaces.

WorkSpaces 支援多種不同的作業系統 (OS)、串流通訊協定和套裝軟體。下表提供每個作業系統支援之授權、串流通訊協定和套裝軟體的相關資訊。

作業系統	授權	串流協定	支援的套件	生命週期政策/退休日期
Windows Server 2016	已包含	WSP, PCoIP	值、標準、效能、電源、圖形 (已停用) PowerPro、圖形 .G4dn GraphicsPro、.g4dn GraphicsPro	2027年1月12日
Windows Server 2019	已包含	WSP, PCoIP	值、標準、效能、電源、圖形 (已停用) PowerPro、圖形 .G4dn GraphicsPro、.g4dn GraphicsPro	2029年1月9日
Windows Server 2022	已包含	WSP, PCoIP	標準、效能、電源 PowerPro、圖形 (已停用)、圖形 .G4dn GraphicsPro、.g4dn GraphicsPro	2031年10月14日

作業系統	授權	串流協定	支援的套件	生命週期政策/退休日期
Windows 10	使用自有授權 (BYOL)	WSP, PCoIP	值、標準、效能、電源、圖形 (已停用) PowerPro、圖形 .G4dn GraphicsPro、.g4dn GraphicsPro	在支援中
Windows 11	使用自有授權 (BYOL)	WSP	標準、效能、電源、 PowerPro	在支援中
Amazon Linux 2	已包含	WSP, PCoIP	價值、標準、效能、電源、 PowerPro	2025年6月30日
Ubuntu 22.04 LTS	已包含	WSP	值、標準、效能、功率、圖形 PowerPro、G4dn GraphicsPro	2032 年六月

> **Note**
>
> - 廠商不再 AWS 支援的作業系統版本無法保證可正常運作，且不受支援支援。
> - 若要在 Windows 作業系統上 WorkSpaces 執行，圖形組合僅支援 PCoIP 串流通訊協定。

目錄

套件選項

選取套件之前，確定您要選取的套件與您 WorkSpaces 的協定、作業系統、網路和運算類型相容。如需有關協定的詳細資訊，請參閱 Amazon WorkSpaces 的協定。如需有關網路的詳細資訊，請參閱 Amazon WorkSpaces 用戶端網路需求。

> **Note**
>
> - 對於 PCoIP WorkSpaces，我們建議不要超過 250 毫秒的網路延遲上限。為了獲得最佳的 PCoIP WorkSpaces 使用者體驗，我們建議將網路延遲保持在 100 毫秒以下。當往返時間 (RTT) 超過 375 毫秒時，WorkSpaces 用戶端連線將會關閉。為了獲得最佳的 WorkSpaces 串流協定 (WSP) 使用者體驗，我們建議將 RTT 保持在 250 毫秒以下。如果 RTT 介於 250 毫秒到 400 毫秒之間，使用者可以存取 WorkSpace，但效能會大幅降低。
> - 建議執行並使用可複寫使用者日常工作的應用程式，以測試您要在測試環境中選擇的套件效能。

> **Important**
>
> - 在 2023 年 11 月 30 日之後，不再支援 Graphics 套件。我們建議您使用圖形套件來切換至 WorkSpaces 的 Graphics.g4dn 套件。
> - 亞太 (孟買) 區域目前無法在使用 Graphics 和 GraphicsPro 套件。

以下是 WorkSpaces 提供的套件。如需 WorkSpaces 中套件的相關資訊，請參閱 Amazon WorkSpaces 套件。

超值套件

此套件非常適合下列各項：

- 基本文字編輯和資料輸入
- 輕度使用的網頁瀏覽
- 即時訊息

不建議將此套件用於文字處理、音訊和視訊會議、螢幕共用、軟體開發工具、商業智慧應用程式和圖形應用程式。

標準套件

此套件非常適合下列各項：

- 基本文字編輯和資料輸入
- 網頁瀏覽
- 即時訊息
- 電子郵件

不建議將此套件用於音訊和視訊會議、螢幕共用、文字處理、軟體開發工具、商業智慧應用程式和圖形應用程式。

效能套件

此套件非常適合下列各項：

- 網頁瀏覽
- 文字處理
- 即時訊息
- 電子郵件
- 試算表
- 音訊處理
- 課程教材

不建議將此套件用於視訊會議、螢幕共用、軟體開發工具、商業智慧應用程式和圖形應用程式

Power 套件

此套件非常適合下列各項：

- 網頁瀏覽
- 文字處理
- 電子郵件

- 即時訊息
- 試算表
- 音訊處理
- 軟體開發 (整合式開發環境 (IDE))
- 入門到中級資料處理
- 音訊和視訊會議

不建議將此套件用於螢幕共用、軟體開發工具、商業智慧應用程式和圖形應用程式。

PowerPro 套件

此套件非常適合下列各項：

- 網頁瀏覽
- 文字處理
- 電子郵件
- 即時訊息
- 試算表
- 音訊處理
- 軟體開發 (整合式開發環境 (IDE))
- 資料倉儲
- 商業智慧應用程式
- 音訊和視訊會議

不建議將此套件用於機器學習模型訓練和圖形應用程式

GraphicsPro 套件

此套件可為 WorkSpaces 提供基準層級的圖形效能，以及高層級的 CPU 效能和記憶體。其非常適合下列各項：

- 網頁瀏覽
- 文字處理

- 電子郵件
- 即時訊息
- 試算表
- 音訊會議
- 軟體開發 (整合式開發環境 (IDE))
- 資料倉儲
- 商業智慧應用程式
- 圖形設計
- 影像處理

不建議將此套件用於音訊和視訊會議、3D 轉譯和相片寫實風格設計

Graphics.g4dn 套件

此套件為 WorkSpaces 提供高層級的圖形效能，以及中等層級的 CPU 效能和記憶體，非常適合下列各項：

- 網頁瀏覽
- 文字處理
- 電子郵件
- 試算表
- 即時訊息
- 音訊會議
- 軟體開發 (整合式開發環境 (IDE))
- 入門到中級資料處理
- 資料倉儲
- 商業智慧應用程式
- 圖形設計
- CAD/CAM (電腦輔助設計/電腦輔助製造)

不建議將此套件用於音訊和視訊會議、3D 轉譯、相片寫實風格設計和機器學習模型訓練

GraphicsPro.g4dn

GraphicsPro.g4dn 套件

此套件可為 WorkSpaces 提供高等級的圖形效能、CPU 效能和記憶體，非常適合下列各項：

- 網頁瀏覽
- 文字處理
- 電子郵件
- 試算表
- 即時訊息
- 音訊會議
- 軟體開發 (整合式開發環境 (IDE))
- 入門到中級資料處理
- 資料倉儲
- 商業智慧應用程式
- 圖形設計
- CAD/CAM (電腦輔助設計/電腦輔助製造)
- 視訊轉碼
- 3D 轉譯
- 相片寫實風格設計
- 遊戲串流
- ML (機器學習) 模型訓練與 ML 推論

不建議將此套件用於音訊和視訊會議。

建立自訂 WorkSpaces 映像檔和套裝軟體

如果您已啟動 Windows 或 Linux WorkSpace 並進行了自訂，則可以從中建立自訂映像檔和自訂套裝軟體 WorkSpace。

自訂映像僅包含的作業系統、軟體和設定 WorkSpace。自訂套裝軟體是該自訂映像檔和 WorkSpace 可從中啟動的硬體的組合。

> **Note**
>
> 請確保在刪除套裝軟體後至少等待 2 小時，然後再建立具有相同名稱的新套裝軟體。

建立自訂映像後，您可以建置自訂套件，其結合自訂映像以及您選取的基礎運算和儲存組態。然後，您可以在啟動新的時候指定此自訂套裝軟體， WorkSpaces 以確保新組態 WorkSpaces 具有相同的一致組態 (硬體和軟體)。

藉由為每個套件選取不同的運算和儲存選項，您可使用相同的自訂映像來建立各種自訂套件。

> **Important**
>
> - 如果您打算從 Windows 10 建立映像檔，請注意 WorkSpace，已從一個版本的視窗 10 升級為較新版本的視窗 10 (視窗功能/版本升級) 的 Windows 10 系統上不支援建立映像檔。不過， WorkSpaces 影像建立程序支援 Windows 累積或安全性更新。
> - 在 2020 年 1 月 14 日之後，就無法從公用 Windows 7 套件建立映像。您可能需要考慮將視窗 7 遷移 WorkSpaces 到視窗 10。如需詳細資訊，請參閱 遷移 WorkSpace。
> - 在 2023 年 11 月 30 日之後，不再支援 Graphics 套件。我們建議您移轉 WorkSpaces 至圖形 .g4dn 套裝軟體。如需詳細資訊，請參閱 遷移 WorkSpace。
> - 亞太區域 (孟買) 地區目前不提供圖形和 GraphicsPro 組合包。
> - 自訂服務包儲存磁碟區不能小於映像儲存磁碟區。

自訂套件的成本與建立來源的公用套件相同。如需有關定價的詳細資訊，請參閱 Amazon WorkSpaces 定價。

目錄

- Linux WorkSpace 自訂映像檔包含哪些內容

建立 Windows 自訂映像的需求

> **Note**
>
> Windows 目前將 1 GB 定義為 1,073,741,824 個位元組。客戶必須確保在 C 磁碟機上有超過 12,884,901,888 位元組 (或 12 GiB)，且使用者設定檔小於 10,737,418,240 位元組 (或 10 GiB)，才能建立一個映像檔。 WorkSpace

- 的狀態 WorkSpace 必須為「可用」，且其修改狀態必須為「無」。
- WorkSpaces 映像上的所有應用程式和使用者設定檔都必須與 Microsoft Sysprep 相容。
- 要包含在映像中的所有應用程式都必須安裝在 C 磁碟機上。
- 對於 Windows 7 WorkSpaces，其總大小（文件和數據）必須小於 10 GB。
- 對於 Windows 7 WorkSpaces，C磁碟機必須至少有 12 GB 的可用空間。
- 在上執行的所有應用程式服務都 WorkSpace 必須使用本機系統帳戶，而非網域使用者認證。例如，您不能使用網域使用者的認證執行 Microsoft SQL Server Express 安裝。
- 不 WorkSpace 得加密。目前不支援從加密 WorkSpace 的映像建立。
- 映像中需要下列元件。如果沒有這些元件 WorkSpaces ，您從映像啟動的功能將無法正常運作。如需詳細資訊，請參閱 the section called “必要組態”。
  - 視窗 3.0 或更新 PowerShell 版本
  - 遠端桌面服務
  - AWS 光伏驅動器
  - Windows 遠端管理 (WinRM)
  - Teradici PCoIP 代理程式和驅動程式
  - STXHD 代理程式和驅動程式
  - AWS 和 WorkSpaces 證書
  - Skylight 代理程式

建立 Linux 自訂映像的需求

- 的狀態 WorkSpace 必須為「可用」，且其修改狀態必須為「無」。

- 要包含在映像中的所有應用程式都必須安裝在使用者磁碟區 (/home 目錄) 之外。
- 根磁碟區 (/) 的填滿程序應小於 97%。
- 不 WorkSpace 得加密。目前不支援從加密 WorkSpace 的映像建立。
- 映像中需要下列元件。如果沒有這些元件 WorkSpaces ，您從映像啟動的功能將無法正常運作：
  - Cloud-init
  - Teradici PCoIP 或 WSP 代理程式和驅動程式
  - Skylight 代理程式

最佳實務

從建立影像之前 WorkSpace，請執行下列動作：

- 使用未連線到生產環境的個別 VPC。
- 在私有子網路 WorkSpace 中部署，並將 NAT 執行個體用於輸出流量。
- 使用小型 Simple AD 目錄。
- 使用來源的最小磁碟區大小 WorkSpace，然後在建立自訂套裝軟體時視需要調整磁碟區大小。
- 在. 上安裝所有作業系統更新 (Windows 功能/版本更新除外) 和所有應用程式更新。 WorkSpace如需詳細資訊，請參閱本主題開頭的重要備註。
- 刪除套件中不應包含的快取資料 (例如，瀏覽器歷程記錄、快取檔案和瀏覽器 Cookie)。 WorkSpace
- 刪除套件中不應包含的組態設定 (例如，電子郵件設定檔)。 WorkSpace
- 使用 DHCP 切換到動態 IP 地址設定。
- 請確認您沒有超過區域中允許的 WorkSpace 圖片配額。默認情況下，每個區域允許您 40 張 WorkSpace 圖像。如果您已達到此配額，建立映像的新嘗試將會失敗。若要要求提高配額，請使用WorkSpaces 限制表單。
- 確保您沒有嘗試從加密創建圖像 WorkSpace。目前不支援從加密 WorkSpace 的映像建立。
- 如果您在上執行任何防毒軟體 WorkSpace，請在嘗試建立映像時將其停用。
- 如果您啟用了防火牆 WorkSpace，請確保它沒有阻止任何必要的端口。如需詳細資訊，請參閱 的 IP 位址和連接埠需求 WorkSpaces。
- 對於 Windows WorkSpaces，請勿在建立映像之前設定任何群組原則物件 (GPO)。
- 對於 Windows WorkSpaces，請勿在建立映像之前自訂預設使用者設定檔 (C:\Users\Default)。建議您透過 GPO 對使用者設定檔進行任何自訂，並在建立映像之後套用自訂。GPO 可輕易地加以修改或回復，因此比對預設使用者設定檔進行的自訂更不容易發生錯誤。

- 對於 Linux WorkSpaces，另請參閱「為 Linux 映像準備 Amazon WorkSpaces 的最佳實踐」白皮書。
- 如果您想要在啟用 WorkSpaces 串流通訊協定 (WSP) WorkSpaces 的 Linux 上使用智慧卡，請參閱以使用智慧卡進行驗證取得在建立映像 WorkSpace 之前必須對 Linux 進行的自訂項目。
- 請務必更新網路相依性驅動程式，例如 ENA、NVMe 和 PV 驅動程式。 WorkSpaces您應該至少每 6 個月執行一次。如需詳細資訊，請參閱針對 Windows 執行個體安裝或升級彈性網路介面卡 (ENA) 驅動程式和升級 Windows 執行個體上的 PV 驅動程式。AWS NVMe 驅動程式
- 請務必定期將 EC2Config、EC2Launch 和 EC2Launch V2 代理程式更新為最新版本。您應該至少每 6 個月執行一次。如需詳細資訊，請參閱更新 EC2Config 和 EC2 啟動。

(選用) 步驟 1：指定映像的自訂電腦名稱格式

對於從您的自訂或使用您自己的授權 (BYOL) 映像 WorkSpaces 啟動的，您可以為電腦名稱格式指定自訂首碼，而不是使用預設的電腦名稱格式。若要指定自訂前置詞，請遵循適合您映像類型的程序。

若要指定自訂映像的自訂電腦名稱格式

> **Note**
>
> 根據預設，視窗 10 的電腦名稱格DESKTOP-XXXXX式 WorkSpaces 為視窗 11 WorkSpaces、WORKSPA-XXXXX.

1. 在您用來創建自定義圖像的上，`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`在記事本或其他文本編輯器中打開。 WorkSpace 如需有關使用 `Unattend.xml` 檔案的詳細資訊，請參閱 Microsoft 文件中的回應檔案 (unattend.xml)。

   > **Note**
   >
   > 若要從您的 Windows 檔案總管存取 C: 磁碟機 WorkSpace，請**`C:\`**在網址列中輸入。

2. 在 `<settings pass="specialize">` 區段中，確定 `<ComputerName>` 已設定為星號 (*)。如果 `<ComputerName>` 設定為任何其他值，則會忽略您的自訂電腦名稱設定。如需有關`<ComputerName>`設定的詳細資訊，請參閱 Microsoft 說明文件 ComputerName中的。
3. 在 `<settings pass="specialize">` 區段中，將 `<RegisteredOrganization>` 和 `<RegisteredOwner>` 設定為您偏好的值。

在 Sysprep 期間，您為 <RegisteredOwner> 和 <RegisteredOrganization> 指定的值會串連在一起，而且合併字串的前 7 個字元用於建立電腦名稱。例如，如果您指定**Amazon.comEC2**為<RegisteredOrganization>和<RegisteredOwner>，從自訂服務包 WorkSpaces 建立的電腦名稱將以 EC2AMAZ-*xxxxxxx* 開頭。

> **Note**
>
> <settings pass="oobeSystem"> 區段中的 <RegisteredOrganization> 和 <RegisteredOwner> 值會被 Sysprep 忽略。

4. 儲存您對 Unattend.xml 檔案所做的變更。

若要為 BYOL 映像指定自訂電腦名稱格式

1. 如果您使用 Windows 10，請在記事本或其他文字編輯器中開啟 C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml。如果您使用 Windows 11，請開啟 C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml。
2. 在 <settings pass="specialize"> 區段中，取消註解 <ComputerName>*</ComputerName>，並確定 <ComputerName> 已設定為星號 (*)。如果 <ComputerName> 設定為任何其他值，則會忽略您的自訂電腦名稱設定。如需有關<ComputerName>設定的詳細資訊，請參閱 Microsoft 說明文件 ComputerName中的。
3. 在 <settings pass="specialize"> 區段中，將 <RegisteredOrganization> 和 <RegisteredOwner> 設定為您偏好的值。

   在 Sysprep 期間，您為 <RegisteredOwner> 和 <RegisteredOrganization> 指定的值會串連在一起，而且合併字串的前 7 個字元用於建立電腦名稱。例如，如果您指定**Amazon.comEC2**為<RegisteredOrganization>和<RegisteredOwner>，從自訂服務包 WorkSpaces 建立的電腦名稱將以 EC2AMAZ-*xxxxxxx* 開頭。

   > **Note**
   >
   > <settings pass="oobeSystem"> 區段中的 <RegisteredOrganization> 和 <RegisteredOwner> 值會被 Sysprep 忽略。

4. 如果您使用 Windows 10，請儲存您對 Sysprep2008.xml 檔案所做的變更。如果您使用 Windows 11，請儲存您對 OOBE_unattend.xml 所做的變更。

步驟 2：執行映像檢查程式

> **Note**
>
> 影像檢查程式僅適用於 Windows WorkSpaces。如果您要從 Linux 建立映像檔 WorkSpace，請跳至步驟 3：建立自訂映像和自訂套件。

若要確認您的 Windows WorkSpace 符合建立映像檔的需求，建議您執行影像檢查程式。影像檢查程式會針對您要用來建立映像 WorkSpace 的影像執行一系列測試，並提供如何解決發現的任何問題的指引。

> **Important**
>
> - WorkSpace 必須通過映像檢查器運行的所有測試，然後才能將其用於映像創建。
> - 在執行映像檢查程式之前，請確認您已安裝最新的 Windows 安全性和累積更新 WorkSpace。

若要取得映像檢查程式，請執行下列其中一項操作：

- 重新啟動您的 WorkSpace. 映像檢查程式會在重新啟動期間自動下載並安裝於 `C:\Program Files\Amazon\ImageChecker.exe`。
- 從下載 Amazon WorkSpaces 圖像檢查器 https://tools.amazonworkspaces.com/ ImageChecker .zip `ImageChecker.exe`將此檔案複製到 `C:\Program Files\Amazon\`。

若要執行映像檢查程式

1. 開啟 `C:\Program Files\Amazon\ImageChecker.exe` 檔案。
2. 在 Amazon 影 WorkSpaces 像檢查器對話方塊中，選擇執行。
3. 每次測試完成後，您可以檢視測試的狀態。

   對於狀態為失敗的任何測試，請選擇資訊以顯示如何解決造成失敗之問題的相關資訊。如需有關如何解決這些問題的資訊，請參閱 用以解決映像檢查程式偵測到的問題的秘訣。

   如果有任何測試顯示警告狀態，請選擇修正所有警告按鈕。

此工具會在映像檢查程式所在的相同目錄中產生輸出日誌檔。此檔案的預設位置為 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`。

> **Tip**
>
> 請勿刪除此日誌檔。如果發生問題，此日誌檔可能有助於疑難排解。

4. 如果適用，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。您必須先解決所有失敗和警告，才能建立映像。
5. WorkSpace 通過所有測試後，您會看到「驗證成功」訊息。您現在可以建立自訂套件。

用以解決映像檢查程式偵測到的問題的秘訣

除了諮詢下列秘訣以解決映像檢查程式偵測到的問題之外，務必檢閱映像檢查程式日誌檔，網址為 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`。

PowerShell 必須安裝 3.0 版或更新版本

安裝最新版本的 Microsoft 視窗 PowerShell。

> **Important**
>
> 必須將 PowerShell 執行原則設 WorkSpace 定為允許RemoteSigned指令碼。若要檢查執行原則，請執行 G et-ExecutionPolicy PowerShell 命令。如果執行原則未設定為 [未受限制] RemoteSigned，或執行 S et ExecutionPolicy -ExecutionPolicy RemoteSigned 命令來變更執行原則的值。該RemoteSigned設置允許在 Amazon 上執行腳本 WorkSpaces，這是創建映像所需的。

只有 C 和 D 磁碟機可以存在

只有C和D磁碟機可以出現在用於複製影像 WorkSpace 的磁碟機上。移除所有其他磁碟機，包括虛擬磁碟機。

無法偵測到由於 Windows Update 的擱置中重新啟動

- 直到 Windows 重新啟動以完成安裝安全或累積更新，才能執行「建立映像」程序。重新啟動 Windows 以套用這些更新，並確定不需要安裝其他擱置中的 Windows 安全或累積更新。

- 不支援在從某個 Windows 10 版本升級到較新 Windows 10 版本 (Windows 功能/版本升級) 的 Windows 10 系統上建立映像。不過， WorkSpaces 影像建立程序支援 Windows 累積或安全性更新。

Sysprep 檔案必須存在且不能空白

如果您的 Sysprep 檔案有問題，請聯絡 AWS Support 中心，以修復 EC2Config 或 EC2Launch。

使用者設定檔大小必須少於 10 GB

對於視窗 7 WorkSpaces，使用者設定檔 (`D:\Users\username`) 總計必須少於 10 GB。視需要移除檔案，以減少使用者設定檔的大小。

磁碟機 C 必須有足夠的可用空間

對於 Windows 7 WorkSpaces，您必須在驅動器上至少有 12 GB 的可用空間C。視需要移除檔案以釋放磁碟機 C 上的空間。如果您收到FAILED訊息且磁碟空間超過 2GB WorkSpaces，請忽略 Windows 10。

任何服務都不能在網域帳戶下執行

若要執行「建立映像」程序，上的任何服務都無法在網域帳戶下執行。 WorkSpace 所有服務都必須在本機帳戶下執行。

若要在本機帳戶下執行服務

1. 開啟 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` 並尋找在網域帳戶下執行的服務清單。
2. 在 Windows 搜尋方塊中，輸入 **`services.msc`** 以開啟 Windows Services Manager。
3. 在登入身分之下，尋找在網域帳戶下執行的服務。(以本機系統、本機服務或網路服務形式執行的服務不會干擾映像建立。)
4. 選取在網域帳戶下執行的服務，然後依序選擇動作、內容。
5. 開啟登入索引標籤。在登入身分之下，選擇本機系統帳戶。
6. 選擇確定。

必 WorkSpace 須配置為使用 DHCP

您必須在上設定所有網路介面卡， WorkSpace 才能使用 DHCP 而非靜態 IP 位址。

若要將所有網路介面卡設定為使用 DHCP

1. 在 Windows 搜尋方塊中，輸入 **`control panel`** 以開啟「控制台」。
2. 選擇網路和網際網路。
3. 選擇網路和共用中心。
4. 選擇變更介面卡設定，然後選取介面卡。
5. 選擇變更此連線的設定。
6. 在網路索引標籤上，選取網際網路通訊協定第 4 版 (TCP/IPv4)，然後選擇內容。
7. 在網際網路通訊協定第 4 版 (TCP/IPv4) 內容對話方塊中，選取自動取得 IP 地址。
8. 選擇確定。
9. 對上的所有網路介面卡重複此程序 WorkSpace。

必須啟用遠端桌面服務

「建立映像」程序需要啟用遠端桌面服務。

若要啟用遠端桌面服務

1. 在 Windows 搜尋方塊中，輸入 **`services.msc`** 以開啟 Windows Services Manager。
2. 在名稱欄中，尋找遠端桌面服務。
3. 選取遠端桌面服務，然後依序選擇動作、內容。
4. 在一般索引標籤上，針對啟動類型選擇手動或自動。
5. 選擇確定。

使用者設定檔必須存在

您用來建立影像的使用者設定檔必須有使用者設定檔 (`D:\Users\`*`username`*)。 WorkSpace 如果測試失敗，請聯絡 AWS Support 中心尋求協助。

環境變數路徑必須設定正確

本機電腦的環境變數路徑缺少 System32 和 Windows PowerShell 的項目。執行「建立映像」時需要這些項目。

若要設定環境變數路徑

1. 在 Windows 搜尋方塊中，輸入 **`environment variables`**，然後選擇編輯系統環境變數。

2. 在系統內容對話方塊中，開啟進階索引標籤，然後選擇環境變數。
3. 在環境變數對話方塊的系統變數之下，選取路徑項目，然後選擇編輯。
4. 選擇新增，然後新增下列路徑：

   ```
   C:\Windows\System32
   ```
5. 再次選擇新增，然後新增下列路徑：

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. 選擇確定。
7. 重新啟動 WorkSpace.

> **Tip**
>
> 項目出現在環境變數路徑中的順序很重要。若要判斷正確的順序，您可能想要將您的環境變數路徑 WorkSpace 與新建立的 WorkSpace 或新 Windows 執行個體的環境變數路徑進行比較。

必須啟用 Windows Modules Installer

「建立映像」程序需要啟用 Windows Modules Installer 服務。

若要啟用 Windows Modules Installer 服務

1. 在 Windows 搜尋方塊中，輸入 **`services.msc`** 以開啟 Windows Services Manager。
2. 在名稱欄中，尋找 Windows Modules Installer。
3. 選取 Windows Modules Installer，然後依序選擇動作、內容。
4. 在一般索引標籤上，針對啟動類型選擇手動或自動。
5. 選擇確定。

必須停用 Amazon SSM Agent

「建立映像」程序需要停用 Amazon SSM Agent 服務。

若要停用 Amazon SSM Agent 服務

1. 在 Windows 搜尋方塊中，輸入 **`services.msc`** 以開啟 Windows Services Manager。

2. 在名稱欄中，尋找 Amazon SSM Agent。
3. 選取 Amazon SSM Agent，然後依序選擇動作、內容。
4. 在一般索引標籤上，針對啟動類型，選擇停用。
5. 選擇確定。

必須啟用 SSL3 和 TLS 1.2 版

若要設定 Windows 的 SSL/TLS，請參閱 Microsoft Windows 文件中的如何啟用 TLS 1.2。

只有一個使用者設定檔可以存在於 WorkSpace

您用來建立影像的使用 WorkSpaces 者設定檔 (`D:\Users\username`) 只能有一個使用者設定檔 ()。WorkSpace 刪除不屬於預定使用者的任何使用者設定檔 WorkSpace。

若要建立映像檔，您只 WorkSpace 能有三個使用者設定檔：

- WorkSpace（`D:\Users\username`）的預期用戶的用戶配置文件
- 預設使用者設定檔 (也稱為「預設設定檔」)
- 管理員使用者設定檔

如果有其他使用者設定檔，您可以透過 Windows 控制台中的進階系統內容將其刪除。

若要刪除使用者設定檔

1. 若要存取進階系統內容，請執行下列其中一項操作：
   - 按 Windows 鍵+Pause Break，然後在控制台 > 系統和安全性 > 系統對話方塊的左窗格中選擇進階系統設定。
   - 在 Windows 搜尋方塊中，輸入 **`control panel`**。在 [控制台] 中，選擇系統和安全性，然後選擇 [系統]，然後在控制台 > 系統和安全性系統 > 系統對話方塊的左窗格中選擇 進階系統設定。
2. 在系統內容對話方塊的進階索引標籤上，選擇使用者設定檔之下的設定。
3. 如果除了「管理員」設定檔、「預設設定檔」和預定 WorkSpaces使用者的設定檔以外列出任何設定檔，請選取該額外的設定檔，然後選擇「刪除」。
4. 當系統詢問您是否要刪除設定檔時，請選擇是。
5. 如有必要，請重複步驟 3 和 4 以移除不屬於的任何其他設定檔 WorkSpace。
6. 選擇確定兩次，然後關閉控制台。

7. 重新啟動 WorkSpace.

任何 AppX 套件都不能處於暫存狀態

一或多個 AppX 套件處於暫存狀態。這可能在建立映像期間造成 Sysprep 錯誤。

若要移除所有暫存 AppX 套件

1. 在 Windows 搜尋方塊中，輸入 **powershell**。選擇以管理員身分執行。
2. 當系統詢問「您要允許此應用程式對裝置進行變更嗎？」時，請選擇是。
3. 在 Windows PowerShell 視窗中，輸入下列命令以列出所有暫存的 AppX 套件，然後在每個套件之後按 Enter。

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. 輸入下列命令以移除所有暫存 AppX 套件，然後按 Enter 鍵。

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. 再次執行映像檢查程式。如果此測試仍然失敗，請輸入下列命令以移除所有 AppX 套件，並在每個套件之後按 Enter 鍵。

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows 不得從以前的版本升級

不支援在從某個 Windows 10 版本升級到較新 Windows 10 版本 (Windows 功能/版本升級) 的 Windows 系統上建立映像。

若要建立映像檔，請使 WorkSpace 用尚未進行 Windows 功能/版本升級的。

Windows 重設授權計數不得為 0

重設授權功能允許您延長 Windows 試用版的啟用期間。建立映像程序要求重設授權計數必須是 0 以外的值。

若要檢查 Windows 重設授權計數

1. 在 Windows Start (開始) 功能表，選擇 Windows System (Windows 系統)，然後選擇 Command Prompt (命令提示字元)。
2. 在命令提示視窗中，輸入以下命令，然後按 Enter 鍵。

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

若要將重設授權計數重設為 0 以外的值，請參閱 Microsoft Windows 文件中的 Sysprep (一般化) Windows 安裝。

其他疑難排解秘訣

如果您 WorkSpace 通過了 Image Checker 執行的所有測試，但仍無法從中建立映像 WorkSpace，請檢查下列問題：

- 請確定 WorkSpace 未指派給網域訪客群組中的使用者。若要檢查是否有任何網域帳戶，請執行下列 PowerShell命令。

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- WorkSpaces 僅適用於 Windows 7：如果在建立映像檔期間複製使用者設定檔時發生問題，請檢查下列問題：
  - 較長的設定檔路徑可能導致映像建立錯誤。請確定使用者設定檔內所有資料夾的路徑都少於 261 個字元。
  - 務必將設定檔資料夾的完整許可授與系統和所有應用程式套件。

  - 如果使用者設定檔中有任何檔案被處理程序鎖定或在建立映像期間正在使用中，則複製設定檔可能會失敗。
- 在 Windows 執行個體設定期間，當 EC2Config 服務或 EC2Launch 指令碼請求 RDP 憑證指紋時，有些群組政策物件 (GPO) 會限制對 RDP 憑證指紋的存取。在您嘗試建立映像之前，請先移 WorkSpace 至具有封鎖繼承且未套用 GPO 的新組織單位 (OU)。
- 請確定 Windows 遠端管理 (WinRM) 服務已設定為自動啟動。請執行下列操作：
  1. 在 Windows 搜尋方塊中，輸入 **`services.msc`** 以開啟 Windows Services Manager。
  2. 在名稱欄中，尋找 Windows 遠端管理 (WS-管理)。
  3. 選取 Windows 遠端管理 (WS-管理)，然後依序選擇動作、內容。
  4. 在一般索引標籤上，針對啟動類型，選擇自動。
  5. 選擇確定。

步驟 3：建立自訂映像和自訂套件

驗證 WorkSpace 映像後，您可以繼續建立自訂映像檔和自訂套裝軟體。

若要建立自訂映像和自訂套件

1. 如果您仍然連線到 WorkSpace，請在用 WorkSpaces 戶端應用程式中選擇 Amazon WorkSpaces 並中斷連線來中斷連線。
2. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
3. 在導覽窗格中，選擇 WorkSpaces。
4. 選取 WorkSpace 以開啟其詳細資訊頁面，然後選擇 [建立映像]。如果狀態 WorkSpace 為 [已停止]，您必須先啟動它 (選擇 [動作]、[啟動] WorkSpaces)，然後才能選擇 [動作] > [建立映像]。

   > **Note**
   >
   > 若要以程式設計方式建立映像，請使用 CreateWorkspaceImage API 動作。如需詳細資訊，請 CreateWorkspaceImage參閱 Amazon WorkSpaces API 參考中的。

5. 將顯示一條消息，提示您 WorkSpace在繼續之前重新啟動（ 重新啟動 ）。重新啟動您的 Amazon WorkSpaces 軟件 WorkSpace 更新到最新版本。

   關閉訊息並遵循中的步驟，以重新啟動您的 WorkSpace 重新啟動 a WorkSpace。完成後，請重複此程序的Step 4，但這次在重新啟動訊息出現時選擇下一步。若要建立映像，的狀態 WorkSpace 必須為「可用」，且其修改狀態必須為「無」。

6. 輸入映像名稱和描述以協助您識別映像，然後選擇建立映像。在建立映像時，狀態為「 WorkSpace 已暫停」，且無 WorkSpace 法使用。

> **Note**
>
> 輸入圖片描述時，請確保您沒有使用特殊字符「-」，否則您將收到錯誤信息。

7. 在導覽窗格中，選擇映像。當狀態 WorkSpace 變更為 [可用] 時，影像即完成 (最多可能需要 45 分鐘)。
8. 選取映像，然後依序選擇動作、建立套件。

> **Note**
>
> 若要以程式設計方式建立套件，請使用 CreateWorkspaceBundle API 動作。如需詳細資訊，請參閱 Amazon WorkSpaces API 參考資料 CreateWorkspaceBundle中的。

9. 輸入套件名稱和描述，然後執行以下操作：

   - 針對「套裝軟體」硬體類型，選擇 WorkSpaces 從此自訂套裝軟體啟動時要使用的硬體。
   - 針對儲存設定，選取根磁碟區和使用者磁碟區大小的預設組合之一，或選取自訂，然後輸入根磁碟區大小和使用者磁碟區大小的值 (最大 2000 GB)。

     根磁碟區 (Microsoft Windows 為 C 磁碟機，而 Linux 為 /) 和使用者磁碟區 (Windows 為 D 磁碟機，而 Linux 為 /home) 的預設可用大小組合如下所示：

     - 根磁碟機：80 GB，使用者：10 GB、50 GB 或 100 GB
     - 根磁碟機：175 GB，使用者：100 GB
     - 僅適用於圖形 GraphicsPro .g4dn、圖形和 GraphicsPro WorkSpaces 僅限根目錄：100 GB，使用者：100 GB

     或者，您可以將根磁碟區和使用者磁碟區擴充為每個 2000 GB。

> **Note**
>
> 若要確保您的資料得以保留，您無法在啟動之後減少根磁碟區或使用者磁碟區的大小 WorkSpace。相反地，請務必在啟動時指定這些磁碟區的最小大小 WorkSpace。您可以啟動「值」、「標準」、「效能」、「電源」，或 PowerPro WorkSpace 啟動根磁碟區至少為 80 GB，使用者磁碟區啟動 10 GB。您可以啟動圖形 .g4dn、

GraphicsPro .g4dn、圖形，或者根磁碟區至少為 100 GB， GraphicsPro WorkSpace 使用者磁碟區的使用者磁碟區至少為 100 GB。

10. 選擇建立套件。
11. 若要確認您的套件已建立，請選擇套件並確認已列出該套件。

什麼是包含在視窗 WorkSpaces 自定義圖像

當您從視窗 7、視窗 10 或視窗 11 創建映像時 WorkSpace，C驅動器的全部內容都包括在內。

對於 Windows 10 或 11 WorkSpaces，中的使用者設定檔`D:\Users\username`不會包含在自訂映像中。

對於 Windows 7 WorkSpaces，除了下列項目外，其中`D:\Users\username`包含使用者設定檔的全部內容：

- 聯絡人
- 下載
- 音樂
- 圖片
- 儲存的遊戲
- 影片
- Podcast
- 虛擬機器
- .virtualbox
- 追蹤
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\

- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Linux WorkSpace 自訂映像檔包含哪些內容

當您從 Amazon Linux 建立映像檔時 WorkSpace，會移除使用者磁碟區 (/home) 的全部內容。除了下列已移除的適用資料夾和金鑰之外，包含根磁碟區 (/) 的內容：

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules

- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/ /用AccountsService戶

在建立自訂映像期間，下列金鑰會被銷毀：

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

更新自訂 WorkSpaces 套件

您可以修改以套件為基礎的 WorkSpace，從 WorkSpace 建立映像，以及使用新映像來更新套件，進而更新現有的自訂 WorkSpaces 套件。然後，您可以使用更新的套件來啟動新的 WorkSpaces。

> **Important**
>
> 當您更新現有 WorkSpaces 所依據的套件時，不會自動更新現有 WorkSpaces。若要更新以您已更新的套件為基礎的現有 WorkSpaces，您必須重新建置 WorkSpaces 或刪除並重新建立它們。

使用主控台更新套件

1. 連線至以套件軟體為基礎的 WorkSpace，並進行您想要的變更。例如，您可以套用最新的作業系統和應用程式修補程式，並安裝其他應用程式。

   或者，您可使用與用於建立套件的映像相同的基礎軟體套件 (增強或標準) 來建立新的 WorkSpace，並進行變更。
2. 如果您仍然連線至 WorkSpace，請在 WorkSpaces 用戶端應用程式中選擇 Amazon WorkSpaces 和中斷連線來中斷連線。
3. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
4. 在導覽窗格中，選擇 WorkSpaces。
5. 選取 WorkSpace，然後選擇動作、建立映像。如果 WorkSpace 的狀態為 STOPPED，您必須先加以啟動 (選擇動作、啟動 WorkSpaces)，然後才能選擇動作、建立映像。
6. 輸入映像名稱和描述，然後選擇建立映像。正在建立映像時，無法使用 WorkSpace。如需映像建立程序的詳細資訊，請參閱 建立自訂 WorkSpaces 映像檔和套裝軟體。
7. 在導覽窗格中，選擇套件。
8. 選擇套件以開啟其詳細資訊頁面，然後在來源映像之下選擇編輯。
9. 在更新來源映像頁面上，選取您建立的映象，然後選擇更新套件。
10. 視需要重新建置 WorkSpaces 或予以刪除並重新建立，以便更新以套件為基礎的任何現有 WorkSpaces。如需詳細資訊，請參閱 重建 WorkSpace。

以程式設計方式更新套件

若要以程式設計方式更新套件，請使用 UpdateWorkspaceBundle API 動作。如需詳細資訊，請參閱《Amazon WorkSpaces API 參考》中的 UpdateWorkspaceBundle。

複製自訂 WorkSpaces 映像

您可以在 AWS 區域內或跨區域複製自訂 WorkSpaces 映像。複製映像就會建立具有自己唯一識別符的相同映像。

只要目的地區域已啟用自帶授權 (BYOL)，您就可以將 BYOL 映像複製到其他區域。確定已針對所有相關帳戶和區域啟用 BYOL。

> **Note**
>
> 在中國 (寧夏) 區域，您只能複製相同區域內的映像。

在 AWS GovCloud (US) Region 中，若要將映像複製到其他 AWS 區域或從中複製映像，請聯絡 AWS 支援。
在選擇加入區域中，若要將映像複製到其他區域，請聯絡 AWS 支援。如需選擇加入區域的詳細資訊，請參閱可用區域。

您也可以複製其他 AWS 帳戶與您共用的映像。如需共用映像的詳細資訊，請參閱 共用或取消共用自訂 WorkSpaces 映像。

在區域內或跨區域複製映像無須額外收費。不過會套用目的地區域中映像數量的配額。如需 Amazon WorkSpaces 配額的詳細資訊，請參閱 Amazon WorkSpaces 配額。

複製映像的 IAM 許可

若您使用 IAM 使用者來複製映像，該使用者必須具備 `workspaces:DescribeWorkspaceImages` 和 `workspaces:CopyWorkspaceImage` 的許可。

下列範例政策允許使用者將指定的映像複製到指定區域中的指定帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

如果您要建立 IAM 政策，以便替未擁有映像的帳戶複製共用映像，則無法在 ARN 中指定帳戶 ID。您必須針對帳戶 ID 使用 *，如以下範例政策所示。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

只有當該帳戶擁有要複製的映像時，您才可以在 ARN 中指定帳戶 ID。

如需使用 IAM 的詳細資訊，請參閱 適用於 WorkSpaces 的身分和存取管理。

大量複製映像

您可以使用主控台來逐一複製映像。若要大量複製映像，請使用 CopyWorkspaceImage API 操作或 AWS Command Line Interface (AWS CLI) 中的 copy-workspace-image 命令。如需詳細資訊，請參閱《Amazon WorkSpaces API 參考》中的 CopyWorkspaceImage，或參閱《AWS CLI 命令參考》中的 copy-workspace-image。

Important

複製共用映像之前，務必確認已從正確的 AWS 帳戶共用該映像。若要判斷映像是否已共用以及查看擁有映像的 AWS 帳戶 ID，請使用 DescribeWorkSpaceImages 和 DescribeWorkspaceImagePermissions API 操作或 AWS CLI 中的 describe-workspace-images 和 describe-workspace-image-permissions 命令。

若要使用主控台複製映像

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇映像。
3. 選取快照，然後依序選擇動作、複製。

4. 在選取目的地中，選取要將映像複製到的目標 AWS 區域。
5. 在複製的名稱中，輸入所複製映像的新名稱，然後針對描述輸入所複製映像的描述。
6. (選用) 在標籤下，輸入所複製映像的標籤。如需更多詳細資訊，請參閱 標記 WorkSpaces 資源。
7. 選擇複製映像。

共用或取消共用自訂 WorkSpaces 映像

您可以在相同的 AWS 區域內跨 AWS 帳戶共用自訂 WorkSpaces 映像。共用映像之後，收件者帳戶可視需要將映像複製到其他 AWS 區域。如需複製映像的詳細資訊，請參閱 複製自訂 WorkSpaces 映像。

> **Note**
>
> 在中國 (寧夏) 區域，您只能複製相同區域內的映像。
> 在 AWS GovCloud (US) Region中，若要將映像複製到其他 AWS 區域或從中複製映像，請聯絡 AWS 支援。

共用映像無須額外收費。不過會套用 AWS 區域中映像數量的配額。直到收件者複製映像，共用的映像才會計入收件者帳戶的配額。如需 Amazon WorkSpaces 配額的詳細資訊，請參閱 Amazon WorkSpaces 配額。

若要刪除共用的映像，您必須先取消共用映像，才能加以刪除。

共用自帶授權映像

您只能與啟用 BYOL 的 AWS 帳戶共用自帶授權 (BYOL) 映像。您要與其共用 BYOL 映像的 AWS 帳戶也必須是您組織的一部分 (在相同的付款人帳戶下)。

> **Note**
>
> AWS GovCloud (美國西部) 和 AWS GovCloud (美國東部) 區域目前不支援跨 AWS 帳戶共用 BYOL 映像。若要跨 AWS GovCloud (美國西部) 和 AWS GovCloud (美國東部) 區域中的帳戶共用 BYOL 映像，請聯絡 AWS 支援。

與您共用的映像

如果與您共用映像，您可以複製它們。接著，您可使用共用映像的複本來建立套件，以便啟動新的 WorkSpaces。

> **Important**
>
> 複製共用映像之前，務必確認已從正確的 AWS 帳戶共用該映像。若要以程式設計方式判斷映像是否已共用，請使用 DescribeWorkSpaceImages 和 DescribeWorkspaceImagePermissions API 操作，或在 AWS 命令列介面 (CLI) 中使用 describe-workspace-images 和 describe-workspace-image-permissions 命令。

針對與您共用的映像所顯示的建立日期是映像的最初建立日期，而不是與您共用映像的日期。

如果與您共用映像，您就無法與其他帳戶進一步共用該映像。

共用映像

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇映像。
3. 選擇映像以開啟其詳細資訊頁面。
4. 在映像詳細資訊頁面的共用的帳戶區段中，選擇新增帳戶。
5. 在新增帳戶頁面的新增要共用的帳戶底下，輸入您要與其共用映像之帳戶的帳戶 ID。

   > **Important**
   >
   > 共享映像之前，請確認您共用的 AWS 帳戶 ID 是正確的。

6. 選擇共用映像。

   > **Note**
   >
   > 若要使用共用的映像，收件者帳戶必須先複製映像。接著，收件者帳戶可以使用共用映像的複本來建立套件，以便啟動新的 WorkSpaces。

停止共用映像

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/。

2. 在導覽窗格中，選擇映像。
3. 選擇映像以開啟其詳細資訊頁面。
4. 在映像詳細資訊頁面的共用的帳戶區段中，選取您要停止共用的 AWS 帳戶，然後選擇取消共用。
5. 當系統提示您確認取消共用映像時，請選擇取消共用。

> **Note**
>
> 如果要在取消共用映像後刪除該映像，您必須先從共用該映像的所有帳戶中取消共用該映像。

如果您停止共用映像，收件者帳戶無法再複製映像。不過，已存在於收件者帳戶中共用映像的任何複本都會保留在該帳戶中，而且可以從這些複本啟動新的 WorkSpaces。

以程式設計方式共用或取消共用映像

若要以程式設計方式共用或取消共用映像，請使用 UpdateWorkspaceImagePermission API 操作或 update-workspace-image-permission AWS Command Line Interface (AWS CLI) 命令。若要判斷映像是否已共用，請使用 DescribeWorkspaceImagePermissions API 操作或 describe-workspace-image-permissions CLI 命令。

刪除自訂 WorkSpaces 套裝軟體或影像

您可以視需要刪除未使用的自訂套件或自訂映像。

刪除套件

若要刪除套裝軟體，您必須先刪除以套裝軟體 WorkSpaces 為基礎的所有套裝軟體。

若要使用主控台刪除套件

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇套件。
3. 選取套件，然後選擇刪除。
4. 出現確認提示時，請選擇刪除。

若要以程式設計方式刪除套件

若要以程式設計方式刪除套件，請使用 DeleteWorkspaceBundle API 動作。如需詳細資訊，請 DeleteWorkspaceBundle參閱 Amazon WorkSpaces API 參考中的。

> **Note**
>
> 請確保在刪除套裝軟體後至少等待 2 小時，然後再建立具有相同名稱的新套裝軟體。

刪除映像

刪除自訂套件後，您可以刪除用於建立或更新套件的映像。

若要刪除映像，您必須先刪除與該映像相關聯的任何套件，或者必須更新這些套映以使用其他來源映像。如果映像與其他帳戶共用，您也必須取消共用該映像。映像也不能處於待定或驗證中狀態。

若要使用主控台刪除映像

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇映像。
3. 選取映像，然後選擇刪除。
4. 出現確認提示時，請選擇刪除。

若要以程式設計方式刪除映像

若要以程式設計方式刪除映像，請使用 DeleteWorkspaceImage API 動作。如需詳細資訊，請 DeleteWorkspaceImage參閱 Amazon WorkSpaces API 參考中的。

自帶 Windows 桌上型電腦授權

如果您與 Microsoft 的授權合約允許，您可以在您的 WorkSpaces. 若要這麼做，您必須啟用自帶授權 (BYOL)，並提供符合下列需求的 Windows 10 或 11 授權。如需有關在上使用 Microsoft 軟體的詳細資訊 AWS，請參閱 Amazon Web Services 和 Microsoft。

若要遵守 Microsoft 授權條款，請在雲端專屬於您的硬體 WorkSpaces上 AWS 執行 BYOL。 AWS 使用自己的授權，您可以為使用者提供一致的體驗。如需詳細資訊，請參閱WorkSpaces 定價。

> **Important**
>
> 已從一個版本的視窗 10 或 11 升級到較新版本的視窗 10 或 11 (視窗功能/版本升級) 的系統上，不支援建立映像檔。不過， WorkSpaces 影像建立程序支援 Windows 累積或安全性更新。

目錄

要求

開始之前，確認下列事項：

- 您的 Microsoft 授權合約允許在虛擬託管環境中執行 Windows。
- 如果您要使用未啟用 GPU 的套裝軟體 (圖形 .g4dn、 GraphicsPro .g4dn、圖形和以外的套裝軟體 GraphicsPro)，請確認您將在每個區域使用至少 100 個。 WorkSpaces 這些 100 WorkSpaces 可以是 AlwaysOn 和的任何混合 AutoStop WorkSpaces。 WorkSpaces 在專用硬體上執行您的需求， WorkSpaces 每個區域至少使用 100 個。您必須 WorkSpaces 在專用硬體上執行，才能符合 Microsoft 授權需求。專用硬體會在 AWS 側邊佈建，因此您的 VPC 可以維持預設租用。

如果您計劃使用已啟用 GPU (Graphics.g4dn、 GraphicsPro .g4dn、圖形和 GraphicsPro) 服務包，請確認您每月在專用硬體上至少要在某個區域中執行啟用 4 AlwaysOn 或 20 AutoStop 個 GPU。WorkSpaces

> **Note**
>
> - 此時只能為 PCoIP 通訊協定建立圖形 GraphicsPro .g4dn、.g4dn、圖形和 GraphicsPro 套裝軟體。
> - 在 2023 年 11 月 30 日之後，不再支援 Graphics 套件。我們建議您移轉 WorkSpaces 至圖形 .g4dn 套裝軟體。如需詳細資訊，請參閱 遷移 WorkSpace。
> - 亞太區域 (孟買) 地區目前不提供圖形和 GraphicsPro 組合包。
> - 非洲 (開普敦) 地區目前不提供圖形 GraphicsPro .g4dn、.g4dn、繪圖卡和 GraphicsPro 套件組合。
> - 要 WorkSpaces 在非洲（開普敦）地區運行，您必須 WorkSpaces 在非洲（開普敦）地區至少運行 400 人。
> - Windows 11 套件只能針對 WSP 協定建立。
> - 圖形 .g4dn 和 GraphicsPro .g4dn 套裝軟體目前不適用於視窗 11。
> - 視窗 11 不支援圖形和 GraphicsPro 套裝軟體。
> - 超值套件不適用於 Windows 11。若要取得有關移轉現有值套件的更多資訊，WorkSpaces 請參閱遷移 WorkSpace。
> - 為了獲得最佳的視頻會議體驗，我們建議使用 Power 或 PowerPro 捆綁
> - Windows 11 需要整合可延伸韌體介面 (UEFI) 開機模式才能運作。請務必將選用`--boot-mode`參數指定為 UEFI，以便成功匯入虛擬機器。

- WorkSpaces 可以使用 /16 IP 位址範圍內的管理介面。管理介面連接至用於互動式串流的安全 WorkSpaces 管理網路。這允許 WorkSpaces 管理您的 WorkSpaces. 如需詳細資訊，請參閱 網路介面。您必須為此目的，從下列至少一個 IP 地址址範圍中保留一個 /16 網路遮罩：
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

> **Note**
>
> - 當您採用 WorkSpaces 服務時，可用的管理介面 IP 位址範圍會經常變更。若要判斷目前可用的範圍，請執行 list-available-management-cidr- range AWS Command Line Interface (AWS CLI) 指令。
> - 除了您選取的 /16 CIDR 區塊之外，54.239.224.0/20 IP 位址範圍還用於所有區域中的管理介面流量。 AWS

- 確保你已經打開了必要的管理界面端口 Microsoft 視窗和 Microsoft 辦公室 KMS 激活 BYO WorkSpaces L。如需詳細資訊，請參閱 管理介面連接埠。
- 您具有執行支援 64 位元版本的 Windows 的虛擬機器 (VM)。如需支援的版本清單，請參閱本主題中的下一節：BYOL 支援的 Windows 版本。VM 必須也符合下列需求：
  - Windows 作業系統必須針對您的金鑰管理伺服器啟動。
  - Windows 作業系統必須以英文 (美國) 作為主要語言。
  - 無法在 VM 上安裝超出 Windows 隨附的軟體。您可以在稍後建立自訂映像檔時新增其他軟體，例如防毒解決方案。
  - 建立映像之前，請勿自訂預設使用者設定檔 (`C:\Users\Default`) 或進行其他自訂。應在建立映像後進行所有自訂。建議您透過群組政策物件 (GPO) 對使用者設定檔進行任何自訂，並在建立映像之後套用自訂。這是因為透過 GPO 完成的自訂可以輕易修改或回復，而且比對預設使用者設定檔進行的自訂更不容易發生錯誤。
  - 您必須先建立具有本機管理員存取權的 WorkSpaces_BYOL 帳戶，才能共用映像。稍後可能需要此帳戶的密碼，所以請記下密碼。
  - 虛擬機器必須位於大小上限為 70 GB 且至少有 10 GB 可用空間的單一磁碟區上。如果您也打算訂閱 Microsoft Office 以取得您的 BYOL 映像，則虛擬機器必須位於大小上限為 70 GB 且至少有 20 GB 可用空間的單一磁碟區上。根磁碟區所在的磁碟不能超過 70GB。
  - 您的虛擬機器必須執行 Windows 4 或更新 PowerShell 版本。
- 在 步驟 3：在 Windows 虛擬機器上執行 BYOL 檢查程式 PowerShell 指令碼 中執行 BYOL 檢查程式指令碼之前，請確定您已安裝最新的 Microsoft Windows 修補程式。

> **Note**
>
> - 對於 BYOL AutoStop WorkSpaces，大量並行登入可能會大幅增加可用的時間 WorkSpaces 。如果您希望有許多用戶同時登錄您的 BYOL AutoStop WorkSpaces ，請諮詢您的客戶經理以獲取建議。
> - 匯入程序不支援加密的 AMI。確保您停用用於建立 EC2 AMI 的執行個體具有 EBS 加密。在佈建最終版 WorkSpaces 本之後，可以啟用加密。

BYOL 支援的 Windows 版本

您的虛擬機器必須執行下列其中一個 Windows 版本：

- Windows 10 版本 21H2 (2021 年 12 月更新)
- Windows 10 版本 22H2 (2022 年 11 月更新)
- 視窗 10 企業有限公司 2019 (1809)
- 視窗 10 企業有限公司 2021 年上半年
- 視窗 11 企業下半年二十三月 (2023 年 10 月版本)
- 視窗 11 企業 22 下半年 (2022 年 10 月版本)

所有支援的作業系統版本都支援您使用的 AWS 區域中所有可用的運算類型 WorkSpaces。不保證不再受 Microsoft 支援的 Windows 版本可以正常運作，也不會受到支援的 Sup AWS port。

> **Note**
>
> Windows 10 N 和 Windows 11 N 版本目前不支援 BYOL。

將 Microsoft Office 新增到您的 BYOL 映像

在 BYOL 映像擷取過程中，如果您使用的是視窗 10，您可以選擇透過訂閱 Microsoft 辦公室專業版 2016 (32 位元) 或 2019 年 (64 位元)。 AWS如果您使用的 Windows 11，您可以訂閱 Microsoft Office 專業版 2019 (64 位元)。如果您選擇其中一個選項，Microsoft Office 會預先安裝在您的 BYOL 映像中，並包含在您從此映像啟動 WorkSpaces 的任何選項中。

如果您選擇透過訂閱 Office AWS，則需要支付額外費用。如需詳細資訊，請參閱WorkSpaces 定價。

Important

- 如果您用來建立 BYOL 映像的虛擬機器上已安裝 Microsoft Office，如果您想要透過訂閱 Office，則必須從虛擬機器解除安裝該虛擬機器。 AWS
- 如果您打算透過訂閱 Office AWS，請確定您的虛擬機器至少有 20 GB 的可用磁碟空間。
- 在映像匯入期間，您可以訂閱 Office 2016 或 2019，但無法訂閱 Office 2021。對於 Office 2021 和其他應用程式，如 Microsoft Visio 2021 和 Microsoft Project 2021，請參閱管理應用程式。
- 若要在 Amazon 上為基於瀏覽器和桌面應用程式使用自己的 Microsoft 365 授權 WorkSpaces，請在 BYOL 映像擷取程序完成後，在 BYOL 映像檔上安裝 Microsoft 365 應用程式。

Note

圖形. G4dn 和 GraphicsPro .g4dn 自攜影像僅支援辦公室 2019，不支援辦公室 2016。

如果您選擇訂閱 Office，BYOL 映像擷取程序至少需要 3 小時。

如需在 BYOL 擷取過程中訂閱 Office 的詳細資訊，請參閱 步驟 6：使用主控台建立 BYOL 映像 WorkSpaces 。

Office 語言設定

我們會根據您執行 BYOL 映像擷取的 AWS 區域，選擇 Office 訂閱所使用的語言。例如，如果您要在亞太 (東京) 區域執行 BYOL 映像擷取，您的 Office 訂閱會以日文做為其語言。

根據預設，我們會在您的 WorkSpaces. 如果未安裝您想要的語言套件，您可以從 Microsoft 下載其他語言套件。如需詳細資訊，請參閱 Microsoft 文件中的 Office 語言配件套件。

若要變更 Office 的語言，您有幾個選項：

選項 1：允許個別使用者自訂其 Office 語言設定

個別使用者可以在其上調整 Office 語言設定 WorkSpaces。如需詳細資訊，請參閱 Microsoft 文件中的新增編輯或撰寫語言或在 Office 中設定語言偏好設定。

選項 2：使用 GPO 系統管理範本 (.admx/.adml) 為所有使用者強制執行預設的 Office 語言設定 WorkSpaces

您可以使用群組原則物件 (GPO) 設定，為您的使用 WorkSpaces 者強制執行預設 Office 語言設定。

> **Note**
>
> 您的 WorkSpaces 使用者將無法覆寫透過 GPO 強制執行的語言設定。

如需有關使用 GPO 來設定 Office 語言的詳細資訊，請參閱 Microsoft 文件中的自訂 Office 語言安裝與設定。Office 2016 和 Office 2019 使用相同的 GPO 設定 (標示為 Office 2016)。

若要處理 GPO，您必須安裝 Active Directory 管理工具。如需使用 Active Directory 管理工具來處理 GPO 的相關資訊，請參閱 設定 WorkSpaces 的 Active Directory 管理工具。

您必須先從 Microsoft 下載中心下載 Office 的管理範本檔案 (.admx/.adml)，才能設定 Office 2016 或 Office 2019 政策設定。下載系統管理範本檔案之後，您必須將`office16.admx`和`office16.adml`檔案新增至 WorkSpaces 目錄的網域控制站的中央存放區。(`office16.admx` 和 `office16.adml` 檔案適用於 Office 2016 和 Office 2019。) 如需使用 `.admx` 和 `.adml` 檔案的相關資訊，請參閱 Microsoft 文件中的如何在 Windows 中建立和管理群組政策管理範本的中央存放區。

下列程序說明如何建立中央存放區並將管理範本檔案新增到中央存放區。對加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體執行下 WorkSpaces 列程序。

若要安裝 Office 的群組政策管理範本檔案

1. 從 Microsoft 下載中心下載 Office 的管理範本檔案 (.admx/.adml)。
2. 在加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體上，開啟 Windows 檔案總管，然後在網址列中輸入組織的完整網域名稱 (FQDN)，例如。 WorkSpaces `\\example.com`
3. 開啟 `SYSVOL` 資料夾。
4. 開啟具有 *`FQDN`* 名稱的資料夾。
5. 開啟 `Policies` 資料夾。您現在應該在 `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies` 中。
6. 如果它不存在，請建立名為 `PolicyDefinitions` 的資料夾。
7. 開啟 `PolicyDefinitions` 資料夾。
8. 將 `office16.admx` 檔案複製到 `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions` 資料夾中。

9. 在 PolicyDefinitions 資料夾中建立名為 en-US 的檔案。
10. 開啟 en-US 資料夾。
11. 將 office16.adml 檔案複製到 *FQDN*\SYSVOL*FQDN*\Policies\PolicyDefinitions\en-US 資料夾中。

若要設定 Office 的 GPO 語言設定

1. 在加入目錄的目錄管理 WorkSpace 或 Amazon EC2 執行個體上 WorkSpaces ，開啟群組原則管理工具 (gpmc.msc)。
2. 展開樹系 (樹系：***FQDN***)。
3. 展開網域。
4. 展開您的 FQDN (例如，example.com)。
5. 選取您的 FQDN、開啟內容 (滑鼠右鍵) 功能表，或開啟動作功能表，然後選擇在此網域建立 GPO 並連結到此處。
6. 為您的 GPO 命名 (例如，**Office**)。
7. 選取 GPO、開啟內容 (滑鼠右鍵) 功能表或開啟動作功能表，然後選擇編輯。
8. 在群組政策管理編輯器中，選擇使用者設定、政策、從本機電腦擷取的管理範本政策定義 (ADMX 檔案)、Microsoft Office 2016 和語言偏好設定。

   > **Note**
   >
   > Office 2016 和 Office 2019 使用相同的 GPO 設定 (標示為 Office 2016)。如果您在使用者設定、政策 之下看不到從本機電腦擷取的管理範本政策定義 (ADMX 檔案)，則網域控制站上未正確安裝 office16.admx 和 office16.adml 檔案。

9. 在語言偏好設定之下，針對下列設定指定您想要的語言。請務必將每個設定設為已啟用，然後在選項之下選取您想要的語言。選擇確定以儲存每個設定。
   - 顯示語言 > 顯示說明的語言
   - 顯示語言 > 顯示功能表和對話方塊的語言
   - 編輯語言 > 主要編輯語言
10. 完成後關閉群組政策管理工具。
11. 群組原則設定變更會在下一次群組原則更新後生效，以 WorkSpace 及 WorkSpace 工作階段重新啟動之後。若要套用群組政策變更，請執行下列其中一項：

- 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）。
- 在管理命令提示中輸入 gpupdate /force。

選項 3：更新您的 Office 語言登錄設定 WorkSpaces

若要透過登錄設定 Office 語言設定，請更新下列登錄設定：

- HKEY_ 當前用戶\ 軟件\ Microsoft\ 辦公室\ 16.0\ 常用\\ 設置 LanguageResources
- 目前使用者\ 軟體\ Microsoft\ 辦公室\ 16.0\ 通用\\ LanguageResources HelpLanguage

針對這些設定，新增具有適當 Office 地區設定 ID (LCID) 的 DWORD 金鑰值。例如，英文 (美國) 的 LCID 是 1033。由於 LCID 是十進位值，因此您必須將 DWORD 值的基礎選項設定為十進位。如需辦公室 LCID 的清單，請參閱 Microsoft 文 OptionState 件中的 Office 2016 中的語言識別碼和識別碼值。

您可以透 WorkSpaces 過 GPO 設定或登入指令碼，將這些登錄設定套用至您。

如需有關處理 Office 語言設定的詳細資訊，請參閱 Microsoft 文件中的自訂 Office 語言安裝與設定。

將辦公室新增至您現有的 BYOL WorkSpaces

您也可以執行下列動作，將 Office 的訂閱新增至您現有的 BYOL WorkSpaces 。

- 管理應用程式 (建議)-您可以安裝和設定 Microsoft 辦公室、Microsoft Visio 或 Microsoft 專案 2021 在您現有 WorkSpaces的. 如需詳細資訊，請參閱管理應用程式。
- 移轉 WorkSpace-安裝 Office 的 BYOL 套裝軟體之後，您可以使用 WorkSpaces 移轉功能將現有的 BYOL WorkSpaces 移轉至已訂閱 Office 的 BYOL 服務包。如需詳細資訊，請參閱 遷移 WorkSpace。

> **Note**
>
> 管理應用程序選項可用於安裝 Microsoft 辦公室 2021 和其他應用程序, 如 Microsoft Visio 2021 和 Microsoft 項目 2021 到你 WorkSpaces. 要安裝 Microsoft 辦公室 2016 或 2019 在您的 WorkSpaces，請使用遷移 WorkSpace。

在 Microsoft Office 版本之間遷移

若要從 Microsoft Office 版本遷移到另一個版本，您有下列選項：

- 管理應用程式 (建議使用) — 您可以解除安裝原始的 Office 版本，並安裝 Office 2021 和其他應用程式，例如 Microsoft Visio 2021 和 Microsoft 專案 2021，在您現有 WorkSpaces的。例如，若要從 Microsoft Office 2019 遷移到 Microsoft Office 2021，請使用管理應用程式工作流程來解除安裝 Microsoft Office 2019 並安裝 Microsoft Office 2021。如需詳細資訊，請參閱管理應用程式。
- 遷移 WorkSpace-從 Microsoft 辦公軟件 2016 遷移到 Microsoft 辦公室 2019 或從 Microsoft 辦公軟件 2019 年遷移到 Microsoft 辦公室 2016，您必須創建一個 BYOL 捆綁，訂閱您要遷移到的辦公室版本。然後，使用 WorkSpaces 移轉功能，將訂閱 Office 的現有 BYOL WorkSpaces 移轉至訂閱您要移轉至的 Office 版本的 BYOL 服務包。例如，從 Microsoft 辦公室 2016 遷移到 Microsoft 辦公室 2019，創建一個訂閱 Microsoft 辦公室 2019 的自攜服務包。然後使用 WorkSpaces 移轉功能，將訂閱 Office 2016 的現有自攜 WorkSpaces 裝置，移轉至訂閱 Office 2019 的自攜服務包。如需詳細資訊，請參閱移轉 WorkSpace.

您可以使用這些選項將您 WorkSpaces 的訂閱 Microsoft 辦公室通過 Microsoft 365 應 AWS 用程序遷移。但是，管理應用程序僅限於從您的 WorkSpace. 您必須攜帶自己的工具和安裝程式 Microsoft 才能在您的 WorkSpaces.

> **Note**
>
> 使用管理應用程序，您可以安裝或卸載 Microsoft 辦公室，Microsoft Visio，或 MicrosoftProject 2021 在您 WorkSpaces的. 對於 Microsoft 辦公室 2016 或 2019 版本，您只能將它們從您的 WorkSpaces. 要安裝 Microsoft 辦公室 2016 或 2019 在您的 WorkSpaces, 遷移 WorkSpace.

如需遷移程序的詳細資訊，請參閱 遷移 WorkSpace。

取消訂閱 Office

若要取消訂閱 Office，您有下列選項。

- 管理應用程序（推薦）-您可以卸載 Microsoft Office 和其他應用程序，如 Microsoft Visio 和 Microsoft 項目從您 WorkSpaces的. 如需詳細資訊，請參閱管理應用程式。

- 移轉 WorkSpace-您可以建立未訂閱 Office 的 BYOL 套裝軟體。然後使用 WorkSpaces 移轉功能將現有的 BYOL 移轉 WorkSpaces 至未訂閱 Office 的 BYOL 服務包。如需詳細資訊，請參閱 遷移 WorkSpace。

Office 更新

如果您已經透過訂閱 Office AWS，Office 更新會包含在一般 Windows 更新中。為了保持所有安全性修補程式和更新的最新狀態，我們建議您定期更新 BYOL 基礎映像。

步驟 1：使用 Amazon 主控台檢查您的帳戶是否符合 BYOL 的資格 WorkSpaces

您必須先進行驗證程序以確認您符合 BYOL 的資格，才能針對 BYOL 啟用您的帳戶。在您完成此程序之前，Amazon WorkSpaces 主控台中將無法使用「啟用 BYOL」選項。

> **Note**
>
> 驗證過程至少需要一個工作日。如果您要將現有 AWS 帳戶的 CIDR 範圍和 BYOL 組態套用到另一個帳戶，您可以將它們連結在一起，以使用相同的基礎硬體。若要連結您的 AWS 帳戶，您不需要提交支援票證。您可以使用 API，例如 CreateAccountLinkInvitations和AcceptAccountLinkInvitation來連接您的 AWS 帳戶。如需詳細資訊，請參閱 連結自攜裝置帳戶。

使用 Amazon 主控台檢查您的帳戶是否符合 BYOL 的資格 WorkSpaces

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在功能窗格中，選擇 [帳戶設定]，然後在 [使用您自己的授權 (BYOL)] 下，選擇 [檢視 WorkSpaces B YOL 設定]。如果您的帳戶目前不符合 BYOL 的資格，則有訊息提供後續步驟的指引。若要開始使用，請聯絡您的 AWS 客戶經理或銷售代表，或聯絡中AWS Support 心。您的聯絡人將驗證您是否符合 BYOL 的資格。

   若要判定您是否符合 BYOL 的資格，您的聯絡人需要您提供特定資訊。例如，您可能會被要求回答下列問題。

   - 您是否已檢閱並接受先前列出的 BYOL 要求？
   - 您需要在哪些 AWS 地區啟用 BYOL 帳戶？
   - 您計劃在每 AWS 個區域部署多少 BYOL WorkSpaces ？

- 您的提升計劃為何？
- 您是否向經銷 WorkSpaces 商購買產品？
- BYOL 需要哪些套件類型？
- 您的組織是否在相同地區啟用 BYOL 的任何其他 AWS 帳戶？ 若是如此，您是否要連結這些帳戶，以便它們使用相同的基礎硬體？

  如果帳戶已連結，則這些帳戶中 WorkSpaces 部署的總數會彙總在一起，以確定您是否符合 BYOL 的資格。如果這兩個問題的答案都是肯定的，您可以將您的帳戶連結在一起。您可以使用 API，例如 CreateAccountLinkInvitations和AcceptAccountLinkInvitation來連接您的 AWS 帳戶。如果您想要連結其他已啟用 BYOL 的帳戶，但想要使用不同的 BYOL 設定 (CIDR 範圍和影像)，請連絡 Sup AWS port 部門以啟用 BYOL 的新帳戶。

3. 確認 BYOL 的資格後，您可以繼續下一步，在 Amazon 主控台為帳戶啟用 BYOL。 WorkSpaces

步驟 2：使用 Amazon 主控台為您的 BYOL 帳戶啟用 BYOL WorkSpaces

若要為您的帳戶啟用 BYOL，您必須指定管理網路介面。此界面連接到一個安全的 Amazon WorkSpaces 管理網絡。它用於 WorkSpace 桌面到 Amazon WorkSpaces 客戶端的交互式流，並允許 Amazon WorkSpaces 管理 WorkSpace.

> **Note**
>
> 您只需在每個區域執行此程序中的步驟一次，即可為您的帳戶啟用 BYOL。

使用 Amazon 主控台為您的帳戶啟用 BYOL WorkSpaces

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在功能窗格中，選擇 [帳戶設定]，然後在 [使用您自己的授權 (BYOL)] 下，選擇 [檢視 WorkSpaces B YOL 設定]。
3. 在帳戶設定頁面的自帶授權 (BYOL) 下，選擇啟用 BYOL。

   如果您沒有看到啟用 BYOL 選項，這表示您的帳戶目前不符合 BYOL 的資格。如需詳細資訊，請參閱 步驟 1：使用 Amazon 主控台檢查您的帳戶是否符合 BYOL 的資格 WorkSpaces 。
4. 在自帶授權 (BYOL) 底下的管理網路介面 IP 地址範圍區域中，選擇 IP 地址範圍，然後選擇顯示可用的 CIDR 區塊。

Amazon 會在您指定的範圍內，以 IPv4 無類別網域間路由 (CIDR) 區塊的形式 WorkSpaces 搜尋並顯示可用的 IP 位址範圍。如果您需要特定的 IP 地址範圍，您可以編輯搜尋範圍。

> **Important**
>
> 指定 IP 地址範圍之後，就無法加以修改。務必指定 IP 地址範圍，而該範圍不會與內部網路使用的範圍衝突。如果您對要指定的範圍有任何疑問，請聯絡您的 AWS 客戶經理或業務代表，或在繼續之前聯絡AWS Support 中心。

5. 從結果清單中選擇您要的 CIDR 區塊，然後選擇啟用 BYOL。

   此程序可能需要幾個小時。啟 WorkSpaces 用 BYOL 帳戶時，請繼續進行下一個步驟。

步驟 3：在 Windows 虛擬機器上執行 BYOL 檢查程式 PowerShell 指令碼

在為您的帳戶啟用 BYOL 之後，您必須確認您的虛擬機器符合 BYOL 的需求。若要這麼做，請執行下列步驟以下載並執行 WorkSpaces BYOL 檢查程式 PowerShell 指令碼。此指令碼會在您打算用來建立映像的 VM 上執行一系列測試。

> **Important**
>
> VM 必須先通過所有測試，您才能將其用於 BYOL。

若要下載 BYOL 檢查程式指令碼

請確認 VM 上已安裝最新的 Windows 安全性更新，然後再下載和執行 BYOL 檢查程式指令碼。執行此指令碼時，其會停用 Windows Update 服務。

1. 將 BYOL 檢查程式指令碼 .zip 檔案從 https://tools.amazonworkspaces.com/BYOLChecker.zip 下載到您的資料夾。`Downloads`
2. 在您的 `Downloads` 資料夾中，建立 `BYOL` 資料夾。
3. 從 `BYOLChecker.zip` 解壓縮檔案並將其複製到 `Downloads\BYOL` 資料夾。
4. 刪除 `Downloads\BYOLChecker.zip` 資料夾，以便僅保留解壓縮的檔案。

執行下列步驟來執行 BYOL 檢查程式指令碼。

若要執行 BYOL 檢查程式指令碼

1. 從視窗桌面開啟視窗 PowerShell。選擇 Windows 開始按鈕，在 Windows 上按一下滑鼠右鍵 PowerShell，然後選擇「以系統管理員身 如果「使用者帳戶控制」提示您選擇是否 PowerShell 要對裝置進行變更，請選擇「是」。
2. 在 PowerShell 命令提示字元中，切換至 BYOL 檢查程式指令碼所在的目錄。例如，如果指令碼位於 Downloads\BYOL 目錄中，請輸入下列命令並按 Enter 鍵：

   ```
   cd C:\Users\username\Downloads\BYOL
   ```

3. 輸入下列命令以更新電腦上的 PowerShell 執行原則。這麼做可讓 BYOL 檢查程式指令碼執行：

   ```
   Set-ExecutionPolicy AllSigned
   ```

4. 當系統提示您確認是否要變更 PowerShell 執行原則時，請輸入A以將「全部都是」指定為「是」。
5. 輸入以下命令以執行 BYOL 檢查程式指令碼。

   ```
   .\BYOLChecker.ps1
   ```

6. 如果出現安全通知，請按 R 鍵以執行一次。
7. 在「WorkSpaces 影像驗證」對話方塊中，選擇「開始測試」。
8. 每次測試完成後，您可以檢視測試的狀態。對於狀態為失敗的任何測試，請選擇資訊以顯示如何解決造成失敗之問題的相關資訊。如果有任何測試顯示警告狀態，請選擇修正所有警告按鈕。
9. 如果適用，請解決導致測試失敗和警告的任何問題，並重複 Step 7和 Step 8，直到虛擬機器通過所有測試為止。匯出虛擬機器之前，必須先解決所有失敗和警告。
10. BYOL 指令碼檢查程式會產生兩個日誌檔：`BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` 及 `ImageInfo.text`。這些檔案位於包含 BYOL 檢查程式指令碼檔案的目錄中。

    > **Tip**
    >
    > 請勿刪除這些檔案。如果發生問題，其可能有助於疑難排解。

11. VM 通過所有測試之後，您會收到驗證成功訊息。檢閱工具中顯示的 VM 地區設定。若要更新地區設定，請遵循 Microsoft 文件中的這些指示，然後再次執行 BYOL 檢查程式指令碼。
12. 關閉 VM 並建立其快照。

13. 重新啟動 VM。選擇執行 Sysprep。如果 Sysprep 成功，您在Step 12 之後匯出的 VM 可以匯入 Amazon Elastic Compute Cloud (Amazon EC2) 中。否則，請檢閱 Sysprep 日誌、回復至在 Step 12 擷取的快照、解決報告的問題、建立新的快照，然後再次執行 BYOL 檢查程式指令碼。

    Sysprep 失敗的最常見原因是未針對所有使用者解除安裝現代 AppX 套件。您可以使用Remove-AppxPackage PowerShell 指令程式移除 AppX 套件。
14. 成功建立映像後，您可以移除 WorkSpaces_BYO L 帳戶。

錯誤訊息和錯誤修正清單

BYOL 匯入需要 PowerShell 4.0 或更高版本。不支援的 PowerShell 已安裝版本。

PowerShell 必須安裝 4.0 或更高版本。如需詳細資訊，請參閱 Microsoft 視窗 PowerShell。

BYOL 匯入不支援已安裝作用中 Microsoft Office 的系統。

Microsoft Office 必須在匯入之前解除安裝。如需詳細資訊，請參閱從電腦解除安裝 Office。

BYOL 匯入需要沒有 PCoIP 代理程式的系統。

解除安裝 PCoIP 代理程式。如需解除安裝 PCoIP 代理程式的相關資訊，請參閱解除安裝適用於 Mac 的 Teradici PCoIP 軟體用戶端

BYOL 匯入要求停用 Windows 更新。

請依照下列步驟停用 Windows 更新：

1. 按 Windows 鍵 + R。鍵入 `services.msc`，然後按 Enter 鍵。
2. 以滑鼠右鍵按一下 Windows Upate，然後選擇屬性。
3. 在一般所以標籤下，將啟動類型設定為停用。
4. 選擇停止。
5. 選擇套用，然後選擇確定。
6. 重新啟動電腦。

BYOL 匯入需要啟用「自動掛載」。

您必須啟用「自動掛載」。以管理員身分在 PowerShell 中執行下列命令。

```
C:\> diskpart
DISKPART> automount enable
```

已啟用自動掛載新磁碟區。

BYOL 匯入需要啟用 WorkSpaces _BYOL 帳戶

WorkSpaces必須啟用 _BYOL 帳戶。如需詳細資訊，請參閱使用 Amazon 主控台為您的帳戶啟用 BYOL 的 BYOL。 WorkSpaces

BYOL 匯入需要網路介面才能使用 DHCP 來自動指派 IP 地址。網路介面目前使用靜態 IP 地址。

必須變更網路介面才能使用 DHCP。如需詳細資訊，請參閱變更 TCP/IP 設定。

BYOL 匯入需要本機磁碟上有超過 20 GB 的空間。

本機磁碟必須有足夠的空間，並要求您釋放 20 GB 以上的空間。

BYOL 匯入需要具有 1 個本機磁碟機的系統。還有其他本地、可移除或網路磁碟機。

只有 C 和 D 驅動器可以存在 WorkSpace 於用於導入圖像的。移除所有其他磁碟機，包括虛擬磁碟機。

BYOL 匯入需要 Windows 10 或 Windows 11。

使用 Windows 10 或 Windows 11 作業系統。

BYOL 匯入需要未加入 AD 網域的系統。

系統必須取消加入 AD 網域。如需詳細資訊，請參閱 Azure Active Directory 裝置管理常見問答集。

BYOL 匯入需要未加入 Azure 網域的系統。

系統必須取消加入 Azure 網域。如需詳細資訊，請參閱 Azure Active Directory 裝置管理常見問答集。

BYOL 匯入需要停用 Windows 公用防火牆。

必須停用公用防火牆設定檔。如需詳細資訊，請參閱開啟或關閉 Microsoft Defender 防火牆。

BYOL 匯入需要不含 VMware 工具的系統。

必須將 VMware 工具解除安裝。如需詳細資訊，請參閱在 VMware Fusion 中解除安裝和手動安裝 VMware 工具 (1014522)。

BYOL 匯入需要本機磁碟小於 80 GB。

磁碟必須小於 80 GB。縮減磁碟大小。

BYOL 匯入在本機磁碟機上需要少於 2 個分割區。此外，所有 Windows 10 分割區必須進行 MBR 分割，而所有 Windows 11 分割區則必須進行 GPT 分割。

磁碟區必須針對 Windows 10 進行 MBR 分割，以及針對 Windows 11 進行 GPT 分割。如需詳細資訊，請參閱管理磁碟。

BYOL 匯入要求完成所有需要重新開機的擱置更新。

安裝所有更新並重新啟動作業系統。

BYOL 匯入需要停用此功能 AutoLogon 。

若要停用 AutoLogon 登錄：

1. 按 Windows 鍵 + R 並在命令提示中鍵入 `Regedit.exe`。
2. 向下捲動至 `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`
3. 新增 `DontDisplayLastUserName` 的值。
4. 針對類型，輸入 `REG_SZ`。
5. 針對值，輸入 `0`。

> **Note**
>
> - `DontDisplayLastUserName` 值可決定登入對話方塊是否顯示上次登入電腦之使用者的使用者名稱。
> - 此值預設不存在。如果存在，您必須將其設定為，`0`否則的值`DefaultUser`將會被清除並 AutoLogon 失敗。

BYOL 匯入要求啟用 **`RealTimeIsUniversal`**。

RealTimeUniversal 必須啟用登錄機碼。如需詳細資訊，請參閱設定 Windows Server 2008 和更新版本的時間設定。

BYOL 匯入需要具有一個可開機分割區的系統。

可開機分割區的數目不得超過一個。

若要移除其他分割區

1. 按 Windows 標誌 + R 鍵以開啟執行方塊。輸入 `msconfig` 並按鍵盤上的 Enter 鍵來開啟 [系統組態] 視窗。
2. 從視窗中選擇開機索引標籤，然後檢查您要使用的作業系統是否設為目前的作業系統；預設作業系統。若未設定，請從視窗中選擇所需的作業系統，然後在相同視窗上選擇設為預設值。
3. 若要刪除其他分割區，請選擇該分割區，然後依序選取刪除、套用、確定。

如果錯誤仍然出現，請從安裝或修復光碟啟動電腦，然後按照下列步驟操作。

1. 跳過初始語言畫面，然後在主安裝畫面上選擇修復您的電腦。
2. 在選擇選項畫面上，選擇疑難排解。
3. 在進階選項畫面上，選擇命令提示。
4. 在命令提示中，輸入 `bootrec.exe /fixmbr`，然後按 Enter 鍵。

BYOL 匯入需要 64 位元系統。

必須使用 64 位元作業系統映像。如需詳細資訊，請參閱 BYOL 支援的 Windows 版本。

BYOL 匯入需要一個尚未重設授權的系統。

映像重設授權計數不得為 0。重設授權功能允許您延長 Windows 試用版的啟用期限。建立映像程序要求重設授權計數必須是 0 以外的值。

若要檢查 Windows 重設授權計數

1. 在 Windows 開始功能表，選擇 Windows 系統，然後選擇命令提示。
2. 在命令提示中輸入 `cscript C:\Windows\System32\slmgr.vbs /dlv`，然後按 Enter 鍵。
3. 若要將重設授權計數重設為 0 以外的值。如需詳細資訊，請參閱 Sysprep (一般化) Windows 安裝。

BYOL 匯入需要尚未就地升級的系統。此系統已就地升級。

Windows 不得從以前的版本升級。

BYOL 匯入要求系統上未安裝任何防毒軟體。

您必須將防毒軟體解除安裝。執行 BYOLChecker 以取得要解除安裝之防毒軟體的詳細資訊。

BYOL 匯入要求 Windows 10 系統具有舊版開機模式。

舊版 BIOS BootMode 必須用於 Windows 10。如需詳細資訊，請參閱「開機模式」。

步驟 4：從虛擬化環境匯出 VM

若要為 BYOL 建立映像，您必須先從虛擬化環境匯出 VM。虛擬機器必須位於大小上限為 70 GB 且至少有 10 GB 可用空間的單一磁碟區上。如需詳細資訊，請參閱虛擬化環境的文件，以及 VM Import/Export 使用者指南中的從虛擬化環境匯出 VM。

Windows 11 針對 Unified Extensible Firmware Interface (UEFI)、Trusted Platform Module (TPM) 2.0 和安全開機支援設定了新的硬體需求。VM Import/Export 可使用 Microsoft 金鑰和 NitRTP 自動啟用 UEFI 安全開機，這是 Windows 11 匯入的獨特功能。如需詳細資訊，請參閱使 AWS 用虛擬機器匯入/匯出將 Windows 11 映像帶入。

步驟 5：將 VM 作為映像匯入 Amazon EC2

匯出 VM 之後，請檢閱從 VM 匯入 Windows 作業系統的需求。視需要採取行動。如需詳細資訊，請參閱 VM Import/Export 需求。

> **Note**
>
> 不支援匯入含有加密磁碟的虛擬機器。如果您選擇 Amazon Elastic Block Store (Amazon EBS) 磁碟區使用預設加密，則在匯入 VM 之前必須取消選取該選項。

將 VM 匯入 Amazon EC2 做為 Amazon Machine Image (AMI)。使用下列其中一種方法：

- 使用 import-image 命令搭配 AWS CLI。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 import-image。
- 使用 ImportImage API 操作。如需詳細資訊，請參閱亞 Amazon EC2 API 參考ImportImage中的。

如需詳細資訊，請參閱《VM Import/Export 使用者指南》中的將 VM 匯入為映像。

步驟 6：使用主控台建立 BYOL 映像 WorkSpaces

執行這些步驟來建立 WorkSpaces BYOL 影像。

> **Note**
>
> 若要執行此程序，請確認您具有 AWS Identity and Access Management (IAM) 許可，可執行下列作業：
>
> - 打電 WorkSpaces **`ImportWorkspaceImage`**話
> - 在您要用來建立 BYOL 映像的 Amazon EC2 映像上呼叫 Amazon EC2 **`DescribeImages`**。
> - 在您要用來建立 BYOL 映像的 Amazon EC2 映像上呼叫 Amazon EC2 **`ModifyImageAttribute`**。確保 Amazon EC2 映像上的啟動許可不受限。此映像必須在整個 BYOL 映像建立過程中可共用。
>
> 如需 BYOL 特定的 IAM 政策範例 WorkSpaces，請參閱。適用於 WorkSpaces 的身分和存取管理如需處理 IAM 許可的詳細資訊，請參閱《IAM 使用者指南》中的變更 IAM 使用者的許可。
> 若要從您的映像檔建立 Graphics.g4dn、 GraphicsPro .g4dn、圖形或 GraphicsPro 套裝軟體，請聯絡AWS Support 中心，將您的帳戶新增至允許清單。當您的帳戶位於允許清單中之後，您可以使用指 AWS CLI import-workspace-image令擷取圖形 .g4dn、 GraphicsPro .g4dn、圖形或影像。 GraphicsPro 如需詳細資訊，請參閱 AWS CLI 命令參考中的 import-workspace-image。

若要從 Windows VM 建立映像

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇映像。
3. 選擇建立 BYOL 映像。
4. 在建立 BYOL 映像頁面上，執行下列動作：
   - 針對 AMI ID，選擇 EC2 主控台連結，然後選擇您匯入的 Amazon EC2 映像，如上一節 (步驟 5：將 VM 作為映像匯入 Amazon EC2) 所述。映像名稱必須以 `ami-` 開頭且後面接著 AMI 的識別碼 (例如，`ami-1234567e`)。
   - 針對映像名稱，輸入映像的唯一名稱。

- 針對描述，輸入描述以協助您快速識別映像。
- 針對執行個體類型，請根據您要用於映像的通訊協定 (PCoIP 或串流通訊協定 (WSP GraphicsPro)，選擇適當的套裝軟體類型 (「一般」、「Graphics.G4dn」、「圖形」或「圖形」)。 WorkSpaces 如果您要建立 GraphicsPro .g4dn 套裝軟體，請選擇「圖形 .g4dn」。對於未啟用 GPU 的套裝軟體 (圖形 .g4dn、 GraphicsPro .g4dn、圖形或以外的套裝軟體)，請選擇「一般」。 GraphicsPro

  > **Note**
  >
  > - 目前只能為 PCoIP 通訊協定建立圖形 GraphicsPro .g4dn、.g4dn、圖形和 GraphicsPro 影像。
  > - Windows 11 映像只能針對 WSP 協定建立。
  > - 圖形 .g4dn 和 GraphicsPro .g4dn 套裝軟體目前不適用於視窗 11。
  > - 視窗 11 不支援圖形和 GraphicsPro 影像。

- (選用) 針對選取應用程式，請選擇您要訂閱的 Microsoft Office 版本。如需詳細資訊，請參閱 將 Microsoft Office 新增到您的 BYOL 映像。
- (選用) 針對標籤，選擇新增標籤，將標籤與此映像產生關聯。如需詳細資訊，請參閱 標記 WorkSpaces 資源。

5. 選擇建立 BYOL 映像。

   建立映像時，主控台的映像頁面上映像的狀態會顯示為待定。BYOL 攝取程序至少需要 90 分鐘。如果您也已訂閱 Office，則預計此程序至少需要 3 小時。

   如果映像驗證不成功，主控台會顯示錯誤碼。映像建立完成時，狀態會變更為可用。

步驟 7：從 BYOL 映像建立自訂套件

建立 BYOL 映像之後，您可使用該映像來建立自訂套件。如需相關資訊，請參閱 建立自訂 WorkSpaces 映像檔和套裝軟體。

步驟 8：註冊專用目錄 WorkSpaces

若要將 BYOL 映像用於 WorkSpaces，您必須為此目的註冊一個目錄。

若要為以下項目註冊目錄 WorkSpaces

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在導覽窗格中，選擇目錄。
3. 選取目錄，然後選擇動作、註冊。
4. 在 [註冊目錄] 對話方塊中，對於 [啟用專用] WorkSpaces，選擇 [是]。
5. 選擇註冊。

如果您已經註冊的 AWS Managed Microsoft AD 目錄或 AD Connector 目錄並未在專用硬體上執行，您可以為此目的設定新的 AWS Managed Microsoft AD 目錄或 AD Connector 目錄。 WorkSpaces 您也可以取消註冊目錄，然後將其重新註冊為專用目錄。 WorkSpaces若要執行此操作，請執行這些步驟。

> **Note**
>
> 只有在沒有與目錄相關聯的情況 WorkSpaces 下，才能執行此程序。

若要取消註冊目錄並將其重新註冊為專用 WorkSpaces

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 終止現有的 WorkSpaces。
3. 在導覽窗格中，選擇目錄。
4. 選取目錄，然後選擇動作、取消註冊。
5. 出現確認的提示時，請選擇取消註冊。
6. 再次選取目錄，然後依序選擇動作、註冊。
7. 在 [註冊目錄] 對話方塊中，對於 [啟用專用] WorkSpaces，選擇 [是]。
8. 選擇註冊。

步驟 9：啟動您的自攜裝置 WorkSpaces

註冊專用目錄後 WorkSpaces，您可以 WorkSpaces 在此目錄中啟動 BYOL。如需有關如何啟動的資訊 WorkSpaces，請參閱使用 WorkSpaces 啟動虛擬桌面。

連結自攜裝置帳戶

您可以使用 BYOL 連結來連結帳戶並共用 BYOL 組態。BYOL 組態包括您的帳戶所使用的 CIDR 範圍，以及您用來透過 Windows 授權建立 WorkSpaces 的映像檔。所有連結的帳戶都共用相同的基礎硬體基礎結構。

啟用 BYOL 連結的帳戶是基礎硬體基礎結構的主要擁有者，稱為來源帳戶。來源帳戶會管理對基礎硬體基礎結構的存取。目標帳戶是連結至來源帳戶的帳戶。

Important

中目前無法使用 BYOL 帳戶連結的 API。 AWS GovCloud (US) Region

Note

您要連結的 AWS 帳戶必須是您組織的一部分，且位於相同付款人帳戶下。您只能連結同一地區內的帳號。

連結來源與目標帳戶

1. 使用 CreateAccountLinkInvitationAPI 將邀請連結從您的來源帳戶傳送至 Target 帳戶。
2. 使用 AcceptAccountLinkInvitationAPI 接受 Target 帳戶中的擱置連結。
3. 確認連結是否已使用 GetAccountLink或連ListAccount結 API 建立。

監控您的 WorkSpaces

您可以使用下列功能來監控您的 WorkSpaces.

CloudWatch 度量

Amazon WorkSpaces 發布數據點到 Amazon CloudWatch 關於你 WorkSpaces. CloudWatch 可讓您擷取有關這些資料點的統計資料，做為一組排序的時間序列資料 (稱為指標)。您可以使用這些指標來驗證您的執行 WorkSpaces 是否如預期。如需詳細資訊，請參閱 監控您的 WorkSpaces 使用 CloudWatch 指標。

CloudWatch 活動

Amazon WorkSpaces 可以在用戶登錄到您的 Amazon CloudWatch 事件提交事件 WorkSpace。這可讓您在事件發生時做出回應。如需詳細資訊，請參閱 監控您 WorkSpaces 使用 Amazon EventBridge。

CloudTrail 日誌

AWS CloudTrail 可提供由使用者、角色或 AWS 服務在 WorkSpaces 中所採取之動作的記錄。使用收集的資訊 CloudTrail，您可以判斷提出的要求 WorkSpaces、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。如需詳細資訊，請參閱使用記錄 WorkSpaces API 呼叫 CloudTrail。 AWS CloudTrail為智慧卡使用者記錄成功和失敗的登入事件。如需詳細資訊，請參閱 瞭解智慧卡使用者的 AWS 登入事件。

CloudWatch 互聯網監控

Amazon CloudWatch Internet Monitor 可讓您瞭解網際網路問題如何影響託管於您的應用程式與最終使用者之間的效能AWS和可用性。您也可以使用 CloudWatch 網際網路監視器來：

- 為一個或多個 WorkSpace 目錄創建監視器。
- 監控網際網路效能。
- 針對使用者城市網路 (包括其位置和 ASN) (通常是網際網路服務供應商 (ISP) 及其區域之間的問題，取得警示。 WorkSpace

網路監視器會使用 AWS 從其全域網路足跡擷取的連線資料，計算面向網際網路流量的效能和可用性基準。網路監視器目前無法為個人最終使用者提供網際網路效能，但其可提供城市和 ISP 層級的效能。

使用 CloudWatch 自動儀表板監控您的 WorkSpaces 健康

您可以 WorkSpaces 使用 CloudWatch 自動儀表板進行監視，該儀表板會收集原始數據並將其處理為可讀的近乎實時的指標。這些指標會保留 15 個月，以存取歷史資訊並監控 Web 應用程式或服務的效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

當您使用AWS帳戶設定您的 WorkSpaces. CloudWatch 儀表板可讓您監控跨區域的 WorkSpaces 指標，例如其健康狀態和效能。您也可以將儀表板用於以下目的：

- 識別運作狀態不良的 WorkSpace 執行
- 識別執行個體運作狀態不佳的 WorkSpace 執行模式、通訊協定和作業系統。
- 檢視一段時間的重要資源使用率。
- 識別異常情況以協助進行疑難排解。

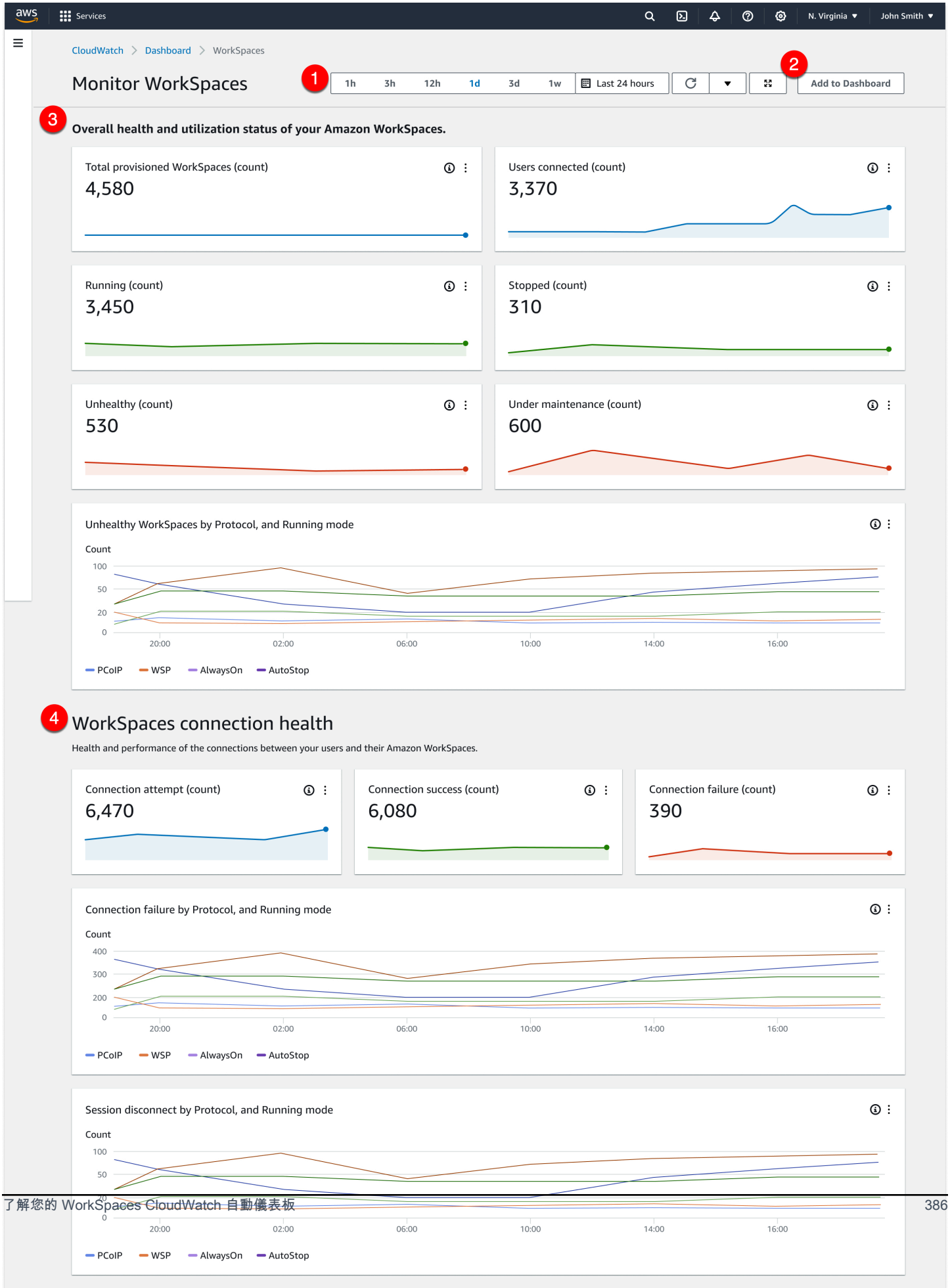
WorkSpaces CloudWatch 自動儀表板可在所有AWS商業區域使用。

使用 WorkSpaces CloudWatch 自動管控面板的步驟

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 Dashboards (儀表板)。
3. 選擇「自動儀表板」頁籤。
4. 選擇WorkSpaces。

了解您的 WorkSpaces CloudWatch 自動儀表板

CloudWatch 自動儀表板可讓您深入瞭解 WorkSpaces 資源效能，並協助您識別效能問題。


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

圖標板由下列功能組成：

1. 使用時間和日期範圍控制項檢視歷史資料。
2. 將自訂儀表板檢視新增至 CloudWatch 自訂儀表板。
3. 執行下列動作，監控您 WorkSpaces 的整體健全狀況和使用狀態：
    a. 檢視佈建的總數、連線的使用者數目 WorkSpaces、運作狀態不良且運作良好的 WorkSpace 執行個體數目。
    b. 檢視狀況不良 WorkSpaces 及其不同的變數，例如通訊協定和運算模式。
    c. 將滑鼠游標暫留在折線圖上，即可檢視特定通訊協定和 WorkSpace 執行模式在一段時間內，狀態良好或狀態不良的執行處理數目。
    d. 選擇省略符號功能表，然後選擇在量度中檢視以時間比例圖表檢視量度。
4. 檢視您的連線指標及其不同變數，例如在任何指定時間的 WorkSpaces 環境中嘗試連線次數、成功連線和失敗的連線。
5. 檢視影響使用者體驗的 InSession 延遲情況，例如往返時間 (RTT)，以判斷連線健康狀態和封包遺失，以監控網路健康狀態。
6. 檢視主機效能和資源使用率，以識別和疑難排解潛在的效能問題。

監控您的 WorkSpaces 使用 CloudWatch 指標

WorkSpaces 和 Amazon CloudWatch 已整合，因此您可以收集和分析效能指標。您可以使用 CloudWatch 主控台、 CloudWatch 命令列介面或以程式設計方式使用 CloudWatch API 監視這些指標。 CloudWatch 您也可以在達到指定的量度臨界值時設定警示。

如需使用 CloudWatch 和警示的詳細資訊，請參閱 Amazon 使用 CloudWatch 者指南。

必要條件

若要取得 CloudWatch 指標，請在`us-east-1`區域中的`AMAZON`子集上啟用連接埠 443 的存取權。如需詳細資訊，請參閱 的 IP 位址和連接埠需求 WorkSpaces。

目錄

WorkSpaces 度量

AWS/WorkSpaces 命名空間包含下列指標。

指標	描述	維度	統計資料	單位
Available [1]	傳回狀況良好狀態的 WorkSpaces 數目。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數
Unhealthy [1]	傳回狀態不良狀態的 WorkSpaces 數目。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數
ConnectionAttempt [2]	連線嘗試次數。	DirectoryId WorkspaceId RunningMode Protocol ComputeType	平均值、總和、最大值、最小值、資料樣本	計數

指標	描述	維度	統計資料	單位
		BundleId UserName		
ConnectionSuccess [2]	成功連線數目。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數
ConnectionFailure [2]	失敗連線數目。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數

指標	描述	維度	統計資料	單位
SessionLaunchTime	啟動 WorkSpaces 工作階段所需的時間。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	秒 (時間)
InSessionLatency	WorkSpaces 用戶端與之間的往返時間 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	毫秒 (時間)
SessionDisconnect	已關閉的連線數目，包括使用者起始和失敗的連線。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數

指標	描述	維度	統計資料	單位
UserConnected [3]	已連線使用者的編號。WorkSpaces	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數
Stopped	已停止 WorkSpaces 的數量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數
Maintenance [4]	正在維護 WorkSpaces 的數量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、總和、最大值、最小值、資料樣本	計數

指標	描述	維度	統計資料	單位
TrustedDeviceValidationAttempt [5、6]	裝置驗證簽章驗證嘗試次數。	DirectoryId	平均值、總和、最大值、最小值、資料樣本	計數
TrustedDeviceValidationSuccess [5、6]	成功的裝置驗證簽章驗證數目。	DirectoryId	平均值、總和、最大值、最小值、資料樣本	計數
TrustedDeviceValidationFailure [5、6]	失敗的裝置驗證簽章驗證數目。	DirectoryId	平均值、總和、最大值、最小值、資料樣本	計數
TrustedDeviceCertificateDaysBeforeExpiration [6]	與目錄相關聯的根憑證到期前的剩餘天數。	CertificateId	平均值、總和、最大值、最小值、資料樣本	計數
CPUUsage	使用的 CPU 資源百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比

指標	描述	維度	統計資料	單位
MemoryUsage	使用的本機記憶體百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比
RootVolumeDiskUsage	使用的根磁碟區百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比
UserVolumeDiskUsage	使用的使用者磁碟區百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比

指標	描述	維度	統計資料	單位
UDPPacketLossRate [7]	用戶端和閘道之間丟棄的封包百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值、資料樣本	百分比
UpTime	自上次重新開機以來的時間 WorkSpace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值、資料樣本	秒鐘

[1] WorkSpaces 定期傳送狀態要求至 WorkSpace. A WorkSpace 在響應這些請求Available時以及無法響應這些請求Unhealthy時標記。這些量度可以按每個精細度WorkSpace 層級提供，並彙總給組織 WorkSpaces 中的所有人。

[2] WorkSpaces 記錄與每個連接的指標 WorkSpace。這些指標會在使用者透過用戶端成功驗證，然後用 WorkSpaces 戶端啟動工作階段之後發出。這些指標可以每個精細度WorkSpace 層級提供，也會彙總目錄 WorkSpaces 中的所有指標。

[3] WorkSpaces 定期將連線狀態要求傳送至 WorkSpace. 當使用者主動使用其工作階段時，系統會回報使用者已連線。此量度可用於每個詳細程度WorkSpace 層級，也會彙總組織 WorkSpaces 中的所有人。

[4] 此測量結果適用於使 WorkSpaces 用 AutoStop 執行模式設定的測量結果。如果您已為您啟用維護 WorkSpaces，則此指標會擷取目前 WorkSpaces 正在維護的數目。此量度可在每個粒度WorkSpace 層級提供，其中說明 WorkSpace 進入維護的時間和移除的時間。

[5] 如果目錄啟用受信任裝置功能，Amazon WorkSpaces 會使用憑證型身份驗證來判斷裝置是否受信任。當使用者嘗試存取其時 WorkSpaces，會發出這些指標，以指出信任裝置驗證成功或失敗。這些指標以每個目錄的粒度層級提供，而且僅適用於 Amazon WorkSpaces Windows 和 macOS 用戶端應用程式。

[6] 不適用於 WorkSpaces 網頁存取。

[7] 此度量度量平均封包遺失。

- 在 PCoIP 上：測量來自用戶端之閘道的平均封包遺失。
- 在 WSP 上：測量從用戶端到閘道的平均封包遺失。

量度的維 WorkSpaces 度

若要篩選指標資料，請使用下列維度。

維度	描述
DirectoryId	將測量結果資料篩選至指定目錄 WorkSpaces 中的。目錄 ID 的形式為 d-XXXXXXXXXX 。
WorkspaceId	將測量結果資料篩選為指定的 WorkSpace。WorkSpace ID 的形式是ws-XXXXXXXXXX 。
CertificateId	篩選指標資料至與目錄相關聯的指定根憑證。憑證 ID 的形式為 wsc-XXXXXXXXX 。
RunningMode	WorkSpaces 依據其執行模式篩選測量結果資料。執行模式的形式為 AutoStop 或 AlwaysOn。
BundleId	WorkSpaces 依通訊協定篩選測量結果資料。捆綁的形式是wsb-XXXXXXXXXX 。
ComputeType	WorkSpaces 依運算類型將指標資料篩選為。

維度	描述
Protocol	WorkSpaces 依協定類型將測量結果資料篩選為。
UserName	WorkSpaces 依使用者名稱將度量資料篩選為。

監控範例

下列範例將示範如何使用 AWS CLI 來回應 CloudWatch 警示，並判斷目錄 WorkSpaces 中哪一個發生連線失敗。

若要回應 CloudWatch 鬧鐘

1. 使用 describe-alarms 命令來判斷警示套用至哪個目錄。

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. 使用描述工作 WorkSpaces 區命令取得指定目錄中的清單。

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
```

```
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. 使用取得 CloudWatch 量度統計資料命令，取得目錄 WorkSpace 中每個指標的度量。

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

監控您 WorkSpaces 使用 Amazon EventBridge

您可以使用 Amazon 的事件 WorkSpaces 來檢視、搜尋、下載、封存、分析和回應成功登入 WorkSpaces。例如，您可以針對下列目的使用事件：

- 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，然後使用策略僅允許使用者存取符合在事件類型中找到之存取準則的檔案或資料`WorkSpaces Access`。 WorkSpaces
- 使用分析登入資料並執行自動化動作 AWS Lambda。
- 使用政策控制來封鎖來自未經授權的 IP 地址對檔案和應用程式的存取。
- 找出用於連線的用 WorkSpaces 戶端版本 WorkSpaces。

Amazon WorkSpaces 以最大的努力為基礎發布這些事件。活動會以近乎即時 EventBridge 的方式傳送到。使用 EventBridge，您可以建立規則來觸發程式設計動作以回應事件。例如，您可以設定可呼叫 SNS 主題的規則來傳送電子郵件通知，或叫用 Lambda 函數採取某些動作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。

WorkSpaces 訪問事件

WorkSpaces 用戶端應用`WorkSpaces Access`程式會在使用者成功登入 WorkSpace. 所有 WorkSpaces 用戶端傳送這些事件。

WorkSpaces 使用 WorkSpaces 串流通訊協定 (WSP) 所發出的事件需要用 WorkSpaces 戶端應用程式版本 4.0.1 或更新版本。

事件會以 JSON 物件的形式表示。以下是 `WorkSpaces Access` 事件的範例資料。

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
```

```
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

事件特定欄位

`clientIpAddress`

用戶端應用程式的 WAN IP 地址。如果是 PCoIP 零客戶端，則此為 Terdici 驗證用戶端的 IP 地址。

`actionType`

這個值一律為 `successfulLogin`。

`workspacesClientProductName`

下列值會區分大小寫。

- `WorkSpaces Desktop client`—Windows、macOS 和 Linux 用戶端
- `Amazon WorkSpaces Mobile client`—iOS 用戶端
- `WorkSpaces Mobile Client`—Android 用戶端
- `WorkSpaces Chrome Client`—Chromebook 用戶端
- `WorkSpacesWebClient`—Web Access 用戶端
- `AmazonWorkSpacesThinClient`— Amazon WorkSpaces 瘦客戶端設備
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` —零客戶端

`loginTime`

使用者登入的時間 WorkSpace。

`clientPlatform`

- `Android`
- `Chrome`

- iOS
- Linux
- OSX
- Windows
- Teradici PCoIP Zero Client and Tera2
- Web

directoryId

的目錄識別碼 WorkSpace。您必須在目錄識別碼前面加上 domain/。例如 "domain/d-123456789"。

clientVersion

用於連線的用戶端版本 WorkSpaces。

workspaceId

WorkSpace 的識別碼。

建立規則來處理 WorkSpaces 事件

使用下列程序建立規則來處理 WorkSpaces 事件。

先決條件

若要接收電子郵件通知，請建立 Amazon Simple Notification Service 主題。

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇主題。
3. 請選擇建立主題。
4. 針對類型，選擇標準。
5. 在 Name (名稱) 中，輸入主題名稱。
6. 請選擇建立主題。
7. 選擇建立訂閱。
8. 對於通訊協定，選擇電子郵件。
9. 在 Endpoint (端點) 中，輸入接收通知的電子郵件地址。
10. 選擇建立訂閱。

11. 您會收到帶有下列主旨行的電子郵件訊息：AWS Notification - Subscription Confirmation。請依照指示來確認訂閱。

若要建立規則來處理 WorkSpaces 事件

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 選擇建立規則。
3. 在 Name (名稱) 中，輸入規則名稱。
4. 針對規則類型，選擇具有事件模式的規則。
5. 選擇下一步。
6. 針對 Event pattern (事件模式)，請執行下列動作：
   a. 在 Event source (事件來源)，選擇 AWS 服務。
   b. 針對 AWS 服務，選擇 WorkSpaces。
   c. 針對 [事件類型] 選擇 [WorkSpaces存取權]
   d. 根據預設，我們會傳送每個事件的通知。如果您想要，可以建立事件模式來篩選特定用戶端或工作區的事件。
7. 選擇下一步。
8. 如下所示指定目標：
   a. 對於 Target types (目標類型)，選擇 AWS 服務。
   b. 對於 Select a target (選取目標)，選擇 SNS topic (SNS 主題)。
   c. 對於主題，選擇您為通知建立的 SNS 主題。
9. 選擇下一步。
10. (選用) 將標籤新增至您的規則。
11. 選擇下一步。
12. 選擇建立規則。

瞭解智慧卡使用者的 AWS 登入事件

AWS CloudTrail 為智慧卡使用者記錄成功和失敗的登入事件。這包括每次提示使用者解決特定憑證挑戰或要素時擷取的登入事件，以及該特定憑證驗證請求的狀態。使用者只會在完成所有必要的憑證挑戰後才會登入，這會導致 `UserAuthentication` 事件被記錄。

下表擷取每個登入 CloudTrail 事件名稱及其目的。

事件名稱	事件目的
CredentialChallenge	通知 AWS 登入已請求使用者解決特定憑證挑戰，並指定所需的 CredentialType (例如 SMARTCARD)。
CredentialVerification	通知使用者已嘗試解決特定 CredentialChallenge 請求，並指定該憑證是成功還是失敗。
UserAuthentication	通知使用者遭到挑戰的所有驗證需求都已成功完成，且使用者已成功登入。當使用者無法順利完成所需的憑證挑戰時，不會記錄任何 UserAuthentication 事件。

下表擷取特定登入 CloudTrail 事件中包含的其他實用事件資料欄位。

事件名稱	事件目的	登入事件適用性	範例值
AuthWorkflowID	使整個登入序列中發出的所有事件產生關聯。對於每次使用者登入，AWS 登入可以發出多個事件。	CredentialChallenge，CredentialVerification，UserAuthentication	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
CredentialType	通知使用者已嘗試解決特定 CredentialChallenge 請求，並指定該憑證是成功還是失敗。	CredentialChallenge，CredentialVerification，UserAuthentication	CredentialType": "SMARTCARD" (現今可能的值：SMARTCARD)
LoginTo	通知使用者遭到挑戰的所有驗證需求都已成功完成，且使用者已成功登入。當使用者無法順利完成所需的憑證挑戰時，不會記錄任何 UserAuthentication 事件。	UserAuthentication	"LoginTo": "https://skylight.local“

AWS 登入案例的範例事件

下列範例顯示不同登入案例中 CloudTrail 事件的預期序列。

目錄

使用智慧卡驗證時登入成功

下列事件序列會擷取智慧卡登入成功的範例。

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
```

```
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

成功的 CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
```

```
}
```

成功的 UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

僅使用智慧卡驗證時登入失敗

下列事件序列會擷取智慧卡登入失敗的範例。

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

失敗的 CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Amazon 的業務連續性 WorkSpaces

Amazon 建立 WorkSpaces 在AWS全球基礎設施上，該基礎設施分為區AWS域和可用區域。這些區域和可用區域在實體隔離和資料備援方面提供彈性。如需詳細資訊，請參閱 Amazon WorkSpaces 的恢復能力。

Amazon WorkSpaces 還提供跨區域重新導向，這項功能可與您的網域名稱系統 (DNS) 路由政策搭配使用，以便在使用者的主要伺服器 WorkSpaces 無法使用 WorkSpaces 時將 WorkSpaces 使用者重新導向至替代方案。例如，透過使用 DNS 容錯移轉路由原則，您可以在使用者無法存取主要區域 WorkSpaces 中的容錯移轉區域時，將使用者連線至指定 WorkSpaces 的容錯移轉區域。

您可以使用跨區域重新導向來實現區域彈性和高可用性。您也可以將其用於其他目的，例如流量分配或 WorkSpaces 在維護期間提供替代方案。如果您使用 Amazon Route 53 進行 DNS 組態，您可以利用運作狀態檢查來監控 Amazon CloudWatch 警示。

Amazon WorkSpaces 多區域復原能力在次要區域提供自動化的備援虛擬桌面基礎設施，並在主要 WorkSpace 區域因服務中斷而無法連接時，簡化將使用者重新導向至次要區域的程序。

您可以將 WorkSpaces 多區域復原與跨區域重新導向搭配使用，在次要區域部署備援虛擬桌面基礎架構，並設計跨 WorkSpace 區域容錯移轉策略，以準備應對中斷性事件。您也可以將此解決方案用於其他目的，例如流量分配或 WorkSpaces 在維護期間提供替代方案。如果您使用 Route 53 做為 DNS 組態，您可以利用監控 CloudWatch 警示的健康狀態檢查。

目錄

Amazon 的跨區域重新導向 WorkSpaces

使用 Amazon 中的跨區域重新導向功能 WorkSpaces，您可以使用完整網域名稱 (FQDN) 作為. WorkSpaces 跨區域重新導向可與您的網域名稱系統 (DNS) 路由原則搭配使用，以便在 WorkSpaces 使用者的主要伺服器 WorkSpaces 無法使用 WorkSpaces 時將使用者重新導向至 例如，透過使用 DNS 容錯移轉路由原則，您可以在使用者無法存取主要區域 WorkSpaces 中的容錯移轉AWS區域時，將使用者連線至指定 WorkSpaces 的容錯移轉區域。

您可以使用跨區域重新導向搭配 DNS 容錯移轉路由政策，以達到區域彈性和高可用性。您也可以將此功能用於其他目的，例如流量分配或 WorkSpaces 在維護期間提供替代方案。如果您使用 Amazon Route 53 進行 DNS 組態，您可以利用運作狀態檢查來監控 Amazon CloudWatch 警示。

若要使用此功能，您必須 WorkSpaces 為兩個 (或更多) AWS 區域中的使用者進行設定。您也必須建立稱為連線別名的特殊 FQDN 型註冊碼。這些連線別名會取代您使用者的區域特定註冊碼 WorkSpaces 。(區域特定註冊碼仍然有效；不過，若要讓跨區域重新導向運作，您的使用者必須改用 FQDN 做為其註冊碼。)

若要建立連線別名，請指定連接字串，這是 FQDN，例如 `www.example.com` 或 `desktop.example.com`。若要使用此網域進行跨區域重新導向，您必須向網域註冊機構註冊，並為您的網域設定 DNS 服務。

建立連線別名後，您可以將它們與不同區域中的 WorkSpaces 目錄建立關聯，以建立關聯配對。每個關聯配對都有一個主要區域和一或多個容錯移轉區域。如果主要區域發生中斷，您的 DNS 容錯移轉路由原則會將您的 WorkSpaces 使用者重新導向至您在容錯移轉區域中為他們設定的使用者。WorkSpaces

若要指定主要和容錯移轉區域，您可以在設定 DNS 容錯移轉路由政策時定義區域優先順序 (主要或次要)。

目錄

必要條件

- 您必須擁有並註冊要在連線別名中當作 FQDN 使用的網域。如果您尚未使用其他網域註冊機構，您可使用 Amazon Route 53 來註冊您的網域。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的使用 Amazon Route 53 註冊網域名稱。

  > **Important**
  >
  > 您必須擁有所有必要的權利，才能使用與 Amazon 搭配使用的任何網域名稱 WorkSpaces。您同意網域名稱不違反或侵犯任何第三方的合法權利，或以其他方式違反適用法律。

  您的網域名稱總長度不得超過 255 個字元。如需有關網域名稱的詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的 DNS 網域名稱格式。

  跨區域重新導向適用於公用網域名稱和私有 DNS 區域中的網域名稱。如果您使用的是私有 DNS 區域，則必須提供虛擬私人網路 (VPN) 連線至包含您 WorkSpaces的. 如果您的使用 WorkSpaces 者嘗試從公用網際網路使用私人 FQDN，用 WorkSpaces 戶端應用程式會傳回下列錯誤訊息：

  ```
  "We're unable to register the WorkSpace because of a DNS server issue.
  Contact your administrator for help."
  ```

- 您必須設定 DNS 服務並設定必要的 DNS 路由政策。跨區域重新導向會與 DNS 路由原則搭配使用，視需要重新導向 WorkSpaces 使用者。
- 在您要設定跨區域重新導向的每個主要區域和容錯移轉區域中， WorkSpaces 為您的使用者建立。請務必在每個區域的每個 WorkSpaces 目錄中使用相同的使用者名稱。若要讓 Active Directory 使用者資料保持同步，我們建議您使用 AD Connector 指向您 WorkSpaces 為使用者設定的每個區域中的相同 Active Directory。如需有關建立的詳細資訊 WorkSpaces，請參閱 Launch WorkSpaces。

  > **Important**
  >
  > 如果您為多區域複寫設定AWS受管 Microsoft AD 目錄，則只能註冊主要區域中的目錄以便與 Amazon WorkSpaces 搭配使用。嘗試在複寫區域中註冊目錄以與 Amazon 搭配使用 WorkSpaces 將會失敗。在複寫區域內，不支援使用AWS受管 Microsoft AD 進 Amazon 多區 WorkSpaces 域複寫。

完成跨區域重新導向的設定後，您必須確定您的使用 WorkSpaces 者使用的是 FQDN 型註冊碼，而不是以區域為基礎的註冊碼 (例如) 做為其主要地WSpdx+ABC12D區。若要執行此操作，您必須使用步驟 5：將連接字符串發送給您的 WorkSpaces 用戶 中的程序，傳送包含 FQDN 連接字串的電子郵件給他們。

> **Note**
>
> 如果您在 WorkSpaces 主控台中建立使用者，而不是在 Active Directory 中建立使用者，則每當您啟 WorkSpaces 動新的時候，都會自動傳送邀請電子郵件給您的使用者，並以區域為基礎的註冊碼。 WorkSpace這表示當您在容錯移轉區域中 WorkSpaces 為使用者設定時，您的使用者也會自動接收這些容錯移轉的電子郵件 WorkSpaces。您需要指示使用者忽略包含區域型註冊碼的電子郵件。

限制

- 跨區域重新導向不會自動檢查與主要區域的連線是否失敗，然後容錯 WorkSpaces 移轉至其他區域。換句話說，不會發生自動容錯移轉。

  若要實作自動容錯移轉案例，您必須使用其他機制搭配跨區域重新導向。例如，您可以使用 Amazon Route 53 容錯移轉 DNS 路由政策，搭配 Route 53 運作狀態檢查來監控主要區域中的 CloudWatch 警示。如果觸發主要區域中的 CloudWatch 警示，您的 DNS 容錯移轉路由原則會將您的 WorkSpaces 使用者重新導向至您在容錯移轉區域中為他們設定的警示。 WorkSpaces
- 當您使用跨區域重新導向時，使用者資料不會保留 WorkSpaces 在不同區域之間。若要確保使用者能夠從不同區域存取其檔案，建議您 WorkDocs 為 WorkSpaces 使用者設定 Amazon (如果您的主要和容錯移轉區域支援 Amazon WorkDocs)。有關 Amazon 的更多信息 WorkDocs，請參閱 Amazon WorkDocs 管理指南中的 Amazon WorkDocs 驅動器。如需為 WorkSpace 使用者啟用 Amazon WorkDocs 的詳細資訊，請參閱向 WorkSpaces 註冊目錄和為 AWS Managed Microsoft AD 啟用 Amazon WorkDocs。有關使 WorkSpaces 用者如何在其 WorkDocs 上設定 Amazon 的詳細資訊 WorkSpaces，請參閱 Amazon WorkSpaces 使用者指南 WorkDocs中的「與整合」。
- 只有 3.0.9 版或更新版本的 Linux、macOS 和 Windows WorkSpaces 用戶端應用程式才支援跨區域重新導向。您也可以使用跨區域重新導向搭配 Web Access。
- 所有提供 Amazon 服務的區AWS域均可使 WorkSpaces 用跨區域重新導向，但中國和寧夏區域除外。AWS GovCloud (US) Region

步驟 1：建立連線別名

使用相同的 AWS 帳戶，在您要設定跨區域重新導向的每個主要和容錯移轉區域中，建立連線別名。

若要建立連線別名

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主機的右上角，選取您的主要AWS地區 WorkSpaces。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。
4. 在跨區域重新導向之下，選擇建立連線別名。
5. 在連接字串中，輸入 FQDN，例如 `www.example.com` 或 `desktop.example.com`。連接字串最多可以是 255 個字元。其只能包含字母 (A-Z 和 a-z)、數字 (0-9) 和下列字元： .-

   > **Important**
   >
   > 建立連接字串之後，其一律與您的 AWS 帳戶相關聯。即使您從原始帳戶中刪除連接字串的所有執行個體，也無法使用不同的帳戶重新建立相同的連接字串。連接字串會全域保留給您的帳戶使用。

6. (選用) 在標籤下，指定要與連線別名產生關聯的任何標籤。
7. 選擇建立連線別名。
8. 重複這些步驟Step 2，但請務必在中為您選取 WorkSpaces. 如果您有多個容錯移轉區域，請為每個容錯移轉區域重複這些步驟。請務必使用相同的 AWS 帳戶，在每個容錯移轉區域中建立連線別名。

(選用) 步驟 2：與其他帳戶共用連線別名

您可以與 AWS 同一區域中的另一個 AWS 帳戶共享連線別名。與另一個帳戶共享連線別名會授予該帳戶的許可，您只能將該別名與相同區域中該帳戶擁有的目錄建立關聯或解除關聯。只有擁有連線別名的帳戶才能刪除別名。

> **Note**
>
> 連線別名只能與每個 AWS 區域一個目錄建立關聯。如果您與另一個 AWS 帳戶共享連線別名，則只有一個帳戶 (您的帳戶或共享帳戶) 可以將別名與該區域中的目錄建立關聯。

若要與其他 AWS 帳戶共用連線別名

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主控台的右上角，選取您要與其他 AWS 帳戶共用連線別名的 AWS 區域。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。
4. 在跨區域重新導向關聯底下，選取連接字串，然後選擇動作、共用/取消共用連線別名。

   您也可以從連線別名的詳細資訊頁面共用別名。若要這麼做，請在共用帳戶下，選擇共用連線別名。
5. 在共用/取消共用連線別名頁面的與帳戶共用底下，輸入您要在此 AWS 區域中共用連線別名的 AWS 帳戶 ID。
6. 選擇共用。

步驟 3：將連線別名與每個區域中的目錄建立關聯

將相同的連線別名與兩個或多個 Region 中的目 WorkSpaces 錄建立目錄之間的關聯配對。每個關聯配對都有一個主要區域和一或多個容錯移轉區域。

例如，如果您的主要區域是美國西部 (奧勒岡) 區域，您 WorkSpaces 可以將美國西部 (奧勒岡) 區域中的 WorkSpaces 目錄與美國東部 (維吉尼亞北部) 區域中的目錄配對。如果主要區域發生中斷，跨區域重新導向會搭配 DNS 容錯移轉路由原則，以及您在美國西部 (奧勒岡) 區域進行的任何健康狀態檢查一起運作，以便將您的使用者重新導向至 WorkSpaces 您在美國東部 (維吉尼亞北部) 區域設定的使用者。如需有關跨區域重新導向體驗的詳細資訊，請參閱 跨區域重新導向期間發生什麼狀況。

> **Note**
>
> 如果您的 WorkSpaces 使用者與容錯移轉區域相距很遠 (例如，數千英里外)，他們的 WorkSpaces 體驗可能會比平常的回應速度降低。若要檢查從您所在位置到各個AWS區域的往返時間 (RTT)，請使用 Amazon WorkSpaces 連線運作 Health 檢查。

若要建立連線別名與目錄的關聯

每個 AWS 區域只能將連線別名與一個目錄建立關聯。如果您已與其他 AWS 帳戶共享連線別名，則只有一個帳戶 (您的帳戶或共享帳戶) 可以將別名與該區域中的目錄建立關聯。

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/

2. 在主機的右上角，選取您的主要AWS地區 WorkSpaces。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。
4. 在跨區域重新導向關聯底下，選取連接字串，然後選擇動作、關聯/取消關聯。

   您也可以從連線別名的詳細資訊頁面，建立連線別名與目錄的關聯。若要這麼做，請在關聯的目錄下選擇關聯目錄。
5. 在關聯/取消關聯頁面的關聯至目錄下，選取您要在此 AWS 區域中與連線別名建立關聯的目錄。

   > **Note**
   >
   > 如果您為多區域複寫設定AWS受管 Microsoft AD 目錄，則只有主要區域中的目錄可以與 Amazon WorkSpaces 搭配使用。嘗試使用 Amazon 複寫區域中的目錄 WorkSpaces 將會失敗。在複寫區域內，不支援使用AWS受管 Microsoft AD 進 Amazon 多區 WorkSpaces 域複寫。
6. 選擇 Associate (關聯)。
7. 重複這些步驟Step 2，但請務必在中為您選取 WorkSpaces. 如果您有多個容錯移轉區域，請為每個容錯移轉區域重複這些步驟。務必將相同的連線別名與每個容錯移轉區域中的目錄產生關聯。

步驟 4：設定您的 DNS 服務並設定 DNS 路由政策

建立連線別名和連線別名關聯配對之後，您可以接著為您在連接字串中使用的網域設定 DNS 服務。您可以為此目的使用任何 DNS 服務供應商。如果您還沒有偏好的 DNS 服務供應商，您可以使用 Amazon Route 53。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的設定 Amazon Route 53 做為 DNS 服務。

為網域設定 DNS 服務之後，您必須設定要用於跨區域重新導向的 DNS 路由政策。例如，您可以使用 Amazon Route 53 運作狀態檢查來判斷使用者是否可以連線到他們 WorkSpaces 在特定區域中。如果您的使用者無法連線，您可使用 DNS 容錯移轉政策，將 DNS 流量從一個區域路由傳送到另一個區域。

如需有關選擇 DNS 路由政策的資訊，請參閱《Amazon Route 53 開發人員指南》中的選擇路由政策。如需有關 Amazon Route 53 運作狀態檢查的詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的 Amazon Route 53 如何檢查資源的運作狀態。

當您設定 DNS 路由原則時，您需要連線別名和主要區域中 WorkSpaces 目錄之間關聯的連線識別碼。您也需要連線別名與容錯移轉區域或區域中 WorkSpaces 目錄之間關聯的連線識別碼。

> **Note**
>
> 連線識別符與連線別名 ID 不同。連線別名 ID 的開頭為 `wsca-`。

若要尋找連線別名關聯的連線識別符

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主機的右上角，選取您的主要AWS地區 WorkSpaces。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。
4. 在跨區域重新導向關聯下，選取連接字串文字 (FQDN) 以檢視連線別名詳細資訊頁面。
5. 在連線別名的詳細資訊頁面上，於關聯的目錄之下，記下針對連線識別符所顯示的值。
6. 重複這些步驟Step 2，但請務必在中為您選取 WorkSpaces. 如果您有多個容錯移轉區域，請重複這些步驟以尋找每個容錯移轉區域的連線識別符。

範例：使用 Route 53 設定 DNS 容錯移轉路由政策

下列範例會為您的網域設定公用託管區域。不過，您可以設定公用或私有託管區域。如需有關設定託管區域的詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的使用託管區域。

此範例也會使用容錯移轉路由政策。您可以針對跨區域重新導向策略使用其他路由政策類型。如需有關選擇 DNS 路由政策的資訊，請參閱《Amazon Route 53 開發人員指南》中的選擇路由政策。

當您在 Route 53 中設定容錯移轉路由政策時，主要區域需要進行運作狀態檢查。如需在 Route 53 中建立運作狀態檢查的詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的建立 Amazon Route 53 運作狀態檢查及設定 DNS 容錯移轉和建立、更新及刪除運作狀態檢查。

如果您想要在 Route 53 運作狀態檢查中使用 Amazon CloudWatch 警示，您還需要設定 CloudWatch 警示來監控主要區域中的資源。有關更多信息 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。如需有關 Route 53 如何在其運作狀態檢查中使用 CloudWatch 警示的詳細資訊，請參閱 Amazon Route 53 開發人員指南中的 Route 53 如何判斷用於監控 CloudWatch 警示和監控警示的運作狀態檢查狀態。 CloudWatch

若要在 Route 53 中設定 DNS 容錯移轉路由政策，您必須先為網域建立託管區域。

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇託管區域，然後選擇建立託管區域。
3. 在已建立的託管區域頁面上，在網域名稱之下輸入您的網域名稱 (例如 `example.com`)。

4. 在類型之下，選擇公共託管區域。
5. 選擇建立託管區域。

然後針對主要區域建立運作狀態檢查。

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇運作狀態檢查，然後選擇建立運作狀態檢查。
3. 在設定運作狀態檢查頁面上，輸入運作狀態檢查的名稱。
4. 對於要監控的內容，選取端點、其他健全狀況檢查的狀態 (計算的健全狀況檢查) 或 CloudWatch 警示狀態。
5. 根據您在上一個步驟中選取的項目，設定運作狀態檢查，然後選擇下一步。
6. 在運作狀態檢查失敗時收到通知頁面上，針對建立警示，選擇是或否。
7. 選擇建立運作狀態檢查。

建立運作狀態檢查之後，您可以建立 DNS 容錯移轉記錄。

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 在託管區域頁面上，選取您的網域名稱。
4. 在您網域名稱的詳細資訊頁面上，選擇建立記錄。
5. 在選擇路由政策頁面上選取容錯移轉，然後選擇下一步。
6. 在設定記錄頁面的基本組態下，針對記錄名稱，輸入您的子網域名稱。例如，如果您的 FQDN 是 `desktop.example.com`，請輸入 **`desktop`**。

   > **Note**
   >
   > 如果您想要使用根網域，請將記錄名稱保留空白。不過，我們建議您使用子網域，例如`desktop`或`workspaces`，除非您已設定網域僅供您 WorkSpaces的.

7. 針對記錄類型，選取 TXT - 用於驗證電子郵件寄件者和應用程式特定值。
8. 將 TTL 秒數設定保留為預設值。
9. 在要新增至 ***`your_domain_name`*** 的容錯移轉記錄下，選擇定義容錯移轉記錄。

現在，您需要針對主要和容錯移轉區域設定容錯移轉記錄。

範例：設定主要區域的容錯移轉記錄

1. 在定義容錯移轉記錄對話方塊中，針對值/路由傳送流量至，選取取決於記錄類型的 IP 位址或其他值。
2. 隨即開啟一個方塊，供您輸入範例文字項目。輸入主要區域之連線別名關聯的連線識別符。
3. 針對容錯移轉記錄類型，選取主要。
4. 針對運作狀態檢查，選取您為主要區域建立的運作狀態檢查。
5. 針對記錄 ID，輸入用於識別此記錄的描述。
6. 選擇定義容錯移轉記錄。您的新容錯移轉記錄會出現在要新增至 ***your_domain_name*** 的容錯移轉記錄之下。

範例：設定容錯移轉區域的容錯移轉記錄

1. 在要新增至 ***your_domain_name*** 的容錯移轉記錄下，選擇定義容錯移轉記錄。
2. 在定義容錯移轉記錄對話方塊中，針對值/路由傳送流量至，選取取決於記錄類型的 IP 位址或其他值。
3. 隨即開啟一個方塊，供您輸入範例文字項目。輸入容錯移轉區域之連線別名關聯的連線識別符。
4. 針對容錯移轉記錄類型，選取次要。
5. (選用) 針對運作狀態檢查，輸入您為容錯移轉區域建立的運作狀態檢查。
6. 針對記錄 ID，輸入用於識別此記錄的描述。
7. 選擇定義容錯移轉記錄。您的新容錯移轉記錄會出現在要新增至 ***your_domain_name*** 的容錯移轉記錄之下。

如果您為主要區域設定的健康狀態檢查失敗，您的 DNS 容錯移轉路由原則會將您的 WorkSpaces 使用者重新導向至容錯移轉區域。Route 53 會繼續監控您主要區域的健康狀態檢查，當您主要區域的健康狀態檢查不再失敗時，Route 53 會自動將您的 WorkSpaces 使用者重新導向至主要區域 WorkSpaces 中的使用者。

如需有關建立 DNS 記錄的詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的使用 Amazon Route 53 主控台建立記錄。如需有關設定 DNS TXT 記錄的詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的 TXT 記錄類型。

步驟 5：將連接字符串發送給您的 WorkSpaces 用戶

若要確保在中斷期間視需要重新導向使用者，您必須 WorkSpaces 將連接字串 (FQDN) 傳送給使用者。如果您已向 WorkSpaces 使用者核發區域註冊碼 (例如WSpdx+ABC12D)，則這些代碼仍然有效。不過，若要讓跨區域重新導向運作，您的使用 WorkSpaces 者 WorkSpaces 在用 WorkSpaces 戶端應用程式中註冊時，必須使用連接字串做為其註冊碼。

> **Important**
>
> 如果您在 WorkSpaces 主控台中建立使用者，而不是在 Active Directory 中建立使用者，則每當您啟 WorkSpaces 動新的時候，都會自動將邀請電子郵件傳送給您的使用者，其中包含區域型註冊碼 (例如WSpdx+ABC12D)。 WorkSpace即使您已經設定了跨區域重新導向，自動傳送給新的邀請電子郵件也會 WorkSpaces 包含此區域型註冊碼，而不是您的連線字串。
> 若要確定您的使用 WorkSpaces 者使用的是連接字串，而不是以區域為基礎的註冊碼，您必須使用下列程序傳送另一封含有連接字串的電子郵件給他們。

將連接字串傳送給您的 WorkSpaces 使用者

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主機的右上角，選取您的主要AWS地區 WorkSpaces。
3. 在導覽窗格中，選擇 WorkSpaces。
4. 在WorkSpaces頁面上，使用搜尋方塊來搜尋您要傳送邀請的使用者，然後 WorkSpace 從搜尋結果中選取對應的使用者。您一次只能選取一個 WorkSpace 。
5. 選擇動作、邀請使用者。
6. 在 [邀請使用者加入他們的 WorkSpaces] 頁面上，您會看到要傳送給使用者的電子郵件範本。
7. (選擇性) 如果有一個以上的連線別名與您的 WorkSpaces 目錄相關聯，請從 [連線別名字串] 清單中選取您希望使用者使用的連接字串。電子郵件範本會更新，以顯示您所選擇的字串。
8. 複製電子郵件範本文字，並使用您自己的電子郵件應用程式將其貼到給使用者的電子郵件中。在電子郵件應用程式中，您可以視需要修改內文。邀請電子郵件準備就緒時，請將其傳送給您的使用者。

跨區域重定向架構圖

下圖說明跨區域重新導向的部署程序。

> **Note**
>
> 跨區域重新導向僅有助於跨區域容錯移轉和後援。它不會促進次要區域中的建立和維護 WorkSpaces ，也不允許跨區域資料複寫。 WorkSpaces 在主要和次要區域中，應分別管理。

啟動跨區域重新導向

在中斷的情況下，您可以手動更新 DNS 記錄，或根據健康狀態檢查 (決定容錯移轉區域) 使用自動路由原則。我們建議遵循使用 Amazon Route 53 建立災難復原機制中概述的災難復原機制。

跨區域重新導向期間發生什麼狀況

在區域容錯移轉期間，您的 WorkSpaces 使用者會與其 WorkSpaces 在主要區域中斷連線。當他們嘗試重新連線時，他們會收到下列錯誤訊息：

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

然後系統會提示使用者再次登入。如果他們使用 FQDN 做為註冊碼，當他們再次登入時，您的 DNS 容錯移轉路由原則會將它們重新導向至您 WorkSpaces 在容錯移轉區域中為他們設定的。

> **Note**
>
> 在某些情況下，使用者可能無法於再次登入時重新連線。如果發生這種情況，它們必須關閉並重新啟動用 WorkSpaces 戶端應用程式，然後嘗試再次登入。

取消連線別名與目錄的關聯

只有擁有目錄的帳戶才能取消連線別名與目錄的關聯。

如果您已與其他帳戶共用連線別名，且該帳戶已將連線別名與該帳戶擁有的目錄建立關聯，則該帳戶必須用於取消連線別名與目錄的關聯。

若要取消連線別名與目錄的關聯

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主控台的右上角，選取含有您要取消關聯之連線別名的 AWS 區域。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。

4. 在跨區域重新導向關聯底下，選取連接字串，然後選擇動作、關聯/取消關聯。

   您也可以從連線別名詳細資訊頁面取消連線別名的關聯。若要這麼做，請在關聯的目錄下選擇取消關聯。

5. 在關聯/取消關聯頁面上，選擇取消關聯。
6. 在要求您確認取消關聯的對話方塊中，選擇取消關聯。

取消共用連線別名

只有連線別名的擁有者可以取消共用別名。如果您取消與某個帳戶共用連線別名，該帳戶就無法再將連線別名與目錄產生關聯。

若要取消共用連線別名

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主控台的右上角，選取含有您要取消共用之連線別名的 AWS 區域。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。
4. 在跨區域重新導向關聯底下，選取連接字串，然後選擇動作、共用/取消共用連線別名。

   您也可以從連線別名詳細資訊頁面取消共用連線別名。若要這麼做，請在共用帳戶底下選擇取消共用。

5. 在共用/取消共用連線別名頁面上，選擇取消共用。
6. 在要求您確認取消共用連線別名的對話方塊中，選擇取消共用。

刪除連線別名

只有在連線別名由您的帳戶擁有且並未與目錄相關聯時，您才可以刪除連線別名。

如果您已與其他帳戶共用連線別名，且該帳戶已將連線別名與該帳戶擁有的目錄建立關聯，則該帳戶必須先取消連線別名與目錄的關聯，您才能刪除連線別名。

> **Important**
>
> 建立連接字串之後，其一律與您的 AWS 帳戶相關聯。即使您從原始帳戶中刪除連接字串的所有執行個體，也無法使用不同的帳戶重新建立相同的連接字串。連接字串會全域保留給您的帳戶使用。

> **Warning**
>
> 如果您不再使用 FQDN 做為使用 WorkSpaces 者的註冊碼，則必須採取某些預防措施以防止潛在的安全性問題。如需詳細資訊，請參閱 停止使用跨區域重新導向時的安全性考量。

若要刪除連線別名

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主控台的右上角，選擇含有您要刪除之連線別名的 AWS 區域。
3. 在導覽窗格中，選擇 Account Settings (帳戶設定)。
4. 在跨區域重新導向關聯底下，選取連接字串，然後選擇刪除。

   您也可以從連線別名詳細資訊頁面刪除連線別名。若要這麼做，請選擇頁面右上角的刪除。

   > **Note**
   >
   > 如果已停用刪除按鈕，請確定您是別名的擁有者，並確定別名與目錄沒有關聯。

5. 在要求您要確認刪除的對話方塊中，選擇刪除。

關聯和取消關聯連線別名的 IAM 許可

如果您使用 IAM 使用者來建立或取消連線別名的關聯，該使用者必須具有 `workspaces:AssociateConnectionAlias` 和 `workspaces:DisassociateConnectionAlias` 的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
```

```
    }
  ]
}
```

Important

如果您要建立 IAM 政策來針對不擁有連線別名的帳戶，建立或取消連線別名的關聯，則無法在 ARN 中指定帳戶 ID。您必須改為使用 * 帳戶 ID，如下列範例政策所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

只有當該帳戶擁有要關聯或取消關聯的連線別名時，您才可以在 ARN 中指定帳戶 ID。

如需使用 IAM 的詳細資訊，請參閱 適用於 WorkSpaces 的身分和存取管理。

停止使用跨區域重新導向時的安全性考量

如果您不再使用 FQDN 作為使用 WorkSpaces 者的註冊碼，則必須採取下列預防措施，以防止潛在的安全性問題：

- 請務必向使用 WorkSpaces 者核發其 WorkSpaces 目錄的區域特定註冊碼 (例如`WSpdx+ABC12D`)，並指示他們停止使用 FQDN 做為其註冊碼。
- 如果您仍然擁有此網域，務必更新 DNS TXT 記錄以移除此網域，使其無法在網路釣魚攻擊中遭到利用。如果您從 DNS TXT 記錄中移除此網域，而您的使用 WorkSpaces 者嘗試使用 FQDN 做為其註冊碼，則他們的連線嘗試將無害地失敗。

- 如果您不再擁有此網域，您的使用 WorkSpaces 者必須使用其特定地區的註冊碼。如果他們繼續嘗試使用 FQDN 做為註冊碼，則可能會將其連線嘗試重新導向至惡意網站。

Amazon 的多區域彈性 WorkSpaces

Amazon WorkSpaces 多區域復原力 (MRR) 可讓您在主要區域因中斷事件而無法連線時，將使用者重新導向至次要 WorkSpaces 區域，而不需要使用者在登入待命時切換註冊碼。 WorkSpaces備用 WorkSpaces 是 Amazon WorkSpaces 多區域復原的一項功能，可簡化備用部署的建立和管理作業。在次要區域中設定使用者目錄後，請 WorkSpace 在您的主要區域中選取您要為其建立待命區域 WorkSpace 的。系統會自動將主要 WorkSpace 套裝軟體映像鏡像到次要區域。然後它會自動 WorkSpace 在您的次要區域佈建新的待命區域

Amazon WorkSpaces 多區域復原力建立在跨區域重新導向之上，該重新導向運用 DNS 運作狀態檢查和容錯移轉功能 它可讓您使用完整網域名稱 (FQDN) 做為 WorkSpaces 註冊碼。當您的使用者登入時 WorkSpaces，您可以根據 FQDN 的網域名稱系統 (DNS) 原則，在支援的 WorkSpaces 區域中重新導向使用者。如果您使用 Amazon Route 53，建議您在設計跨區域重新導向策略時，使用運作狀態檢查來監控 Amazon CloudWatch 警示。 WorkSpaces如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的建立 Amazon Route 53 運作狀態檢查和設定 DNS 容錯移轉。

資料複製是待命的附加功能， WorkSpaces 可將資料從主要區域單向複製到次要區域。啟用資料複製後，系統和使用者磁碟區的 EBS 快照會每 12 小時建立一次。多區域復原力會定期檢查是否有新的快照。找到快照後，它會啟動次要區域的副本。當副本到達次要區域時，它們會用來更新次要區域 WorkSpace。

目錄

必要條件

- 在建立待命狀態之前，您必須在主要區域中 WorkSpaces 為您的使用者建立 WorkSpaces。如需建立的更多資訊 WorkSpaces，請參閱使用 WorkSpaces 啟動虛擬桌面。
- 若要在待命時啟用資料複寫 WorkSpaces，您應該有一個自我管理的 Active Directory 或 AWS 受管理的 Microsoft AD 設定為複寫到您的待命區域。如需詳細資訊，請參閱建立 AWS 受管理的 Microsoft AD 目錄和新增複寫的區域。
- 請務必更新主要 WorkSpaces伺服器上的網路相依性驅動程式，例如 ENA、NVMe 和 PV 驅動程式。您應該至少每 6 個月執行一次。如需詳細資訊，請參閱針對 Windows 執行個體安裝或升級彈性網路介面卡 (ENA) 驅動程式和升級 Windows 執行個體上的 PV 驅動程式。AWS NVMe 驅動程式
- 請務必定期將 EC2Config、EC2Launch 和 EC2Launch V2 代理程式更新為最新版本。您應該至少每 6 個月執行一次。如需詳細資訊，請參閱更新 EC2Config 和 EC2 啟動。
- 若要確保資料複寫正確，請確定 FQDN、OU 和使用者 SID 的主要和次要區域中的作用中目錄是同步的。
- 待命的預設配額 (限制) WorkSpaces 為 0。在建立待命狀態之前，您必須要求提高服務配額 WorkSpace。如需詳細資訊，請參閱 Amazon WorkSpaces 配額。
- 確保您使用客戶管理的金鑰來加密您的主要金鑰和待命金鑰 WorkSpaces。您可以使用單一區域金鑰或多區域金鑰來加密主要金鑰和待命 WorkSpaces金鑰。

限制

- 「待命」 WorkSpaces 只會複製主要影像的套裝影像， WorkSpaces 但不會從主要磁碟區複製系統磁碟區 (C 磁碟機) 或使用者磁碟區 (磁碟機 D) WorkSpaces。若要將系統磁碟區 (C 磁碟機) 或使用者磁碟區 (磁碟機 D) 從主磁碟區複製 WorkSpaces 到備用磁碟區 WorkSpaces，您必須啟用資料複製。
- 您無法直接修改、重建、還原或移轉待命 WorkSpace。
- 跨區域重新導向的容錯移轉是由 DNS 設定所控制。若要實作自動容錯移轉案例，您必須使用不同機制搭配跨區域重新導向。例如，您可以使用 Amazon Route 53 容錯移轉 DNS 路由政策，搭配 Route 53 運作狀態檢查來監控主要區域中的 CloudWatch 警示。如果呼叫主要區域中的 CloudWatch 警示，您的 DNS 容錯移轉路由原則會將您的 WorkSpaces 使用者重新導向至您在容錯移轉區域中為他們設定的警示。 WorkSpaces
- 資料複製只有一種方法，將資料從主要區域複製到次要區域。在待命 WorkSpaces 容錯移轉期間，您可以在 12 到 24 小時之間存取資料和應用程式。中斷後，請手動備份您在次要資料上建立的所有

資料 WorkSpace 並登出。我們建議您將工作儲存到外接式磁碟機 (例如網路磁碟機)，以便您可以從主要磁碟機存取資料 WorkSpace。

- 資料複製不支援 S AWS imple AD。
- 當您在待命時啟用資料複製時 WorkSpaces，會每 12 小時建立主要磁碟區 WorkSpaces (包括根磁碟區和系統磁碟區) 的 EBS 快照。特定資料磁碟區的初始快照已完整，而後續快照則是增量快照。因此，指 WorkSpace 定的第一個複製需要比後續複製更長的時間。快照會根據內部的排程啟動 WorkSpaces ，您無法控制時間。
- 如果主要 WorkSpace 和待命 WorkSpace 加入使用相同的網域，我們建議您僅在指定時間點連線到主要 WorkSpace 或待命狀態 WorkSpace ，以避免失去與網域控制站的連線。
- 如果您 AWS Managed Microsoft AD 設定多區域複寫，則只有主要區域中的目錄可以註冊以與搭配 WorkSpaces使用。如果您嘗試在複寫的區域中註冊目錄以供搭配使用 WorkSpaces，它將會失敗。AWS Managed Microsoft AD 不支援在複寫區域 WorkSpaces 內使用的多區域複寫。
- 如果您已經設定跨區域重新導向，並且 WorkSpaces 在主要和次要區域中建立而未使用待命區域 WorkSpaces，則無法 WorkSpace 直接將次要區域 WorkSpace 中的現有區域轉換為待命區域。相反地，您需要在次要區域中關閉， WorkSpace 在您的主要區域 WorkSpace 中選取要 WorkSpace 為其建立待命的區域，然後使用 standby WorkSpaces 來建立待命狀態 WorkSpace。
- 中斷後，請手動備份您在次要資料上建立的所有資料 WorkSpace 並登出。我們建議您將工作儲存到外接式磁碟機 (例如網路磁碟機)，以便您可以從主要磁碟機存取資料 WorkSpace。
- WorkSpaces 以下地區目前提供多區域復原能力：
  - 美國東部 (維吉尼亞北部) 區域
  - 美國西部 (奧勒岡) 區域
  - 歐洲 (法蘭克福) 區域
  - 歐洲 (愛爾蘭) 區域
- WorkSpaces 只有在 3.0.9 版或更新版本的 Linux、macOS 和 Windows WorkSpaces 用戶端應用程式上才支援多區域復原能力。您也可以使用多區域恢復能力搭配 Web Access。
- WorkSpaces 多區域復原能力支援 Windows 和自攜授權 (BYOL)。 WorkSpaces它不支持 Amazon Linux，Ubuntu WorkSpaces 或 GPU 啟用 WorkSpaces （例如圖形，圖形 GraphicsPro，G4dn 或 .g4dn）。 GraphicsPro
- 容錯移轉或容錯回復完成後，請等待 15 到 30 分鐘，然後再連線到您的 WorkSpace.

設定您的多區域彈性待命 WorkSpace

設定您的多區域彈性待命 WorkSpace

1. 在主要和次要區域中設定使用者目錄。請務必在每個區域的每個 WorkSpaces 目錄中使用相同的使用者名稱。

   若要讓 Active Directory 使用者資料保持同步，我們建議您使用 AD Connector 指向您 WorkSpaces 為使用者設定的每個區域中的相同 Active Directory。如需有關建立目錄的詳細資訊，請參閱使用註冊目錄 WorkSpaces。

   > **Important**
   >
   > 如果您將 AWS Managed Microsoft AD 目錄設定為多區域複寫，則只有主要區域中的目錄可以註冊以與搭配 WorkSpaces使用。嘗試在複製的區域中註冊目錄以供使用 WorkSpaces 將會失敗。 AWS Managed Microsoft AD 不支援在複寫區域 WorkSpaces 內使用的多區域複寫。

2. 在主要區域中 WorkSpaces 為您的使用者建立。如需有關建立的詳細資訊 WorkSpaces，請參閱 Launch WorkSpaces。
3. 在次要區域 WorkSpace 中建立待命。如需有關建立待命的詳細資訊 WorkSpace，請參閱建立待命 WorkSpace。
4. 建立連接字串 (FQDN) 並將其與主要和次要區域中的使用者目錄建立關聯。

   您必須在帳戶中啟用跨區域重新導向，因為待命 WorkSpaces 是建立在跨區域重新導向的基礎上。請遵循 Amazon WorkSpaces 跨區域重新導向指示的步驟 1-3。
5. 設定 DNS 服務並設定 DNS 路由原則。

   您必須設定 DNS 服務並設定必要的 DNS 路由原則。跨區域重新導向會與 DNS 路由原則搭配使用，視需要重新導向 WorkSpaces 使用者。
6. 完成跨區域重新導向的設定時，您必須將含有 FQDN 連接字串的電子郵件傳送給使用者。如需詳細資訊，請參閱步驟 5：將連接字串傳送給 WorkSpaces 使用者。請確定您的使用 WorkSpaces 者使用 FQDN 型註冊碼，而不是以區域為基礎的註冊碼 (例如，WSPDX+ABC12d) 做為其主要區域。

> **Important**
>
> - 如果您在 WorkSpaces 主控台中建立使用者，而不是在 Active Directory 中建立使用者，則每當您啟 WorkSpaces 動新的時候，都會自動傳送邀請電子郵件給您的使用者，並以區域為基礎的註冊碼。 WorkSpace這表示當您 WorkSpaces 為次要區域的使用者設定時，您的使用者也會自動收到這些次要區域的電子郵件 WorkSpaces。您需要指示使用者忽略包含區域型註冊碼的電子郵件。
> - 區域特定的註冊碼仍然有效；不過，若要讓跨區域重新導向運作，您的使用者必須改用 FQDN 做為其註冊碼。

建立待命 WorkSpace

在建立待命之前 WorkSpace，請確定您已完成先決條件，包括在主要和次要區域中建立使用者目錄、在主要區域中 WorkSpaces 為使用者佈建、在帳戶中設定跨區域重新導向，以及透過服務配額要求提高待命 WorkSpaces 限制。

建立待命 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主機的右上角，選取您的主要 AWS 地區 WorkSpaces。
3. 在導覽窗格中，選擇 WorkSpaces。
4. 選取 WorkSpace 您要為其建立待命 WorkSpace 的備用項目。
5. 選擇動作，然後選擇建立待命 WorkSpace。
6. 選取您要在其中建立待命區域的次要區域 WorkSpace，然後選擇 [下一步]。
7. 選取次要區域中的使用者目錄，然後選擇下一步。
8. (選擇性) 新增加密金鑰、啟用資料加密及管理標籤。
   - 若要新增加密金鑰，請在「輸入加密金鑰」下輸入加密金鑰。
   - 若要啟用資料複製，請選擇 [啟用資料複製]。然後，勾選核取方塊以確認您授權每月額外費用。
   - 若要新增標籤，請選擇「新增標籤」。

   然後選擇下一步。

> **Note**
>
> - 如果原始檔案 WorkSpace 已加密，則會預先填入此欄位。但是，您可選擇以自己的加密金鑰來取代它。
> - 更新資料複製狀態需要幾分鐘的時間。
> - 使用主要快照成功更新待命 WorkSpace 之後 WorkSpace，您可以在 [復原快照] 底下找到快照的時間戳記。

9. 檢閱待命設定， WorkSpaces 然後選擇 [建立]。

> **Note**
>
> - 若要檢視待命資訊 WorkSpaces，請前往主要 WorkSpace 詳細資訊頁面。
> - 待命模式 WorkSpace 只會複製主要磁碟區的套裝軟體映像， WorkSpace 但不會從您的主要磁碟區複製系統磁碟區 (C 磁碟機) 或使用者磁碟區 (磁碟機 D) WorkSpaces。預設情況下，資料複製處於關閉狀態。若要將系統磁碟區 (C 磁碟機) 或使用者磁碟區 (磁碟機 D) 從主磁碟區複製 WorkSpaces 到備用磁碟區 WorkSpaces，您必須啟用資料複製。

管理待命 WorkSpace

您無法直接修改、重建、還原或移轉待命 WorkSpace。

啟用待命資料複製 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 轉到您的主要區域，選擇主要 WorkSpace ID。
3. 向下捲動至待命 WorkSpace 區段，然後選擇編輯待命狀態 WorkSpace。
4. 選擇 [啟用資料複製]。然後，勾選核取方塊以確認您授權每月額外費用。然後選擇 Save (儲存)。

Note

- 待命 WorkSpaces 無法進入休眠狀態。如果您停止待命 WorkSpace，則不會保留您未儲存的工作。我們建議使用者在結束待命之前一律儲存工作 WorkSpaces。
- 若要在待命時啟用資料複寫 WorkSpaces，您應該有一個自我管理的 Active Directory 或 AWS 受管理的 Microsoft AD 設定為複寫到您的待命區域。若要設定目錄，請按照使用 Amazon WorkSpaces 和 AWS Directory 服務建立業務連續性逐步解說一節中的步驟 1 到 3 進行操作，或參閱在 Amazon WorkSpaces 搭配使用多區域 AWS 受管 Active Directory。只有 AWS 受管理 Microsoft AD 的企業版才支援多區域複寫。
- 更新資料複製狀態需要幾分鐘的時間。
- 使用主要快照成功更新待命 WorkSpace 之後 WorkSpace，您可以在 [復原快照] 底下找到快照的時間戳記。

刪除待命 WorkSpace

您可以使用與終止常規相同 WorkSpace 的方式終止待命 WorkSpace。

刪除待命 WorkSpace

1. 請在以下位置開啟 WorkSpaces 主控台。 https://console.aws.amazon.com/workspaces/
2. 在主機的右上角，選取您的主要 AWS 地區 WorkSpaces。
3. 在導覽窗格中，選擇 WorkSpaces。
4. 選取待 WorkSpace 命，然後選擇刪除。刪除待命狀態大約需要 5 分鐘 WorkSpace。刪除期間，待命狀態 WorkSpace 將設定為「終止」。刪除完成後，待命狀態 WorkSpace 會從主控台中消失。

Note

刪除待命 WorkSpace 是永久動作，無法復原。待命 WorkSpace 用戶的數據不會持續存在並被銷毀。如需備份使用者資料的協助，請聯絡 Sup AWS port 部門。

單向備用資料複製 WorkSpaces

在「多區域復原」中啟用資料複製功能，可讓您將資料從主要區域複製到次要區域。在穩定狀態下，多區域恢復力 WorkSpaces 每 12 小時捕獲一次主系統（C 槽）和主驅動器數據（D 驅動器）的快照。這些快照會傳輸到次要區域，並用來更新待命 WorkSpaces。依預設，待命狀態為停用資料複製 WorkSpaces。

啟用待命資料複製後 WorkSpaces，特定資料磁碟區的初始快照就會完成，而後續的快照則是增量的。因此，指定 WorkSpace 的第一個複製需要比後續複製更長的時間。快照會以預先決定的間隔在內觸發， WorkSpaces 且使用者無法控制時間。

在容錯移轉期間，當使用者被重新導向至次要區域時，他們可以使 WorkSpaces 用 12 到 24 小時之間的資料和應用程式存取其待命狀態。當使用者使用待命時 WorkSpaces，「多區域復原」不會強制使用者登出待命狀態， WorkSpaces 或使用主要區域 WorkSpaces 的快照更新待命狀態。

中斷後，使用者應手動備份他們在其次要資料上建立的任何資料，然後 WorkSpaces 再登出待命狀態 WorkSpaces。當他們再次登入時，系統會將他們導向至主要區域及其主要區域 WorkSpaces。

計劃保留 Amazon EC2 容量以進行恢復

Amazon 多區域復原力 (MRR) 預設依賴 Amazon EC2 隨需儲存池。如果特定的 Amazon EC2 執行個體類型無法支援您的復原，MRR 會自動嘗試重複擴展執行個體，直到找到可用的執行個體類型為止，但在極端情況下，執行個體可能並不總是可用。若要改善最關鍵執行個體類型所需的可用性 WorkSpaces，請聯絡 Sup AWS port 部門，我們將協助您進行容量規劃。

Amazon WorkSpaces 的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。如要了解適用於 WorkSpaces 的合規計劃，請參閱合規計劃的 AWS 服務範圍。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規

本文件有助於您了解如何在使用 WorkSpaces 時套用共同責任模型。它會示範如何設定 WorkSpaces 以符合您的安全性和合規目標。您也會了解如何使用其他 AWS 服務來協助監控並保護 WorkSpaces 資源。

目錄

Amazon 的數據保護 WorkSpaces

AWS 共同責任模型適用於 Amazon 中的資料保護 WorkSpaces。如此模型所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API WorkSpaces 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

如需 WorkSpaces 和 FIPS 端點加密的詳細資訊，請參閱針對 FedRAMP 授權或 DoD SRG 合規設定 Amazon WorkSpaces。

靜態加密

您可以 WorkSpaces 使用 AWS KMS Key 來加密儲存磁碟區 AWS Key Management Service。如需詳細資訊，請參閱 加密 WorkSpaces。

使 WorkSpaces 用加密磁碟區建立時，請 WorkSpaces 使用 Amazon Elastic Block Store (Amazon EBS) 來建立和管理這些磁碟區。EBS 會使用業界標準的 AES-256 演算法資料金鑰加密您的磁碟區。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的亞馬遜 EBS 加密。

傳輸中加密

對於 PCoIP，傳輸中的資料會使用 TLS 1.2 加密和 SigV4 要求簽署加密。PCoIP 通訊協定使用加密的 UDP 流量 (採用 AES 加密) 來串流像素。使用連接埠 4172 (TCP 和 UDP) 的串流連線已使用 AES-128 和 AES-256 密碼加密，但加密預設為 128 位元。您可以使用 Windows 的設定 PCoIP 安全性設定群組原則設定，或修改 Amazon Linux 檔案中的 PCoIP 安全性設定 WorkSpaces，將此預設值變更為 256 位元。`pcoip-agent.conf` WorkSpaces

若要進一步了解 Amazon 的群組原則管理 WorkSpaces，請參閱設定 PCoIP 安全設定中的管理您的視窗 WorkSpaces。若要進一步了解如何修改 `pcoip-agent.conf` 檔案，請參閱 Teradici 文件中的 控制 Amazon 伺服器上的 PCoIP 代理程式行為 WorkSpaces 和 PCoIP 安全設定。

對於 WorkSpaces 串流通訊協定 (WSP)，傳輸中的串流和控制資料會使用 DTLS 1.2 加密來加密 UDP 流量，並針對 TCP 流量使用 TLS 1.2 加密 (使用 AES-256 加密) 加密。

適用於 WorkSpaces 的身分和存取管理

根據預設，IAM 使用者不具備 WorkSpaces 資源和操作的許可。若要允許 IAM 使用者管理 WorkSpaces 資源，您必須建立 IAM 政策，明確將許可授予使用者，然後將該政策連接到需要該些許可的 IAM 使用者或群組。

若要提供存取權，請新增許可到您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

  建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的建立許可集合中的指示。
- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請遵循《IAM 使用者指南》的為第三方身分提供者 (聯合) 建立角色中的指示。
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請遵循《IAM 使用者指南》的為 IAM 使用者建立角色中的指示。
  - (不建議) 將政策直接連接至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的新增許可到使用者 (主控台)中的指示。

如需 IAM 政策的詳細資訊，請參閱《IAM 使用者指南》中的政策和許可。

WorkSpaces 也會建立 IAM 角色 `workspaces_DefaultRole`，讓 WorkSpaces 服務能夠存取必要的資源。

如需 IAM 的詳細資訊，請參閱身分和存取管理 (IAM) 和 IAM 使用者指南。您可以在《IAM 使用者指南》中的 Amazon WorkSpaces 的動作、資源和條件索引鍵，找到可用於 IAM 許可政策的 WorkSpaces 特有資源、動作和條件內容索引鍵。

如需協助您建立 IAM 政策的工具，請參閱 AWS 政策產生器。您也可以使用 IAM 政策模擬器，測試政策會允許還是拒絕對 AWS 的特定請求。

> **Note**
>
> Amazon WorkSpaces 不支援在 WorkSpace 中佈建 IAM 憑證 (例如使用執行個體設定檔)。

目錄

政策範例

以下範例顯示您可以用來控制 IAM 使用者具有之 Amazon WorkSpaces 許可的政策陳述式。

Example 1：執行所有 WorkSpaces 任務

下列政策陳述式授予 IAM 使用者執行所有 WorkSpaces 任務的許可，包括建立和管理目錄。它還授予執行快速設定程序的許可。

雖然 Amazon WorkSpaces 在使用 API 和命令列工具時完全支援 `Action` 和 `Resource` 元素，但若要從 AWS Management Console 使用 Amazon WorkSpaces，IAM 使用者必須具有下列動作和資源的許可：

- 動作：`workspaces:*" 和 "ds:*"`
- 資源：`"Resource": "*"`

下列政策範例顯示如何允許 IAM 使用者從 AWS Management Console 使用 Amazon WorkSpaces。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
```

```
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Example 2：執行 WorkSpace 特有任務

下列政策陳述式授予 IAM 使用者執行 WorkSpace 特定工作 (例如啟動和移除 WorkSpaces) 的許可。在政策陳述式中，ds:* 動作可授與廣泛的許可—完全控制帳戶中的所有目錄服務物件。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

若要同時授予使用者在 WorkSpaces 內為使用者啟用 Amazon WorkDocs 的能力，請新增下列範例所示的 workdocs 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

若要同時授予使用者使用「啟動 WorkSpaces」精靈的能力，請新增如下列範例所示的 kms 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3：執行 BYOL WorkSpaces 的所有 WorkSpaces 任務

下列政策陳述式授予 IAM 使用者執行所有 WorkSpaces 任務的許可，包括建立自帶授權 (BYOL) WorkSpaces 所需的 Amazon EC2 任務。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
```

```
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

在 IAM 政策中指定 WorkSpaces 資源

若要在政策陳述式的 `Resource` 元素中指定 WorkSpaces 資源，請使用資源的 Amazon Resource Name (ARN)。您可藉由允許或拒絕使用 IAM 政策陳述式的 `Action` 元素中指定的 API 動作的許可，控制對 WorkSpaces 資源的存取。WorkSpaces 定義 WorkSpaces、套件、IP 群組和目錄的 ARN。

WorkSpace ARN

WorkSpace ARN 具有下列範例所示的語法。

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

WorkSpace 所在的區域 (例如 us-east-1)。

account_id

AWS 帳戶的 ID，無連字號 (例如 123456789012)。

workspace_identifier

WorkSpace 的 ID (例如 ws-a1bcd2efg)。

以下是識別特定 WorkSpace 之政策陳述式的 Resource 元素格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

您可使用 * 萬用字元來指定屬於特定區域中特定帳戶的所有 WorkSpaces。

映像 ARN

WorkSpace 映像 ARN 具有下列範例所示的語法。

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

region

WorkSpace 映像所在的區域 (例如 us-east-1)。

account_id

AWS 帳戶的 ID，無連字號 (例如 123456789012)。

bundle_identifier

WorkSpace 映像的 ID (例如 wsi-a1bcd2efg)。

以下是識別特定映象之政策陳述式 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

您可使用 * 萬用字元來指定屬於特定區域中特定帳戶的所有映像。

套件 ARN

套件 ARN 具有下列範例所示的語法。

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

region

WorkSpace 所在的區域 (例如 us-east-1)。

account_id

AWS 帳戶的 ID，無連字號 (例如 123456789012)。

bundle_identifier

WorkSpace 套件的 ID (例如 wsb-a1bcd2efg)。

以下是識別特定套件之政策陳述式 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

您可使用 * 萬用字元來指定屬於特定區域中特定帳戶的所有套件。

IP 群組 ARM

IP 群組 ARN 具有下列範例所示的語法。

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

region

WorkSpace 所在的區域 (例如 us-east-1)。

account_id

AWS 帳戶的 ID，無連字號 (例如 123456789012)。

ipgroup_identifier

IP 群組的 ID (例如 wsipg-a1bcd2efg)。

以下是識別特定 IP 群組之政策陳述式 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

您可使用 * 萬用字元來指定屬於特定區域中特定帳戶的所有 IP 群組。

目錄 ARN

目錄 ARN 具有下列範例所示的語法。

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

region

WorkSpace 所在的區域 (例如 us-east-1)。

account_id

AWS 帳戶的 ID，無連字號 (例如 123456789012)。

directory_identifier

目錄的 ID (例如 d-12345a67b8)。

以下是識別特定目錄之政策陳述式 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

您可使用 * 萬用字元來指定屬於特定區域中特定帳戶的所有目錄。

連線別名 ARN

連線別名 ARN 具有下列範例所示的語法。

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

region

連線別名所在的區域 (例如 us-east-1)。

account_id

AWS 帳戶的 ID，無連字號 (例如 123456789012)。

connectionalias_identifier

連線別名的 ID (例如 wsca-12345a67b8)。

以下是識別特定連線別名之政策陳述式 Resource 元素的格式。

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

您可使用 * 萬用字元來指定屬於特定區域中特定帳戶的所有連線別名。

不支援資源層級許可的 API 動作

您不能使用以下 API 動作指定資源 ARN：

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages

- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

對於不支援資源層級許可的 API 動作，您必須指定下列資源陳述式，如下列範例所示。

```
"Resource": "*"
```

不支援共用資源帳戶層級限制的 API 動作

對於下列 API 動作，如果帳戶並未擁有資源，則無法在資源 ARN 中指定帳號 ID：

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

對於這些 API 動作，只有在帳戶擁有要採取動作的資源時，您才可在資源 ARN 中指定帳戶 ID。當帳戶並未擁有資源時，您必須針對帳戶 ID 指定 *，如以下範例所示。

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

建立 workspaces_DefaultRole 角色

您必須先確認名為 workspaces_DefaultRole 的角色是否存在，才能使用 API 註冊目錄。此角色是由快速設定建立，或者如果您使用 AWS Management Console 啟動 WorkSpace，此角色則可授予 Amazon WorkSpaces 代表您存取特定 AWS 資源的許可。如果此角色不存在，您可以使用下列程序加以建立。

建立 workspaces_DefaultRole 角色

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。

2. 在左側導覽窗格中，選擇 Roles (角色)。
3. 選擇建立角色。
4. 在 Select type of trusted entity (選取信任的實體類型) 下，選擇 Another AWS account (另一個 帳戶)。
5. 針對帳戶 ID，輸入不含連字號或空格的帳戶 ID。
6. 針對選項，請勿指定多重要素驗證 (MFA)。
7. 選擇 Next: Permissions (下一步：許可)。
8. 在附加許可證測頁面上，選取 AWS 受管政策 AmazonWorkSpacesServiceAccess 和 AmazonWorkSpacesSelfServiceAccess。
9. 在設定許可界限之下，建議您不要使用許可界限，因為附加至此角色的政策可能發生衝突。這類衝突可能會封鎖角色的某些必要許可。
10. 選擇下一步：標籤。
11. 在新增標籤 (選用) 頁面上，視需要新增標籤。
12. 選擇 Next:Review (下一步：檢閱)。
13. 在 Review (檢閱) 頁面，針對 Role name (角色名稱) 輸入 **workspaces_DefaultRole**。
14. (選用) 針對 Role description (角色描述)，輸入描述。
15. 選擇建立角色。
16. 在 workspaces_DefaultRole 角色的摘要頁面上，選擇信任關係索引標籤。
17. 在 Trust relationships (信任關係) 標籤上，選擇 Edit trust relationship (編輯信任關係)。
18. 在編輯信任關係頁面上，以下列陳述式取代現有的政策陳述式。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. 選擇 Update Trust Policy (更新信任政策)。

建立 AmazonWorkSpacesPCAAccess 服務角色

您必須先確認名為 AmazonWorkSpacesPCAAccess 的角色是否存在，使用者才能使用憑證型驗證進行登入。當您在使用 AWS Management Console 的目錄上啟用憑證型驗證時，就會建立此角色，並授予 Amazon WorkSpaces 代表您存取 AWS Private CA 資源的許可。如果因為您未使用主控台來管理憑證型驗證而不存在此角色，您可以使用下列程序加以建立。

使用 AWS CLI 建立 AmazonWorkSpacesPCAAccess 服務角色

1. 使用以下文字建立名為 AmazonWorkSpacesPCAAccess.json 的 JSON 檔案。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 視需要調整 AmazonWorkSpacesPCAAccess.json 路徑並執行下列 AWS CLI 命令以建立服務角色，並附加 AmazonWorkspacesPCAAccess 受管政策。

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

WorkSpaces 的 AWS 受管政策

相較於自己撰寫政策，使用 AWS 受管政策更容易將許可新增至使用者、群組和角色。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中可用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 服務會維護和更新 AWS 受管政策。您無法更改 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外，AWS 支援跨越多項服務之任務職能的受管政策。例如，ReadOnlyAccess AWS 受管政策提供針對所有 AWS 服務和資源的唯讀存取權限。當服務啟動新功能時，AWS 會為新的操作和資源新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的 AWS 受管政策。

AWS 受管政策：AmazonWorkSpacesAdmin

此政策提供對 Amazon WorkSpaces 管理動作的存取許可。其可提供下列許可：

- workspaces - 允許存取以對 WorkSpaces 資源執行管理動作。
- kms - 允許存取以列出和描述 KMS 金鑰以及列表別名。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
```

```
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管政策：AmazonWorkspacesPCAAccess

此受管政策可供存取 AWS 帳戶中的 AWS Certificate Manager 私有憑證授權機構 (私有 CA) 資源，以進行憑證型驗證。其包含在 AmazonWorkSpacesPCAAccess 角色中，並提供下列許可：

- `acm-pca` - 允許存取 AWS 私有 CA 以管理憑證型驗證。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

AWS 受管政策：AmazonWorkSpacesSelfServiceAccess

此政策可供存取 Amazon WorkSpaces 服務，以執行使用者初始的 WorkSpaces 自助式動作。其包含在 `workspaces_DefaultRole` 角色中，並提供下列許可：

- `workspaces` - 允許存取使用者的自助式 WorkSpaces 管理功能。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 受管政策：AmazonWorkSpacesServiceAccess

此政策可供客戶帳戶存取 Amazon WorkSpaces 服務，以便啟動 WorkSpace。其包含在 `workspaces_DefaultRole` 角色中，並提供下列許可：

- `ec2` - 允許存取以管理與 WorkSpace 相關聯的 Amazon EC2 資源，例如網路介面。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

WorkSpaces 對 AWS 受管政策的更新

檢視自此服務開始追蹤這些變更以來，有關 WorkSpaces 的 AWS 受管政策更新詳細資訊。

變更	描述	日期
the section called “AmazonWorkSpacesAdmin” - 更新的政策	WorkSpaces 將 `workspaces:RestoreWorkspace` 動作新增至 Amazon WorkSpacesAdmin 受管政策，並授予管理員還原 WorkSpaces 的存取權。	2023 年 6 月 25 日
the section called “AmazonWorkspacesPCAAccess” - 新增的政策。	WorkSpaces 新增了新的受管政策來授與管理 AWS 私有 CA 的 `acm-pca` 許可，以便管理憑證型驗證。	2022 年 11 月 18 日
WorkSpaces 已開始追蹤變更	WorkSpaces 已開始追蹤其 WorkSpaces 受管政策的變更。	2021 年 3 月 1 日

Amazon WorkSpaces 的合規驗證

在多個 AWS 合規計劃中，第三方稽核人員會評估 Amazon WorkSpaces 的安全與合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計畫的 AWS 服務範圍清單，請參閱合規計畫的 AWS 服務範圍。如需一般資訊，請參閱 AWS 合規計劃。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

如需 WorkSpaces 和 FedRAMP 的詳細資訊，請參閱 針對 FedRAMP 授權或 DoD SRG 合規設定 Amazon WorkSpaces。

您使用 WorkSpaces 時的合規責任取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供以下資源協助您處理合規事宜：

- 安全與合規快速入門指南：這些部署指南討論架構考量，並提供在 AWS 上部署以安全及合規為重心之基準環境的步驟。
- Amazon Web Services 的 HIPAA 安全與合規架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規範的應用程式。
- AWS 合規資源：這組手冊和指南可能適用於您的產業和位置。
- 《AWS Config 開發人員指南》中的使用規則評估資源：AWS Config 可評估資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub：此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

Amazon WorkSpaces 的恢復能力

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需有關 AWS 區域與可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

Amazon WorkSpaces 也提供跨區域重新導向，這項功能可與您的網域名稱系統 (DNS) 容錯移轉路由政策搭配運作，以在 WorkSpaces 使用者的主要 WorkSpaces 無法使用時，將他們重新導向至另一個 AWS 區域中的替代 WorkSpaces。如需詳細資訊，請參閱 Amazon 的跨區域重新導向 WorkSpaces。

Amazon WorkSpaces 的基礎設施安全

Amazon WorkSpaces 是一項受管服務，受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 WorkSpaces。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密 (PFS) 的密碼套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

網路隔離

Virtual Private Cloud (VPC) 是 AWS 雲端中您自己的邏輯隔離區域中的虛擬網路。您可以將 WorkSpaces 部署到 VPC 的私有子網路。如需詳細資訊，請參閱 設定虛 VPC WorkSpaces。

若要只允許來自特定位址範圍的流量 (例如，來自您的公司網路)，請更新 VPC 的安全群組或使用 IP 存取控制群組。

您可使用有效的憑證來限制 WorkSpace 對受信任裝置的存取。如需詳細資訊，請參閱 限制對 WorkSpaces 受信任設備的訪問。

實體主機上的隔離

相同實體主機上的不同 WorkSpaces 已透過 Hypervisor 彼此隔離。就好像它們位於不同的實體主機上一樣。刪除 WorkSpace 時，Hypervisor 會先清除配置給它的記憶體 (設定為零)，然後再將其配置到新的 WorkSpace。

公司使用者驗證

使用 WorkSpaces 時，目錄可透過 AWS Directory Service 管理。您可以為使用者建立獨立的受管理目錄。或者，您也可與現有的 Active Directory 環境整合，讓使用者可以使用其目前的認證來取得企業資源的無縫存取權。如需詳細資訊，請參閱 管理 WorkSpaces 的目錄。

若要進一步控制對 WorkSpaces 的存取，請使用多重要素驗證。如需詳細資訊，請參閱如何啟用 AWS 服務的多重要素驗證。

透過 VPC 介面端點提出 Amazon WorkSpaces API 請求

您可以透過虛擬私有雲端 (VPC) 中的介面端點直接連線至 Amazon WorkSpaces API 端點，而不是透過網際網路進行連線。使用 VPC 介面端點時，VPC 與 Amazon WorkSpaces API 端點之間的通訊會完全在 AWS 網路內安全地進行。

> **Note**
>
> 此功能只能用於連線到 WorkSpaces API 端點。若要使用 WorkSpaces 用戶端連線至 WorkSpaces，需要網際網路連線能力，如 的 IP 位址和連接埠需求 WorkSpaces 所述。

Amazon WorkSpaces API 端點支援由 AWS PrivateLink 提供支援的 Amazon Virtual Private Cloud (Amazon VPC) 介面端點。每個 VPC 端點都是由您的 VPC 子網路中一個或多個具私有 IP 地址的網路介面 (也稱為彈性網路介面，或 ENI) 來表示。

VPC 介面端點可直接將 VPC 連線至 Amazon WorkSpaces，不需透過網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公用 IP 位址，就能與 Amazon WorkSpaces API 端點進行通訊。

您可以建立介面端點，以使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI) 命令連線到 Amazon WorkSpaces。如需說明，請參閱建立界面端點。

建立 VPC 端點之後，您可透過下列使用 `endpoint-url` 參數的 CLI 命令範例，將介面端點指定至 Amazon WorkSpaces API 端點：

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

如果您為 VPC 端點啟用私有 DNS 主機名稱，則不需要指定端點 URL。CLI 和 Amazon WorkSpaces SDK 根據預設使用的 Amazon WorkSpaces API DNS 主機名稱 (https://api.workspaces.*Region*.amazonaws.com) 會解析為您的 VPC 端點。

Amazon WorkSpaces API 端點在所有可使用 Amazon VPC 和 Amazon WorkSpaces 的 AWS 區域中支援 VPC 端點。Amazon WorkSpaces 支援在您的 VPC 內呼叫其所有的公用 API。

若要進一步了解 AWS PrivateLink，請參閱 AWS PrivateLink 文件。請參閱 VPC 定價以取得 VPC 端點的價格。若要進一步了解 VPC 與端點，請參閱 Amazon VPC。

若要查看各區域的 Amazon WorkSpaces API 端點清單，請參閱 WorkSpaces API 端點。

> **Note**
>
> 聯邦資訊處理標準 (FIPS) Amazon WorkSpaces 區 API 端點不支援具有 AWS PrivateLink 的 Amazon WorkSpaces API 端點。

為 Amazon WorkSpaces 建立 VPC 端點政策。

您可以為 Amazon WorkSpaces 的 Amazon VPC 端點建立政策，以指定下列各項：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制服務的存取。

> **Note**
>
> 聯邦資訊處理標準 (FIPS) Amazon WorkSpaces 端點不支援 VPC 端點政策。

以下 VPC 端點政策範例指定所有可存取 VPC 介面端點的使用者都獲准調用名為 `ws-f9abcdefg` 的 Amazon WorkSpaces 託管端點。

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
}
```

在這個範例中，下列動作會遭到拒絕：

- 調用 `ws-f9abcdefg` 以外 Amazon WorkSpaces 託管的端點。

- 對指定資源 (WorkSpace ID：`ws-f9abcdefg`) 以外的任何資源執行動作。

> **Note**
>
> 在這個範例中，使用者仍然可以從 VPC 外部執行其他 Amazon WorkSpaces API 動作。若要限制 VPC 內的 API 呼叫，請參閱 適用於 WorkSpaces 的身分和存取管理 以取得有關使用身分型政策來控制 Amazon WorkSpaces API 端點存取權的相關資訊。

將私有網路連線到 VPC

若要透過 VPC 來呼叫 Amazon WorkSpaces API，您必須從 VPC 內的執行個體進行連線，或使用 AWS Virtual Private Network (AWS VPN) 或 AWS Direct Connect 將私有網路連線到 VPC。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 VPN 連線。如需有關 AWS Direct Connect 的資訊，請參閱《AWS Direct Connect 使用者指南》中的建立連線。

更新中的管理 WorkSpaces

我們建議您定期修補、更新和保護您的 WorkSpaces. 您可以將您的配置 WorkSpaces 為在定期維護 WorkSpaces 期間進行更新，也可以自行更新它們。如需詳細資訊，請參閱 WorkSpace 維護。

對於您的應用程式 WorkSpaces，您可以使用提供的任何自動更新服務，或遵循建議來安裝應用程式廠商提供的更新。

排解 WorkSpaces 問題

下列資訊可協助您疑難排解 WorkSpaces.

啟用進階記錄

若要協助疑難排解使用者可能遇到的問題，您可以在任何 Amazon 用 WorkSpaces 戶端上啟用進階記錄。

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。對於 1.0+ 和 2.0 多個用戶端，這些進階記錄檔案會自動上傳到中的資料庫。 AWS

> **Note**
>
> 若要 AWS 檢閱進階記錄檔案，並取得 WorkSpaces 客戶問題的技術支援，請連絡 AWS Support。如需詳細資訊，請參閱 AWS Support 中心。

若要啟用 Web Access 的進階記錄

若要啟用 Web Access 的進階記錄

1. 打開您的 Amazon WorkSpaces 網絡訪問客戶端。
2. 在 WorkSpaces 登入頁面頂端，選擇 [診斷記錄]。
3. 在快顯對話方塊中，確定已啟用診斷記錄。
4. 針對日誌層級，選擇進階記錄。

若要在 Google Chrome、Microsoft Edge 和 Firefox 中存取日誌檔案

1. 在瀏覽器上開啟內容 (滑鼠右鍵) 功能表，或在鍵盤上按 Ctrl+Shift+I (或對於 Mac，按 command+option+I)，以開啟開發人員工具面板。
2. 在開發人員工具面板中，選擇控制台索引標籤以尋找日誌檔案。

若要在 Safari 中存取日誌檔案

1. 依序選擇 Safari、設定。
2. 在設定視窗上，選擇進階索引標籤。

3. 選擇在功能表列中顯示開發功能表。
4. 從功能表列的開發索引標籤中，選擇開發 > 顯示 Web Inspector。
5. 在 Safari Web Inspector 面板中，選擇主控台索引標籤以尋找日誌檔案。

若要為 4.0+ 用戶端啟用進階記錄

Windows 用戶端日誌會儲存在下列位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

若要為 Windows 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。
2. 開啟命令提示應用程式。
3. 使用-l3旗標啟動 WorkSpaces 用戶端。

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 如果 WorkSpaces 為一個使用者而非所有使用者安裝，請使用下列命令：
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon
> WorkSpaces"
> workspaces.exe -l3
> ```

macOS 用戶端日誌會儲存在下列位置：

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

若要為 macOS 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。

2. 開啟終端機。
3. 執行下列命令。

```
open -a workspaces --args -l3
```

若要為 Android 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。
2. 開啟 Android 用戶端功能表。
3. 選取支援。
4. 選取記錄設定。
5. 選取啟用進階記錄。

若要在啟用進階記錄後擷取 Android 用戶端的日誌：

- 選取擷取日誌以在本機儲存壓縮的日誌。

Linux 用戶端日誌會儲存在下列位置：

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

若要為 Linux 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。
2. 開啟終端機。
3. 執行下列命令。

```
/opt/workspacesclient/workspacesclient -l3
```

若要為 3.0 用戶端啟用進階記錄

Windows 用戶端日誌會儲存在下列位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

若要為 Windows 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。

2. 開啟命令提示應用程式。
3. 使用-l3旗標啟動 WorkSpaces 用戶端。

```
c:

cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 如果 WorkSpaces 為一個使用者而非所有使用者安裝，請使用下列命令：
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon
> WorkSpaces"
> workspaces.exe -l3
> ```

macOS 用戶端日誌會儲存在下列位置：

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

若要為 macOS 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。
2. 開啟終端機。
3. 執行下列命令。

```
open -a workspaces --args -l3
```

若要為 Android 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。
2. 開啟 Android 用戶端功能表。
3. 選取支援。
4. 選取記錄設定。
5. 選取啟用進階記錄。

若要在啟用進階記錄後擷取 Android 用戶端的日誌：

- 選取擷取日誌以在本機儲存壓縮的日誌。

Linux 用戶端日誌會儲存在下列位置：

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

若要為 Linux 用戶端啟用進階記錄

1. 關閉 Amazon WorkSpaces 客戶端。
2. 開啟終端機。
3. 執行下列命令。

```
/opt/workspacesclient/workspacesclient -l3
```

若要為 1.0+ 和 2.0+ 用戶端啟用進階記錄

1. 開啟用 WorkSpaces 戶端。
2. 選擇用戶端應用程式右上角的齒輪圖示。
3. 選擇 Advanced Settings (進階設定)。
4. 選取啟用進階記錄核取方塊。
5. 選擇儲存。

Windows 用戶端日誌會儲存在下列位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

macOS 用戶端日誌會儲存在下列位置：

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

對特定問題進行疑難排解

下列資訊可協助您疑難排解 WorkSpaces.

問題

- 我無法創建 Amazon Linux， WorkSpace 因為用戶名中有無效字符

- 我改變了 Amazon Linux WorkSpace 的外殼，現在我無法佈建 PCoIP 工作階段
- 我的 Amazon Linux WorkSpaces 無法啟動
- WorkSpaces 在我的連接目錄中啟動經常失敗
- 啟動 WorkSpaces 失敗並出現內部錯誤
- 當我嘗試註冊目錄時，註冊失敗並使目錄處於 ERROR 狀態
- 我的使用者無法使用互動式登入橫幅連線到 Windows WorkSpace
- 我的使用者無法連線到視窗 WorkSpace
- 我的使用者在嘗試 WorkSpaces 從 WorkSpaces Web Access 登入時遇到問題
- Amazon WorkSpaces 客戶端在返回登錄屏幕之前顯示一段時間灰色的「正在加載...」屏幕。不會顯示其他錯誤訊息。
- 我的使用者收到訊息「WorkSpace 狀態：不良狀態。我們無法將您連接到您的 WorkSpace. 請過幾分鐘後再試。」
- 我的使用者收到訊息「此裝置未獲授權存取 WorkSpace. 請聯絡管理員以尋求協助。」
- 我的使用者收到訊息：「沒有網路。網路連線中斷。請檢查您的網路連線或聯絡您的管理員尋求協助。」 當嘗試連接到 WSP 時 WorkSpace
- WorkSpaces 客戶端給我的用戶一個網絡錯誤，但他們可以在他們的設備上使用其他具有網絡功能的應用程序
- 我的 WorkSpace 使用者會看到下列錯誤訊息：「裝置無法連線至註冊服務。請檢查您的網路設定。」
- 我的 PCoIP 零客戶端使用者會收到錯誤訊息「提供的憑證因為時間戳記而無效」
- USB 印表機和其他 USB 周邊設備不適用於 PCoIP 零客戶端
- 我的使用者略過了更新其 Windows 或 macOS 用戶端應用程式，但沒收到安裝最新版本的提示
- 我的使用者無法在其 Chromebook 上安裝 Android 用戶端應用程式
- 我的使用者並未收到邀請電子郵件或密碼重設電子郵件
- 我的使用者在用戶端登入畫面上看不到「忘記密碼？」選項
- 當我嘗試在 Windows 上安裝應用程序時，收到消息「系統管理員已設置策略以阻止此安裝」WorkSpace
- 我的目錄 WorkSpaces 中沒有可以連接到互聯網
- 我失去 WorkSpace 了互聯網接入
- 當我嘗試連線到內部部署目錄時，收到「DNS 無法使用」錯誤
- 當我嘗試連線到內部部署目錄時，收到「偵測到連線問題」錯誤

- 當我嘗試連線到內部部署目錄時，收到「SRV 記錄」錯誤
- 我的窗戶 WorkSpace 在閒置時進入睡眠狀態
- 我的一個 WorkSpaces 有狀態 UNHEALTHY
- 我 WorkSpace 意外崩潰或重新啟動
- 相同的使用者名稱有多個 WorkSpace，但使用者只能登入其中一個 WorkSpaces
- 我在 Amazon 上使用 Docker 時遇到問題 WorkSpaces
- 我收到一些 API 調用的 ThrottlingException 錯誤
- 當我讓它在後台運行時，我一 WorkSpace 直斷開連接
- SAML 2.0 聯合並未運作。我的使用者沒有授權串流他們的 WorkSpaces 桌面。
- 我的使用者每隔 60 分鐘就會從 WorkSpaces 工作階段中斷連線。
- 當我的使用者使用 SAML 2.0 身分識別提供者 (IdP) 起始的流程進行聯合時，使用者會收到重新導向 URI 錯誤，或者每次我的使用者在聯合至 IdP 後嘗試從用 WorkSpaces 戶端登入時啟動用戶端應用程式的其他執行個體。
- 我的使用者在聯合 IdP 之後嘗試登入用 WorkSpaces 戶端應用程式時，會收到「發生錯誤：啟動您的時候發生錯誤 WorkSpace」訊息。
- 我的使用者在聯合 IdP 後嘗試登入用 WorkSpaces 戶端應用程式時，會收到「無法驗證標籤」訊息。
- 我的使用者收到「用戶端和伺服器無法通訊，因為其沒有通用的演算法」訊息。
- 我的麥克風或網路攝影機無法在 Windows 上運作 WorkSpaces。
- 我的使用者無法使用憑證型驗證登入，當他們連線至桌面工作階段時，系統會在用 WorkSpaces 戶端或 Windows 登入畫面上提示輸入密碼。
- 我正在嘗試做一些需要 Windows 安裝媒體但 WorkSpaces 不提供它的事情。
- 我想要 WorkSpaces 使用在不支援的 WorkSpaces 區域中建立的現有 AWS 受管目錄來啟動。
- 我想在 Amazon Linux 2 上更新 Firefox。
- 我的用戶可以使用 WorkSpaces 客戶端重置密碼，忽略配置的細粒密碼策略（FFGP）設置。 AWS Managed Microsoft AD
- 我的使用者在嘗試使用 WorkSpace網頁存取存取 Windows/Linux 時收到錯誤訊息「此作業系統/WorkSpace 平台未獲授權存取您的」

我無法創建 Amazon Linux， WorkSpace 因為用戶名中有無效字符

對於 Amazon Linux WorkSpaces，使用者名稱：

- 最多可包含 20 個字元
- 可包含可以 UTF-8 表示的英文字母、空格和數字
- 可包含下列特殊字元：_.-#
- 不能以連字號 (-) 開頭作為使用者名稱的第一個字元

> **Note**
>
> 這些限制不適用於視窗 WorkSpaces。Windows WorkSpaces 支援使用者名稱中所有字元的 @ 和-符號。

我改變了 Amazon Linux WorkSpace 的外殼，現在我無法佈建 PCoIP 工作階段

若要覆寫 Linux 的預設外殼 WorkSpaces，請參閱覆蓋 Amazon Linux 的默認外殼 WorkSpaces。

我的 Amazon Linux WorkSpaces 無法啟動

自 2020 年 7 月 20 日起，Amazon Linux WorkSpaces 將使用新的許可證書。這些新憑證僅與 PCoIP 代理程式的 2.14.1.1、2.14.7、2.14.9 及 20.10.6 版或更新版本相容。

如果您使用不受支援的 PCoIP 代理程式版本，則必須將其升級至最新版本 (20.10.6)，其中包含與新憑證相容的最新修正程式和效能改進。如果您未在 7 月 20 日前進行這些升級，則 Linux 的工作階段佈建 WorkSpaces 將會失敗，且您的使用者將無法連線至其 WorkSpaces。

若要將 PCoIP 代理升級到最新版本

1. 開啟主 WorkSpaces 控台，網址為 https://console.aws.amazon.com/workspaces/。
2. 在導覽窗格中，選擇 WorkSpaces。
3. 選取您的 Linux WorkSpace，然後選擇「動作」、「重新開機」來重新開機 WorkSpaces。如果 WorkSpace 狀態為STOPPED，您必須 WorkSpaces先選擇 [動作]、[啟動]，然後等到狀態為止，AVAILABLE才能重新開機。
4. 重新開機 WorkSpace 且其狀態為之後AVAILABLE，建議您在執行此升級ADMIN_MAINTENANCE時 WorkSpace 將的狀態變更為。完成后，請將的狀態變更 WorkSpace 為AVAILABLE。如需有關 ADMIN_MAINTENANCE 模式的詳細資訊，請參閱手動維護。

若要將狀態變更 WorkSpace 為ADMIN_MAINTENANCE，請執行下列操作：

a. 選取 WorkSpace 並選擇「動作」、「修改」 WorkSpace。

b. 選擇修改狀態。

c. 針對預期狀態，選取 ADMIN_MAINTENANCE。

d. 選擇 Modify (修改)。

5. WorkSpace 透過安全殼層 Connect 到您的 Linux。如需詳細資訊，請參閱 為您的 Linux 啟用安全殼層連線 WorkSpaces。

6. 若要更新 PCoIP 代理程式，請執行下列命令：

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. 若要驗證代理程式版本並確認更新成功，請執行下列命令：

```
rpm -q pcoip-agent-standard
```

驗證命令應產生以下結果：

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. 斷開連接 WorkSpace 並重新啟動。

9. 如果將狀態設定 WorkSpace 為 ADMIN_MAINTENANCE inStep 4，請重複Step 4並將 [預期狀態] 設定為AVAILABLE。

如果您的 Linux 在升級 PCoIP 代理程式之後 WorkSpace 仍無法啟動，請連絡 AWS Support 部門。

WorkSpaces 在我的連接目錄中啟動經常失敗

確認當您連線到內部部署目錄時，可從指定的每個子網路存取該目錄中的兩個 DNS 伺服器或網域控制站。在每個子網路中啟動 Amazon EC2 執行個體，並使用這兩個 DNS 伺服器的 IP 地址將執行個體加入您的目錄，即可驗證此連線能力。

啟動 WorkSpaces 失敗並出現內部錯誤

檢查您的子網路是否設定為自動指派 IPv6 位址給子網路中啟動的執行個體。若要檢查此設定，請開啟 Amazon VPC 主控台，選取您的子網路，然後選擇子網路動作、修改自動指派 IP 設定。如果啟用此設

定，您將無法 WorkSpaces 使用效能或圖形服務包啟動。請改為停用此設定，並在啟動執行個體時手動指定 IPv6 位址。

當我嘗試註冊目錄時，註冊失敗並使目錄處於 ERROR 狀態

如果您嘗試註冊已設定多區域複寫的 AWS 受管理 Microsoft AD 目錄，就可能會發生這個問題。雖然主要區域中的目錄可以成功註冊以與 Amazon 搭配使用 WorkSpaces，但嘗試在複寫區域中註冊目錄失敗。在複寫區域內，不支援使用 AWS 受管 Microsoft AD 進 Amazon 多區 WorkSpaces 域複寫。

我的使用者無法使用互動式登入橫幅連線到 Windows WorkSpace

如果已實作互動式登入訊息來顯示登入橫幅，這會防止使用者存取其 Windows WorkSpaces。PCo WorkSpaces IP 目前不支援互動式登入訊息群組原則設定。移 WorkSpaces 至未套用Interactive logon: Message text for users attempting to log on群組原則的組織單位 (OU)。WSP 支援登入訊息 WorkSpaces，使用者必須在接受登入橫幅後再次登入。

我的使用者無法連線到視窗 WorkSpace

我的使用者在嘗試連線至其 Windows 時收到下列錯誤 WorkSpaces：

```
"An error occurred while launching your WorkSpace. Please try again."
```

當無法使用 PCoIP 加載 Windows 桌面時，通常會發生此錯誤。 WorkSpace 請檢查以下內容：

- 如果未執行 Windows 服務的 PCoIP 標準代理程式，就會出現此訊息。使用 RDP 連線以確認服務是否正在執行、已設定為自動啟動，以及可透過管理介面 (eth0) 進行通訊。

- 如果 PCoIP 代理程式已解除安裝，請 WorkSpace 透過 Amazon WorkSpaces 主控台重新啟動，以自動重新安裝。

- 如果將WorkSpaces安全群組修改為限制輸出流量，則在長時間延遲後，您也可能會在 Amazon WorkSpaces 用戶端上收到此錯誤。限制輸出流量可防止 Windows 與您的目錄控制器通訊來進行登入。確認您的安全性群組允許透過主要網路介面與所有必要連接埠上的目錄控制器通訊。WorkSpaces

此錯誤的另一個原因與使用者權限指派群組政策有關。如果下列群組原則設定不正確，則會阻止使用者存取其 Windows WorkSpaces：

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- 不正確的政策：

  政策：從網路存取此電腦

  設定：####\網域電腦

  獲勝的 GPO：允許檔案存取

- 正確的政策：

  政策：從網路存取此電腦

  設定：####\網域使用者

  獲勝的 GPO：允許檔案存取

> **Note**
>
> 此政策設定應套用至網域使用者，而非網域電腦。

如需詳細資訊，請參閱 Microsoft Windows 文件中的從網路存取此電腦 - 安全政策設定和設定安全政策設定。

我的使用者在嘗試 WorkSpaces 從 WorkSpaces Web Access 登入時遇到問題

Amazon WorkSpaces 依賴特定的登入畫面組態，讓使用者能夠從其 Web 存取用戶端成功登入。

若要讓 Web Access 使用者登入其 WorkSpaces，您必須設定群組原則設定和三個安全性原則設定。如果未正確設定這些設定，使用者在嘗試登入時可能會遇到較長的登入時間或畫面變黑 WorkSpaces。若要進行這些設定，請參閱 啟用和設定 Amazon WorkSpaces 網路存取。

> **Important**
>
> 自 2020 年 10 月 1 日起，客戶將無法再使用 Amazon WorkSpaces 網路存取用戶端連線到 Windows 7 自訂版 WorkSpaces 或 Windows 7 自攜授權 (BYOL)。 WorkSpaces

Amazon WorkSpaces 客戶端在返回登錄屏幕之前顯示一段時間灰色的「正在加載...」屏幕。不會顯示其他錯誤訊息。

此行為通常表示 WorkSpaces 用戶端可以透過連接埠 443 進行驗證，但無法透過連接埠 4172 (PCoIP) 或連接埠 4195 (WSP) 建立串流連線。如果不符合網路必要條件，就可能會發生這種情況。用戶端的問題通常會導致用戶端的網路檢查失敗。若要查看哪些運作狀態檢查失敗，請選擇網路檢查圖示 (通常為 2.0+ 用戶端的登入畫面右下角有驚嘆號的紅色三角形，或是 3.0+ 用戶端右上角的網路圖示)。

> **Note**
>
> 此問題的最常見原因是用戶端防火牆或 Proxy 防止透過連接埠 4172 或 4195 (TCP 和 UDP) 進行存取。如果此運作狀態檢查失敗，請檢查您的本機防火牆設定。

如果網路檢查通過，則的網路組態可能有問題 WorkSpace。例如，Windows 防火牆規則可能會封鎖管理介面上的連接埠 UDP 4172 或 4195。 WorkSpace 使用遠端桌面通訊協定 (RDP) 用戶端連線至，以確認 WorkSpace 符合必要的 Connect 埠需求。

我的使用者收到訊息「WorkSpace 狀態：不良狀態。我們無法將您連接到您的 WorkSpace. 請過幾分鐘後再試。」

此錯誤通常表示 SkyLightWorkSpacesConfigService 服務沒有回應健康狀態檢查。

如果您剛剛重新啟動或啟動 WorkSpace，請等待幾分鐘，然後再試一次。

如果 WorkSpace 已執行一段時間，但您仍然看到此錯誤，請使用 RDP 連線以確認 SkyLightWorkSpacesConfigService 服務：

- 正在執行。
- 已設定為自動啟動。
- 可透過管理介面 (eth0) 進行通訊。
- 不會被任何第三方防毒軟體封鎖。

我的使用者收到訊息「此裝置未獲授權存取 WorkSpace. 請聯絡管理員以尋求協助。」

此錯誤表示 IP 存取控制群組已在 WorkSpace 目錄上設定，但未列出用戶端 IP 位址。

檢查您目錄上的設定。確認使用者連線的公用 IP 位址是否允許存取 WorkSpace。

我的使用者收到訊息：「沒有網路。網路連線中斷。請檢查您的網路連線或聯絡您的管理員尋求協助。」 當嘗試連接到 WSP 時 WorkSpace

如果發生此錯誤且使用者沒有連線問題，請確定網路防火牆上已開啟連接埠 4195。若要 WorkSpaces 使用 WorkSpaces 串流通訊協定 (WSP)，用來串流用戶端工作階段的連接埠已從 4172 變更為 4195。

WorkSpaces 客戶端給我的用戶一個網絡錯誤，但他們可以在他們的設備上使用其他具有網絡功能的應用程序

用 WorkSpaces 戶端應用程式需要存取 AWS雲端中的資源，而且需要至少提供 1 Mbps 下載頻寬的連線。如果裝置與網路間歇性連線，用 WorkSpaces 戶端應用程式可能會回報網路問題。

WorkSpaces 自 2018 年 5 月起，強制使用 Amazon 信任服務發行的數位憑證。在受支援的作業系統上，Amazon 信任服務已經是受信任的根 CA WorkSpaces。如果作業系統的根 CA 清單不是最新的，則裝置無法連線到，而 WorkSpaces 且用戶端會發生網路錯誤。

若要辨識憑證失敗所造成的連線問題

- PCoIP 零客戶端—下列錯誤訊息會顯示。

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- 其他用戶端—運作狀態檢查失敗並出現網際網路的紅色警告三角形。

若要解決憑證失敗

- Windows 用戶端應用程式
- PCoIP 零客戶端
- 其他用戶端應用程式

Windows 用戶端應用程式

針對憑證失敗，使用下列其中一個解決方案。

解決方案 1：更新用戶端應用程式

從下載並安裝最新的視窗用戶端應用程式 https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east 在安裝期間，用戶端應用程式可確保您的作業系統信任 Amazon Trust Services 發行的憑證。

解決方案 2：將 Amazon Trust Services 新增至本機根 CA 清單

1. 開啟 https://www.amazontrust.com/repository/。
2. 下載 DER 格式的 Starfield 憑證 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92)。
3. 開啟 Microsoft Management Console。(從命令提示，執行 mmc。)
4. 選擇 File (檔案)、Add/Remove Snap-in (新增/移除嵌入式管理單元)、Certificates (憑證)、Add (新增)。
5. 在 Certificates snap-in (憑證嵌入式管理單元) 頁面中，選取 Computer account (電腦帳戶)，然後選擇 Next (下一步)。保留預設值 Local computer (本機電腦)。選擇 Finish (完成)。選擇確定。
6. 展開憑證 (本機電腦) 並選取可信任的根憑證授權單位。選擇 Action (動作)、All Tasks (所有任務)、匯入 (Import)。
7. 遵循精靈來匯入您下載的憑證。
8. 結束並重新啟動用 WorkSpaces 戶端應用程式。

解決方案 3：使用群組政策將 Amazon Trust Services 部署為可信任的 CA

使用群組政策將 Starfield 憑證新增至網域可信任的根 CA。如需詳細資訊，請參閱使用政策來散發憑證。

PCoIP 零客戶端

若要直接連線至 WorkSpace 使用韌體 6.0 版或更新版本，請下載並安裝 Amazon 信任服務發行的憑證。

若要將 Amazon Trust Services 新增為可信任的根 CA

1. 開啟 https://certs.secureserver.net/repository/。

2. 下載 Starfield Certificate Chain 之下具有指紋 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58 的憑證。
3. 將憑證上傳到零客戶端。如需詳細資訊，請參閱 Teradici 文件中的上傳憑證。

其他用戶端應用程式

從 Amazon Trust Services 新增 Starfield 憑證 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92)。如需如何新增根 CA 的詳細資訊，請參閱下列文件：

- Android：新增和移除憑證
- Chrome 作業系統：管理 Chrome 裝置上的用戶端憑證
- macOS 和 iOS：在測試裝置上安裝 CA 的根憑證

我的 WorkSpace 使用者會看到下列錯誤訊息：「裝置無法連線至註冊服務。請檢查您的網路設定。」

發生註冊服務失敗時，您的 WorkSpace 使用者可能會在 [連線 Health 全狀況檢查] 頁面上看到下列錯誤訊息：「您的裝置無法連線至 WorkSpaces 註冊服務。您將無法註冊您的裝置 WorkSpaces。請檢查您的網路設定。」

當用 WorkSpaces 戶端應用程式無法連線到註冊服務時，就會發生此錯誤。通常，當 WorkSpaces 目錄已被刪除時，會發生這種情況。若要解決此錯誤，請確定註冊碼有效且對應於 AWS 雲端中執行的目錄。

我的 PCoIP 零客戶端使用者會收到錯誤訊息「提供的憑證因為時間戳記而無效」

如果 Teradici 中未啟用網路時間協定 (NTP)，PCoIP 零客戶端使用者可能會收到憑證失敗錯誤。若要設定 NTP，請參閱 為 WorkSpaces 設定 PCoIP 零用戶端。

USB 印表機和其他 USB 周邊設備不適用於 PCoIP 零客戶端

從 PCoIP 代理程式 20.10.4 版開始，Amazon 預設會透過 Windows 登錄 WorkSpaces 停用 USB 重新導向。當您的使用者使用 PCoIP 零用戶端裝置連線至 USB 周邊裝置時，此登錄設定會影響 USB 周邊設備的行為。 WorkSpaces

如果您使用的 WorkSpaces 是 20.10.4 或更新版本的 PCoIP 代理程式，則在您啟用 USB 重新導向之前，USB 周邊裝置將無法與 PCoIP 零用戶端裝置搭配使用。

> **Note**
>
> 如果您使用 32 位元的虛擬印表機驅動程式，您也必須將這些驅動程式更新為 64 位元版本。

若要啟用 PCoIP 零客戶端裝置的 USB 重新導向

我們建議您將這些登錄變更推送至您 WorkSpaces 透過群組原則。如需詳細資訊，請參閱 Teradici 文件中的設定代理程式和可設定的設定。

1. 將下列登錄機碼值設為 1 (已啟用)：

   KeyPath = 本地機器\ 軟體\ 政策\ 原則\ PCoIP\ 管理員

   KeyName = pcoip.啟用/usb

   KeyType = DWORD

   KeyValue = 1
2. 將下列登錄機碼值設為 1 (已啟用)：

   KeyPath = HKY_ 本地機器\ 軟體\ 政策\ 原則\ PCoIP\ pcoip_ 管理員預設值

   KeyName = pcoip.啟用/usb

   KeyType = DWORD

   KeyValue = 1
3. 如果您尚未這麼做，請登出 WorkSpace，然後重新登入。您的 USB 裝置現在應可運作。

我的使用者略過了更新其 Windows 或 macOS 用戶端應用程式，但沒收到安裝最新版本的提示

當使用者略過 Amazon WorkSpaces Windows 用戶端應用程式的更新時，系統會設定SkipThis版本登錄機碼，而且在發行新版用戶端時，系統不再提示他們更新其用戶端。若要更新至最新版本，您可以按照 Amazon WorkSpaces 使用者指南中的「將 WorkSpaces Windows 用戶端應用程式更新為較新版本」中所述編輯登錄。您也可以執行下列 PowerShell 命令：

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

當使用者略過 Amazon WorkSpaces macOS 用戶端應用程式的更新時，會設定SUSkippedVersion偏好設定，並且在發行新版用戶端時不再提示他們更新用戶端。若要更新至最新版本，您可以按照 Amazon WorkSpaces 使用指南中的「將 WorkSpaces macOS 用戶端應用程式更新為較新版本」中所述重設此偏好設定。

我的使用者無法在其 Chromebook 上安裝 Android 用戶端應用程式

版本 2.4.13 是 Amazon WorkSpaces Chromebook 客戶端應用程序的最終版本。由於谷歌正逐步淘汰對 Chrome 應用程序的支持，因此 WorkSpaces Chromebook 客戶端應用程序不會進一步更新，並且不支持其使用。

對於支持安裝 Android 應用程序的 Chromebook，我們建議您改用 WorkSpaces Android 客戶端應用程序。

在某些情況下，您可能需要啟用使用者的 Chromebook 才能安裝 Android 應用程式。如需詳細資訊，請參閱 針對 Chromebook 設定 Android。

我的使用者並未收到邀請電子郵件或密碼重設電子郵件

使用者不會自動收到使用 AD Connector 或信任網域建立 WorkSpaces 的歡迎使用或密碼重設電子郵件。如果使用者已經存在於 Active Directory 中，也不會自動傳送邀請電子郵件。

若要手動傳送歡迎電子郵件給這些使用者，請參閱 傳送邀請電子郵件。

若要重設使用者密碼，請參閱 設定 WorkSpaces 的 Active Directory 管理工具。

我的使用者在用戶端登入畫面上看不到「忘記密碼？」選項

如果您使用 AD Connector 或可信任的網域，使用者將無法重設自己的密碼。（忘記密碼？ WorkSpaces 客戶端應用程序登錄屏幕上的選項將不可用。）如需重設使用者密碼的詳細資訊，請參閱 設定 WorkSpaces 的 Active Directory 管理工具。

當我嘗試在 Windows 上安裝應用程序時，收到消息「系統管理員已設置策略以阻止此安裝」 WorkSpace

您可以修改 Windows 安裝程式群組政策設定來解決此問題。若要將此原則部署到目錄 WorkSpaces 中的多個，請將此設定套用至從加入網域的 EC2 執行個體連結至 WorkSpaces 組織單位 (OU) 的群

組原則物件。如果您使用 AD Connector，您可以從網域控制站進行這些變更。如需有關使用 Active Directory 管理工具來處理群組政策物件的詳細資訊，請參閱《AWS Directory Service 管理指南》中的安裝 Active Directory 管理工具。

下列程序顯示如何設定 WorkSpaces 群組原則物件的 Windows 安裝程式設定。

1. 請確定您的網域中已安裝最新的WorkSpaces 群組原則系統管理範本。
2. 在 Windows WorkSpace 用戶端上開啟 [群組原則管理] 工具，然後瀏覽至 WorkSpaces 電腦帳戶並選取 [WorkSpaces 群組原則] 物件。從主功能表，依序選擇動作、編輯。
3. 在群組政策管理編輯器中，選擇電腦設定、政策、管理範本、傳統管理範本、Windows 元件、Windows Installer。
4. 開啟關閉 Windows Installer 設定。
5. 在關閉 Windows Installer 對話方塊中，將未設定變更為已啟用，然後將停用 Windows Installer 設為絕不。
6. 選擇確定。
7. 若要套用群組政策變更，請執行下列其中一項：
   - 重新啟動 WorkSpace（在 WorkSpaces 控制台中，選擇 WorkSpace，然後選擇操作，重新啟動 WorkSpaces）。
   - 在管理命令提示中輸入 gpupdate /force。

我的目錄 WorkSpaces 中沒有可以連接到互聯網

WorkSpaces 默認情況下無法與互聯網通信。您必須明確提供網際網路存取權。如需詳細資訊，請參閱提供您的網際網路存取 WorkSpace。

我失去 WorkSpace 了互聯網接入

如果您 WorkSpace 無法存取網際網路，而您無法使用 RDP 連線至，則此問題可能是由於遺失的公用 IP 位址所造成的 WorkSpace。 WorkSpace 如果您已在目錄級別啟用彈性 IP 地址的自動分配，則彈性 IP 地址（來自亞馬遜提供的池）在啟動 WorkSpace 時將分配給您。但是，如果您將擁有的彈性 IP 地址關聯到一個 WorkSpace，然後您稍後將該彈性 IP 地址與中斷關聯 WorkSpace，則會 WorkSpace 丟失其公共 IP 地址，並且不會自動從 Amazonon 提供的池中獲取新 IP 地址。

若要將 Amazon 提供的集區中的新公用 IP 位址與相關聯 WorkSpace，您必須重建. WorkSpace 如果您不想重建 WorkSpace，則必須將您擁有的另一個彈性 IP 地址與 WorkSpace.

建議您在啟動 WorkSpace後不要修改 elastic network interface。 WorkSpace 將彈性 IP 位址指派給之後 WorkSpace，會 WorkSpace 保留相同的公用 IP 位址 (除 WorkSpace 非重建，在此情況下，它會取得新的公用 IP 位址)。

當我嘗試連線到內部部署目錄時，收到「DNS 無法使用」錯誤

當您連線到內部部署目錄時，您會收到類似下列的錯誤訊息。

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector 必須能夠經由透過連接埠 53 的 TCP 和 UDP 與您的內部部署 DNS 伺服器通訊。確認您的安全群組和內部部署防火牆允許透過此連接埠的 TCP 和 UDP 通訊。

當我嘗試連線到內部部署目錄時，收到「偵測到連線問題」錯誤

當您連線到內部部署目錄時，您會收到類似下列的錯誤訊息。

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connector 必須能夠經由透過下列連接埠的 TCP 和 UDP 與您的內部部署網域控制器通訊。確認您的安全群組和內部部署防火牆允許透過這些連接埠的 TCP 和 UDP 通訊：

- 88 (Kerberos)
- 389 (LDAP)

當我嘗試連線到內部部署目錄時，收到「SRV 記錄」錯誤

當您連線到內部部署目錄時，您會收到類似下列一或多個錯誤訊息：

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

連線到您的目錄時，AD Connector 需要取得 _ldap._tcp.*dns-domain-name* 和 _kerberos._tcp.*dns-domain-name* SRV 記錄。如果此服務無法從您在連線到目錄時所指定的 DNS 伺服器取得這些記錄，您會收到此錯誤。確定您的 DNS 伺服器包含這些 SRV 記錄。如需詳細資訊，請參閱 Microsoft TechNet 上的 SRV 資源記錄。

我的窗戶 WorkSpace 在閒置時進入睡眠狀態

若要解決此問題，請連線至 WorkSpace 並使用下列程序將電源計劃變更為 [高效能]：

1. 從開啟 [控制台]，然後選擇 [硬體] 或選擇 [硬體和音效] (名稱可能會有所不同，視您的 Windows 版本而定)。 WorkSpace
2. 在電源選項下，選擇選擇電源計畫。
3. 在選擇或自訂電源計畫窗格中，選擇高效能電源計畫，然後選擇變更計畫設定。
   - 如果停用了選擇高效能電源計畫的選項，請選擇變更目前無法使用的設定，然後選擇高效能電源計畫。
   - 如果看不到高效能計畫，請選擇顯示其他計畫右側的箭頭加以顯示，或在左側導覽中選擇建立電源計畫，選擇高效能，為電源計畫命名，然後選擇下一步。
4. 在變更計畫設定：高效能頁面上，確定關閉顯示器和 (可用的話) 讓電腦進入睡眠狀態設定為絕不。
5. 如果您對高效能計畫進行了任何變更，請選擇儲存變更 (如果您要建立新計畫，請選擇建立)。

如果上述步驟無法解決問題，請執行下列操作：

1. 從開啟 [控制台]，然後選擇 [硬體] 或選擇 [硬體和音效] (名稱可能會有所不同，視您的 Windows 版本而定)。 WorkSpace
2. 在電源選項下，選擇選擇電源計畫。
3. 在選擇或自訂電源計畫窗格中，選擇高效能電源計畫右側的變更計畫設定連結，然後選擇變更進階電源設定連結。
4. 在電源選項對話方塊的設定清單中，選擇硬碟左側的加號以顯示相關設定。
5. 確認插電的在下列時間後關閉硬碟值大於使用電池的值 (預設值為 20 分鐘)。
6. 選擇 PCI Express 左側的加號，然後對連結狀態電源管理執行相同的操作。
7. 確認連結狀態電源管理設定為關閉。
8. 選擇確定 (或者您變更了任何設定，則選擇套用) 以關閉對話方塊。
9. 在變更計畫設定窗格中，如果您變更了任何設定，請選擇儲存變更。

我的一個 WorkSpaces 有狀態 **UNHEALTHY**

此 WorkSpaces 服務會定期傳送狀態要求至 WorkSpace. A WorkSpace 在無法回應這些要求UNHEALTHY時標記。這個問題的常見原因是：

- 上的應用程 WorkSpace 式封鎖網路通訊埠，防 WorkSpace 止回應狀態要求。
- CPU 使用率高會 WorkSpace 阻止及時回應狀態要求。
- 的電腦名稱 WorkSpace 已變更。這樣可以防止在 WorkSpaces 和之間建立安全通道 WorkSpace。

您可以嘗試使用下列方法更正此情況：

- WorkSpace 從 WorkSpaces 控制台重新啟動。
- WorkSpace 使用下列程序 Connect 到狀況不良，該程序僅應用於疑難排解目的：

  1. Connect 到與狀 WorkSpace 況不良 WorkSpace相同的目錄中的操作。
  2. 從操作中 WorkSpace，使用遠程桌面協議（RDP）連接到不健康的 IP 地址 WorkSpace 使用不健康的 IP 地址。 WorkSpace根據問題的程度，您可能無法連接到不健康 WorkSpace的問題。
  3. 在狀況不良的情況下 WorkSpace，確認符合最低連接埠需求。
- 確定 SkyLightWorkSpacesConfigService 服務可以回應健康狀態檢查。若要對此問題進行疑難排解，請參閱 我的使用者收到訊息「WorkSpace 狀態：不良狀態。我們無法將您連接到您的 WorkSpace. 請過幾分鐘後再試。」。
- WorkSpace 從主 WorkSpaces 控台重建。因為重建 a WorkSpace 可能會造成資料遺失，因此只有在所有其他嘗試修正問題都不成功時，才應使用此選項。

我 WorkSpace 意外崩潰或重新啟動

如果您 WorkSpace 設定的 PCoIP 重複當機或重新開機，而您的錯誤記錄檔或損毀傾印指向`spacedeskHookKmode.sys`或的問題`spacedeskHookUmode.dll`，或者如果您收到下列錯誤訊息，您可能需要停用 Web Access： WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - 這些疑難排解步驟不適用於 WorkSpaces 為 WorkSpaces 串流通訊協定 (WSP) 設定的步驟。它們僅適用於針對 PCoIP 設定的設定。 WorkSpaces

- 只有在您不允許使用者使用 Web Access 時，才應停用 Web Access。

若要停用對的 Web 存取 WorkSpace，您必須停用 WorkSpaces 目錄中的 Web 存取，然後重新開機 WorkSpace。

相同的使用者名稱有多個 WorkSpace，但使用者只能登入其中一個 WorkSpaces

如果您刪除 Active Directory (AD) 中的使用者，而不先刪除他們， WorkSpace 然後再將使用者新增回 Active Directory 並 WorkSpace 為該使用者建立新的使用者，相同的使用者名稱現在會有兩個 WorkSpaces 在相同的目錄中。但是，如果使用者嘗試連線至其原始檔案 WorkSpace，則會收到下列錯誤：

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

此外，在 Amazon WorkSpaces 主控台中搜尋使用者名稱時，只會傳回新的使用者名稱 WorkSpace，即使兩者 WorkSpaces 仍然存在。（您可以 WorkSpace 通過搜索 WorkSpace ID 而不是用戶名來查找原始文件。）

如果您重新命名 Active Directory 中的使用者，而不先刪除使用者，也可能會發生這種情況 WorkSpace。如果您接著將其使用者名稱變更回原始使用者名稱，並 WorkSpace 為使用者建立新的使用者名稱，則相同的使用者名稱在目錄 WorkSpaces 中會有兩個。

發生這個問題的原因是 Active Directory 使用使用者的安全識別碼 (SID) (而不是使用者名稱) 來唯一識別使用者。若在 Active Directory 中刪除並重建使用者，即使其使用者名稱保持不變，也會指派新的 SID 給使用者。在搜尋使用者名稱期間，Amazon WorkSpaces 主控台會使用 SID 搜尋作用中目錄中的相符項目。Amazon 用 WorkSpaces 戶端也會在使用者連線時使用 SID 來識別使用者 WorkSpaces。

若要解決此問題，請執行下列其中一項：

- 如果因為在 Active Directory 中刪除並重建使用者而發生這個問題，若已啟用 Active Directory 中的資源回收筒功能，您可能能夠還原原始刪除的使用者物件。如果您能夠還原原始使用者物件，請確定使用者可以連線到原始使用者物件 WorkSpace。如果可以的話，您可以 WorkSpace在手動備份並將任何用戶數據從新數據傳輸 WorkSpace 到原始文件 WorkSpace（如果需要）後刪除新的數據。

- 如果您無法還原原始使用者物件，請刪除使用者的原始物件 WorkSpace。用戶應該能夠連接到並使用他們的新 WorkSpace 的。請務必手動備份任何使用者資料，並將任何使用者資料從原始檔案傳輸 WorkSpace 到新資料 WorkSpace。

> **Warning**
>
> 刪除 WorkSpace 是永久動作，無法復原。用 WorkSpace 戶的數據不會持續存在並被銷毀。如需備份使用者資料的協助，請聯絡 AWS 支援。

我在 Amazon 上使用 Docker 時遇到問題 WorkSpaces

視窗 WorkSpaces

在 Windows 上不支援巢狀虛擬化 (包括使用泊塢視窗 WorkSpaces)。如需詳細資訊，請參閱 Docker 文件。

Linux WorkSpaces

若要在 Linux 上使用泊塢視窗 WorkSpaces，請確定 Docker 所使用的 CIDR 區塊不會與與. WorkSpace 如果您在 Linux 上使用 Docker 時遇到問題 WorkSpaces，請聯絡 Docker 尋求協助。

我收到一些 API 調用的 ThrottlingException 錯誤

WorkSpaces API 呼叫的預設允許率是每秒兩次 API 呼叫的固定速率，允許的最大「突發」速率為每秒五個 API 呼叫。下表顯示高載速率限制如何針對 API 請求運作。

秒	傳送的請求數	允許的淨請求	詳細資訊
1	0	5	在第 1 秒期間，允許五個請求，高達每秒五次呼叫的高載速率上限。
2	2	5	由於第 1 秒內發出了兩次或更少呼叫，因此仍可使用五次呼叫的完整高載容量。
3	5	5	由於第 2 秒內只發出了兩次呼叫，因此仍可使用五次呼叫的完整高載容量。

秒	傳送的請求數	允許的淨請求	詳細資訊
4	2	2	由於第 3 秒內使用了完整高載容量，因此只能使用每秒兩次呼叫的恆定速率。
5	3	2	由於沒有剩餘的高載容量，因此此時只允許兩次呼叫。這意味著三個 API 呼叫中的一個遭到限流。一個節流的呼叫將在短暫延遲之後回應。
6	0	1	由於第 5 秒內的其中一次呼叫會在第 6 秒內重試，所以第 6 內只有一次額外呼叫的容量，因為每秒兩次呼叫的恆定速率限制。
7	0	3	既然佇列中不再有任何限流的 API 呼叫，速率限制就會持續增加，直到五次呼叫的高載速率限制為止。
8	0	5	由於第 7 秒內沒有發出任何呼叫，因此允許最大請求數。
9	0	5	即使在第 8 秒內沒有發出任何呼叫，但速率限制也不會增加到超過五。

當我讓它在後台運行時，我一 WorkSpace 直斷開連接

若為 Mac 使用者，檢查「高效小睡」功能是否已開啟。如果已開啟，請將其關閉。若要關閉「高效小睡」，請開啟終端機並執行下列命令：

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 聯合並未運作。我的使用者沒有授權串流他們的 WorkSpaces 桌面。

若針對 SAML 2.0 聯合 IAM 角色內嵌的內嵌政策不包含從目錄 Amazon Resource Name (ARN) 串流的許可，便可能發生此情況。IAM 角色由存取 WorkSpaces 目錄的聯合身分使用者承擔。編輯角色權限以包含目錄 ARN，並確定使用者在目錄 WorkSpace 中具有。如需詳細資訊，請參閱 SAML 2.0 驗證和 S AML 2.0 聯合使用的疑難排解。 AWS

我的使用者每隔 60 分鐘就會從 WorkSpaces 工作階段中斷連線。

如果您已將 SAML 2.0 驗證設定為 WorkSpaces，視您的身分識別提供者 (IdP) 而定，您可能需要設定 IdP 作為 SAML 屬性傳遞的資訊，做為驗證回 AWS 應的一部分。這包括設定屬性元素，其 SessionDuration 屬性設定為 https://aws.amazon.com/SAML/Attributes/SessionDuration。

SessionDuration 指定在需要重新驗證之前，使用者的聯合串流工作階段可以保持作用中的時間上限。雖然 SessionDuration 是選用屬性，但我們建議您將它包含在 SAML 驗證回應中。如果您未指定此屬性，工作階段持續時間會預設為 60 分鐘。

若要解決此問題，請將 IdP 設定為在 SAML 驗證回應中包含 SessionDuration 值，然後視需要設定此值。如需詳細資訊，請參閱步驟 5：針對 SAML 驗證回應建立聲明。

當我的使用者使用 SAML 2.0 身分識別提供者 (IdP) 起始的流程進行聯合時，使用者會收到重新導向 URI 錯誤，或者每次我的使用者在聯合至 IdP 後嘗試從用 WorkSpaces 戶端登入時啟動用戶端應用程式的其他執行個體。

由於轉送狀態 URL 無效而發生這個錯誤。請確定 IdP 聯合設定中的轉送狀態正確，並且 WorkSpaces 目錄內容中的 IdP 聯盟正確設定使用者存取 URL 和轉送狀態參數名稱。如果有效且問題仍然存在，請連絡 Sup AWS port 部門。如需詳細資訊，請參閱設定 SAML。

我的使用者在聯合 IdP 之後嘗試登入用 WorkSpaces 戶端應用程式時，會收到「發生錯誤：啟動您的時候發生錯誤 WorkSpace」訊息。

檢閱您的聯合適用的 SAML 2.0 聲明。S AML 主體 NameID 值必須與 WorkSpaces 使用者名稱相符，而且通常與使用中目錄使用者的 SAM AccountName 屬性相同。此外，屬性設定為的 A PrincipalTag:Email ttribute 元素https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email必須與 WorkSpaces 目錄中定義的 WorkSpaces 使用者電子郵件地址相符。如需詳細資訊，請參閱設定 SAML。

我的使用者在聯合 IdP 後嘗試登入用 WorkSpaces 戶端應用程式時，會收到「無法驗證標籤」訊息。

檢閱您的聯合的 SAML 2.0 聲明中的 PrincipalTag 屬性值，例如 https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email。標籤值可包含字元 _ . : / = + - @、字母、數字和空格的組合。如需詳細資訊，請參閱 IAM 和 AWS STS.

我的使用者收到「用戶端和伺服器無法通訊，因為其沒有通用的演算法」訊息。

如果您未啟用 TLS 1.2，就可能發生這個問題。

我的麥克風或網路攝影機無法在 Windows 上運作 WorkSpaces。

藉由開啟開始功能表來檢查您的隱私權設定

- 開始 > 設定 > 隱私權 > 相機
- 開始 > 設定 > 隱私權 > 麥克風

如果已關閉，請將其打開。

或者， WorkSpaces 系統管理員可以建立群組原則物件 (GPO)，以視需要啟用麥克風和/或網路攝影機。

我的使用者無法使用憑證型驗證登入，當他們連線至桌面工作階段時，系統會在用 WorkSpaces 戶端或 Windows 登入畫面上提示輸入密碼。

工作階段的憑證型驗證失敗。如果問題仍然存在，則憑證型驗證失敗可能是由下列其中一個問題所造成：

- 不支援 WorkSpaces 或用戶端。使用最新 WorkSpaces Windows 用戶端應用程式的 Windows WorkSpaces WorkSpaces 串流通訊協定 (WSP) 服務包支援憑證型驗證。
- 在目錄上啟用憑證型驗證之後， WorkSpaces 需要重新開機。 WorkSpaces
- WorkSpaces 無法與通訊 AWS Private CA，或 AWS Private CA 未簽發憑證。檢查 AWS CloudTrail 以判斷是否已發行憑證。如需詳細資訊，請參閱 管理憑證型驗證。
- 網域控制站沒有用於智慧卡登入的網域控制站憑證，或憑證已過期。如需詳細資訊，請參閱 必要條件 中的步驟 7「使用網域控制站憑證設定網域控制站以驗證智慧卡使用者」。
- 憑證不受信任。如需詳細資訊，請參閱 必要條件 中的步驟 7「將 CA 發佈到 Active Directory」。`certutil -viewstore -enterprise NTAuth`在網域控制站上執行，以確認 CA 已發佈。
- 快取中有憑證，但是憑證無效的使用者的屬性已變更。連絡人 AWS Support 以在憑證到期前清除快取 (24 小時)。如需詳細資訊，請參閱 AWS Support 中心。

- `UserPrincipalName`SAML 屬性的 userPrincipalName 格式未正確格式化或無法解析為使用者的實際網域。如需詳細資訊，請參閱 必要條件 中的步驟 1。
- SAML 聲明中的 (選用) `ObjectSid` 屬性與 SAML_Subject `NameID` 中指定之使用者的 Active Directory 安全識別碼 (SID) 不符。確認您的 SAML 聯合中的屬性對應正確無誤，而且您的 SAML 身分提供者正在同步處理 Active Directory 使用者的 SID 屬性。
- 有些群組政策設定正在修改智慧卡登入的預設 Active Directory 設定，或在智慧卡從讀卡機中移除時採取動作。這些設定可能導致上述錯誤以外的其他非預期行為。憑證型驗證會向執行個體作業系統出示虛擬智慧卡，並在登入完成後將其移除。檢查智慧卡的主要群組政策設定以及其他智慧卡群組政策設定和登錄機碼，包括智慧卡移除行為。
- 私有 CA 的 CRL 發佈點不是線上，也無法從 WorkSpaces 或網域控制站存取。如需詳細資訊，請參閱 必要條件 中的步驟 5。
- 若要檢查網域或樹系中是否有任何過時的 CA，請在 CA `PKIVIEW.msc` 上執行以驗證。如果有過時的 CA，請使用 `PKIVIEW.msc` mmc 手動刪除它們。
- 若要檢查 Active Directory 複寫是否正常運作，而且網域中沒有過時的網域控制站，請執行`repadmin /replsum`。

其他疑難排解步驟包括檢閱 WorkSpaces 執行個體 Windows 事件記錄檔。在 Windows 安全日誌中，要針對登入失敗檢閱的常見事件是事件 4625：帳戶登入失敗。

如果問題仍然存在，請聯繫 AWS Support。如需詳細資訊，請參閱 AWS Support 中心。

我正在嘗試做一些需要 Windows 安裝媒體但 WorkSpaces 不提供它的事情。

如果您使用 AWS提供的公用服務包，則可以在需要時使用 Amazon EC2 提供的 Windows 伺服器作業系統安裝媒體 EBS 快照。

從這些快照建立 EBS 磁碟區，將其附加到 Amazon EC2，然後視需要將檔案傳輸 WorkSpace 到檔案的位置。如果您在 BYOL 上使用 Windows 10， WorkSpaces 並且需要安裝媒體，則需要準備自己的安裝媒體。如需詳細資訊，請參閱使用安裝媒體新增 Windows 元件。由於您無法直接將 EBS 磁碟區連接到一個 WorkSpace，因此您需要將它附加到 Amazon EC2 執行個體並複製檔案。

我想要 WorkSpaces 使用在不支援的 WorkSpaces 區域中建立的現有 AWS 受管目錄來啟動。

若要 WorkSpaces 使用目前不受支援的區域中的目錄啟動 Amazon WorkSpaces，請遵循以下步驟。

> **Note**
>
> 如果您在執行 AWS Command Line Interface 命令時收到錯誤訊息，請確定您使用的是最新 AWS CLI 版本。如需詳細資訊，請參閱確認您執行的是最新版本的 AWS CLI。

步驟 1：與您帳戶中的其他 VPC 建立虛擬私有雲端 (VPC) 對等互連

1. 與不同區域中的 VPC 建立 VPC 對等互連。如需詳細資訊，請參閱在相同帳戶和不同區域中隨著 VPC 建立。
2. 接受 VPC 對等互連。如需詳細資訊，請參閱接受 VPC 對等互連。
3. 啟用 VPC 對等連線後，您可以使用 Amazon VPC 主控台、或 API 來檢視您的 VPC 對等連線。AWS CLI

步驟 2：更新兩個區域中 VPC 對等互連的路由表

更新您的路由表，以開啟透過 IPv4 或 IPv6 與對等 VPC 的通訊。如需詳細資訊，請參閱更新 VPC 對等互連的路由表。

第 3 步：創建一個 AD Connector 並註冊 Amazon WorkSpaces

1. 若要檢閱 AD Connector 必要條件，請參閱 AD Connector 必要條件。
2. 使用 AD Connector 連接現有的目錄。如需詳細資訊，請參閱建立 AD Connector。
3. 當 AD Connector 狀態變更為作用中時，請開啟 AWS Directory Service 主控台，然後選擇目錄 ID 的超連結。
4. 對於 AWS 應用程式和服務，請選擇 Amazon WorkSpaces 以在此目錄 WorkSpaces 上開啟存取權。
5. 使用註冊目錄 WorkSpaces。如需詳細資訊，請參閱使用註冊目錄 WorkSpaces。

我想在 Amazon Linux 2 上更新 Firefox。

步驟 1：確認已啟用自動更新

若要確認已啟用自動更新，請在上執行指令`systemctl status *os-update-mgmt.timer | grep enabled`。 WorkSpace在輸出中，應該有兩行包含 `enabled` 字詞。

步驟 2：起始更新

火狐通常會在 Amazon Linux 2 中自動更新，以 WorkSpaces 及系統中的所有其他軟件包在維護期間。但是，這取決於 WorkSpaces 您使用的類型。

- 對於 AlwaysOn WorkSpaces，每週維護時段是在星期日凌晨 00 點到 04h00，在的時區。WorkSpace
- 從每月的第三個星期一開始，最多兩週，維護時段的開放時間為每天約 00h00 至 05h00，在該地區的時區 AutoStop WorkSpaces。 AWS WorkSpace

如需維護時段的詳細資訊，請參閱 WorkSpace 維護。

您還可以通過重新啟動 WorkSpace並在 15 分鐘後重新連接來啟動立即更新週期。您也可以輸入 `sudo yum update` 以起始更新。若只要起始 Firefox 的更新，請輸入 `sudo yum install firefox`。

如果您無法設定 Amazon Linux 2 儲存庫的存取權，且偏好使用 Mozilla 所建置的二進位檔來安裝 Firefox，請參閱 Mozilla 支援上的從 Mozilla 建置安裝 Firefox。我們建議您完全解除安裝 Firefox 的 RPM 封裝版本，以確保您不會錯誤地執行過時的版本。您可藉由執行命令 `sudo yum remove firefox` 將其解除安裝。

您也可以在不同的機器上執行 `yumdownloader firefox` 命令，從 Amazon Linux 2 儲存庫下載必要的 RPM 套件。然後，將存儲庫側面加載到 WorkSpaces，您可以在其中使用標準YUM命令進行安裝。`sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

> **Note**
>
> 確切的檔案名稱會根據套件版本而變更。

步驟 3：確認已使用 Firefox 儲存庫

Amazon Linux 附加功能自動提供火狐更新 Amazon Linux 2 WorkSpaces. 在 2023 年 7 月 31 日之後 WorkSpaces 創建的 Amazon Linux 2 將已經激活了火狐額外的存儲庫。若要確認您使用的 WorkSpace 是 Firefox 額外儲存庫，請執行以下指令。

```
yum repolist | grep amzn2extra-firefox
```

如果使用 Firefox Extra 儲存庫，命令輸出看起來應該類似 `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10`。如果未使用 Firefox Extra 儲存庫，則輸出會是空的。如果未使用 Firefox Extra 儲存庫，您可以嘗試使用以下命令手動加以啟用：

```
sudo amazon-linux-extras install firefox
```

如果 Firefox Extra 儲存庫啟用仍然失敗，請檢查您的網際網路存取權並確定您的 VPC 端點並未設定。若要繼續 WorkSpaces 透過 YUM 儲存庫接收 Amazon Linux 2 的更新，請確保 WorkSpaces 您能夠連線到 Amazon Linux 2 儲存庫。如需在沒有網際網路存取權的情況下存取 Amazon Linux 2 儲存庫的詳細資訊，請參閱此知識中心文章。

我的用戶可以使用 WorkSpaces 客戶端重置密碼，忽略配置的細粒密碼策略（FFGP）設置。 AWS Managed Microsoft AD

如果使用者的用 WorkSpaces 戶端與相關聯 AWS Managed Microsoft AD，他們必須使用預設的複雜性設定重設密碼。

預設複雜性密碼區分大小寫，且長度必須介於 8 到 64 個字元 (含) 之間。它必須包含以下每個類別中的至少一個字元：

- 小寫字元 (a-z)
- 大寫字元 (A-Z)
- 數字 (0-9)
- 非英數字元 (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

確保密碼不包含不可打印的 unicode 字符，例如空格，換行符，換行符和空字符。

如果您的組織要求您強制執行 FFGP WorkSpaces，請聯絡您的 Active Directory 系統管理員，以直接從 Active Directory (而非用 WorkSpaces 戶端) 重設使用者的密碼。

我的使用者在嘗試使用 WorkSpace網頁存取存取 Windows/Linux 時收到錯誤訊息「此作業系統/ WorkSpace 平台未獲授權存取您的」

您的使用者嘗試使用的作業系統版本與 WorkSpaces Web Access 不相容。確保您在 WorkSpace 目錄的「其他平台」設置下啟用 Web 訪問。如需啟用 Web 存取 WorkSpace的詳細資訊，請參閱啟用和設定 Amazon WorkSpaces 網路存取。

Amazon WorkSpaces 用戶端應用程式生命週期結束政策

Amazon WorkSpaces 生命週期結束 (EOL) 政策適用於不再獲得支援且不再與較新版本進行相容性測試之 WorkSpaces 的特定主要版本 (及其所有次要版本)。

WorkSpaces 用戶端版本的生命週期有三個階段：一般支援、技術指導和生命週期結束 (EOL)。一般支援階段從 WorkSpaces 用戶端的初次公開發行之日開始，並持續一段固定的時間。在一般支援階段，WorkSpaces 支援團隊會針對設定問題提供完整支援。瑕疵解決方案和功能請求會針對 WorkSpaces 用戶端的該主要版本和相關次要版本實作。

從一般支援階段結束到 EOL 日期為止，都會提供技術指導。在技術指導階段，您只會收到支援組態的支援和指導。瑕疵解決方案和功能請求僅針對 WorkSpaces 用戶端的最新版本實作，而不會針對舊版實作。在技術指導階段，如果需要修正程式，AWS 則會針對即將推出的公開發行版本排程該修正程式，而且您可選擇升級至最新的 WorkSpaces 版本，以獲得與修正程式相關的支援。

主要版本的 EOL 會在一般支援和技術指導結束時發生。在 EOL 日期之後，不再提供進一步的支援或維護。AWS 會停止測試相容性問題。如需持續支援，您必須升級至最新的 WorkSpaces 用戶端版本。

如需特定版本支援的詳細資訊，請參考此表格。

Windows 用戶端	一般支援	技術指導	EOL
2.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Linux 用戶端	一般支援	技術指導	EOL
適用於 Ubuntu 18.04 的 4.x	2021 年 8 月 12 日	2023 年 3 月 31 日	2023 年 8 月 31 日
適用於 Ubuntu 18.04 的 3.x	2019 年 11 月 25 日	2023 年 3 月 31 日	2023 年 8 月 31 日

macOS 用戶端	一般支援	技術指導	EOL
2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日

macOS 用戶端	一般支援	技術指導	EOL
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

iPad 用戶端	一般支援	技術指導	EOL
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Android 用戶端	一般支援	技術指導	EOL
2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Web 存取	一般支援		
Google Chrome	目前版本，加上兩個最新的主要版本		
Firefox	目前版本，加上兩個最新的主要版本		
Microsoft Edge	目前版本，加上兩個最新的主要版本		

不支援的用戶端

不支援下列 WorkSpaces 用戶端。

作業系統	用戶端版本	一般支援	技術指導	EOL	備註
Windows	5.11	2023 年 7 月 3 日	2023 年 10 月 1 日	2023 年 10 月 1 日	由於品質問題而不支援

作業系統	用戶端版本	一般支援	技術指導	EOL	備註
Windows	5.10	2023 年 6 月 19 日	2023 年 10 月 1 日	2023 年 10 月 1 日	由於品質問題而不支援
Windows	5.9	2023 年 5 月 9 日	2023 年 10 月 1 日	2023 年 10 月 1 日	由於品質問題而不支援

EOL 常見問答集

我正在使用已達到 EOL 的 WorkSpaces 客戶端版本。我該怎麼做才能升級到支援的版本？

移至 WorkSpaces 用戶端下載頁面，下載並安裝完整支援的 WorkSpaces 版本。

我是否可以使用已達到 EOL 的 WorkSpaces 用戶端版本搭配支援的 WorkSpace？

我們強烈建議將用戶端升級至最新版本，因為先前的解決方案和功能不再套用至已達到 EOL 的用戶端版本。如果您使用的用戶端版本已達到 EOL，請聯絡 AWS 支援團隊以取得詳細資訊。

我正在使用已達到 EOL 的 WorkSpaces 客戶端版本。我仍然可以回報其問題嗎？

您必須先升級至受支援的版本並試著重現問題。如果問題仍存在於支援的版本中，請向 AWS 支援團隊開啟支援案例。

我在已達到 EOL 的作業系統上使用支援的 WorkSpaces 用戶端版本。我仍然可以回報其問題嗎？

已達到 EOL 的作業系統無法再提供技術協助和軟體更新，而且 AWS 不會對使用已達到 EOL 之作業系統的 WorkSpaces 用戶端提供支援。使用支援的作業系統來確保您有 WorkSpaces 用戶端的支援。

Amazon WorkSpaces 配額

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。當您建立 Amazon Web Services 帳戶時，我們會根據您可以建立的資源數量來設定預設配額 (也稱為限制)。

以下是您帳戶的預設配AWS額。 WorkSpaces 您可以使用 Service Quotas 主控台來檢視預設配額和套用配額，或針對可調整的配額請求提高配額。

在某些無法使用 Service Quotas 的區域中，您必須提交支援案例以請求提高限制。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請求提高配額。

資源	預設	描述	可調整
WorkSpaces	1	此帳戶 WorkSpaces 在當前區域中的最大數量。	是
圖形 WorkSpaces	0	目前區域 WorkSpaces 中此帳戶中的最大圖形數目。 **Note** 在 2023 年 11 月 30 日之後，不再支援 Graphics 套件。我們建議您移轉 WorkSpaces 至圖形 .g4dn 套裝軟體。如需詳細資訊，請參閱「遷移 WorkSpace」。	是

資源	預設	描述	可調整
圖形顯示卡 WorkSpaces	0	目前區域中此帳戶中圖形 .g4dn WorkSpaces 的最大數目。	是
GraphicsPro WorkSpaces	0	此帳戶 GraphicsPro WorkSpaces 在當前區域中的最大數量。	是
GraphicsPro.g4dn WorkSpaces	0	目前 WorkSpaces 區 GraphicsPro域中此帳戶的 .g4dn 數目上限。	是
待命 WorkSpaces	0	此帳戶 WorkSpaces 在當前區域中的最大數量。	是
套件	50	在目前區域中，此帳戶的套件數量上限。此配額僅適用於自訂套件，不適用於公用套件。	否
連線別名	20	在目前區域中，此帳戶的連線別名數量上限。	否
目錄	50	目前區域中此帳戶中可註冊以使用 Amazon WorkSpaces 的目錄數目上限。	否
映像	40	在目前區域中，此帳戶的映像數量上限。	是

資源	預設	描述	可調整
IP 存取控制群組	100	在目前區域中，此帳戶的 IP 存取控制群組數量上限。	否
每個目錄的 IP 存取控制群組數量	25	在目前區域中，此帳戶之每個目錄的 IP 存取控制群組數量上限。	否
每個 IP 存取控制群組的規則數量	10	在目前區域中，此帳戶之每個 IP 存取控制群組的規則數量上限。	否

API 限流

允許的速率為每秒呼叫兩次。如需詳細資訊，請參閱限流例外狀況。

WorkSpaces 串流通訊協定 (WSP) 主機代理程式版本

WorkSpaces 串流通訊協定 (WSP) 主機代理程式是在您的 WorkSpace. 它會 WorkSpace 將您的像素串流到用戶端應用程式，並包含工作階段中的功能，例如雙向音訊和視訊，以及列印。如需 WorkSpaces 串流通訊協定 (WSP) 的詳細資訊，請參閱 Amazon WorkSpaces 的通訊協定。

我們建議您將主機代理程式軟體更新為最新版本。您可以手動重新開機 WorkSpaces 以更新 WSP 主機代理程式。在一般 WorkSpaces 預設維護時段期間，WSP 主機代理程式也會自動更新。如需維護時段的詳細資訊，請參閱WorkSpace 維護。其中一些功能需要最新的 WorkSpaces 用戶端版本。如需最新用戶端版本的詳細資訊，請參閱用WorkSpaces 戶端。

下表說明 WSP 主機代理程式的每個版本變更。

發行版本	日期	變更
• 視窗 WorkSpaces -1.1.0.1554	2024年5月15日	• 新增對閒置中斷逾時的支援。 • 新增群組原則設定以設定閒置中斷連線逾時。 • 修正使用者修改顯示設定時中斷連線並顯示白色畫面的問題。WorkSpaces • 錯誤修正與效能改進。
• Ubuntu WorkSpaces	2024 年 2 月 29 日	• 將首選網絡攝像頭分辨率更改為 480x360 和 640x480 之間。 • 錯誤修正與效能改進。
• 視窗系統 WorkSpaces -	2024年2月22 日	• 增加了對在遠程谷歌瀏覽器或 Microsoft Edge 瀏覽器中運行的 Web 應用程序的會話中 WebAuthn 重定向請求的支持。此功能會新增一次性瀏覽器提示，要求使用者啟用 DCV WebAuthn 重新導向延伸模組。它僅在 Windows WorkSpaces 和 WorkSpaces 本機用戶端上受到支援。

發行版本	日期	變更
		• 修正登入時有時會出現白色或凍結畫面的問題。 • 錯誤修正與效能改進。
• 視窗 WorkSpaces -	2024年1月11日	• 修正了與登入時潛在串流凍結相關的錯誤。 • 修正了與記錄相關的錯誤。
• 視窗 WorkSpaces -	2023 年 11 月 16 日	• 在 Windows 10+ 上增加了對間接顯示驅動程序（IDD）的支持，從而降低了 CPU 消耗並提高了流式傳輸性能。 • 添加了新的組策略設置以啟用或禁用 IDD 驅動程序。 • 修復了與剪貼板圖像透明度相關的 bug。 • 修正了保留視窗比例因素的錯誤。 • 錯誤修正與效能改進。
• 一般窗戶 WorkSpaces -2.0.1164	2023 年 10 月 13 日	• 在虛擬顯示驅動程序中新增了對 VSync 的支援。 • 新增群組政策設定以啟用或停用 VSync。 • 改進重新連線和可靠性問題。 • 錯誤修正與效能改進。
• Amazon 亞 WorkSpaces 馬遜 • Ubuntu WorkSpaces	2023 年 8 月 18 日	• 新增設定以啟用或停用時區重新導向。 • 延長登入逾時並新增設定選項。 • 改進閘道，以在中斷後加快重新連線速度。 • 錯誤修正與效能改進。

發行版本	日期	變更
• Amazon WorkSpaces	2023 年 6 月 30 日	• 新增對 DCV 延伸模組 SDK 的支援，以啟用 ISV 特定整合。 • 變更中斷連線行為，以便登出終止使用者的工作階段。 • 新增對時區重新導向的支援。 • 延長登入逾時並新增設定選項。 • 修正升級問題。 • 錯誤修正與效能改進。
• 視窗 WorkSpaces -	2023 年 6 月 8 日	• 變更中斷連線行為，以便登出終止使用者的工作階段。 • 修正與 A/V 同步和日文鍵盤相關的錯誤。 • 改進 WSP 安裝程式可靠性。
• Ubuntu WorkSpaces	2023 年 5 月 16 日	• 變更中斷連線行為，以便登出終止使用者的工作階段。 • 新增對 DCV 延伸模組 SDK 的支援，以啟用 ISV 特定整合。 • 新增對時區重新導向的支援。 • 修正升級問題。

發行版本	日期	變更
• 一般窗戶 WorkSpaces -2.0.0.799	2023 年 5 月 8 日	• 透過多種影像品質和效能優化來增強以 UDP 為基礎的 QUIC 傳輸。 • 新增對 DCV 延伸模組 SDK 的支援，以啟用 ISV 特定整合。 • 新增群組政策設定以啟用或停用擴充模組 SDK。 • 改進韓文、日文和德文鍵盤配置。 • 修正與工作階段凍結問題、硬體加速、印表機重新導向、記錄詳細程度和 target-fps 群組政策設定相關的錯誤。

Note

- 如需如何檢查主機代理程式版本的詳細資訊，請參閱最新版的 WSP 支援哪些用戶端和主機作業系統？。
- 如需如何更新主機代理程式版本的詳細資訊，請參閱如果我已經有 WSP WorkSpace，該如何更新它？。
- 如需 WSP macOS WorkSpaces 用戶端版本版本發行說明，請參閱《使用手冊》中「WorkSpaces macOS 用戶端應用程式」一節中的版本說明。
- 如需 WSP Windows 用戶端版本版本發行說明，請參閱《WorkSpaces 使用者指南》中「WorkSpaces Windows 用戶端應用程式」一節中的版本說明。

WSP 支援的 SDK 延伸模組

Amazon WorkSpaces 串流協定 (WSP) 是使用 NICE DCV 技術建立的，可針對各種工作負載和使用案例提供對 WorkSpaces 執行個體的高效能遠端存取。透過 NICE DCV 延伸模組 SDK，開發人員可以為最終使用者自訂 WSP WorkSpaces 體驗，包括：

- 促進自訂硬體支援。
- 增強遠端工作階段中第三方應用程式的可用性。例如，針對 VoIP 應用程式新增本機音訊終止，或針對會議應用程式新增本機視訊播放
- 為螢幕助讀程式等輔助軟體提供遠端工作階段和遠端執行之應用程式的相關資訊。
- 允許安全性軟體分析本機端點的安全狀態，以允許條件式存取政策。
- 透過已建立的遠端工作階段執行任意資料傳輸。

若要開始使用 NICE DCV 延伸模組 SDK，請參閱 NICE DCV 延伸模組 SDK 文件。您可以在 NICE DCV 延伸模組 SDK GitHub 儲存庫中找到 SDK 本身。此外，您還可以在 NICE DCV 延伸模組 SDK 範例 GitHub 儲存庫中找到 SDK 的整合範例。

WorkSpaces 支援下列各項。

- 串流通訊協定 – WorkSpaces 串流協定 (WSP)
- WorkSpaces Windows 用戶端 – Windows：5.9.0.4110 及以上版本。

> **Note**
>
> WorkSpaces Android、iOS 用戶端、Web 存取不支援 NICE DCV 延伸模組 SDK。

- 支援的 WorkSpaces – Windows、Linux 和 Ubuntu 伺服器

WorkSpaces 的文件歷史記錄

下表說明 2018 年 1 月 1 日起 WorkSpaces 服務和《Amazon WorkSpaces 管理指南》的重要變更。我們也會經常更新文件，以處理您傳送給我們的意見回饋。

如需這些更新的通知，您可以訂閱 WorkSpaces RSS 摘要。

變更	描述	日期
AmazonWorkSpacesAdmin 受管政策更新	WorkSpaces 將 workspaces:RestoreWorkspace 動作新增至 AmazonWorkSpacesAdmin 受管政策，並授予管理員還原 WorkSpaces 的存取權。	2023 年 7 月 17 日
WSP 支援的 SDK 延伸模組	透過 NICE DCV 延伸模組 SDK，開發人員可以為最終使用者自訂 WSP WorkSpaces 體驗。	2023 年 5 月 25 日
WorkSpaces 串流協定 (WSP) 主機代理程式版本	WorkSpaces 串流協定 (WSP) 的版本資訊。	2023 年 5 月 8 日
Amazon WorkSpaces 已在 AWS GovCloud (美國東部) 推出	Amazon WorkSpaces 可在 AWS GovCloud (美國東部) 使用。	2023 年 5 月 3 日
Amazon WorkSpaces 網路攝影機支援	Amazon WorkSpaces 現在透過使用 WorkSpaces 串流協定 (WSP) 將本機網路攝影機視訊輸入無縫重新導向至 Windows WorkSpaces 桌面，以支援即時音訊視訊 (AV)。	2021 年 4 月 5 日
WorkSpaces macOS 客戶端應用程式的 Amazon WorkSpaces 智能卡支援	您現在可以將 Amazon WorkSpaces macOS 用戶端應用程式與通用門禁卡 (CAC) 和個人身分驗證	2021 年 4 月 5 日

	(PIV) 智慧卡搭配使用。使用 WorkSpaces 串流協定 (WSP) 可在 WorkSpaces 上提供智慧卡支援。	
Amazon WorkSpaces 套件管理 API	Amazon WorkSpaces 套件管理 API 現已推出。這些 API 動作支援 WorkSpaces 套件的建立、刪除和映像關聯作業。	2021 年 3 月 15 日
Amazon WorkSpaces 已在亞太區域 (孟買) 推出	Amazon WorkSpaces 可在亞太 (孟買) 區域使用。	2021 年 3 月 8 日
WorkSpaces 串流協定 (WSP)	WorkSpaces 串流協定 (WSP) 現在適用於 Graphics 和 GraphicsPro 以外的所有套件類型上包含授權 (Windows Server 2016) 和以 BYOL Windows 10 為基礎的 WorkSpaces。WSP 也適用於 AWS GovCloud (美國西部) 區域中的 Linux WorkSpaces。	2020 年 12 月 1 日
智慧卡	Amazon WorkSpaces 現在支援在 AWS GovCloud (美國西部) 區域的 Windows 和 Linux WorkSpaces 上進行工作階段前 (登入) 和工作階段內智慧卡身份驗證。	2020 年 12 月 1 日
共用自訂映像	您可以在 AWS 帳戶之間共用自訂 WorkSpaces 映像。共用映像之後，收件者帳戶可複製映像並用於建立可供啟動新 WorkSpaces 的套件。	2020 年 10 月 1 日

跨區域重新導向	您現在可以使用跨區域重新導向，此功能可搭配網域名稱系統 (DNS) 路由政策運作，在使用者的主要 WorkSpaces 無法使用時，將使用者重新導向至替代 WorkSpaces。	2020 年 9 月 10 日
訂閱適用於 BYOL WorkSpaces 的 Microsoft Office 2016 或 2019	您現在可以訂閱自帶 Windows 授權 (BYOL) WorkSpaces 上由 AWS 提供的 Microsoft Office Professional 2016 或 2019。	2020 年 9 月 3 日
中國 (寧夏) 的 BYOL 自動化	您可使用自帶授權 (BYOL) 自動化，簡化在中國 (寧夏) 將 Windows 10 桌面授權使用於 WorkSpaces 的程序。	2020 年 4 月 2 日
映像檢查程式	映像檢查程式工具可協助您判斷 Windows WorkSpace 是否符合建立映像的需求。映像檢查程式會在您要用來建立映像的 WorkSpace 上執行一系列測試，並提供如何解決所發現的任何問題的指引。	2020 年 3 月 30 日
遷移 WorkSpaces	Amazon WorkSpaces 遷移功能可讓您將 WorkSpace 從一個套件遷移到另一個套件，同時將資料保留在使用者磁碟區上。您可以使用此功能，將 WorkSpaces 從 Windows 7 桌面體驗遷移至 Windows 10 桌面體驗。您也可以使用此功能，將 WorkSpaces 從一個公用或自訂套件遷移到另一個套件。	2020 年 1 月 9 日

Amazon WorkSpaces API 的 PrivateLink 整合	您可以透過虛擬私有雲端 (VPC) 中的介面端點直接連線至 Amazon WorkSpaces API 端點，而不是透過網際網路進行連線。使用 VPC 介面端點時，VPC 與 Amazon WorkSpaces API 端點之間的通訊會完全在 AWS 網路內安全地進行。	2019 年 11 月 25 日
Amazon WorkSpaces 的 Linux 用戶端	使用者現在可以使用 Linux 用戶端來存取其 WorkSpaces。	2019 年 11 月 25 日
Amazon WorkSpaces 已在中國（寧夏）推出	Amazon WorkSpaces 可在中國 (寧夏) 區域使用。	2019 年 11 月 13 日
將 WorkSpaces 還原到上次已知的良好狀態	您可以使用還原功能將 WorkSpace 復原至上次已知的良好狀態。	2019 年 9 月 18 日
FIPS 端點加密	若要符合聯邦政府風險與授權管理計畫 (FedRAMP) 或國防部 (DoD) 雲端運算安全要求指南 (SRG)的規範，您可以設定 Amazon WorkSpaces，以在目錄層級使用聯邦政府資訊處理標準 (FIPS) 端點加密。	2019 年 9 月 12 日
複製 WorkSpace 映像	您可以複製相同區域或跨區域複製映像。	2019 年 6 月 27 日
使用者的自助式 WorkSpace 管理功能	您可以為使用者啟用自助式 WorkSpace 管理功能，讓他們能夠更好地控制自己的體驗。	2018 年 11 月 19 日

BYOL 自動化	您可以使用自帶授權 (BYOL) 自動化，簡化將 Windows 7 和 Windows 10 桌面授權使用於 WorkSpaces 的程序。	2018 年 11 月 16 日
PowerPro 和 GraphicsPro 套件	PowerPro 和 GraphicsPro 套件現在可用於 WorkSpaces。	2018 年 10 月 18 日
監控成功的 WorkSpace 登入	您可以使用 Amazon CloudWatch Events 的事件來監控並回應成功的 WorkSpace 登入。	2018 年 9 月 17 日
Windows 10 WorkSpaces 的 Web 存取	使用者現在可以使用 Web 存取用戶端來存取執行 Windows 10 桌面體驗的 WorkSpace。	2018 年 8 月 24 日
URI 登入	您可以使用統一資源識別符 (URI) 為使用者提供對其 WorkSpaces 的存取權。	2018 年 7 月 31 日
Amazon Linux WorkSpaces	您可以為使用者佈建 Amazon Linux WorkSpaces。	2018 年 6 月 26 日
IP 存取控制群組	您可以控制使用者可從中存取其 WorkSpaces 的 IP 位址。	2018 年 4 月 30 日
就地升級	您可以將 Windows 10 BYOL WorkSpaces 升級至較新版本的 Windows 10。	2018 年 3 月 9 日

舊版更新

下表說明 2018 年 1 月 1 日之前 Amazon WorkSpaces 服務及其文件集的重要增補。

變更	描述	日期
彈性運算選項	您可以在超值、標準、效能和強力套件之間切換 WorkSpaces	2017 年 12 月 22 日
可設定的儲存體	您可以在啟動 WorkSpaces 時設定根磁碟區和使用者磁碟區的大小，並在稍後增加這些磁碟區的大小。	2017 年 12 月 22 日
控制裝置存取	您可以指定可存取 WorkSpaces 的裝置類型。此外，您可限制 WorkSpaces 對信任裝置 (也稱為受管裝置) 的存取。	2017 年 6 月 19 日
樹系間信任	您可以在 AWS Managed Microsoft AD 與內部部署 Microsoft Active Directory 網域之間建立信任關係，然後在內部部署網域中為使用者佈建 WorkSpaces。	2017 年 2 月 9 日
Windows Server 2016 套件	WorkSpaces 提供包含 Windows 10 桌面體驗的套件 (由 Windows Server 2016 提供支援)。	2016 年 11 月 29 日
Web Access	您可以使用 WorkSpaces Web Access，從 Web 瀏覽器存取 Windows WorkSpaces。	2016 年 11 月 18 日
每小時 WorkSpaces	您可以設定 WorkSpaces，讓使用者按小時計費。	2016 年 8 月 18 日
Windows 10 BYOL	您可以將您的 Windows 10 桌面授權帶到 WorkSpaces (BYOL)。	2016 年 7 月 21 日
標記支援	您可使用標籤來管理和追蹤 WorkSpaces。	2016 年 5 月 17 日
已儲存的註冊	每次您輸入新的註冊碼時，WorkSpaces 用戶端會加以儲存。這樣可以更輕鬆地在不同目錄或區域中的 WorkSpaces 之間切換。	2016 年 1 月 28 日

變更	描述	日期
Windows 7 BYOL、Chromebook 用戶端、WorkSpace 加密	您可以將 Windows 7 桌面授權帶到 WorkSpaces (BYOL)、使用 Chromebook 用戶端，以及使用 WorkSpace 加密。	2015 年 10 月 1 日
CloudWatch 監控	已新增有關 CloudWatch 監控的資訊。	2015 年 4 月 28 日
自動工作階段重新連線	已新增 WorkSpaces 桌面用戶端應用程式中的自動工作階段重新連線功能相關資訊。	2015 年 3 月 31 日
公用 IP 位址	您可以自動將公用 IP 位址指派給 WorkSpaces。	2015 年 1 月 23 日
WorkSpaces 已在亞太區域 (新加坡) 推出	WorkSpaces 可在亞太 (新加坡) 區域使用。	2015 年 1 月 15 日
新增了超值套件、標準套件更新、新增了 Office 2013	超值套件已可用，標準套件硬體已經升級，以及 Microsoft Office 2013 可用於增值套件。	2014 年 11 月 6 日
映像和套件支援	您可以從已自訂的 WorkSpace 建立映像，以及從映像建立自訂 WorkSpace 套件。	2014 年 10 月 28 日
PCoIP 零用戶端支援	您可以存取 WorkSpaces PCoIP 零用戶端裝置。	2014 年 10 月 15 日
WorkSpaces 已在亞太區域 (東京) 推出	WorkSpaces 可在亞太 (東京) 區域使用。	2014 年 8 月 26 日
本機印表機支援	您可以為 WorkSpaces 啟用本機印表機支援。	2014 年 8 月 26 日
多重要素驗證	您可以使用已連線目錄中的多重要素驗證。	2014 年 8 月 11 日
預設 OU 支援和目標網域支援	您可以選取放置 WorkSpace 機器帳戶的預設組織單位 (OU)，以及在其中建立 WorkSpace 機器帳戶的個別網域。	2014 年 7 月 7 日

變更	描述	日期
新增安全群組	您可以將安全群組新增至 WorkSpaces。	2014 年 7 月 7 日
WorkSpaces 已在亞太區域 (雪梨) 推出	WorkSpaces 可在亞太 (雪梨) 區域使用。	2014 年 5 月 15 日
WorkSpaces 已在歐洲 (愛爾蘭) 推出	WorkSpaces 可在歐洲 (愛爾蘭) 區域可在。	2014 年 5 月 5 日
公開試用版	WorkSpaces 可以公開試用版的形式提供。	2014 年 3 月 25 日

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。