部署 Amazon WorkSpaces 應用程式的最佳實務

部署 Amazon WorkSpaces 應用程式的最佳實務:

Table of Contents

部署 Amazon WorkSpaces 應用程式的最佳實務

發佈日期：2022 年 1 月 19 日 (文件修訂)

摘要

本白皮書概述了部署 Amazon WorkSpaces 應用程式 的一組最佳實務。白皮書涵蓋 Amazon Virtual Private Cloud (VPC) 設計、映像建立和管理、機群自訂和機群自動擴展策略。它包含使用者連線方法、身分驗證，以及與 Microsoft Active Directory 的整合。本文也包含設計 WorkSpaces 應用程式安全性、監控和成本最佳化的建議。

此白皮書旨在快速存取相關資訊。它適用於網路工程師、應用程式交付專家、目錄工程師或安全工程師。

簡介

Amazon WorkSpaces 應用程式是一項全受管應用程式串流服務，可讓使用者從任何地方立即存取其桌面應用程式。WorkSpaces 應用程式會管理託管和執行應用程式所需的 AWS 資源。它會自動擴展，並隨需為您的使用者提供存取權。WorkSpaces 應用程式可讓最終使用者存取自己選擇的裝置上所需的應用程式，並提供回應式使用者體驗，與原生安裝的應用程式無異。

下列各節提供 Amazon WorkSpaces 應用程式的詳細資訊、說明服務的運作方式、說明啟動服務所需的內容，以及告訴您可使用哪些選項和功能。為最終使用者部署 WorkSpaces 應用程式時，請務必實作最佳實務，以提供卓越的使用者體驗。此外，所有規模的公司都受益於成本最佳化，可降低每月營運成本。

重要概念

若要充分利用 WorkSpaces 應用程式，請熟悉下列概念：

- 映像 — 映像是預先設定的執行個體範本。映像包含您可以串流給使用者的應用程式，以及預設 Windows 和應用程式設定，可讓您的使用者快速開始使用其應用程式。 AWS 提供基本映像，可讓您用來建立包含自己應用程式的影像。建立映像後，您即無法變更它。若要新增其他應用程式、更新現有的應用程式或變更映像設定，您必須建立新的映像。您可以將映像複製到其他 ，AWS 區域或與相同區域中的其他 AWS 帳戶共用。
- 映像建置器 — 映像建置器是您用來建立映像的虛擬機器。您可以使用 WorkSpaces 應用程式主控台啟動並連線至映像建置器。在您連線到映像建置器後，您可以安裝、新增和測試您的應用程式，然後使用映像建置器建立映像。您可以透過使用您自己的私有映像，來啟動新的映像建置器。
- 機群 — 機群包含執行您指定映像的機群執行個體 （ 也稱為串流執行個體 ）。您可以為機群設定所需的串流執行個體數量，並設定政策以根據需求自動擴展機群。請注意，每個使用者都需要一個執行個體。
- 堆疊 — 堆疊包含相關聯的機群、使用者存取政策和儲存組態。您可以設定堆疊，然後開始將應用程式串流至使用者。
- 串流執行個體 — 串流執行個體 （ 也稱為機群執行個體) 是可供單一使用者用於應用程式串流的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。使用者的工作階段完成後，Amazon EC2 會終止執行個體。

VPC 設計

設計指導方針

將 WorkSpaces 應用程式部署至專用 VPC。設計 WorkSpaces 應用程式 VPC 時，預測成長的大小。為新的使用案例預留 IP 地址容量，以及稍後可能會新增的其他可用區域 (AZs)。WorkSpaces 應用程式的基本設計點是只有一個使用者可以使用 WorkSpaces 應用程式執行個體。配置 IP 空間時，請將一個使用者視為每個 WorkSpaces 應用程式執行個體的一個 IP 地址。透過 WorkSpaces 應用程式，使用者可以使用多個 WorkSpaces 應用程式執行個體。因此，規劃 IP 空間也必須考慮需要額外 WorkSpaces 應用程式執行個體的使用案例。

雖然 VPC 無類別網域間路由 (CIDR) 的大小上限為 /16，但 AWS 建議不要過度配置私有 IP 地址。您可以將 VPC 的大小延伸到其他 CIDRs，但對此有限制；因此，請從一開始就配置所需的項目。

如果 WorkSpaces 應用程式部署已加入 Active Directory 網域，則 VPC 的 DHCP 選項集必須設定網域 DNS。網域名稱伺服器應指定 Active Directory 網域的授權 DNS IP 地址，或 DNS 應將 DNS 請求轉送至 Active Directory 網域的授權 DNS 執行個體。此外，VPC 必須已`EnableDnsSupport`設定`enableDnsHostnames`和 。

可用區域

可用區域 (AZ) 是一個或多個離散的資料中心，在 中具有備援電源、聯網和連線能力 AWS 區域。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

Amazon WorkSpaces 應用程式只需要一個子網路，機群才能啟動。最佳實務是設定至少兩個可用區域，每個唯一的可用區域一個子網路。若要最佳化機群自動擴展，請使用兩個以上的可用區域。水平擴展具有在子網路中新增 IP 空間以進行增長的額外優勢，如本文件的下列子網路大小一節所述。AWS 管理主控台只會在建立機群期間指定兩個子網路。使用 AWS Command Line Interface(AWS CLI) 或 AWS CloudFormation 允許兩個以上的子網路 IDs。

調整子網大小

專用於 WorkSpaces 應用程式機群的子網路，以允許路由政策和網路存取控制清單的彈性。Stacks 可能有個別的資源需求。例如，WorkSpaces Applications Stacks 可以有隔離需求來提供分隔規則集的方法。當多個 Amazon WorkSpaces 應用程式機群使用相同的子網路時，請確保所有機群的最大容量總和不超過可用的 IP 地址總數。

如果相同子網路中所有機群的最大容量可能或已超過可用的 IP 地址總數，請將機群遷移至專用子網路。這可防止自動擴展事件耗盡配置的 IP 空間。如果機群的總容量超過指派子網路的配置 IP 空間，請使用 API 或 AWS CLI「更新機群」來指派更多子網路。如需詳細資訊，請參閱 Amazon VPC 配額，以及如何增加配額。

最佳實務是擴展子網路數量，相應地調整子網路大小，同時保留在 VPC 中增長的容量。此外，請確保 WorkSpaces 應用程式機群上限不超過子網路配置的總 IP 空間。對於 中的每個子網路 AWS，在計算 IP 空間總量時，會保留五個 IP 地址。使用兩個以上的子網路並水平擴展可提供數種優點，例如：

- 因可用區域故障而提高彈性
- 自動擴展機群執行個體時的輸送量更高
- 更有效率地使用私有 IP 地址，避免 IP 燒毀

調整 Amazon WorkSpaces 應用程式的子網路大小時，請考慮子網路總數，以及尖峰使用率期間的預期尖峰並行。這可以使用 (`InUseCapacity`) 加上機群的預留容量 (`AvailableCapacity`) 進行監控。在 Amazon WorkSpaces 應用程式中，耗用和available-to-be-consumed WorkSpaces 應用程式機群執行個體的總和會標記為 `ActualCapacity`。若要正確調整總 IP 空間的大小，請預測所需的 `ActualCapacity`，然後除以指派給機群的子網路數量，減去一個子網路的彈性。

例如，如果尖峰時的預期機群執行個體數量上限為 1000，且業務需求是在一個可用區域故障時具有彈性，則 3 x/23 子網路可滿足技術和業務需求。

- /23 = 512 個主機 — 5 個預留 = 每個子網路 507 個機群執行個體
- 3 個子網路 — 1 個子網路 = 2 個子網路
- 2 個子網路 x 每個子網路 507 個機群執行個體 = 尖峰 1，014 個機群執行個體

子網路大小範例

雖然 2 x /22 子網路也可以滿足彈性，但請考慮下列事項：

- 而不是保留 1，536 個 IP 地址，使用兩個 AZs 會導致保留 2，048 個 IP 地址，浪費可能前往其他函數的 IP 地址。
- 如果無法存取一個 AZ，擴展機群執行個體的能力會受到 AZ 輸送量的限制。這可以延長 的持續時間`PendingCapacity`。

子網路由

最佳實務是為 WorkSpaces 應用程式執行個體建立私有子網路，並透過集中式 VPC 路由至公有網際網路以進行傳出流量。WorkSpaces 應用程式工作階段串流的傳入流量會透過 Amazon WorkSpaces 應用程式服務透過串流閘道處理：您不需要為此設定公有子網路。

區域間連線

對於加入 Active Directory 網域的 WorkSpaces 應用程式機群執行個體，請在每個執行個體的共用服務 VPC 中設定 Active Directory 網域控制器 AWS 區域。Active Directory 的來源可以是 Amazon EC2 型網域控制器或 AWS Microsoft Managed AD。共用服務和 WorkSpaces 應用程式 VPCs之間的路由可以透過 VPC 互連連線或傳輸閘道進行。雖然傳輸閘道可解決大規模路由的複雜性，但有許多原因使得 VPC 對等互連在大多數設定中較適合：

- VPC 對等互連是兩個 VPCs之間的直接連線 （沒有額外的跳轉）。
- 不收取每小時費用，僅收取可用區域之間的標準資料傳輸率。
- 頻寬沒有限制。
- 支援在 VPCs之間存取安全群組。

如果 WorkSpaces 應用程式執行個體連線到共用服務 VPC 中具有大型資料集的應用程式基礎設施和/或檔案伺服器，則尤其如此。透過最佳化這些常用資源的路徑，即使在透過傳輸閘道執行所有其他 VPC 和網際網路路由的設計中，還是偏好 VPC 互連連線。

傳出網際網路流量

雖然直接路由至共用服務主要是透過對等連線進行最佳化，但 WorkSpaces 應用程式的傳出流量可以透過使用 AWS Transit Gateway 從多個 VPCs建立單一網際網路結束點來設計。在多 VPC 設計中，標準實務是擁有控制所有傳出網際網路流量的專用 VPC。使用此組態，傳輸閘道具有更大的彈性，並控制連接至子網路之標準路由表的路由。此設計也支援無額外複雜性的傳輸路由，並不需要在每個 VPC 中使用備援網路位址轉譯 (NAT) 閘道或 NAT 執行個體。

一旦將所有傳出網際網路流量集中到單一 VPC 中，NAT 閘道或 NAT 執行個體是常見的設計選擇。若要判斷哪個最適合您的組織，請檢視管理指南來比較 NAT 閘道和 NAT 執行個體。AWS Network Firewall 可以在路由層級保護 ，並在 OSI 模型中提供從第 3 層到第 7 層的無狀態和有狀態規則，藉此將保護延伸到安全群組和網路存取控制層級之外。如需詳細資訊，請參閱 AWS Network Firewall 的部署模型。如果您的組織已選擇執行 URL 篩選等進階功能的第三方產品，請將服務部署到您的傳出網際網路 VPC。這可以取代 NAT 閘道或 NAT 執行個體。遵循第三方供應商提供的準則。

現場部署

當需要連線到內部部署資源時，特別是加入 Active Directory 的 WorkSpaces 應用程式執行個體，請透過 建立高彈性的連線 AWS Direct Connect。

VPC 端點

Amazon S3 VPC 端點

許多 Amazon WorkSpaces 應用程式部署都需要透過主資料夾和應用程式設定維持使用者狀態。啟用與這些 Amazon Simple Storage Service (Amazon S3) 位置的私有通訊，避免使用公有網際網路。您可以透過 VPC 端點閘道達成此目標。VPC 端點閘道優於 AWS PrivateLink Amazon S3 的，因為：

- 其成本已針對 WorkSpaces 應用程式網路存取需求進行最佳化
- 內部部署資源不需要 Amazon S3 儲存貯體存取
- 自訂政策文件可用來限制只能從 WorkSpaces 應用程式執行個體存取

建立 VPC 端點閘道後，最佳實務是透過建立自訂政策來保護私有連線。自訂政策從 WorkSpaces 應用程式服務 Identity and Access Management 角色的 Amazon Resource Name (ARN) 開始。明確指定使用者狀態持續性所需的 S3 動作。

> **Note**
>
> `Resources` 區段中的下列範例會先指定狀態主資料夾路徑，再指定應用程式設定路徑。

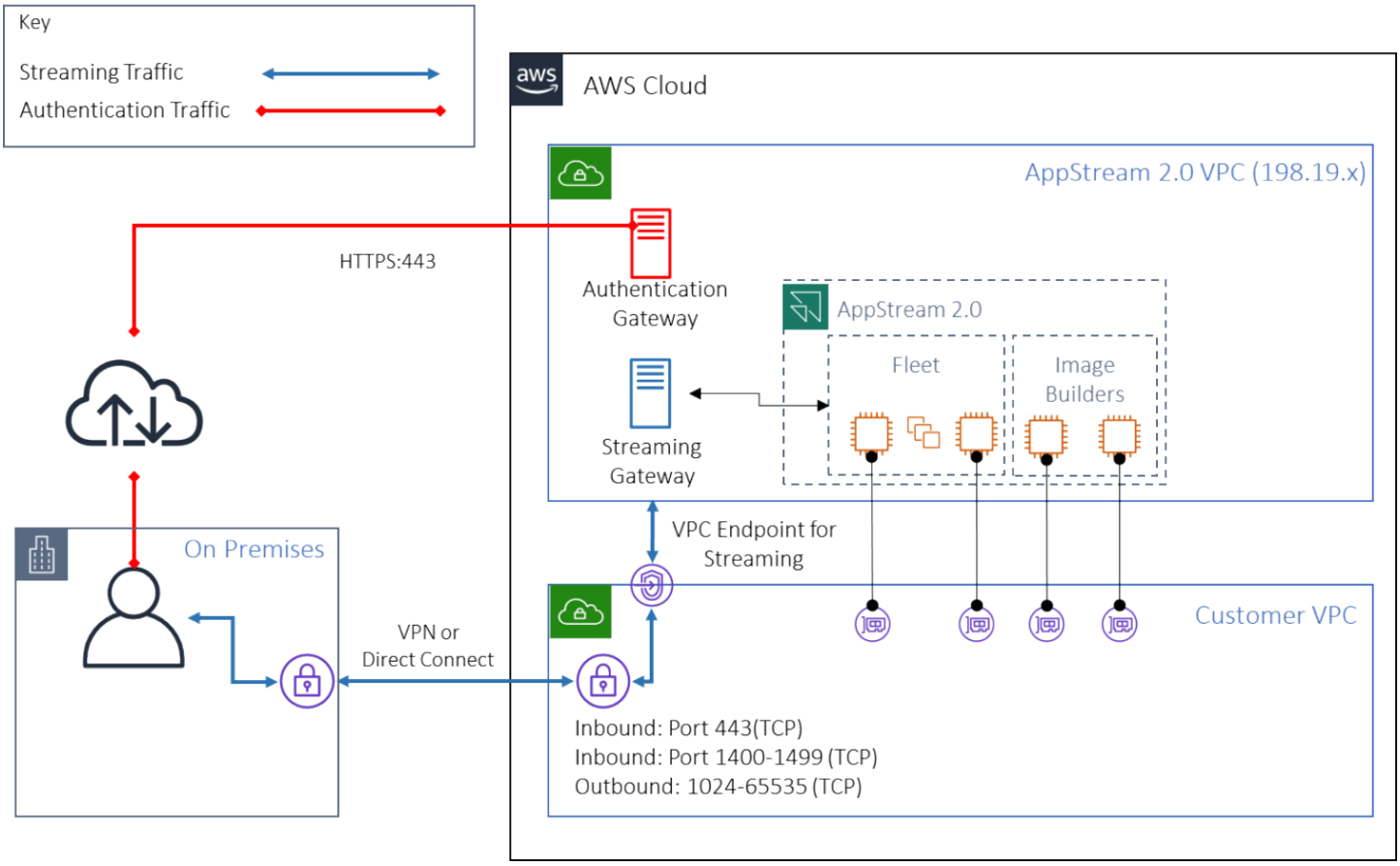
Example

Amazon WorkSpaces 應用程式 API 介面 VPC 端點

在對 Amazon WorkSpaces 應用程式發出 API 和 CLI 命令的設計案例中，請透過介面 VPC 端點將這些程式設計呼叫私有化。

Amazon WorkSpaces 應用程式串流介面 VPC 端點

雖然可以透過介面 VPC 端點路由 Amazon WorkSpaces 應用程式串流流量，但請謹慎使用此組態。透過公有網際網路的預設串流行為是 Amazon WorkSpaces 應用程式串流流量最有效率且效能最佳的交付方法。



Amazon WorkSpaces 應用程式串流介面 VPC 端點

如上圖所示，公有網際網路是 Amazon WorkSpaces 應用程式串流閘道最有效率的路徑。透過客戶受管 VPC 和聯網進行路由會增加複雜性和延遲。它也會增加資料傳輸費用 Direct Connect。

> **Note**
>
> VPC 端點僅支援串流，且身分驗證仍必須透過公有網際網路進行。SAML 單一登入 (SSO) 身分提供者 (IdP) 等先決條件存取仍然是只能透過公有網際網路存取的要求。

映像建立和管理

在 WorkSpaces 應用程式中啟動機群或映像建置器時，您必須選取其中一個 WorkSpaces 應用程式基礎映像。然後，管理員可以在基礎映像上建置，以新增自己的應用程式和組態設定。

建置映像以確保應用程式正確且安全地運作時，有重要的考量。此外，還有如何維護該映像的設計考量。

建置 WorkSpaces 應用程式映像

建立新映像時，請務必考量下列事項：

- 作業系統
- 應用程式
- 使用者設定檔
- 安全
- 效能
- 代理程式版本
- 映像助理 CLI

建置 WorkSpaces 應用程式映像

2021 年 11 月，WorkSpaces 應用程式啟動了對 Amazon Linux 2 的支援。透過此公告，WorkSpaces 應用程式現在支援四種平台類型：

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Amazon Linux 2

您可能需要根據應用程式的需求選擇特定平台（例如，如果您的應用程式需要 Windows，Amazon Linux 2 將不是選項）。除了應用程式需求之外，請參考下列比較矩陣，以協助您選擇最適合使用案例和環境的平台類型：

表 1 — 平台類型、使用時機和定價

平台類型	使用情況	機群定價*
Windows Server (2012 R2、2016 或 2019)	您的應用程式只能在 Windows 中執行（且不支援 Amazon Linux 2)。您希望網域加入您的串流執行個體。您希望在 WorkSpaces 應用程式串流執行個體上使用現有的群組政策 (Linux 不遵循群組政策，但您可以在工作階段開始時使用工作階段指令碼來自動化組態）。您將使用桌面檢視，您的使用者偏好 Windows 桌面體驗。您偏好使用提供step-by-step精靈的映像助理應用程式來建立應用程式目錄和映像。目前，您必須使用終端機命令建立 Amazon Linux 2 映像（如需詳細資訊，請參閱本教學課程）。您想要使用應用程式設定持久性。Linux 型堆疊目前不支援啟用應用程式設定持續性。	RDS SAL (Microsoft 遠端桌面服務訂閱者存取授權） 費用為每位唯一使用者每月 4.19 USD**，再加上下列項目： 1. Always-On 隨需機群每小時 0.10 美元 2. 彈性機群每小時 0.15 美元
Amazon Linux 2	您想要利用成本較低的串流執行個體，並避免 RDS SAL 授權費用。您的應用程式與 Amazon Linux 2 相容	與 Window 執行個體相比，Linux 執行個體的成本較低。使用 Linux，您無需支付 RDS SAL 費用和下列每小時費用： 1. Always-On 隨需機群每小時 0.084 美元 2. 彈性機群每小時 0.112 美元

* 根據 N Virginia 區域中的 stream.standard.medium

** 符合資格的客戶可以自行取得授權，以免除 AWS RDS SAL 費用。如需詳細資訊，請參閱 WorkSpaces 應用程式定價頁面。教育客戶也可能符合特殊資格。學校、大學和特定公有機構可能符合 Microsoft RDS SAL 使用者費用的折扣資格。

應用程式

安裝應用程式之前，請務必檢閱應用程式需求，例如應用程式相依性和硬體需求。在映像建置器執行個體上成功安裝應用程式後，請務必在測試使用者內容下切換使用者和測試應用程式。

規劃應用程式部署時，請注意服務端點和配額。此外，在建立映像之前，請清除安裝程式和協助程式檔案，以最佳化 C 磁碟機總空間。提醒您，WorkSpaces 應用程式執行個體有一個 200 GB 的固定大小磁碟區。安裝後最佳化磁碟空間是最佳實務，可確保絕不超過固定大小的磁碟區。

如果您想要修改使用者可即時存取的應用程式目錄，動態應用程式架構會提供 API 操作。由動態應用程式提供者管理的應用程式可位於映像中，也可以在執行個體以外 (例如來自 Windows 檔案共享或應用程式虛擬化技術)。此功能需要加入 Microsoft Active Directory 網域的 WorkSpaces 應用程式機群。如需詳細資訊，請參閱搭配使用 Active Directory 與 WorkSpaces 應用程式。

應用程式區塊

應用程式區塊代表啟動使用者將使用的應用程式所需的設定指令碼和應用程式檔案。虛擬硬碟 (VHD) 可以是 Amazon S3 中的任何物件。建議此物件小於 1.5GB，因為必須先完全下載，使用者才能存取應用程式。

最佳化應用程式區塊

對於 Windows 型機群，建議您建立 VHDX 檔案以包含您的應用程式。對於 Linux 型機群，建議您建立映像 (IMG)。這些虛擬磁碟應建立得越小越好，以託管應用程式檔案。虛擬磁碟可以壓縮，以進一步減少其大小。在設定指令碼中，您需要先解壓縮磁碟，再進行掛載。Windows PowerShell 設定指令碼範例包含解壓縮功能。擴展封存 (zip) 和下載速度之間存在權衡。有些測試可能需要尋找提供最快應用程式啟動時間的平衡。

更新應用程式

應用程式可以同時進行次要和主要變更。對於次要更新，請在託管應用程式區塊檔案的 Amazon S3 儲存貯體上使用啟用版本控制。此設定可讓管理員透過變更有問題的應用程式 VHD 物件版本來回復到特定應用程式的先前版本，而無需變更應用程式區塊組態。使用主要更新，為更新的 VHD 建立新的應用程式區塊。這將允許管理員在應用程式區塊層級分隔主要應用程式變更，而不是版本控制層級，這為管理應用程式管理提供了更有條理的方法。

使用者設定檔自訂

Amazon WorkSpaces 應用程式是透過設計非持久性應用程式和桌面解決方案。當使用者工作階段終止時，系統與使用者變更也會終止。僅在需要時啟用應用程式設定持續性。它會為登入程序增加額外負荷，以及所需 S3 儲存體的成本考量。

在需要應用程式設定持久性的情況下， AWS 建議透過自訂政策和 S3 VPC 閘道端點保護該連線。評估整體應用程式設定大小，並將應用程式設定持久性中儲存的設定降至最低，以最佳化成本和效能。

您可以在 WorkSpaces 應用程式映像建置器執行個體上設定使用者設定檔自訂。這包括新增和修改登錄機碼、新增檔案和其他使用者特定的組態。從 WorkSpaces 應用程式映像助理中，您可以選擇建立使用者設定檔。這會將範本使用者設定檔複製到預設使用者設定檔。部署映像到機群後，從機群串流工作階段的最終使用者將從預設使用者設定檔建立其使用者設定檔。請務必考慮將使用者設定檔大小降至最低，尤其是在啟用應用程式設定持續性時。根據預設，使用者設定檔的 VHDx 大小上限為 1 GB。每次串流工作階段啟動時，都會從 S3 儲存貯體下載使用者設定檔 VHDx 檔案。這會增加串流工作階段準備時間，並帶來超出限制的風險，這會導致使用 VHDx 檔案的使用者設定檔掛載失敗。

對於需要大於 1 GB 的使用者設定檔的使用案例，AWS 建議使用替代方法來存放設定檔。例如，在 Amazon FSx for Windows File Server 等共用儲存體上使用漫遊設定檔或 FSLogix 設定檔容器。FSx 如需詳細資訊，請參閱使用 Amazon FSx for Windows File Server 和 FSLogix 來最佳化 Amazon WorkSpaces 應用程式上的應用程式設定持續性。

安全

開發人員需要考慮不同的安全性測量。WorkSpaces 應用程式管理員負責安裝和維護 Windows 作業系統、您的應用程式及其相依性的更新。如需將基礎映像保持在最新狀態的其他指導，請參閱將 WorkSpaces 應用程式映像保持在Up-to-Date，以取得將基礎映像保持在最新狀態的其他指導。

根據預設，WorkSpaces 應用程式允許使用者或應用程式在執行個體上啟動任何程式，超出映像應用程式目錄中指定的程式。當您的應用程式依賴另一個應用程式做為工作流程的一部分，但您不希望使用者能夠直接啟動該相依應用程式時，這會很有用。例如，您的應用程式會啟動瀏覽器，以提供來自應用程式廠商網站的說明說明，但您不希望使用者直接啟動瀏覽器。在某些情況下，您可能想要控制哪些應用程式可以在串流執行個體上啟動。Microsoft AppLocker 是應用程式控制軟體，使用明確的控制政策來啟用或停用使用者可以執行的應用程式。

防毒軟體可能會對串流工作階段和映像建置器執行個體造成負面影響。 AWS 建議您不要啟用防毒軟體的自動更新。如需 Windows Defender 的詳細資訊，請參閱防毒軟體。

效能

建立新映像之前，請務必以測試使用者身分測試應用程式。以測試使用者身分進行測試可讓您確保應用程式可在非管理員使用者內容下執行。此外，使用 Task Manager 和 Performance Monitor 等內建工具來檢查應用程式效能和使用者體驗。最佳實務是監控資源使用率，例如 CPU、記憶體和 GPU 記憶體。如果有 CPU、記憶體或 GPU 記憶體資源限制，請考慮升級執行個體類型。若要增強效能：

- 停用瀏覽器快顯視窗
- 停用增強的 IE 安全性

WorkSpaces 應用程式代理程式版本選擇

建立新映像時，您可以選擇使用最新的 WorkSpaces 應用程式代理程式軟體，或不更新。WorkSpaces 應用程式代理程式軟體的每個版本都包含錯誤修正和功能增強功能。使用up-to-date軟體來保留映像。在本文件的影像更新區段中檢閱此項目的機制。

您可以選擇使用最新的代理程式選項。此選項可確保啟動時一律安裝最新的 WorkSpaces 應用程式代理程式。不過，非預期的變更可能會影響使用者體驗，而代理程式更新可能會增加啟動執行個體的時間。更新基礎映像需要重新建立映像。您也務必在將更新的映像推出生產環境之前執行測試，以將啟動時間降至最低。

映像助理命令列界面 (CLI)

對於想要自動化或以程式設計方式建立 WorkSpaces 應用程式映像的開發人員，請使用映像助理 CLI。您可以在映像建置器上使用 2019 年 7 月 26 日當天或之後發行的 WorkSpaces 應用程式代理程式軟體。下列高階概觀說明以程式設計方式建立 WorkSpaces 應用程式映像的程序：

1. 使用應用程式安裝自動化在映像建置器上安裝所需的應用程式。此安裝可能包含使用者將啟動的應用程式、任何依存項目，與背景應用程式。
2. 決定要最佳化的檔案和資料夾。
3. 如果適用，請使用映像助理 `add-application` CLI 操作來指定 WorkSpaces 應用程式映像的應用程式中繼資料和最佳化資訊清單。
4. 若要為 WorkSpaces 應用程式映像指定其他應用程式，請視需要為每個應用程式重複步驟 1 到 3。
5. 如果適用，請使用映像助理 `update-default-profile` CLI 操作覆寫預設 Windows 設定檔，並為使用者建立預設應用程式和 Windows 設定。
6. 使用映像助理 `create-image` CLI 操作來建立映像。

如需詳細資訊，請參閱使用映像助理 CLI 操作以程式設計方式建立 WorkSpaces 應用程式映像。

管理使用者的串流體驗

使用工作階段指令碼自訂

WorkSpaces 應用程式提供執行個體上的工作階段指令碼。當使用者的串流工作階段發生特定事件時，您可以使用這些指令碼來執行您自己的自訂指令碼。例如，您可以在使用者的串流工作階段開始之前，使用自訂指令碼來準備 WorkSpaces 應用程式環境。在使用者完成其串流工作階段之後，您也可以使用自訂指令碼來清除串流執行個體。

在 WorkSpaces 應用程式映像中指定工作階段指令碼。如需設定工作階段指令碼的詳細資訊，請參閱管理指南的章節，了解如何使用工作階段指令碼來管理使用者體驗。與網路共用或 AWS Identity and Access Management(IAM) 設定檔搭配使用，您可以使用工作階段指令碼從儲存位置擷取其他指令碼。透過此額外的指令碼，您可以執行進一步的使用者體驗最佳化。這可以將交付應用程式環境給使用者所需的映像和機群數量降至最低。

使用 Active Directory 群組政策

如果您打算在 Active Directory 網域中使用 WorkSpaces 應用程式機群，您可以使用群組政策物件 (GPOs) 來管理使用者體驗。GPOs可以指派給建立 WorkSpaces 應用程式執行個體的組織單位 (OU)。若要簡化映像建立，請在封鎖繼承的 OU 中啟動基本 WorkSpaces 應用程式映像。這可防止其他網域政策影響 WorkSpaces 應用程式使用者體驗。使用建立環境的唯一 GPOs，將每個機群部署到其專用 OU 中，one-to-many合併優勢。 WorkSpaces

使用群組政策的範例是為每個 WorkSpaces 應用程式機群指定映像集不同的 Internet Explorer 首頁。

映像更新

軟體修補對於運算資源的安全性和效能至關重要。頻繁修補列為 Well-Architected Framework 安全支柱中的最佳實務。

建置並部署映像時，WorkSpaces 應用程式映像中有四種需要修補的軟體類別：

- 應用程式和相依性 — 您負責修補映像中的應用程式和相依性。
- Microsoft Windows 作業系統 — 您負責安裝和維護 Windows 的更新。
- 軟體元件 — 這些是 WorkSpaces 應用程式操作所需的驅動程式、代理程式和其他軟體（例如 Amazon CloudWatch代理程式）。WorkSpaces 應用程式會定期發行包含新代理程式和驅動程式的

新基礎映像。您可以使用最新的 基礎來重建映像，讓其映像上的軟體元件達到最新的基準。當有許多應用程式或安裝複雜的應用程式時，在最新基礎上重建映像的程序可能既耗時又繁瑣。

- WorkSpaces 應用程式代理程式 — 您可以在映像助理中選擇一律使用最新的代理程式版本。使用此選項時，從映像啟動的串流執行個體會自動使用最新版本的代理程式。

您可以執行下列任一動作，讓 WorkSpaces 應用程式映像保持在最新狀態：

- 使用受管 WorkSpaces 應用程式映像更新來更新映像 – 此更新方法提供最新的 Windows 作業系統更新和驅動程式更新，以及最新的 WorkSpaces 應用程式代理程式軟體。此受管方法會更新服務和 Microsoft 作業系統元件，但不允許您更新應用程式元件。當應用程式安裝複雜或需要手動設定時，最佳實務是使用此方法。
- 使用受管 WorkSpaces 應用程式映像版本更新 WorkSpaces 應用程式代理程式軟體 – 此更新方法提供最新的 WorkSpaces 應用程式代理程式軟體。此方法確實可讓您更新應用程式元件。

機群自訂

機群類型

建立機群時，客戶必須選擇機群類型。每種機群類型為使用者體驗、成本和維護開銷提供不同的優勢。無論選擇的機群類型為何，每個選項都支援 Windows 和 Linux 平台類型，以及桌面檢視或應用程式檢視。

客戶現在可以從下列機群類型中選擇：

- Always-On — 此機群類型可讓使用者即時存取其應用程式。即使沒有使用者在串流應用程式，您仍需支付機群中所有執行中執行個體的費用。
- 隨需 — 選取此機群類型以最佳化串流成本。使用隨需機群時，使用者的工作階段開始時間約為一到兩分鐘。不過，只有在使用者連線時才會向您收取串流執行個體費用，而且機群中每個執行個體若不是串流應用程式，將按小時支付少許費用。
- 彈性 — 彈性機群可用於不需要安裝的應用程式，並且可以從虛擬硬碟 (VHD) 執行。彈性機群不支援 WorkSpaces 應用程式映像，也不需要擴展政策。您只需支付串流工作階段期間的費用。

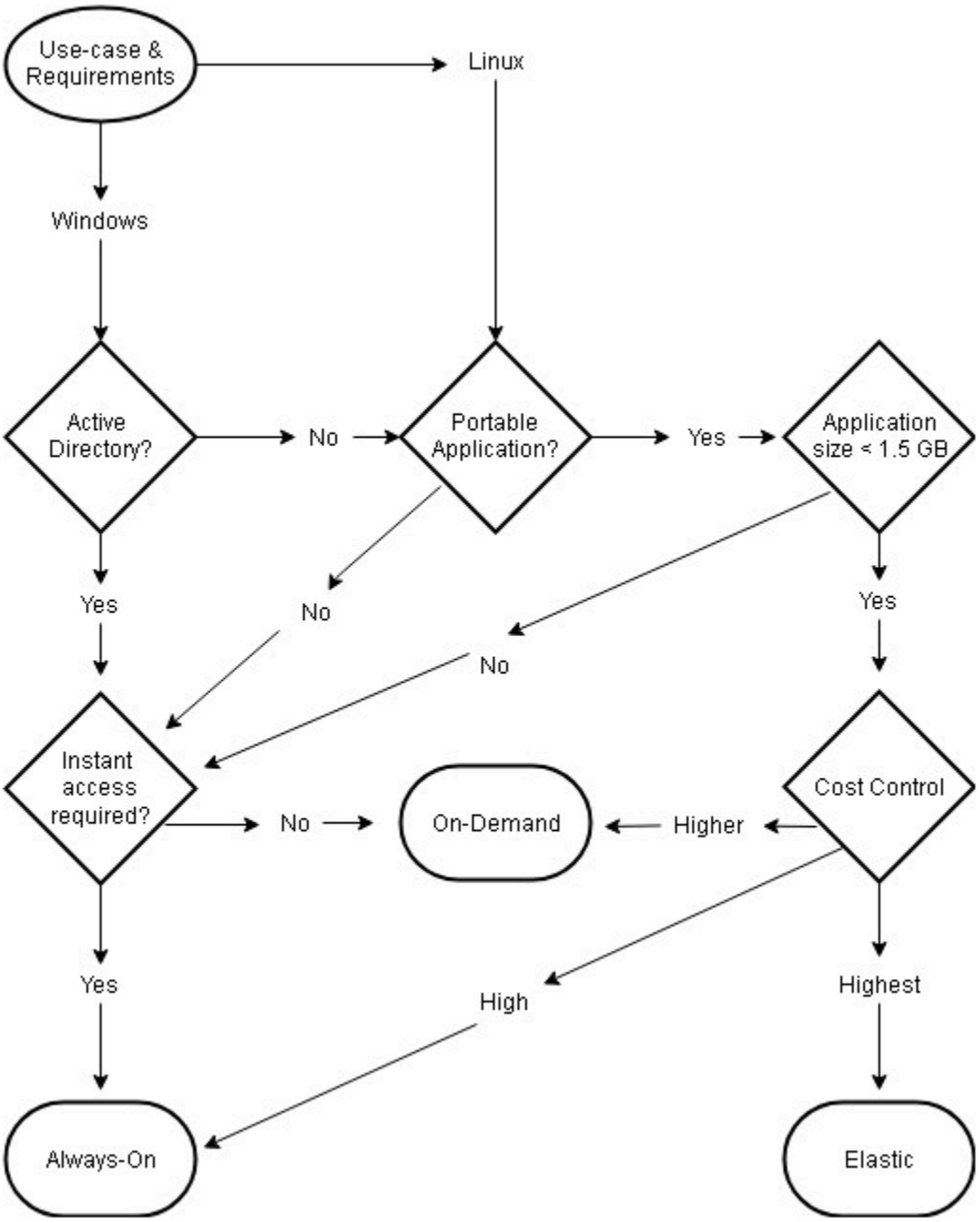
表 2 — Amazon WorkSpaces 應用程式機群類型

機群類型	使用情況	使用者體驗	定價方式	備註
Always-On	您的使用者在啟動工作階段時需要立即存取應用程式。您的機群中不會有大量多餘的容量，可能是因為您的用量模式是可預測的，而且您可以使用擴展政策可靠地控制成本。	即時存取應用程式	您可以為機群中可用的每個執行個體支付完整價格（無論是否用於工作階段）。	支援自訂映像和擴展政策。
On-Demand	您必須在fleet sYou 您想要最符	使用者會在啟動工作階段後等待	您只需為具有作用中工作階段的	支援自訂映像和擴展政策。

機群類型	使用情況	使用者體驗	定價方式	備註
	合成本最佳化的環境，並且不想為未使用的capacityYour使用者可以在啟動工作階段後等待一到兩分鐘來存取其應用程式。您正在使用較大的執行個體類型。執行中執行個體的每小時成本比停止的執行個體費用更昂貴。	一到兩分鐘來存取其應用程式。	串流執行個體支付完整價格，然後為閒置執行個體支付小額的每小時成本。	

機群類型	使用情況	使用者體驗	定價方式	備註
彈性	您的應用程式及其相依性小於 ~1.5 GB。每次使用者在彈性機群中啟動工作階段時，您的虛擬硬碟 (VHD) 檔案都必須從 Amazon S3 下載到工作階段。因此，較大的 VHD 檔案（即大小大於 1.5 GB) 會導致最終使用者體驗不佳。您的應用程式是可攜式的。也就是說，您的應用程式及其所有相依性可以放置在 VHD 上，並從 VHD 啟動。您不需要加入網域的串流執行個體 （網域加入目前不適用於彈性機群） 您只想為作用中工作階段付費 （亦即，您不需要為機群中未使用的容量付費）。您的使用者可以在啟動工作階段後等待 45 秒以上來存取其應用程式。您希	使用者會在啟動工作階段後等待 45 秒到 3 分鐘來存取應用程式（等待時間取決於虛擬硬碟的大小）。	您只需支付串流工作階段期間的費用。由於沒有彈性機群閒置執行個體的概念，因此未使用的執行個體不會產生任何費用。	不支援自訂映像（客戶向應用程式提供 VHD) 或擴展政策。目前支援 `stream.standard.small` 和 `stream.standard.medium` 執行個體。如果您的使用案例需要不同的執行個體類型，請聯絡您的 AWS 客戶團隊。

機群類型	使用情況	使用者體驗	定價方式	備註
	望 AWS 為您管理擴展（無需管理擴展政策）。			



機群類型使用案例和需求

機群大小

最小容量和排程擴展

調整 WorkSpaces 應用程式機群的大小時，有幾個直接轉換為使用者體驗和成本的考量事項。輸入的最小容量值可確保 WorkSpaces 應用程式執行個體數目很少低於此值。WorkSpaces 應用程式工作階段結束後，如果 WorkSpaces 應用程式執行個體總數小於最小容量值，就會啟動新的機群執行個體。一如往常，請務必記住一個 WorkSpaces 應用程式執行個體會直接映射到一個使用者工作階段，直接影響最小容量的值。

為超出預期並行的最小容量輸入值會導致成本增加，但使用者體驗不會受到影響。值太低會導致低成本，但當請求總數超過可用容量時，會影響使用者體驗。管理員會在這種情況下觀察到「容量不足」錯誤。例如，當一天開始時的預期連線數目是可預測的一致值時，等待`PendingCapacity`成為`AvailableCapacity`是使用者時間的效率低落。

從容納典型離峰時數的最小容量開始，然後使用排程擴展政策，在工作日開始之前有效地重設最小容量。請勿忘記建立另一個排程擴展政策，將最小容量還原為離峰時數。如需擴展政策以及如何實作政策的詳細資訊，請參閱本文件中的機群自動擴展策略一節。

最大容量和服務配額

設定最大容量可能是任意值，但當正確預測和設定時，它會最佳化總資源消耗和成本。輸入的值若高於您 中 WorkSpaces 應用程式機群的服務配額 AWS 帳戶 ，可能看起來是有效的，但當自動擴展事件嘗試將資源擴展到最大容量時，會無法啟動，因為最大容量值超過可用的服務配額。確保為所需的最大容量提出服務配額請求，以確保依照您的組織預期自動擴展函數。

設定最大容量值時的另一個重要考量是成本。如需詳細資訊，請參閱本文件的使用機群類型選擇最佳化成本一節。

選擇桌面檢視或應用程式檢視

選擇應用程式檢視或桌面檢視的判斷不會影響效能或成本。每個 WorkSpaces 應用程式機群隨時只能存取一個檢視。您可以變更串流檢視選項。在離峰上班時間規劃此變更，因為變更串流檢視需要重新啟動機群。

串流檢視沒有單一最佳實務。串流檢視選項的影響摘要如下：

- 透過管理員的用量報告功能，詳細報告應用程式用量
- 最終使用者的整體體驗和工作流程（例如，完整的桌面是否滿足使用案例的需求，或只檢視應用程式是否足夠？)。

桌面檢視

對於在工作階段中執行所有使用者工作流程的使用案例，桌面檢視透過將所有應用程式集中在一個環境中來簡化使用者體驗。桌面檢視可為需要與作業系統 (OS) 整合的 3-5 個以上應用程式提供更一致的使用者體驗。桌面檢視在維護兩個獨立且不同的環境時有效。例如，使用者可以同時存取生產環境和生產前桌面環境，以驗證配置、組態和應用程式存取的變更。

WorkSpaces 應用程式用量報告會建立桌面檢視的每日應用程式報告。應用程式產生的輸出只是「桌面」，直接映射到 WorkSpaces 應用程式工作階段。如需詳細資訊，請參閱本文件的監控使用者用量一節。

僅限應用程式檢視

當 WorkSpaces 應用程式堆疊旨在間歇性地提供一些應用程式時，僅限應用程式檢視也有效。在資訊站環境中，透過 Application View 交付安全鎖定的應用程式交付。透過應用程式檢視，WorkSpaces 應用程式會將預設 Windows shell 取代為自訂 shell。此自訂 Shell 僅呈現執行中的應用程式，將作業系統的攻擊面降至最低。

對於使用 WorkSpaces 應用程式來擴增現有組織的桌面環境的使用案例，偏好僅應用程式檢視。允許完整使用鍵盤快速鍵，以原生應用程式模式部署 WorkSpaces 應用程式 Windows 用戶端，將使用者的混淆降到最低。

Amazon WorkSpaces 應用程式用量報告會建立應用程式檢視的每日應用程式報告。如需更精細的應用程式報告和執行使用，請考慮在作業系統層級報告第三方解決方案。您可以在報告模式中使用 Microsoft AppLocker，或考慮 中提供的解決方案 AWS Marketplace，例如 Liquidware 的 Stratusphere UX。

AWS Identity and Access Management 角色組態

如果工作負載需要 WorkSpaces 應用程式最終使用者 AWS 從其工作階段內存取其他服務，最佳實務是透過使用 AWS Identity and Access Management (IAM) 角色委派存取權。IAM 角色可以透過機群層級的指派直接連接到最終使用者的工作階段。如需搭配 WorkSpaces 應用程式使用 IAM 角色的其他最佳實務，請參閱 管理員指南的本節。

使用靜態登入資料

有些工作負載可能需要 IAM 存取金鑰的靜態輸入，而不是從連接的角色繼承它們。有兩種方法可以接收這些登入資料。第一種方法是將存取金鑰存放在 AWS 服務中，然後提供最終使用者明確的 IAM 存取權，以從服務提取該特定值。存取金鑰儲存機制的兩個範例是使用 AWS Secrets Manager或 AWS SSM 參數存放區。第二個方法是使用 WorkSpaces 應用程式登入資料提供者來存取連接角色的存取金鑰。這可以透過叫用登入資料提供者並剖析存取金鑰和私密金鑰的輸出來完成。以下範例說明如何在 PowerShell 中執行此動作。

```
$CMD = 'C:\Program Files\Amazon\Photon\PhotonRoleCredentialProvider
\PhotonRoleCredentialProvider.exe'
$role = 'Machine'

$output = & $CMD --role=$role
$parsed = $output | ConvertFrom-Json

$access_key = $parsed.AccessKeyId
$secret_key = $parsed.SecretAccessKey
$session_token = $parsed.SessionToken
```

保護您的 WorkSpaces 應用程式 S3 儲存貯體

如果您的 WorkSpaces 應用程式工作負載使用主資料夾和/或應用程式持久性設定，則最佳實務是保護存放持久性資料的 Amazon S3 儲存貯體，避免未經授權的存取或意外刪除。第一層保護是新增 Amazon S3 儲存貯體政策，以防止意外刪除儲存貯體。第二層保護是新增符合最低權限原則的儲存貯體政策。僅允許儲存貯體存取必要方，即可與原則保持一致。

機群自動擴展策略

了解 WorkSpaces 應用程式執行個體

WorkSpaces 應用程式機群執行個體具有 1：1 的使用者與機群執行個體比率。這表示每個使用者都有自己的串流執行個體。您同時連線的使用者數量將決定機群的大小。

擴展政策

WorkSpaces 應用程式機群會在 Application Auto Scaling 群組中啟動。這可讓機群根據用量進行擴展，以滿足需求。隨著用量增加，機群會向外擴展，隨著使用者中斷連線，機群會向內擴展。這是透過設定擴展政策來控制。您可以設定排程型擴展、步驟擴展和目標追蹤擴展政策。如需這些擴展政策的詳細資訊，請參閱適用於 Amazon WorkSpaces 應用程式的 Fleet Auto Scaling。

步驟擴展

這些政策會將機群容量增加或減少目前機群大小或特定執行個體數量的百分比。步驟擴展政策是由 WorkSpaces 應用程式 CloudWatch 指標 `Capacity Utilization`、`Available Capacity`或 觸發`Insufficient Capacity Errors`。

使用步驟擴展政策時， AWS 建議您新增容量百分比，而不是固定數量的執行個體。這可確保您的擴展動作與機群的大小成正比。當您的機群很小時，這將有助於避免橫向擴展太慢的情況（因為您相對於機群大小新增了少量執行個體）或太多執行個體。

目標追蹤

使用此政策可指定機群的容量使用率層級。Application Autoscaling 會建立和管理觸發擴展政策的 CloudWatch 警示。這會新增或移除容量，讓機群保持在或接近指定的目標值。為了確保應用程式的可用性，您的機群會盡可能快速地按比例擴展到指標，但會更逐步地擴展。設定目標追蹤時，請考慮擴展冷卻時間，以確保以所需的間隔進行向外擴展和向內擴展。

目標追蹤適用於高流失情況。流失是指大量使用者在短時間內開始或結束工作階段。您可以透過檢查機群的 CloudWatch 指標來識別流失。機群在所需容量沒有變更（或幾乎沒有變更）的情況下有非零待處理容量的期間，表示可能發生高流失。在流失率高的情況下，設定目標追蹤政策，其中 (100 – 目標使用率百分比）在 15 分鐘期間內超過流失率。例如，如果 10% 的機群因使用者周轉而在 15 分鐘內終止，請將容量使用率目標設定為 90% 或更少，以抵銷高流失率。

排程型擴展

這些政策可讓您根據以時間為基礎的排程來設定所需的機群容量。當您了解登入行為時，此政策就會生效，並且可以預測需求的變化。

例如，在工作日開始時，您可能會預期 100 名使用者在上午 9：00 請求串流連線。您可以設定排程型擴展政策，將最小機群大小設定為上午 8：40 的 100。這可讓機群執行個體在工作日開始時建立並變成可用，並允許 100 個使用者同時連線。然後，您可以設定另一個排程政策，在機群中於下午 5：00 擴展至最少十個。這可讓您節省成本，因為下班後工作階段的需求低於工作日。

生產中的擴展政策

您可以選擇在單一機群中結合不同類型的擴展政策，以協助為您的使用者行為定義精確的擴展政策。在上述範例中，您可以將排程擴展政策與目標追蹤或步驟擴展政策結合，以維持特定的使用率層級。排程擴展和目標追蹤擴展的組合有助於在需要立即容量時，減少使用率層級急劇增加的影響。

當擴展政策變更所需執行個體數量時，連線至串流工作階段的使用者不會受到縮減或橫向擴展的影響。擴展政策不會結束現有的串流工作階段。現有的工作階段會持續不中斷，直到使用者結束工作階段或機群逾時政策為止。

使用 CloudWatch 指標監控 WorkSpaces 應用程式用量，可協助您隨著時間最佳化擴展政策。例如，在初始設定期間過度佈建資源很常見，您可能會看到長時間的低使用率。或者，如果機群佈建不足，您可能會看到高容量使用率和「容量不足」錯誤。檢閱 CloudWatch 指標有助於推動擴展政策的調整，以協助緩解這些錯誤。如需詳細資訊，以及您可以使用的 WorkSpaces 應用程式擴展政策範例，請參閱擴展 Amazon WorkSpaces 應用程式機群。

擴展政策設計的最佳實務

合併擴展政策

許多客戶選擇在單一機群中結合不同類型的擴展政策，以提高 WorkSpaces 應用程式中 Auto Scaling 的強大功能和彈性。例如，您可以設定排程的擴展政策，在預期使用者開始工作日的上午 6：00 增加機群最小值，並在使用者停止工作之前於下午 4：00 減少機群最小值。您可以將此排程擴展政策與目標追蹤或步進擴展政策結合，以在一天中維持特定層級的使用率和縮減或縮減，以處理尖峰用量。排程擴展和目標追蹤擴展的組合有助於在需要立即容量時，減少使用率層級急劇增加的影響。

避免擴展流失

考慮您的機群是否會因為使用案例而經歷高度流失。當大量使用者在短時間內開始和結束工作階段時，會發生流失。當許多使用者在簽署前只同時存取機群中的應用程式幾分鐘時，可能會發生這種情況。

在這種情況下，您的機群大小可能會遠低於所需的容量，因為執行個體會在使用者結束其工作階段時結束。步驟擴展政策可能無法快速新增執行個體來抵銷流失，因此您的機群會卡在特定大小。

您可以透過檢查機群的 CloudWatch 指標來識別流失。當您的機群具有非零的待定容量，而所需容量沒有變更（或幾乎沒有變更）時，表示可能發生高流失。為了考量流失率高的情況，請使用目標追蹤擴展政策並挑選目標使用率，讓 (100 – 目標使用率百分比）在 15 分鐘期間內超過流失率。例如，如果 10% 的機群因使用者周轉而在 15 分鐘內結束，請將容量使用率目標設定為 90% 或更少，以抵銷高流失率。

了解最大佈建速率

為大量使用者管理 WorkSpaces 應用程式機群的客戶應考慮佈建速率限制。此限制會影響執行個體新增至機群或跨 內所有機群的速度 AWS 帳戶。

有兩項限制需要考慮：

- 對於單一機群，WorkSpaces 應用程式佈建的最高速率為每分鐘 20 個執行個體。
- 對於單一 WorkSpaces 應用程式 AWS 帳戶，以每分鐘 60 個執行個體的速率佈建（每分鐘爆量 100 個執行個體）。

如果平行擴展超過三個機群，則會在這些機群之間共用帳戶佈建速率限制（例如，平行擴展六個機群，每個機群每分鐘最多可佈建 10 個執行個體）。此外，請考慮特定串流執行個體完成佈建以回應

擴展事件的時間長度。對於未加入 Active Directory 網域的機群，這通常為 15 分鐘。對於加入 Active Directory 網域的機群，這可能需要長達 25 分鐘的時間。

考慮到這些限制條件，請考慮下列範例：

- 如果您想要將單一機群從 0 擴展到 1000 個執行個體，則佈建需要 50 分鐘（每分鐘 1000 個執行個體/20 個執行個體）才能完成，然後，所有執行個體多需要 15-25 分鐘才能供最終使用者使用，總共需要 65-75 分鐘。
- 如果您想要同時將三個機群從 0 擴展到 333 個執行個體（在 中總共 999 個執行個體 AWS 帳戶），所有機群大約需要 17 分鐘（每分鐘 999/60 個執行個體）才能完成佈建，然後又需要 15 分鐘讓這些執行個體可供最終使用者使用，總共需要 32-42 分鐘。

利用多個可用區域

在 區域中為機群部署選擇多個 AZs。當您為機群選取多個可用AZs時，會增加機群能夠新增執行個體以回應擴展事件的可能性。CloudWatch 指標 PendingCapacity 是評估機群 AZ 設計在大型機群部署中最佳化的起點。PendingCapacity 的高持續值可能表示需要擴展水平（跨 AZs) 擴展。如需詳細資訊，請參閱監控 Amazon WorkSpaces 應用程式資源。

例如，如果自動擴展嘗試佈建執行個體以增加機群的大小，且所選 AZ 的容量不足，則自動擴展會改為在您為機群指定的其他 AZs 中新增執行個體。如需可用區域和 WorkSpaces 應用程式設計的詳細資訊，請參閱本文件中的可用區域。

監控容量不足錯誤指標

「容量不足錯誤」是 WorkSpaces 應用程式機群的 CloudWatch 指標。此指標會指定因容量不足而拒絕的工作階段請求數目。

當您變更擴展政策時，建立 CloudWatch 警示，以便在發生任何容量不足錯誤時通知您。這可讓您快速調整擴展政策，以最佳化使用者的可用性。管理指南提供監控 WorkSpaces 應用程式資源的詳細步驟。

連線方法

在 WorkSpaces 應用程式中串流工作階段時，使用者有兩種連線方法可用：

- Web 瀏覽器存取 — 支援任何HTML5-capable瀏覽器。不需要外掛程式或下載。
- WorkSpaces 應用程式 Windows 用戶端

最佳實務是考慮使用者使用案例的功能和裝置需求，以調整最適合支援其需求的瀏覽器或裝置。

> **Note**
>
> 螢幕解析度小於 1024 x 768 像素的裝置不支援 WorkSpaces 應用程式。

摘要功能和裝置支援

表 3 — 摘要功能和裝置支援

	Web 瀏覽器存取	WorkSpaces 應用程式 Windows 用戶端
多監視器（最高 2k 解析度）	支援	支援
多監視器（最高 4k 解析度）	N/A	支援
繪製平板電腦支援	支援*	支援
觸控螢幕裝置支援	支援	N/A
USB 傳遞裝置支援	N/A	支援
鍵盤快速鍵	支援	支援
相對滑鼠位移	支援	支援
檔案傳輸	支援	支援
本機印表機重新導向	N/A	支援

	Web 瀏覽器存取	WorkSpaces 應用程式 Windows 用戶端
本機磁碟機重新導向	N/A	支援
網路攝影機支援	支援	支援

*僅限 Google Chrome 和 Mozilla Firefox

Web 瀏覽器存取

WorkSpaces 應用程式 Web 瀏覽器存取允許存取應用程式，而不需要安裝專用用戶端。使用者可以使用支援的支援 HTML5-capable瀏覽器進行連線。不需要任何瀏覽器外掛程式或擴充功能。

Web 瀏覽器存取提供廣泛的終端裝置作業系統和類型選擇。

適用於 Windows 的 WorkSpaces 應用程式用戶端

適用於 Windows 的 WorkSpaces 應用程式用戶端是您安裝在 Windows PC 上的應用程式。 當您使用 Web 瀏覽器存取 WorkSpaces 應用程式時，此應用程式提供無法使用的其他功能。例如，WorkSpaces 應用程式用戶端可讓您執行下列動作：

- 使用兩個以上的監視器或 4K 解析度
- 將 USB 裝置與透過 WorkSpaces 應用程式串流的應用程式搭配使用
- 在串流工作階段期間存取本機磁碟機和資料夾
- 將列印任務從串流應用程式重新導向至連線至本機電腦的印表機
- 在串流工作階段中使用本機網路攝影機進行視訊和音訊會議
- 在串流工作階段期間存取的應用程式中使用鍵盤快速鍵
- 與遠端串流應用程式互動的方式與與與本機安裝的應用程式互動的方式大致相同

WorkSpaces 應用程式用戶端連線模式

WorkSpaces 應用程式用戶端提供兩種連線模式：原生應用程式模式和傳統模式。您選擇的連線模式會決定您在應用程式串流期間可以使用的選項，以及串流應用程式的運作和顯示方式。管理員可以控制使用者在原生應用程式模式和傳統模式之間切換的能力。

- 傳統模式會在 WorkSpaces 應用程式工作階段視窗中串流應用程式。這類似於最終使用者在 Web 瀏覽器中串流應用程式的方式。如果最終使用者偏好以與瀏覽器相同的方式串流應用程式，同時使用其他功能，例如本機檔案和印表機重新導向的連線。Classic 模式是建議的預設連線模式。Classic 模式是桌面檢視唯一支援的模式。
- 原生應用程式模式可讓最終使用者以類似其他本機安裝應用程式的方式使用遠端串流應用程式。如果最終使用者用於處理本機安裝的應用程式，原生應用程式模式可提供無縫的體驗。遠端串流應用程式的運作方式與本機安裝的應用程式大致相同。應用程式圖示會顯示在本機 PC 的工作列，就像本機應用程式的圖示一樣。與本機應用程式的圖示不同，原生應用程式模式下串流應用程式的圖示包含 WorkSpaces 應用程式標誌。當使用者想要使用應用程式鍵盤快速鍵，並使用鍵盤快速鍵在個別本機和個別遠端應用程式之間輕鬆切換時，原生應用程式模式是建議的連線模式。

用戶端部署和管理

使用者可以自行安裝 WorkSpaces 應用程式用戶端，或者管理員可以透過遠端執行 PowerShell 指令碼，或使用自訂設定重新封裝 WorkSpaces 應用程式用戶端， WorkSpaces 來為其安裝 WorkSpaces 應用程式用戶端。

您必須符合您要讓使用者與串流工作階段搭配使用的 USB 裝置資格。如果其 USB 裝置不符合資格，WorkSpaces 應用程式將無法偵測到，也無法與工作階段共用。合格裝置之後，您的使用者每次啟動新的串流工作階段時，都必須與 WorkSpaces 應用程式共用裝置。

大規模部署 WorkSpaces 應用程式用戶端時， AWS 建議使用企業部署工具。企業部署工具包含 WorkSpaces 應用程式用戶端安裝檔案和群組政策管理範本。

自訂網域

以程式設計方式部署 WorkSpaces 應用程式時，可以建立自訂網域，為使用者提供熟悉的串流工作階段體驗。在 WorkSpaces 應用程式的 SAML 2.0 IdP 部署中，請務必強調使用者存取從 IdP 開始，而不是 WorkSpaces 應用程式。使用者不需要 WorkSpaces 應用程式 URLs，因為這些 URL 會在身分驗證後由 IdP 提供。因此，SAML 2.0 IdP 部署不需要自訂網域名稱。

身分驗證

使用 WorkSpaces 應用程式時，身分驗證可以在 Amazon WorkSpaces 應用程式之外進行，或做為 WorkSpaces 應用程式服務的一部分進行。選擇對 WorkSpaces 應用程式部署進行身分驗證的方式，是設計的基本考量。組織針對不同的使用案例進行多個 WorkSpaces 應用程式部署並不常見。每個使用案例可以有不同的身分驗證方法。

WorkSpaces 應用程式的身分驗證方法有三種類型：

- SAML 2.0
- 使用者集區
- 程式設計

判斷最佳化方法

Amazon WorkSpaces 應用程式架構靈活，適用於大多數的組織設計需求。判斷最佳化的身分驗證方法時，最佳實務是考慮使用服務的使用者的目標和目的，以及組織政策和程序。

以下是結合使用案例與組織目標的一些範例。

表 4 — 具有組織目標的使用案例

範例	Description	身分驗證
需要加入網域的機群執行個體	安裝在 WorkSpaces 應用程式映像上的應用程式只能存取加入網域的資源。	SAML 2.0
與 Microsoft 服務高度整合	對開發 Microsoft 群組政策和後端基礎設施的組織依賴性	SAML 2.0
現有企業單一登入 (SSO)	所有新服務都必須利用已建立數個報告和安全程序的企業 SSO 解決方案。	SAML 2.0
應用程式的智慧卡支援	智慧卡（例如私有身分驗證和通用存取卡），用於透過智慧	SAML 2.0

範例	Description	身分驗證
	卡讀取器串流應用程式進行工作階段內身分驗證。	
具有臨時人員配置的季節性人力	在一年中的幾個月內，臨時工作者會被指派一組不包含內部資源以完成活動的小型應用程式。	使用者集區
有限的 IT 支援	擁有少於 50 個使用者和有限 IT 人員的小型組織，希望消除維護身分提供者 (IdP) 的額外負荷	使用者集區
獨立軟體廠商 (ISV)	由您的組織建置的專屬解決方案，其中包含使用者權利和身分驗證，將 WorkSpaces 應用程式延伸為解決方案的一部分。*	程式設計
技術展示	完全暫時性的環境，展示專屬技術做為 解決方案導覽的一部分，無需儲存使用者資訊。	程式設計
互動式網站體驗	讓您的網站與串流 Windows 應用程式互動。**	程式設計

*請參閱軟體廠商：將您的應用程式交付至任何使用者裝置，以取得詳細資訊。

**如需詳細資訊，請參閱內嵌 WorkSpaces 應用程式串流工作階段。

如果您的組織具有未列在先前提供範例中的使用案例或政策，最佳實務是預測 WorkSpaces 應用程式工作流程耗用量的所需結束狀態，以確保身分驗證解決方案不會與其衝突。

設定您的身分提供者

SAML 2.0

安全聲明標記語言 (SAML) 2.0 是常見的部署選項，可讓使用者使用 AWS 資源。各種第三方 SAML 2.0 身分提供者支援 WorkSpaces 應用程式 。無論您的 WorkSpaces 應用程式資源是否加入網域，SAML 2.0 IdP 都需要您使用 IAM。

由於大多數 IdPs會為每個 SAML 應用程式產生具有特定 SAML 屬性的唯一中繼資料.xml，因此每個 WorkSpaces 應用程式堆疊都需要與 SAML IdP 具有信任關係的角色，以及具有單一許可以 appstream：Stream 的條件符合 SAML IdP 和 WorkSpaces 應用程式堆疊的 ARN。

WorkSpaces 應用程式管理指南提供單一 WorkSpaces 應用程式堆疊設計的範例組態。對於多個堆疊部署，請參閱使用 SAML 2.0 多堆疊應用程式目錄的選用步驟。

使用者集區

WorkSpaces 應用程式中的使用者集區索引標籤是小型概念驗證的有效選項。最佳實務是避免使用者集區用於使用 WorkSpaces 應用程式交付生產應用程式的任何使用案例和組織。

使用者集區需要注意的一個重要事項是，使用者的電子郵件地址區分大小寫；因此最佳實務是確保使用者了解如何正確輸入使用者登入資料。

串流 URL

對於從集中式服務 （ 通常是 ISVs) 呼叫 WorkSpaces 應用程式資源的部署，程式設計身分驗證依賴應用程式對 進行程式設計呼叫 AWS ，以動態傳遞資訊並為使用者建立 WorkSpaces 應用程式工作階段。使用 CreateStreamingURL 操作建立串流 URLs 時，請使用 API 身分驗證方法 （ 通常稱為「程式設計」)。進行`CreateStreamingURL`呼叫的使用者必須使用具有 許可的有效使用者或角色`appstream:CreateStreamingURL`。

建立程式設計存取的政策時，最佳實務是透過在資源區段中指定確切的 WorkSpaces 應用程式堆疊 ARN 來保護存取，而不是預設的「*」。例如：

Example

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appstream:createStreamingURL"
            ],
            "Resource": "arn:aws:appstream:us-east-1:031421429609:stack/
BestPracticesStack"
        }
    ]
}
```

> **Note**
>
> 您可以使用描述堆疊 API 或 AWS CLI，快速擷取 WorkSpaces 應用程式堆疊的 ARNs。https://awscli.amazonaws.com/v2/documentation/api/latest/reference/appstream/describe-stacks.html

WorkSpaces 應用程式執行個體應以一般執行個體開始。透過從應用程式傳遞給該應用程式的資訊，WorkSpaces 應用程式執行個體會使用工作階段內容來建立環境，讓使用者的實物變得動態。

雖然本機 GPOs可用來在使用者登入時指定設定，但工作階段內容是使用 時最佳實務`CreateStreamingURL`，並傳遞要在 WorkSpaces 應用程式工作階段中使用的金鑰屬性，例如客戶 ID 或資料庫連線設定。

應用程式權利

WorkSpaces 應用程式可以動態建置提供給使用者的應用程式目錄。應用程式權利是根據 SAML 2.0 屬性，或使用 WorkSpaces 應用程式動態應用程式架構。

在大多數情況下，建議使用 SAML 2.0 的屬性型應用程式權利。若要管理應用程式套件交付，建議使用動態應用程式架構。

與 Microsoft Active Directory 整合

Amazon WorkSpaces 應用程式映像建置器和機群可與 Microsoft Active Directory 整合。這可讓您為使用者身分驗證、授權提供集中式方法，並將 Active Directory 群組政策套用至加入網域的 WorkSpaces 應用程式執行個體。使用加入網域的 WorkSpaces 應用程式機群，可提供與內部部署環境相同的管理優勢。這包括集中管理網路檔案共享、使用者應用程式權利、漫遊設定檔、印表機存取和其他以政策為基礎的設定。

將 WorkSpaces 應用程式環境與 Active Directory 整合時，請務必注意WorkSpaces 應用程式堆疊的初始身分驗證仍由 SAML2.0 IdP 管理。在使用者成功驗證 IdP 之後，當使用者啟動工作階段時，他們必須輸入其網域密碼或 Active Directory 網域的智慧卡身分驗證。

設計將與 WorkSpaces 應用程式搭配使用的 Active Directory Domain Services (ADDS) 環境時，有兩種服務選項和許多部署案例可供使用。此外，請確定已與您的 Active Directory 網站拓撲擁有者一起檢閱 WorkSpaces 應用程式聯網。

服務選項

Active Directory 也可以使用 AWS Managed Microsoft Active Directory (AD) 部署。 AWS Managed Microsoft AD 是一種全受管服務，可讓您執行 Microsoft Active Directory。Microsoft Active Directory 也可以在 EC2 或內部部署上執行的自我託管環境中使用。

部署案例

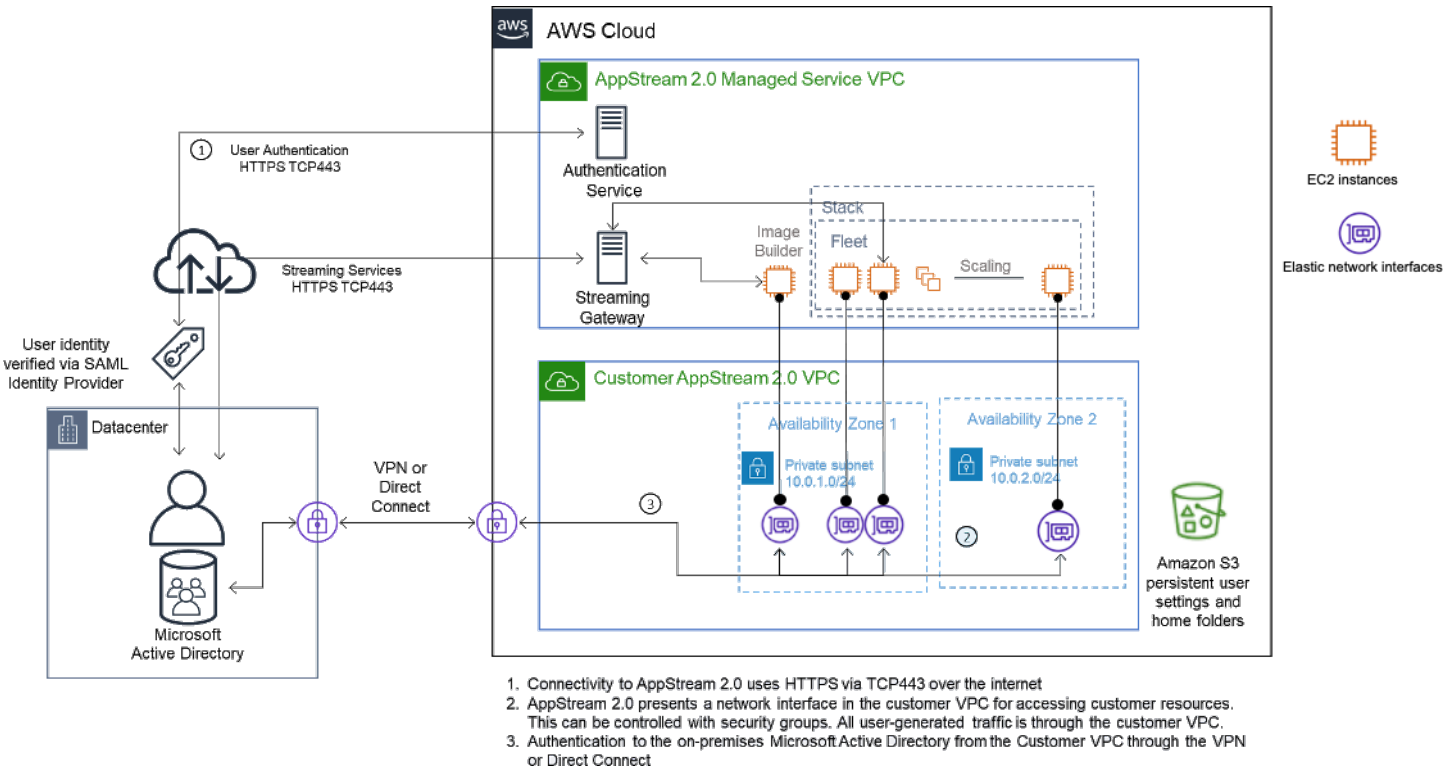
下列部署案例是 WorkSpaces 應用程式與 Microsoft Managed AD 或客戶自我管理 Active Directory 的常用和建議整合選項。以下列出的所有架構圖都使用核心 Amazon 建構。

- Amazon Virtual Private Cloud (VPC) — 建立專用於 WorkSpaces 應用程式服務的 Amazon VPC，其中至少有四個私有子網路分散在四個AZs。兩個私有子網路用於 WorkSpaces 應用程式機群和映像建置器。其餘兩個子網路用於 EC2 或 Microsoft Managed AD 上的網域控制站）。
- 動態主機組態協定 (DHCP) 選項集 — 提供將組態資訊傳遞至 WorkSpaces 應用程式機群和映像建置器的標準，該機群將在 VPC 中佈建。DHCP 選項集是在 VPC 層級定義。它可讓客戶定義指定的網域名稱和 DNS 設定，這些設定將與佈建時所執行個體的 WorkSpaces 應用程式搭配使用。
- AWS Directory Services — Amazon Microsoft Managed AD 可以部署到兩個私有子網路中，這些子網路將與 WorkSpaces 應用程式工作負載搭配使用。
- WorkSpaces 應用程式機群 — WorkSpaces 應用程式機群或映像建置器託管在 AWS 受管 VPC 中。每個 WorkSpaces 應用程式執行個體都有兩個彈性網路界面 (ENI)。主要界面 (`eth0`) 用於管理目

的，並透過串流閘道代理最終使用者與執行個體的連線。次要界面 (eth1) 會注入到客戶 VPC 中，可用於存取自訂 VPC 或內部部署中的其他資源。

案例 1：現場部署的 Active Directory Domain Services (ADDS)

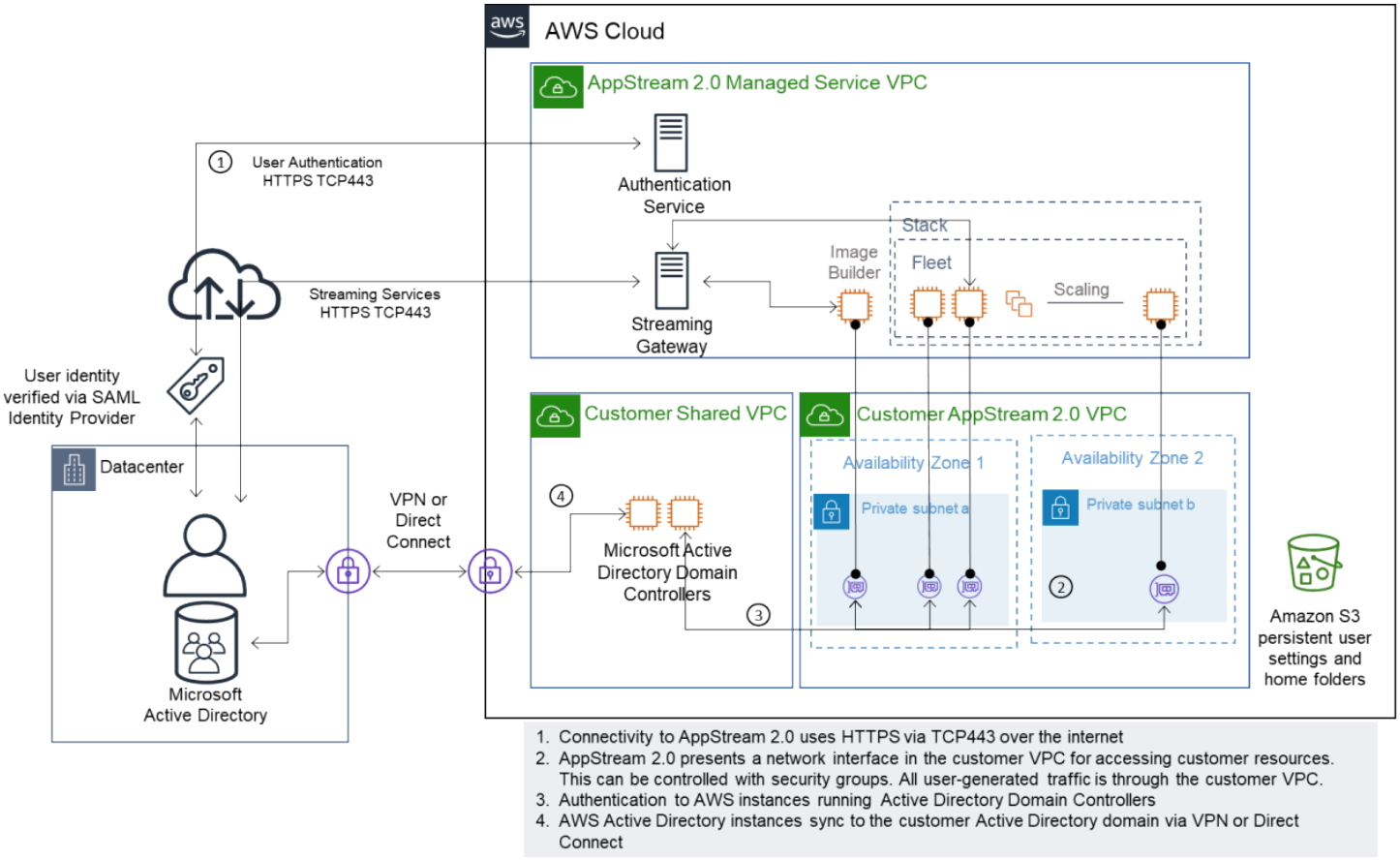
所有身分驗證流量都會周遊從客戶 VPC 到客戶閘道的 VPN 或 Direct Connect 連線。此案例的優點是使用可能已部署的 AD 環境，而無需在客戶 VPC 中佈建額外的網域控制站。缺點是依賴 VPN 或 Direct Connect 來驗證和授權 WorkSpaces 應用程式機群的使用者。如果有任何網路連線問題，WorkSpaces 應用程式機群或映像建置器會直接受到影響。提供具有不同路徑的雙 VPN 通道或 Direct Connect 連線可降低此潛在風險。



案例 1：現場部署的 Active Directory Domain Services (ADDS)

案例 2：將作用中網域服務 (ADDS) 擴展到 AWS 客戶 VPC

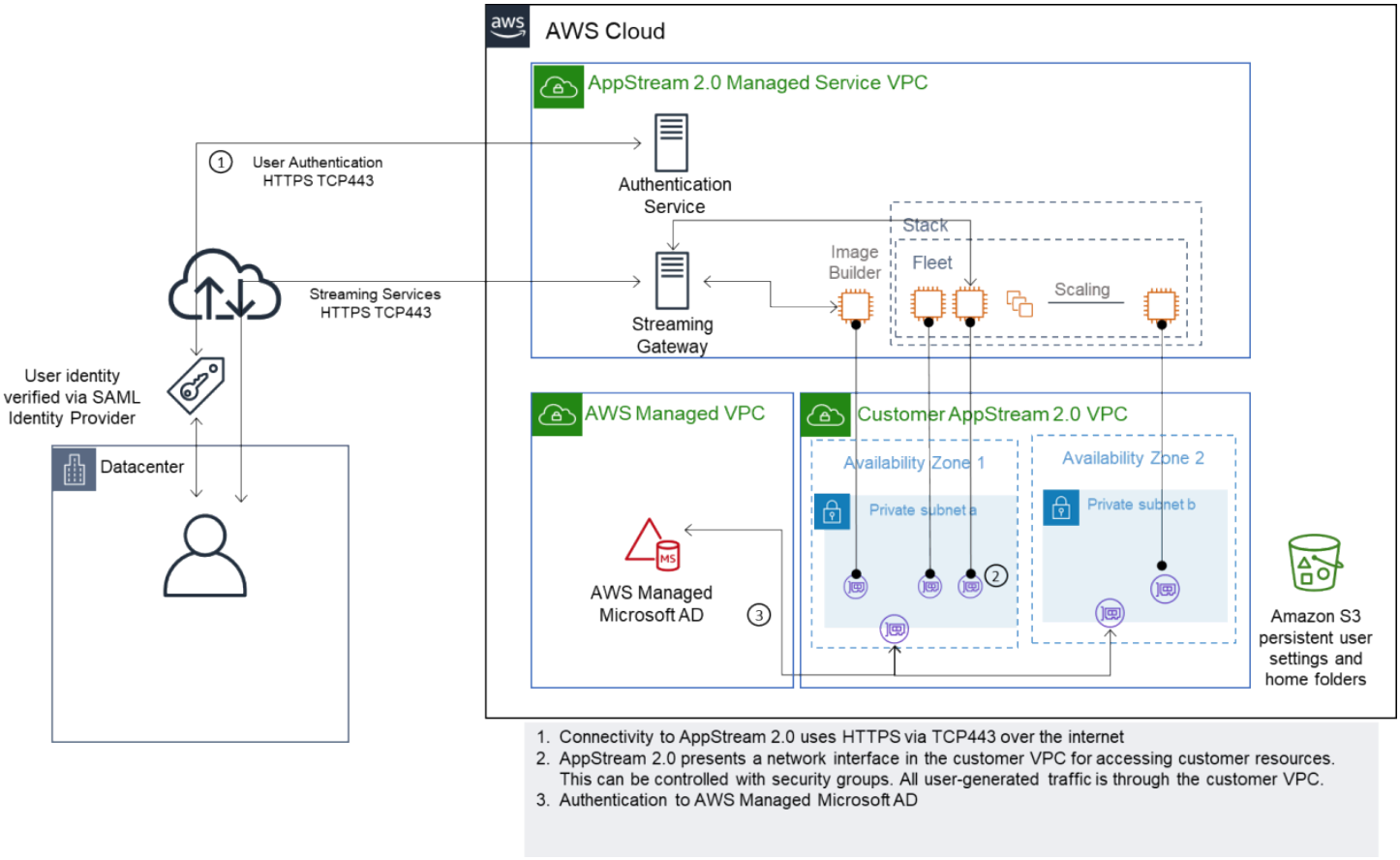
Active Directory 會擴展至您的客戶 VPC。應為客戶 VPC 中的新網域控制站建立 Active Directory 網站。身分驗證流量會路由到 AWS 客戶 VPC 中的網域控制站，而不是周遊 VPN 或 Direct Connect 連線。



案例 2 — 將作用中網域服務擴展到 AWS 客戶虛擬私有雲端

案例 3： AWS 受管 Microsoft Active Directory

AWS Managed Microsoft AD 部署在 中， AWS 雲端 並用作 WorkSpaces 應用程式機群和映像建置器的身分和資源網域。



案例 3 — 受 AWS 管 Active Directory

Active Directory 服務網站拓撲

Active Directory 服務網站拓撲是實體網路的邏輯表示法。

網站拓撲可協助您有效率地路由用戶端查詢和 Active Directory 複寫流量。設計完善且維護良好的網站拓撲可協助您的組織實現下列優點：

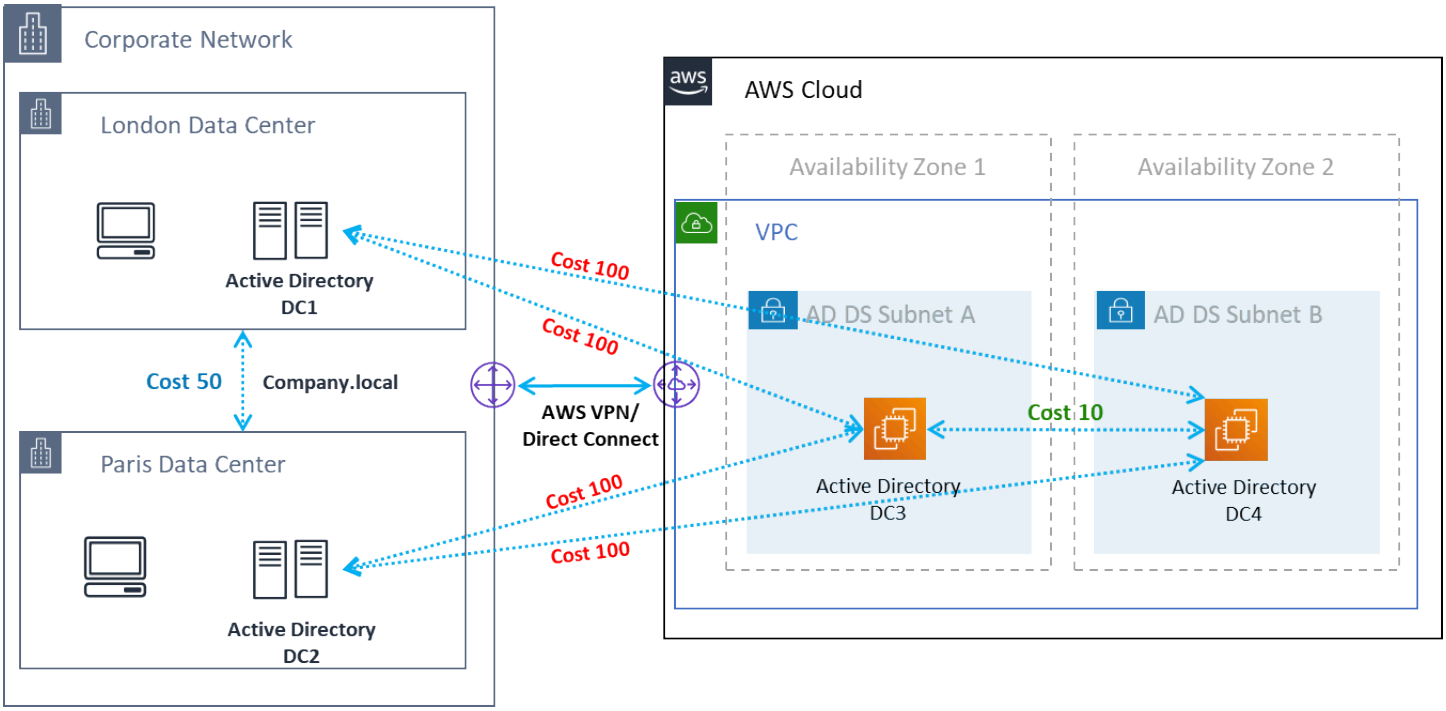
- 在內部部署和 之間同步時，將複寫 Active Directory 資料的成本降至最低 AWS 雲端。
- 最佳化用戶端電腦尋找最近資源的能力，例如網域控制站。這有助於透過慢速廣域網路 (WAN) 連結減少網路流量、改善登入和登出程序，以及加速資源存取操作。

介紹 WorkSpaces 應用程式服務時，請確定用於 WorkSpaces 應用程式執行個體子網路的地址範圍已指派給您環境的正確網站。

對於案例 1 和案例 2，網站和服務是在登入時間和 Active Directory 資源存取時間方面獲得最佳使用者體驗的關鍵元件。

站點拓撲負責控制同一站點內及跨站點邊界的網域控制站之間的 Active Directory 複寫。

定義正確的網站拓撲可確保用戶端親和性，這表示用戶端 （ 在此情況下為 WorkSpaces 應用程式串流執行個體 ） 使用其偏好的本機網域控制站。



Active Directory 網站和服務 — 用戶端親和性

> **Tip**
>
> 最佳實務是為內部部署 AD DS 和 AWS 雲端之間的網站連結定義高成本。上圖是您應該指派給網站連結的成本範例 （ 成本 100)，以確保與網站無關的用戶端親和性。

如需網站拓撲的詳細資訊，請參閱設計網站拓撲。

Active Directory 組織單位

AWS 建議將組織單位 (OUs) 儲存在單一 WorkSpaces 應用程式目錄 Config 物件中設定。每個 WorkSpaces 應用程式堆疊都有自己的 OU 是最佳實務。這可讓您靈活地擁有每個堆疊的特定 GPOs。確保 OUs專用於 WorkSpaces 應用程式電腦物件，以避免將 WorkSpaces 應用程式特定的政策與內部部署桌面混合。請考慮為您 AWS 區域 部署 WorkSpaces 應用程式的每個 使用 sub-OUs。

Active Directory 電腦物件清除

WorkSpaces 應用程式執行個體是暫時性的。隨著機群向外擴展和向內擴展，機群會建立和重複使用 Active Directory 電腦物件。

AWS 建議建立 AD 清除程序，以刪除移除 WorkSpaces 應用程式機群後可能存在的過時 Active Directory 電腦物件。

安全

雲端安全是 Amazon Web Services (AWS) 最重視的一環。安全與合規是 AWS 和 客戶之間的共同責任。如需詳細資訊，請參閱 共同責任模型。身為 AWS 和 WorkSpaces 應用程式客戶，在堆疊、機群、映像和聯網等不同層上實作安全措施非常重要。

由於 WorkSpaces 應用程式具有暫時性性質，因此通常偏好 WorkSpaces 應用程式做為應用程式和桌面交付的安全解決方案。考慮 Windows 部署中常見的防毒解決方案是否與使用者工作階段結束時預先定義和清除的環境的使用案例相關。防毒為虛擬化執行個體增加額外負荷，因此這是減輕不必要的活動的最佳實務。例如，在開機時掃描系統磁碟區 （ 暫時性 ） 並不會增加 WorkSpaces 應用程式的整體安全性。

安全 WorkSpaces 應用程式的兩個關鍵問題以 為中心：

- 保留工作階段以外的使用者狀態是否為必要？
- 使用者在工作階段中應擁有多少存取權？

保護持久性資料

WorkSpaces 應用程式的部署可能需要以某種形式保留使用者狀態。這可能是為個別使用者保留資料，或使用共用資料夾保留資料以進行協同合作。WorkSpaces 應用程式執行個體儲存體是暫時性的，沒有加密選項。

WorkSpaces 應用程式透過 Amazon S3 中的主資料夾和應用程式設定提供使用者狀態持續性。有些使用案例需要更妥善地控制使用者狀態持久性。對於這些使用案例， AWS 建議使用伺服器訊息區塊 (SMB) 檔案共用。

使用者狀態和資料

由於大多數 Windows 應用程式在與使用者建立的應用程式資料共置時執行最佳且最安全，因此最佳實務是將此資料保留在與 WorkSpaces 應用程式機群 AWS 區域 相同的 中。加密此資料是最佳實務。使用者主資料夾的預設行為是使用來自金鑰 AWS 管理服務 () 的 Amazon S3-managed加密金鑰來加密靜態檔案和資料夾AWS KMS。請務必注意，具有 AWS 主控台或 Amazon S3 儲存貯體存取權的 AWS 管理使用者將能夠直接存取這些檔案。

在需要來自 Windows 檔案共享的伺服器訊息區塊 (SMB) 目標來存放使用者檔案和資料夾的設計中，程序為自動或需要組態。

表 5 — 保護使用者資料的選項

SMB 目標	Encryption-at-rest	Encryption-in-transit	防毒 (AV)
FSx for Windows File Server	透過 AWS KMS 自動執行	透過 SMB 加密自動執行	安裝在遠端執行個體上的 AV 會在映射的磁碟機上執行掃描
檔案閘道、 AWS Storage Gateway	根據預設，存放在 S3 AWS Storage Gateway 中的所有資料都會使用 Amazon S3-Managed管加密金鑰 (SSE-S3) 加密伺服器端。您可以選擇性地設定不同的閘道類型，以使用 AWS Key Management Service (KMS) 加密儲存的資料	在任何類型的閘道設備與 AWS 儲存體之間傳輸的所有資料都會使用 SSL 加密。	安裝在遠端執行個體上的 AV 會在映射的磁碟機上執行掃描
EC2-based Windows 檔案伺服器	啟用 EBS 加密	PowerShell； `Set- SmbServer Configuration - EncryptData $True`	安裝在伺服器上的 AV 會在本機磁碟機上執行掃描

端點安全與防毒

Amazon WorkSpaces 應用程式執行個體的短暫性本質和資料的持久性不足表示需要不同的方法，以確保使用者體驗和效能不會因持久性桌面上所需的活動而受到影響。端點安全代理程式會在有組織政策或與外部資料輸入搭配使用時，安裝在 WorkSpaces 應用程式映像中，例如電子郵件、檔案傳入、外部 Web 瀏覽。

移除唯一識別符

Endpoint Security 代理程式可能有全域唯一識別符 (GUID)，必須在機群執行個體建立程序期間重設。供應商在映像中安裝其產品的指示，將確保為每個從映像產生的執行個體產生新的 GUID。

為了確保不會產生 GUID，請先安裝端點安全代理程式做為最後一個動作，再執行 WorkSpaces 應用程式助理來產生映像。

效能最佳化

端點安全廠商提供最佳化 WorkSpaces 應用程式效能的切換和設定。設定因廠商而異，可以在其文件中找到，通常是在 VDI 的 區段中。某些常見的設定包括但不限於：

- 關閉開機掃描，以確保執行個體建立、啟動和登入時間降到最低
- 關閉排程掃描以防止不必要的掃描
- 關閉簽章快取以防止檔案列舉
- 啟用 VDI 最佳化 IO 設定
- 應用程式確保效能所需的排除項目

端點安全廠商提供與虛擬桌面環境搭配使用的指示，以最佳化效能。

- 適用於虛擬桌面基礎設施的 Trend Micro Office Scan Support - Apex One/OfficeScan (trendmicro.com：//)
- CrowdStrike 和如何在資料中心安裝 CrowdStrike Falcon
- Sophos 和 Sophos Central Endpoint：如何在黃金映像上安裝 ，以避免重複的身分和 Sophos Central：在虛擬桌面環境中安裝 Windows 端點時的最佳實務
- 在虛擬桌面基礎設施系統上佈建和部署 McAfee 和 McAfee 代理程式 McAfee
- Microsoft Endpoint Security 和為非持久性 VDI 機器設定 Microsoft Defender 防毒 - Microsoft Tech Community

掃描排除項目

如果安全軟體安裝在 WorkSpaces 應用程式執行個體中，則安全軟體不得干擾下列程序。

表 6 — WorkSpaces 應用程式處理安全軟體時，不得干擾下列程序。

服務	Processes
AmazonCloudWatchAgent	「C：\Program Files\Amazon\AmazonCloudWatchAgent\start-amazon- cloudwatch-agent.exe」

服務	Processes
AmazonSSMAgent	「C：\Program Files\Amazon\SSM\amazon-ssm-agent.exe」
NICE DCV	"C：\Program Files\NICE\DCV\Server\bin\dcvserver.exe" "C：\Program Files\NICE\DCV\Server\bin\dcvagent.exe"
WorkSpaces 應用程式	「C：\ProgramFiles\Amazon\AppStream2\StorageConnector\StorageConnector.exe" 在資料夾 "C：\Program Files\Amazon\Photon\" 中 "。\Agent\PhotonAgent.exe" "。\Agent\s5cmd.exe" "。\WebServer\PhotonAgentWebServer.exe" "。\CustomShell\PhotonWindowsAppSwitcher.exe" "。\CustomShell\PhotonWindowsCustomShell.exe" "。\CustomShell\PhotonWindowsCustomShellBackground.exe"

資料夾

如果安全軟體安裝在 WorkSpaces 應用程式執行個體中，則軟體不得干擾下列資料夾：

Example

```
C:\Program Files\Amazon\*
C:\ProgramData\Amazon\*
C:\Program Files (x86)\AWS Tools\*
```

```
C:\Program Files (x86)\AWS SDK for .NET\*
C:\Program Files\NICE\*
C:\ProgramData\NICE\*
C:\AppStream\*
C:\Program Files\Internet Explorer\*
C:\Program Files\nodejs\
```

端點安全主控台衛生

每次使用者連線超過閒置和中斷連線逾時時，Amazon WorkSpaces 應用程式都會建立新的唯一執行個體。執行個體會有唯一的名稱，並會在端點安全管理 condoles 中建置。將超過 4 天或更長時間（或更短時間，視 WorkSpaces 應用程式工作階段逾時而定）的未使用過時機器設定為刪除，可將主控台中過期的執行個體數量降至最低。

網路排除

WorkSpaces 應用程式管理網路範圍 (198.19.0.0/16) 和下列連接埠和地址不應被 WorkSpaces 應用程式執行個體內的任何安全/防火牆或防毒解決方案封鎖。

表 7 — WorkSpaces 應用程式串流執行個體安全軟體中的連接埠不得干擾

連接埠	用途
8300、3128	這用於建立串流連線
8000	這用於管理 WorkSpaces 應用程式串流執行個體
8443	這用於管理 WorkSpaces 應用程式串流執行個體
53	DNS

表 8 — WorkSpaces 應用程式受管服務地址安全軟體不得干擾

連接埠	用途
169.254.169.123	NTP
169.254.169.249	NVIDIA GRID 授權服務
169.254.169.250	KMS
169.254.169.251	KMS
169.254.169.253	DNS
169.254.169.254	中繼資料

保護 WorkSpaces 應用程式工作階段

限制應用程式和作業系統控制

WorkSpaces 應用程式可讓管理員指定可在應用程式串流模式下從網頁啟動哪些應用程式。不過，這並不保證只有指定的應用程式才能執行。

Windows 公用程式和應用程式可透過其他方法透過作業系統啟動。 AWS 建議使用 Microsoft AppLocker 以確保只有您組織所需的應用程式才能執行。預設規則必須修改，因為它們會授予每個人關鍵系統目錄的路徑存取權。

> **Note**
>
> Windows Server 2016 和 2019 需要執行 Windows Application Identity 服務，才能強制執行 AppLocker 規則。使用 Microsoft AppLocker 從 WorkSpaces 應用程式存取應用程式的詳細資訊，請參閱 WorkSpaces 應用程式管理員指南。

對於加入 Active Directory 網域的機群執行個體，請使用群組政策物件 (GPOs) 提供使用者和系統設定，以保護使用者應用程式和資源存取。

防火牆和路由

建立 WorkSpaces 應用程式機群時，必須指派子網路和安全群組。子網路具有網路存取控制清單 (NACLs) 和路由表 (NACL) 的現有指派。您可以在啟動新的映像建置器時關聯最多五個安全群組，或在

建立新的機群安全群組時，最多可以從現有的安全群組進行五個指派。對於每個安全群組，您可以新增規則來控制來自和傳入執行個體的傳出和傳入網路流量

NACL 是 VPC 的選用安全層，可做為無狀態防火牆來控制傳入和傳出一或多個子網路的流量。您可以使用與您的安全群組相似的規則來設定網路 ACL，以為您的 VPC 新增額外的安全 layer。如需安全群組和網路 ACLs 之間差異的詳細資訊，請參閱比較安全群組和 NACLs頁面。

設計和套用安全群組和 NACL 規則時，請考慮 AWS Well-Architected 最佳實務的最低權限。最低權限是僅授予完成任務所需許可的原則。

對於具有高速私有網路將內部部署環境連線至 AWS （透過 AWS Direct Connect) 的客戶，您可以考慮使用適用於 WorkSpaces 應用程式的 VPC 端點，這表示串流流量將透過私有網路連線路由，而不是透過公有網際網路。如需本主題的詳細資訊，請參閱本文件的 WorkSpaces 應用程式串流介面 VPC 端點一節。

資料外洩防護

我們將探討兩種類型的資料遺失預防。

用戶端對 WorkSpaces 應用程式執行個體資料傳輸控制

表 9 — 控制資料輸入和輸出的指引

設定	選項	指引
剪貼簿	• 僅複製並貼到遠端工作階段 • 僅複製到本機裝置 • Disabled	停用此設定不會停用工作階段中的複製和貼上。如果需要將資料複製到工作階段，請選擇僅貼到遠端工作階段，以將資料外洩的可能性降至最低。
檔案傳輸	• 上傳和下載 • 僅上傳 • 僅下載 • Disabled	避免啟用此設定以防止資料外洩。
列印至本機裝置	• 已啟用 • Disabled	如果需要列印，請使用由組織控制和監控的網路映射印表機。

考慮現有組織資料傳輸解決方案相較於堆疊設定的優點。這些組態並非設計用來取代全方位的安全資料傳輸解決方案。

控制來自 WorkSpaces 應用程式執行個體的輸出流量

當資料遺失是問題時，請務必涵蓋使用者在 WorkSpaces 應用程式執行個體內時可存取的內容。網路結束（或輸出）路徑是什麼樣子？一般要求使用者在其 WorkSpaces 應用程式執行個體內擁有公有網際網路存取，因此需要考慮在網路路徑中放置 WebProxy 或內容篩選解決方案。其他考量包括本機防毒應用程式和 WorkSpaces 應用程式執行個體內的其他端點安全措施（如需詳細資訊，請參閱「端點安全和防毒」一節）。

使用 AWS 服務

AWS Identity and Access Management

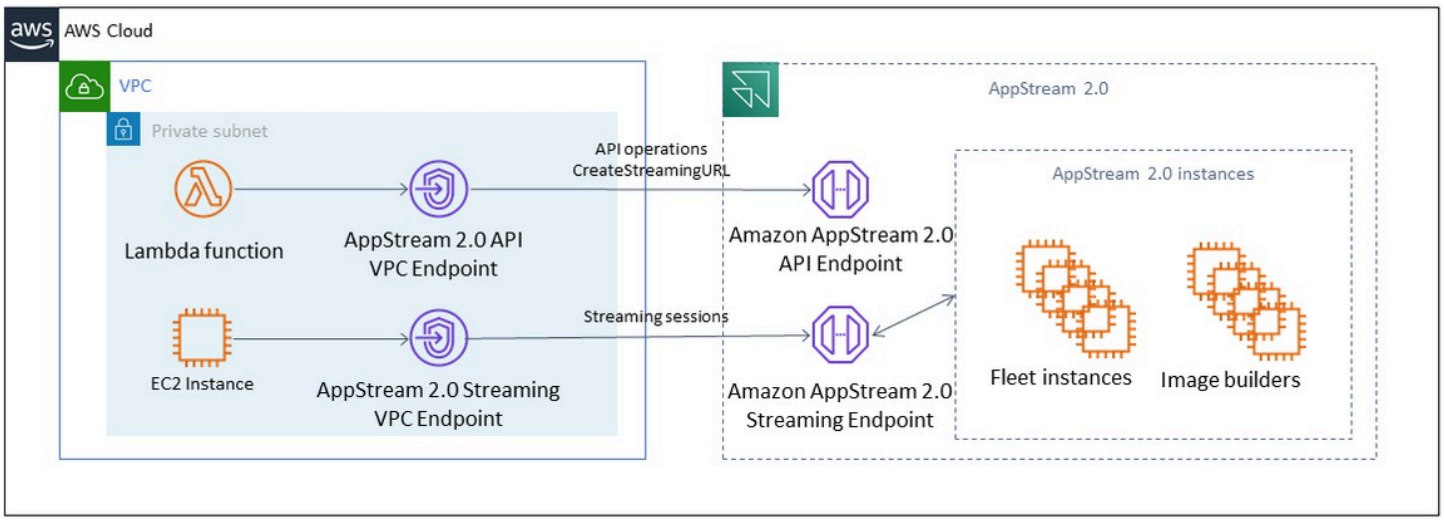
使用 IAM 角色來存取 AWS 服務，並在連接到服務的 IAM 政策中具有特定性，這是最佳實務，只提供 WorkSpaces 應用程式工作階段中的使用者存取，而無需管理其他登入資料。遵循將 IAM 角色與 WorkSpaces 應用程式搭配使用的最佳實務。

建立 IAM 政策以保護為將使用者資料保留在主資料夾和應用程式設定持續性而建立的 Amazon S3 儲存貯體。這可防止非 WorkSpaces 應用程式管理員存取。

VPC 端點

VPC 端點可讓您的 VPC 與支援的 AWS 服務，以及採用 技術的 VPC 端點服務之間的私有連線 AWS PrivateLink。 AWS PrivateLink 是一種技術，可讓您使用私有 IP 地址來私有存取服務。VPC 與另一個服務之間的流量都會保持在 Amazon 網路的範圍內。如果只有 AWS 服務需要公有網際網路存取，VPC 端點會完全移除對 NAT 閘道和網際網路閘道的需求。

在自動化常式或開發人員需要對 WorkSpaces 應用程式進行 API 呼叫的環境中，為 WorkSpaces 應用程式 API 操作建立介面 VPC 端點。例如，如果私有子網路中有 EC2 執行個體沒有公有網際網路存取，則 WorkSpaces 應用程式 API 的 VPC 端點可用來呼叫 WorkSpaces 應用程式 API 操作，例如 CreateStreamingURL。下圖顯示範例設定，其中 Lambda 函數和 EC2 執行個體會耗用 WorkSpaces 應用程式 API 和串流 VPC 端點。



VPC 端點

串流 VPC 端點可讓您透過 VPC 端點串流工作階段。此串流界面端點可將串流流量保持在 VPC 內。串流流量包含像素、USB、使用者輸入、音訊、剪貼簿、檔案上傳和下載，以及印表機流量。若要使用 VPC 端點，必須在 WorkSpaces 應用程式堆疊中啟用 VPC 端點設定。這可做為從網際網路存取受限的位置，透過公有網際網路串流使用者工作階段的替代方案，並受益於透過 Direct Connect 執行個體存取 。透過 VPC 端點串流使用者工作階段需要下列項目：

- 與介面端點相關聯的安全群組必須允許從使用者連線的 IP 地址範圍存取連接埠 443(TCP) 和連接埠 1400-1499(TCP)。
- 子網路的網路存取控制清單必須允許從暫時性網路連接埠 1024-65535(TCP) 到使用者連線之 IP 地址範圍的傳出流量。
- 需要網際網路連線才能驗證使用者，並提供 WorkSpaces 應用程式運作所需的 Web 資產。

若要進一步了解如何使用 WorkSpaces 應用程式限制 AWS 服務的流量，請參閱從 VPC 端點建立和串流的管理指南。

需要完整公有網際網路存取時，最佳實務是在映像建置器上停用 Internet Explorer 增強型安全組態 (ESC)。如需詳細資訊，請參閱 WorkSpaces 應用程式管理指南，以停用 Internet Explorer 增強型安全組態。

災難復原

Amazon AppStream 2.0 已跨最多三個可用區域內建備援。這表示如果使用者在可用區域中具有降級的作用中工作階段，他們可以直接中斷連線並重新連線，以將工作階段保留在運作狀態良好的可用區域中，前提是您有容量。雖然這可在 區域內提供高可用性，但如果服務在區域層級遇到問題，則不會提供災難復原解決方案。

若要為您的 WorkSpaces 應用程式使用者提供災難復原計劃，您必須先在次要區域中建置 WorkSpaces 應用程式環境。從設計角度來看，如果適用，此環境應具有與內部部署環境的備援連線，且不應依賴主要區域。例如，如果您的 WorkSpaces 應用程式機群已加入網域，您應該在次要區域中設定了 Site and Services 的其他網域控制站。從 WorkSpaces 應用程式的觀點來看，此環境應該包含您在主要區域中擁有的相同機群和堆疊設定。機群本身應執行相同的基礎映像，可透過主控台或以程式設計方式複製到次要區域。如果在 WorkSpaces 應用程式工作階段中執行的應用程式具有與您的主要區域繫結的後端相依性，則該應用程式也應該具有區域備援，以確保使用者仍然可以在主要區域停機時存取應用程式的後端。目的地區域中的服務層級限制應與主要區域相符。

身分路由

在 DR 案例中提供應用程式存取權的方法有兩種。在高階，這兩種方法會因使用者導向容錯移轉區域的方式而有所不同。第一個方法在 IdP 中使用單一 WorkSpaces 應用程式組態執行，第二個方法有兩個不同的應用程式組態。

方法 1：變更應用程式的轉送狀態

當使用者從身分提供者 (IdP) 登入 WorkSpaces 應用程式時，在身分驗證後，他們會轉送至符合其預期可存取的區域和堆疊的特定 URL。如需轉送狀態 URL 的詳細資訊，請參閱 Amazon WorkSpaces 應用程式管理指南。管理員可以設定在與主要區域相同的 WorkSpaces 應用程式映像上建置的跨區域堆疊，讓使用者容錯移轉。管理員只需更新轉送狀態 URL 以指向容錯移轉堆疊，即可控制此容錯移轉。若要讓此方法正常運作，相關聯的 IAM 政策將需要反映對兩個堆疊的存取：主要和容錯移轉。如需如何設定這些 IAM 政策的詳細資訊，請參閱下列範例政策。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "appstream:Stream",
            "Resource": [
                "arn:aws:appstream:us-east-1:190836837966:stack/StackName",
                "arn:aws:appstream:us-east-1:190836837966:stack/StackName"
            ],
            "Condition": {
                "StringEquals": {
                    "appstream:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

方法 2：在您的 IdP 中設定兩個 WorkSpaces 應用程式

此方法需要管理員在 IdP 中為 WorkSpaces 應用程式建置兩個不同的應用程式。然後，他們可以顯示這兩個應用程式，讓使用者選擇要前往何處，或鎖定/隱藏應用程式，直到容錯移轉為止。此方法更符合讓全域使用者經常四處移動的使用案例。這些使用者應該從最接近的端點串流，因此指派兩個應用程式給他們選擇為最接近的區域設定的應用程式。這也可以自動化，如需詳細資訊，請參閱此部落格文章。

儲存體持久性

利用 WorkSpaces 應用程式包含的資料持久性功能時，例如 Application Persistence 和 Home Folder Synchronization，您將需要將該資料複寫到您的容錯移轉區域。這些功能會將持久性資料存放在指定 WorkSpaces 應用程式區域的 Amazon S3 儲存貯體中。若要讓資料保留跨區域，您需要將來源儲存貯體上的所有變更複寫至容錯移轉區域 WorkSpaces 應用程式儲存貯體。這可以透過原生 Amazon S3 功能完成，例如 Amazon S3 跨區域複寫。每個使用者持久性資料都會位於其雜湊使用者名稱的資料夾下。由於使用者名稱將雜湊相同的跨區域，因此只要複寫資料即可在次要區域中提供資料持久性。如需 WorkSpaces 應用程式所用 Amazon S3 儲存貯體的詳細資訊，請參閱本指南。

監控

使用儀表板

監控機群使用率是一項定期活動，可透過 CloudWatch 指標執行並建立儀表板。或者，從 WorkSpaces 應用程式主控台，使用機群用量索引標籤。定期監控您的機群用量，因為使用者行為並非總是可預測的，而且需求甚至可能超過一級前期規劃。您可以在監控資源下的 WorkSpaces 應用程式管理指南中找到 CloudWatch 的 WorkSpaces 應用程式指標和維度的完整清單。

預期成長

每當 發生大幅跳躍時`PendingCapacity`，就會發生自動擴展事件。在新的 WorkSpaces 應用程式機群執行個體可用於託管使用者工作階段時，請務必確認 `AvailableCapacity`和 `PendingCapacity` 具有反向關係。`InsufficientCapacityError` 為每個 WorkSpaces 應用程式機群建立 CloudWatch 警示，以通知管理員，確保自動擴展不會落後於需求。

如果需求超過容量且`InsufficientCapacityError`指標值很常見，請考慮在工作日開始時透過排程擴展政策提高最小容量。此外，具有第二個排程擴展政策，可在滿足需求後降低最小容量。請記住，降低最小容量的值不會影響現有的工作階段。在工作日結束前降低最小容量，可透過降低 的值，有效地讓擴展如預期般運作`ActualCapacity`。這可最佳化成本。

如果需求持續無法預測，請使用目標追蹤擴展政策，以確保 WorkSpaces 應用程式機群`AvailableCapacity`有足夠的空間來滿足需求，同時判斷使用模式。繼續監控，因為目標追蹤會使用機群耗用量的百分比。隨著機群執行個體總數的增加，未使用的機群執行個體總數會倍增。除非最大容量設定為保守值，否則這會變得浪費。使用多種擴展政策類型 （ 例如排程和目標追蹤 ） 來平衡可靠性與成本最佳化。

監控使用者用量

監控唯一使用者，因為以使用者費用的形式存在與該使用者相關聯的成本。此使用者費用是由映像助理 (RDS) 訂閱者存取授權 (SAL) 所產生。評估唯一使用者可以透過執行身分驗證的 IdP 報告，或透過用量報告來執行。

用量報告會以個別`.csv`檔案形式存放在 S3 儲存貯體中，您可以使用第三方商業智慧 (BI) 工具下載和分析。您可以在 中分析用量資料， AWS 而無需下載報告或建立自訂日期範圍的報告，而無需串連多個`.csv`檔案。例如，您可以使用 Amazon Athena 和 Amazon Quick 來建立 WorkSpaces 應用程式用量資料的自訂報告和視覺化。

持久性應用程式和 Windows 事件日誌

WorkSpaces 應用程式執行個體工作階段完成時，執行個體會結束。這表示工作階段中使用的所有應用程式和 Windows 事件日誌都會遺失。如果需要保留這些應用程式和 Windows 事件日誌，其中一種方法是使用 Amazon Data Firehose 將它們即時交付至 S3，並使用 Amazon OpenSearch Service (OpenSearch Service) 進行搜尋。如果預期查詢不會頻繁發生，若要最佳化成本，請使用 Amazon Athena 進行搜尋，而不是執行 Amazon OpenSearch Service。

稽核網路和管理活動

如果尚未設定 ，最佳實務是 AWS 帳戶 使用 Amazon WorkSpaces 應用程式AWS CloudTrail為設定 。若要特別稽核 WorkSpaces 應用程式 API 呼叫，請使用值為 的篩選事件來源`appstream.amazonaws.com`。

啟用 VPC 流程日誌，以稽核對客戶受管資源的存取。VPC 流程日誌可以發佈至 CloudWatch Logs，以在需要稽核時執行查詢。

隨著 WorkSpaces 應用程式機群的成長，監控子網路 IP 配置非常重要。透過執行 describe-subnets CLI 來報告 IP 指派，以報告指派給機群之每個子網路中的可用 IP 地址。確保您的組織有足夠的 IP 地址容量，以滿足以最大容量執行的所有機群的需求。

成本最佳化

成本最佳化著重於避免不必要的成本。關鍵主題包括了解和控制花費金錢的位置，以及選擇最適合且正確的資源類型數量。分析一段時間內的支出和擴展，以滿足業務需求。下列 WorkSpaces 應用程式資源會產生pay-as-you-go：

- Always-On 機群執行個體
- 隨需機群執行個體
- 隨需停止執行個體費用
- 映像建置器執行個體
- 使用者費用

如需最新的定價資訊，請參閱 AWS Amazon WorkSpaces 應用程式定價的網站。 Amazon WorkSpaces

設計具成本效益的 WorkSpaces 應用程式部署

規劃和設計 WorkSpaces 應用程式部署的第一步是使用簡單的定價工具來估計與用量相關的 AWS 費用基準。提供您的使用者總數、每小時的實際並行使用量、執行個體類型和機群使用率，定價工具會估算每個使用者的價格。它也會顯示當您使用隨需機群而非 Always-On 機群時的預估節省價格。

像 WorkSpaces 應用程式定價模式的客戶，只需為他們佈建的執行個體付費，以滿足使用者的串流需求。此模型與其現有的應用程式串流環境不同。這些通常是根據尖峰容量的佈建，即使在夜間、週末和假日，負載較低時也是如此。Amazon AppStream 2.0 定價工具僅提供與您使用 WorkSpaces 應用程式 相關的 AWS 費用估算，不包含任何可能適用的稅金。您的實際費用取決於各種因素，包括實際使用 AWS 服務。

WorkSpaces 應用程式定價工具以 Microsoft Excel 或 OpenOffice Calc 試算表的形式提供，可讓您輸入機群的基本資訊，然後根據您的使用模式為隨需和全年無休機群提供 WorkSpaces 應用程式環境的成本估算。您可以根據歷史或預期的用量趨勢來模擬成本。彈性機群內建這些功能，讓管理員無須預測用量、建立、維護擴展政策和映像。執行 Amazon Linux 2 的彈性機群和執行個體 （所有機群類型） 會在串流工作階段期間以秒為單位計費，最少 15 分鐘。

選擇執行個體類型來最佳化成本

對於機群和映像建置器執行個體，您可以為應用程式選擇各種不同的執行個體系列和類型。

最終使用者測試 — 下一步是將 WorkSpaces 應用程式機群推展到一組試驗使用者，以進行測試來驗證我們選擇的執行個體類型。請務必請求試行使用者測試其所有一般和繁重的工作流程，以擷取記憶體、CPU 和圖形的指標，以便您可以擷取基準效能指標。試行群組應包含各種使用應用程式的使用者角色，以確保您從多個使用者體驗進行測試。使用者接受度測試可讓您收集有關串流工作階段體驗的意見回饋。建立或更新堆疊時，可以選擇使用自訂意見回饋 URL。使用者選擇傳送意見回饋連結以提交有關其應用程式串流體驗的意見回饋後，就會重新導向至此 URL。如果有效能瓶頸，請使用 Windows 效能指標來分析資源限制。例如，如果目前的機群執行個體類型 stream.standard.medium 顯示資源限制，請將執行個體類型升級至 stream.standard.large。相反地，如果效能指標顯示大量資源使用不足，請考慮降級執行個體類型。

使用機群類型選擇來最佳化成本

建立新的 WorkSpaces 應用程式機群時，開發人員必須選擇 Always- On 或 On-Demand 機群類型。從定價角度選擇執行個體類型時，請務必了解 WorkSpaces 應用程式如何管理機群執行個體。對於 Always-On 機群，機群執行個體會保持在執行中狀態。因此，當使用者嘗試串流工作階段時，機群執行個體一律準備好開始串流工作階段。

對於隨需機群，在機群執行個體啟動後，它們會保持在停止狀態。停止的執行個體費用低於執行中的執行個體費用，這有助於降低成本。隨需機群執行個體必須從停止狀態啟動。使用者必須等待約兩分鐘，才能使用其串流工作階段。

彈性機群非常適合獨立運作的應用程式，並且可以安裝在儲存在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的虛擬硬碟。由於僅收取串流期間的每秒帳單，彈性機群可能會進一步降低某些使用案例的成本。速率是您在建立機群時所選擇的執行個體類型、大小和作業系統的函數。

如果最終使用者在上班時間需要機群執行個體，最好保留相同的串流工作階段。這是因為機群執行個體每小時收費，而且每次新的串流工作階段啟動時都會產生另一個機群執行個體費用。

表 10 — WorkSpaces 應用程式機群類型比較

機群類型	優點	考量
Always-On	減少串流工作階段的等待時間	使用者會支付每小時執行個體費用，因為沒有讓執行個體保持在停止狀態的選項。
On-Demand	執行個體保持停止狀態時節省的成本	串流工作階段的等待時間較長

機群類型	優點	考量
彈性	每秒計費對於可在虛擬硬碟上安裝之應用程式具有零星使用模式的使用案例可能很有用	隨著應用程式虛擬硬碟的大小變大，將其掛載到串流執行個體所需的時間可能很長

WorkSpaces 應用程式會監控您的機群使用率，並自動調整機群容量，以盡可能最低的成本滿足您的使用者需求。容量調整是根據您根據目前使用率或排程定義的擴展政策進行。定期檢閱機群用量指標，以驗證機群擴展政策沒有高層級的備用容量。

擴展政策

機群 Auto Scaling 可讓您最佳化機群資源，無需過度遞交等待使用者登入的資源。管理員可以根據各種使用率調整機群的大小，以符合使用者需求。使用 CloudWatch WorkSpaces 應用程式機群指標或第三方監控工具來了解使用者活動，並設定擴展政策，根據預期的用量來擴展或縮減 WorkSpaces 應用程式機群。使用者日誌是了解實際使用情況的必要機制。此洞見可用來根據 Auto Scaling 動態變更機群大小。

在許多情況下，WorkSpaces 應用程式機群是根據使用者數量上限建立的，而且不會針對一天和一週的不同時間進行調整，例如夜間和週末。串流應用程式並行使用者計數通常小於使用者總數，特別是當使用者具有遠端工作的彈性時。在投影用量模式時，請務必考量這些因素。過度估算會導致 WorkSpaces 應用程式執行個體過度佈建，進而產生額外的成本。若要獲得最佳組態，您可能需要結合一或多個排程擴展政策與橫向擴展政策。

若要進一步了解如何實作擴展政策，請檢閱擴展 Amazon AppStream 2.0 機群。

使用者費用

在使用者從 WorkSpaces 應用程式機群執行個體串流應用程式的每個 AWS 區域 中，使用者每月都會向每位使用者收取費用。為 WorkSpaces 應用程式使用者提供一致的使用者 IDs，而不是產生不同的使用者 IDs。連線至映像建置器時，不會收取使用者費用。

學校、大學和特定公有機構可能符合 Microsoft RDS SAL 使用者費用折扣的資格，每位使用者每月 0.44 美元。如需資格要求，請參閱 Microsoft 授權條款和文件。

如果您有 Microsoft 授權行動性，您可能有資格使用自己的 Microsoft RDS 用戶端存取授權 CALs)，並將其與 Amazon WorkSpaces 應用程式搭配使用。如果您擁有自己的授權，則不會產生每月使用者費

用。如需如何搭配 Amazon WorkSpaces 應用程式使用現有 Microsoft RDS CAL 授權的詳細資訊，請參閱AWS 授權行動性指南，或諮詢您的 Microsoft 授權代表。

映像建置器用量

WorkSpaces 應用程式映像建置器執行個體會每小時收費。Image Builder 執行個體費用包括運算、儲存和串流通訊協定使用的任何網路流量。所有正在執行的映像建置器執行個體都會收取適用的執行執行個體費用。此費用是根據執行個體類型和大小而定，即使沒有連接管理員也一樣。

作為最佳化成本的最佳實務，請在不使用 Image Builder 執行個體時將其關閉。CloudWatch Events 規則可用來排程每日任務，例如叫用 Lambda 函數來停止映像建置器執行個體。

您可以使用受管 WorkSpaces 應用程式映像更新，讓 WorkSpaces 應用程式映像保持up-to-date狀態。此更新方法提供最新的 Windows 作業系統更新和驅動程式更新，以及最新的 WorkSpaces 應用程式代理程式軟體。使用此方法更新映像時，映像建置器會自動啟動和停止，作為受管服務程序的一部分。

結論

使用 WorkSpaces 應用程式，您可以輕鬆將現有的桌面應用程式新增至 ， AWS 並讓使用者能夠立即串流。Windows 使用者可以使用 WorkSpaces 應用程式用戶端或HTML5-capable的 Web 瀏覽器進行應用程式串流。您可以保留每個應用程式的單一版本，讓管理應用程式更為容易。而您使用者存取的永遠都是最新版本的應用程式。您的應用程式在 AWS 運算資源上執行，而且資料永遠不會存放在使用者的裝置上，這表示他們永遠都能獲得高效能、安全的體驗。

與桌面應用程式串流的傳統現場部署解決方案不同，WorkSpaces 應用程式提供pay-as-you-go定價，無需預付投資，也無需維護基礎設施。您可以立即和全域擴展，確保您的使用者始終擁有卓越的體驗。

Amazon WorkSpaces 應用程式旨在整合到現有的 IT 系統和程序中，本白皮書說明了執行此操作的最佳實務。遵循本白皮書中的準則的結果是經濟實惠的雲端桌面部署，可以安全地擴展全球 AWS 基礎設施上的業務。

貢獻者

本文件的貢獻者包括：

- 安德魯伍德，資深解決方案架構師，Amazon Web Services
- 安德魯·摩根，歐盟專家 SA，Amazon Web Services
- 阿倫 PC, 高級 EUC 專家 SA, Amazon Web Services
- 亞馬遜網路服務高級解決方案架構師阿斯瑞爾農業
- 達斯汀·謝爾頓, 高級 EUC 專家 SA, Amazon Web Services
- 傑里米·希弗，高級解決方案架構師，Amazon Web Services
- 納維馬吉，首席解決方案架構師，Amazon Web Services
- Amazon Web Services 高級雲端 Support 工程師皮特·弗格斯
- 菲爾·佩爾森, 首席 EUC 專家 SA, Amazon Web Services
- 理查德·斯帕文, 高級 EUC 專家 SA, Amazon Web Services
- 斯賓塞 DeBrosse，資深解決方案架構師，Amazon Web Services
- 斯蒂芬·斯特勒，資深解決方案架構師，Amazon Web Services
- 松本塔卡，資深雲端 Support 工程師，Amazon Web Services
- 瓦桑特·西爾塞特, 高級 EUC 專家 SA, Amazon Web Services

深入閱讀

如需其他資訊，請參閱：

- Amazon WorkSpaces 應用程式管理指南
- Amazon WorkSpaces 應用程式 API 參考
- 使用 Amazon FSx for Windows File Server 和 FSLogix 最佳化 Amazon WorkSpaces 應用程式上的應用程式設定持續性
- 使用 Amazon ElasticSearch 和 Amazon Firehose 監控 Amazon WorkSpaces 應用程式 ElasticSearch
- 使用 Amazon Athena 和 Amazon Quick 分析 Amazon WorkSpaces 應用程式用量報告 Amazon Athena
- 擴展 Amazon WorkSpaces 應用程式機群
- 使用 Microsoft AppLocker 管理 Amazon WorkSpaces 應用程式上的應用程式體驗
- 搭配 Amazon WorkSpaces 應用程式使用自訂網域
- 如何將自己的 Microsoft RDS CALs與 WorkSpaces 應用程式搭配使用？
- Amazon WorkSpaces 應用程式定價工具
- 使用 WorkSpaces 應用程式建立線上軟體試用
- 使用 Amazon WorkSpaces 應用程式建立 SaaS 入口網站

文件修訂

若要收到有關此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
文件已更新	更新包括 Elastic 叢集、基於問題的應用程式權利、多堆疊應用程式目錄、Linux 型叢集、資料輸入和輸出、災難復原及其他更新。	2022 年 6 月 14 日
文件已更新	HTML 版本已發佈。	2022年1月19日
初始出版	白皮書已出版。	2021 年 6 月 8 日

注意

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

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。