部署 Amazon AppStream 2.0 的最佳實務

部署 Amazon AppStream 2.0 的最佳實務:

Table of Contents

部署亞馬遜 AppStream 2.0 的最佳實踐

出版日期：二零二二年一月十九日 (文件修訂)

摘要

本白皮書概述了部署 Amazon AppStream 2.0 的一組最佳實務。該 paper 涵蓋 Amazon Virtual Private Cloud (VPC) 設計、映像建立和管理、車隊自訂以及車隊自動擴展策略。它包括用戶連接方法，身份驗證，並與 Microsoft 活動目錄集成。本 paper 還包括設計 AppStream 2.0 安全性、監控和成本最佳化的建議。

本白皮書的撰寫目的是讓您能夠快速存取相關資訊。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 AppStream 2.0 是全受管的應用程式串流服務，可讓使用者從任何地方立即存取其桌面應用程式。 AppStream 2.0 管理託管和運行應用程序所需的AWS資源。它會自動擴展，並根據需求提供對用戶的訪問。 AppStream 2.0 可讓使用者存取他們所選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法區別。

以下各節提供有關 Amazon AppStream 2.0 的詳細資訊、說明服務的運作方式、說明啟動服務所需的項目，以及告訴您可以使用哪些選項和功能。為使用者部署 AppStream 2.0 時，請務必實作最佳做法，以提供出色的使用者體驗。此外，各種規模的公司都可以從降低每月營運成本的成本優化中受益。

重要概念

為了充分利用 AppStream 2.0，請熟悉以下概念：

- Image — 映像檔是預先設定的執行個體範本。影像包含可串流給使用者的應用程式，以及預設的 Windows 和應用程式設定，讓您的使用者能夠快速開始使用其應用程式。 AWS提供基本映像，您可以用來建立包含您自己應用程式的映像檔。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。您可以將圖像複製到其他圖像，AWS區域也可以與同一區域中的其他AWS 帳戶圖像共享。
- 映像產生器 — 映像產生器是用來建立映像的虛擬機器。您可以使用 AppStream 2.0 主控台啟動並連線到映像產生器。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。
- 叢集 — 叢集由執行您指定映像檔的叢集執行個體 (也稱為串流執行個體) 組成。您可以為叢集設定所需的串流執行個體數量，並設定原則以根據需求自動擴展叢集。請注意，每個用戶都需要一個實例。
- 堆疊 — 堆疊包含相關聯的叢集、使用者存取原則和儲存區組態。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 (也稱為叢集執行個體) 是 Amazon 彈性運算雲端 (Amazon EC2) 執行個體，可供單一使用者使用，以進行應用程式串流。使用者的工作階段完成後，Amazon EC2 就會終止執行個體。

VPC 設計

設計指引

將 AppStream 2.0 部署到專用 VPC 中。在設計 AppStream 2.0 VPC 時，預測的成長規模。保留新使用案例的 IP 位址容量，以及稍後可新增的其他可用區域 (AZ)。 AppStream 2.0 的基本設計要點是只有一個用戶可以使用 AppStream 2.0 實例。配置 IP 空間時，請將一位使用者視為每個 AppStream 2.0 執行個體一個 IP 位址。使用 AppStream 2.0 時，使用者可以使用多個 AppStream 2.0 執行個體。因此，規劃 IP 空間也必須考慮需要額外 AppStream 2.0 個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建議您不要過度配置私有 IP 位址。您可以透過額外的 CIDR 來擴充 VPC 的大小，但是有一個限制；因此，從一開始就分配所需的內容。

如果 AppStream 2.0 部署已加入使用中目錄網域，則為 VPC 設定的 DHCP 選項必須已設定網域 DNS。網域名稱伺服器應該指定作用中目錄網域授權的 DNS IP 位址，或者 DNS 應該將 DNS 要求轉寄至作用中目錄網域的授權 DNS 執行個體。此外，VPC 必須具有`enableDnsHostnames`並進行`EnableDnsSupport`配置。

可用區域

可用區域 (AZ) 是一或多個獨立資料中心，在AWS 區域. 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。

Amazon AppStream 2.0 只需要一個子網路即可在叢集中啟動。最佳做法是至少設定兩個可用區域，每個唯一可用區域一個子網路。若要最佳化叢集 auto 擴充，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 空間以促進成長的額外好處，本文件的下列子網路大小一節涵蓋。AWS 管理主控台僅提供在建立叢集期間指定的兩個子網路。使用 AWS Command Line Interface(AWSCLI) 或允AWS CloudFormation許兩個以上的子網路 ID。

調整子網大小

將子網路專用於 AppStream 2.0 叢集，讓路由原則和網路存取控制清單具有彈性。堆疊可能會有不同的資源需求。例如， AppStream 2.0 堆棧可以具有隔離要求，以便分離規則集。當多個 Amazon AppStream 2.0 叢集使用相同的子網路時，請確保所有叢集的最大容量總和不超過可用 IP 地址的總數。

如果相同子網路中所有叢集的最大容量可能 (或已超過可用的 IP 位址總數)，請將叢集遷移至專用子網路。這可防止自動調整規模事件耗盡配置的 IP 空間。如果叢集的總容量超過指派子網路的配置 IP 空

間，請使用 API 或 AWS CLI「更新叢集」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。

最佳做法是擴展子網路的數量，相應地調整子網路大小，同時保留 VPC 中成長的容量。此外，請確保 AppStream 2.0 叢集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 位址。使用兩個以上的子網路並水平擴展可提供數個好處，例如：

- 可用區域故障提供更高的復原能力
- 自動擴展叢集執行個體時，輸送量
- 更有效地使用私有 IP 地址，避免 IP 燒錄

調整 Amazon AppStream 2.0 子網路的大小時，請考慮子網路的總數，以及尖峰使用率期間預期的峰值並行。這可以使用 (`InUseCapacity`) 加上叢集的預留容量 (`AvailableCapacity`) 進行監控。在 Amazon AppStream 2.0 中，已消耗執行個體和 available-to-be-consumed AppStream 2.0 叢集執行個體的總和都會加上標籤`ActualCapacity`。若要正確調整總 IP 空間的大小，請預測所需的`ActualCapacity`，然後除以子網路數目，減去一個指派給叢集的恢復子網路。

例如，如果預期尖峰時的叢集執行個體數目上限為 1000 個，而業務需求在一個可用區域故障中具有復原能力，則 3 個 x/23 子網路可滿足技術和業務需求。

- /23 = 512 部主機 — 5 個保留 = 每個子網路 507 個叢集執行個體
- 3 個子網路 — 1 個子網路 = 2 個子網路
- 每個子網路 2 個子網路 x 507 個叢集執行個體 = 尖峰時有 1,014 個叢集執行個體

子網路大小範例

雖然 2 x /22 子網路也能滿足復原能力，但請考慮下列事項：

- 而不是保留 1,536 個 IP 地址，而是使用兩個 AZ 會導致 2,048 個 IP 地址被保留，浪費可以使用其他功能的 IP 地址。
- 如果一個 AZ 無法存取，向外擴充叢集執行個體的能力會受到 AZ 的輸送量的限制。這可以延長的持續時間`PendingCapacity`。

子網路由

最佳做法是為 AppStream 2.0 執行個體建立私有子網路，並透過集中式 VPC 路由至公用網際網路以取得輸出流量。 AppStream 2.0 工作階段串流的輸入流量是透過串流閘道透過 Amazon AppStream 2.0 服務處理：您不需要為此設定公有子網路。

區域內連接

對於加入至作用中目錄網域的 AppStream 2.0 叢集執行個體，請在每個AWS 區域共用服務 VPC 中設定作用中目錄網域控制站。活動目錄的來源可以是基於 Amazon EC2 的域控制器或 AWSMicrosoft 受管 AD。共用服務與 AppStream 2.0 VPC 之間的路由可以是透過 VPC 對等連線或傳輸閘道。雖然傳輸閘道可以解決大規模路由的複雜性，但在大多數設定中，VPC 對等互連的原因有很多：

- VPC 對等互連是兩個 VPC 之間的直接連線 (無額外躍點)。
- 無需每小時費用，只需支付可用區域之間的標準資料傳輸費率。
- 頻寬沒有限制。
- Support 存取 VPC 之間的安全群組。

如果 AppStream 2.0 執行個體連線到共用服務 VPC 中含有大型資料集的應用程式基礎結構和/或檔案伺服器，則尤其如此。透過最佳化這些通常存取資源的路徑，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，VPC 對等連線也是最佳選擇。

出站互聯網流量

雖然直接路由至共用服務大部分是透過對等連線最佳化的，但 AppStream 2.0 的輸出流量可以透過使用 AWS Transit Gateway 從多個 VPC 建立單一網際網路出口點來設計。在多虛擬私人雲端設計中，擁有可控制所有傳出網際網路流量的專用 VPC 是一項標準作法。透過此組態，Transit Gateway 具有更大的彈性，並可控制附加至子網路的標準路由表格上的路由。此設計也支援傳遞路由，不需要額外的複雜性，並且不需要在每個 VPC 中使用冗餘網路位址轉譯 (NAT) 閘道或 NAT 執行個體。

將所有輸出網際網路流量集中到單一 VPC 後，NAT 閘道或 NAT 執行個體就是常見的設計選擇。若要判斷哪一種最適合您的組織，請檢視比較 NAT 閘道和 NAT 執行個體的管理指南。 AWSNetwork Firewall 可以透過在路由層級進行保護，並在 OSI 模型中提供第 3 層到第 7 層的無狀態和可設定狀態規則，從而將保護範圍擴展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 AWSNetwork Firewall 的部署模式。如果您的組織選擇了執行進階功能 (例如 URL 篩選) 的協力廠商產品，請將服務部署到輸出網際網路 VPC 中。這可以取代 NAT 閘道或 NAT 執行個體。請遵循第三方廠商提供的準則。

現場部署

當需要與內部部署資源的連線時，特別是對於加入 Active Directory 的 AppStream 2.0 執行個體，請透過以下方式建立高度彈性的連線AWS Direct Connect。

VPC 端點

Amazon S3 VPC 端點

許多 Amazon AppStream 2.0 部署都需要透過主資料夾和應用程式設定保存使用者狀態。啟用與這些 Amazon 簡單儲存服務 (Amazon S3) 位置的私人通訊，因為這樣可避免使用公用網際網路。您可以透過 VPC 端點閘道達成此目的。AWS PrivateLink對於 Amazon S3，較偏好使用 VPC 端點閘道，因為：

- 它針對 AppStream 2.0 網路存取需求進行了最佳化的成本
- 不需要從現場部署資源存取 Amazon S3 儲存貯體
- 自訂政策文件可用來限制僅限 AppStream 2.0 執行個體的存取

建立 VPC 端點閘道後，最佳做法是透過建立自訂原則來保護私有化連線的安全。自訂政策從 AppStream 2.0 服務 Identity and Access Management 角色的 Amazon 資源名稱 (ARN) 開始。明確指定使用者狀態持續性所需的 S3 動作。

> **Note**
>
> 下列`Resources`區段中的範例會先指定狀態主資料夾路徑，並指定應用程式設定路徑的第二個路徑。

Example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-AppStream-to-access-home-folder-and-
application-settings",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:sts::account-id-without-hyphens:assumed-
role/AmazonAppStreamServiceAccess/AppStream2.0"
      },
      "Action": [
        "s3:ListBucket",
```

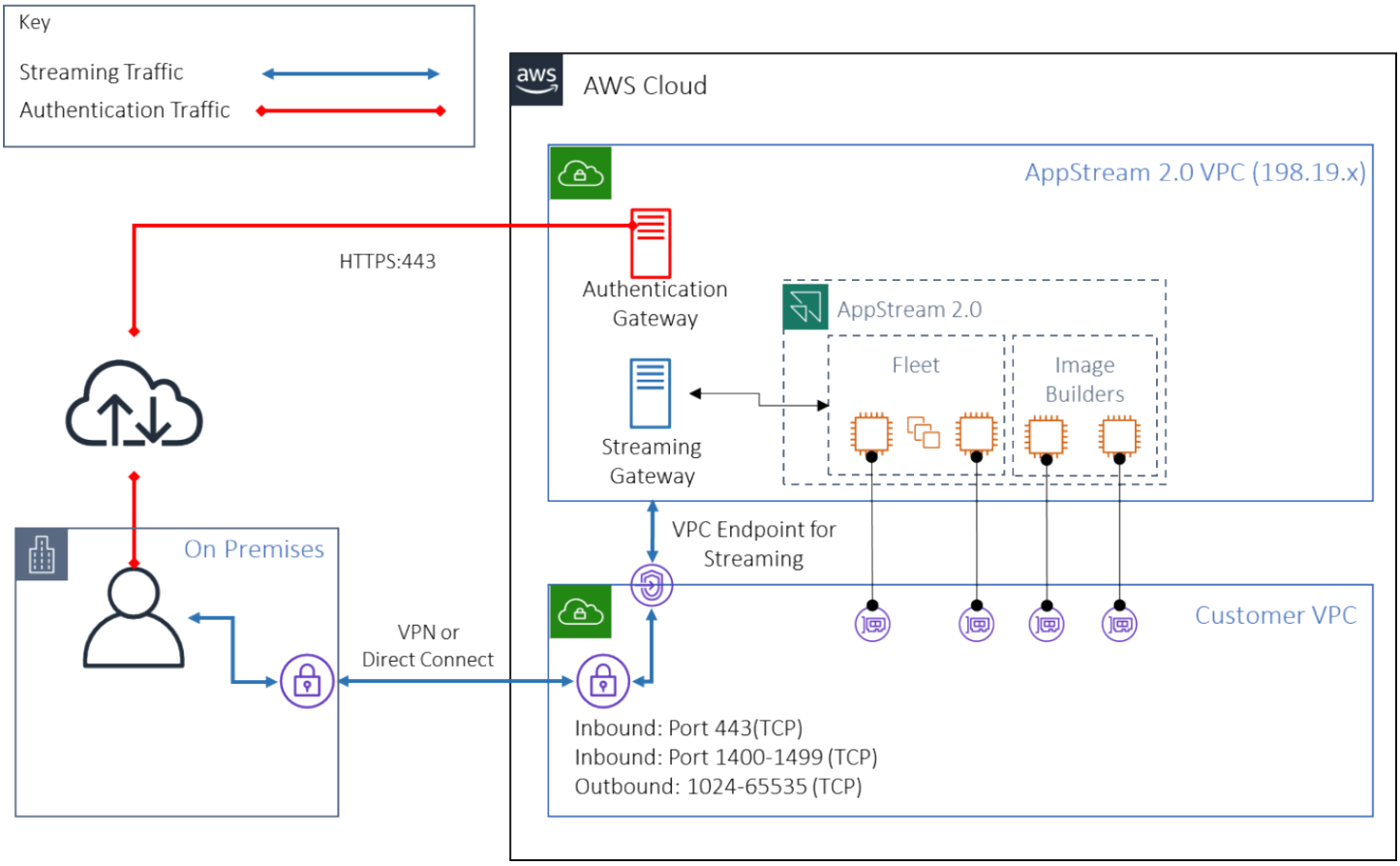
```
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*"
      ]
    }
  ]
}
```

亞馬遜 AppStream 2.0 API 接口 VPC 端點

在 Amazon AppStream 2.0 的 API 和 CLI 命令源自您的虛擬私人雲端的設計案例中，請透過介面 VPC 端點將這些程式化呼叫私有化。

亞馬遜 AppStream 2.0 流媒體界面 VPC 端點

雖然可以透過界面 VPC 端點路由 Amazon AppStream 2.0 串流流量，但請謹慎使用此組態。透過公用網際網路進行的預設串流行為是 Amazon AppStream 2.0 串流流量最有效率且最高效能的交付方式。



亞馬遜 AppStream 2.0 流媒體界面 VPC 端點

如上圖所示，公用網際網路是通往 Amazon AppStream 2.0 串流閘道的最有效途徑。透過客戶管理的 VPC 和網路進行路由會增加複雜性和延遲時間。它還增加了數據傳輸費用AWS Direct Connect。

> **Note**
>
> VPC 端點僅支援串流，且驗證仍必須透過公用網際網路進行。SAML 單一登入 (SSO) 身分識別提供者 (IdP) 等先決條件存取仍然是只能透過公用網際網路存取的必要條件。

影像建立與管理

在 AppStream 2.0 中啟動叢集或映像產生器時，您必須選取其中一個 AppStream 2.0 基本映像。然後，管理員可以根據基礎映像進行建置，以新增自己的應用程式和組態設定。

建置映像檔時，有一些重要的考量，以確保應用程式正確且安全地運作。此外，還有針對如何維護該影像的設計考量。

建立一個 AppStream 2.0 映像檔

建立新影像時，請務必考慮下列事項：

- 作業系統
- 應用程式
- 使用者概況
- 安全性
- 效能
- 代理版本
- 影像助 CLI

建立一個 AppStream 2.0 映像檔

2021 年十一月， AppStream 2.0 推出了對亞馬遜 Linux 2 的支持。根據此公告， AppStream 2.0 現在支援四種平台類型：

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

您可能必須根據應用程式所需的內容來選擇特定平台 (例如，如果您的應用程式需要 Windows，則 Amazon Linux 2 將不是一個選項)。除了應用程式需求之外，請參考下列比較矩陣，協助您選擇最適合您使用案例和環境的平台類型：

表 1 — 平台類型、使用時機及定價

平台類型	使用情況	車隊定價 *
視窗伺服器 (二零一六年或 2019 年 R2)	您的應用程序只能在視窗中運行（並且它不支持亞馬遜 Linux 2）。您希望加入串流執行個體的網域。您希望在 AppStream 2.0 串流執行個體上使用現有的群組原則 (Linux 不遵守群組原則，但您可以使用工作階段指令碼在工作階段啟動時自動設定)。您將使用桌面視圖，您的用戶更喜歡 Windows 桌面體驗。您偏好使用提供 step-by-step 精靈的 Image Assistant 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 映像檔 (如需詳細資訊，請參閱本教學課程)。您想要使用「應用程式設定持續性」。Linux 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) 費用為每個唯一使用者每月 4.19 美元 ** 加上下列項目： 1. 永遠在線的隨選叢集每小時 0.10 USD 2. 彈性車隊每小時 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	與窗口實例相比，Linux 實例的成本更低。使用 Linux 時，您無需支付 RDS SAL 費用和下列每小時費用： 1. 每小時 0.084 美元，適用於永遠在線的隨選機隊 2. 彈性車隊每小時 0.112 美元

* 基於 N 維吉尼亞州的流. 標準. 中

** 符合資格的客戶可以攜帶自己的授權以免除 AWS RDS SAL 費用。如需詳細資訊，請參閱 AppStream 2.0 定價頁面。教育機構客戶也可能有資格獲得特殊優惠。學校、大學和某些公共機構可能符合降低 Microsoft RDS SAL 使用者費用的資格。

應用程式

在安裝應用程式之前，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。在映像產生器執行個體上成功安裝應用程式之後，請務必在測試使用者內容下切換使用者並測試應用程式。

規劃應用程式部署時，請注意服務端點和配額。此外，在創建映像之前，請清理安裝程序和幫助程序文件以優化 C 槽的總空間。提醒您， AppStream 2.0 執行個體有一個 200 GB 固定大小的磁碟區。安裝後最佳化磁碟空間是確保永遠不會超過固定大小磁碟區的最佳作法。

如果您想要修改使用者可以即時存取的應用程式目錄，動態應用程式架構會提供 API 作業。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 作用中目錄網域的 AppStream 2.0 叢集。如需詳細資訊，請參閱搭配使用使用中目錄 AppStream 2.0。

應用程序塊

應用程序塊代表啟動用戶將使用的應用程序所需的設置腳本和應用程序文件。虛擬硬碟 (VHD) 可以是來自 Amazon S3 的任何物件。建議使用此物件小於 1.5GB，因為必須在使用者存取應用程式之前完全下載。

優化應用程序塊

對於以 Windows 為基礎的叢集，建議您建立 VHDX 檔案來包含您的應用程式。對於以 Linux 為基礎的叢集，建議您建立映像檔 (IMG)。這些虛擬磁碟應建立盡可能小，以託管應用程式檔案。可以壓縮虛擬磁碟以進一步減少其大小。在安裝指令碼中，您必須先解壓縮磁碟才能掛載。範例 Windows PowerShell 安裝程式指令碼包含解壓縮功能。擴展存檔（zip）和下載速度之間存在折衷。為了找到提供最快應用程序啟動時間的平衡，可能需要進行一些測試。

更新應用

應用程序可以有輕微和重大變化。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。此設定可讓系統管理員變更有問題的應用程式 VHD 物件版本，而不需變更應用程式區塊組態，藉此復原至特定應用程式的先前版本。通過重大更新，為更新的 VHD 創建一個新的應用程序塊。這將允許管理員在應用程序塊級別與版本控制級別相反，分隔主要的應用程序更改，這為管理應用程序管理提供了更有條理的方法。

自訂使用者設定

Amazon AppStream 2.0 是通過設計非持久性應用程序和桌面解決方案。當使用者工作階段終止時，系統和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。它可能會增加登入程序的額外負荷，以及所需 S3 儲存的成本考量。

在需要應用程式設定持續性的情況下，AWS建議您透過自訂政策和 S3 VPC 閘道端點保護該連線。評估整體應用程式設定大小，並將儲存在應用程式設定持續性中的設定最小化，以最佳化成本和效能。

您可以在 AppStream 2.0 Image Builder 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，以及其他使用者特定組態。在 AppStream 2.0 影像助理中，您可以選擇建立使用者設定檔。這會將範本使用者紀要複製到預設的使用者紀要。將映像部署到叢集後，從叢集串流處理工作階段的使用者將會從預設使用者設定檔建立其使用者設定檔。請務必考慮最小化使用者設定檔大小，尤其是在啟用「應用程式設定持續性」時。依預設，使用者設定檔的最大 vHDX 大小為 1 GB。每次串流工作階段開始時，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，並造成超過限制的風險，這會導致使用 VHDX 檔案掛載使用者設定檔失敗。

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，在共用儲存 (例如 Windows 檔案伺服器的 Amazon FSx) 上使用漫遊設定檔或 FSLogix 設定檔容器。如需詳細資訊，請參閱使用適用於 FSx for Windows File Server 的 Amazon FSx 和 FSLogix 優化 Amazon 2.0 上的應用程式設定持續性。 AppStream

安全性

開發人員需要考慮不同的安全性測量。 AppStream 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引，請參閱讓 AppStream 2.0 映像保持在最新狀態，以取得保持基礎映像為最新狀態的其他指引。

根據預設， AppStream 2.0 允許使用者或應用程式在執行個體上啟動任何程式，而不是影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，以提供應用程式廠商網站的說明指示，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 是應用程序控制軟件，使用明確的控制策略來啟用，或禁用，哪些應用程序的用戶可以運行。

防毒軟體可能對串流工作階段和映像產生器執行個體產生不利 AWS建議您不要啟用防毒軟體的自動更新。如需 Windows 防御者的詳細資訊，請參閱防毒軟體。

效能

在建立新映像之前，請務必以測試使用者身分測試應用程式。以測試使用者身分測試可讓您確保應用程式可以在非系統管理員使用者內容下執行。此外，請使用工作管理員和效能監視器等內建工具檢查應用程式效能和使用者體驗。監視資源使用率 (例如 CPU、記憶體和 GPU 記憶體) 是最佳作法。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
- 停用增強型 IE 安全性

AppStream 2.0 代理程式版本選擇

建立新映像時，您可以選擇使用最新的 AppStream 2.0 代理程式軟體，或不更新。 AppStream 2.0 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。使用最多的 up-to-date 軟件保留您的圖像。在本文件的 [影像更新] 一節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。此選項可確保在啟動時始終安裝最新的 AppStream 2.0 代理程式。不過，未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存放映像。同樣重要的是，在將更新的映像推出至生產環境之前執行測試，以將啟動時間降至最低。

影像助理命令列介面 (CLI)

對於想要自動化或以程式設計方式建立 AppStream 2.0 映像的開發人員，請使用影像助理 CLI。此功能可在 2019 年 7 月 26 日或之後發行的 AppStream 2.0 代理程式軟體的映像建置器上使用。下列高階概觀說明以程式設計方式建立 AppStream 2.0 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 Image Assistant `add-application` CLI 作業來指定 AppStream 2.0 映像的應用程式中繼資料和最佳化資訊清單。
4. 若要為 AppStream 2.0 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 作業覆寫預設的 Windows 設定檔，並為您的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 作業以程式設計方式建立 AppStream 2.0 映像。

管理使用者串流體驗

使用工作階段指令碼

AppStream 2.0 提供實例會話腳本。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，您可以使用自訂指令碼，在使用者的串流工作階段開始之前準備 AppStream 2.0 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 AppStream 2.0 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，請參閱有關使用工作階段指令碼管理使用者體驗的管理指南一節。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。透過此額外指令碼，您可以執行進一步的使用者體驗最佳化。這樣可以最大限度地減少向使用者提供應用程式環境所需的影像和叢集數量。

使用作用中目錄群組原則

如果您打算在 Active Directory 網域中使用 AppStream 2.0 叢集，您可以使用群組原則物件 (GPO) 來管理使用者體驗。GPO 可以指派給建立 AppStream 2.0 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 中啟動基礎 AppStream 2.0 映像。這可以防止影響 AppStream 2.0 使用者體驗的其他網域原則。將每個叢集部署到其專屬 OU 中，透過建立環境的獨特 GPO，提供 AppStream 2.0 映像管理的 one-to-many 整合優勢。

使用群組原則的範例是指定映像設定不同的互聯網資源管理器首頁為每個 AppStream 2.0 叢集。

影像更新

軟體修補對於運算資源的安全性和效能至關重要。經常修補會列為 Well-Architected 架構的安全性支柱中的最佳作法。

建立和部署映像後， AppStream 2.0 映像中有四種軟體需要修補：

- 應用程式和相依性 — 您必須負責修補映像中的應用程式和相依性。
- Microsoft 視窗作業系統 — 你有責任安裝和維護更新視窗.
- 軟體元件 — 這些是 AppStream 2.0 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)。 AppStream 2.0 會定期發行包含新代理程式和驅動程式的新基礎映像檔。

您可以使用最新的基礎來重建映像，將映像上的軟體元件帶到最新的基準。當有許多應用程式或安裝複雜的應用程式時，以最新的基礎重建映像的程序可能非常耗時且繁瑣。

- AppStream 2.0 代理程式 — 您可以選擇「一律使用影像助理」中的最新代理程式版本。使用此選項，從映像檔啟動的串流執行個體會自動使用最新版本的代理程式。

您可以通過執行以下任一操作來保持 AppStream 2.0 圖像的最新狀態：

- 使用受管理的 AppStream 2.0 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 AppStream 2.0 代理程式軟體。此受管理方法不會更新服務和 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，最佳做法是使用此方法。
- 使用受管理的 AppStream 2.0 映像版本更新 AppStream 2.0 代理程式軟體 — 此更新方法提供最新的 AppStream 2.0 代理程式軟體。此方法確實允許您更新應用程序組件。

車隊定制

艦隊類型

建立叢集時，客戶必須選擇叢集類型。每種車隊類型為用戶體驗，成本和維護開銷提供了不同的好處。無論選擇的叢集類型為何，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」。

客戶現在可以從以下機群類型中進行選擇：

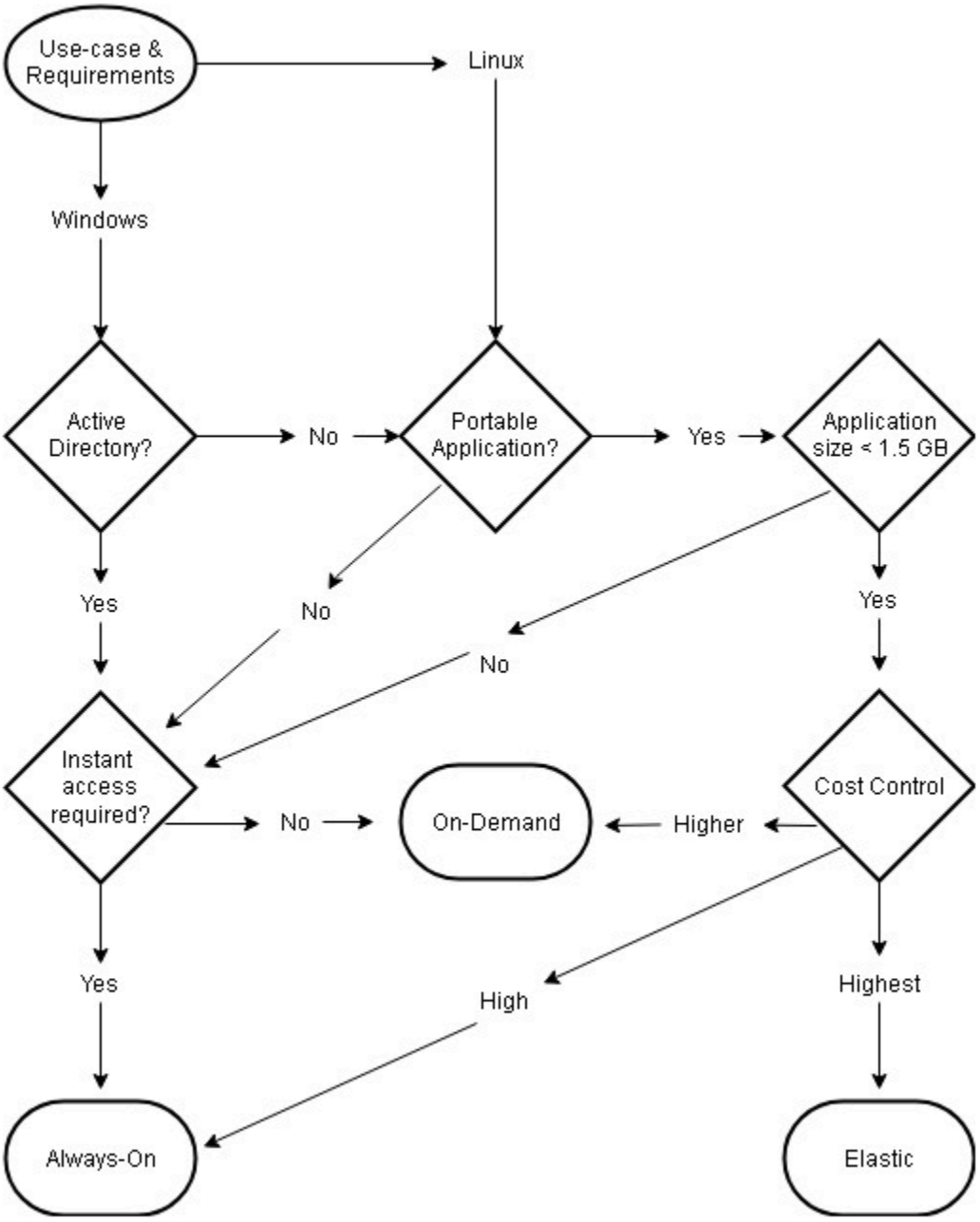
- 永遠在線 — 此叢集類型為使用者提供即時啟動存取其應用程式。即使沒有使用者串流應用程式，您仍需支付叢集中所有執行中的執行個體費用。
- 隨選 — 選取此叢集類型以最佳化串流成本。使用隨選叢集時，使用者的工作階段開始時間約為一到兩分鐘。不過，只有在使用者連線時，才會向您收取串流執行個體費用，而叢集中未串流應用程式的每個執行個體只需支付小時費用。
- 彈性 — 彈性叢集可用於不需要安裝且可從虛擬硬碟 (VHD) 執行的應用程式。彈性叢集不支援 AppStream 2.0 張映像，也不需要擴展政策。只會在串流工作階段期間向您收費。

表 2 — 亞馬遜 AppStream 2.0 車隊類型

艦隊類型	使用情況	使用者體驗	定價方式	備註
永遠在線	您的使用者需要在啟動工作階段時立即存取應用程式。您的叢集中不會有大量過剩的容量，也許是因為您的使用模式是可預測的，而且您可以透過擴展政策可靠地控制成本。	即時存取應用程式	您必須為叢集中可用的每個執行個體支付全額費用 (無論該執行個體是否用於工作階段)。	支援自訂映像和縮放原則。
按需	您必須在叢集中維持可觀的過剩	使用者在啟動工作階段後，等待	您只需為具有作用中工作階段的	支援自訂映像和縮放原則。

艦隊類型	使用情況	使用者體驗	定價方式	備註
	容量您想要最符合成本效益最佳化的環境，而且不想為未使用的容量支付全額費用您的使用者可以等待一到兩分鐘，以便在開始工作階段後存取其應用程式。您正在使用較大的執行個體類型。執行中執行個體的小時費用比停止的執行個體費用貴得多。	一到兩分鐘才能存取其應用程式。	串流執行個體支付全價，然後針對閒置執行個體支付小時費用。	

艦隊類型	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。每次使用者在彈性叢集中啟動工作階段時，您的虛擬硬碟 (VHD) 檔案都必須從 Amazon S3 下載到工作階段中。因此，較大的 VHD 檔案 (即大小超過 1.5 GB) 會導致使用者體驗不佳。您的應用程式是可攜式的。您不需要加入網域的串流執行個體 (Elastic 叢集目前無法使用網域加入) 您只想為使用中工作階段付費 (也就是說，您不需要為叢集中未使用的容量付費)。管理）。	使用者會在啟動工作階段後等待 45 秒到 3 分鐘才能存取應用程式 (等待時間取決於虛擬硬碟的大小)。	只會在串流工作階段期間向您收費。由於 Elastic 叢集沒有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 (客戶提供 VHD 應用程式) 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。



機隊類型使用案例和需求

車隊規模

最小容量和排程擴展

調整 AppStream 2.0 叢集的大小時，有幾項考量可直接轉換為使用者體驗和成本。輸入的最小容量值可確保 AppStream 2.0 個執行個體的數量很少小於此值。 AppStream 2.0 工作階段結束後，如果總共

AppStream 2.0 個執行個體小於最小容量值，則會啟動新的叢集執行個體。與往常一樣，請務必記住一個 AppStream 2.0 執行個體直接對應至一個使用者工作階段，直接影響最小容量的值。

輸入超出預期並行的最小容量值會導致成本增加，雖然使用者體驗不會受到影響。太低的值會導致成本較低，但是當請求總數超過可用容量時會影響使用者體驗。在這種情況下，系統管理員會發現「容量不足」錯誤。例如，當一天開始的預期連線數目`AvailableCapacity`是可預測的一致值時，等待`PendingCapacity`成為使用者時間的使用效率不佳。

從容納典型離峰時間的最小容量開始，然後使用排定的擴展政策在工作日開始之前有效地重設最小容量。不要忘記建立另一個排程擴展政策，將容量下限還原為離峰時間。如需擴展政策及其實作方式的詳細資訊，請參閱本文件中的叢集 auto-scaling 策略一節。

最大容量和服務配額

設定最大容量可能看起來是任意值，但如果正確預測和設定，則會將總資源耗用量和成本最佳化。輸入的值高於您中 AppStream 2.0 叢集的服務配額AWS 帳戶可能看起來有效，但是，當 auto Scaling 事件嘗試將資源擴展到最大容量時，由於容量上限值超過可用的服務配額，因此無法啟動。確保針對所需的最大容量提出服務配額請求，以確保您的組織預期的自動擴展功能。

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 < 利用叢集類型選項最佳化成本 > 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決定不會影響效能或成本。每個 AppStream 2.0 叢集在任何指定時間都只能存取一個檢視。您可以更改流視圖選項。在離峰工作時間規劃此變更，因為變更串流檢視需要重新啟動叢集。

串流檢視沒有單一的最佳做法。串流檢視選項的影響摘要如下：

- 透過管理員的使用情況報告功能，提供應用程式使用情況
- 一般使用者的整體經驗和工作流程 (例如，完整的桌面是否能滿足使用案例的需求，還是只檢視應用程式就足夠了？)。

桌面視圖

對於在工作階段中執行所有使用者工作流程的使用案例，Desktop View 會將所有應用程式集中在一個環境中，以簡化使用者體驗。對於需要與作業系統 (OS) 整合的 3-5 個以上應用程式的部署，桌面檢視可提供更一致的使用者體驗。當維護兩個獨立且不同的環境時，桌面檢視是有效的。例如，使用者可同時存取生產環境與生產前桌面環境，以驗證版面配置、組態及應用程式存取權的變更。

AppStream 2.0 使用情況報告會建立桌面檢視的每日應用程式報告。應用程序的結果輸出只是「桌面」，直接映射到 AppStream 2.0 會話。如需詳細資訊，請參閱本文件的「監控使用者使用情況」一節。

僅應用程式檢視

當 AppStream 2.0 堆疊旨在提供一些間歇性需要的應用程式時，「僅限應用程式」檢視也會有效。在 Kiosk 環境中，可透過應用程式檢視提供安全鎖定的應用程式交付。在「應用程式檢視」中，AppStream 2.0 會以自訂的殼層取代預設的 Windows 殼層。這個自訂殼層只會顯示執行中的應用程式，將作業系統的攻擊面降到最低。

對於使用 AppStream 2.0 來擴充現有組織桌面環境的使用案例，則偏好使用「僅限應用程式」檢視。在原生應用程式模式中部署 AppStream 2.0 Windows 用戶端，藉由允許完整使用鍵盤快速鍵，將使用者混淆降到最低。

Amazon 2.0 用量報告會為應用程式檢視建立每日應用程式報告。如需更精細的應用程式報告和執行使用情況，請考慮在作業系統層級報告的協力廠商解決方案。您可以 AppLocker 在報告模式下使用 Microsoft，或考慮可用的解決方案AWS Marketplace，例如液體軟件的使用者體驗。

AWS Identity and Access Management 角色組態

如果工作負載要求 AppStream 2.0 使用者從工作階段中存取其他AWS服務，最佳做法是透過使用 AWS Identity and Access Management(IAM) 角色委派存取權。IAM 角色可以透過叢集層級的指派直接附加到最終使用者的工作階段。如需將 IAM 角色與 AppStream 2.0 搭配使用時的其他最佳做法，請參閱管理員指南的這一節。

使用靜態認證

某些工作負載可能需要 IAM 存取金鑰的靜態輸入，而不是從附加的角色繼承它們。有兩種方法可以接收這些認證。第一種方法涉及將存取金鑰儲存在AWS服務中，然後為最終使用者提供明確的 IAM 存取權，以便從服務中提取該特定值。存取金鑰儲存機制的兩個範例是使用AWS Secrets Manager或AWSSSM 參數存放區。第二種方法是使用 AppStream 2.0 認證提供者來存取連結角色的存取金鑰。這可以通過調用憑據提供程序並解析訪問密鑰和密鑰的輸出來完成。以 PowerShell 下是如何在中執行此動作的範例。

```
$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 AppStream 2.0 S3 儲存貯體

如果您的 AppStream 2.0 工作負載設定了主資料夾和/或應用程式持續性，則最佳做法是保護存放持續性資料的 Amazon S3 儲存貯體，防止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。對齊原則可以通過僅允許存儲桶訪問必要的各方來完成。

車隊自動擴展策略

了解 AppStream 2.0 執行個體

AppStream 2.0 叢集執行個體的使用者對叢集執行個體比例為 1:1。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叢集的大小。

擴展政策

AppStream 2.0 叢集是在應用程式自動調整群組中啟動的。這可讓叢集根據使用情況進行擴充，以滿足需求。隨著使用量的增加，叢集會向外擴充，而當使用者中斷連線時，叢集會重新擴充。這是透過設定資源調整政策來控制。您可以設定以排程為基礎的擴展、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 Amazon AppStream 2.0 的叢集 Auto Scaling。

步進縮放

這些原則會依目前叢集大小的百分比或特定數目的執行個體來增加或減少叢集容量。步驟擴展政策由`Capacity Utilization`、`Available Capacity`或的 AppStream 2.0 CloudWatch 指標觸發`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叢集的大小成正比。這將有助於避免擴展過慢的情況（因為您新增了少量的執行個體相對於叢集大小），或在叢集較小時發生過多的執行個體。

目標追蹤

使用此原則可指定叢集的容量使用率層級。應用程式自動調度資源會建立和管理 CloudWatch警示，以觸發擴展政策。這會增加或移除將叢集保持在指定目標值或接近指定目標值的容量。為了確保應用程式可用性，您的叢集會盡可能快地按比例擴展量度，但會逐步擴展。設定目標追蹤時，請考慮縮放冷卻時間，以確保在所需的間隔內進行擴充和縮放。

目標跟踪對高流失情況有效。流失率是指大量使用者在短時間內開始或結束工作階段的時間。您可以通過檢查車隊的 CloudWatch指標來識別流失率。您的叢集具有非零閒置容量而未變更 (或極少變更) 所需容量的期間，表示可能會發生高流失率。在高流失情況下，請設定目標追蹤原則，其中 (100 — 目標使用率百分比) 在 15 分鐘內超過流失率。例如，如果 10% 的叢集因使用者流失而在 15 分鐘內終止，請將容量使用率目標設定為 90% 以下，以抵消高流失率。

以排程為基礎的縮放

這些原則可讓您根據以時間為基礎的排程來設定所需的叢集容量。當您瞭解登入行為並可預測需求變更時，此原則就會生效。

例如，在工作日開始時，您可能會預期有 100 位使用者在上午 9:00 要求串流連線。您可以設定以排程為基礎的擴展政策，在上午 8:40 將叢集大小下限設為 100。這可讓叢集執行個體在工作日開始時建立並提供使用，並允許 100 位使用者同時連線。然後，您可以設定另一個已排程的政策，以便在下午 5:00 將叢集中調整至少 10 個。這可讓您節省成本，因為下班後的工作階段需求少於工作日的需求。

在生產環境中擴展原

您可以選擇在單一叢集中合併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。在前面的範例中，您可以將排程的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結合，有助於在立即需要容量時減少使用率層級急劇增加的影響。

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擴充或擴充的影響。擴展政策不會結束現有的串流工作階段。現有工作階段將持續不中斷，直到工作階段由使用者或叢集逾時原則結束為止。

透過 CloudWatch 指標監控 AppStream 2.0 使用情況可協助您隨著時間的推移最佳化擴展政策。例如，在初始設定期間過度佈建資源是很常見的，而且您可能會看到長時間的低使用率。或者，如果叢集佈建不足，您可能會看到高容量使用率和「容量不足」錯誤。檢閱 CloudWatch 指標可協助您調整資源調整政策，以協助減輕這些錯誤。如需詳細資訊以及您可以使用的 AppStream 2.0 擴展政策範例，請參閱擴展 Amazon AppStream 2.0 叢集。

擴展政策設計的最佳做法

結合擴展政策

許多客戶選擇將不同類型的擴展政策結合在一個叢集中，以提高 AppStream 2.0 版 Auto Scaling 的功能和靈活性。例如，您可以設定排程擴展政策，以便預期使用者開始工作日的上午 6:00，將叢集的最小值增加至少，並在使用者停止工作之前在下午 4:00 減少叢集的最小值。您可以將此排程的擴展政策與目標追蹤或步驟擴展政策結合使用，以維持特定的使用率層級，並在白天進入或縮小以處理尖峰使用量。排程擴展和目標追蹤擴展的結合，有助於在立即需要容量時減少使用率層級急劇增加的影響。

避免擴展流失

請考慮您的機隊是否可能因為您的使用案例而遭受高度流失。當大量使用者在短時間內開始然後結束工作階段時，就會發生流失。當許多使用者在登出之前，在短短幾分鐘內同時存取叢集中的應用程式時，可能會發生這種情況。

在這種情況下，您的叢集規模可能會遠低於所需容量，因為使用者結束工作階段時，執行個體就會結束。步驟擴展政策可能無法快速新增執行個體以抵消客戶流失，因此，您的叢集卡在特定大小上。

您可以通過檢查車隊的 CloudWatch 指標來識別流失率。您的叢集具有非零擱置容量而未變更 (或極少變更) 所需容量的期間，表示可能會發生高流失率。若要解決高流失情況，請使用目標追蹤擴展政策並挑選目標使用率，使 (100 — 目標使用率百分比) 在 15 分鐘內超過流失率。例如，如果有 10% 的叢集因使用者流失而在 15 分鐘內結束，請將容量使用率目標設定為 90% 或更低，以抵消高流失率。

瞭解最高佈建速率

為大量使用者管理 AppStream 2.0 叢集的客戶應考慮佈建速率限制。此限制將影響執行個AWS 帳戶體新增至叢集或.

有兩個限制需要考慮：

- 對於單一叢集，以每分鐘 20 個執行個體的最高速率佈建 AppStream 2.0。
- 對於單一 AppStream 2.0 佈建AWS 帳戶，速率為每分鐘 60 個執行個體 (每分鐘突發 100 個執行個體)。

如果 parallel 擴充超過三個叢集，則帳戶佈建速率限制會在這些叢集之間共用 (例如，六個 parallel 擴充叢集可以每分鐘佈建最多 10 個執行個體)。此外，請考慮指定串流執行個體完成佈建以回應擴展事件

的時間量。對於未加入使用中目錄網域的叢集，通常為 15 分鐘。對於加入活動目錄網域的叢集，這可能需要長達 25 分鐘的時間。

鑑於這些限制，請考慮下列範例：

- 如果您想要將單一叢集從 0 擴展到 1000 個執行個體，則需要 50 分鐘 (每分鐘 1000 個執行個體 /20 個執行個體) 才能完成佈建，然後再花 15 到 25 分鐘的時間讓使用者使用所有執行個體，總共 65-75 分鐘。
- 如果您想要同時將三個叢集從 0 擴展到 333 個執行個體 (中總共有 999 個執行個體AWS 帳戶)，則所有叢集大約需要 17 分鐘 (每分鐘 999/60 個執行個體) 才能完成佈建，然後再額外 15 分鐘讓使用者使用這些執行個體，總計 32-42 分鐘。

利用多個可用區域

為您的叢集部署選擇區域中的多個 AZ。當您為叢集選取多個 AZ 時，您的叢集可以新增執行個體以回應擴展事件的可能性。此指 CloudWatch 標 PendingCapacity 是評估叢集 AZ 設計在大型叢集部署中如何最佳化的起點。的持續值較高 PendingCapacity 可表示需要延伸水平 (跨 AZ) 縮放。如需詳細資訊，請參閱監控亞馬遜 AppStream 2.0 資源。

例如，如果 auto Scaling 嘗試佈建執行個體以增加叢集的大小，而選取的 AZ 容量不足，則 auto Scaling 會改為在您為叢集指定的其他 AZ 中新增執行個體。如需可用區域和 AppStream 2.0 設計的詳細資訊，請參閱本文件中的可用區域。

監視容量不足錯誤度量

「容量不足錯誤」是 AppStream 2.0 車隊的 CloudWatch 指標。此測量結果指定因容量不足而拒絕的階段作業要求數目。

當您變更資源調整原則時，建立 CloudWatch 警示以在發生任何容量不足錯誤時通知您很有幫助。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 AppStream 2.0 資源的詳細步驟。

連接方法

在 AppStream 2.0 中串流工作階段時，使用者有兩種可用的連線方法：

- 網頁瀏覽器存取 — 支援任何具備 HTML5 功能的瀏覽器。無需插件或下載。
- AppStream 2.0 視窗用戶端

最佳做法是考慮使用者使用案例的功能和裝置需求，以調整最能支援其需求的瀏覽器或裝置。

> **Note**
>
> AppStream 螢幕解析度小於 1024 x 768 像素的裝置不支援 2.0。

摘要功能和裝置支援

表 3 — 摘要功能和裝置支援

	網頁瀏覽器存取	AppStream 2.0 視窗用戶端
多重監視器 (高達 2k 解析度)	支援	支援
多顯示器（高達 4k 分辨率）	N/A	支援
繪圖板支持	支援*	支援
觸摸屏設備支持	支援	N/A
USB 直通裝置支援	N/A	支援
鍵盤快速鍵	支援	支援
相對滑鼠偏移量	支援	支援
檔案傳輸	支援	支援
本機印表機重新	N/A	支援
本機磁碟重新導	N/A	支援

	網頁瀏覽器存取	AppStream 2.0 視窗用戶端
網路攝影機支援	支援	支援

* 谷歌瀏覽器和火狐瀏覽器只

網頁瀏覽器存取

AppStream 2.0 Web 瀏覽器訪問允許訪問應用程序，而無需安裝專用客戶端。使用者可以使用支援的 HTML5 瀏覽器進行連線。沒有任何瀏覽器插件或擴展的要求。

Web 瀏覽器存取提供多種終端裝置作業系統和類型選擇。

AppStream 2.0 視窗用戶端

AppStream 2.0 用戶端視窗是您在電腦上安裝的應用程式。此應用程序提供了當您使用 Web 瀏覽器訪問 AppStream 2.0 時無法使用的其他功能。例如， AppStream 用戶端可讓您執行下列動作：

- 使用兩個以上的顯示器或 4K 分辨率
- 將 USB 裝置與透 AppStream 過 2.0 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
- 將列印工作從串流應用程式重新導向至連接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您與本機安裝的應用程式互動的方式大致相同

AppStream 2.0 客戶端連接模式

AppStream 2.0 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 AppStream 2.0 工作階段視窗中串流應用程式。這類似於終端使用者在 Web 瀏覽器中串流應用程式的方式。如果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)，請使用傳統模式。建議使用傳統模式的預設連線模式。傳統模式是「桌面檢視」支援的唯一模式。

- 原生應用程式模式可讓使用者以與其他本機安裝的應用程式類似的方式處理遠端串流應用程式。如果使用者習慣於使用本機安裝的應用程式，原生應用程式模式可提供順暢的體驗。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，在原生應用程式模式下，串流應用程式的圖示包含 AppStream 2.0 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切換時，建議使用原生應用程式模式。

用戶端部署與管理

使用者可以自行安裝 AppStream 2.0 用戶端，或者管理員可以透過遠端執行 PowerShell 指令碼來為其安裝 AppStream 2.0 用戶端，或使用自訂設定重新封裝 AppStream 2.0 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。如果他們的 USB 設備不合格，AppStream 2.0 將不會檢測到它，並且無法與會話共享。在他們的設備合格後，您的用戶必須在每次啟動新的流會話時與 AppStream 2.0 共享設備。

大規模部署 AppStream 2.0 用戶端時，AWS建議使用企業部署工具。企業部署工具包括 AppStream 用戶端安裝檔案和群組原則系統管理範本。

自訂網域

以程式設計方式部署 AppStream 2.0 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 SAML 2.0 IdP 部署 AppStream 2.0 中，重要的是要強調使用者存取從 IdP 開始，而不是 2.0。 AppStream 使用者不需要 AppStream 2.0 URL，因為這些 URL 是由 IdP 在驗證後提供的。因此，SAML 2.0 IdP 部署不需要自訂網域名稱。

身分驗證

使用 AppStream 2.0 時，身份驗證可以在 Amazon AppStream 2.0 之外進行，也可以作為 AppStream 2.0 服務的一部分進行。選擇 AppStream 2.0 部署的驗證方式是您設計的基本考量因素。組織針對不同的使用案例進行多個 AppStream 2.0 部署並不罕見。每個使用案例都可以有不同的驗證方法。

AppStream 2.0 有三種類型的驗證方法：

- SAML 2.0
- 使用者集區
- 程序化

確定優化方法

Amazon AppStream 2.0 的架構具有彈性，可應用於大部分的組織設計需求。決定驗證的最佳化方法時，最佳做法是考量使用服務者的目標和目的，以及組織原則和程序。

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
需要網域加入叢集執行個體	AppStream 映像上安裝的應用程式只能由加入網域的資源存取。	SAML 2.0
與 Microsoft 服務的大量集成	組織依賴於開發 Microsoft 群組原則和後端基礎結構	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多個報告和安全性程序的企業 SSO 解決方案。	SAML 2.0
智慧卡支援應用程式	智慧卡 (例如私人身分驗證和一般存取卡)，用於透過智慧卡讀卡機串流應用程式的工作階段內驗證。	SAML 2.0

範例	Description	身分驗證
臨時人員配置的季節性勞動力	一年中的幾個月，臨時工作者會被分配一小組應用程序，這些應用程序不包括內部資源來完成活動。	使用者集區
有限的 IT Support	使用者少於 50 名且 IT 人員有限的小型組織，希望消除維護身分識別提供者 (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，其中包括使用者權利和驗證，並在您的解決方案中延伸 AppStream 2.0。 *	程序化
技術展示	完全短暫的環境，展示專有技術作為解決方案導覽的一部分，無需存儲用戶信息。	程序化
互動式網站體驗	使您的網站與流媒體 Windows 應用程序進行交互。 **	程序化

* 請參閱軟體廠商：將您的應用程式交付到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 AppStream 2.0 串流工作階段。

如果您的組織的使用案例或原則未列在先前提供的範例中，最佳做法是預測 AppStream 2.0 工作流程耗用的所需結束狀態，以確保驗證解決方案不會與其衝突。

設定您的身分提供者

SAML 2.0

安全性宣告標記語言 (SAML) 2.0 是一種常見的部署選項，可讓使用者使AWS用資源。各種第三方 SAML 2.0 身分識別提供者都支援 AppStream 2.0。無論您的 AppStream 2.0 資源是否已加入網域，SAML 2.0 IdP 都會要求您使用 IAM。

由於大多數人都會為每個 SAML 應用程式 IdPs 產生具有特定 SAML 屬性的唯一 metadata.xml，因此每個 AppStream 2.0 堆疊都需要與 SAML IdP 具有信任關係的角色，以及具有單一權限的應用程式串流：串流的原則，且條件符合 SAML IdP 和 2.0 堆疊的 ARN 需求。 AppStream

AppStream 2.0 管理指南提供單一 AppStream 2.0 堆疊設計的範例組態。如需多重堆疊部署，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

AppStream 2.0 中的「使用者集區」索引標籤是小概念驗證的有效選項。最佳做法是，針對使用 AppStream 2.0 來交付生產應用程式的任何使用案例和組織，最好避免使用使用者集區。

有關使用者集區的一個重要注意事項，就是使用者的電子郵件地址區分大小寫；因此，最佳作法是確保使用者接受如何正確輸入使用者認證的教育。

流媒體網址

對於從集中式服務 (通常是 ISV) 呼叫 AppStream 2.0 資源的部署，程式設計驗證依賴應用程式來進行程式設計呼叫，以AWS動態傳遞資訊並為其使用者建立 AppStream 2.0 工作階段。使用 URL 作業建立串流 CreateStreamingURL 時，請使用 API 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權限的有效使用者或角色`appstream:CreateStreamingURL`。

建立以程式設計方式存取的原則時，最佳作法是在 [資源] 區段中指定確切的 AppStream 2.0 Stack ARN 來取代預設的 '*'，以確保存取安全。例如：

Example

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

> **Note**
>
> 您可以使用描述的堆疊 API 或 AWS CLI 快速擷取 AppStream 2.0 堆疊的 ARN。

AppStream 2.0 實例應作為泛型實例啟動。透過從應用程式傳遞給它的資訊， AppStream 2.0 執行個體會使用工作階段內容建立環境，讓使用者的動態作業。

雖然本機 GPO 可以用來指定使用者登入時的設定，但工作階段內容是在使`CreateStreamingURL`用和傳遞重要屬性 (例如客戶 ID 或資料庫連線設定) 時的最佳作法，以便在 AppStream工作階段中使用。

申請權利

AppStream 2.0 可以動態建置呈現給使用者的應用程式目錄。應用程式權利是以 SAML 2.0 屬性為基礎，或使用 AppStream 2.0 動態應用程式架構。

在大多數情況下，建議使用 SAML 2.0 以屬性為基礎的應用程式權利。要管理應用程序包交付，建議使用動態應用程序框架。

與 Microsoft 活動目錄集成

亞馬遜 AppStream 2.0 映像生成器和車隊可以與 Microsoft 活動目錄集成。這可讓您提供使用者驗證、授權的集中方法，以及將 Active Directory 群組原則套用至網域加入的 AppStream 2.0 執行個體。使用加入網域的 AppStream 叢集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用、使用者應用程式權限、漫遊設定檔、印表機存取，以及其他原則式設定。

將 AppStream 2.0 環境與使用中目錄整合時，請務必注意 AppStream 2.0 堆疊的初始驗證仍由 SAML2.0 IdP 管理。使用者成功向 IdP 驗證後，當使用者啟動工作階段時，必須輸入 Active Directory 網域的網域密碼或智慧卡驗證。

當設計將與 AppStream 2.0 搭配使用的 Active Directory 網域服務 (ADDS) 環境時，有兩個服務選項和許多可用的部署案例。此外，請確定 AppStream 2.0 網路已與您的作用中目錄網站拓撲擁有者一起檢閱。

服務選項

活動目錄也可以使用AWS管理 Microsoft 活動目錄（AD）進行部署。 AWS託管 Microsoft AD 是一個完全託管的服務，允許您運行 Microsoft 活動目錄。Microsoft 活動目錄也可以在自託管環境中使用，在 EC2 或現場部署上運行。

部署案例

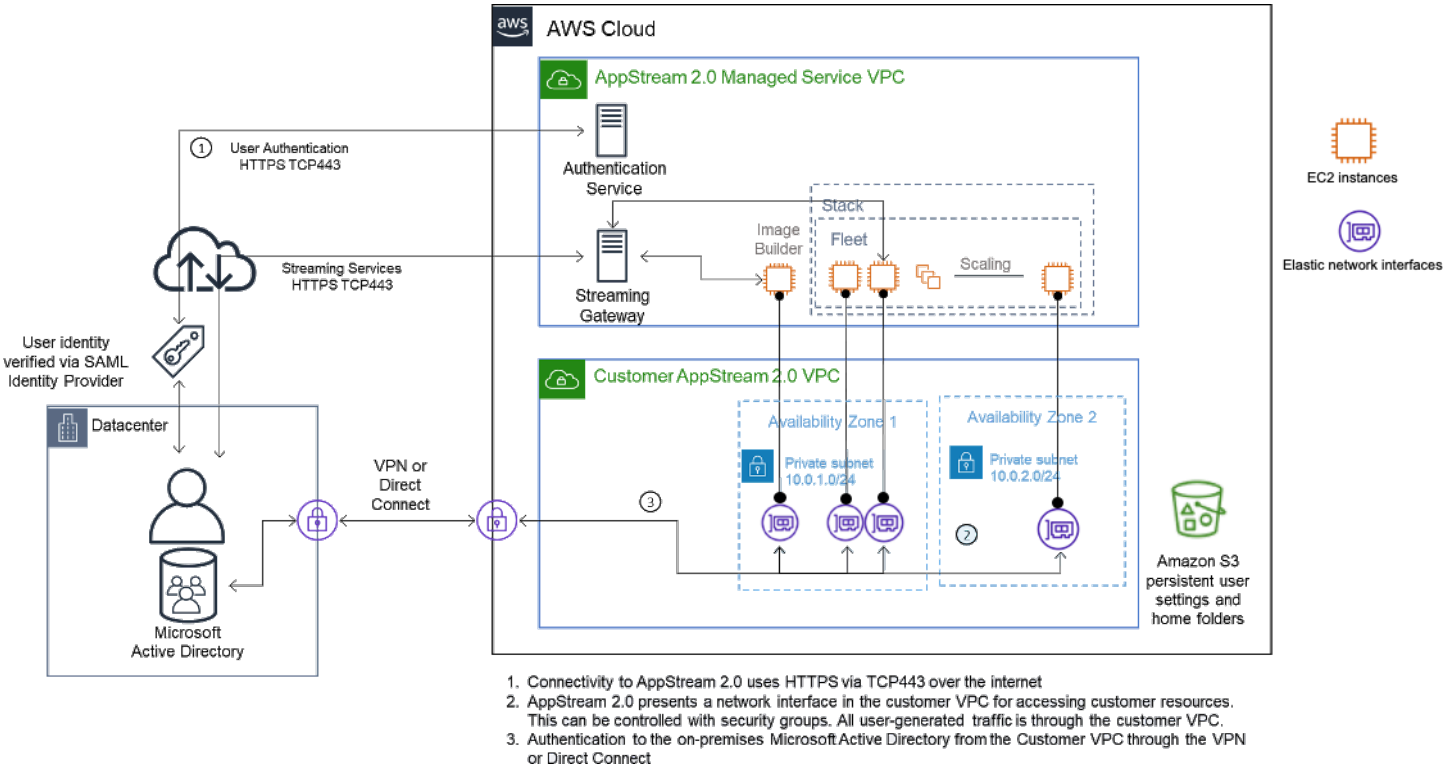
下列所列的部署案例是 AppStream 2.0 與 Microsoft 受管理 AD 或客戶自我管理的 Active Directory 的常用和建議整合選項。下面列出的所有架構圖都使用 Amazon 核心構造。

- Amazon Virtual Private Cloud (VPC) — 建立專用於 AppStream 2.0 服務的 Amazon VPC，其中至少四個私有子網路分佈在四個 AZ 中。其中兩個私有子網路用於 AppStream 叢集和映像產生器。其餘的兩個子網路會用於 EC2 或 Microsoft 受管 AD 上的網域控制站)。
- 動態主機設定通訊協定 (DHCP) 選項集 — 提供將組態資訊傳遞給將在 VPC 中佈建的 AppStream 2.0 叢集和映像產生器的標準。DHCP 選項組是在虛擬私人 VPC 層級定義的。它可讓客戶定義指定的網域名稱和 DNS 設定，以便在佈建時搭配實例化 AppStream 2.0 使用。
- AWS目錄服務 — Amazon Microsoft 受管 AD 可部署到兩個私有子網路中，這些子網路將與 AppStream 2.0 個工作負載搭配使用。
- AppStream 2.0 叢集 — AppStream 2.0 叢集或映像產生器託管於AWS受管理的 VPC 中。每個 AppStream 2.0 執行個體都有兩個彈性網路介面 (ENI)。主要介面 (`eth0`) 用於管理目的，並透過串

流閘道代理終端使用者與執行個體的連線。次要介面 (eth1) 會插入至客戶-虛擬私人雲端，可用來存取自訂 VPC 或內部部署中的其他資源。

案例 1：在內部部署的作用中目錄網域服務 (ADDS)

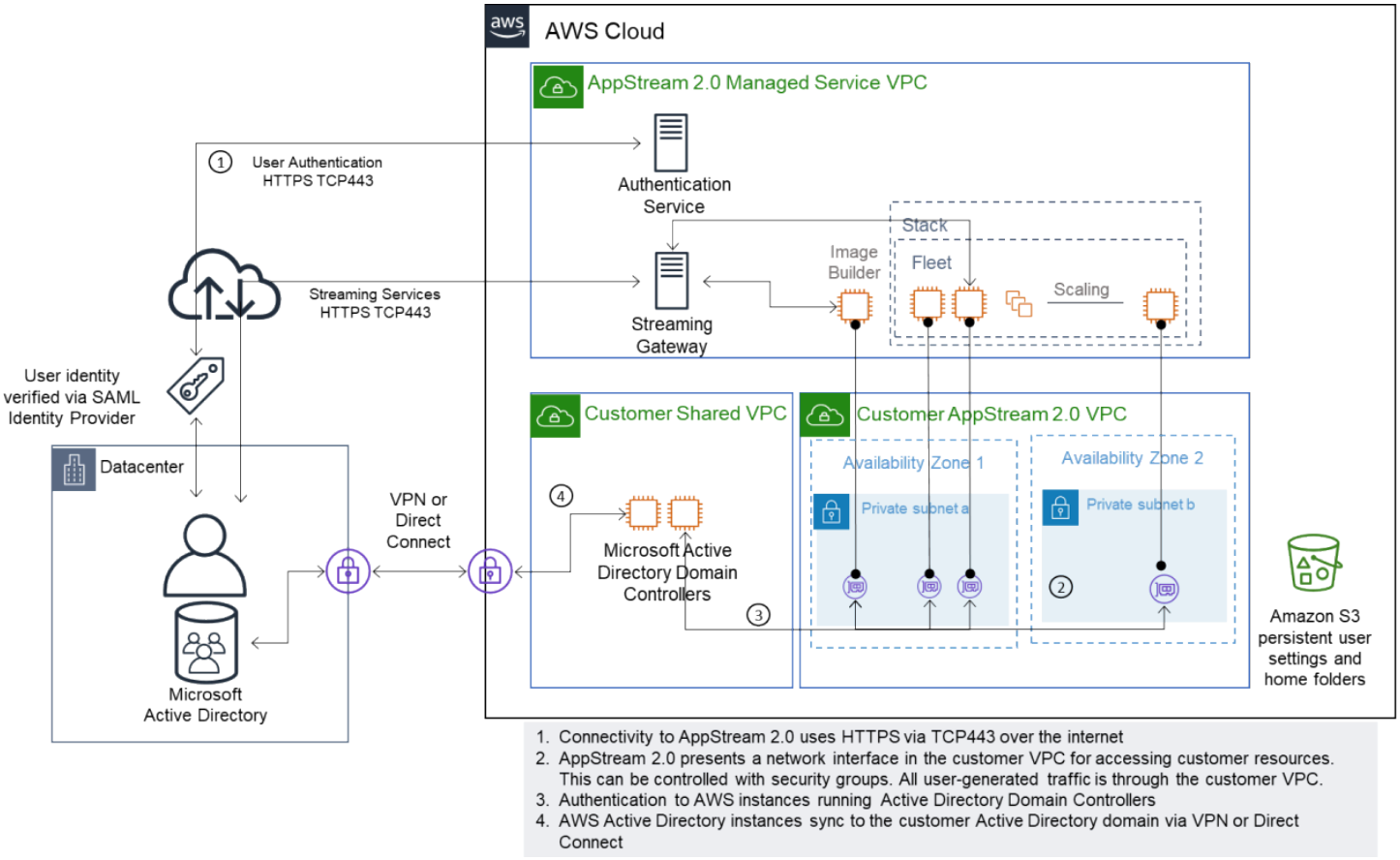
所有驗證流量都會遍歷 VPN 或「直 Connect 連線」連線，從客戶 VPC 到客戶閘道。這種情況的優點是使用可能已部署的 AD 環境，而不必在客戶 VPC 中佈建其他網域控制站的好處。缺點是唯一依賴 VPN 或直接 Connect 來驗證和授權 AppStream 2.0 機隊的用戶。如果發生任何網路連線問題，AppStream 2.0 叢集或映像產生器會受到直接影響。提供雙 VPN 通道或具有不同路徑的直接 Connect 可以減輕此潛在風險。



案例 1 — 在內部部署作用中目錄網域服務 (ADDS)

案例 2：將作用中網域服務 (ADDS) 延伸至AWS客戶 VPC

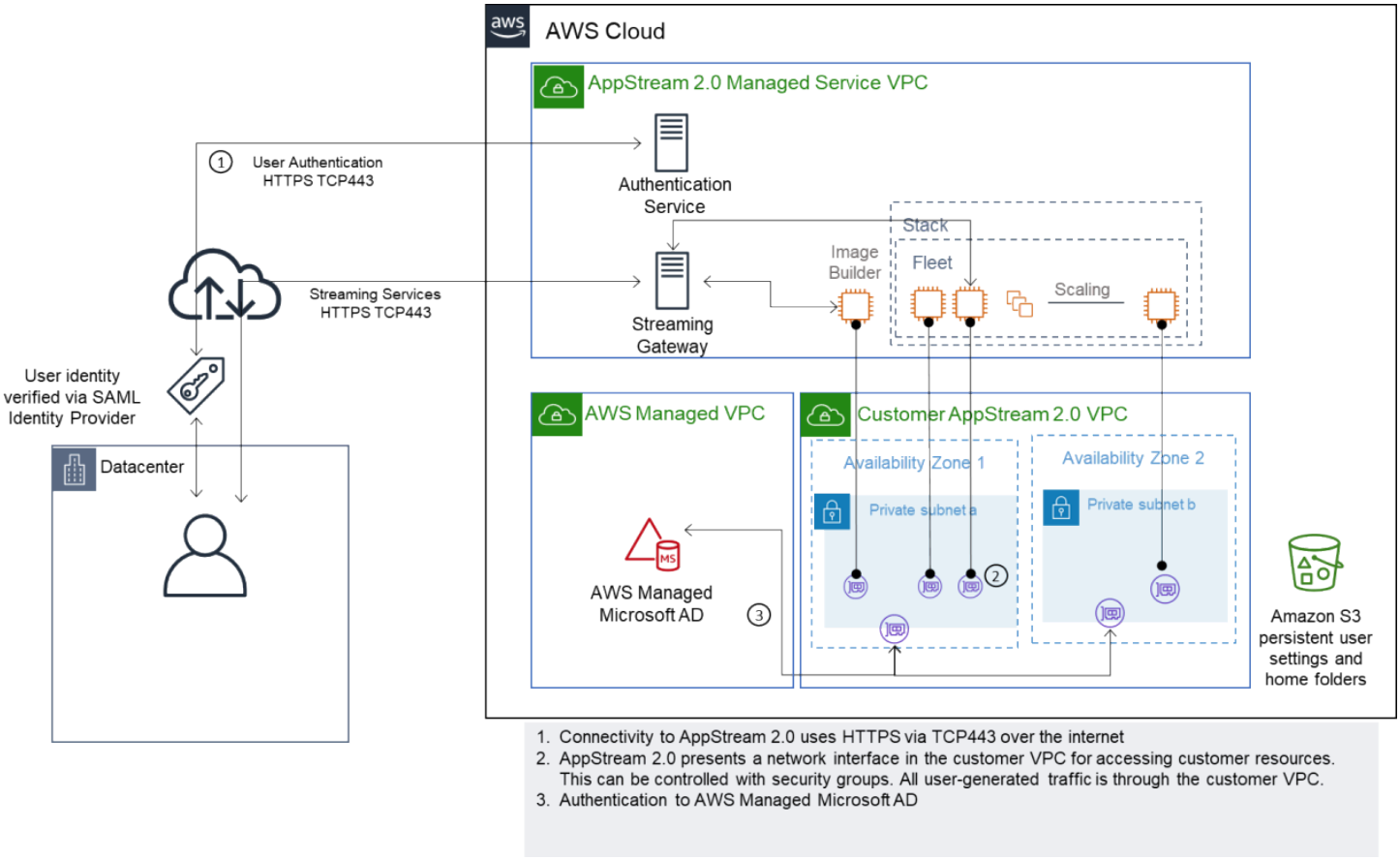
活動目錄擴展到您的客戶 VPC。應為客戶 VPC 中的新網域控制站建立使用中目錄站台。驗證流量會路由至AWS客戶 VPC 中的網域控制站，而不是周遊 VPN 或直 Connect 連線連線。



案例 2 — 將使用中網域服務延伸至AWS客戶虛擬私有雲

案例 3：AWS受管理的 Microsoft 活動目錄

AWS受管理的 Microsoft AD 部署在中，AWS 雲端並用作 AppStream 2.0 叢集和映像產生器的身分識別和資源網域。



案例 3 — AWS 受管理的使用中目錄

作用中 Directory Service 網站拓撲

使用中的目錄服務站台拓撲是您實體網路的邏輯表示法。

站台拓撲可協助您有效地路由用戶端查詢和 Active Directory 複寫流量。精心設計和維護的站台拓撲可協助您的組織達到下列優點：

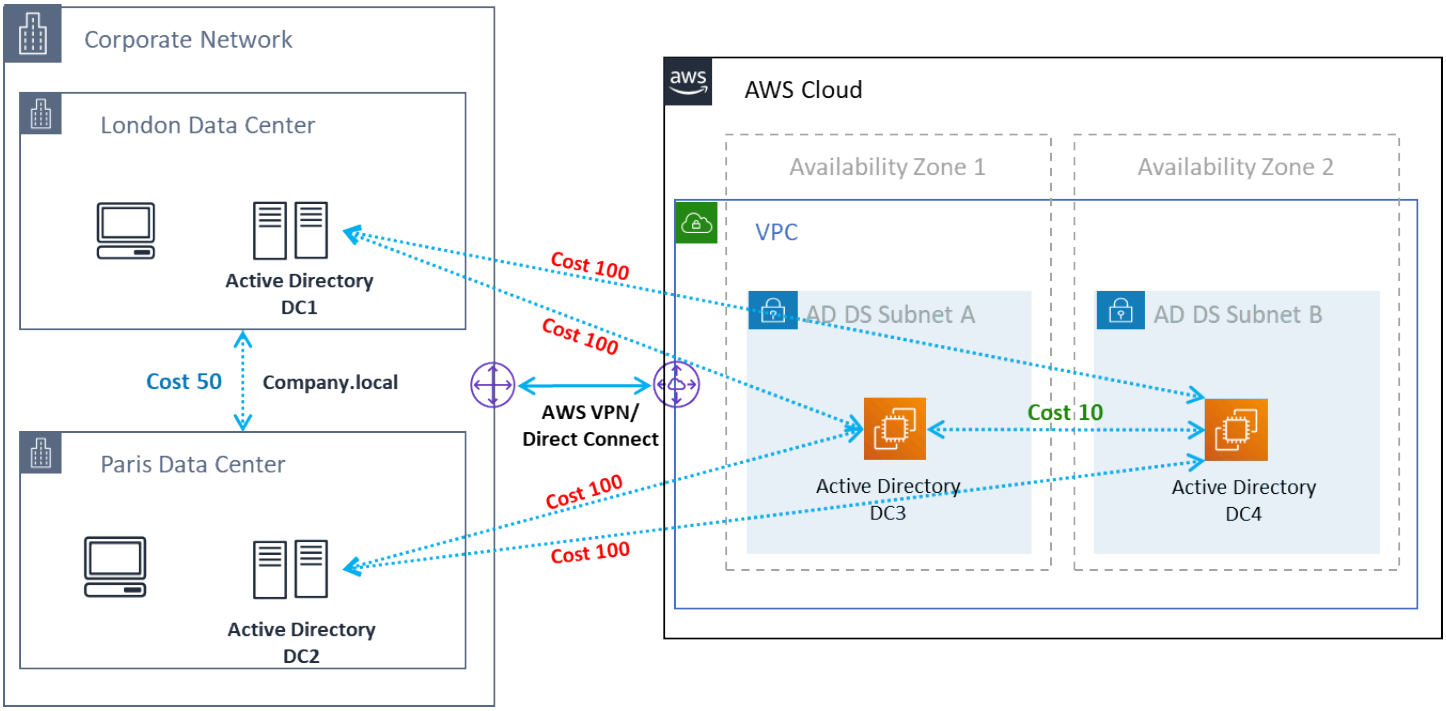
- 在內部部署和之間進行同步處理時，將複寫 Active Directory 資料的成本降到最低。AWS 雲端
- 最佳化用戶端電腦尋找最近資源 (例如網域控制站) 的能力。這有助於減少慢速廣域網路 (WAN) 連結上的網路流量、改善登入和登出程序，以及加速資源存取作業。

引入 AppStream 2.0 服務時，請確定已將用於 AppStream 2.0 執行個體子網路的位址範圍指派給您環境的正確站台。

對於案例 1 和案例 2，站台和服務是最佳使用者體驗的關鍵元件，就登入時間和 Active Directory 資源存取的時間而言。

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。

定義正確的站台拓撲可確保用戶端相似性，表示用戶端 (在此例中為 AppStream 2.0 串流執行個體) 會使用其慣用的本機網域控制站。



作用中目錄站台和服務 — 用戶端相關性

> **Tip**
>
> 最佳實務是為現場部署 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站台連結的成本範例 (成本 100)，以確保與站台無關的用戶端相似性。

若要取得有關站台拓樸的更多資訊，請參閱設計站台拓樸。

作用中目錄組織單位

AWS 建議將設定的組織單位 (OU) 存放在單一 AppStream 2.0 目錄設 Config 物件中。每個 AppStream 2.0 堆疊都擁有自己的 OU 是最佳作法。這可讓您彈性地在每個堆疊中擁有特定的 GPO。確定 OU 專用於 AppStream 2.0 電腦物件，以避免將 AppStream 2.0 特定原則與內部部署桌面混合使用。請考慮針對AWS 區域您將 AppStream 2.0 部署到的每一個使用子 OU。

活動目錄計算機對象清理

AppStream 2.0 實例是短暫的。當叢集向外擴充和擴充時，叢集會建立並重複使用 Active Directory 電腦物件。

AWS建議您建立 AD 清理程序，以刪除移除 AppStream 叢集之後可能存在的過時 Active Directory 電腦物件。

安全

雲端安全是 Amazon Web Services (AWS) 最重視的一環。安全性和合規性是 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 AppStream 2.0 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。

由於其短暫性質， AppStream 2.0 通常偏好作為應用程式和桌面交付的安全解決方案。考慮 Windows 部署中常用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。Antivirus 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（短暫）不會增加 AppStream 2.0 的整體安全性。

安全性 AppStream 2.0 的兩個關鍵問題以下列為中心：

- 持續使用者狀態超過工作階段是否為一項要求？
- 使用者在工作階段中應該擁有多少存取權？

保護持久性資料

部署 AppStream 2.0 可能需要使用者狀態以某種形式保留。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作。 AppStream 2.0 執行個體儲存是暫時性的，沒有加密選項。

AppStream 2.0 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。某些使用案例需要對使用者狀態持久性有更好的控制。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，因此最好將這些資料保留在與 AWS 區域 AppStream 2.0 機群相同的 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金鑰 AWS 管理服務（ ）中的 Amazon S3-managed加密金鑰，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 File Share 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，此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 適用於 Windows File Server	自動通過 AWS KMS	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，儲存在 S3 AWS Storage Gateway 中的所有資料都會使用 Amazon S3-Managed加密伺服器端。SSE-S3 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 加密SSL。	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以 為基礎的 Windows File Server	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

端點安全和防毒

Amazon AppStream 2.0 執行個體的短暫性質和資料缺乏持久性，意味著需要不同的方法，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。有組織政策或搭配外部資料輸入使用時，例如電子郵件、檔案傳入、外部 Web 瀏覽時，Endpoint Security 代理程式會安裝在 AppStream 2.0 映像中。

移除唯一識別碼

Endpoint Security 代理程式可能具有全域唯一識別碼（GUID），必須在機群執行個體建立過程中重設。供應商在映像中安裝其產品的指示，可確保為每個從映像產生的執行個體GUID產生新的 。

若要確保GUID未產生 ，請先安裝 Endpoint Security 代理程式作為最後一個動作，再執行 AppStream 2.0 Assistant 來產生映像。

效能最佳化

Endpoint Security Vendors 提供最佳化 AppStream 2.0 效能的交換器和設定。這些設定會因廠商而異，您可以在其文件中找到，通常是在 的 區段中VDI。某些常見設定包括但不限於：

- 關閉開機掃描，以確保執行個體建立、啟動和登入時間最小化
- 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最佳化的 IO 設定
- 應用程式為確保效能所需的排除項目

端點安全供應商提供與虛擬桌面環境搭配使用的指示，以最佳化效能。

- 趨勢科技 Office Scan Support for Virtual Desktop Infrastructure - Apex One/OfficeScan（trendmicro.com）
- CrowdStrike 以及如何在資料中心安裝 CrowdStrike Falcon
- Sophos 和 Sophos 中央端點：如何在黃金映像上安裝 ，以避免重複的身分，以及 Sophos 中央：在虛擬桌面環境中安裝 Windows 端點時的最佳實務
- McAfee McAfee 在虛擬桌面基礎設施系統上佈建和部署 和 代理程式
- Microsoft Endpoint Security 和為非持久性VDI機器設定 Microsoft Defender Antivirus - Microsoft Tech Community

掃描排除項目

如果在 AppStream 2.0 執行個體中安裝安全軟體，則安全軟體不得干擾下列程序。

表 6 — AppStream 2.0 處理安全軟體時，不得干擾下列程序。

服務	Processes
AmazonCloudWatchAgent	"C：\Program Files\AmazonAmazonCloudWatchAgent\start-amazon- cloudwatch-agent.exe"

服務	Processes
AmazonSSMAgent	"C：\Program Files\AmazonSSM\amazon-ssm-agent.exe"
NICE DCV	"C：\Program FilesNICE\DCV\Server\bin\dcvserver.exe" "C：\Program Files\NICE\DCV\Server\bin\dcvagent.exe"
AppStream 2.0	"C：ProgramFiles\Amazon\AppStream2StorageConnector\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

如果在 AppStream 2.0 執行個體中安裝安全軟體，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 AppStream 2.0 都會建立新的唯一執行個體。執行個體將具有唯一的名稱，並將在端點安全管理 condoles 中建置。將超過 4 天（或更短時間，視 AppStream 2.0 工作階段逾時而定）的未使用過時機器設定為刪除，可將主控台中過期執行個體的數量降至最低。

網路排除項目

AppStream 2.0 管理網路範圍（198.19.0.0/16）和下列連接埠和地址不應被 AppStream 2.0 執行個體內的任何安全/防火牆或防毒解決方案封鎖。

表 7 — AppStream 2.0 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	這用於在 AppStream 2.0 之前管理串流執行個體
8443	這用於在 AppStream 2.0 之前管理串流執行個體
53	DNS

表 8 — AppStream 2.0 受管服務解決安全軟體不得干擾

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 AppStream 工作階段

限制應用程式和作業系統控制項

AppStream 2.0 可讓管理員指定可以在應用程式串流模式下從網頁啟動哪些應用程式。不過，這並不保證只能執行指定的應用程式。

Windows 公用程式和應用程式可以透過作業系統透過 additional means. AWS recommends 使用 Microsoft AppLocker 啟動，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 從 AppStream 2.0 取得的應用程式存取權 AppLocker 詳述於 AppStream 管理指南。

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 AppStream 2.0 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（ ）的現有指派。啟動新映像建置器時，或建立新機群安全群組時，您最多可以關聯五個安

全群組，最多可以有五個來自現有安全群組 的指派。針對每個安全群組，您可以新增規則，以控制來自執行個體的傳出和傳入網路流量

NACL 是您的選用安全層VPC，可做為無狀態防火牆，用於控制一或多個子網路的進出流量。您可以設定ACLs具有類似安全群組之規則的網路，以便將額外的安全層新增至您的 VPC。如需安全群組與網路之間差異的詳細資訊ACLs，請參閱比較安全群組和第 NACLs 頁。

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

對於具有將內部部署環境連線至 AWS（透過 AWS Direct Connect）的高速私有網路的客戶，您可以考慮使用 的VPC端點 AppStream，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。如需此主題的詳細資訊，請參閱本文件的 AppStream 2.0 串流介面VPC端點一節。

資料外洩防護

我們將探討兩種資料外洩預防。

用戶端至 AppStream 2.0 執行個體資料傳輸控制項

表 9 — 控制資料輸入和輸出的指引

設定	選項	指引
剪貼簿	• 僅複製並貼上至遠端工作階段 • 僅複製到本機裝置 • 已停用	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，以將資料洩漏的可能性降至最低。
檔案傳輸	• 上傳和下載 • 僅上傳 • 僅下載 • 已停用	避免啟用此設定以防止資料洩漏。
列印至本機裝置	• 已啟用 • 已停用	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。

考量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面的安全資料傳輸解決方案。

控制來自 AppStream 2.0 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 AppStream 2.0 執行個體內時可以存取的內容。網路結束（或輸出）路徑是什麼樣子？ 一般要求使用者在其 AppStream 2.0 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。其他考量事項包括本機防毒應用程式和 AppStream 執行個體內部的其他端點安全措施（如需詳細資訊，請參閱「端點安全性和防毒」一節）。

使用 AWS 服務

AWS Identity and Access Management

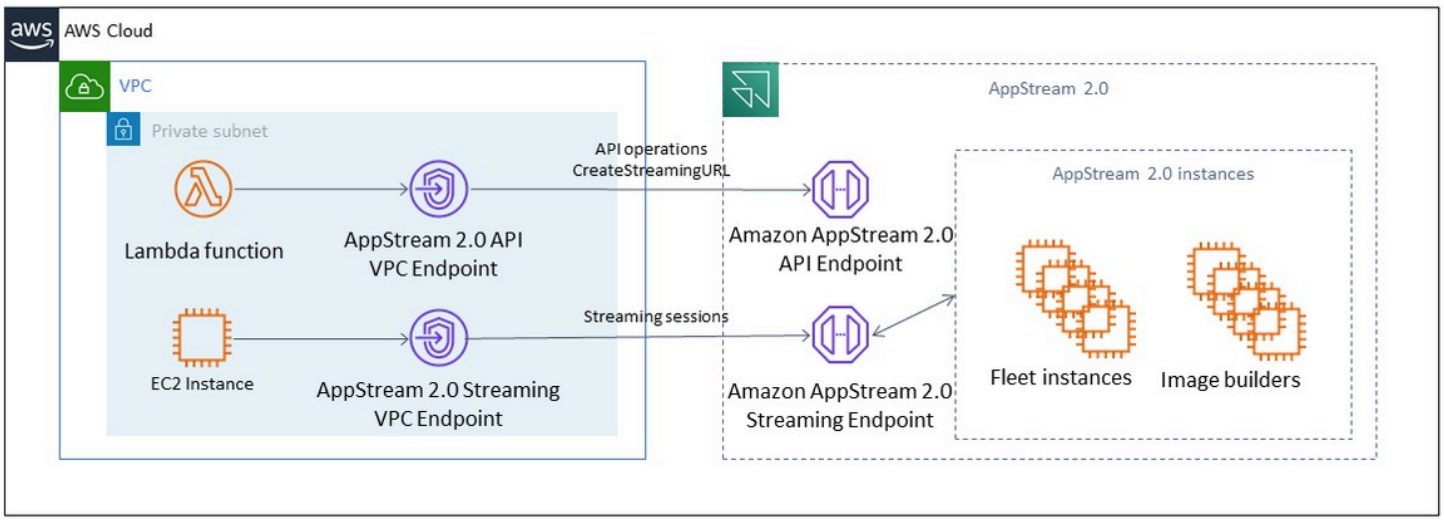
使用 IAM角色來存取 AWS 服務，並在附加到它的IAM政策中具體化，是最佳實務，僅提供 AppStream 2.0 工作階段中的使用者存取，而無需管理其他憑證。遵循將IAM角色與 AppStream 2.0 搭配使用的最佳實務。

建立IAM政策以保護為在主資料夾和應用程式設定持久性中保留使用者資料而建立的 Amazon S3 儲存貯體。這可防止非 AppStream 2.0 管理員存取。

VPC 端點

VPC 端點可讓您在 VPC 和 支援的 AWS 服務與由 支援的 VPC 端點服務之間進行私有連線 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。您的 VPC與其他 服務之間的流量不會離開 Amazon 網路。如果僅 AWS 服務需要公有網際網路存取，VPC端點會完全移除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API呼叫 AppStream 2.0 的環境中，為 AppStream 2.0 API操作建立介面VPC端點。例如，如果私有子網路EC2中有執行個體沒有公有網際網路存取，則 AppStream 2.0 的VPC端點API可用來呼叫 AppStream 2.0 API操作，例如 CreateStreamingURL。下圖顯示 Lambda 函數API和EC2執行個體使用 AppStream 2.0 和串流VPC端點的範例設定。



VPC 端點

串流VPC端點可讓您透過VPC端點串流工作階段。串流介面端點會在您的 中維護串流流量VPC。串流流量包括像素、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 AppStream 2.0 堆疊上啟用VPC端點設定。這可做為從網際網路存取有限，且將受益於透過 Direct Connect 執行個體存取之位置透過公有網際網路串流使用者工作階段的替代方案。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 AppStream 2.0 運作所需的 Web 資產。

若要進一步了解如何使用 AppStream 2.0 限制流量至 AWS 服務，請參閱從VPC端點建立和串流的管理指南。

當需要完整公有網際網路存取時，最佳實務是在 Image Builder 上停用 Internet Explorer 增強型安全組態（ESC）。如需詳細資訊，請參閱 AppStream 2.0 管理指南，以停用 Internet Explorer 增強型安全組態。

災難復原

Amazon AppStream 2.0 已內建多達三個可用區域的備援功能。這表示，如果使用者在可用區域中的作用中工作階段變得降級，他們可以簡單地中斷連線並重新連線，假設您有容量，就會在健全的可用區域中保留工作階段。雖然這在區域內提供高可用性，但如果服務在地區層級遇到問題，則不會提供災難復原解決方案。

若要為 AppStream 2.0 使用者提供災難復原計畫，您首先需要在次要區域建置 AppStream 2.0 環境。從設計的角度來看，這個環境應該具有與您的內部部署環境的冗餘連接（如果適用），並且不應該依賴於主要區域。例如，如果您的 AppStream 2.0 叢集已加入網域，您應該在次要區域中有其他網域控制站，且已設定網站和服務。從 AppStream 2.0 的角度來看，此環境應包含您在主要區域中擁有的相同叢集和堆疊設定。車隊本身應該運行相同的基本映像，可以通過控制台或以編程方式將其複製到輔助區域。如果在 AppStream 2.0 工作階段中執行的應用程式具有與您的主要區域相關聯的後端相依性，該後端相依性也應該具有區域備援，以確保使用者在主要區域停止運作時仍可存取應用程式的後端。目的地區域的服務等級限制應符合您的主要地區。

身分路由

有兩種不同的方法可以在 DR 案例中提供對應用程式的存取權。在高層級上，這兩種方法會因為將使用者導向至容錯移轉區域的方式而有所不同。第一種方法是使用 IdP 中的單一 AppStream 2.0 應用程式組態來執行，而第二種方法則具有兩個獨立的應用程式組態。

方法 1：變更應用程式的中繼狀態

當使用者從身分識別提供者 (IdP) 登入 AppStream 2.0 時，在驗證之後，他們會轉送至與區域對齊的特定 URL，以及要存取的堆疊。如需有關轉送狀態 URL 的詳細資訊，請參閱 Amazon AppStream 2.0 管理指南。系統管理員可以設定建置在與主要區域相同 AppStream 2.0 映像上的跨區域堆疊，以便使用者容錯移轉至。系統管理員只要將轉送狀態 URL 更新為指向容錯移轉堆疊，即可控制此容錯移轉。若要讓此方法正常運作，相關聯的 IAM 政策將需要反映對這兩個堆疊的存取權，包括主要和容錯移轉。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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "appstream:Stream",
```

```
            "Resource": [
            "arn:aws:appstream:PrimaryRegion:190836837966:stack/StackName",
            "arn:aws:appstream:FailoverRegion:190836837966:stack/StackName"
            ],
            "Condition": {
                "StringEquals": {
                    "appstream:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

方法 2：在 IdP 中設定兩個 AppStream 2.0 應用程式

此方法需要管理員在 IdP 內為 AppStream 2.0 建立兩個獨立的應用程式。然後，它們可以同時顯示這兩個應用程序，並讓用戶選擇去哪裡，或者他們鎖定/隱藏應用程序，直到它的時間容錯移轉。這種方法更好地與經常移動的全局用戶的用例一致。這些用戶應該從最近的端點進行流式傳輸，因此兩個應用程序都分配給他們可以選擇為其最近的區域配置的應用程序的選項。這也可以自動化，有關更多信息，請參閱此博客文章。

儲存持續性

利用 AppStream 2.0 隨附的資料持續性功能 (例如「應用程式持續性」和「主資料夾同步處理」) 時，您需要將該資料複寫到容錯移轉區域。這些功能會將持續性資料存放在指定 AppStream 2.0 區域的 Amazon S3 儲存貯體中。若要讓資料跨區域保存，您需要將來源儲存貯體上的所有變更複寫到容錯移轉區域 AppStream 2.0 儲存貯體。這可以使用 Amazon S3 原生功能來完成，例如 Amazon S3 跨區域複寫。每個用戶持久性數據將駐留在其哈希用戶名的文件夾下。由於使用者名稱會在相同的跨區域進行雜湊處理，因此只要複製資料就能在次要區域中提供資料持續性。如需 AppStream 2.0 所使用之 Amazon S3 儲存貯體的詳細資訊，請參閱本指南。

監控

使用儀表板

監控叢集使用率是一種常規活動，可透過 CloudWatch 指標執行並建立儀表板。或者，從 AppStream 2.0 主控台，使用 [叢集使用量] 索引標籤。定期監控您的車隊使用情況，因為使用者行為並不總是可預測，而且需求甚至可能超過一流的前期規劃。 CloudWatch 您可以在監控資源下的 AppStream 2.0 管理指南中找到 AppStream 2.0 個指標和維度的完整清單。

預期增長

每當有一個大的跳躍`PendingCapacity`，就會發生 auto 縮放事件。請務必確認`AvailableCapacity`並`PendingCapacity`具有反向關係，同時新的 AppStream 2.0 叢集執行個體可供託管使用者工作階段使用。為每個 AppStream 2.0 叢集建立 CloudWatch 警示，以通知管理員，以確保自動調整規模不會落後`InsufficientCapacityError`於需求。

如果需求超過容量且`InsufficientCapacityError`測量結果值很常見，請考慮透過「排程擴展」政策在工作日開始時提高最小容量。此外，使用第二個「排程擴展」政策，以便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。在工作日結束之前降低最小容量，可以透過降低的值來有效地擴展功能`ActualCapacity`。這樣可以最佳化成本。

如果需求始終無法預測，請使用 Target Tracking 擴展政策來確保 AppStream 2.0 叢集`AvailableCapacity`中有足夠的滿足需求，同時確定使用模式。繼續監控，因為目標追蹤使用的叢集耗用量百分比。隨著叢集執行個體總數的增加，未使用的叢集執行個體總數會相乘。除非將最大容量設置為保守值，否則這可能會變得浪費。使用多種類型的擴展政策 (例如「排程」和「目標追蹤」)，在可靠性與成本最佳化之間取得平衡。

監控使用者使用

監控獨特的用戶，因為有相關的成本，在用戶費的形式。此使用者費用是由影像助理 (RDS) 使用者存取授權 (SAL) 所產生的。評估唯一使用者可透過執行驗證的 IdP 報告，或透過使用情況報告來執行。

使用情況報告會以個別`.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) 工具下載和分析這些檔案。您可以在中分析使用情況資料， AWS 而無需下載報告，也可以在自訂日期範圍內建立報告，而無需串連多個`.csv`檔案。例如，您可以使用 Amazon Athena 和 Amazon QuickSight 為 AppStream 2.0 使用量資料建立自訂報告和視覺效果。

保存應用程式和 Windows 事件記錄檔

當 AppStream 2.0 執行個體工作階段完成時，執行個體就會結束。這表示工作階段中使用的所有應用程式和 Windows 事件記錄檔都會遺失。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 資料 Firehose 將它們即時交付到 S3，並使用 Amazon OpenSearch 服務 (服 OpenSearch 務) 進行搜尋。如果預計不會頻繁查詢，為了優化成本，請使用 Amazon Athena 進行搜索，而不是運行 Amazon OpenSearch 服務。

稽核網路與行政活動

如果尚未設定，最佳做法是 AWS 帳戶 使用 Amazon AppStream 2.0 AWS CloudTrail進行配置。若要特別稽核 AppStream 2.0 API 呼叫，請使用值為的篩選器事件來源`appstream.amazonaws.com`。

啟用 VPC 流程記錄，以稽核對客戶管理資源的存取。VPC 流程記錄可以發佈至 CloudWatch 記錄檔，以便在需要稽核時執行查詢。

隨著 AppStream 2.0 個叢集的成長，監控子網路 IP 配置非常重要。透過執行描述子網路 CLI 來報告指派給叢集的每個子網路中可用的 IP 位址，以報告 IP 指派。確保您的組織擁有足夠的 IP 位址容量，以滿足以最大容量執行的所有叢集的需求。

成本最佳化

成本優化著重於避免不必要的成本。關鍵主題包括了解和控制花錢的位置，以及選擇最合適和正確的資源類型數量。分析隨時間推移的支出並擴展以滿足業務需求。以下 AppStream 2.0 資源會產生 pay-as-you-go 費用：

- 永遠在線的叢集執行個體
- 隨需叢集實例
- 隨需停止執行個體費
- 映像建置器執行個體
- 使用者費用

如需目前的定價資訊，請參閱AWS網站以瞭解 Amazon AppStream 2.0 定價。

設計具成本效益的 AppStream 2.0 部署

規劃和設計 AppStream 2.0 部署的第一步是使用簡單的定價工具來估算與使用量相關的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、執行個體類型和叢集使用率，而定價工具會估算每位使用者的價格。當您使用隨需叢集而非永遠在線的叢集時，它也會顯示預估節省的價格。

客戶喜歡 AppStream 2.0 定價模式，只需為佈建的執行個體付費，以滿足使用者的串流需求。此模型與現有的應用程式串流環境不同。這些通常是以尖峰容量佈建為基礎，即使在夜間、週末和節假日，當負載較低時也是如此。Amazon AppStream 2.0 定價工具僅提供與您使用 AppStream 2.0 相關的 AWS 費用估算，不包括任何可能適用的稅金。您的實際費用取決於各種因素，包括 AWS 服務的實際使用情況。

AppStream 2.0 定價工具是以 Microsoft Excel 或 OpenOffice Calc 試算表的形式提供，可讓您輸入叢集的基本資訊，然後根據您的使用模式，為隨需和永遠在線的叢集提供 AppStream 2.0 環境的成本估算。您可以根據歷史或預期的使用趨勢來模擬成本。透過內建這些功能，Elastic 叢集可讓管理員免除預測使用情況、建立、維護擴展政策和映像的需求。執行 Amazon Linux 2 的彈性叢集和執行個體 (所有叢集類型) 按串流工作階段的持續時間計費，以秒為單位，最少 15 分鐘。

透過選擇執行個體類型來優化成本

對於叢集和映像產生器執行個體，您可以為應用程式選擇一系列不同的執行個體系列和類型。

一般使用者測試 — 下一步是將 AppStream 2.0 叢集推出給一群試驗使用者進行測試，以驗證我們選擇的執行個體類型。請務必要求試驗使用者測試其所有常規和繁重的工作流程，以擷取記憶體、CPU 和圖形周圍的指標，以便擷取基準效能指標。試驗群組應包含使用應用程式的各種使用者角色，以確保您是從多個使用者經驗中進行測試。使用者接受度測試可讓您收集串流工作階段體驗的意見反應。建立或更新堆疊時，可以選擇使用自訂意見反應 URL。使用者選擇 [傳送意見反應] 連結以提交有關其應用程式串流體驗的意見反應之後，就會被重新導向至 如果發生效能瓶頸，請使用 Windows 效能測量結果來分析資源限制條件。例如，如果目前的叢集執行個體類型 stream.standard.medium 顯示資源限制，請將執行個體類型升級為串流 .standard.large。相反地，如果效能指標顯示資源使用率過高，請考慮降級執行個體類型。

通過車隊類型選擇優化成本

建立新的 AppStream 2.0 叢集時，開發人員必須選擇永遠開啟或隨選叢集類型。從定價角度選擇執行個體類型時，了解 AppStream 2.0 如何管理叢集執行個體非常重要。對於永遠在線的叢集，叢集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，叢集執行個體隨時可以開始串流工作階段。

對於隨需叢集，叢集執行個體啟動後，它們會保持在停止狀態。停止的執行個體費用低於執行中執行個體費用，有助於降低成本。隨需叢集執行個體必須從停止狀態啟動。使用者必須等待大約兩分鐘，才能使用串流工作階段。

彈性叢集是獨立應用程式的最佳選擇，可安裝到儲存在 Amazon Simple Storage Service (Amazon S3) 貯體中的虛擬硬碟。由於僅在串流期間每秒計費，彈性叢集可能會進一步降低某些使用案例的成本。費率是您在建立叢集時選擇的執行個體類型、大小以及作業系統的函數。

如果使用者在工作時間需要叢集執行個體，最好保留相同的串流工作階段。這是因為叢集執行個體按小時計費，而且每次新的串流工作階段啟動時，會產生另一個叢集執行個體費用。

表十- AppStream 2.0 車隊類型比較

艦隊類型	優點	考量
永遠在線	減少串流工作階段的等待時間	使用者需支付每小時執行個體費用，因為無法讓執行個體保持停止狀態。
按需求	執行個體保持在停止狀態時節省成本	更長的串流工作階段等待時間

艦隊類型	優點	考量
彈性	對於可以安裝在虛擬硬碟上的應用程式具有零星使用模式的使用案例，每秒計費可能很有用	隨著應用程序虛擬硬盤的大小變大，將其掛接到流實例所花費的時間可能會很長

AppStream 2.0 會監控您的車隊使用率，並自動調整車隊容量，以盡可能低的成本滿足您的使用者需求。容量調整是根據您定義的擴展政策，根據目前的使用率或根據排程進行。定期檢閱叢集使用量指標，以驗證叢集擴展政策沒有高層級的備用容量。

擴展政策

Fleet Auto Scaling 可讓您不必過度認可等待使用者登入的資源，從而最佳化叢集資源。管理員可以根據不同的使用率調整叢集的大小，以符合使用者的需求。使用 CloudWatch AppStream 2.0 叢集指標或第三方監控工具來瞭解使用者活動，並設定擴展政策，以根據預期使用情況擴充或縮小 AppStream 2.0 叢集。用戶日誌是了解實際使用情況的重要機制。透過 Auto Scaling，您可以使用此深入分析資料來動態變更叢集大小。

在許多情況下， AppStream 2.0 車隊是根據最大用戶數量創建的，而不是針對一天和一周中的不同時間（例如夜晚和周末）進行調整。串流應用程式的並行使用者人數通常會少於使用者總數，尤其是當使用者具備遠端工作彈性時。在投影使用模式時考慮到這些因素是非常重要的。高估計時會導致超額佈建 AppStream 2.0 個執行個體，導致額外成本。若要達到最佳組態，您可能需要將一或多個排程擴充政策與向外延展政策結合。

若要進一步了解實作擴展政策，請參閱擴展 Amazon AppStream 2.0 叢集。

使用者費用

使用者從 AppStream 2.0 叢集執行個體串流應用程式時，每AWS 區域個使用者每月收取使用者費用。為 AppStream 2.0 使用者提供一致的使用者 ID，而不是產生不同的使用者 ID。連線至映像產生器時，不會收取使用者費用。

學校、大學和某些公共機構可能有資格獲得每位使用者每月 0.44 USD 的 Microsoft RDS SAL 使用者費用降低。如需資格需求，請參閱 Microsoft 授權條款與文件。

如果您擁有 Microsoft 授權行動性，您可能有資格攜帶自己的 Microsoft RDS 用戶端存取授權 (CAL)，並將其與亞馬遜 AppStream 2.0 搭配使用。如果您擁有自己的授權，就不會產生每月使用者費用。如

需有關是否可以將現有的 Microsoft RDS CAL 授權與 Amazon AppStream 2.0 搭配使用的詳細資訊，請參閱AWS授權行動性指南，或洽詢您的 Microsoft 授權代表。

Image Builder 使用

AppStream 2.0 Image Builder 執行個體按小時計費。Image Builder 執行個體費用包括串流通訊協定使用的運算、儲存和任何網路流量。所有正在執行的 Image Builder 執行個體都會收取適用的執行中執行個體費 這筆費用是根據執行個體類型和大小計算的，即使沒有管理員連線也是如此。

最佳做法是將成本最佳化，請在未使用 Image Builder 執行個體時關閉該執行個體。 CloudWatch 事件規則可用於排程每日工作，例如叫用 Lambda 函數來停止映像產生器執行個體。

您可以使用受管理的 AppStream 2.0 映像更新 up-to-date 來保留 AppStream 2.0 映像檔。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 AppStream 2.0 代理程式軟體。使用此方法更新映像時，Image Builder 會在受管理的服務程序中自動啟動和停止。

結論

借助 AppStream 2.0，您可以輕鬆地將現有的桌面應用程序添加到AWS並使用戶能夠立即流式傳輸它們。Windows 使用者可以使用 AppStream 2.0 用戶端或具備 HTML5 功能的網頁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。您的應用程式在運AWS算資源上執行，而且資料永遠不會儲存在使用者的裝置上，這表示它們永遠都能獲得高效能、安全的體驗。

與傳統的桌面應用程式串流內部部署解決方案不同， AppStream 提供 pay-as-you-go 定價，無需前期投資，也無須維護基礎架構。您可以立即和全球擴展，確保您的用戶始終擁有出色的體驗。

Amazon AppStream 2.0 旨在整合到現有的 IT 系統和程序中，而本白皮書描述了執行此操作的最佳實務。遵循本白皮書中指導方針的結果是符合成本效益的雲端桌面部署，可隨著您的企業在AWS全球基礎架構上安全地擴充。

貢獻者

本文件的貢獻者包括：

- 安德魯伍德，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 AppStream 2.0 管理指南
- Amazon AppStream API 參考
- 使用適用於 FSx for Windows File Server 和 FSLogix 的 Amazon FSx 來優化 Amazon 2.0 上的應用程式設定持續性 AppStream
- 使用 Amazon ElasticSearch 和 Amazon Firehose 監控 Amazon AppStream 2.0
- 使用 Amazon 雅典娜和 Amazon 分析您的亞馬遜 AppStream 2.0 使用量 QuickSight
- 擴展您的 Amazon AppStream 2.0 車隊
- 使用 Microsoft 管 AppLocker 理 Amazon AppStream 2.0 上的應用程序體驗
- 使用自定義域與 Amazon AppStream 2.0
- 如何在 AppStream 2.0 中使用我自己的 Microsoft RDS CAL？
- Amazon AppStream 2.0 定價工具
- 使用 AppStream 2.0 建立線上軟體試用
- 使用 Amazon AppStream 2.0 創建一個 SaaS 門戶

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。