管理員指南

# Amazon WorkSpaces 精簡型客戶端

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon WorkSpaces 精簡型客戶端: 管理員指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 Amazon WorkSpaces 精簡型用戶端管理員主控台？ ... 1
您是第一次使用 的新手嗎？ ... 1
架構 ... 1
設定 Amazon WorkSpaces 精簡型客戶端管理員主控台 ... 4
註冊 AWS ... 4
建立 IAM 使用者 ... 4
適用於 Amazon WorkSpaces 的 VDI 精簡型客戶端管理員主控台入門 ... 6
為 WorkSpaces 精簡型客戶端設定 WorkSpaces Personal ... 6
開始之前 ... 6
步驟 1：確認您的系統符合 WorkSpaces Personal 所需的功能 ... 7
步驟 2：使用進階設定來啟動 WorkSpace ... 8
業務持續性 ... 8
為 WorkSpaces 精簡型客戶端設定 WorkSpaces 集區 ... 9
開始之前 ... 10
建立 WorkSpaces 集區 ... 10
設定 WorkSpaces 精簡型客戶端存取 ... 12
為 Amazon WorkSpaces 精簡型客戶端設定 AppStream 2.0 ... 13
步驟 1：確認您的系統符合 AppStream 2.0 所需的功能 ... 13
步驟 2：設定 AppStream 2.0 堆疊 ... 14
為 Amazon WorkSpaces 精簡型客戶端設定 Amazon WorkSpaces 安全瀏覽器 ... 14
步驟 1：確認您的系統符合 Amazon WorkSpaces 安全瀏覽器所需的功能 ... 14
步驟 2：設定 WorkSpaces 安全瀏覽器入口網站 ... 15
啟動 WorkSpaces 精簡型用戶端管理員主控台 ... 16
涵蓋區域 ... 16
啟動 WorkSpaces 精簡型客戶端管理員主控台 ... 17
使用 WorkSpaces 精簡型客戶端管理員主控台 ... 18
環境 ... 19
環境清單 ... 19
環境詳細資訊 ... 20
建立環境 ... 24
編輯環境 ... 27
刪除環境 ... 27
裝置 ... 28
裝置清單 ... 28

裝置詳細資訊 ... 30
編輯裝置名稱 ... 36
重設和取消註冊裝置 ... 36
封存裝置 ... 37
刪除裝置 ... 37
匯出裝置詳細資訊 ... 37
軟體更新 ... 38
更新環境軟體 ... 38
更新裝置軟體 ... 39
WorkSpaces 精簡型客戶端軟體版本 ... 39
在 WorkSpaces 精簡型客戶端資源上使用標籤 ... 47
安全 ... 50
資料保護 ... 50
資料加密 ... 51
靜態加密 ... 52
傳輸中加密 ... 65
金鑰管理 ... 65
網路工作流量隱私權 ... 65
身分與存取管理 ... 66
目標對象 ... 66
使用身分驗證 ... 67
使用政策管理存取權 ... 69
Amazon WorkSpaces 精簡型客戶端如何搭配 IAM 運作 ... 71
身分型政策範例 ... 77
AWS 受管政策 ... 81
故障診斷 ... 86
恢復能力 ... 88
漏洞分析和管理 ... 88
監控 ... 90
CloudTrail 日誌 ... 90
CloudTrail 資料事件 ... 91
CloudTrail 管理事件 ... 92
CloudTrail 事件範例 ... 92
AWS CloudFormation 資源 ... 97
WorkSpaces 精簡型用戶端和 AWS CloudFormation 範本 ... 97
進一步了解 AWS CloudFormation ... 97

AWS PrivateLink ..... 98
考量事項 ..... 98
建立介面端點 ..... 98
建立端點政策 ..... 98
文件歷史紀錄 ..... 100
..... cii

# 什麼是 Amazon WorkSpaces 精簡型用戶端管理員主控台？

透過 Amazon WorkSpaces 精簡型用戶端管理員主控台，管理員可以透過 WorkSpaces 精簡型用戶端入口網站管理 WorkSpaces 精簡型用戶端環境和裝置。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 精簡型用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 精簡型用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。這些需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？
- 架構


## 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

## 架構

每個 WorkSpaces 精簡型用戶端都與虛擬桌面介面 (VDI) 供應商相關聯。WorkSpaces 精簡型用戶端支援三個 VDI 供應商：

- Amazon WorkSpaces
- AppStream 2.0
- Amazon WorkSpaces 安全瀏覽器

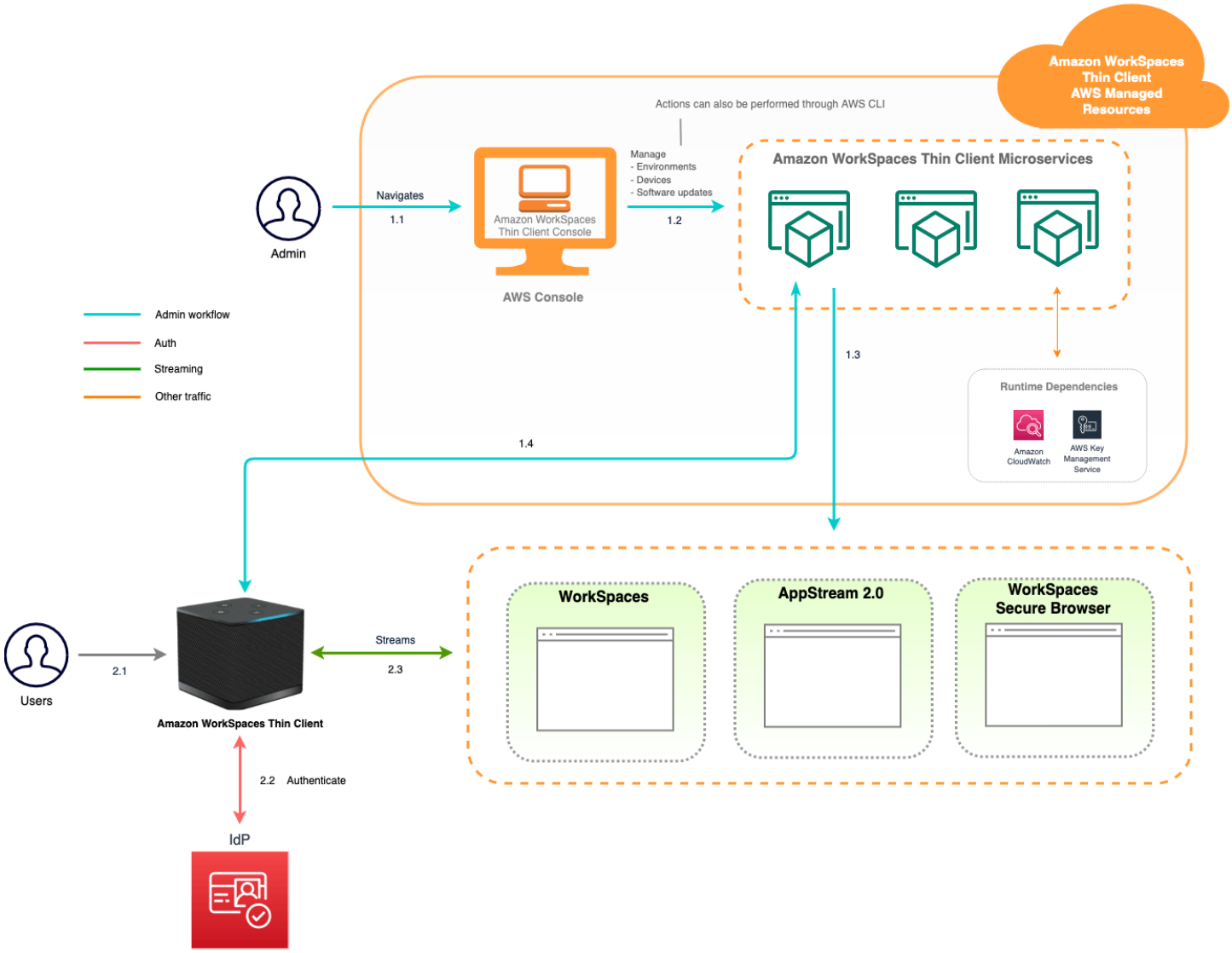
根據使用的 VDI，WorkSpaces 精簡型用戶端的資訊可透過 WorkSpaces 的目錄、AppStream 2.0 的堆疊和 WorkSpaces Secure Browser 的 Web 入口網站端點進行存取和管理。

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 AWS Directory Service，提供下列選項：Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory，也稱為 AWS Managed Microsoft AD。如需詳細資訊，請參閱 AWS Directory Service 管理員指南。

如需 AppStream 2.0 的詳細資訊，請參閱開始使用 Amazon AppStream 2.0：設定範例應用程式。AppStream 2.0 可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。AppStream 2.0 可讓使用者在自選裝置上存取所需的應用程式，並提供回應靈敏、流暢且與原生安裝的應用程式相同的使用者體驗。

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 Secure Browser 是一項隨需、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 精簡型用戶端的架構。


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
- 建立 IAM 使用者


## 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<br><br>(建議) | 使用短期憑證存取 AWS。<br><br>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<br><br>(不建議使用) | 使用長期憑證存取 AWS。 | 遵循《IAM 使用者指南》中為緊急存取建立 IAM 使用者的指示。 | 《IAM 使用者指南》中的透過管理 IAM 使用者的存取金鑰來設定程式設計存取。 |

# 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
- 為 WorkSpaces 精簡型客戶端設定 WorkSpaces 集區
- 為 Amazon WorkSpaces 精簡型客戶端設定 AppStream 2.0
- 為 Amazon WorkSpaces 精簡型客戶端設定 Amazon WorkSpaces 安全瀏覽器


## 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 |
| --- | --- |
| Web 存取 | 已啟用 |
| 支援的作業系統 | • Windows 10<br>• Windows 10 (自帶授權)<br>• Windows 11<br>• Windows 11 (自帶授權) |
| 支援的套件 | • Microsoft Power 搭配 Windows 10（伺服器 2016、2019 和 2022 型）<br>• Microsoft Power 搭配 Windows 10（伺服器 2016、2019 和 2022 型）與 Office<br>• Microsoft PowerPro 搭配 Windows 10（以伺服器 2016、2019 和 2022 為基礎）<br>• 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）<br>• 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的對應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超過 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前的 5 分鐘仍連線到串流執行個體，系統會提示他們儲存所有開啟的文件，然後才中斷連線。超過此時間後，執行個體會終止，並替換為新的執行個體。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。不然的話，他們會連線到含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，然後立即從串流執行個體中斷連線。然後，使用者使用的執行個體就會終止。
- 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。使用者會在由於未活動而導致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。不然的話，他們會連線到含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**
>
> 當使用者在其串流工作階段期間停止提供鍵盤或滑鼠輸入時，便會將其視為閒置。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。
  - 選擇新增縮減政策，並在指定的容量使用率小於或大於指定的閾值時，輸入移除指定執行個體的值。
- 針對標籤，指定您要使用的金鑰對值。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。

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` 使用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 AppStream 2.0

AppStream 2.0 執行個體將根據堆疊名稱列出，且需要在「建立環境」頁面上設定 IdP 登入 URL。由於 AppStream 2.0 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 AppStream 2.0 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 AppStream 2.0，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 AppStream 2.0 管理員指南中的設定 SAML，以建立身分提供者。<br><br>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<br><br>在 AppStream 2.0 堆疊層級設定 |
| 檔案傳輸 | 停用<br><br>在 AppStream 2.0 堆疊層級設定 |
| 列印至本機裝置 | 停用<br><br>在 AppStream 2.0 堆疊層級設定 |

也支援透過 AppStream 2.0 上的 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 AppStream 2.0 堆疊

為串流您的應用程式，AppStream 2.0 的環境需包括與堆疊相關聯的機群和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 Get Started with AppStream 2.0: Set Up With Sample Applications 中的程序。

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 |
| --- | --- |
| 剪貼簿 | 停用 |
| 檔案傳輸 | 停用 |
| 列印至本機裝置 | 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
- 啟動 WorkSpaces 精簡型客戶端管理員主控台


## 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 |

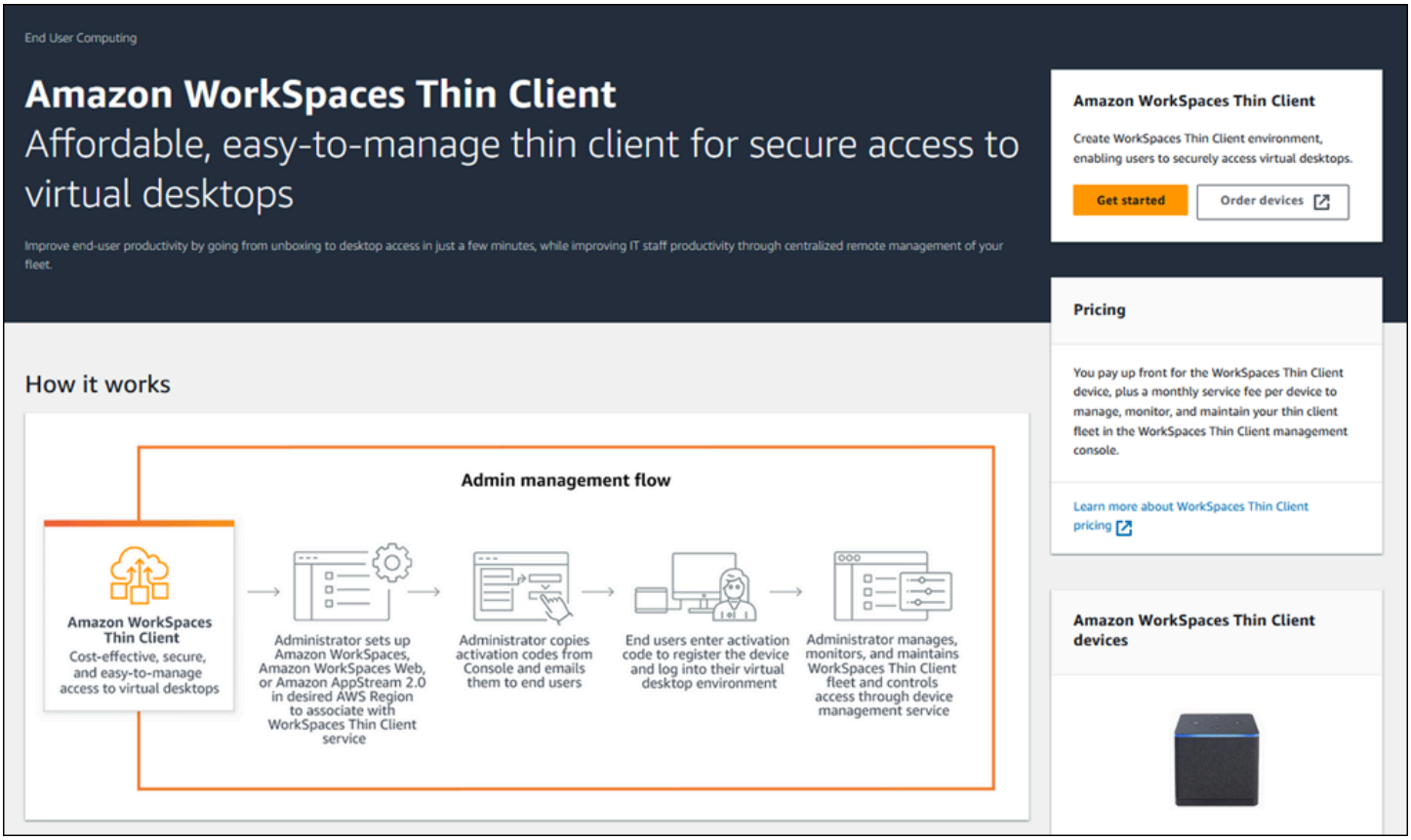
| 區域名稱 | 區域 | 端點 | 主控台連結 |
| --- | --- | --- | --- |
| 加拿大 (中部) | ca-central-1 | thinclient.ca-central-1.amazonaws.com | https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home |
| 歐洲 (法蘭克福) | eu-central-1 | thinclient.eu-central-1.amazonaws.com | https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home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

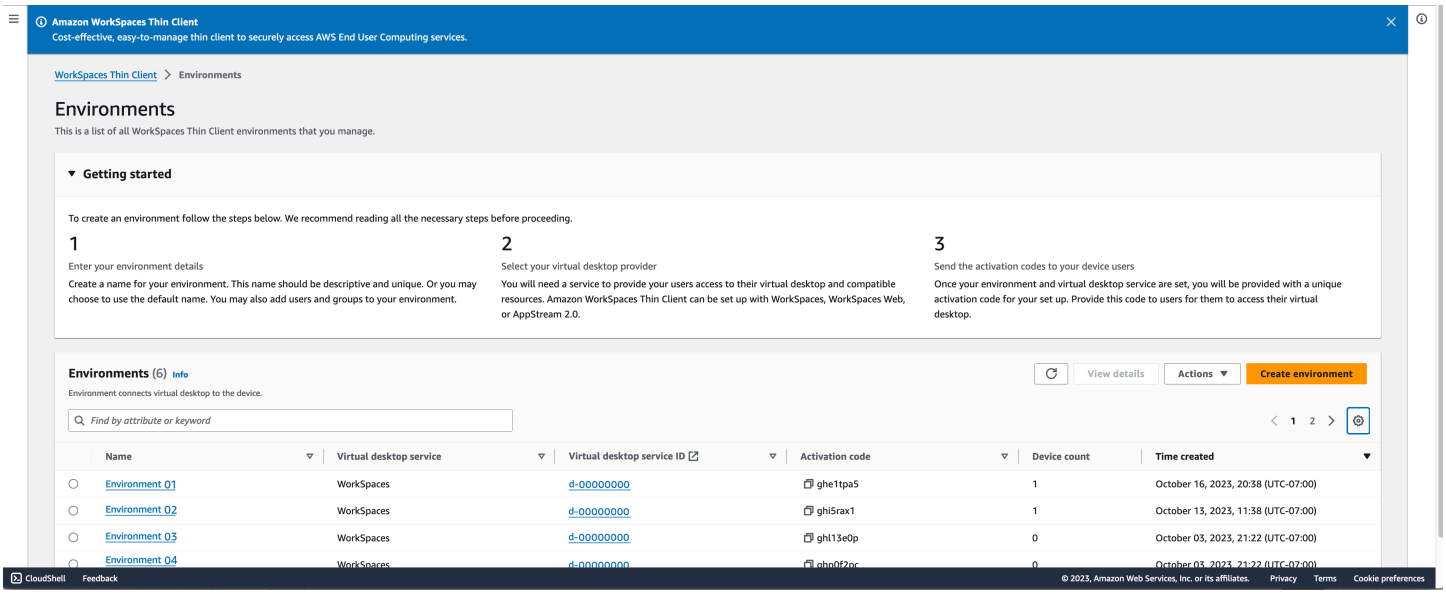
# 環境

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
- AppStream 2.0
- 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 | 描述 |
| --- | --- |
| 名稱 | 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 | 描述 |
| --- | --- |
| 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 | 描述 |
| --- | --- |
| 搜尋 | 搜尋您管理的所有環境。 |
| 重新整理 | 重新整理環境清單。 |
| View details (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

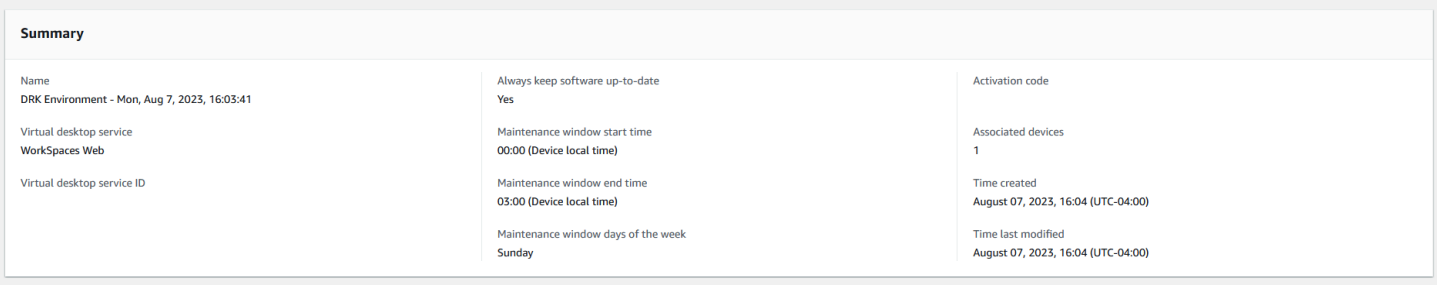
當您選取環境時，WorkSpaces 精簡型客戶端主控台會顯示該環境的詳細資訊，供您檢閱。主控台也會顯示此環境使用的虛擬桌面提供者詳細資訊。

主題


- Summary
- 虛擬桌面環境詳細資訊


## Summary

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。



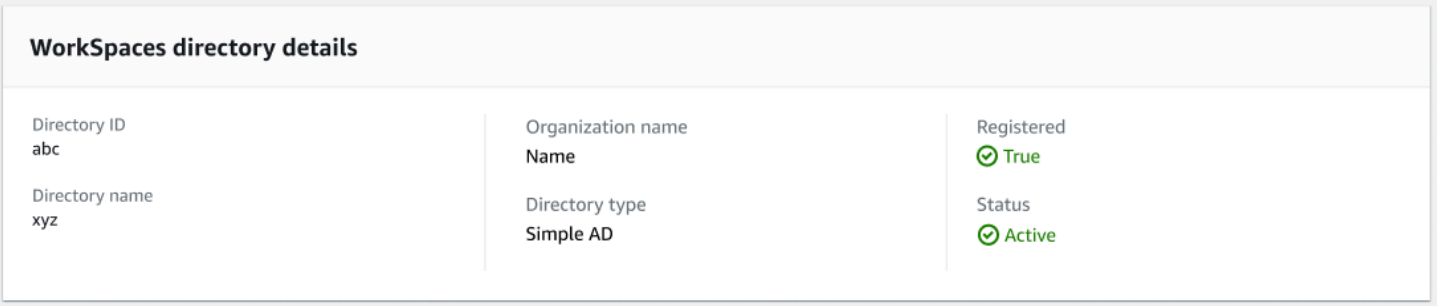

| Element | 描述 |
| --- | --- |
| 名稱 | 與此環境相關聯的唯一識別符。 |
| 虛擬桌面服務 | 此環境使用的虛擬桌面提供者。 |
| 虛擬桌面服務名稱 | 虛擬桌面服務提供者指派給此環境的唯一識別符。 |
| 啟用碼 | 最終使用者使用此程式碼來存取虛擬桌面環境。 |
| 隨時將軟體保持在up-to-date | 此設定會啟用自動軟體更新。 |
| 維護時段開始時間 | 每週自動軟體更新開始的時間。 |
| 維護時段結束時間 | 每週自動軟體更新完成的時間。 |
| 一週中的維護時段天數 | 自動軟體更新發生的日期。 |
| 關聯的裝置 | 存取此環境的 WorkSpaces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

## 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

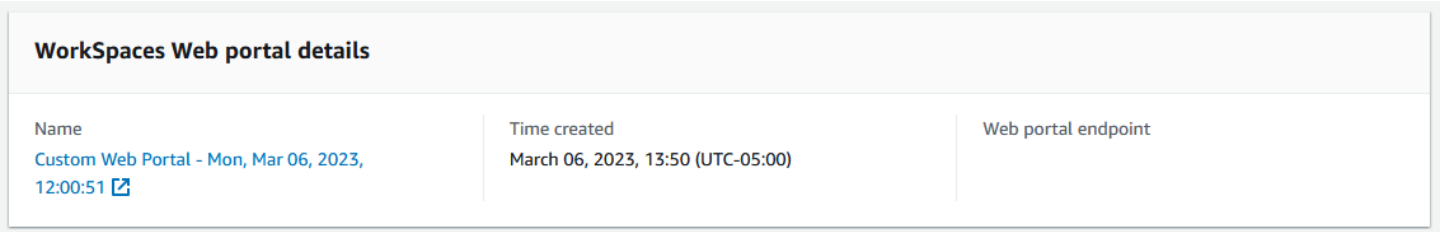
在 Amazon WorkSpaces Amazon WorkSpaces 精簡型客戶端環境會使用目錄來建立和執行虛擬桌面。下表列出詳細資訊中的每個元素及其運作方式。




| Element | 描述 |
| --- | --- |
| 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。 |
| Status | 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

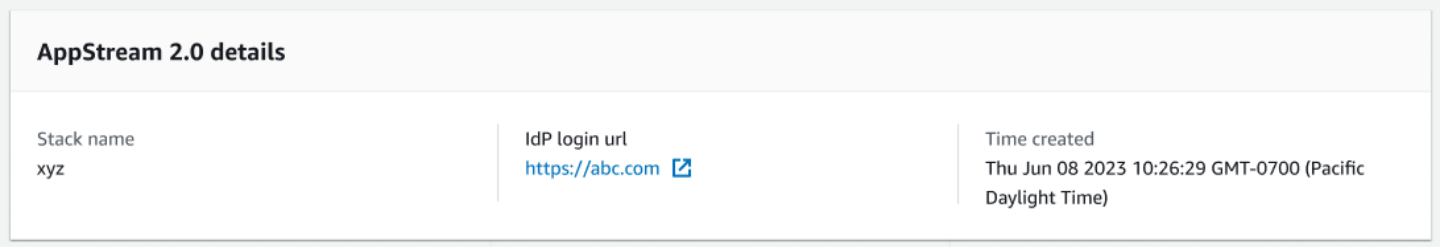
在 Amazon WorkSpaces Amazon WorkSpaces 精簡型客戶端環境會使用 Web 入口網站來建立和執行虛擬桌面。下表列出詳細資訊中的每個元素及其運作方式。




| Element | 描述 |
| --- | --- |
| 名稱 | 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。 |

## AppStream 2.0 詳細資訊

WorkSpaces 精簡型客戶端環境會在 AppStream 2.0 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 | 描述 |
| --- | --- |
| Stack name (堆疊名稱) | 與此 AppStream 2.0 堆疊相關聯的唯一識別符。 |
| IdP 登入 URL | 用於登入和登出 AppStream 2.0 堆疊的身分提供者 URL。 |
| 建立時間 | 建立此 AppStream 2.0 堆疊的日期和時間。 |

# 建立環境

若要開始，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 AppStream 2.0
- 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
- 步驟 2：選取虛擬桌面提供者
- 步驟 3：將啟用代碼傳送至裝置使用者


## 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
- AppStream 2.0

## 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 AppStream 2.0

AppStream 2.0 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 AppStream 2.0 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 AppStream 2.0，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。如需有關建立 AppStream 2.0 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 精簡型客戶端的詳細資訊，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。

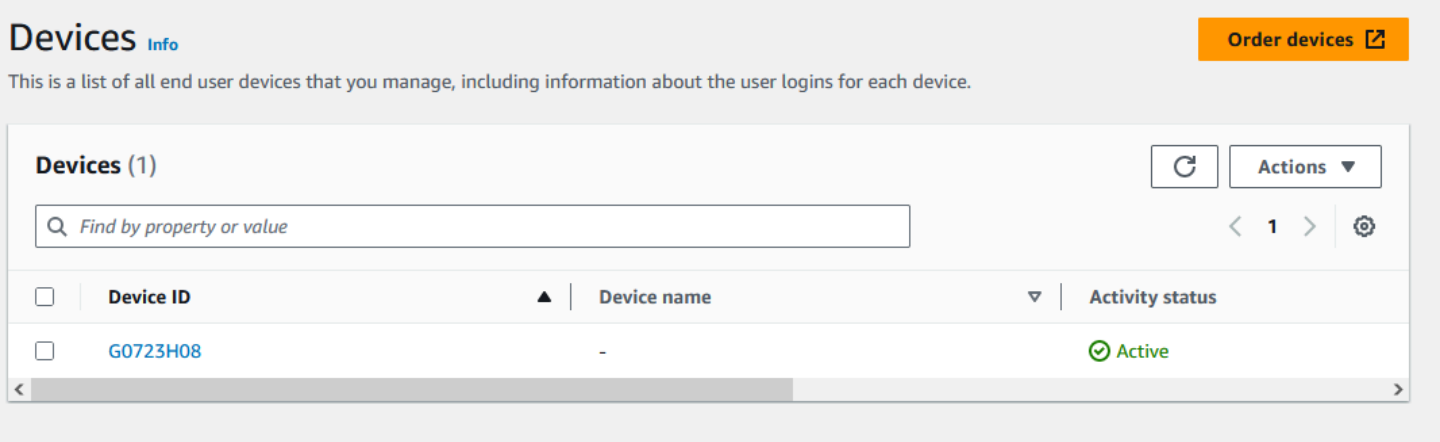
# 裝置

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 | 描述 |
| --- | --- |
| 裝置 ID | 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。 |
| 活動狀態 | 裝置目前的狀態。有兩種狀態：<br>• 作用中 – 至少在過去七天內連線至網路一次。<br>• 非作用中 – 在過去七天內未連線至網路。 |
| 註冊狀態 | 確認裝置已設定、與此 AWS 帳戶相關聯，而且是特定環境的一部分。它可以處於下列其中一種狀態： |

| Element | 描述 |
| --- | --- |
| | • 已註冊 – 這是預設狀態。<br>• 取消註冊 – 裝置正在重設和取消註冊程序。<br>Note<br>如果裝置處於取消註冊狀態，您可以刪除該裝置。<br>• 已取消註冊 – 裝置已成功取消註冊。<br>Note<br>您只能刪除處於取消註冊或取消註冊狀態的裝置。<br>• 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：<br>• 合規<br>• 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 | 描述 |
| --- | --- |
| 搜尋 | 搜尋您管理的所有裝置。 |
| 重新整理 | 重新整理裝置清單。 |
| View details (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： |

| Element | 描述 |
| --- | --- |
| | • 編輯裝置名稱<br>• 取消註冊<br>• 封存<br>• 刪除<br>• 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

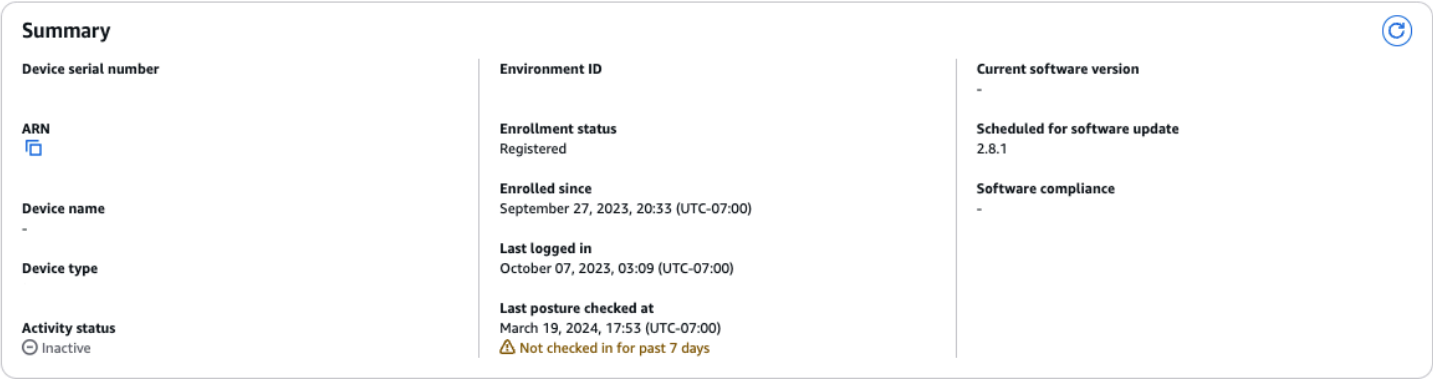
當您選取裝置時，WorkSpaces 精簡型客戶端主控台會顯示該裝置的詳細資訊，供您檢閱。主控台也會顯示裝置網路類型和連線周邊裝置的詳細資訊。

主題

- Summary
- 裝置設定
- 使用者活動

## Summary

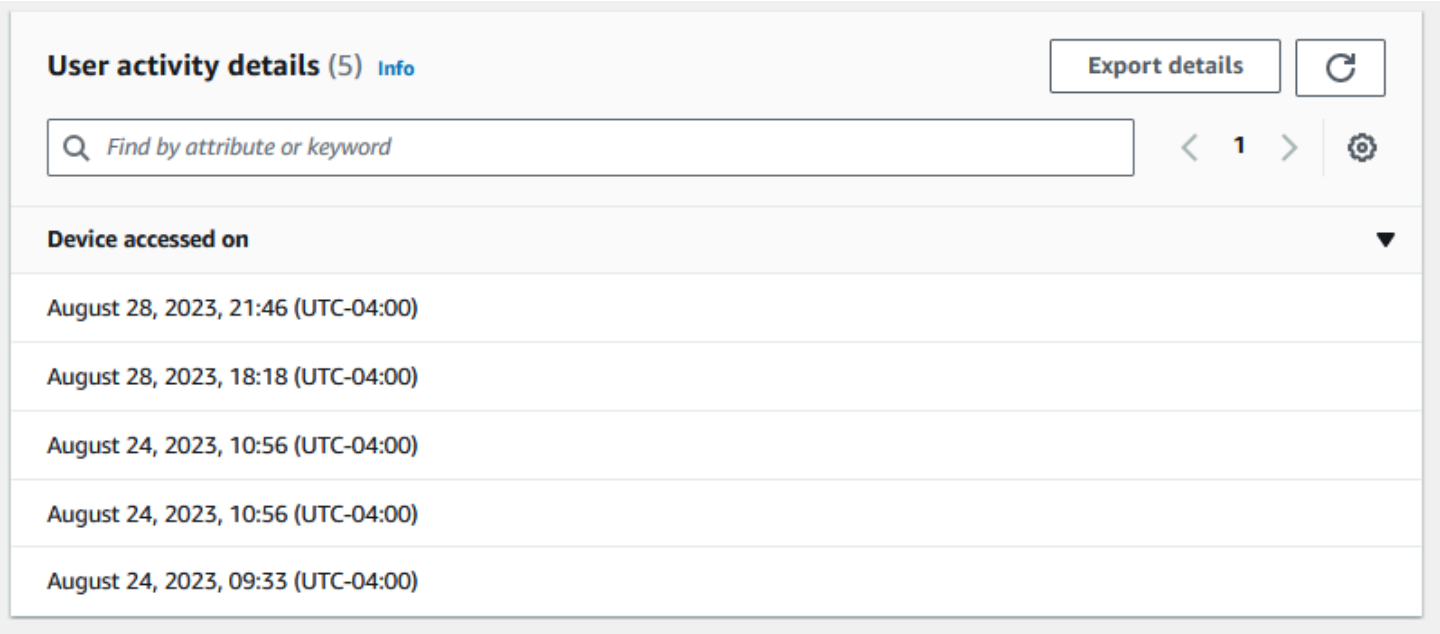
摘要區段提供 WorkSpaces 精簡型客戶端裝置主要功能的高階概觀。下表列出摘要中的每個元素及其運作方式。




| Element | 描述 |
| --- | --- |
| 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：<br>• 作用中<br>• 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，而且是特定環境的一部分。它可以處於下列四種狀態之一：<br>• 已註冊 – 這是預設狀態。<br>• 取消註冊 – 裝置正在重設和取消註冊程序。<br>• 已取消註冊 – 裝置已成功取消註冊。 |

| Element | 描述 |
| --- | --- |
| | Note<br>您只能刪除處於已取消註冊或已封存狀態的裝置。<br>• 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：<br>• 合規<br>• 不合規 |

## 使用者日誌




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

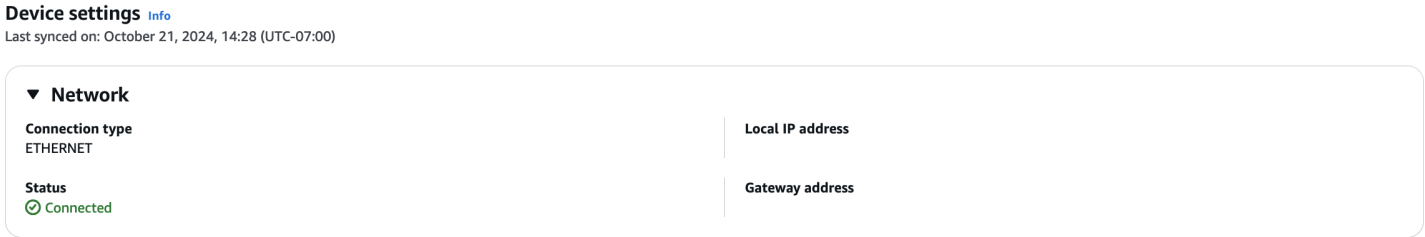
## 裝置設定

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

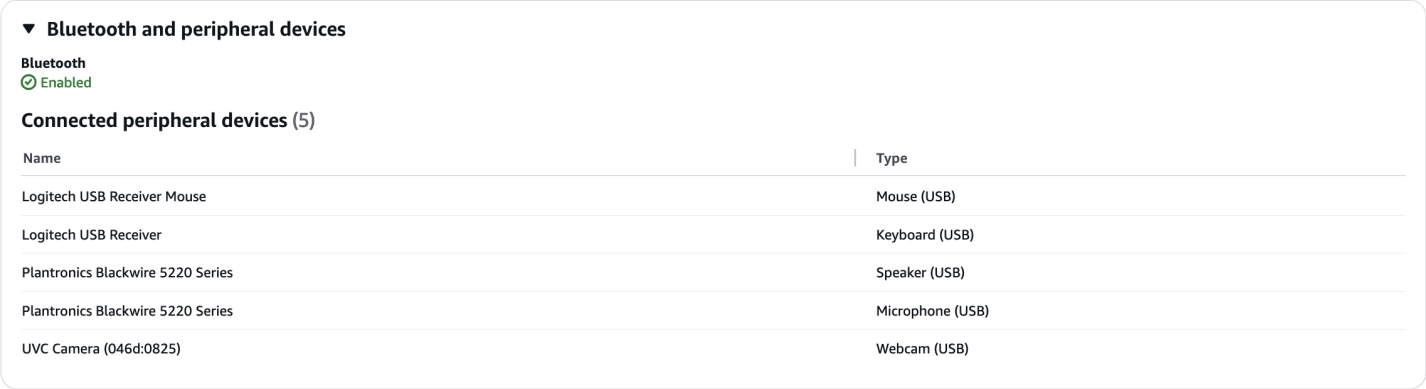
WorkSpaces 精簡型客戶端裝置詳細資訊提供裝置網路連線的概觀。下表列出每個元素及其運作方式。



| Element | 描述 |
| --- | --- |
| 上次同步於 | 最新的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。 |
| Status | 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，狀態會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到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 | 描述 |
| --- | --- |
| 藍牙 | 裝置的藍牙狀態。兩種狀態為：<br>• 已啟用<br>• 已停用 |

| Element | 描述 |
| --- | --- |
| 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)。 |

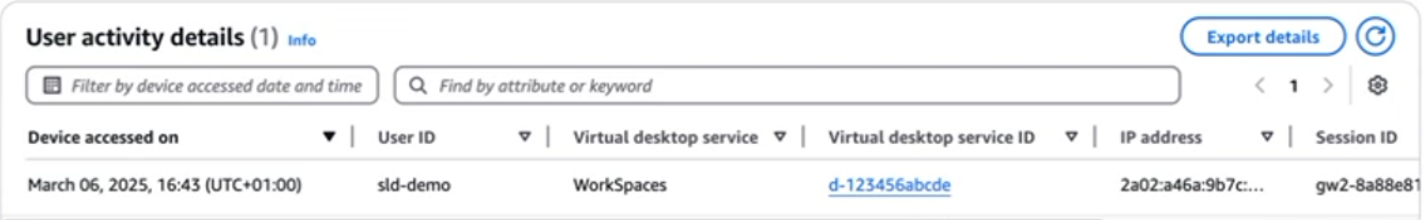
### 電源和睡眠

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 | 描述 |
| --- | --- |
| 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 | 描述 |
| --- | --- |
| 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 | 描述 |
| --- | --- |
| IP 地址 | 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。

# 軟體更新

WorkSpaces 精簡型客戶端有時需要引進新功能的軟體更新，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 WorkSpaces 精簡型客戶端裝置的軟體應用程式或作業系統更新。在此主控台中，您可以選擇立即更新軟體，也可以在環境的維護時段期間排程自動更新。

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。

主題


- 更新環境軟體
- 更新裝置軟體
- WorkSpaces 精簡型客戶端軟體版本


## 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 |
| --- | --- | --- |
| 2.16.1 | 7-3-2025 | • 針對 Chromium 的 CVE-2025-6554 重大安全問題進行修正。 |
| 2.16.0 | 6-27-2025 | • 新增網路延遲的通知。<br>• 新增從工作階段期間變暗的第二個監視器復原的功能。 |

| 軟體集 | 版本日期 | 變更 |
| --- | --- | --- |
| | | • 修正在裝置從休眠模式返回後，顯示白色畫面或未自動延伸的監視器問題。 |
| 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。<br>• 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。 |
| 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。<br>• 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。<br>• 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。<br>• 最終使用者會在監視器連線和中斷連線時看到通知。<br>• 裝置會從作業系統收集診斷資訊，以改善服務。<br>• 修正在軟體安裝日期的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。<br>• 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。<br>• 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。<br>• 最終使用者會在監視器連線和中斷連線時看到通知。<br>• 裝置會從作業系統收集診斷資訊，以改善服務。<br>• 修正在軟體安裝日期的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。<br>• 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。<br>• WorkSpaces 精簡型客戶端現在支援單一螢幕的 2K 解析度監控。<br>• 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。<br>• 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。<br>• 已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 | • 精簡型客戶端支援具有 4K 解析度的監視器。<br>• 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。<br>• 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。<br>• 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。<br>• 修正工具列語言未影響裝置語言變更的問題。<br>• 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。<br>• 裝置設定可讓使用者忘記儲存的 WiFi 網路。<br>• 改善工作階段中音訊/視訊通話的效能。<br>• 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。<br>• 裝置工具列上的首頁按鈕已重新命名為登入。<br>• 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。<br>• 已修正允許在 WorkSpaces 登入頁面上的 AWS 和隱私權連結上按一下滑鼠右鍵，以獨立模式開啟瀏覽器的問題。 |
| 2.4.0 | 05-09-2024 | • 修正封鎖 "accounts.google.com" 並防止使用 Google Workspace 做為 AppStream 2.0 工作階段 IDP 的問題。<br>• 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。<br>• 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。<br>• 修正「about：blank」URL 出現在第二個顯示器上的問題。<br>• 修正延長顯示關閉時導致白色畫面的問題。<br>• 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。<br>• 改善與鎖定功能相關的最終使用者延遲。<br>• 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。共同責任模型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 精簡型用戶端中的資料保護。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 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 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 精簡型用戶端，或使用主控台、API AWS CLI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 精簡型用戶端會收集並提供使用者使用 WorkSpaces 精簡型用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
- Amazon WorkSpaces 精簡型客戶端的靜態資料加密
- 傳輸中加密
- 金鑰管理
- 網路工作流量隱私權


## 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 精簡型用戶端使用 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 精簡型用戶端預設會使用 AWS KMS 加密所有敏感資料，以保護內容和中繼資料。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 精簡型用戶端預設提供加密，以使用 AWS 擁有的加密金鑰來保護靜態敏感客戶資料。

- AWS 擁有的金鑰 — Amazon WorkSpaces 精簡型用戶端預設使用這些金鑰自動加密個人識別資料。您無法檢視、管理或使用 AWS 擁有的金鑰或稽核其使用。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 精簡型用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<br><br>WorkSpaces 精簡型客戶端環境名稱 | 已啟用 | 已啟用 |
| 裝置名稱<br><br>WorkSpaces 精簡型客戶端裝置名稱 | 已啟用 | 已啟用 |
| 裝置設定<br><br>WorkSpaces 精簡型用戶端裝置設定 | 已啟用 | 已啟用 |
| 裝置建立標籤<br><br>WorkSpaces 精簡型用戶端環境裝置建立標籤 | 已啟用 | 已啟用 |

> **Note**
>
> Amazon WorkSpaces 精簡型用戶端使用 AWS 擁有的金鑰來保護個人識別資料，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 精簡型用戶端如何使用 AWS KMS

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

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

- 傳送`GenerateDataKey`請求至 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 精簡型用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 精簡型用戶端可以驗證金鑰。
- `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以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驗證資料，以支援驗證加密。當您在加密資料的請求中包含加密內容時， AWS KMS 會將加密內容繫結到加密的資料。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 精簡型用戶端在所有 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 精簡型用戶端資源使用 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 精簡型用戶端傳送至 AWS KMS 的請求。

下列範例是適用於 `DescribeKey`、`GenerateDataKey`、 的 AWS CloudTrail 事件`Decrypt`，用於監控 Amazon WorkSpaces 精簡型用戶端呼叫的 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 精簡型用戶端環境。系統會為 WorkSpaces 精簡型用戶端裝置記錄類似的 CloudTrail 事件。

DescribeKey

Amazon WorkSpaces 精簡型用戶端使用 `DescribeKey`操作來驗證 KMS AWS 客戶受管金鑰。

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 精簡型用戶端使用 `GenerateDataKey`儲存裝置資訊時，`GenerateDataKey`操作會用來加密資料。

`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 精簡型用戶端裝置存取環境或裝置資訊時，`Decrypt`操作會用來解密資料。`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 連線傳送，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 精簡型用戶端。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 精簡型用戶端會使用 AWS 擁有的金鑰。您可以使用 AWS SDK 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 Monitor your WorkSpaces、Monitoring and Reporting for AppStream 2.0 或 WorkSpaces Web 的 User access logging。

# 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
- 使用身分驗證
- 使用政策管理存取權
- Amazon WorkSpaces 精簡型客戶端如何搭配 IAM 運作
- Amazon WorkSpaces 精簡型客戶端的身分型政策範例
- AWS Amazon WorkSpaces 精簡型客戶端的 受管政策
- 疑難排解 Amazon WorkSpaces 精簡型客戶端身分和存取


## 目標對象

使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您在 WorkSpaces 精簡型客戶端中執行的工作。

服務使用者：如果您使用 WorkSpaces 精簡型客戶端服務來執行任務，管理員會為您提供所需的憑證和許可。當您使用更多 WorkSpaces 精簡型客戶端功能來執行工作時，您可能會需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。若您無法存取 WorkSpaces 精簡型客戶端中的某項功能，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：如果您負責公司內的 WorkSpaces 精簡型客戶端資源，您可能具備 WorkSpaces 精簡型客戶端的完整存取權限。您的任務是判斷服務使用者應該存取哪些 WorkSpaces 精簡型客戶端功能及資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司可搭配 WorkSpaces 精簡型客戶端使用 IAM 的方式，請參閱Amazon WorkSpaces 精簡型客戶端如何搭配 IAM 運作。

IAM 管理員：如果您是 IAM 管理員，建議您了解有關如何撰寫政策以管理 WorkSpaces 精簡型客戶端存取權限的詳細資訊。若要檢視您可以在 IAM 中使用的範例 WorkSpaces 精簡型客戶端身分型政策，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 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

## AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務 和 資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，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

根據最佳實務， 要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者 AWS 服務來使用臨時憑證來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、Identity Center 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便

在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

## IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。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。

- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。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權給 AWS 服務。
  - 服務連結角色 – 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。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

## 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。政策是 中的物件， AWS 當與身分或資源相關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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。

預設情況下，使用者和角色沒有許可。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 取得角色資訊。

## 身分型政策

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。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

## 資源型政策

資源型政策是連接到資源的 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。

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

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。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

## 其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政

策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。

- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 之多個 的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，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) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 (RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

### 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多個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 |

| IAM 功能 | WorkSpaces 精簡型客戶端支援 |
| --- | --- |
| 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》中的與 IAM AWS 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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。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，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。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，哪個主體在什麼条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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

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，請以逗號分隔它們，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。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示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 (或 `Condition` 區塊) 可讓您指定使陳述式生效的條件。`Condition` 元素是選用項目。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。

若您在陳述式中指定多個 `Condition` 元素，或是在單一 `Condition` 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯OR操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定的條件金鑰。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，可根據屬性來定義許可。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接到 IAM 實體 （使用者或角色） 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需其他資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的 使用 IAM。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的從使用者切換至 IAM 角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 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 中的暫時性安全憑證。

## 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

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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權給 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。在表格中尋找服務，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。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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 受管政策並轉向最低權限許可 – 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，以進一步減少許可。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其存取權 AWS 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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html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。我們建議您定義使用案例專屬的客戶管理政策，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 操作可供現有服務使用時， 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《AWS 受管政策參考》中的 AmazonWorkSpacesThinClientReadOnlyAccess。

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。這用於檢查您的 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` (AppStream 2.0) – 允許描述 AppStream 2.0 堆疊的許可。這用於檢查您的 AppStream 2.0 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。

```
{
  "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。這用於檢查您的 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` (AppStream 2.0) – 允許描述 AppStream 2.0 堆疊的許可。這用於檢查您的 AppStream 2.0 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。

```
{
  "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": "*"
    }
  ]
}
}
```

## WorkSpaces 精簡型客戶端更新受 AWS 管政策

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AmazonWorkSpacesThinClientReadOnlyAccess – 已更新政策 | 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 |
| AmazonWorkSpacesThinClientFullAccess – 已更新政策 | 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 – 已更新政策 | WorkSpaces 精簡型客戶端已更新政策，以包含 AppStream 2.0、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 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 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 Management Console 告訴您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是提供您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 來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 和 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 AppStream 2.0 和 WorkSpaces Web 交叉整合。如需每個 服務更新管理的詳細資訊，請參閱下列連結：

- Amazon AppStream 2.0 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 精簡型用戶端和您其他 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 精簡型用戶端、在發生錯誤時報告，並在適當時採取自動動作：

- AWS CloudTrail 會擷取由您的帳戶或代表 AWS 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 AWS CloudTrail記錄 Amazon WorkSpaces 精簡型客戶端 API 呼叫

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

Amazon WorkSpaces 精簡型用戶端已與 整合AWS CloudTrail，此服務提供使用者、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。使用 CloudTrail 收集的資訊，您可以判斷對 WorkSpaces 精簡型用戶端提出的請求、提出請求的 IP 地址、提出請求的時間，以及其他詳細資訊。

所有 Amazon WorkSpaces 精簡型用戶端動作都會由 CloudTrail 記錄，並記錄在 Amazon WorkSpaces 精簡型用戶端 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，請建立追蹤或 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 Management Console 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 精簡型用戶端資料事件

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 精簡型用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 Management Console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 精簡型用戶端資源類型。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該`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<br>• 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 精簡型用戶端管理事件

管理事件提供在 資源上執行的管理操作的相關資訊 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 精簡型用戶端會將所有 WorkSpaces 精簡型用戶端控制平面操作記錄為管理事件。如需 WorkSpaces 精簡型用戶端記錄到 CloudTrail 的 Amazon WorkSpaces 精簡型用戶端控制平面操作清單，請參閱 Amazon WorkSpaces 精簡型用戶端 API 參考。 WorkSpaces CloudTrail

## WorkSpaces 精簡型用戶端事件範例

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 建立 Amazon WorkSpaces 精簡型用戶端資源 AWS CloudFormation

Amazon WorkSpaces 精簡型用戶端已與 整合 AWS CloudFormation，此服務可協助您建立模型並設定 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 AWS CloudFormation 佈建和設定這些資源。

使用 時 AWS CloudFormation，您可以重複使用範本來持續且重複地設定 WorkSpaces 精簡型用戶端資源。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 精簡型用戶端和 AWS CloudFormation 範本

若要為 WorkSpaces 精簡型用戶端和相關服務佈建和設定資源，您必須了解 AWS CloudFormation 範本。範本是 JSON 或 YAML 格式的文字檔案。這些範本說明您想要在 AWS 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 AWS CloudFormation 設計工具來協助您開始使用 AWS CloudFormation 範本。如需更多詳細資訊，請參閱 AWS CloudFormation 使用者指南中的 什麼是 AWS CloudFormation 設計器？。

WorkSpaces 精簡型用戶端支援在 中建立環境 AWS 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 精簡型用戶端資源類型參考。

## 進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- AWS 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 精簡型用戶端

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

您可以透過建立 支援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 精簡型用戶端建立介面端點AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立介面端點。

使用下列服務名稱建立 WorkSpaces 精簡型用戶端的介面端點：

```
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 精簡型用戶端提出 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 精簡型用戶端。若要控制從 VPC 授予 WorkSpaces 精簡型用戶端的存取權，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 精簡型用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：AmazonWorkSpacesThinClientFullAccess | Amazon WorkSpaces 精簡型用戶端已新增 AmazonWorkSpacesThinClientFullAccess 受管政策第 2 版。 | 2025 年 1 月 9 日 |
| AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess | Amazon WorkSpaces 精簡型用戶端新增了 AmazonWorkSpacesThinClientReadOnlyAccess 受管政策第 3 版。 | 2025 年 1 月 9 日 |
| 使用 AWS CloudTrail 記錄 Amazon WorkSpaces 精簡型用戶端 API 呼叫<br><br>裝置設定<br><br>Amazon WorkSpaces 精簡型用戶端的靜態資料加密 | 新增資料事件的新區段。<br><br>新增裝置設定的新區段。<br><br>更新 章節中靜態資料加密的 KMS 資訊。 | 2024 年 10 月 28 日 |
| 業務連續性 | 新增了業務連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 精簡型用戶端新增了 AmazonWorkSpacesThinClientFullAccess 受管政策。 | 2024 年 8 月 9 日 |
| AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess | Amazon WorkSpaces 精簡型用戶端新增了 AmazonWorkSpacesThinClientR | 2024 年 8 月 9 日 |

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| | eadOnlyAccess 受管政策第 2 版。 | |
| 為 WorkSpaces 精簡型用戶端設定 WorkSpaces Personal | 已更新新 WorkSpaces Personal 的 。 | 2024 年 8 月 7 日 |
| 為 WorkSpaces 精簡型用戶端設定 WorkSpaces 集區 | 已新增新 WorkSpaces 集區的新區段。 | 2024 年 8 月 7 日 |
| AWS 受管政策：AmazonWorkSpacesThinClientReadOnlyAccess | Amazon WorkSpaces 精簡型用戶端新增了 AmazonWorkSpacesThinClientReadOnlyAccess 受管政策。 | 2024 年 7 月 19 日 |
| AWS Amazon WorkSpaces 精簡型用戶端的 受管政策 | Amazon WorkSpaces 精簡型用戶端開始追蹤變更。 | 2024 年 7 月 19 日 |
| 為 Amazon WorkSpaces 精簡型用戶端設定 WorkSpaces Amazon WorkSpaces | 已更新作業系統清單。 | 2024 年 2 月 12 日 |
| 為 Amazon WorkSpaces 精簡型用戶端設定 AppStream 2.0 | 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。