aws

管理員指南

Amazon WorkSpaces 瘦客戶端

Amazon WorkSpaces 瘦客戶端: 管理員指南

Table of Contents

什麼是 Amazon WorkSpaces 精簡型用戶端管理員主控台？

使用 Amazon WorkSpaces 精簡型用戶端管理員主控台，管理員可透過 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精簡型用戶 WorkSpaces 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中建立或修改。

> **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？

如果您是精簡型用戶 WorkSpaces 端管理員主控台的第一次使用者，建議您先閱讀下列章節：

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

架構

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

- Amazon WorkSpaces
- AppStream 2.0
- Amazon 瀏 WorkSpaces 覽器

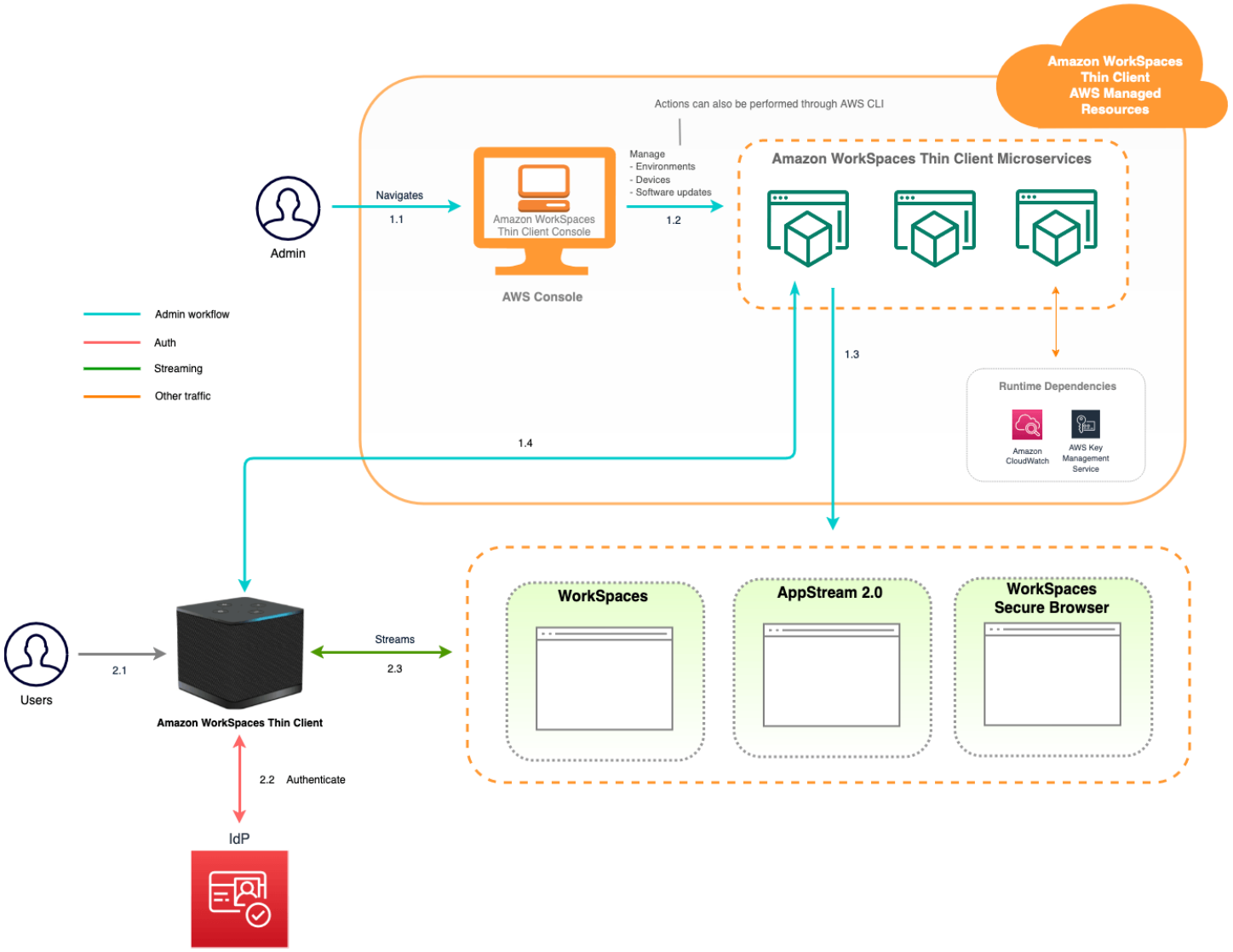
視所使用的 VDI 而定，您的 WorkSpaces 精簡型用戶端資訊可透過的目錄 WorkSpaces、 AppStream 2.0 堆疊和 WorkSpaces 安全瀏覽器的 Web 入口網站端點存取和管理。

如需 Amazon 的詳細資訊 WorkSpaces，請參閱快 WorkSpaces 速設定開始使用。目錄是通過 AWS Directory Service，它提供了以下選項管理：Simple AD，AD Connector，或 AWS Directory Service Microsoft 活動目錄，也稱為 AWS 託管 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：使用範例應用程式設定。 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，並視需求提供使用者存取權限。 AppStream 2.0 可讓使用者在自選裝置上存取所需的應用程式，並提供回應迅速、流暢的使用者體驗，與原生安裝的應用程式無法區別。

如需有關安 WorkSpaces 全瀏覽器的資訊，請參閱 Amazon WorkSpaces 安全瀏覽器入門。Amazon WorkSpaces 安全瀏覽器是一種按需、全受管、以 Linux 為基礎的服務，旨在促進瀏覽器對內部網站和 software-as-a-service (SaaS) 應用程式的安全存取。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。

下圖顯示了 WorkSpaces 精簡客戶端的體系結構。


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 精簡型用戶端管理員主控台

主題

註冊 AWS

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 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，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

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	By	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。	AWS IAM Identity Center 在《使用AWS Command Line Interface 者指南》中設定 AWS CLI 要使用的，以設定程式設計方式存取。

選擇一種管理管理員的方式	到	By	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 使用者指南中建立您的第一個 IAM 管理員使用者和使用者群組的說明。	請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰，設定程式設計存取。

開始使用適用於 Amazon WorkSpaces 精簡型用戶端的 VDI

Amazon WorkSpaces 精簡型用戶端是符合成本效益的精簡型用戶端裝置，可與 AWS 使用者運算服務搭配使用，為您提供安全、即時存取應用程式和虛擬桌面。

選擇虛擬桌面基礎結構 (VDI)，並將其設定為搭配精簡型用戶 WorkSpaces 端使用。

> **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。這些需求會列在每個虛擬桌面提供者的組態程序中。

WorkSpaces 精簡型用戶端需要特定的軟體組態，視您的虛擬桌面供應商而定。

主題

- WorkSpaces 為 Amazon WorkSpaces 精簡用戶端設定
- 為 Amazon WorkSpaces 精簡型用戶端設定 AppStream 2.0
- 為 Amazon WorkSpaces 精簡型用戶端設定 Amazon WorkSpaces 安全瀏覽

WorkSpaces 為 Amazon WorkSpaces 精簡用戶端設定

若要與 Amazon 搭配使用 WorkSpaces 精簡型用戶端 WorkSpaces，您的服務必須設定才能存取 WorkSpaces 目錄。Amazon WorkSpaces 根據主 AWS 控台內的 WorkSpaces 精簡型用戶端建立環境頁面上的目錄名稱列出。

> **Note**
>
> 首次使用主控台之前，必須先進行設定。不建議您在開始使用主控台之後修改任何必要條件功能。

開始之前

請確定您擁有可建立或管理的 AWS 帳戶 WorkSpace。但是，設備用戶不需要 AWS 帳戶即可連接和使用他們的 WorkSpaces。

在繼續進行組態之前，請檢閱並瞭解下列概念：

- 啟動時 WorkSpace，請選取 WorkSpace 套裝軟體。如需詳細資訊，請參閱 Amazon WorkSpaces 套裝軟體。
- 啟動時 WorkSpace，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 的協定 WorkSpaces。
- 啟動時 WorkSpace，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設定檔。關於 WorkSpaces 和使用者的資訊儲存在目錄中。如需詳細資訊，請參閱管理的目錄 WorkSpaces。
- 當您啟動時 WorkSpace，啟用並設定 WorkSpaces Web 存取。如需詳細資訊，請參閱啟用和設定 Amazon WorkSpaces 網路存取

步驟 1：確認您的系統符合 WorkSpaces 所需的功能

為了讓 WorkSpaces 精簡型用戶端管理員主控台能夠與 Amazon 正常運作 WorkSpaces，您的系統必須符合下列特定需求。此表格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 電源與視窗 10（基於服務器 2016，2019 和 2022 年） • Microsoft 電源與視窗 10（基於服務器 2016 年，2019 年和 2022 年）在辦公室 • Microsoft PowerPro 與視窗 10（基於服務器 2016 年，2019 年和 2022 年） • Microsoft PowerPro 與視窗 10（基於服務器 2016 年，2019 年和 2022 年）在辦公室

功能	需求
	• Microsoft 性能與視窗 10（基於服務器 2016，2019 和 2022 年） • Microsoft 性能與視窗 10（基於服務器 2016 年，2019 年和 2022 年）在辦公室
支援的通訊協定	只有 WSP

步驟 2：使用進階設定啟動 WorkSpace

若要使用進階設定來啟動 WorkSpace

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

為 Amazon WorkSpaces 精簡型用戶端設定 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 驗證僅支援起始的驗證，因此系統管理員必須手動輸入正確的登入 URL。

> **Note**
>
> 首次使用主控台之前，必須先進行設定。不建議您在開始使用主控台之後修改任何必要條件功能。

步驟 1：確認您的系統符合 AppStream 2.0 的必要功能

為了讓 WorkSpaces 精簡型用戶端管理員主控台能夠正常使用 AppStream 2.0，您的系統必須符合下列特定需求。此表格列出所有這些支援的功能及其需求。

功能	需求
身分提供者	移至 AppStream 2.0 管理員指南中的設定 SAML 以建立身分識別提供者。 當系統提示您建立 env 主控台時，請輸入您的 IDP 登入 URL。
作業系統	Windows
平台類型	Windows Server (2012 R2、2016 或 2019)
串流通訊協定	TCP 串流 如果 UDP 不可用，則會有 TCP 的自動後援機制。
本機複製與貼上	停用 在 AppStream 2.0 堆疊層級設定
本機資料夾共用	停用 在 AppStream 2.0 堆疊層級設定
本機列印	停用 在 AppStream 2.0 堆疊層級設定

也支援透過 AppStream 2.0 版 SAML 驗證進行的螢幕鎖定要求。 WorkSpaces 精簡型用戶端不支援使用者集區和程式化驗證機制。

步驟 2：設定 AppStream 2.0 堆疊

若要串流應用程式， AppStream 2.0 需要包含與堆疊相關聯的叢集的環境，以及至少一個應用程式映像檔。請遵循下列步驟來設定叢集和堆疊，並提供使用者對堆疊的存取權。如果您尚未這麼做，建議您嘗試使用 AppStream 2.0 入門：使用範例應用程式設定中的程序。

如果您想要建立要使用的映像，請參閱教學課程：使用 AppStream 2.0 主控台建立自訂 AppStream 2.0 映像。

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，請參閱搭配 AppStream 2.0 使用作用中目錄。

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 精簡型用戶端設定 Amazon WorkSpaces 安全瀏覽

Amazon WorkSpaces Secure 瀏覽器是以 AWS 主控台內 WorkSpaces 精簡型用戶端建立環境頁面上的網路入口網站端點為基礎。

> **Note**
>
> 首次使用主控台之前，必須先進行設定。不建議您在開始使用主控台之後修改任何必要條件功能。

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

為了讓 WorkSpaces 精簡型用戶端管理員主控台能夠與 Amazon WorkSpaces Secure 瀏覽器正常運作，您的系統必須符合下列特定需求。此表格列出所有這些支援的功能及其需求。

功能	需求
本機複製與貼上	停用
本機資料夾共用	停用

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

步驟 2：設定 WorkSpaces 安全瀏覽器入口網站

WorkSpaces 精簡型用戶端可在特定組態中搭配 WorkSpaces 安全瀏覽器 VPC 搭配使用：

1. 使用AWS CodeBuild 雲形範本建立 VPC。
2. 設定身分提供者。
3. 創建一個 Amazon WorkSpaces 安全瀏覽器門戶。
4. 測試您新的 Amazon WorkSpaces 安全瀏覽器門戶。

啟動 WorkSpaces 精簡用戶端管理員主控台

WorkSpaces 精簡型用戶端是符合成本效益的精簡型用戶端裝置，可搭配 AWS 使用者運算服務使用，為您提供安全、即時存取應用程式和虛擬桌面。

主題

涵蓋區域

WorkSpaces 精簡型用戶端可在下列區域使用。

這些區域僅提供 WorkSpaces 精簡型用戶端管理員主控台。 WorkSpaces 精簡型用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	思想客戶. 我們東部-亞馬遜	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
美國西部 (奧勒岡)	us-west-2	思想客戶. 美國西部-亞馬遜	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
亞太區域 (孟買)	ap-south-1	思想客戶. 南 1. 亞馬遜	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home
歐洲 (愛爾蘭)	eu-west-1	思想客戶歐洲西部 1. 亞馬遜	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
加拿大 (中部)	ca-central-1	思想客戶 .ca-中央-阿馬遜	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home

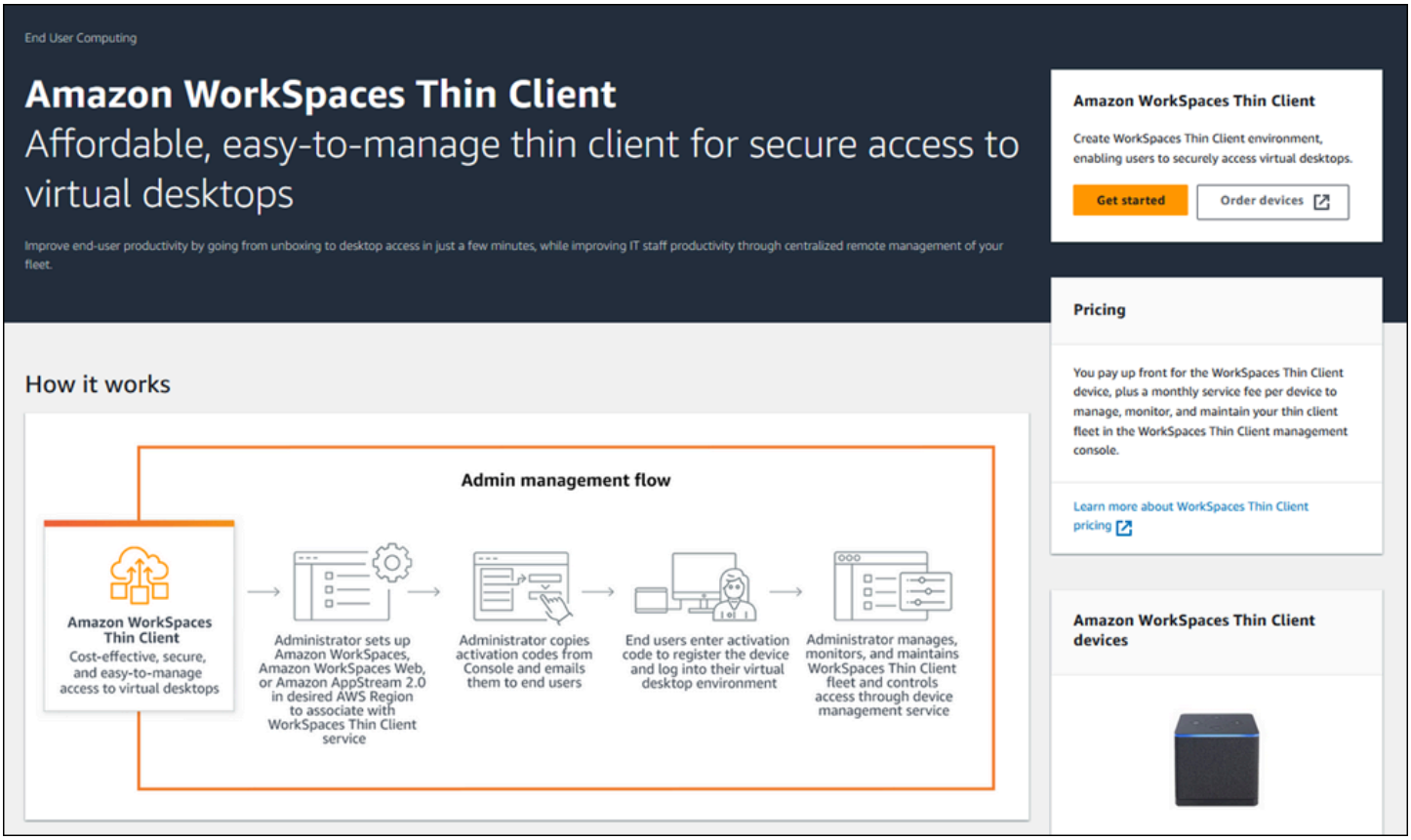
區域名稱	區域	端點	主控台連結
歐洲 (法蘭克福)	eu-central-1	思想客戶歐盟中心 1. 亞馬遜	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
歐洲 (倫敦)	eu-west-2	思想客戶歐洲西部 2. 亞馬遜	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

啟動 WorkSpaces 精簡用戶端管理員主控台

當您擁有 AWS 帳戶時，您可以啟動管理員主控台並移至 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. 登錄到您的 AWS 帳戶。
2. 存取WorkSpaces 精簡型用戶端主控台。
3. 選取開始使用，系統會將您導向環境。

使用 WorkSpaces 精簡型用戶端管理員



歡迎使用 WorkSpaces 精簡型用戶端管理員主控台！

從這裡，您可以為您的團隊管理 WorkSpaces 精簡型用戶端裝置和環境。

如需有關 WorkSpaces 精簡型用戶端裝置的資訊，請參閱WorkSpaces 精簡型用戶端使用者指南。

讓我們開始使用吧！

主題

- 環境
- 裝置
- 軟體更新

環境

每個 WorkSpaces 精簡型用戶端裝置都使用個別的虛擬桌面環境來存取其線上資源。使用者可以使用下列其中一個虛擬桌面提供者存取此環境：

- Amazon WorkSpaces
- AppStream 2.0
- Amazon 瀏 WorkSpaces 覽器

環境清單

環境清單詳細資訊

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碼。

啟動碼-一般使用者用來存取虛擬桌面環境的代碼。

裝置計數-存取此環境的 WorkSpaces 精簡型用戶端裝置數目。

環境清單動作

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

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

當您選取某個環境時，WorkSpaces 精簡型用戶端主控台會顯示該環境的詳細資料供您檢閱。主控台也會顯示此環境使用之虛擬桌面提供者的詳細資料。

主題

- Summary
- 虛擬桌面環境詳細資訊

Summary

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碼。

啟用代碼：此代碼供最終使用者用來存取虛擬桌面環境。

永遠保留軟體 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。

一週的維護時段天數：自動軟體更新發生的天數。

關聯的裝置-存取此環境的 WorkSpaces 精簡型用戶端裝置數目。

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

Amazon WorkSpaces 目錄詳情

目錄 ID-與此環境相關聯的 Amazon WorkSpaces 目錄。

目錄名稱-與此 Amazon 目 WorkSpaces 錄相關聯的唯一識別碼。

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。

註冊-此 Amazon WorkSpaces 目錄是否已註冊。

狀態-此 Amazon WorkSpaces 目錄是否處於活動狀態。

Amazon 的 WorkSpaces 安全瀏覽器門戶

名稱-與此 Amazon WorkSpaces 安全瀏覽器入口網站相關聯的唯一識別碼。

建立時間-建立此 AppStream 2.0 堆疊的日期和時間。

Web 入口網站端點：用來存取虛擬桌面環境的 URL。

AppStream 2.0 詳細資料

堆棧名稱-與此 AppStream 2.0 堆棧關聯的唯一標識符。

IdP 登入網址-用於登入和登出 AppStream 2.0 堆疊的身分識別提供者網址。

建立時間-建立此 AppStream 2.0 堆疊的日期和時間。

建立環境

首先，每個設備都需要一個 AWS 終端使用者運算服務。 WorkSpaces 精簡型用戶端使用下列服務：

- Amazon WorkSpaces 通過分配的目錄
- AppStream 2.0 通過分配的堆棧
- Amazon WorkSpaces 安全瀏覽器通過門戶網站地址

您必須將服務指派給現有環境或建立新環境。

> **Note**
>
> WorkSpaces 精簡型用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 [永遠保留軟體] 方塊 up-to-date。

> **Note**
>
> 如果未啟用自動軟體更新，則在您手動推送更新或軟體到期且系統強制執行更新之前，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版本。

3. 選取您要為環境排程維護時段的時間。
   - 套用整個系統的維護時段-在每週確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 瀏 WorkSpaces 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資源。

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

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。

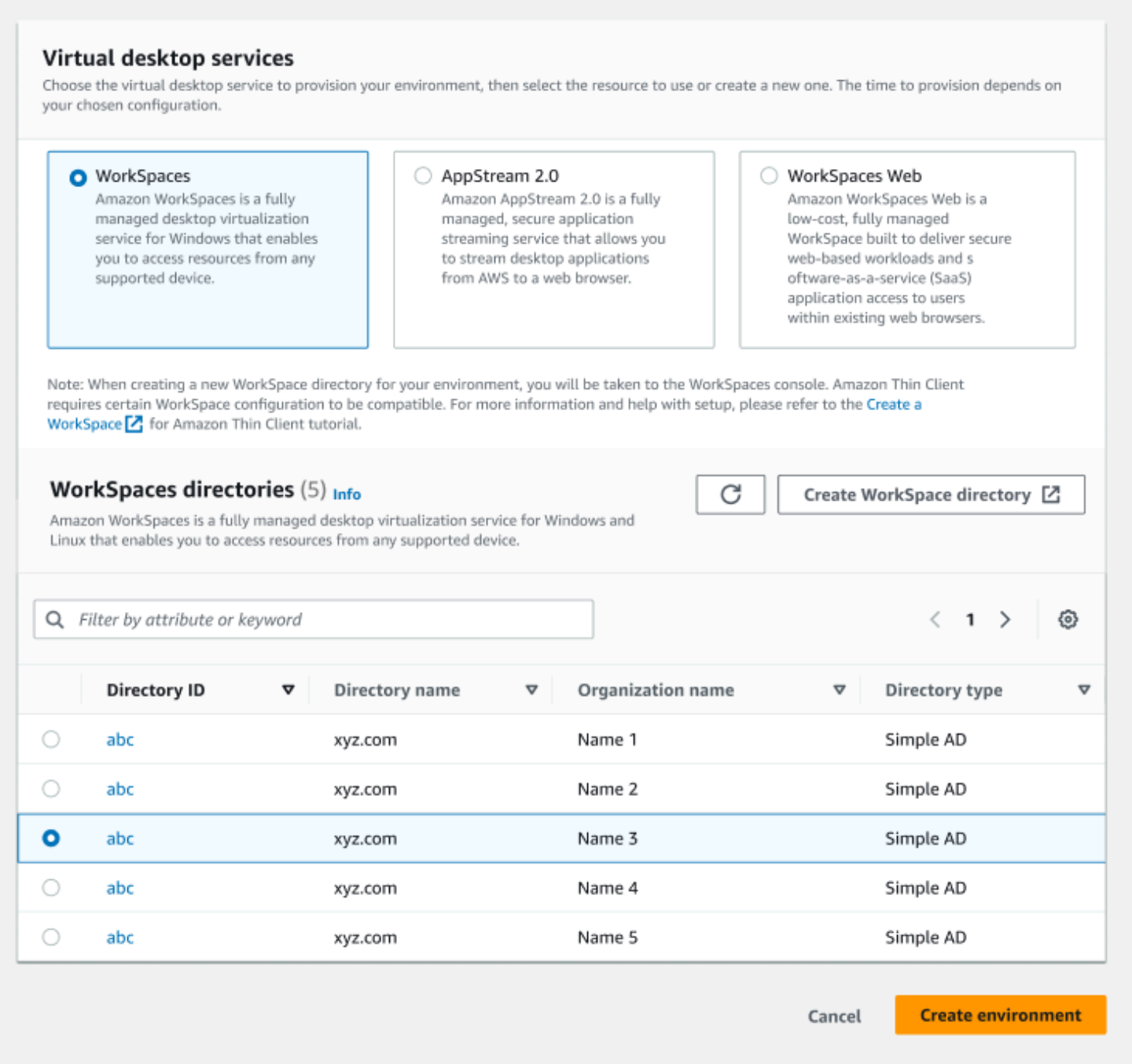
1. 要使用 Amazon WorkSpaces，請執行以下操作之一：

- 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。

  > **Note**
  >
  > 如果您在清單中沒有看到現有的目錄，請在 WorkSpaces 管理主控台中確認該目錄是否符合 WorkSpaces 精簡型用戶端需求。

- 選取建立目錄按鈕來建立 WorkSpaces 目錄。如需有關建立 WorkSpaces 目錄的詳細資訊，請參閱管理的目錄 WorkSpaces。

2. 選取「建立環境」按鈕。



當您建立環境時，您仍然可以在稍後編輯詳細資料。如需詳細資訊，請參閱編輯環境。

使用 AppStream 2.0

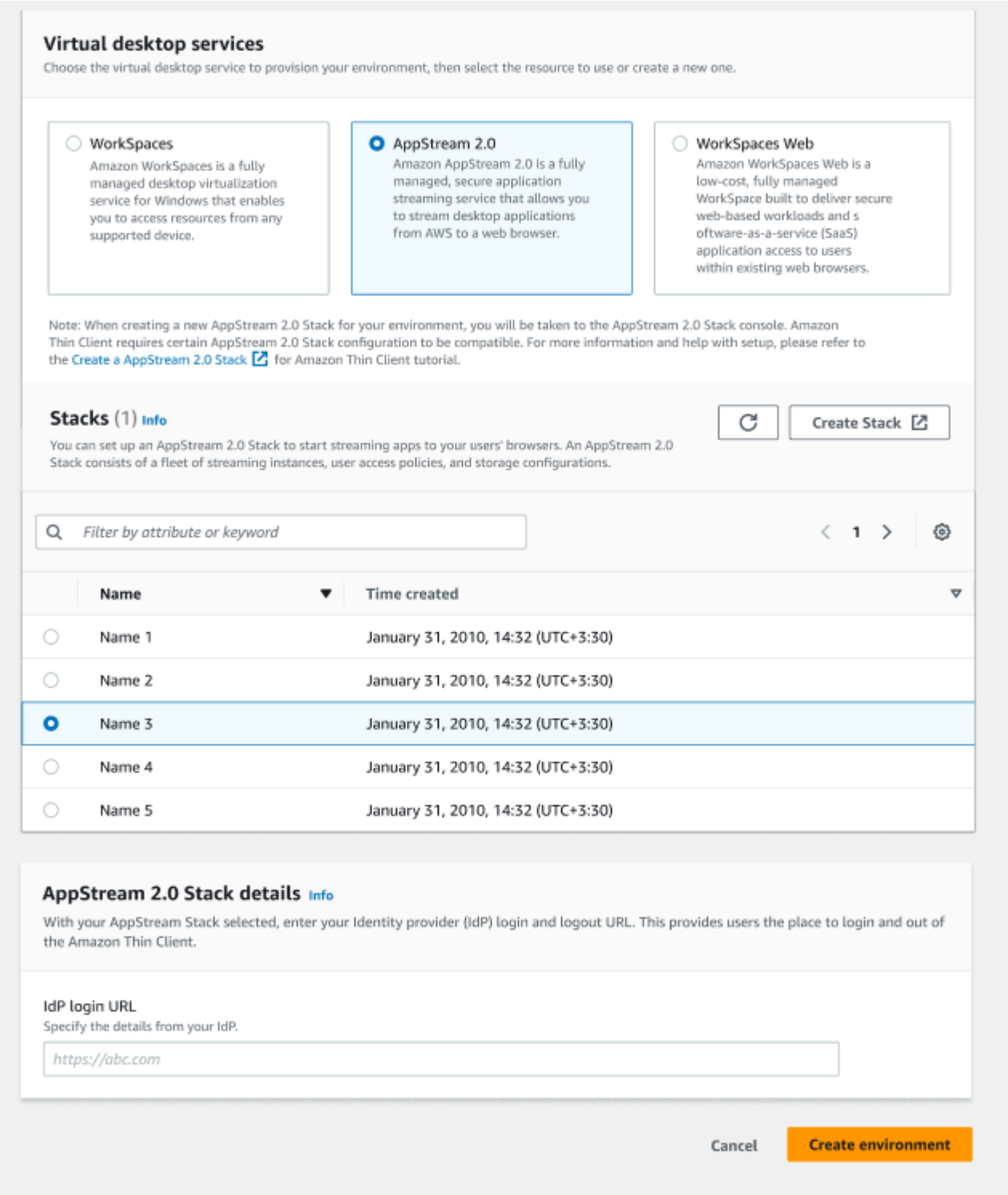
AppStream 2.0 是全受管、安全的應用程式串流服務，可用來串流桌面應用程式 AWS 至網頁瀏覽器。

> **Warning**
>
> 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，請執行下列其中一個動作：
   - 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搜尋堆疊。

     > **Note**
     >
     > 如果您在清單中沒有看到現有的堆疊，請在 AppStream 2.0 管理主控台中確認其符合 WorkSpaces 精簡型用戶端需求。

   - 選取「建立堆疊」按鈕以建立堆疊。如需建立 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。這為使用者提供登入和登出精簡型用戶 WorkSpaces 端的位置。
3. 選取「建立環境」按鈕。



建立環境之後，您仍然可以在稍後編輯詳細資料。如需詳細資訊，請參閱編輯環境。

使用 Amazon WorkSpaces 安全瀏覽

Amazon WorkSpaces Secure Browser 是一種低成本、全受管的 WorkSpaces 主控台，可為現有網頁瀏覽器中的使用者提供安全的網頁式工作負載和軟體即服務 (SaaS) 應用程式存取權。

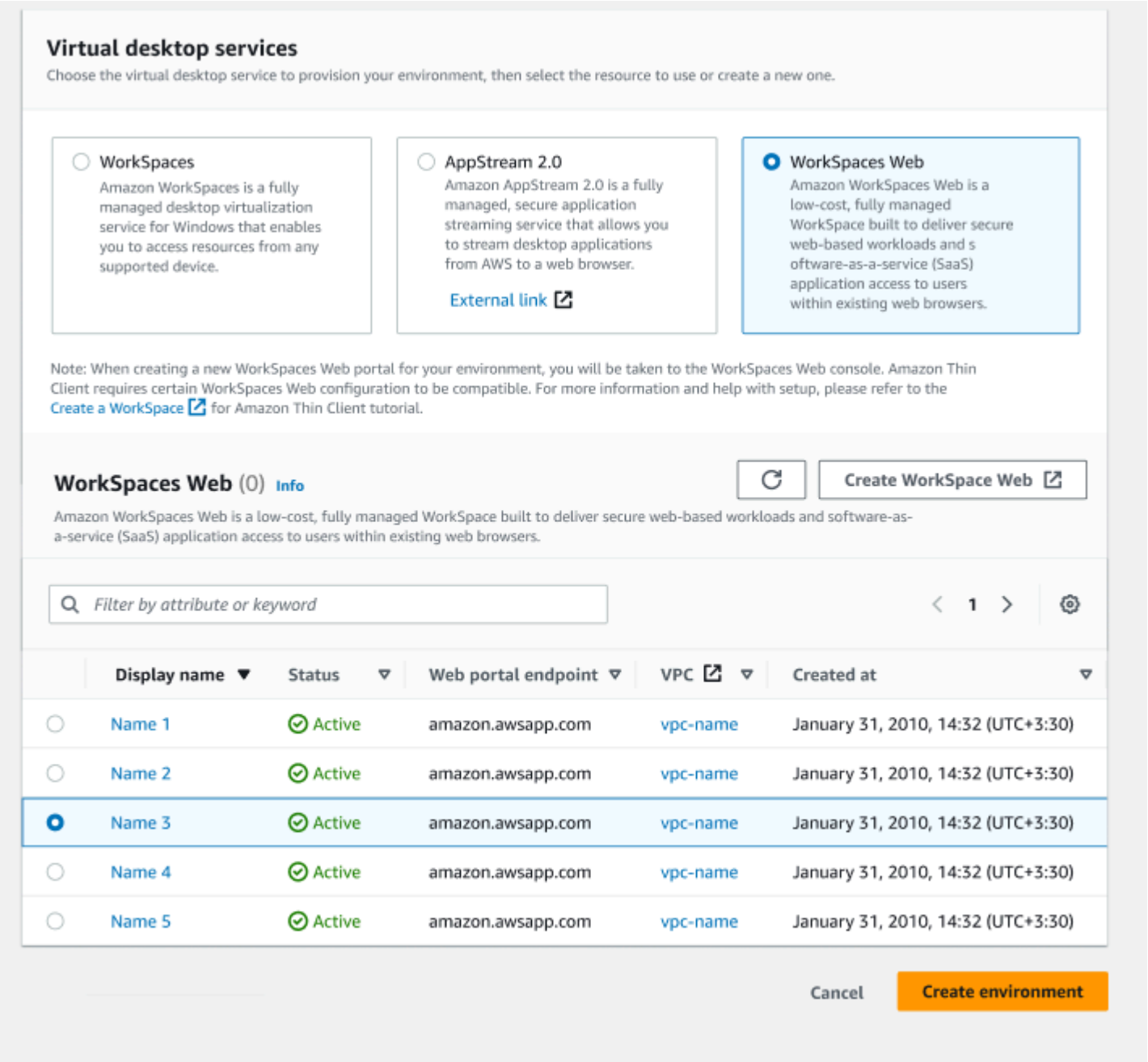
1. 若要設定 Amazon WorkSpaces 安全瀏覽器，請執行下列其中一個動作：

   - 選取您要用於您環境的入口網站。您可以瀏覽下拉式清單，也可以使用搜尋欄位來搜尋入口網站。

     > **Note**
     >
     > 如果您在清單中沒有看到現有的入口網站，請在 WorkSpaces 安全瀏覽器管理主控台中確認其符合 WorkSpaces 精簡型用戶端需求。

   - 選取 [建立 WorkSpaces 安全瀏覽器] 按鈕，建立 Web 入口網站。如需建立安 WorkSpaces 全瀏覽器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，您仍然可以在稍後編輯詳細資料。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

在您設定環境和虛擬桌面服務之後，您將在 AWS 管理主控台上收到一組用於設定的唯一啟動碼。

將此啟動碼提供給任何 WorkSpaces 精簡型用戶端裝置使用者，他們就可以使用它來存取其虛擬桌面。

如需有關如何協助裝置使用者設定其 Amazon WorkSpaces 精簡型用戶端的其他資訊，請參閱精簡型用戶 WorkSpaces 端使用指南。

編輯環境

WorkSpaces 精簡型用戶端管理主控台可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. 從下拉列表中選擇編輯。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。
   - 變更自動軟體修補程式更新軟體更新詳細資料的核取方塊。
   - 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. 從下拉列表中選擇刪除。 [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 精簡型用戶端終端使用者都有一個專用裝置，可將他們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 精簡型用戶端管理員主控台進行管理。

您可以從這個主控台為團隊訂購裝置。

裝置清單

裝置清單詳細資訊

裝置 ID：指派給個別裝置的識別號碼。

裝置名稱-(選擇性) 您指定給裝置的唯一名稱。

活動狀態-裝置的目前狀態。狀態狀態有兩種：

- 作用中：在過去七天裡至少連線至網路一次。
- 非作用中：過去七天裡未連線至網路。

註冊狀態-確認裝置已設定、與此 AWS 帳戶建立關聯，且屬於特定環境的一部分。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-裝置處於「重設與取消註冊」程序中。

> **Note**
>
> 如果裝置處於取消註冊狀態，您可以將其刪除。

- 已取消註冊：裝置已成功取消註冊。

> **Note**
>
> 您只能在裝置處於「取消註冊」或「取消註冊」狀態時刪除該裝置。

- 已封存：裝置已封存。

環境 ID：連接此裝置之環境的識別符。

軟體合規性：裝置軟體的合規性狀態。狀態狀態有兩種：

- 合規
- 不合規

裝置清單動作

搜尋：搜尋您管理的所有裝置。

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
- 取消登錄
- 存檔
- Delete
- 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

Summary

裝置序號-指派給個別裝置的識別號碼。

ARN-裝置的唯一識別碼，採用 Amazon 資源名稱 (ARN) 格式。

裝置名稱-您提供給裝置的名稱。如果您尚未創建名稱，則可以為其命名，否則將獲得默認名稱。

裝置類型-連結至帳戶的一般使用者裝置類型。

活動狀態：此裝置的目前狀態。這兩種狀態為：

- 作用中
- 非作用中

環境 ID-裝置使用之環境的識別號碼。

註冊狀態-確認裝置已設定、與此 AWS 帳戶建立關聯，且屬於特定環境的一部分。它可以處於以下四種狀態之一：

- 已註冊-這是預設狀態。
- 取消註冊-裝置處於「重設與取消註冊」程序中。
- 已取消註冊：裝置已成功取消註冊。

> **Note**
>
> 只有在裝置處於「已取消註冊」或「已封存」狀態時，才能刪除該裝置。

- 已封存-管理員已將此裝置標示為目前未服務。

註冊時間：裝置啟動的日期。

上次登入：最近一次登入的日期和時間。

上次檢查姿勢時間-最近一次裝置簽入的日期和時間。

目前的軟體版本：此裝置目前使用的軟體版本。

排程軟體更新-裝置上已排程的軟體版本。

軟體合規性：確認軟體集有效。狀態狀態有兩種：

- 合規

- 不合規

使用者日誌

上次存取裝置-上次使用此裝置的日期和時間。

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」視窗即會出現。
4. 在確認欄位中輸入 "deregister"。
5. 選取取消註冊按鈕。

> **Note**
>
> 取消註冊強制登出使用者，並需要在工作階段中重新啟動其 WorkSpaces 精簡型用戶端裝置。

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搜尋裝置。
2. 選取「動作」按鈕。
3. 從下拉列表中選擇存檔。 [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**
>
> 封存裝置會強制登出使用者，並需要在工作階段中重新啟動其 WorkSpaces 精簡型用戶端裝置。

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搜尋裝置。
2. 選取「動作」按鈕。
3. 從下拉列表中選擇刪除。 [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。

> **Note**
>
> 成功刪除裝置後，使用者必須將 WorkSpaces 精簡型用戶端裝置退回 Amazon。

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搜尋裝置。
2. 選取「動作」按鈕。
3. 從下拉列表中選擇導出設備詳細信息。所選裝置的詳細資料會以試算表格式下載。

軟體更新

WorkSpaces 精簡型用戶端有時需要引入新功能並套用安全性修補程式的軟體更新。這些更新由已建立版本的軟體集表示。

軟體集可以包含精簡型用戶 WorkSpaces 端裝置之軟體應用程式或作業系統的更新。您可以從此主控台選擇立即更新軟體，或者在環境的維護時段期間排程自動更新。

如需發行的軟體組清單，請參閱 WorkSpaces 精簡型用戶端環境軟體集。

主題

更新環境軟體

WorkSpaces 精簡型用戶端是一種 AWS 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 精簡型用戶端環境軟體集。
2. 選取 [安裝] 按鈕。
3. 在頁面頂端選取環境。
4. 從「環境」段落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**
     >
     > 現在更新軟件可能會中斷任何活動用戶會話。

   - 在每個環境維護期間更新軟體-在排定的環境維護時段期間更新環境軟體。
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 精簡型用戶端是一種 AWS 終端使用者運算服務，可提供精簡型用戶端裝置，將使用者連線至專用虛擬桌面。這些裝置會定期更新為新軟體。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一或多個裝置。如需軟體集的清單，請參閱WorkSpaces 精簡型用戶端環境軟體集。
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**
     >
     > 現在更新軟件可能會中斷任何活動用戶會話。

   - 在每個裝置維護期間更新軟體-在裝置的排定維護時段期間更新環境軟體。
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 精簡用戶端軟體版本

WorkSpaces 精簡型用戶端是一 AWS 種使用者運算服務，可讓使用者存取裝置上的虛擬桌面。這些裝置會定期更新為新的軟體集。下表說明所有已發行的軟體集。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
2.5.0	06-13-2024	• 修復了設備在啟動會話之前從睡眠中醒來時短暫顯示鍵盤和鼠標設置屏幕的問題。 • 裝置工具列上的 [首頁] 按鈕已重新命名為 [登入]。 • 改善工作階段中音訊/視訊呼叫的效能。
2.4.3	05-29-2024	• 銘 CVE-2024-5274 關鍵安全問題的零時差修復。
2.4.2	05-17-2024	• 銘 CVE-2024-4947 關鍵安全問題的零時差修復。

軟體集	版本日期	變更
2.4.1	05-15-2024	• 針對銘 CVE-2024-4671 和 CVE-2024-4761 關鍵安全性問題的零時差修正。 • 修正允許在 WorkSpaces 登入頁面上按一下 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	• 修正了阻止「帳戶 .google.com」並阻止使用谷歌工作區作為 IDP 2.0 會話的問題。AppStream • 只要在螢幕上的任何區域按一下，裝置設定工具列就會自動摺疊。
2.3.0	04-05-2024	• 裝置設定會顯示在摺疊的工具列中，以便更好地利用可見螢幕。 • 終端使用者現在可以設定在裝置閒置時進入睡眠狀態之前等待的持續時間。 • 修復了「關於：空白」網址顯示在第二個顯示屏上的問題。 • 修正延伸顯示關閉時導致白色畫面的問題。 • 終端使用者設定的音量現在會在裝置重新啟動期間保留。

軟體集	版本日期	變更
2.2.1	02-16-2024	• 修正在登入程序期間發生的問題，該問題會導致使用者無法登入 WorkSpaces 設定為 SAML 2.0 驗證。
2.2.0	02-08-2024	• 增加了對具有英語（英國），法語，德語，意大利語，西班牙語語言環境的 ISO 鍵盤的支持。
2.1.2	01-26-2024	• 銘 CVE-2024-0519 關鍵安全問題的零時差修復。 • 改進與鎖定功能相關的最終用戶延遲。 • 面向裝置的內部端點會切換至「精簡用戶端 *」網域。
2.1.1	12-21-2023	• 銘 CVE-2023-7024 關鍵安全問題的零時差修復。
2.1.0	12-20-2023	• 在裝置設定中新增主畫面按鈕，並啟用 Meta 金鑰的支援。這允許最終用戶通過按 Meta+L 調用鎖定屏幕。
2.0.1	12-06-2023	• 銘 CVE-2024-6345 關鍵安全問題的零時差修復。
2.0.0	11-15-2023	• 初始版本

在精簡用戶 WorkSpaces 端資源上使用標籤

您可以將自己的中繼資料指派給每個資源作為標籤，來組織和管理 WorkSpaces 精簡型用戶端的資源。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。您可以使用標籤做為管理 AWS 資源和組織資料 (包括帳單資料) 的簡單但功能強大的方式。

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 精簡型用戶端裝置，則在 8 月 1 日之前，這些標籤才會出現在您的成本分配報告中。如需詳細資訊，請參閱 AWS 帳單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 精簡型用戶端資源標籤，您必須按照《AWS Billing 使用者指南》中的〈啟動使用者定義的成本配置標籤〉中的指示，啟動已套用至 WorkSpaces 精簡型用戶端資源的標籤。
>
> 標籤會在啟用後 24 小時顯示，但與這些標籤相關聯的值可能需要 4-5 天才會顯示在 Cost Explorer 中。此外，若要在 Cost Explorer 中顯示並提供成本資料，已標記的 WorkSpaces 精簡型用戶端資源必須在該期間產生費用。Cost Explorer 只會顯示啟用標籤時的成本資料。目前沒有可用的歷史資料。

您可以標記的資源：

- 您可以在建立標籤時將標籤新增至下列資源 — WorkSpaces 精簡型用戶端環境。
- 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。

標籤限制

- 每一資源標籤數上限：50
- 金鑰長度上限：128 個統一字元
- 最大值長度 —256 個萬字元
- 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:前置詞，因為它已保留供 AWS 使用。您不可編輯或刪除具此字首的標籤名稱或值。

使用主控台更新現有環境的標籤

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。
   - 若要刪除標記，請選擇標籤旁邊的「移除」。
5. 當您完成更新標籤時，請選擇 [儲存]。

使用主控台更新現有裝置的標籤

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料頁面。
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。
   - 若要刪除標記，請選擇標籤旁邊的「移除」。
6. 當您完成更新標籤時，請選擇 [儲存]。

使用主控台更新軟體更新標籤

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。
- 若要刪除標記，請選擇標籤旁邊的「移除」。

5. 當您完成更新標籤時，請選擇 [儲存]。

Amazon WorkSpaces 精簡型用戶端中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon WorkSpaces 精簡型用戶端的合規計劃，請參閱合規計劃AWS 服務範圍內的合規計劃AWS的服務。
- 雲端安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用 WorkSpaces 精簡型用戶端時套用共同的責任模型。下列主題說明如何設定 WorkSpaces 精簡型用戶端以符合安全性與合規性目標。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 精簡型用戶端資源。

主題

Amazon WorkSpaces 精簡型用戶端中的資料保護

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。

- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

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，可用記憶體、網路診斷、網路資訊、裝置連線、SAML 認證、裝置識別資訊和損毀報告。這些信息用於為您提供服務，並可能用於改善用戶使用服務的體驗。此外，僅為了向您提供服務，信息可能會傳輸到用戶正在使用服務的 AWS 地區之外。我們會根據AWS 隱私權聲明處理此資訊。

主題

資料加密

WorkSpaces 精簡型用戶端會收集環境和裝置自訂資料，例如使用者設定、裝置識別碼、身分識別提供者資訊，以及串流桌面識別碼。 WorkSpaces 精簡用戶端也會收集工作階段時間戳記 收集到的資料會存放在 Amazon DynamoDB 和 Amazon S3 中。 WorkSpaces 精簡型用戶端使用 AWS Key Management Service (KMS) (KMS) 進行加密。

若要保護您的內容，請遵循下列指示：

- 實作最低權限存取，並建立用於精簡型用戶 WorkSpaces 端動作的特定角色。
- end-to-end 透過提供客戶管理的金鑰來保護資料，讓 WorkSpaces 精簡型用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：
  - 管理員必須登入 WorkSpaces 精簡型用戶端主控台，且使用者必須提供 WorkSpaces 精簡型用戶端設定的啟動碼，使用認證才能登入串流桌面。
  - 擁有實體存取權的任何人都可以設定 WorkSpaces 精簡型用戶端，但除非擁有有效的啟用碼和使用者認證可以登入，否則他們無法啟動工作階段。
- 使用者可以使用裝置工具列選擇鎖定螢幕、重新開機或關閉裝置，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 AWS 用 KMS 加密所有敏感資料，藉此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 精簡型用戶端的靜態資料加密

Amazon WorkSpaces 精簡型用戶端預設提供加密功能，透過使用 AWS 擁有的加密金鑰保護靜態的敏感客戶資料。

- AWS 擁有的金鑰 — Amazon WorkSpaces 精簡型用戶端預設會使用這些金鑰來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，也無法稽核其使用。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，以便在現有 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，因此您可以執行下列工作：
  - 建立和維護金鑰政策
  - 建立和維護 IAM 政策和授予操作
  - 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。

下表摘要說明 Amazon WorkSpaces 精簡型用戶端如何加密個人識別資料。

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 精簡用戶端環境名稱	已啟用	已啟用
裝置名稱 WorkSpaces 精簡用戶端裝置名稱	已啟用	已啟用

> **Note**
>
> Amazon WorkSpaces 精簡型用戶端會使用 AWS 擁有的金鑰免費保護個人身分資料，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 精簡型用戶端如何在 AWS KMS 中使用授權

Amazon WorkSpaces 精簡型用戶端需要授權供您使用客戶受管金鑰。

當您建立使用客戶受管金鑰加密的 WorkSpaces 精簡型用戶端環境時，Amazon WorkSpaces 精簡型用戶端會向 AWS KMS 傳送 CreateGrant 請求，代表您建立授權。 AWS KMS 中的授權用於授予 Amazon WorkSpaces 精簡型用戶端存取客戶帳戶中的 KMS 金鑰。

當新的精簡型用戶端裝置使用客戶受管金鑰向 WorkSpaces 精簡型用戶端加密環境註冊，且該裝置的名稱發生變更時，Amazon WorkSpaces 精簡型用戶端會向 AWS KMS 傳送 CreateGrant 請求，代表您建立授權。 AWS KMS 中的授權用於授予 Amazon WorkSpaces 精簡型用戶端存取客戶帳戶中的 KMS 金鑰。

Amazon WorkSpaces 精簡型用戶端需要授權，才能在下列內部作業中使用客戶受管金鑰：

- 傳送解密要求至 AWS KMS 以解密加密的資料

您可以撤銷授權的存取權，也可以隨時移除服務對客戶管理金鑰的存取權。如果這樣做，Amazon WorkSpaces 精簡型用戶端將無法存取由客戶管理金鑰加密的任何資料，這會影響依賴於該資料的操作。例如，如果您嘗試取得 Amazon WorkSpaces 精簡型用戶端無法存取的環境詳細資料，則作業會傳回錯`AccessDeniedException`誤。此外， WorkSpaces 精簡型用戶端裝置將無法使用 WorkSpaces 精簡型用戶端環境。

建立客戶受管金鑰

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

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。

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

- `kms:DescribeKey`— 提供客戶受管的金鑰詳細資訊，讓 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。
- `kms:CreateGrant`：將授予新增至客戶自管金鑰。授予指定 KMS 金鑰的控制權存取權，以允許存取 Amazon WorkSpaces 精簡型用戶端所需的授權操作。如需有關使用授予操作的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。

這可讓 Amazon WorkSpaces 精簡型用戶端執行下列動作：

- 呼叫 `Decrypt` 以解密加密的資料。

以下是您可以為 Amazon WorkSpaces 精簡型用戶端新增的政策聲明範例：

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "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*",
                "kms:RevokeGrant"
```

```
            ],
            "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》。

指定 WorkSpaces 精簡型用戶端的客戶管理金鑰

您可以將客戶自管金鑰指定為下列資源的第二層加密：

- WorkSpaces 精簡用戶端環境

建立環境時，您可以提供 Amazon WorkSpaces 精簡型用戶端用來加密可識別個人資料的指定資料金鑰。`kmsKeyArn`

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

當新的 WorkSpaces 精簡型用戶端裝置新增至使用客戶管理金鑰加密的 WorkSpaces 精簡型用戶端環境時， WorkSpaces 精簡型用戶端裝置會從精 WorkSpaces 簡型用戶端環境繼承客戶管理的金鑰設定。

加密內容是一組選用的索引鍵值配對，其中包含有關資料的其他內容資訊。

AWS KMS 會使用加密內容做為其他驗證資料，以支援驗證的加密。當您在加密資料的要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，請在要求中包含相同的加密內容。

Amazon WorkSpaces 精簡型用戶端加密內容

Amazon WorkSpaces 精簡型用戶端在所有 AWS KMS 加密操作中使用相同的加密內容，其中金鑰為`aws:thinclient:arn`，值為 Amazon 資源名稱 (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

當您使用對稱的客戶管理金鑰來加密 WorkSpaces 精簡型用戶端環境和裝置資料時，您也可以在稽核記錄和記錄中使用加密內容，以識別客戶管理金鑰的使用方式。加密內容也會出現在 AWS CloudTrail 或 Amazon 日誌產生的 CloudWatch 日誌中。

使用加密內容控制對客戶受管金鑰的存取

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。您也可以在授予中使用加密內容條件。

Amazon WorkSpaces 精簡型用戶端在授權中使用加密內容約束來控制對您帳戶或區域中客戶受管金鑰的存取。授予條件會要求授予允許的操作使用指定的加密內容。

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 精簡型用戶端的加密金鑰

當您將 AWS KMS 客戶受管金鑰與 Amazon WorkSpaces 精簡型用戶端資源搭配使用時，您可以使用 AWS CloudTrail 或 Amazon CloudWatch 日誌追蹤 Amazon WorkSpaces 精簡型用戶端傳送至 AWS KMS 的請求。

下列範例是針對DescribeKey、、CreateGrantGenerateDataKeyDecrypt、Decrypt (使用Grant) 監控 Amazon WorkSpaces 精簡型用戶端呼叫的 KMS 操作以存取由客戶管理金鑰加密的資料的 AWS CloudTrail 事件：

在下列範例中，您可以看到 WorkSpaces 精簡型encryptionContext用戶端環境。 WorkSpaces 精簡型用戶端裝置會記錄類似的 CloudTrail 事件。

DescribeKey

Amazon WorkSpaces 精簡型用戶端會使用此DescribeKey作業來驗證 AWS KMS 客戶受管金鑰。

下面的範例事件會記錄 DescribeKey 操作：

```
{
    "eventVersion": "1.08",
    "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"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
```

```
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "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"
}
```

CreateGrant

Amazon WorkSpaces 精簡型用戶端會使用此`CreateGrant`作業建立 KMS 授權，讓您在裝置存取資料時解密資料。

下面的範例事件會記錄 `CreateGrant` 操作：

```
{
    "eventVersion": "1.08",
    "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"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "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 精簡型用戶端會使用此GenerateDataKey作業來加密資料。

下面的範例事件會記錄 GenerateDataKey 操作：

```
{
    "eventVersion": "1.08",
    "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"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "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",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces 精簡型用戶端會使用此Decrypt作業來解密資料。

下面的範例事件會記錄 Decrypt 操作：

```
{
    "eventVersion": "1.08",
    "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"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "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",
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

當 WorkSpaces 精簡型用戶端裝置存取環境或裝置資訊時，會使用Decrypt作業，這是透過 KMS 金鑰允許的Grant。

下列範例事件會記錄透過授權的Decrypt作業Grant：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "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",
        "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",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "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 AWS Key Management Service 安全最佳實務的詳細資訊，請參閱AWS 金鑰管理服務開發人員指南。

傳輸中加密

WorkSpaces 精簡型用戶端會透過 HTTPS 和 TLS 1.2 加密傳輸中的資料。您可以使用主控台或直接 API 呼叫，將要求傳送至 WorkSpaces 精簡型用戶端。傳輸的要求資料會透過 HTTPS 或 TLS 連線傳送來加密。請求數據可以從 AWS 控制台， AWS 命令行界面或 AWS SDK 傳輸到 WorkSpaces 精簡客戶端。這也包括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代管 AWS KMS 金鑰來加密您的客戶資訊。如果您不提供金鑰， 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。

互聯網工作流量隱私

管理員可以檢視 WorkSpaces 精簡型用戶端工作階段事件，包括開始時間和擱置中的軟體更新資訊。這些記錄檔經過加密，並在精簡型用戶 WorkSpaces 端主控台中安全地傳送給客戶。桌面服

務會記錄個別串流桌面工作階段的使用者資訊和進一步詳細資料。如需詳細資訊，請參閱監視您的 WorkSpaces、 AppStream 2.0 的監視和報告或 WorkSpaces Web 的使用者存取記錄。

Amazon WorkSpaces 精簡型用戶端的身分識別和存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 WorkSpaces 精簡型用戶端資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

根據您在精簡型用戶 WorkSpaces 端中執行的工作而定，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 WorkSpaces 精簡型用戶端服務來執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 WorkSpaces 精簡型用戶端功能來完成工作時，您可能需要額外的權限。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。如果您無法存取 WorkSpaces 精簡型用戶端中的功能，請參閱疑難排解 Amazon WorkSpaces 精簡型用戶端身分識別。

服務管理員 — 如果您負責公司的 WorkSpaces 精簡型用戶端資源，您可能擁有 WorkSpaces 精簡型用戶端的完整存取權。決定您的服務使用者應該存取哪些 WorkSpaces 精簡型用戶端功能和資源是您的工作。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。若要深入瞭解貴公司如何搭配精簡型用戶 WorkSpaces 端使用 IAM，請參閱Amazon WorkSpaces 精簡型用戶端如何使用 IAM。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理 WorkSpaces 精簡型用戶端存取權的詳細資訊。若要檢視可在 IAM 中使用的 WorkSpaces 精簡型用戶端身分型政策範例，請參閱。Amazon WorkSpaces 精簡型用戶端的身分識別原則範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴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識別的範例。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 AWS 用同盟存取時，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。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

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 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需詳細資訊，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》中的在 AWS中使用多重要素驗證 (MFA)。

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，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 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作業。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

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

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，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程

式 AWS 帳戶 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 使用者是您內部的身分，具 AWS 帳戶 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。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials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，但角色僅提供暫時憑證。若要進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 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》中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要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》中的為第三方身分供應商建立角色。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：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。角色是授予跨帳户存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳户存取權和資源型政策間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源類型政策的差異。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。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。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。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 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。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性憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的相關資訊，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哪些內容。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。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以連接到身分 (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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 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 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 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 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原則類型。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：許可界限是一種進階功能，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的限制。所有這

類政策中的明確拒絕都會覆寫該允許。如需許可邊界的相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可邊界。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。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 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的 SCP 運作方式。
- 工作階段政策：工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合身分使用者的暫時工作階段時，作為參數傳遞。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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon WorkSpaces 精簡型用戶端如何使用 IAM

在您使用 IAM 管理精簡型用戶 WorkSpaces 端的存取權限之前，請先了解哪些 IAM 功能可用於 WorkSpaces 精簡型用戶端。

您可以搭配 Amazon WorkSpaces 精簡型用戶端使用的 IAM 功能

IAM 功能	WorkSpaces 精簡用戶端支援
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

IAM 功能	WorkSpaces 精簡用戶端支援
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	否

若要深入瞭解 WorkSpaces 精簡型用戶端和其他 AWS 服務如何搭配大多數 IAM 功能使用，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

精簡型用戶端的身分識別型原則 WorkSpaces

支援身分型政策	是

身分型政策是可以連接到身分 (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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。

精簡型用戶端的身分識別原則範例 WorkSpaces

若要檢視 WorkSpaces 精簡型用戶端身分型原則的範例，請參閱。Amazon WorkSpaces 精簡型用戶端的身分識別原則範例

精簡型用戶端內的資源 WorkSpaces 型政策

支援以資源基礎的政策	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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作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。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。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 角色與資源型政策有何差異。

WorkSpaces 精簡型用戶端的原則動作

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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。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 精簡型用戶端動作清單，請參閱服務授權參考中的 Amazon WorkSpaces 精簡型用戶端定義的動作。

精簡型用戶 WorkSpaces 端中的原則動作會在處理行動前使用下列前置詞：

```
workspaces-thin-client
```

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": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

若要檢視 WorkSpaces 精簡型用戶端身分型原則的範例，請參閱。Amazon WorkSpaces 精簡型用戶端的身分識別原則範例

WorkSpaces 精簡型用戶端的原則資源

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哪些內容。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 精簡型用戶端資源類型及其 ARN 的清單，請參閱服務授權參考中由 Amazon WorkSpaces 精簡型用戶端定義的資源。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon WorkSpaces 精簡型用戶端定義的動作。

若要檢視 WorkSpaces 精簡型用戶端身分型原則的範例，請參閱。Amazon WorkSpaces 精簡型用戶端的身分識別原則範例

WorkSpaces 精簡型用戶端的原則條件金鑰

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哪些內容。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，請使用邏輯OR運算來 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。如需詳細資訊，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條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 WorkSpaces 精簡型用戶端條件金鑰清單，請參閱服務授權參考中的 Amazon WorkSpaces 精簡型用戶端的條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon WorkSpaces 精簡型用戶端定義的動作。

若要檢視 WorkSpaces 精簡型用戶端身分型原則的範例，請參閱。Amazon WorkSpaces 精簡型用戶端的身分識別原則範例

精簡型用戶 WorkSpaces 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。

使用精簡型用戶 WorkSpaces 端的 ABAC

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。您可以將標籤附加到 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。

若要根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件金鑰，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》中的什麼是 ABAC?。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)。

搭配精簡用戶 WorkSpaces 端使用臨時登入

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。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》中的切換至角色 (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 精簡型用戶端的跨服務主體權限

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，您會被視為主體。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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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 精簡型用戶端的服務角色

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 服務服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 WorkSpaces 精簡型用戶端功能。只有在 WorkSpaces 精簡型用戶端提供指引時，才編輯服務角色。

WorkSpaces 精簡型用戶端的服務連結角色

支援服務連結角色。	否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。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 精簡型用戶端的身分識別原則範例

根據預設，使用者和角色沒有建立或修改 WorkSpaces 精簡型用戶端資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。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。

若要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。

如需 WorkSpaces 精簡型用戶端定義的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 精簡型用戶端適用的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用精簡型用戶 WorkSpaces 端主控台
- 授與 WorkSpaces 精簡型用戶端的唯讀存取
- 允許使用者檢視他們自己的許可

- 授予 WorkSpaces 精簡用戶端的完整存取權

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以在您的帳戶中建立、存取或刪除 WorkSpaces 精簡型用戶端資源。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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱《IAM 使用者指南〉中的 AWS 受管政策或工作職能的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，這也稱為最低許可許可。如需使用 IAM 套用許可的詳細資訊，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。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 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，可協助您編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 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 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》中的設定 MFA 保護的 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。

使用精簡型用戶 WorkSpaces 端主控台

若要存取 Amazon WorkSpaces 精簡型用戶端主控台，您必須擁有最少一組許可。這些權限必須允許您列出和檢視有關 AWS 帳戶. WorkSpaces 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。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。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。

授與 WorkSpaces 精簡型用戶端的唯讀存取

此範例顯示如何建立允許 IAM 使用者檢視精簡型用戶 WorkSpaces 端設定但不進行變更的政策。此政策包含使用 AWS CLI 或 AWS API 在主控台或程式上完成此動作的許可。

```
{
    "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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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 WorkSpaces 精簡用戶端的完整存取權

此範例顯示如何建立政策，以授予精簡型用戶 WorkSpaces 端 IAM 使用者的完整存取權。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 精簡型用戶端動作的許可。

```
{
    "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/*"]
        }
    ]
}
```

疑難排解 Amazon WorkSpaces 精簡型用戶端身分識別

使用下列資訊可協助您診斷和修正使用精簡型用戶 WorkSpaces 端和 IAM 時可能會遇到的常見問題。

主題

- 我沒有授權在 WorkSpaces 精簡客戶端中執行操作
- 我想要檢視我的存取金鑰
- 我是系統管理員，想要允許其他人存取 WorkSpaces 精簡型用戶端
- 我想允許我以外的人訪問我 AWS 帳戶 的 WorkSpaces 精簡客戶端資源

我沒有授權在 WorkSpaces 精簡客戶端中執行操作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。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 workspaces-thin-client:*ListDevices* 許可時發生。

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

在此情況下，Mateo 會要求管理員更新其策略，以允許他使用workspaces-thin-client:*ListDevices*動作存取*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。通過這樣做，您可能會讓某人永久訪問您的 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。

我是系統管理員，想要允許其他人存取 WorkSpaces 精簡型用戶端

若要允許其他人存取 WorkSpaces 精簡型用戶端，您必須為需要存取的個人或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的憑證來存取 AWS。然後，您必須將原則附加至實體，以便在 WorkSpaces 精簡型用戶端中授予他們正確的權限。

若要立即開始使用，請參閱《IAM 使用者指南》中的建立您的第一個 IAM 委派使用者及群組。

如需詳細資訊，請參閱 授予 WorkSpaces 精簡用戶端的完整存取權。

我想允許我以外的人訪問我 AWS 帳戶 的 WorkSpaces 精簡客戶端資源

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資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解 WorkSpaces 精簡型用戶端是否支援這些功能，請參閱Amazon WorkSpaces 精簡型用戶端如何使用 IAM。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要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)。
- 若要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 角色與資源型政策的差異。

Amazon WorkSpaces 精簡型用戶端的彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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 全域基礎結構。

除了 AWS 全球基礎架構之外， WorkSpaces 精簡型用戶端還提供多種功能，可協助您支援資料復原和備份需求。

Amazon WorkSpaces 精簡型用戶端中的漏洞分析和管理

配置和 IT 控制是與您之間共同 AWS 的責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

Amazon WorkSpaces 精簡型用戶端與 Amazon WorkSpaces、Amazon AppStream 2.0 和 WorkSpaces 網路交叉整合。如需有關這些服務的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 的更新管理 WorkSpaces
- Amazon WorkSpaces 網站中的配置和漏洞分析

Amazon 精 WorkSpaces 簡型用戶端

監控是維護 Amazon WorkSpaces 精簡型用戶端和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供下列監控工具來監視 WorkSpaces 精簡型用戶端、在發生錯誤時回報，並在適當時採取自動處理行動：

- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 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 位址，以及發生呼叫的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》。

使用記錄 Amazon WorkSpaces 精簡型用戶端 API 呼叫 AWS CloudTrail

Amazon WorkSpaces 精簡型用戶端與服務整合在一起 AWS CloudTrail，該服務可提供精 WorkSpaces 簡型用戶端中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 擷取 WorkSpaces 精簡型用戶端的所有 API 呼叫做為事件。擷取的呼叫包括來自 WorkSpaces 精簡型用戶端主控台的呼叫，以及對 WorkSpaces 精簡型用戶端 API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續傳遞 CloudTrail事件到 Amazon S3 儲存貯體，包括精簡型用戶 WorkSpaces 端的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 WorkSpaces 精簡型用戶端提出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

WorkSpaces 精簡型用戶端資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 WorkSpaces 精簡型用戶端中發生時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需持續記錄您 AWS 帳戶的事件 (包括 WorkSpaces 精簡型用戶端的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀

- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有 WorkSpaces 精簡型用戶端動作都會記錄在 Amazon WorkSpaces 精簡型用戶端 API 參考中，CloudTrail 並記錄在其中。例如，呼叫`CreateEnvironment`、`ListDevices`、和`GetSoftwareSet`動作會在 CloudTrail 記錄檔中產生項目。

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：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 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。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

瞭解 WorkSpaces 精簡型用戶端記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`GetDevice`動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
```

```
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
}
```

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

Amazon WorkSpaces 精簡型用戶端整合了這項服務 AWS CloudFormation，可協助您建立資源模型和設定資 AWS 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。您可以建立描述您想要的所有 AWS 資源 (例如環境) 的範本，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，以一致且重複地設定 WorkSpaces 精簡型用戶端資源。描述您的資源一次，然後在多個區域中重複佈建相同 AWS 帳戶 的資源。

WorkSpaces 精簡型用戶端和 AWS CloudFormation 範本

若要佈建和設定 WorkSpaces 精簡型用戶端及相關服務的資源，您必須瞭解AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式格式化的文字檔案。這些範本說明您要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML 格式，可以使用 AWS CloudFormation 設計工具來協助您開始 AWS CloudFormation 使用範本。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 AWS CloudFormation. 如需詳細資訊，包括適用於環境的 JSON 和 YAML 範本範本，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 指令行介面使用者指南

使用界面端點存取 Amazon WorkSpaces 精簡型用戶端 (AWS PrivateLink)

您可以使 AWS PrivateLink 用在 VPC 和 Amazon WorkSpaces 精簡型用戶端之間建立私有連線。您可以將 WorkSpaces 精簡型用戶端存取為 VPC，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用 IP 位址即可存取 WorkSpaces 精簡型用戶端。

您可以建立由支援的介面端點來建立此私人連線 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。這些是由要求者管理的網路介面，可做為傳送至精簡型用戶端之流量的進入點。 WorkSpaces

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 精簡型用戶端的考量

在為 WorkSpaces 精簡型用戶端設定介面端點之前，請先檢閱AWS PrivateLink 指南中的考量事項。

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

為 WorkSpaces 精簡型用戶端建立介面端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 為 WorkSpaces 精簡型用戶端建立介面端點。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 精簡型用戶端建立介面端點：

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

如果您為介面端點啟用私有 DNS，則可以使用精簡型用戶端的預設區域 DNS 名稱向 WorkSpaces 精簡型用戶端發出 API 要求。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。預設端點原則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 授與 WorkSpaces 精簡型用戶端的存取權，請將自訂端點原則附加到介面端點。

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：用於 WorkSpaces 精簡型用戶端動作的 VPC 端點原則

以下是自訂端點政策的範例。當您將此原則附加到介面端點時，它會授與對所有資源上所有主體列出的 WorkSpaces 精簡型用戶端動作的存取權。

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

WorkSpaces 精簡型用戶端管理員指南的文件歷程

下表說明《 WorkSpaces 精簡型用戶端管理員指南》發行版本的文件歷程記錄。

變更	描述	日期
• WorkSpaces 為 Amazon WorkSpaces 精簡用戶端設定 • 為 Amazon WorkSpaces 精簡型用戶端設定 AppStream 2.0	• 更新了操作系統列表。 • 已更新身分識別提供者程序。	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。