aws

管理員指南

Amazon WorkSpaces 精簡型客戶端

Amazon WorkSpaces 精簡型客戶端: 管理員指南

Table of Contents

什麼是 Amazon WorkSpaces 精簡型客戶端管理員主控台？

透過 Amazon WorkSpaces 精簡型客戶端管理員主控台，管理員可以透過 WorkSpaces 精簡型客戶端入口網站管理 WorkSpaces 精簡型客戶端環境和裝置。管理員可以透過此 Web 主控台，為其網路中的 WorkSpaces 精簡型客戶端使用者建立環境、管理裝置及設定參數。

您用於 WorkSpaces 精簡型客戶端的虛擬桌面環境必須在自己的主控台內建立或修改。

> **Important**
>
> 若要讓 WorkSpaces 精簡型客戶端管理員主控台正常運作，您的系統必須先符合特定需求。這些要求會列在先決條件和組態中。

主題

您是第一次使用 的新手嗎？

如果您是首次使用 WorkSpaces 精簡型客戶端管理員主控台，建議您從閱讀下列章節開始：

- 啟動 WorkSpaces 精簡型用戶端管理員主控台
- 使用 WorkSpaces 精簡型客戶端管理員主控台

Architecture

每個 WorkSpaces 精簡型客戶端都與虛擬桌面界面 (VDI) 供應商相關聯。WorkSpaces 精簡型客戶端支援三個 VDI 供應商：

- Amazon WorkSpaces
- WorkSpaces 應用程式
- Amazon WorkSpaces 安全瀏覽器

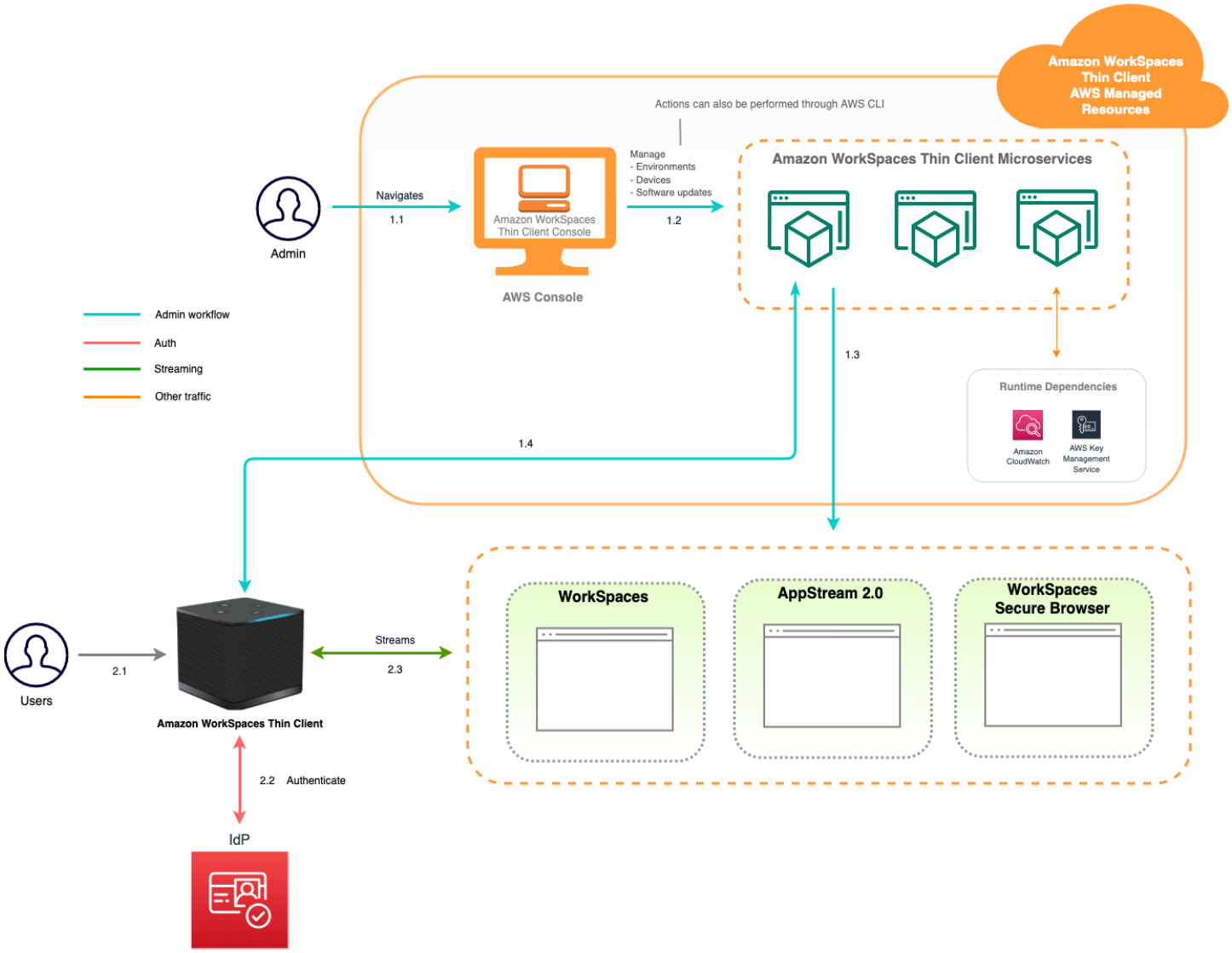
根據使用的 VDI，WorkSpaces 精簡型客戶端的資訊會透過 WorkSpaces 的目錄、WorkSpaces 應用程式的堆疊和 WorkSpaces 安全瀏覽器的 Web 入口網站端點進行存取和管理。

如需 Amazon WorkSpaces 的詳細資訊，請參閱開始使用 WorkSpaces 快速設定。目錄是透過 管理 Directory Service，提供下列選項：Simple AD、AD Connector 或 Directory Service for Microsoft Active Directory，也稱為 AWS Managed Microsoft AD。如需詳細資訊，請參閱 Directory Service 管理員指南。

如需 WorkSpaces 應用程式的詳細資訊，請參閱開始使用 Amazon WorkSpaces 應用程式：設定範例應用程式。WorkSpaces 應用程式會管理託管和執行應用程式所需的 AWS 資源、自動擴展，以及隨需提供使用者存取權。WorkSpaces 應用程式可讓使用者存取自己選擇之裝置上的所需應用程式，提供與原生安裝應用程式不同的回應式流暢使用者體驗。

如需 WorkSpaces 安全瀏覽器的資訊，請參閱 Amazon WorkSpaces 安全瀏覽器入門。Amazon WorkSpaces 安全瀏覽器是一種隨需、全受管的 Linux 型服務，旨在促進安全瀏覽器存取內部網站和 software-as-a-service(SaaS) 應用程式。從現有的網頁瀏覽器存取服務，無需擔心基礎設施管理、專用用戶端軟體或虛擬私有網路 (VPN) 解決方案等管理上的負擔。

下圖顯示 WorkSpaces 精簡型客戶端的架構。


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
Admin workflow
Auth
Streaming
Other traffic
1.4
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
2.2 Authenticate
IdP

設定 Amazon WorkSpaces 精簡型客戶端管理員主控台

主題

註冊 AWS

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

建立 IAM 使用者

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	根據	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	在 AWS Command Line Interface 使用者指南中設定 AWS CLI 以使用 來設定 AWS IAM Identity Center程式設計存取。

選擇一種管理管理員的方式	到	根據	您也可以
	者指南中的 IAM 安全最佳實務。		
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循《IAM 使用者指南》中建立 IAM 使用者以進行緊急存取 的指示。	請依照《IAM 使用者指南》中的管理 IAM 使用者的存取金鑰設定以程式設計方式存取。

適用於 Amazon WorkSpaces 精簡型客戶端的 VDI 入門

Amazon WorkSpaces 精簡型客戶端是一種經濟實惠的精簡型客戶端裝置，旨在與 AWS 最終使用者運算服務搭配使用，為您提供安全、即時的應用程式和虛擬桌面存取。

選擇虛擬桌面基礎設施 (VDI)，並將其設定為使用 WorkSpaces 精簡型客戶端。

> **Important**
>
> 若要讓 WorkSpaces 精簡型客戶端管理員主控台正常運作，您的系統必須先符合特定需求。這些要求會列在每個虛擬桌面供應商的組態程序中。

WorkSpaces 精簡型客戶端需要特定的軟體組態，具體取決於虛擬桌面提供者。

主題

為 WorkSpaces 精簡型客戶端設定 WorkSpaces Personal

若要讓 WorkSpaces 精簡型客戶端與 Amazon WorkSpaces Personal 搭配使用，您的服務將需要設定為存取 WorkSpaces 目錄。Amazon WorkSpaces Personal 目錄會根據其目錄名稱列在 AWS 主控台的 WorkSpaces 精簡型客戶端建立環境頁面上。

> **Note**
>
> 第一次使用 主控台之前，必須先進行組態。不建議您在開始使用主控台後修改任何先決條件功能。

開始之前

請確定您擁有可建立或管理 WorkSpace AWS 的帳戶。不過，裝置使用者不需要 AWS 帳戶即可連線到和使用其 WorkSpaces。

在您繼續設定之前，請檢閱並了解下列概念：

- 當您啟動 WorkSpace 時，請選取 WorkSpace 套件。如需詳細資訊，請參閱 Amazon WorkSpaces 套件。
- 當您啟動 WorkSpace 時，請選取您要搭配套件使用的通訊協定。如需詳細資訊，請參閱 Amazon WorkSpaces Personal 的通訊協定。
- 當您啟動 WorkSpace 時，請指定每個使用者的設定檔資訊，包括使用者名稱和電子郵件地址。使用者透過建立密碼來完成其設定檔。有關 WorkSpaces 和使用者的資訊儲存在目錄中。如需詳細資訊，請參閱管理 WorkSpaces Personal 的目錄。
- 當您啟動 WorkSpace 時，請啟用和設定 WorkSpaces 精簡型客戶端 Web 存取。如需詳細資訊，請參閱設定 WorkSpaces 精簡型客戶端

步驟 1：確認您的系統符合 WorkSpaces Personal 所需的功能

若要讓 WorkSpaces 精簡型客戶端管理員主控台與 Amazon WorkSpaces Personal 正常運作，您的系統必須符合下列特定要求。此資料表列出所有這些支援的功能及其需求。

功能	需求
Web 存取	已啟用
支援的作業系統	• Windows 10 • Windows 10 (自帶授權) • Windows 11 • Windows 11 (自帶授權)
支援的套件	• Microsoft Power 搭配 Windows 10（以伺服器 2016、2019 和 2022 為基礎） • Microsoft Power 搭配 Windows 10（伺服器 2016、2019 和 2022 型）與 Office • Microsoft PowerPro 搭配 Windows 10（以伺服器 2016、2019 和 2022 為基礎） • Microsoft PowerPro 搭配 Windows 10（伺服器 2016、2019 和 2022 型）與 Office

功能	需求
	• 搭配 Windows 10 的 Microsoft 效能（以伺服器 2016、2019 和 2022 為基礎） • 搭配 Windows 10 的 Microsoft 效能（以伺服器 2016、2019 和 2022 為基礎）w Office
支援的通訊協定	僅限 DCV

步驟 2：使用進階設定來啟動 WorkSpace

使用進階設定啟動 WorkSpace

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/v2/home/。
2. 選擇下列其中一個目錄類型，然後選擇下一步：
   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector
3. 輸入目錄資訊。
4. 從兩個不同的可用區域中選擇 VPC 中的兩個子網路。如需詳細資訊，請參閱具有公用子網路的 VPC。
5. 檢閱您的目錄資訊，然後選擇建立目錄。

業務持續性

WorkSpaces 精簡型客戶端在業務連續性計畫 (BCP) 中提供業務連續性支援。WorkSpaces 精簡型客戶端業務持續性僅適用於 WorkSpaces Personal。如需業務持續性的詳細資訊，請參閱《Amazon WorkSpaces 管理指南》中的 WorkSpaces Personal 的業務持續性。 Amazon WorkSpaces

先決條件

若要讓業務連續性在 WorkSpaces 精簡型客戶端上運作，必須符合下列先決條件：

- 對於 WorkSpaces 跨區域重新導向 – DNS 服務和路由政策已設定。若要設定這些項目，請參閱設定您的 DNS 服務並設定 DNS 路由政策。

- 針對 WorkSpaces 多區域彈性 – 已建立待命 WorkSpaces。若要建立此項目，請參閱建立待命 WorkSpace。
- 區域中使用 WorkSpaces 精簡型客戶端的連線別名。若要驗證您的區域，請參閱涵蓋區域。

設定 WorkSpaces 精簡型客戶端的業務持續性

若要在 Amazon WorkSpaces 精簡型客戶端上啟用 WorkSpaces Personal DR，您需要設定連線別名，以使用 SDK 對應至環境。 Amazon WorkSpaces

設定災難復原的範例文件說明：

Example

使用 CLI AWS 為串流桌面使用 WorkSpaces 連線別名建立新環境的範例命令：

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

將 *wsca-id* 取代為您的 WorkSpaces Personal 連線別名。WorkSpaces 連線別名的 ID 可在 WorkSpaces 管理主控台或 SDK 中找到。

最終使用者體驗

設定業務持續性後，裝置必須在過去 15 天內註冊並處於作用中狀態。之後，如果 WorkSpaces 精簡型客戶端管理服務無法使用，則使用者可以與其工作階段保持連線長達 24 小時。在此情況下，裝置將不會收到軟體更新、交換狀態資訊，而且無法啟用。WorkSpaces 精簡型客戶端主控台中對應的裝置項目不會顯示最新資訊。

如果 WorkSpaces 精簡型客戶端裝置管理服務在 24 小時後仍無法使用，則會顯示下列錯誤訊息：

「發生錯誤。請再試一次。如果問題仍然存在，請聯絡您的 IT 管理員。（錯誤碼：3006)。」

為 WorkSpaces 精簡型客戶端設定 WorkSpaces 集區

若要讓 WorkSpaces 精簡型客戶端與 Amazon WorkSpaces 集區搭配使用，您的 SAML 2.0 身分提供者 (IdP) 需要設定為存取 WorkSpaces 集區目錄。Amazon WorkSpaces 集區目錄是指派給使用者群組的非持久性 WorkSpaces 集區。

> **Note**
>
> 第一次使用 主控台之前，必須先進行組態。

開始之前

請確定您擁有可建立或管理 WorkSpace AWS 的帳戶。不過，裝置使用者不需要 AWS 帳戶即可連線到和使用其 WorkSpaces。

在您開始將 Active Directory 與 WorkSpaces 集區搭配使用之前，請先檢閱並了解 Amazon WorkSpaces 管理指南中列出的概念，再繼續您的組態。

建立 WorkSpaces 集區

設定並建立從中啟動和串流使用者應用程式的集區。

> **Note**
>
> 您應該先建立目錄，再建立 WorkSpaces 集區。如需詳細資訊，請參閱設定 SAML 2.0 和建立 WorkSpaces 集區目錄目錄。

設定和建立集區

1. 開啟 WorkSpaces 主控台，網址為 https://console.aws.amazon.com/workspaces/v2/home/。
2. 在導覽窗格中，選擇 WorkSpaces、集區。
3. 選擇建立 WorkSpaces 集區。
4. 在加入 （選用） 下，您可以根據我的使用案例選擇建議選項，以取得您想要使用的 WorkSpaces 類型建議。如果您知道想要使用 WorkSpaces 集區，可以略過此步驟。
5. 在設定 WorkSpaces 下，輸入下列詳細資訊：

   - 在名稱中，輸入集區的唯一名稱識別符。不允許使用特殊字元。
   - 針對描述，輸入集區的描述 （最多 256 個字元）。
   - 針對套件，從下列您想要用於 WorkSpaces 的套件類型中進行選擇。
     - 使用基本 WorkSpaces 套件 – 從下拉式清單中選擇其中一個套件。如需所選套件類型的詳細資訊，請選擇套件詳細資訊。若要比較集區提供的套件，請選擇比較所有套件。

- 使用您自己的自訂套件 – 選擇您先前建立的套件。若要建立自訂套件，請參閱建立 WorkSpaces Personal 的自訂 WorkSpaces 映像和套件。

> **Note**
>
> BYOL 目前不適用於 WorkSpaces 集區。

- 針對工作階段最長持續時間 (單位分鐘)，選擇串流工作階段可保持作用中的時間長度上限。如果使用者在達到此限制的五分鐘前仍連線到串流執行個體，系統會提示他們在中斷連線之前儲存任何開啟的文件。經過這段時間後，執行個體就會終止，並以新的執行個體取代。您可以在 WorkSpaces 集區主控台中設定的工作階段持續時間上限為 5760 分鐘 (96 小時）。您可以使用 WorkSpaces 集區 API 和 CLI 設定的工作階段持續時間上限為 432000 秒 (120 小時）。
- 針對 Disconnect timeout in minutes (中斷連線逾時 (以分鐘為單位))，選擇在使用者中斷連線之後，串流工作階段會保持作用中的時間長度。如果在這個時間間隔內，使用者於中斷連線或網路中斷後仍嘗試重新連線到此串流工作階段，則會連線到上一個工作階段。否則，它們會連接到具有新串流執行個體的新工作階段。
- 如果使用者透過在集區工具列上選擇結束工作階段或登出來結束工作階段，則不會套用中斷連線逾時。反之，系統會提示使用者儲存任何開啟的文件，然後立即中斷與串流執行個體的連線。接著會終止使用者正在使用的執行個體。
- 針對 Idle disconnect timeout in minutes (閒置中斷連線逾時 (以分鐘為單位))，選擇要等使用者閒置 (非作用中) 多久後，才讓使用者與其串流工作階段中斷連線，並開始計算 Disconnect timeout in minutes (中斷連線逾時 (以分鐘為單位)) 時間間隔。使用者會在因閒置而中斷連線之前收到通知。如果使用者在 Disconnect timeout in minutes (中斷連線逾時 (以分鐘為單位)) 中指定的時間間隔過去之前就嘗試重新連線至串流工作階段，系統會將使用者連線至其先前的工作階段。否則，它們會連接到具有新串流執行個體的新工作階段。將此值設定為 0 便可加以停用。當此值停用時，使用者就不會由於未活動而導致中斷連線。

> **Note**
>
> 當使用者在串流工作階段期間停止提供鍵盤或滑鼠輸入時，會被視為閒置。對於加入網域的集區，在使用者使用其 Active Directory 網域密碼或智慧卡登入之前，閒置中斷連線逾時的倒數計時不會開始。檔案上傳和下載、音訊輸入、音訊輸出和像素變更無法作為使用者活動。如果使用者在 Idle disconnect timeout in minutes (閒置中斷連線逾時 (以分鐘為單位)) 中的時間間隔過後仍保持閒置狀態，系統便會將其中斷連線。

- 針對排程容量政策 （選用），選擇新增排程容量。根據預期的並行使用者數量下限，指出何時為您的集區佈建執行個體數量下限和上限的開始和結束日期和時間。

- 對於手動擴展政策（選用），指定用於增加和減少集區容量的集區擴展政策。展開手動擴展政策以新增新的擴展政策。

  > **Note**
  >
  > 集區的大小受限於您指定的容量下限和上限。

  - 選擇新增橫向擴展政策，並在指定的容量使用率小於或大於指定的閾值時，輸入新增指定執行個體的值。
  - 選擇在政策中新增擴展，並在指定的容量使用率小於或大於指定的閾值時，輸入移除指定執行個體的值。
- 對於標籤，指定您要使用的金鑰對值。金鑰可以是具有特定關聯值的一般類別，例如「專案」、「擁有者」或「環境」。

6. 在選取目錄頁面上，選擇您建立的目錄。若要建立目錄，請選擇建立目錄。如需詳細資訊，請參閱管理 WorkSpaces 集區的目錄。
7. 選擇建立 WorkSpace 集區。

設定 WorkSpaces 精簡型客戶端存取

設定 WorkSpaces 集區的 Web 存取以使用 WorkSpaces 精簡型客戶端，您將需要使用 AWS 命令登陸介面。

1. 安裝或更新 AWS Command Line Interface。
2. 設定您的AWS CLI 設定。
3. 開啟 AWS CLI。
4. `REGION` 以適當的資訊執行下列取代 `WORKSPACES_DIRECTORY_ID`和 ：

```
aws workspaces modify-workspace-access-properties --resource-
id WORKSPACES_DIRECTORY_ID  --workspace-access-properties
 '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

為 Amazon WorkSpaces 精簡型客戶端設定 WorkSpaces 應用程式 Amazon WorkSpaces

WorkSpaces 應用程式執行個體將根據堆疊名稱列出，並且需要在建立環境頁面上設定 IdP 登入 URL。由於 WorkSpaces 應用程式的 SAML 身分驗證僅支援啟動的身分驗證，因此管理員必須手動輸入正確的登入 URL。

> **Note**
>
> 第一次使用 主控台之前，必須先進行組態。不建議您在開始使用主控台後修改任何先決條件功能。

步驟 1：確認您的系統符合 WorkSpaces 應用程式所需的功能

若要讓 WorkSpaces 精簡型客戶端管理員主控台正確使用 WorkSpaces 應用程式，您的系統必須符合下列特定需求。此資料表列出所有這些支援的功能及其需求。

功能	需求
身分提供者	前往 WorkSpaces 應用程式管理員指南中的設定 SAML，以建立身分提供者。 當系統提示您建立 env 主控台時，輸入您的 IDP 登入 URL。
作業系統	Windows
平台類型	Windows Server (2012 R2、2016 或 2019)
剪貼簿	停用 在 WorkSpaces 應用程式堆疊層級設定
檔案傳輸	停用 在 WorkSpaces 應用程式堆疊層級設定
列印到本機裝置	停用

功能	需求
	在 WorkSpaces 應用程式堆疊層級設定

也支援 WorkSpaces 應用程式上透過 SAML 身分驗證的螢幕鎖定需求。WorkSpaces 精簡型客戶端不支援使用者集區和程式設計身分驗證機制。

步驟 2：設定 WorkSpaces 應用程式堆疊

為了串流您的應用程式，WorkSpaces 應用程式需要一個環境，其中包含與堆疊相關聯的機群，以及至少一個應用程式映像。請依照下列步驟設定機群和堆疊，並讓使用者存取堆疊。如果您尚未這麼做，建議您嘗試開始使用 WorkSpaces 應用程式中的程序：設定範例應用程式。

如果您想要建立要使用的映像，請參閱教學課程：Create a Custom AppStream 2.0 Image by Using the AppStream 2.0 Console。

如果您計劃將機群加入 Active Directory 網域，請先設定您的 Active Directory 網域，再完成以下步驟。如需詳細資訊，請參閱 Using Active Directory with AppStream 2.0。

工作

- 建立機群
- 建立堆疊
- 將存取權限提供給使用者
- 清除資源

為 Amazon WorkSpaces 精簡型客戶端設定 Amazon WorkSpaces 安全瀏覽器

Amazon WorkSpaces 安全瀏覽器是以其 Web 入口網站端點為基礎，位於 AWS 主控台的 WorkSpaces 精簡型客戶端建立環境頁面上。

> **Note**
>
> 第一次使用 主控台之前，必須先進行組態。不建議您在開始使用主控台後修改任何先決條件功能。

步驟 1：確認您的系統符合 Amazon WorkSpaces 安全瀏覽器所需的功能

若要讓 WorkSpaces 精簡型客戶端管理員主控台與 Amazon WorkSpaces 安全瀏覽器正常運作，您的系統必須符合下列特定需求。此資料表列出所有這些支援的功能及其需求。

功能	需求
剪貼簿	停用
檔案傳輸	停用
列印到本機裝置	停用

> **Note**
>
> WorkSpaces 精簡型客戶端目前不支援單一登入的 WorkSpaces 安全瀏覽器延伸。

步驟 2：設定 WorkSpaces 安全瀏覽器入口網站

WorkSpaces 精簡型客戶端可在特定組態中使用 WorkSpaces 安全瀏覽器 VPC：

1. 使用 AWS CodeBuild Cloudformation 範本建立 VPC。
2. 設定身分提供者。
3. 建立 Amazon WorkSpaces 安全瀏覽器入口網站。
4. 測試新的 Amazon WorkSpaces 安全瀏覽器入口網站。

啟動 WorkSpaces 精簡型用戶端管理員主控台

WorkSpaces 精簡型用戶端是一種經濟實惠的精簡型用戶端裝置，旨在與 AWS 最終使用者運算服務搭配使用，為您提供對應用程式和虛擬桌面的安全即時存取。

主題

涵蓋區域

WorkSpaces 精簡型用戶端可在下列區域使用。

只有 WorkSpaces 精簡型用戶端管理員主控台可在這些區域中使用。WorkSpaces 精簡型客戶端裝置目前僅在美國、德國、法國、義大利和西班牙提供。

區域名稱	區域	端點	主控台連結
美國東部 (維吉尼亞北部)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
美國西部 (奧勒岡)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
亞太區域 (孟買)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home
歐洲 (愛爾蘭)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home

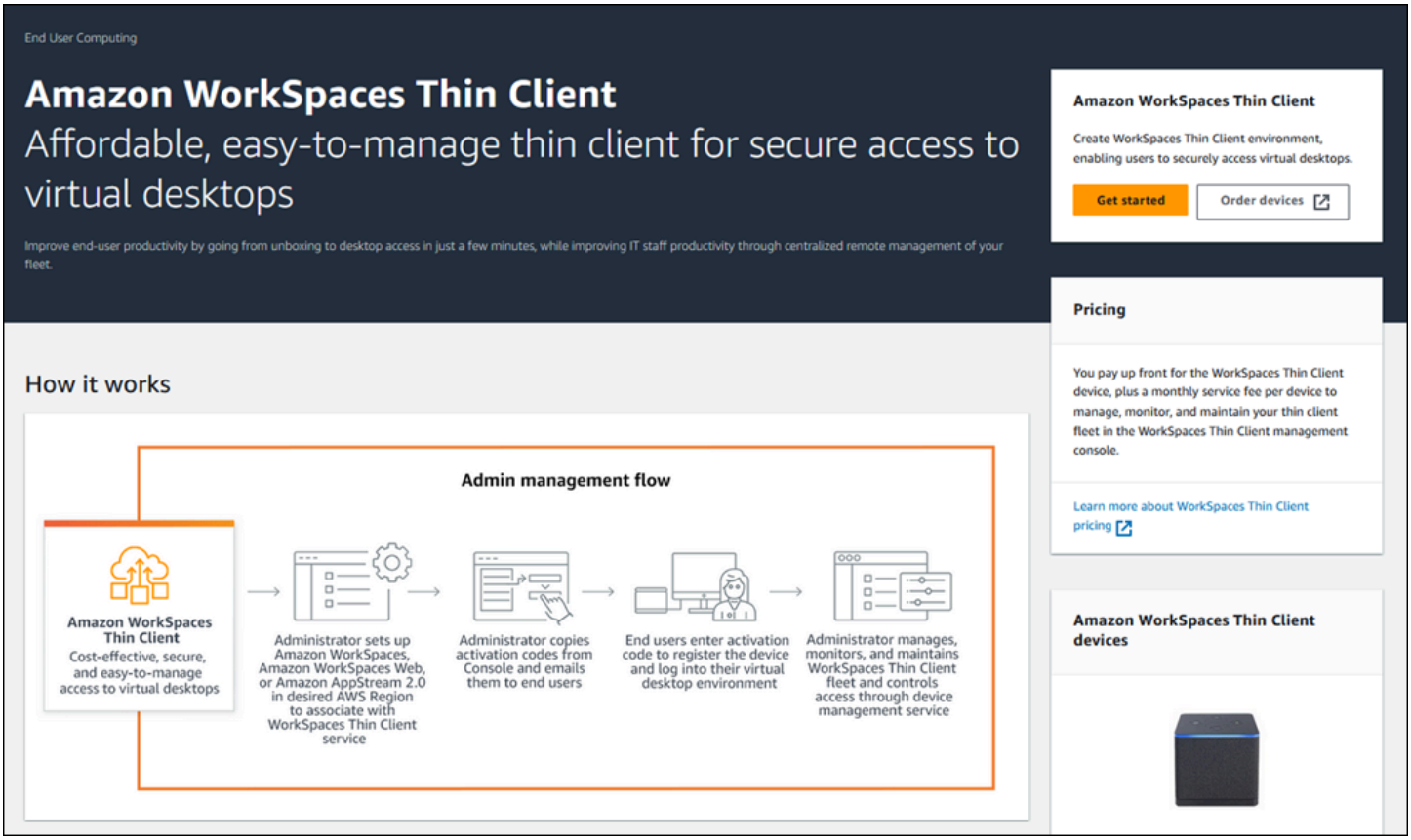
區域名稱	區域	端點	主控台連結
加拿大 (中部)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
歐洲 (法蘭克福)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
歐洲 (倫敦)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

啟動 WorkSpaces 精簡型客戶端管理員主控台

當您有 AWS 帳戶時，您可以啟動管理員主控台，並前往 WorkSpaces 精簡型用戶端主控台。若要啟動 主控台，請執行下列動作：

1. 登入 AWS 您的帳戶。
2. 存取 WorkSpaces 精簡型客戶端主控台。
3. 選取開始使用，系統會將您導向環境。

使用 WorkSpaces 精簡型客戶端管理員主控台



歡迎使用 WorkSpaces 精簡型客戶端管理員主控台！

從這裡，您可以為您的團隊管理 WorkSpaces 精簡型客戶端裝置和環境的機群。

如需 WorkSpaces 精簡型客戶端裝置的相關資訊，請參閱 WorkSpaces 精簡型客戶端使用者指南。

讓我們開始使用吧！

主題

- 環境
- Devices
- 軟體更新

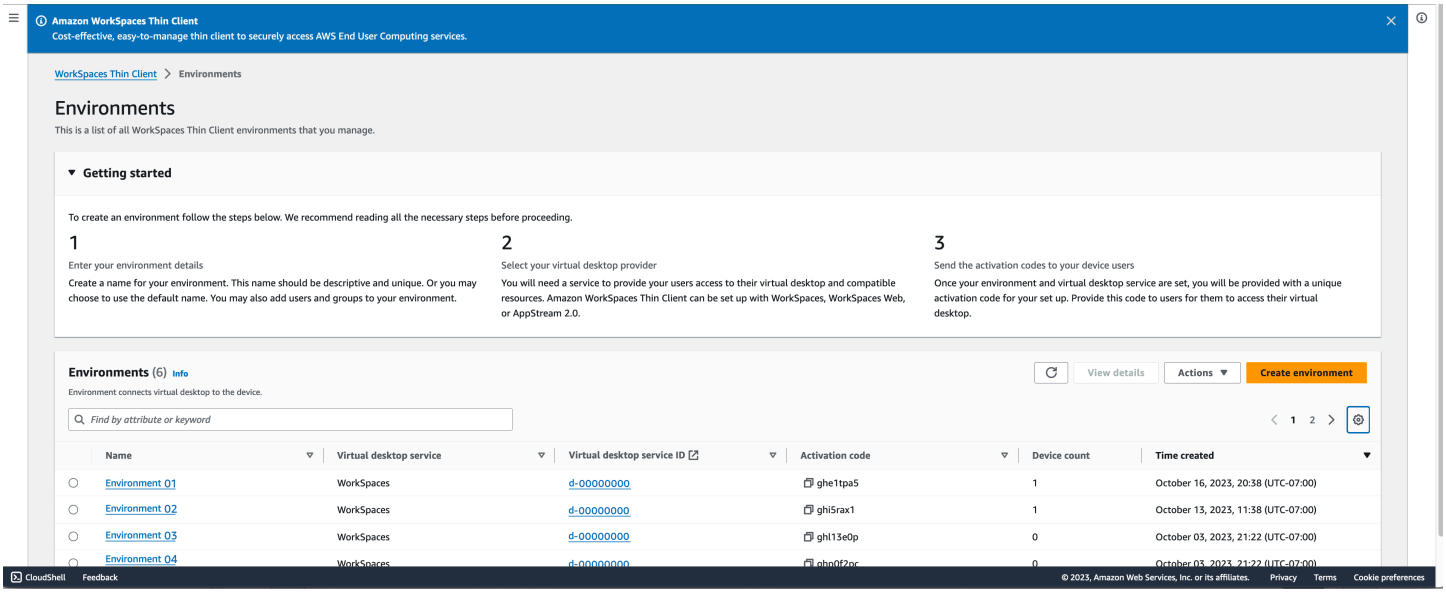
環境

每個 WorkSpaces 精簡型客戶端裝置都使用個別虛擬桌面環境來存取其線上資源。使用者使用下列其中一個虛擬桌面提供者來存取此環境：

- Amazon WorkSpaces
- WorkSpaces 應用程式
- Amazon WorkSpaces 安全瀏覽器

環境清單

您的環境有許多參數供您檢閱，以及您可以採取的一些動作。



環境清單詳細資訊

列出您環境的參數供您檢閱。下表列出摘要中的每個元素及其運作方式。

Element	Description
Name	與此環境相關聯的唯一識別符。
虛擬桌面服務	此環境使用的虛擬桌面提供者。
虛擬桌面服務 ID	虛擬桌面服務提供者指派給此環境的唯一識別符。

Element	Description
啟用碼	最終使用者用來存取虛擬桌面環境的程式碼。
裝置計數	存取此環境的 WorkSpaces 精簡型客戶端裝置數量。
建立時間	建立環境的日期和時間。

環境清單動作

您可以從這裡執行許多動作。選取其中任何一個以執行對應的動作。

Element	Description
搜尋	搜尋您管理的所有環境。
重新整理	重新整理環境清單。
檢視詳細資訊	顯示環境詳細資訊。
動作	開啟下拉式清單，您可以在其中編輯或刪除環境。
建立環境	開始建立環境的程序。

主題

- 環境詳細資訊
- 建立環境
- 編輯環境
- 刪除環境

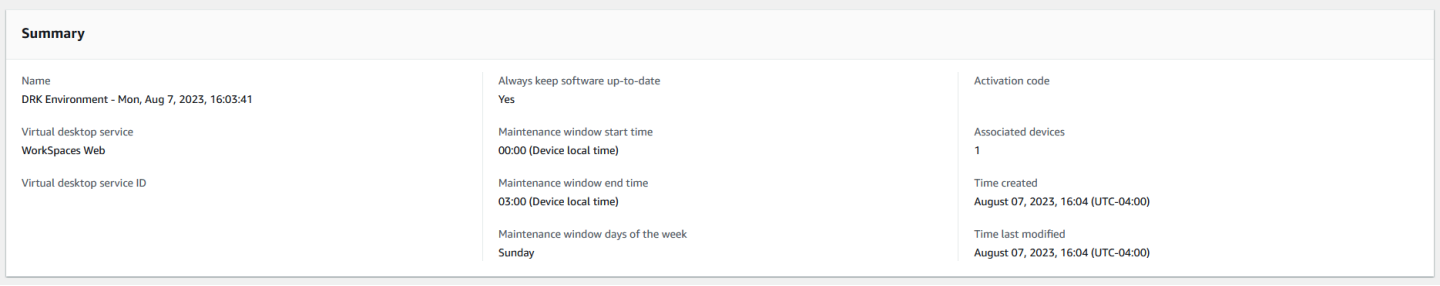
環境詳細資訊

當您選取環境時，WorkSpaces 精簡型客戶端主控台會顯示該環境的詳細資訊，供您檢閱。主控台也會顯示此環境使用的虛擬桌面提供者詳細資訊。

主題

摘要

摘要區段提供 WorkSpaces 精簡型客戶端環境主要功能的高階概觀。下表列出摘要中的每個元素及其運作方式。



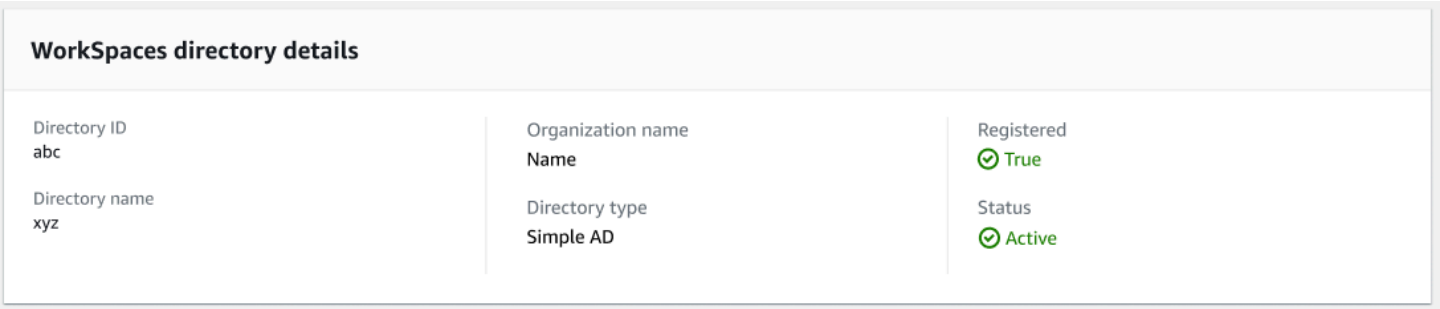
Element	Description
Name	與此環境相關聯的唯一識別符。
虛擬桌面服務	此環境使用的虛擬桌面提供者。
虛擬桌面服務名稱	虛擬桌面服務提供者指派給此環境的唯一識別符。
啟用碼	最終使用者使用此程式碼來存取虛擬桌面環境。
隨時將軟體保持在up-to-date	此設定會啟用自動軟體更新。
維護時段開始時間	每週自動軟體更新開始的時間。
維護時段結束時間	每週自動軟體更新完成的時間。
一週中的維護時段天數	自動軟體更新發生的日期。
關聯的裝置	存取此環境的 WorkSpaces 精簡型客戶端裝置數量。
建立時間	建立此環境的日期和時間。

虛擬桌面環境詳細資訊

WorkSpaces 精簡型客戶端環境是在虛擬桌面介面上執行。每個界面都有一組不同的參數來控制專用環境。

Amazon WorkSpaces 目錄詳細資訊

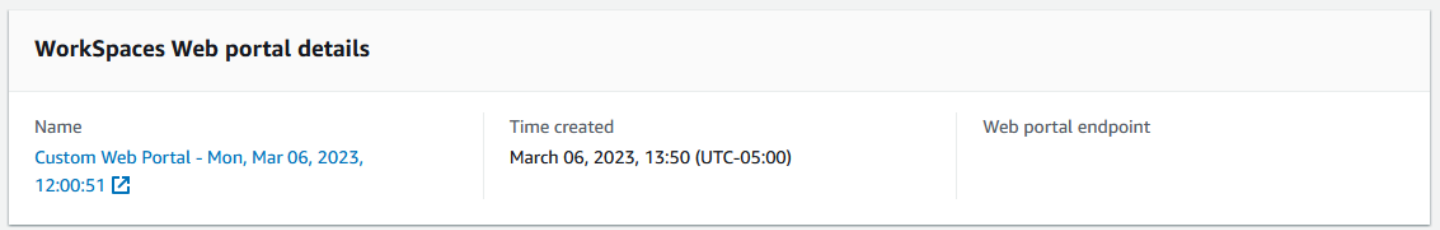
在 Amazon WorkSpaces 上執行的 WorkSpaces 精簡型客戶端環境會使用目錄來建立和執行虛擬桌面。下表列出詳細資訊中的每個元素及其運作方式。



Element	Description
目錄 ID	與此環境相關聯的 Amazon WorkSpaces 目錄。
目錄名稱	與此 Amazon WorkSpaces 目錄相關聯的唯一識別符。
組織名稱	控制 Amazon WorkSpaces 目錄的組織名稱。
目錄類型	Amazon WorkSpaces 目錄的格式。
已登記	此 Amazon WorkSpaces 目錄是否已註冊。
狀態	此 Amazon WorkSpaces 目錄是否處於作用中狀態。

Amazon WorkSpaces 安全瀏覽器入口網站詳細資訊

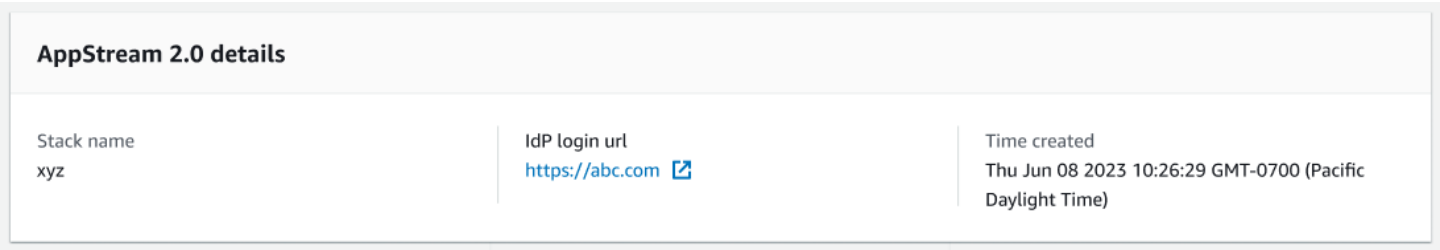
在 Amazon WorkSpaces 安全瀏覽器上執行的 WorkSpaces 精簡型客戶端環境會使用 Web 入口網站來建立和執行虛擬桌面。下表列出詳細資訊中的每個元素及其運作方式。



Element	Description
Name	與此 WorkSpaces 安全瀏覽器入口網站相關聯的唯一識別符。
建立時間	建立此 WorkSpaces 安全瀏覽器入口網站的日期和時間。
Web 入口網站端點	用來存取虛擬桌面環境的 URL。

WorkSpaces 應用程式詳細資訊

WorkSpaces 精簡型客戶端環境會在 WorkSpaces 應用程式資訊堆疊上執行，以建立和執行其虛擬桌面。下表列出詳細資訊中的每個元素及其運作方式。



Element	Description
Stack name (堆疊名稱)	與此 WorkSpaces 應用程式堆疊相關聯的唯一識別符。
IdP 登入 URL	用於登入和登出 WorkSpaces 應用程式堆疊的身分提供者 URL。
建立時間	建立此 WorkSpaces 應用程式堆疊的日期和時間。

建立環境

首先，每個裝置都需要 AWS 最終使用者運算服務。WorkSpaces 精簡型客戶端會使用下列服務：

- 透過指派目錄的 Amazon WorkSpaces
- 透過指派堆疊的 WorkSpaces 應用程式
- 透過 Web 入口網站地址的 Amazon WorkSpaces 安全瀏覽器

您必須將服務指派給現有環境或建立新的環境。

> **Note**
>
> WorkSpaces 精簡型客戶端只會顯示相同區域中的虛擬桌面。

主題

步驟 1：輸入環境詳細資訊

1. 在環境詳細資訊欄位中輸入環境的名稱。
2. 若要設定自動軟體修補程式，請核取始終保持軟體最新方塊。

   > **Note**
   >
   > 如果未啟用自動軟體更新，在您手動推送更新或軟體過期且系統強制更新之前，註冊到此環境的裝置將不會收到軟體更新。
   > 此外，裝置軟體集版本由系統決定。此版本可能不是最新的版本。

3. 選取您想要排程環境維護時段的時間。

   - 套用全系統的維護時段 - 每週在決定的時間自動更新環境軟體。
   - 套用自訂維護時段：設定您希望環境軟體每週更新的日期和時間。

4. 選取虛擬桌面服務。

- Amazon WorkSpaces
- Amazon WorkSpaces 安全瀏覽器
- WorkSpaces 應用程式

步驟 2：選取虛擬桌面提供者

您必須擁有 服務，才能讓使用者存取其虛擬桌面和相容的資源。

> **Important**
>
> 若要讓 WorkSpaces 精簡型客戶端管理員主控台正常運作，系統必須符合特定需求。這些要求會列在先決條件和組態中。
> 在設定主控台之前，請確定您的系統符合這些要求。

使用 Amazon WorkSpaces

Amazon WorkSpaces 是適用於 Windows 的全受管桌面虛擬化服務，可讓您從任何支援的裝置存取資源。

1. 若要使用 Amazon WorkSpaces，請執行下列其中一項操作：
   - 選取您要用於環境的目錄。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋目錄。
   - 選取建立 WorkSpaces 目錄按鈕來建立目錄。如需有關建立 WorkSpaces 目錄的詳細資訊，請參閱 Manage directories for WorkSpaces。
2. 選取建立環境按鈕。

當您建立環境時，您仍然可以稍後編輯詳細資訊。如需詳細資訊，請參閱編輯環境。

使用 WorkSpaces 應用程式

WorkSpaces 應用程式是一項全受管、安全的應用程式串流服務，可用來將桌面應用程式從 串流 AWS 至 Web 瀏覽器。

> **Important**
>
> 若要建立 WorkSpaces 應用程式環境，您必須將 `cli_follow_urlparam`設定為 `false`。若要完成此動作，請執行下列操作：

- 對於預設設定檔，請執行 `aws configure set cli_follow_urlparam false`。
- 對於名為 `ProfileName` 的設定檔，請執行 `aws configure set cli_follow_urlparam false --profile ProfileName`。

1. 若要設定 WorkSpaces 應用程式，請執行下列其中一項操作：
   - 選取您要用於環境的堆疊。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋堆疊。
   - 選取建立堆疊按鈕來建立堆疊。如需建立 WorkSpaces 應用程式堆疊的詳細資訊，請參閱建立堆疊。
2. 在 IdP 登入 URL 欄位中輸入身分提供者登入和登出 URL。這可為使用者提供登入和登出 WorkSpaces 精簡型客戶端的位置。
3. 選取建立環境按鈕。

建立環境之後，您仍然可以稍後編輯詳細資訊。如需詳細資訊，請參閱編輯環境。

使用 Amazon WorkSpaces 安全瀏覽器

Amazon WorkSpaces 安全瀏覽器是一種低成本、全受管的 WorkSpaces 主控台，旨在為現有 Web 瀏覽器中的使用者提供安全的 Web 型工作負載和軟體即服務 (SaaS) 應用程式存取。

1. 若要設定 Amazon WorkSpaces 安全瀏覽器，請執行下列其中一項操作：
   - 選取您要用於您環境的 Web 入口網站。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋 Web 入口網站。
   - 選取建立 WorkSpaces 安全瀏覽器按鈕來建立 Web 入口網站。如需建立 WorkSpaces 安全瀏覽器 Web 入口網站的詳細資訊，請參閱設定 Amazon WorkSpaces 安全瀏覽器。
2. 選取建立環境按鈕。

建立環境之後，您仍然可以稍後編輯詳細資訊。如需詳細資訊，請參閱編輯環境。

步驟 3：將啟用代碼傳送至裝置使用者

設定環境和虛擬桌面服務之後，您會在 AWS 管理主控台上收到設定的唯一啟用碼。

將此啟用碼提供給任何 WorkSpaces 精簡型客戶端裝置使用者，他們可以使用它來存取虛擬桌面。

如需如何協助裝置使用者設定 Amazon WorkSpaces 精簡型客戶端的其他資訊，請參閱 WorkSpaces 精簡型客戶端使用者指南。 Amazon WorkSpaces

編輯環境

WorkSpaces 精簡型客戶端管理主控台會管理個別使用者的虛擬桌面環境。您可以從此主控台編輯或刪除虛擬桌面環境。

1. 選取您想要編輯的環境。

   > **Note**
   >
   > 您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋環境。

2. 選取動作按鈕。
3. 從下拉式清單中選取編輯。系統會將您導向至編輯環境視窗。
4. 編輯下列任何一項：
   - 在環境名稱欄位中變更環境的名稱。
   - 變更自動軟體更新的軟體更新詳細資訊核取方塊。
   - 變更您要為環境安排維護時段的時間。
5. 選取編輯環境按鈕。

刪除環境

> **Note**
>
> 如果環境中已註冊有裝置，則無法刪除該環境。首先，您必須取消註冊並刪除環境中的所有裝置。

1. 選取您想要刪除的環境。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋環境。
2. 選取動作按鈕。
3. 從下拉式清單中選取刪除。刪除環境確認視窗隨即出現。
4. 在確認欄位中輸入 "delete"。
5. 選取刪除按鈕。

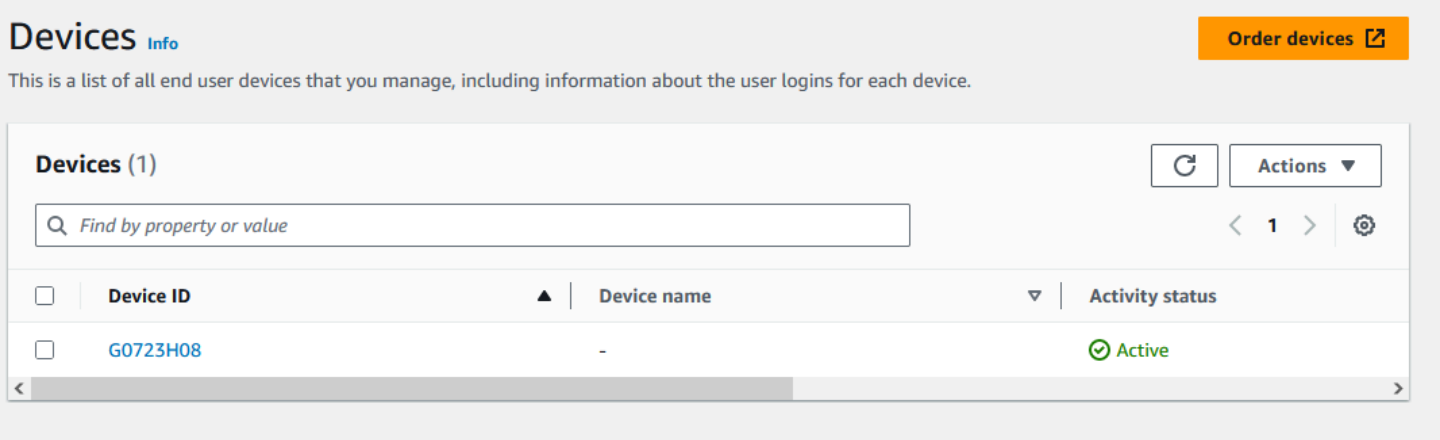
Devices

每個 WorkSpaces 精簡型客戶端最終使用者都有專用的裝置，可將其連線至虛擬桌面環境和線上資源。這些裝置是透過 AWS 網站上的 WorkSpaces 精簡型客戶端管理員主控台來管理。

您可以從這個主控台為團隊訂購裝置。

裝置清單

您網路中的任何裝置都有數個參數供您檢閱，以及您可以採取的一些動作。



裝置清單詳細資訊

列出您裝置的參數供您檢閱。下表列出摘要中的每個元素及其運作方式。

Element	Description
裝置序號	指派給個別裝置的識別號碼。
裝置名稱	（選用）您提供給裝置的唯一名稱。
上次由 使用	存取裝置之使用者的識別號碼。僅在使用 WorkSpaces Personal 時可用。
活動狀態	裝置目前的狀態。有兩種狀態： • 作用中 – 至少在過去七天內連線至網路一次。 • 非作用中 – 在過去七天內未連線至網路。

Element	Description
註冊狀態	確認裝置已設定、與此 AWS 帳戶相關聯，並且是特定環境的一部分。它可以處於下列其中一種狀態： • 已註冊 – 這是預設狀態。 • 取消註冊 – 裝置正在重設和取消註冊程序。 **Note** 如果裝置處於取消註冊狀態，您可以刪除該裝置。 • 已取消註冊 – 裝置已成功取消註冊。 **Note** 您只能刪除處於取消註冊或取消註冊狀態的裝置。 • 已封存 – 裝置已封存。
環境 ID	此裝置所連接環境的識別符。
軟體合規	裝置軟體的合規狀態。有兩種狀態： • 合規 • 不合規

裝置清單動作

您可以從這裡執行許多動作。選取其中任何一個以執行對應的動作。

Element	Description
搜尋	搜尋您管理的所有裝置。

Element	Description
重新整理	重新整理裝置清單。
檢視詳細資訊	顯示裝置詳細資訊。
動作	開啟下拉式清單，您可以在其中執行下列動作： • 編輯裝置名稱 • 取消註冊 • 封存 • 刪除 • 匯出裝置詳細資訊
訂購裝置	開始訂購裝置的程序。

主題

- 裝置詳細資訊
- 編輯裝置名稱
- 重設和取消註冊裝置
- 封存裝置
- 刪除裝置
- 匯出裝置詳細資訊

裝置詳細資訊

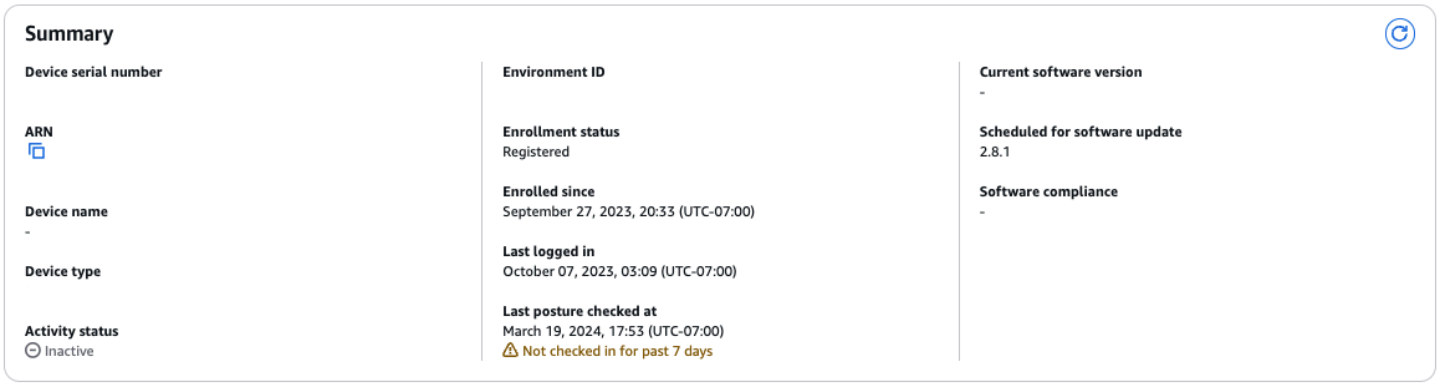
當您選取裝置時，WorkSpaces 精簡型客戶端主控台會顯示該裝置的詳細資訊，供您檢閱。主控台也會顯示裝置網路類型和連線周邊裝置的詳細資訊。

主題

- 摘要
- 裝置設定
- 使用者活動

摘要

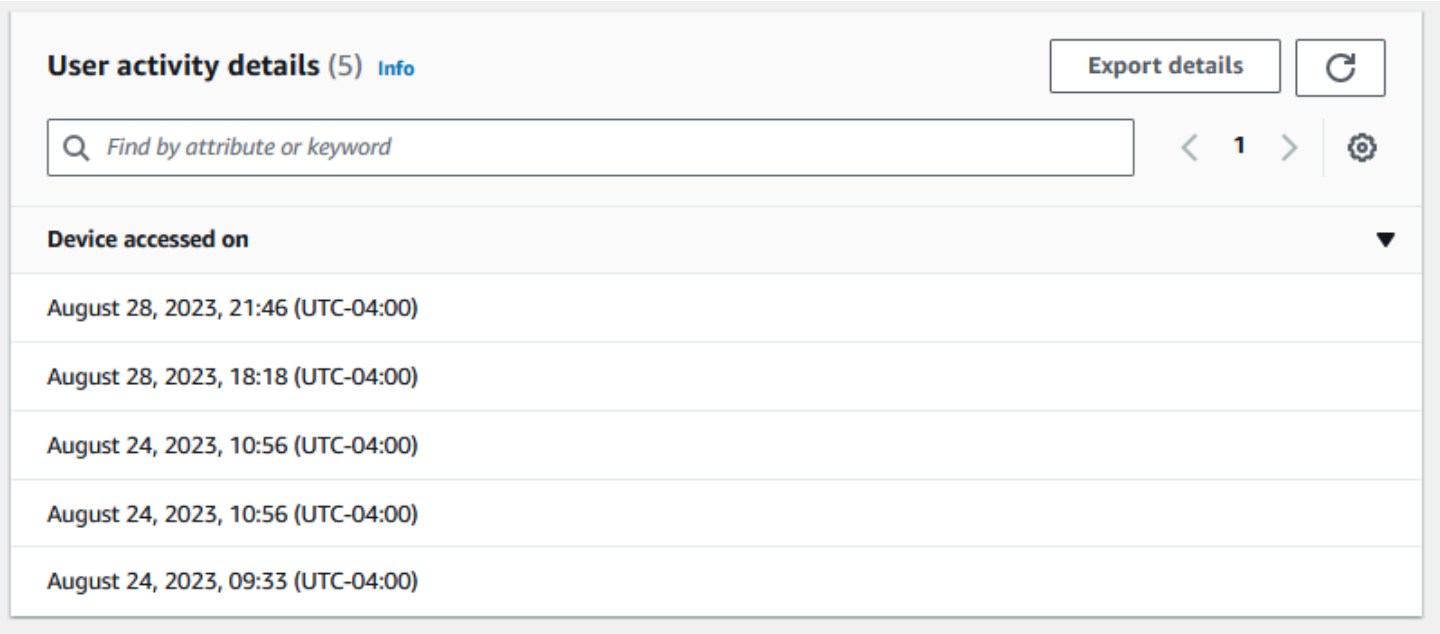
摘要區段提供 WorkSpaces 精簡型客戶端裝置主要功能的高階概觀。下表列出摘要中的每個元素及其運作方式。



Element	Description
裝置序號	指派給個別裝置的識別號碼。
ARN	Amazon Resource Name (ARN) 格式的裝置唯一識別符。
裝置名稱	您提供給裝置的名稱。如果您尚未建立名稱，則可以命名該名稱，否則會取得預設名稱。
裝置類型	連結至帳戶的最終使用者裝置的類型。
活動狀態	此裝置的目前狀態。兩種狀態為： • 作用中 • 非作用中
環境 ID	裝置使用的環境識別號碼。
註冊狀態	確認裝置已設定、與此 AWS 帳戶相關聯，並且是特定環境的一部分。它可以處於下列四種狀態之一： • 已註冊 – 這是預設狀態。 • 取消註冊 – 裝置正在重設和取消註冊程序。

Element	Description
	• 已取消註冊 – 裝置已成功取消註冊。 **Note** 您只能刪除處於已取消註冊或已封存狀態的裝置。 • 已封存 – 管理員已將此裝置標記為目前不在服務中。
自 開始註冊	裝置啟用的日期。
上次登入	最近登入的日期和時間。
上次檢查姿勢於	最近裝置簽入的日期和時間。
目前的軟體版本	此裝置目前正在使用的軟體版本。
排定進行軟體更新	裝置上的排程軟體版本。
軟體合規	確認軟體集有效。有兩種狀態： • 合規 • 不合規
上次由 使用	存取裝置之使用者的識別號碼。僅在使用 WorkSpaces Personal 時可用。

使用者日誌



Element	Description
上次裝置存取	此裝置上次使用的日期和時間。

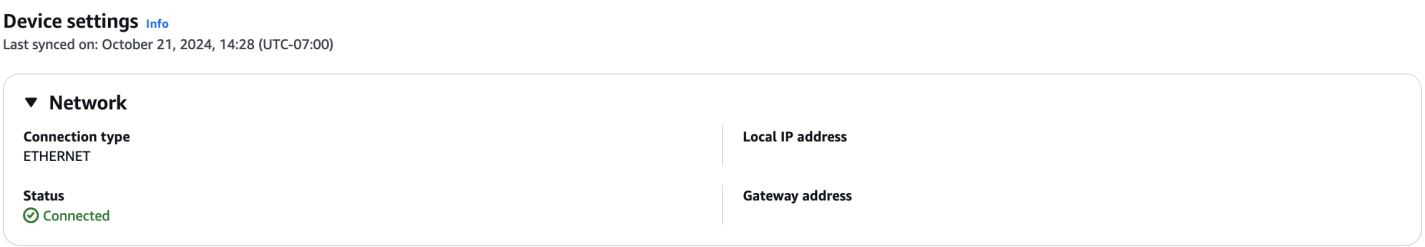
裝置設定

列出您裝置的參數供您檢閱。下表列出每個元素及其運作方式。

> **Note**
>
> 裝置設定資訊只會在裝置上線時更新。如果裝置離線，某些資訊可能已過期。

標題和網路

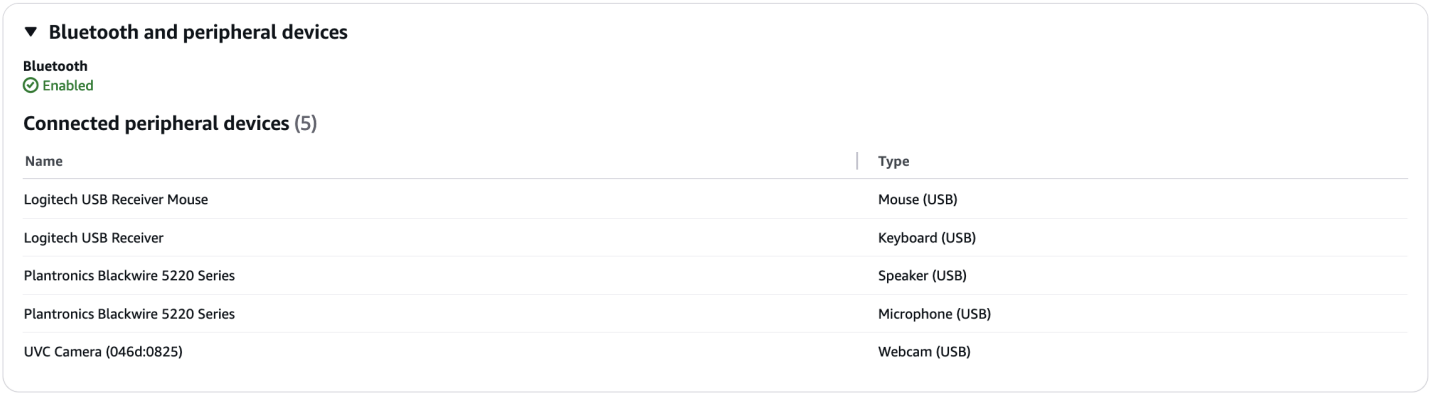
WorkSpaces 精簡型客戶端裝置詳細資訊提供裝置網路連線的概觀。下表列出每個元素及其運作方式。



Element	Description
上次同步於	最近裝置設定與主控台同步的日期和時間。
連線類型	裝置使用的網路連線類型。連線類型可以是乙太網路或 Wifi。
狀態	網路的狀態。如果裝置目前已連線，或在過去 20 分鐘內已連線，狀態會顯示為「已連線」。如果網路已中斷連線超過 20 分鐘，狀態將變更為顯示自從裝置上次連線至網際網路以來經過的時間，例如「上次連線 20 分鐘前」。
本機 IP 地址	連線網路的本機 IP 地址。
閘道地址	連線網路的閘道地址。

藍牙和周邊裝置

WorkSpaces 精簡型客戶端裝置詳細資訊提供連線至裝置的任何連線周邊裝置的清單。下表列出每個元素及其運作方式。

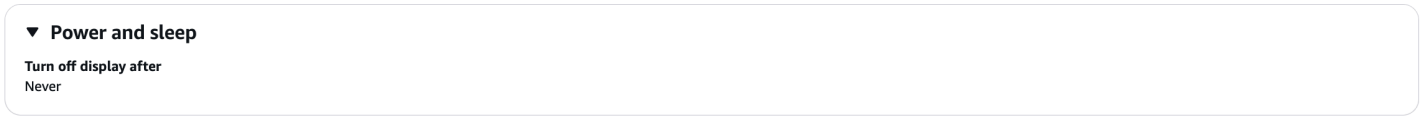


Element	Description
藍牙	裝置藍牙狀態。兩種狀態為： • 已啟用 • Disabled

Element	Description
連接的周邊裝置	連線周邊裝置的名稱清單，例如 Logitech 滑鼠，以及連線周邊裝置的類型，例如滑鼠 (USB)。

電源和睡眠

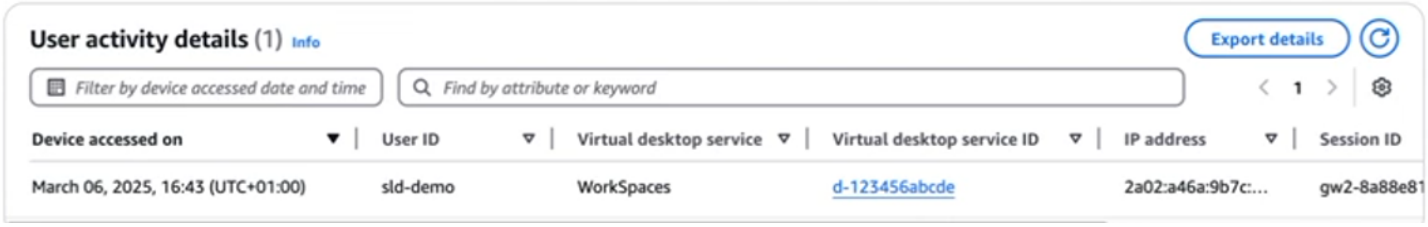
每個 WorkSpaces 精簡型客戶端裝置都有省電模式。下表列出此模式的狀態。



Element	Description
在 之後關閉顯示	裝置關閉其顯示的非作用中時間期間。

使用者活動

此標籤顯示特定裝置的設定和用量資訊的日誌。下表列出此日誌的每個元素。



Element	Description
在 上存取的裝置	裝置啟用的日期和時間。
使用者 ID	存取裝置之使用者的識別號碼。
虛擬桌面服務	裝置使用的虛擬桌面服務。
虛擬桌面服務 ID	與使用者相關聯的虛擬桌面服務 ID 號碼。

Element	Description
IP 位址	存取裝置的 IP 識別號碼。
事件類型	有關裝置使用方式的詳細資訊。

> **Note**
>
> 除了 WorkSpaces Personal 之外，VDIs 只會顯示登入起始事件。

您可以使用資料表上方的搜尋列，在資料表中尋找特定資訊。您也可以依日期和時間篩選資料表結果。

您可以選取匯出詳細資訊按鈕，將資料表匯出至 csv 檔案。

編輯裝置名稱

1. 選取您要編輯的裝置。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋裝置。
2. 選取動作按鈕。
3. 從下拉式清單中選取編輯裝置名稱。編輯裝置名稱視窗隨即出現。
4. 在裝置名稱確認欄位中輸入新的裝置名稱。
5. 選取儲存按鈕。

重設和取消註冊裝置

1. 選取您要取消註冊的裝置。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋裝置。
2. 選取動作按鈕。
3. 從下拉式清單中選取取消註冊。取消註冊視窗隨即出現。
4. 在確認欄位中輸入 "deregister"。
5. 選取取消註冊按鈕。

> **Note**
>
> 取消註冊可強制登出使用者，並要求在工作階段期間重新啟動其 WorkSpaces 精簡型客戶端裝置。

封存裝置

1. 選取您要封存的裝置。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋裝置。
2. 選取動作按鈕。
3. 從下拉式清單中選取封存。封存視窗隨即出現。
4. 在確認欄位中輸入 "reset and archive"。
5. 選取重設並封存按鈕。

> **Note**
>
> 封存裝置強制登出使用者，並要求在工作階段期間重新啟動其 WorkSpaces 精簡型客戶端裝置。

刪除裝置

1. 選取您要刪除的裝置。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋裝置。
2. 選取動作按鈕。
3. 從下拉式清單中選取刪除。刪除視窗隨即出現。
4. 在確認欄位中輸入 "delete"。
5. 選取刪除按鈕。

匯出裝置詳細資訊

1. 選取您要匯出詳細資訊的裝置。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋裝置。
2. 選取動作按鈕。
3. 從下拉式清單中選取匯出裝置詳細資訊。試算表格式的所選裝置下載詳細資訊。

您的 Amazon WorkSpaces 精簡型客戶端 - 使用裝置所產生的資料

您的 Amazon WorkSpaces 精簡型客戶端會產生和收集您與其互動的資料。

資料類型：您的 Amazon WorkSpaces 精簡型客戶端會產生裝置效能、使用模式以及與其他 AWS 服務互動的資料。這包括技術資料（例如狀態和設定）、用量資料（例如登入時間戳記）和診斷資料（例如相關系統日誌）。

資料量和收集：產生的資料量取決於您使用裝置和服務的方式。裝置操作期間會持續收集資料。

資料儲存：來自您裝置的資料安全地存放在裝置本身或 AWS 伺服器上。它以結構化、機器可讀取的格式存放。

資料存取：您可以按照此處列出的說明，透過 AWS 帳戶存取您的裝置資料。如需詳細資訊，包括資料下載的說明和服務品質的相關資訊，請參閱這些頁面。

資料管理：您可以透過 AWS 帳戶檢閱裝置資料。若要進一步了解裝置的資料實務，請檢閱我們的服務條款和隱私權聲明。

資料刪除：您可以透過 AWS 帳戶刪除裝置資料。如需資料保留和刪除選項的相關資訊，請參閱刪除裝置。

與他人共用資料： AWS 不會與第三方共用您的裝置資料。只有授權的第三方可以透過我們的識別和存取管理程序，在您核准後存取您的資料。 會在AWS 隱私權聲明中包含的有限情況下與第三方 AWS 共用個人資料。

需要協助嗎？ 請造訪客戶支援以聯絡我們的支援團隊。這不會影響您根據相關法律提出投訴的權利。

資料持有者：Amazon Web Services EMEA SARL， 38 Avenue John F. Powered， L-1855， Luxembourg

軟體更新

WorkSpaces 精簡型客戶端需要定期更新軟體更新，以引進新功能並套用安全修補程式。這些更新由版本控制的軟體集表示。

軟體組可以包含軟體應用程式或 WorkSpaces 精簡型客戶端裝置的作業系統的更新。在此主控台中，您可以選擇立即更新軟體，或在環境的維護時段期間排程自動更新。

軟體集有兩種類型：

- 引進新功能、修正瑕疵和進行一般改進的軟體集。這些是每月發行。

- 包含重大問題安全性修補程式和修正的軟體集。這些會視需要發行。

身為管理員，如果您尚未在環境中啟用自動軟體更新，註冊到該環境的裝置將不會收到軟體更新，直到您手動推送更新為止。

隨著新軟體集的發行，較舊的軟體集會過期。從具有新功能的軟體集發行日期起，您有 40 天的時間可以讓先前的軟體集過期。

為了確保裝置的安全狀態保持不變，如果偵測到過期的軟體，服務會自動更新裝置。這種類型的更新可能會中斷作用中工作階段，因為它不會遵守維護時段，或允許最終使用者延遲更新。為了避免這種情況，建議您至少每 30 天更新一次軟體集。

> **Note**
>
> 如果發行具有安全性修補程式或重大更新的軟體集，則所有先前的軟體集都會設定為在 3 天後過期。為了確保您的裝置保持安全，並將對日常操作的干擾降至最低，我們建議立即更新這些軟體集。

如需已發行軟體集的清單，請參閱 WorkSpaces 精簡型客戶端環境軟體集。

更新環境軟體

WorkSpaces 精簡型客戶端是一種 AWS 最終使用者運算服務，可讓使用者存取虛擬桌面。這些虛擬桌面會定期更新為新的軟體集。若要更新環境軟體，請執行下列動作：

1. 從可用軟體更新的清單中選取軟體集。如需軟體集的清單，請參閱 WorkSpaces 精簡型客戶端環境軟體集。
2. 選取安裝按鈕。
3. 在頁面頂端選取環境。
4. 從環境區段的清單中選取要更新的環境。
5. 選擇下列其中一項，在安排更新中選取何時更新環境：

    - 立即更新軟體：在所有已註冊的裝置上啟動環境軟體的更新。

    > **Note**
    >
    > 現在更新軟體可能會中斷任何作用中的使用者工作階段。

- 在每個環境維護時段更新軟體 - 在環境的排程維護時段更新環境軟體。

6. 核取此方塊以授權更新。必須核取此方塊才能更新軟體。
7. 選取安裝按鈕。

更新裝置軟體

WorkSpaces 精簡型客戶端是一種 AWS 最終使用者運算服務，提供精簡型客戶端裝置，可將使用者連線至專用虛擬桌面。這些裝置會使用新軟體定期更新。若要更新裝置軟體，請執行下列動作：

1. 從可用軟體更新的清單中選取軟體集。
2. 選取安裝按鈕。
3. 在頁面頂端選取裝置。
4. 從裝置區段的清單中選取要更新的裝置。如需軟體集的清單，請參閱 WorkSpaces 精簡型客戶端環境軟體集。
5. 選擇下列其中一項，在安排更新選項中選取何時更新環境：

   - 立即更新軟體：立即更新裝置軟體。

     > **Note**
     >
     > 現在更新軟體可能會中斷任何作用中的使用者工作階段。

   - 在每個裝置維護時段更新軟體 - 在裝置的排程維護時段更新環境軟體。

6. 核取此方塊以授權更新。必須核取此方塊才能更新軟體。
7. 選取安裝按鈕。

WorkSpaces 精簡型客戶端軟體版本

WorkSpaces 精簡型客戶端是一種 AWS 最終使用者運算服務，可讓使用者存取裝置上的虛擬桌面。這些裝置會使用新的軟體集定期更新。下表說明所有發行的軟體集。管理員可以使用 AWS 管理主控台來檢視可用的軟體集。

軟體集	版本日期	變更
2.20.3	03-19-2026	• 修正 Chromium 的 CVE-2026-3909 和

軟體集	版本日期	變更
		CVE-2026-3910 重大安全問題。
2.20.2	02-23-2026	• 修正 Chromium 的 CVE-2026-2441 嚴重安全問題。
2.20.1	11-18-2025	• 修正 Chromium 的 CVE-2025-13223 和 CVE-2025-13224 重大安全問題。
2.20.0	11-5-2025	• 改善裝置的身分驗證。
2.19.0	9-30-2025	• 重新啟動、關閉和休眠等工具列動作現在需要最終使用者使用 WorkSpaces 重新驗證身分。 • 修正最終使用者無法使用 Ctrl+Space 金鑰在 Excel 中選取資料欄的問題。 • 已變更鎖定和授權頁面的內部 URLs。
2.18.0	8-28-2025	• 已將結束工作階段按鈕新增至裝置工具列。 • 修正在裝置上錯誤顯示活動狀態通知的問題。 • 新增對工作階段身分驗證中 FIDO2 的支援。 • 一般修正和改善。

軟體集	版本日期	變更
2.17.0	7-30-2025	• 可插拔 USB 集線器 UD-3900Z 現在支援與 WorkSpaces 精簡型客戶端搭配使用。 • 新增支援使用西班牙文鍵盤的 AltGr 金鑰。 • 修正導致裝置使用者工作階段活動項目重複的問題。 • 新增對數字鍵盤上的 Enter 鍵的支援。 • 一般修正和改善。
2.16.2	7-22-2025	• 修正 Chromium 的 CVE-2025-6558 嚴重安全問題。
2.16.1	7-3-2025	• 修正 Chromium 的 CVE-2025-6554 重大安全問題。
2.16.0	6-27-2025	• 新增網路延遲的通知。 • 新增從工作階段期間變暗的第二個監視器復原的功能。 • 修正在裝置從休眠模式返回後，顯示器顯示白色畫面或未自動延伸的問題。
2.15.0	6-19-2025	• 新增對拉丁美洲西班牙文和國際英文鍵盤的支援。 • 當裝置長時間未偵測到鍵盤或滑鼠活動時，最終使用者會看到通知。

軟體集	版本日期	變更
2.14.1	6-09-2025	• 修正 Chromium 的 CVE-2025-5419 重大安全問題。
2.13.0	3-31-2025	• 最終使用者將產品滿意度意見回饋問卷視為通知。 • 新增 FIDO2 身分驗證流程的發行前功能支援。請參閱 FIDO2 工作階段前詳細資訊。 • 如果在工作階段中播放音訊/視訊，裝置將不會進入休眠狀態。 • 最終使用者會在監視器連線和中斷連線時看到通知。 • 裝置會從作業系統收集診斷資訊，以改善服務。 • 修正軟體安裝日期設定中顯示不正確日期的問題。
2.14.0	4-29-2025	• 可用性改善和錯誤修正。

軟體集	版本日期	變更
2.13.0	3-31-2025	• 最終使用者將產品滿意度意見回饋問卷視為通知。 • 新增 FIDO2 身分驗證流程的發行前功能支援。請參閱 FIDO2 工作階段前詳細資訊。 • 如果在工作階段中播放音訊/視訊，裝置將不會進入休眠狀態。 • 最終使用者會在監視器連線和中斷連線時看到通知。 • 裝置會從作業系統收集診斷資訊，以改善服務。 • 修正軟體安裝日期設定中顯示不正確日期的問題。
2.12.0	1-30-2025	• 修正最終使用者在按下滑鼠上的返回按鈕時登出工作階段的問題。
2.11.2	1-24-2025	• 修正 呼叫期間音訊在監視器之間移動滑鼠時爆裂的問題。
2.11.1	12-27-2024	• 修正雙監視器自動延伸問題。 • VoiceView 標籤的次要改進。
2.11.0	12-19-2024	• WorkSpaces 精簡型客戶端現在支援 VoiceView 和 Magnifier。

軟體集	版本日期	變更
2.10.0	11-22-2024	• 最終使用者可以使用鍵盤快速鍵收合裝置工具列。
2.9.0	10-28-2024	• 管理員現在可以在特定裝置的裝置詳細資訊頁面下，在 AWS 主控台中檢視其最終使用者的裝置設定。 • WorkSpaces 精簡型客戶端現在支援單一螢幕的 2K 解析度監控。 • 最終使用者可以在其 WorkSpaces 精簡型客戶端裝置上查看與網路診斷相關的通知。 • 最終使用者可以根據自己的偏好，選擇將裝置工具列放在左側或右側。 • 修正裝置在休眠或閒置期間未安裝軟體更新的問題。
2.8.1	09-26-2024	• 已修正在裝置從休眠中喚醒後，無法開啟第二個監視器的重要問題。

軟體集	版本日期	變更
2.8.0	09-06-2024	• 精簡型客戶端支援 4K 解析度的監視器。 • 即使 WorkSpaces 精簡型客戶端裝置管理服務暫時無法使用，使用者仍可連線至 VDI 工作階段。 • 修正 AWS 主控台中的使用者活動詳細資訊區段顯示重複項目的問題。 • 最終使用者可以在 WorkSpaces 精簡型客戶端上串流 WorkSpaces 時使用 PrintScreen 選項。
2.7.1	08-27-2024	• Chromium 的 CVE-2024-7971 和 CVE-2024-7965 重大安全問題的零時差修正。
2.7.0	07-29-2024	• 改善第二個監視器的效能。 • 修正工具列語言未影響裝置語言變更的問題。 • 裝置現在會收集診斷資訊以改善服務。

軟體集	版本日期	變更
2.6.0	07-09-2024	• 使用者可以延遲傳入的軟體更新，以便完成其工作，而不會中斷。 • 裝置設定可讓使用者忘記儲存的 WiFi 網路。 • 改善工作階段中音訊/視訊通話的效能。 • VDI 工作階段的某些使用者設定會在裝置重新啟動期間保留。
2.5.0	06-13-2024	• 修正啟動工作階段之前，裝置從睡眠中喚醒時短暫顯示鍵盤和滑鼠設定畫面的問題。 • 裝置工具列上的首頁按鈕重新命名為登入。 • 改善工作階段中音訊/視訊通話的效能。
2.4.3	05-29-2024	• Chromium 的 CVE-2024-5274 重大安全問題的零時差修正。
2.4.2	05-17-2024	• Chromium 的 CVE-2024-4947 重大安全問題的零時差修正。

軟體集	版本日期	變更
2.4.1	05-15-2024	• Chromium 的 CVE-2024-4671 和 CVE-2024-4761 重大安全問題的零時差修正。 • 已修正允許在 WorkSpaces 登入頁面上以滑鼠右鍵按一下 AWS 和隱私權連結以獨立模式開啟瀏覽器的問題。
2.4.0	05-09-2024	• 已修正封鎖 "accounts.google.com" 並防止使用 Google Workspace 做為 WorkSpaces 應用程式 IDP 工作階段的問題。 • 在畫面上的任何區域中按一下，裝置設定工具列會自動收合。
2.3.0	04-05-2024	• 裝置設定會顯示在收合的工具列中，以便更有效地利用可見畫面。 • 最終使用者可以將持續時間設定為等待，再讓裝置處於閒置狀態。 • 修正「about：blank」URL 出現在第二個顯示器上的問題。 • 修正延長顯示關閉時導致白色畫面的問題。 • 最終使用者設定的磁碟區層級現在會在裝置重新啟動期間持續存在。

軟體集	版本日期	變更
2.2.1	02-16-2024	• 修正登入程序期間發生的問題，導致使用者無法登入使用 SAML 2.0 身分驗證設定的 WorkSpaces。
2.2.0	02-08-2024	• 新增對 ISO 鍵盤的支援，包括英文（英國）、法文、德文、義大利文、西班牙文地區設定。
2.1.2	01-26-2024	• Chromium 的 CVE-2024-0519 重大安全問題的零時差修正。 • 改善與鎖定功能相關的最終使用者延遲。 • 面向內部裝置的端點會切換到 'thinclient*' 網域。
2.1.1	12-21-2023	• Chromium 的 CVE-2023-7024 重大安全問題的零時差修正。
2.1.0	12-20-2023	• 將首頁按鈕新增至裝置設定，並啟用對中繼金鑰的支援。這可讓最終使用者按下 Meta+L 來叫用鎖定畫面。
2.0.1	12-06-2023	• Chromium 的 CVE-2024-6345 重大安全問題的零時差修正。
2.0.0	11-15-2023	• 初始版本

在 WorkSpaces 精簡型客戶端資源上使用標籤

您可以將自己的中繼資料作為標籤指派給每個資源，以整理和管理 WorkSpaces 精簡型客戶端的資源。您可以指定每一個標籤的金鑰和值。索引鍵可以是一般類別，例如「專案」、「擁有者」或「環境」，與特定相關的值。您可以使用標籤作為簡單但強大的方法來管理 AWS 資源和組織資料，包括帳單資料。

當您將標籤新增至現有資源時，這些標籤不會出現在成本配置報告中，直到下個月的第一天為止。例如，如果您在 7 月 15 日將標籤新增至現有的 WorkSpaces 精簡型客戶端裝置，則在 8 月 1 日之前，標籤都不會出現在您的成本分配報告中。如需詳細資訊，請參閱《AWS Billing 使用者指南》中的使用成本分配標籤。

> **Note**
>
> 若要在 Cost Explorer 中檢視 WorkSpaces 精簡型客戶端資源標籤，您必須遵循《AWS Billing 使用者指南》中啟用使用者定義的成本分配標籤中的說明，啟用已套用至 WorkSpaces 精簡型客戶端資源的標籤。
>
> 標籤會在啟用後 24 小時出現，但與這些標籤相關聯的值可能需要 4-5 天才會出現在 Cost Explorer 中。此外，若要在 Cost Explorer 中顯示並提供成本資料，已標記的 WorkSpaces 精簡型客戶端資源必須在該期間產生費用。Cost Explorer 只會顯示從標籤啟動時開始的成本資料。目前沒有可用的歷史資料。

您可以標記的資源：

- 建立以下資源時，您可以將標籤新增至這些資源：WorkSpaces 精簡型客戶端環境。
- 您可以將標籤新增至下列類型的現有資源：WorkSpaces 精簡型用戶端環境、裝置和軟體集。
- 您可以為環境中的裝置設定標籤，以便在註冊裝置時自動套用。

標籤限制

- 每一資源標籤數上限：50
- 金鑰長度上限 — 128 個 Unicode 字元
- 最大值長度—256 個 Unicode 字元
- 標籤金鑰與值皆區分大小寫。允許的字元包括可用 UTF-8 表示的英文字母、空格和數字，還有以下特殊字元：+ - = . _ : / @。不可使用結尾或前方空格。

- 請勿在標籤名稱或值中使用 aws: 字首，因為其已保留供 AWS 使用。您不可編輯或刪除具此字首的標籤名稱或值。

使用 主控台管理現有環境的標籤

1. 開啟 WorkSpaces 精簡型用戶端主控台。
2. 選取環境以開啟其詳細資訊頁面
3. 選擇編輯。
4. 在標籤區段中，執行下列一或多個動作：。
   - 若要新增標籤，請選擇新增標籤，然後編輯索引鍵和值的值。
   - 若要更新標籤，請編輯值的值。
   - 若要刪除標籤，請選擇標籤旁的移除。
5. 完成標籤更新後，請選擇儲存。

使用 主控台管理現有裝置的標籤

1. 開啟 WorkSpaces 精簡型用戶端主控台。
2. 選取裝置以開啟其詳細資訊頁面。
3. 選擇標籤。
4. 選擇管理標籤。
5. 執行下列其中一項或多項：
   - 若要新增標籤，請選擇新增標籤，然後編輯索引鍵和值的值。
   - 若要更新標籤，請編輯值的值。
   - 若要刪除標籤，請選擇標籤旁的移除。
6. 完成標籤更新後，請選擇儲存。

使用 主控台管理新裝置的標籤

1. 開啟 WorkSpaces 精簡型用戶端主控台。
2. 選取環境以開啟其詳細資訊頁面。
3. 選擇編輯。
4. 在裝置建立標籤區段中，執行下列一或多個動作：

- 若要新增標籤，請選擇新增標籤，然後編輯索引鍵和值的值。
- 若要更新標籤，請編輯值的值。
- 若要刪除標籤，請選擇標籤旁的移除。

5. 完成標籤更新後，請選擇儲存。

建立裝置時，它會向環境註冊，並套用裝置建立標籤。這只會在新裝置註冊期間發生。此外，系統會使用做為值的環境 ID 套用`aws:thinclient:environment-id`系統標籤。

使用主控台管理軟體更新的標籤

1. 開啟 WorkSpaces 精簡型用戶端主控台。
2. 選取軟體更新以開啟其詳細資訊頁面。
3. 在標籤區段中，選擇管理標籤。
4. 執行下列其中一項或多項：

- 若要新增標籤，請選擇新增標籤，然後編輯索引鍵和值的值。
- 若要更新標籤，請編輯值的值。
- 若要刪除標籤，請選擇標籤旁的移除。

5. 完成標籤更新後，請選擇儲存。

Amazon WorkSpaces 精簡型客戶端中的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了符合最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模式將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。作為AWS 合規計畫的一部分，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 Amazon WorkSpaces 精簡型客戶端的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 WorkSpaces 精簡型客戶端時套用共同責任模式。下列主題說明如何將 WorkSpaces 精簡型客戶端設定為符合您的安全與合規目標。您也可以了解如何使用其他 AWS 服務來協助您監控和保護 WorkSpaces 精簡型客戶端資源。

主題

- Amazon WorkSpaces 精簡型客戶端中的資料保護
- Amazon WorkSpaces 精簡型客戶端的身分和存取管理
- Amazon WorkSpaces 精簡型客戶端的恢復能力
- Amazon WorkSpaces 精簡型客戶端中的漏洞分析和管理

Amazon WorkSpaces 精簡型客戶端中的資料保護

AWS 共同責任模型適用於 Amazon WorkSpaces 精簡型客戶端的資料保護。如此模型所述， AWS 負責保護執行所有 的 全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱AWS 安全性部落格上的AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 WorkSpaces 精簡型客戶端或使用主控台 AWS CLI、API 或 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

Amazon WorkSpaces 精簡型客戶端會收集並提供使用者使用 WorkSpaces 精簡型客戶端裝置及其與虛擬桌面服務互動的相關資訊。例如，可用的記憶體、網路診斷、網路資訊、裝置連線能力、SAML 登入資料、裝置識別資訊和當機報告。此資訊用於為您提供服務，並可能用於改善服務的使用者體驗。此外，僅為了向您提供服務，資訊可能會傳輸到使用者使用該服務 AWS 的區域之外。我們根據AWS 隱私權聲明處理此資訊。

主題

資料加密

WorkSpaces 精簡型客戶端會收集環境和裝置自訂資料，例如使用者設定、裝置識別符、身分提供者資訊以及串流桌面識別符。WorkSpaces 精簡型客戶端也會收集工作階段時間戳記。收集的資料存放在 Amazon DynamoDB 和 Amazon S3 中。WorkSpaces 精簡型客戶端使用 AWS Key Management Service (KMS) 進行加密。

若要保護內容，請遵循下列指導方針：

- 實作最低權限存取，並建立要用於 WorkSpaces 精簡型客戶端動作的特定角色。
- 透過提供客戶自管金鑰保護端對端資料，以便 WorkSpaces 精簡型客戶端可以使用您提供的金鑰來加密靜態資料。
- 在分享環境啟用代碼和使用者憑證時請小心：
  - 管理員需登入 WorkSpaces 精簡型客戶端主控台，而且使用者需提供啟用代碼，供 WorkSpaces 精簡型客戶端設定使用憑證來登入串流桌面。
  - 擁有實體存取權限的任何人都可以設定 WorkSpaces 精簡型客戶端，但除非他們擁有有效的啟用代碼和使用者憑證進行登入，否則無法啟動工作階段。
- 使用者可以選擇使用裝置工具列鎖定螢幕、重新啟動或關閉裝置，以明確結束其工作階段。如此會捨棄裝置工作階段並清除工作階段憑證。

WorkSpaces 精簡型客戶端預設會使用 AWS KMS 加密所有敏感資料，以保護內容和中繼資料的安全。如果套用現有設定時發生錯誤，則使用者無法存取新的工作階段，且裝置無法套用軟體更新。

Amazon WorkSpaces 精簡型客戶端的靜態資料加密

Amazon WorkSpaces 精簡型客戶端預設提供加密，以使用 AWS 擁有的加密金鑰來保護靜態的敏感客戶資料。

- AWS 擁有的金鑰 — Amazon WorkSpaces 精簡型客戶端預設使用這些金鑰自動加密個人身分識別資料。您無法檢視、管理或使用 AWS 擁有的金鑰或稽核其使用方式。不過，您不必採取任何動作或變更任何程式，即可保護加密您資料的金鑰。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 AWS 擁有的金鑰。

依預設加密靜態資料，有助於降低保護敏感資料所涉及的營運開銷和複雜性。同時，其可讓您建置符合嚴格加密合規性和法規要求的安全應用程式。

雖然您無法停用此層加密或選取替代加密類型，但您可以在建立精簡型客戶端環境時選擇客戶自管金鑰，在 AWS 擁有的現有加密金鑰上新增第二層加密：

- 客戶受管金鑰 — Amazon WorkSpaces 精簡型客戶端支援使用您建立、擁有和管理的對稱客戶受管金鑰，在現有 AWS 擁有的加密上新增第二層加密。由於您可以完全控制此加密層，因此您可以執行如下任務：
  - 建立和維護金鑰政策

- 建立和維護 IAM 政策
- 啟用和停用金鑰政策
- 輪換金鑰密碼編譯資料
- 新增 標籤
- 建立金鑰別名
- 安排金鑰供刪除

如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的客戶自管金鑰。

以下表格摘要說明 Amazon WorkSpaces 精簡型客戶端如何加密個人可識別資料。

資料類型	AWS 擁有的金鑰加密	客戶自管金鑰加密 (選用)
環境名稱 WorkSpaces 精簡型客戶端環境名稱	已啟用	已啟用
裝置名稱 WorkSpaces 精簡型客戶端裝置名稱	已啟用	已啟用
使用者活動 WorkSpaces 精簡型客戶端使用者活動	已啟用	已啟用
裝置設定 WorkSpaces 精簡型客戶端裝置設定	已啟用	已啟用
裝置建立標籤 WorkSpaces 精簡型客戶端環境裝置建立標籤	已啟用	已啟用

> **Note**
>
> Amazon WorkSpaces 精簡型客戶端會使用 AWS 擁有的金鑰來免費保護個人身分識別資料，以自動啟用靜態加密。
> 不過，使用客戶受管金鑰需支付 AWS KMS 費用。如需有關定價的詳細資訊，請參閱 AWS Key Management Service 定價。

Amazon WorkSpaces 精簡型客戶端如何使用 AWS KMS

Amazon WorkSpaces 精簡型客戶端需要金鑰政策，您才能使用客戶受管金鑰。

Amazon WorkSpaces 精簡型客戶端需要金鑰政策，才能將客戶受管金鑰用於下列內部操作：

- 將`GenerateDataKey`請求傳送至 AWS KMS 以加密資料。
- 將`Decrypt`請求傳送至 AWS KMS 以解密加密的資料。

您可以隨時移除服務對客戶受管金鑰的存取權。如果您這麼做，Amazon WorkSpaces 精簡型客戶端就無法存取由客戶自管金鑰加密的任何資料，這會影響與該資料相依的操作。例如，如果您嘗試取得 WorkSpaces 精簡型客戶端無法存取的環境詳細資訊，則操作會傳回`AccessDeniedException`錯誤。 WorkSpaces 此外，WorkSpaces 精簡型客戶端裝置將無法使用 WorkSpaces 精簡型客戶端環境。

建立客戶受管金鑰

您可以使用 AWS 管理主控台或 AWS KMS API 操作來建立對稱客戶受管金鑰。

建立對稱客戶自管金鑰

請依照《AWS Key Management Service 開發人員指南》中的建立對稱客戶自管金鑰的步驟進行。

金鑰政策

金鑰政策會控制客戶受管金鑰的存取權限。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶自管金鑰時，可以指定金鑰政策。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的管理客戶自管金鑰的存取。

若要將客戶自管金鑰與 Amazon WorkSpaces 精簡型客戶端資源搭配使用，必須在金鑰政策中允許下列 API 操作：

- kms:DescribeKey — 提供客戶受管金鑰詳細資訊，以便 Amazon WorkSpaces 精簡型客戶端可以驗證金鑰。
- kms:GenerateDataKey：允許使用客戶自管金鑰來加密資料。
- kms:Decrypt：允許使用客戶自管金鑰來解密資料。

以下是您可以為 Amazon WorkSpaces 精簡型客戶端新增的政策陳述式範例：

```
{
    "Statement":
    [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
 data",
            "Effect": "Allow",
            "Principal": {"Service": "thinclient.amazonaws.com"},
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn":
                         "arn:aws:thinclient:region:111122223333:*",
```

```
                    "kms:EncryptionContext:aws:thinclient:arn":
                        "arn:aws:thinclient:region:111122223333:*"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

如需有關在政策中指定許可的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。

如需有關針對金鑰存取進行疑難排解的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。

為 WorkSpaces 精簡型客戶端指定客戶自管金鑰

您可以將客戶自管金鑰指定為下列資源的第二層加密：

- WorkSpaces 精簡型客戶端環境

建立環境時，您可以透過提供 Amazon WorkSpaces 精簡型客戶端用來加密可識別個人資料的 `kmsKeyArn`，指定資料金鑰。

- `kmsKeyArn` — AWS KMS 客戶受管金鑰的金鑰識別符。提供金鑰 ARN。

當新的 WorkSpaces 精簡型客戶端裝置新增至使用客戶受管金鑰加密的 WorkSpaces 精簡型客戶端環境時，WorkSpaces 精簡型客戶端裝置會從 WorkSpaces 精簡型客戶端環境繼承客戶受管金鑰設定。

加密內容是一組選用的金鑰值對，其中包含有關資料的其他內容資訊。

AWS KMS 使用加密內容做為額外的已驗證資料，以支援已驗證的加密。當您在加密資料的請求中包含加密內容時， AWS KMS 會將加密內容繫結至加密的資料。若要解密資料，請在請求中包含相同的加密內容。

Amazon WorkSpaces 精簡型客戶端加密內容

Amazon WorkSpaces 精簡型客戶端在所有 AWS KMS 密碼編譯操作中使用相同的加密內容，其中金鑰為 ，`aws:thinclient:arn`而值為 Amazon Resource Name (ARN)。

以下是環境加密內容：

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

以下是裝置加密內容：

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

使用加密內容進行監控

使用對稱客戶自管金鑰加密 WorkSpaces 精簡型客戶端環境和裝置資料時，您也可以在稽核記錄和日誌中使用加密內容，以識別客戶自管金鑰的使用方式。加密內容也會出現在 AWS CloudTrail 或 Amazon CloudWatch Logs 產生的日誌中。

使用加密內容控制對客戶自管金鑰的存取權限

您也可以在金鑰政策和 IAM 政策中，使用加密內容來控制對對稱客戶受管金鑰的存取。

以下是授予特定加密內容之客戶自管金鑰存取權限的金鑰政策陳述式範例。此政策陳述式中的條件要求 `kms:Decrypt` 呼叫具有指定加密內容的加密內容限制條件。

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
```

```
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

監控 Amazon WorkSpaces 精簡型客戶端的加密金鑰

當您搭配 Amazon WorkSpaces 精簡型客戶端資源使用 AWS KMS 客戶受管金鑰時，您可以使用 AWS CloudTrail 或 Amazon CloudWatch Logs 來追蹤 Amazon WorkSpaces 精簡型客戶端傳送至 AWS KMS 的請求。

下列範例是 DescribeKey、GenerateDataKey、 的 AWS CloudTrail 事件Decrypt，用於監控 Amazon WorkSpaces 精簡型客戶端呼叫的 KMS 操作，以存取客戶受管金鑰加密的資料：

在下列範例中，您可以查看 encryptionContext 的 WorkSpaces 精簡型客戶端環境。系統會為 WorkSpaces 精簡型客戶端裝置記錄類似的 CloudTrail 事件。

DescribeKey

Amazon WorkSpaces 精簡型客戶端使用 DescribeKey操作來驗證 KMS 客戶受管 AWS 金鑰。

下面的範例事件會記錄 DescribeKey 操作：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
```

```
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces 精簡型客戶端會使用 GenerateDataKey 操作加密資料。

下面的範例事件會記錄 GenerateDataKey 操作：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

當 Amazon WorkSpaces 精簡型客戶端使用 GenerateDataKey儲存裝置資訊時，系統會使用 GenerateDataKey操作來加密資料。

GenerateDataKey 操作在 KMS 金鑰政策陳述式中允許，其中 Sid 為「允許 Amazon WorkSpaces 精簡型用戶端服務加密和解密資料」。

下列範例事件會記錄 GenerateDataKey 操作：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
```

```
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces 精簡型客戶端會使用 `Decrypt` 操作解密資料。

下面的範例事件會記錄 `Decrypt` 操作：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
```

```
}
```

Decrypt (by service)

當 WorkSpaces 精簡型客戶端裝置存取環境或裝置資訊時，系統會使用 Decrypt操作來解密資料。Decrypt 操作在 KMS 金鑰政策陳述式中允許，其中 Sid 為「允許 Amazon WorkSpaces 精簡型用戶端服務加密和解密資料」。

下列範例事件會記錄透過 授權Decrypt的操作Grant：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
```

```
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

進一步了解

下列資源提供有關靜態資料加密的詳細資訊：

- 如需有關 AWS Key Management Service 基本概念的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。
- 如需有關 AWS Key Management Service 安全最佳實務的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。

傳輸中加密

WorkSpaces 精簡型客戶端會加密透過 HTTPS 和 TLS 1.2 傳輸中的資料。您可以使用主控台或直接 API 呼叫，將請求傳送至 WorkSpaces 精簡型客戶端。傳輸的請求資料會透過 HTTPS 或 TLS 連線進行加密。請求資料可以從 AWS 主控台、 AWS 命令列界面或 AWS SDK 傳輸到 WorkSpaces 精簡型客戶端。這也包含裝置上的任何軟體更新。

預設會設定對傳輸中的資料進行加密，預設會設定安全連線 (HTTPS、TLS)。

金鑰管理

您可以提供自己的客戶受管 AWS KMS 金鑰來加密您的客戶資訊。如果您未提供金鑰，WorkSpaces 精簡型客戶端會使用 AWS 擁有的金鑰。您可以使用 AWS SDK 來設定金鑰。

網路工作流量隱私權

管理員可以檢視 WorkSpaces 精簡型客戶端工作階段事件，包括開始時間和待處理軟體更新資訊。這些日誌會在 WorkSpaces 精簡型客戶端主控台中加密並安全地傳送給客戶。桌面服務會記錄個別串流

桌面工作階段的使用者資訊和更多詳細資訊。如需詳細資訊，請參閱監控 WorkSpaces、監控和報告 WorkSpaces 應用程式，或 WorkSpaces Web 的使用者存取記錄。

Amazon WorkSpaces 精簡型客戶端的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可以控制誰能進行身分驗證 (已登入) 和獲得授權 (具有許可) 以使用 WorkSpaces 精簡型客戶端資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 疑難排解 Amazon WorkSpaces 精簡型客戶端身分和存取)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Amazon WorkSpaces 精簡型客戶端如何搭配 IAM 運作)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 Amazon WorkSpaces 精簡型客戶端的身分型政策範例)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和 資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。

- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon WorkSpaces 精簡型客戶端如何搭配 IAM 運作

在您使用 IAM 管理 WorkSpaces 精簡型客戶端的存取權限之前，請了解有哪些 IAM 功能可搭配 WorkSpaces 精簡型客戶端使用。

可與 Amazon WorkSpaces 精簡型客戶端搭配使用的 IAM 功能

IAM 功能	WorkSpaces 精簡型客戶端支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	否

若要全面了解 WorkSpaces 精簡型客戶端和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

WorkSpaces 精簡型客戶端的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

WorkSpaces 精簡型客戶端的身分型政策範例

若要檢視 WorkSpaces 精簡型客戶端身分型政策範例，請參閱Amazon WorkSpaces 精簡型客戶端的身分型政策範例。

WorkSpaces 精簡型客戶端內的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

WorkSpaces 精簡型客戶端的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 WorkSpaces 精簡型客戶端動作的清單，請參閱《服務授權參考》中的 Actions Defined by Amazon WorkSpaces Thin Client。

WorkSpaces 精簡型客戶端中的政策動作會在動作之前使用以下字首：

```
thinclient
```

若要在單一陳述式中指定多個動作，請以逗號分隔，如下列範例所示：

```
"Action": [
      "thinclient:action1",
      "thinclient:action2"
         ]
```

若要檢視 WorkSpaces 精簡型客戶端身分型政策範例，請參閱Amazon WorkSpaces 精簡型客戶端的身分型政策範例。

WorkSpaces 精簡型客戶端的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 WorkSpaces 精簡型客戶端資源類型及其 ARN 的清單，請參閱《服務授權參考》中的 Resources Defined by Amazon WorkSpaces Thin Client。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Actions Defined by Amazon WorkSpaces Thin Client。

若要檢視 WorkSpaces 精簡型客戶端身分型政策範例，請參閱Amazon WorkSpaces 精簡型客戶端的身分型政策範例。

WorkSpaces 精簡型客戶端的政策條件鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 WorkSpaces 精簡型客戶端條件鍵的清單，請參閱《服務授權參考》中的 Condition Keys for Amazon WorkSpaces Thin Client。若要了解您可以搭配哪些動作和資源使用條件鍵，請參閱 Actions Defined by Amazon WorkSpaces Thin Client。

若要檢視 WorkSpaces 精簡型客戶端身分型政策範例，請參閱Amazon WorkSpaces 精簡型客戶端的身分型政策範例。

WorkSpaces 精簡型客戶端中的 ACL

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

ABAC 與 WorkSpaces 精簡型客戶端

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

將臨時憑證與 WorkSpaces 精簡型客戶端搭配使用

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

WorkSpaces 精簡型客戶端的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

WorkSpaces 精簡型客戶端的服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 WorkSpaces 精簡型客戶端功能。只有 WorkSpaces 精簡型客戶端提供指引時，才能編輯服務角色。

WorkSpaces 精簡型客戶端的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon WorkSpaces 精簡型客戶端的身分型政策範例

依預設，使用者和角色不具備建立或修改 WorkSpaces 精簡型客戶端資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需有關 WorkSpaces 精簡型客戶端定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱《服務授權參考》中的 Amazon WorkSpaces 精簡型客戶端的動作、資源和條件鍵。

主題

- 政策最佳實務
- 使用 WorkSpaces 精簡型客戶端主控台
- 授予 WorkSpaces 精簡型客戶端的唯讀存取權
- 允許使用者檢視他們自己的許可
- 授予對 WorkSpaces 精簡型客戶端的完整存取權限

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 WorkSpaces 精簡型客戶端資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 ，例如 使用服務動作 AWS 服務，您也可以使用條件來授予存取 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

使用 WorkSpaces 精簡型客戶端主控台

若要存取 Amazon WorkSpaces 精簡型客戶端主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視 中 WorkSpaces 精簡型客戶端資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

授予 WorkSpaces 精簡型客戶端的唯讀存取權

此範例說明如何建立政策，允許 IAM 使用者檢視 WorkSpaces 精簡型客戶端組態，但不進行變更。此政策包含使用 AWS CLI 或 AWS API 在主控台或程式上完成此動作的許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授予對 WorkSpaces 精簡型客戶端的完整存取權限

此範例說明如何建立授予 WorkSpaces 精簡型客戶端 IAM 使用者完整存取權的政策。此政策包含使用 AWS CLI 或 AWS API 在主控台或程式上完成所有 WorkSpaces 精簡型客戶端動作的許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
```

```
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

AWS Amazon WorkSpaces 精簡型客戶端的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess

您可將 `AmazonWorkSpacesThinClientReadOnlyAccess` 政策連接到 IAM 身分。此政策會將完整存取許可授予 WorkSpaces 精簡型客戶端服務及其相依性。如需此受管政策的詳細資訊，請參閱《 受管政策參考》指南》中的 AmazonWorkSpacesThinClientReadOnlyAccess。 AWS

許可詳細資訊

此政策包含以下許可。

- `thinclient` (WorkSpaces 精簡型客戶端） – 允許唯讀存取所有 WorkSpaces 精簡型客戶端動作。
- `workspaces` (WorkSpaces) – 允許描述 WorkSpaces 目錄和連線別名的許可。這是用來檢查您的 WorkSpaces 資源是否與 WorkSpaces 精簡型客戶端相容。它也用於在 WorkSpaces 精簡型客戶端 AWS 主控台中顯示這些資源。

- `workspaces-web` (WorkSpaces Secure Browser) – 允許描述 WorkSpaces Secure Browser 入口網站和使用者設定的許可。這是用來檢查您的 WorkSpaces Secure Browser 資源是否與 WorkSpaces 精簡型客戶端相容。它也用於在 WorkSpaces 精簡型客戶端 AWS 主控台中顯示這些資源。
- `appstream` (WorkSpaces 應用程式) – 允許描述 WorkSpaces 應用程式堆疊的許可。這用於檢查您的 WorkSpaces 應用程式資源是否與 WorkSpaces 精簡型客戶端相容。它也用於在 WorkSpaces 精簡型客戶端 AWS 主控台中顯示這些資源。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
```

```
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 受管政策：AmazonWorkSpacesThinClientFullAccess

您可將 AmazonWorkSpacesThinClientFullAccess 政策連接到 IAM 身分。此政策會將完整存取許可授予 WorkSpaces 精簡型客戶端服務及其相依性。如需此受管政策的詳細資訊，請參閱《 受管政策參考指南》中的 AmazonWorkSpacesThinClientFullAccess。 AWS

許可詳細資訊

此政策包含以下許可：

- thinclient (WorkSpaces 精簡型客戶端） – 允許完整存取所有 WorkSpaces 精簡型客戶端動作。
- workspaces (WorkSpaces) – 允許描述 WorkSpaces 目錄和連線別名的許可。這是用來檢查您的 WorkSpaces 資源是否與 WorkSpaces 精簡型客戶端相容。它也用於在 WorkSpaces 精簡型客戶端 AWS 主控台中顯示這些資源。
- workspaces-web (WorkSpaces Secure Browser) – 允許描述 WorkSpaces Secure Browser 入口網站和使用者設定的許可。這是用來檢查您的 WorkSpaces Secure Browser 資源是否與 WorkSpaces 精簡型客戶端相容。它也用於在 WorkSpaces 精簡型客戶端 AWS 主控台中顯示這些資源。
- appstream (WorkSpaces 應用程式） – 允許描述 WorkSpaces 應用程式堆疊的許可。這用於檢查您的 WorkSpaces 應用程式資源是否與 WorkSpaces 精簡型客戶端相容。它也用於在 WorkSpaces 精簡型客戶端 AWS 主控台中顯示這些資源。

- `iam` – 允許 WorkSpaces 精簡型客戶端在您的帳戶中建立服務連結角色。此角色可讓 WorkSpaces 精簡型客戶端代表您將指標發佈至 CloudWatch。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "AllowCreateServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

WorkSpaces 精簡型客戶端更新受 AWS 管政策

變更	描述	Date
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy – 已移除政策	WorkSpaces 精簡型客戶端已移除 AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 區段。	2025 年 11 月 12 日
AmazonWorkSpacesThinClientFullAccess - 更新的政策 AmazonWorkSpacesThinClientMonitoringServiceRolePolicy – 新政策	WorkSpaces 精簡型客戶端已更新政策，以包含服務連結角色。	2025 年 8 月 26 日
AmazonWorkSpacesThinClientReadOnlyAccess - 更新的政策	WorkSpaces 精簡型客戶端已更新政策，以包含裝置詳細資訊和 WorkSpaces 連線別名的有限讀取許可。	2025 年 1 月 9 日

變更	描述	Date
AmazonWorkSpacesThinClientFullAccess - 更新的政策	WorkSpaces 精簡型客戶端已更新政策，以包含 WorkSpaces 連線別名的有限讀取許可。	2025 年 1 月 9 日
AmazonWorkSpacesThinClientReadOnlyAccess - 更新的政策	WorkSpaces 精簡型客戶端已更新政策，以包含 WorkSpaces 應用程式、WorkSpaces Web 和 WorkSpaces 的有限讀取許可。	2024 年 8 月 9 日
AmazonWorkSpacesThinClientFullAccess – 新政策	提供對 Amazon WorkSpaces 精簡型客戶端的完整存取權，以及對所需相關服務的有限存取權。	2024 年 8 月 9 日
AmazonWorkSpacesThinClientReadOnlyAccess – 新政策	提供對 Amazon WorkSpaces 精簡型客戶端及其相依性的唯讀存取權。	2024 年 7 月 19 日
WorkSpaces 精簡型客戶端開始追蹤變更	WorkSpaces 精簡型客戶端開始追蹤其 AWS 受管政策的變更。	2024 年 7 月 19 日

疑難排解 Amazon WorkSpaces 精簡型客戶端身分和存取

請使用以下資訊協助您診斷和修正使用 WorkSpaces 精簡型客戶端和 IAM 時可能遇到的常見問題。

主題

- 我未獲授權，不得在 WorkSpaces 精簡型客戶端中執行動作
- 我想要檢視我的存取金鑰
- 我是管理員，想要允許其他人存取 WorkSpaces 精簡型客戶端
- 我想要允許 以外的人員 AWS 帳戶 存取我的 WorkSpaces 精簡型客戶端資源

我未獲授權，不得在 WorkSpaces 精簡型客戶端中執行動作

如果 AWS 管理主控台 告知您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供使用者名稱和密碼的人員。

以下範例錯誤會在 mateojackson IAM 使用者嘗試使用主控台檢視虛構 *my-thin-client-device* 資源的詳細資訊，但卻沒有虛構 thinclient:*ListDevices* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 thinclient:ListDevices on resource: my-thin-client-device
```

在此情況下，Mateo 會要求管理員更新其政策，以允許他使用 thinclient:*ListDevices*動作來存取*my-thin-client-device*資源。

我想要檢視我的存取金鑰

在您建立 IAM 使用者存取金鑰後，您可以隨時檢視您的存取金鑰 ID。但是，您無法再次檢視您的私密存取金鑰。若您遺失了密碼金鑰，您必須建立新的存取金鑰對。

存取金鑰包含兩個部分：存取金鑰 ID (例如 AKIAIOSFODNN7EXAMPLE) 和私密存取金鑰 (例如 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)。如同使用者名稱和密碼，您必須一起使用存取金鑰 ID 和私密存取金鑰來驗證您的請求。就如對您的使用者名稱和密碼一樣，安全地管理您的存取金鑰。

> **Important**
>
> 請勿將您的存取金鑰提供給第三方，甚至是協助尋找您的標準使用者 ID。透過這樣做，您可以讓某人永久存取您的 AWS 帳戶。

建立存取金鑰對時，您會收到提示，要求您將存取金鑰 ID 和私密存取金鑰儲存在安全位置。私密存取金鑰只會在您建立它的時候顯示一次。若您遺失了私密存取金鑰，您必須將新的存取金鑰新增到您的 IAM 使用者。您最多可以擁有兩個存取金鑰。若您已有兩個存取金鑰，您必須先刪除其中一個金鑰對，才能建立新的金鑰對。若要檢視說明，請參閱《IAM 使用者指南》中的管理存取金鑰。

我是管理員，想要允許其他人存取 WorkSpaces 精簡型客戶端

若要允許其他人存取 WorkSpaces 精簡型客戶端，您必須將許可授予需要存取的人員或應用程式。如果您使用 AWS IAM Identity Center 管理人員和應用程式，您可以將許可集指派給使用者或群組，以定

義其存取層級。許可集會自動建立 IAM 政策，並將其指派給與該人員或應用程式相關聯的 IAM 角色。如需詳細資訊，請參閱AWS IAM Identity Center 《 使用者指南》中的許可集。

如果您不是使用 IAM Identity Center，則必須為需要存取的人員或應用程式建立 IAM 實體 （使用者或角色）。然後您必須將政策連接至該實體，以在 WorkSpaces 精簡型客戶端中授予其正確的許可。授予許可後，請將登入資料提供給使用者或應用程式開發人員。他們將使用這些登入資料來存取 AWS。若要進一步了解如何建立 IAM 使用者、群組、政策和許可，請參閱《IAM 使用者指南》中的 IAM 身分和政策和許可。

如需詳細資訊，請參閱授予對 WorkSpaces 精簡型客戶端的完整存取權限。

我想要允許 以外的人員 AWS 帳戶 存取我的 WorkSpaces 精簡型客戶端資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 WorkSpaces 精簡型客戶端是否支援這些功能，請參閱Amazon WorkSpaces 精簡型客戶端如何搭配 IAM 運作。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

Amazon WorkSpaces 精簡型客戶端的恢復能力

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援聯網連接。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和 可用區域的詳細資訊，請參閱AWS 全球基礎設施。

除了 AWS 全球基礎設施之外，WorkSpaces 精簡型用戶端還提供多種功能，以協助支援您的資料彈性和備份需求。

Amazon WorkSpaces 精簡型客戶端中的漏洞分析和管理

組態和 IT 控制是 AWS 與您之間的共同責任。如需詳細資訊，請參閱 AWS 共同的責任模型。

Amazon WorkSpaces 精簡型客戶端與 Amazon WorkSpaces、Amazon WorkSpaces 應用程式和 WorkSpaces Web 交叉整合。如需這些服務更新管理的詳細資訊，請參閱下列連結：

- Amazon WorkSpaces 應用程式中的更新管理
- Amazon WorkSpaces 中的更新管理
- Amazon WorkSpaces Web 中的組態與漏洞分析

監控 Amazon WorkSpaces 精簡型客戶端

監控是維護 Amazon WorkSpaces 精簡型客戶端和其他 AWS 解決方案可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 WorkSpaces 精簡型客戶端、在發生錯誤時回報，並適時採取自動動作：

- AWS CloudTrail 會擷取由 AWS 您的帳戶或代表您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」。

主題

使用 記錄 Amazon WorkSpaces 精簡型客戶端 API 呼叫 AWS CloudTrail

Amazon WorkSpaces 精簡型客戶端與 整合AWS CloudTrail，這項服務可提供使用者、角色或 所採取動作的記錄 AWS 服務。CloudTrail 會將 WorkSpaces 精簡型客戶端的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 WorkSpaces 精簡型客戶端主控台的呼叫，以及對 WorkSpaces 精簡型客戶端 API 操作發出的程式碼呼叫。您可以使用 CloudTrail 所收集的資訊，判斷對 WorkSpaces 精簡型客戶端提出的請求、提出請求的 IP 地址、提出請求的時間，以及其他詳細資訊。

CloudTrail 會記錄所有 Amazon WorkSpaces 精簡型客戶端動作，並記錄在 Amazon WorkSpaces 精簡型客戶端 API 參考中。例如，對 `CreateEnvironment`、`DeleteDevice` 和 `GetSoftwareSet` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是使用根使用者還是使用者憑證提出。
- 請求是否代表 IAM Identity Center 使用者提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

當您建立帳戶 AWS 帳戶 時CloudTrail 會在 中處於作用中狀態，而且您會自動存取 CloudTrail 事件歷史記錄。CloudTrail 事件歷史記錄為 AWS 區域中過去 90 天記錄的管理事件，提供可檢視、可搜尋、可下載且不可變的記錄。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。檢視事件歷史記錄不會產生 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立線索或 CloudTrail Lake 事件資料存放區。

CloudTrail 追蹤

線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。使用 建立的所有線索 AWS 管理主控台 都是多區域。您可以使用 AWS CLI建立單一或多區域追蹤。建議您建立多區域追蹤，因為您擷取 AWS 區域 帳戶中所有 的活動。如果您建立單一區域追蹤，您只能檢視追蹤 AWS 區域中記錄的事件。如需追蹤的詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的為您的 AWS 帳戶建立追蹤和為組織建立追蹤。

您可以透過建立追蹤，免費將持續管理事件的一個複本從 CloudTrail 傳遞至您的 Amazon S3 儲存貯體，但這樣做會產生 Amazon S3 儲存費用。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail Lake 事件資料存放區

CloudTrail Lake 讓您能夠對事件執行 SQL 型查詢。CloudTrail Lake 會將分列式 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。如需 CloudTrail Lake 的詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 AWS CloudTrail Lake。

CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

CloudTrail 中的 WorkSpaces 精簡型客戶端資料事件

資料事件提供有關在資源上執行或在資源中執行的資源操作的資訊 （ 例如，最終使用者註冊裝置 ）。這些也稱為資料平面操作。資料事件通常是大量資料的活動。根據預設，CloudTrail 不會記錄資料事件。CloudTrail 事件歷史記錄不會記錄資料事件。

資料事件需支付額外的費用。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

您可以使用 CloudTrail 主控台或 CloudTrail API 操作 AWS CLI，記錄 WorkSpaces 精簡型客戶端資源類型的資料事件。如需如何記錄資料事件的詳細資訊，請參閱 AWS CloudTrail 使用者指南中的使用 AWS 管理主控台　記錄資料事件和使用 AWS Command Line Interface記錄資料事件。

下表列出您可以記錄資料事件的 WorkSpaces 精簡型客戶端資源類型。資料事件類型 (主控台) 資料行會顯示從 CloudTrail 主控台上的資料事件類型清單中選擇的值。resources.type 值欄會顯示值，您會在使用 AWS CLI 或 CloudTrail APIs 設定進階事件選取器時指定此`resources.type`值。記錄到 CloudTrail 的資料 API 資料行會針對資源類型顯示記錄到 CloudTrail 的 API 呼叫。

資料事件類型 (主控台)	resources.type 值	記錄到 CloudTrail 的資料 API
ThinClientDevice	`AWS::WorkSpacesThinClient::Device`	• RegisterDevice • UpdateDeviceDetails

您可以設定進階事件選取器來篩選 `eventName`、`readOnly` 和 `resources.ARN` 欄位，以僅記錄對您重要的事件。如需這些欄位的詳細資訊，請參閱AWS CloudTrail API 參考中的AdvancedFieldSelector。

CloudTrail 中的 WorkSpaces 精簡型客戶端管理事件

管理事件提供有關在 資源上執行的管理操作的資訊 AWS 帳戶。這些也稱為控制平面操作。根據預設，CloudTrail 記錄管理事件。

Amazon WorkSpaces 精簡型客戶端會將所有 WorkSpaces 精簡型客戶端控制平面操作記錄為管理事件。如需 WorkSpaces 精簡型客戶端記錄到 CloudTrail 的 Amazon WorkSpaces 精簡型客戶端控制平面操作清單，請參閱 Amazon WorkSpaces 精簡型客戶端 API 參考。 CloudTrail

WorkSpaces 精簡型客戶端事件範例

一個事件代表任何來源提出的單一請求，並包含請求 API 操作的相關資訊、操作的日期和時間、請求參數等。CloudTrail 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

以下範例顯示的 CloudTrail 事件會示範 `RegisterDevice` 操作。

```
{
      "eventVersion": "1.10",
      "userIdentity": {
```

```
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-06-19T17:13:44Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "RegisterDevice",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "dsn": "G1X11X11111111XX",
        "activationCode": "xxx1xxx1",
        "model": "AFTGAZL"
      },
      "responseElements": null,
      "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
      "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "eventCategory": "Data"
    }
```

以下範例顯示的 CloudTrail 事件會示範 UpdateDeviceDetails 操作。

```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-10-21T17:46:27Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "UpdateDeviceDetails",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
    "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
    "readOnly": false,
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
      "settings": {
        "network": {
          "ethernet": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          },
          "networkInterfaceInUse": "ETHERNET",
          "wifi": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          }
        },
        "peripherals": {
          "bluetooth": {
```

```
            "enabledStatus": "ENABLED"
          },
          "keyboards": [
            {
              "name": "name",
              "type": "USB"
            }
          ],
          "mice": [
            {
              "name": "name",
              "type": "BLUETOOTH"
            }
          ],
          "sound": {
            "microphones": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "BUILT_IN"
              }
            ],
            "speakers": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "BUILT_IN"
              }
            ]
          },
          "webcams": [
            {
              "name": "name",
              "selectionStatus": "SELECTED",
              "type": "USB"
            }
          ]
        },
        "powerAndSleep": {
          "sleepAfter": "FIFTEEN_MINUTES"
        }
      },
      "updatedAt": "2024-10-21T17:46:27.624Z"
    },
```

```
    "eventCategory": "Data"
  }
```

如需有關 CloudTrail 記錄內容的資訊，請參閱《AWS CloudTrail 使用者指南》中的 CloudTrail record contents。

使用 CloudWatch 指標監控 WorkSpaces 精簡型客戶端

WorkSpaces 精簡型客戶端裝置和 Amazon CloudWatch 已整合，因此您可以收集和分析 WorkSpaces 精簡型客戶端裝置發出的效能指標。您可以使用 CloudWatch 主控台、CloudWatch 命令列界面或以程式設計方式使用 CloudWatch API 來監控這些指標。CloudWatch 也可讓您設定達到指標的指定閾值時的警示。

如需使用 CloudWatch 和警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

先決條件

沒有先決條件。WorkSpaces 精簡型客戶端裝置註冊至 環境後，便會開始發出裝置指標。

目錄

WorkSpaces 精簡型客戶端指標

`AWS/WorkSpacesThinClient` 命名空間包含下列指標。

指標	描述	Dimensions (尺寸)	統計資料	個單位
DeviceSession	連線至裝置工作階段或未處於工作階段中的 ThinClient 裝置數量。	desktopType	平均值、最小值、最大值、總和、範例計數	計數
Connected Devices	目前線上的 ThinClient 裝置數量。	N/A	平均值、最小值、最大值、總和、範例計數	計數

指標	描述	Dimensions (尺寸)	統計資料	個單位
SoftwareSetVersion	執行指定軟體版本的 ThinClient 裝置數量。	softwareSetVersion	平均值、最小值、最大值、總和、範例計數	計數
NetworkConnectionEthernet	目前透過乙太網路連線的 ThinClient 裝置數量。	N/A	平均值、最小值、最大值、總和、範例計數	計數
NetworkConnectionWifi	目前透過 WiFi 連線的 ThinClient 裝置數量。	N/A	平均值、最小值、最大值、總和、範例計數	計數

WorkSpaces 精簡型客戶端指標的維度

維度	描述
desktopType	依裝置上目前工作階段中的桌面類型篩選指標資料。如果使用者登入桌面，且裝置未休眠，則表示裝置在工作階段中。如果裝置在工作階段中，維度值將是使用的桌面類型，例如 WorkSpaces、WorkSpacesSecureBrowser 或 AppStream。如果裝置不在工作階段中，維度值將為 NotInSession。
softwareSetVersion	依裝置上安裝的 Software Set 版本篩選指標資料。X.Y.Z 維度的形式，例如 1.4.2。

使用 建立 Amazon WorkSpaces 精簡型客戶端資源 AWS CloudFormation

Amazon WorkSpaces 精簡型客戶端已與 整合 AWS CloudFormation，這項服務可協助您模型化和設定 AWS 資源。如此一來，您可以花更少的時間建立並管理資源和基礎設施。您可以建立範本來描述您想要的所有 AWS 資源 （例如環境），並為您 CloudFormation 佈建和設定這些資源。

使用 時 CloudFormation，您可以重複使用範本來持續且重複地設定 WorkSpaces 精簡型客戶端資源。描述您的資源一次，然後在多個 AWS 帳戶 和 區域中重複佈建相同的資源。

WorkSpaces 精簡型客戶端和 CloudFormation 範本

若要佈建和設定 WorkSpaces 精簡型客戶端和相關服務的資源，您必須了解 CloudFormation 範本。範本是 JSON 或 YAML 格式的文字檔案。這些範本說明您要在 CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML 格式，您可以使用 CloudFormation 設計工具來協助您開始使用 CloudFormation 範本。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》 中的什麼是 CloudFormation 設計器？。

WorkSpaces 精簡型客戶端支援在 中建立環境 CloudFormation。如需詳細資訊，包括環境的 JSON 和 YAML 範本範例，請參閱AWS CloudFormation 《 使用者指南》中的 Amazon WorkSpaces 精簡型客戶端資源類型參考。

進一步了解 CloudFormation

若要進一步了解 CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- CloudFormation API 參考
- AWS CloudFormation 命令列界面使用者指南

使用介面端點 (AWS PrivateLink) 存取 Amazon WorkSpaces 精簡型客戶端

您可以使用 在 VPC 和 Amazon WorkSpaces 精簡型客戶端之間 AWS PrivateLink 建立私有連線。您可以存取 WorkSpaces 精簡型客戶端做為 VPC，而無需使用網際網路閘道、NAT 裝置、VPN 連接或 Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 WorkSpaces 精簡型客戶端。

您可以透過建立採用 的介面端點來建立此私有連線 AWS PrivateLink。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者受管網路介面，可作為目的地為 WorkSpaces 精簡型客戶端之流量的進入點。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「透過 AWS PrivateLink存取 AWS 服務」。

WorkSpaces 精簡型客戶端的考量事項

在您為 WorkSpaces 精簡型客戶端設定介面端點之前，請檢閱《AWS PrivateLink 指南》中的考量事項。

WorkSpaces 精簡型客戶端支援透過介面端點呼叫其所有 API 動作。

為 WorkSpaces 精簡型客戶端建立介面端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface ()，為 WorkSpaces 精簡型客戶端建立介面端點AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「建立介面端點」。

使用下列服務名稱為 WorkSpaces 精簡型客戶端建立介面端點：

```
com.amazonaws.region.thinclient.api
```

如果您為介面端點啟用私有 DNS，您可以使用其預設的區域 DNS 名稱向 WorkSpaces 精簡型客戶端提出 API 請求。例如 `api.thinclient.us-east-1.amazonaws.com`。

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點政策可讓您透過介面端點完整存取 WorkSpaces 精簡型客戶端。若要控制從 VPC 授予 WorkSpaces 精簡型客戶端的存取權，請將自訂端點政策連接至介面端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「使用端點政策控制對服務的存取」。

範例：WorkSpaces 精簡型客戶端動作的 VPC 端點政策

以下是自訂端點政策的範例。將此政策連接至介面端點後，此政策會針對所有資源上的所有主體，授予列出的 WorkSpaces 精簡型客戶端動作的存取權限。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
}
```

《WorkSpaces 精簡型客戶端管理員指南》的文件歷程記錄

下表說明 WorkSpaces 精簡型客戶端管理員指南版本的文件歷史記錄。

變更	描述	日期
AWS 受管政策：AmazonWorkSpacesThinClientMonitoringServiceRolePolicy	Amazon WorkSpaces 精簡型客戶端已移除 AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 區段。	2025 年 11 月 12 日
AWS 受管政策：AmazonWorkSpacesThinClientMonitoringServiceRolePolicy AWS 受管政策：AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces 精簡型客戶端新增了 AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 受管政策。 Amazon WorkSpaces 精簡型客戶端新增了 AmazonWorkSpacesThinClientFullAccess 受管政策第 3 版。	2025 年 8 月 26 日
AWS 受管政策：AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces 精簡型客戶端已新增 AmazonWorkSpacesThinClientFullAccess 受管政策第 2 版。	2025 年 1 月 9 日
AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces 精簡型客戶端新增了 AmazonWorkSpacesThinClientReadOnlyAccess 受管政策第 3 版。	2025 年 1 月 9 日
使用 AWS CloudTrail 記錄 Amazon WorkSpaces 精簡型客戶端 API 呼叫 裝置設定	已新增資料事件的新區段。 新增裝置設定的新章節。 更新 區段中靜態資料加密的 KMS 資訊。	2024 年 10 月 28 日

變更	描述	日期
Amazon WorkSpaces 精簡型客戶端的靜態資料加密		
業務持續性	新增了業務持續性和災難復原的新章節。	2024 年 9 月 6 日
AWS 受管政策：AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces 精簡型客戶端新增了 AmazonWorkSpacesThinClientFullAccess 受管政策。	2024 年 8 月 9 日
AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces 精簡型客戶端已新增 AmazonWorkSpacesThinClientReadOnlyAccess 受管政策第 2 版。	2024 年 8 月 9 日
為 WorkSpaces 精簡型客戶端設定 WorkSpaces Personal	已更新新 WorkSpaces Personal 的 。	2024 年 8 月 7 日
為 WorkSpaces 精簡型客戶端設定 WorkSpaces 集區	已新增新 WorkSpaces 集區的新章節。	2024 年 8 月 7 日
AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces 精簡型客戶端新增了 AmazonWorkSpacesThinClientReadOnlyAccess 受管政策。	2024 年 7 月 19 日
AWS Amazon WorkSpaces 精簡型客戶端的 受管政策	Amazon WorkSpaces 精簡型客戶端開始追蹤變更。	2024 年 7 月 19 日
為 Amazon WorkSpaces 精簡型客戶端設定 WorkSpaces Amazon WorkSpaces	已更新作業系統清單。	2024 年 2 月 12 日

變更	描述	日期
為 Amazon WorkSpaces 精簡型客戶端設定 WorkSpaces 應用程式 Amazon WorkSpaces	已更新身分提供者程序。	2024 年 2 月 12 日
初始版本	初始版本	2023 年 11 月 26 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。