aws

管理指南

Amazon WorkSpaces 網站

Amazon WorkSpaces 網站: 管理指南

Table of Contents

什麼是 Amazon WorkSpaces Web？

Amazon WorkSpaces Web 是一種隨需、全受管、以 Linux 為基礎的服務，用於協助讓瀏覽器安全存取內部網站和軟體即服務 (SaaS) 應用程式。從現有的網頁瀏覽器存取服務，無需擔心基礎架構管理、專用用戶端軟體或虛擬私有網路 (VPN) 解決方案在管理上的負擔。

主題

使用 WorkSpaces Web 時要知道的術語

您應該熟悉以下概念，以幫助您開始使用 WorkSpaces Web。

Identity provider (IdP) (身分提供者 (IdP))

身分提供者會驗證您的使用者的登入資料。然後會發出身分驗證聲明，以提供存取權給服務提供者。您可以設定您的現有 IdP 以搭配 WorkSpaces Web 使用。

根據您的 IdP，會有不同的設定身分提供者 (IdP) 程序。

您必須將服務提供者中繼資料檔案上傳至您的 IdP。否則您的使用者將無法登入。您還必須授予使用者存取權限，才能在 IdP 中使用 WorkSpaces Web。

身分提供者 (IdP) 中繼資料文件

WorkSpaces Web 需要您身分提供者 (IdP) 的特定中繼資料來建立信任。您可以上傳從 IdP 下載的中繼資料交換檔案，將此中繼資料加入 WorkSpaces Web。

服務供應商 (SP)

服務提供者接受身分驗證斷言並向使用者提供服務。WorkSpaces Web 當成已通過其 IdP 驗證之使用者的服務提供者。

服務供應商 (SP) 中繼資料文件

您需要將服務提供者中繼資料詳細資料加入身分提供者 (IdP) 的組態介面。各提供者會有不同的組態流程詳細資訊。

SAML 2.0

用在 IdP 與服務提供者之間的身分驗證和授權資料交換的標準。

Virtual Private Cloud (VPC)

您可以使用現有或新的 VPC、對應的子網路和安全群組，將您的內容與 WorkSpaces Web 連結。

子網路必須與網際網路保持穩定連線，並且 VPC 和子網路也必須與任何內部網站和軟體即服務 (SaaS) 網站有穩定連線，才能存取這些資源。

列出的 VPC 子網路和安全群組來自與 WorkSpaces Web 主控台的相同區域。

Trust store (信任存放區)

如果使用者透過 WorkSpaces Web 存取網站時收到 NET::ERR_CERT_INVALID 這一類隱私權錯誤訊息，則該網站可能正在使用私有憑證授權單位 (PCA) 所簽署的憑證。您可能需要在信任存放區中新增或變更 PCA。此外，如果使用者的裝置要求您安裝特定憑證才能載入網站，則您需要將該憑證加入信任存放區，以允許您的使用者在 WorkSpaces Web 中存取該網站。

可公開存取的網站通常無需對信任存放區進行任何變更。

Web 入口網站

Web 入口網站可讓您的使用者從其瀏覽器存取內部和 SaaS 網站。您可以在每個帳戶的任何支援區域建立一個 Web 入口網站。若要要求提高多個入口網站的限制，請連絡支援人員。

Web 入口網站端點

Web 入口網站端點是您的使用者在使用針對入口網站設定的身分提供者登入後，啟動 Web 入口網站的存取點。

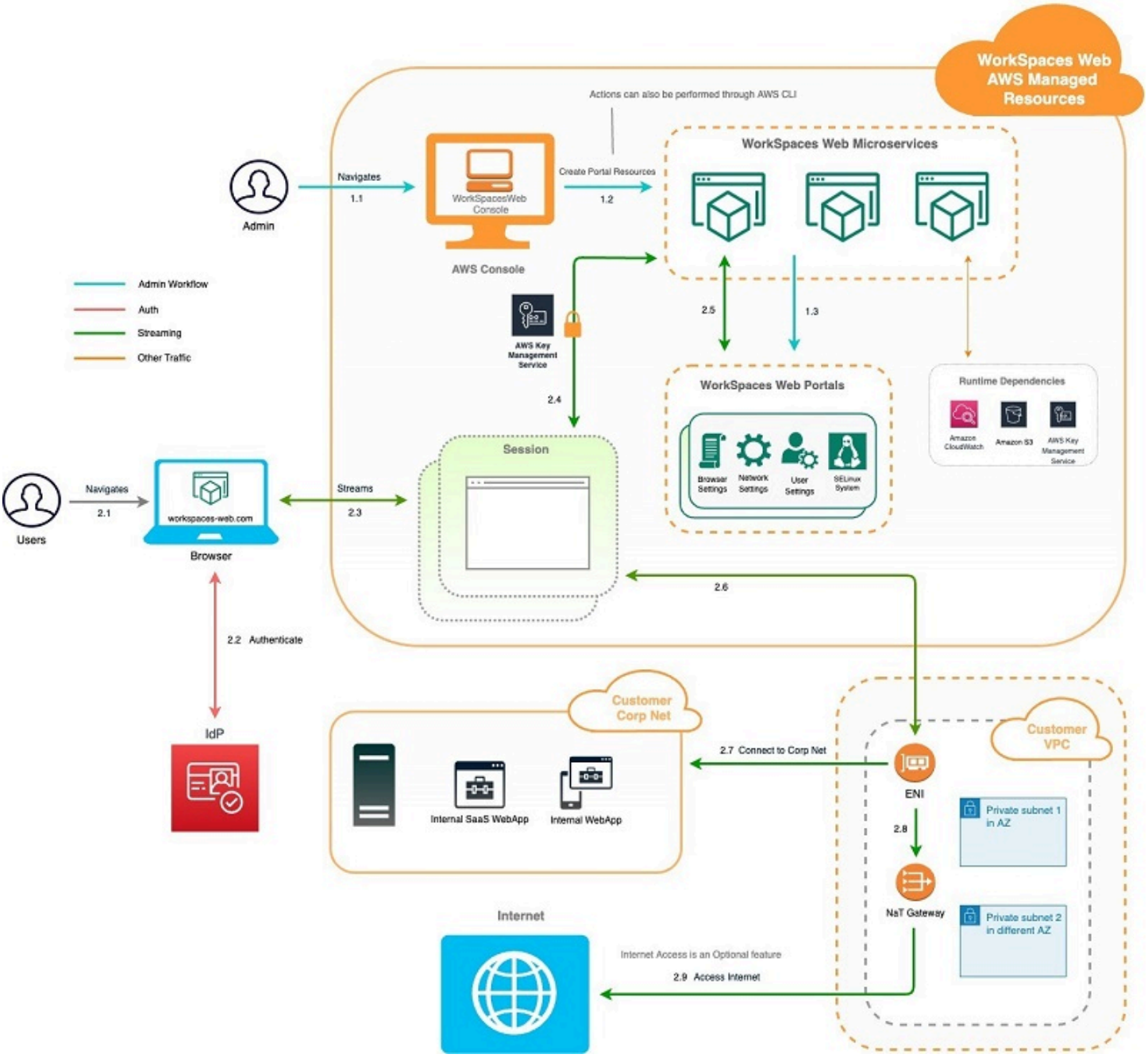
可在網際網路上公開使用端點，且可以嵌入您的網路。

相關服務

WorkSpaces Web 是 AWS 最終使用者運算產品組合中 Amazon WorkSpaces 提供的一項功能。相較於 WorkSpaces 和 AppStream 2.0，WorkSpaces Web 是專為促進安全的網頁式工作負載而打造的一項功能。WorkSpaces Web 會自動管理，且由 AWS 根據需求佈建和更新容量、擴展和映像。例如，您可以選擇為需要存取桌面資源的軟體開發人員提供永久性的 Workspace Desktop，並且選擇將 Amazon WorkSpaces Web 提供給只需要在桌上型電腦上存取少數內部和 SaaS 網站 (包括在網路外部託管的網站) 的客服中心使用者。

架構

下圖顯示 WorkSpaces Web 的基本架構。



存取 Amazon WorkSpaces Web

管理員可以透過 AWS WorkSpaces Web 主控台、SDK、CLI 或 API 存取 Amazon WorkSpaces Web。您的使用者可以透過 Amazon WorkSpaces Web 端點存取它。

設置 Amazon WorkSpaces 網站

您必須完成下列先決條件，才能設定 Amazon WorkSpaces Web 以連線到內部網站和 SaaS 應用程式。

主題

註冊和建立使用者

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

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，並在電話鍵盤輸入驗證碼。

   註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇 我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

當您註冊 AWS 帳戶 之後，請保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立管理使用者，讓您可以不使用根使用者處理日常作業。

保護您的 AWS 帳戶根使用者

1. 選擇 根使用者 並輸入您的 AWS 帳戶電子郵件地址，以帳戶擁有者身分登入 AWS Management Console。在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶根使用者啟用虛擬 MFA 裝置 (主控台)。

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的教學課程，請參閱《使用 AWS IAM Identity Center 使用者指南中的以預設 IAM Identity Center 目錄 設定使用者存取權限。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

  如需有關如何使用 IAM Identity Center 使用者登入的說明，請參閱《AWS 登入 使用者指南》中的登入 AWS存取入口網站。

授予程式設計存取權

若使用者想要與 AWS Management Console 之外的 AWS 互動，則需要程式設計存取權。授予程式設計存取權的方式取決於存取 AWS 的使用者類型。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請依照您要使用的介面所提供的指示操作。 • 關於 AWS CLI，請參閱 AWS Command Line Interface使用者指南 中的 設定 AWS CLI 來使用 AWS IAM Identity Center。 • 關於 AWS SDKs、工具和 AWS APIs，請參閱 AWSSDKs 和工具參考指南 中的 IAM Identity Center 驗證。
IAM	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請遵循 IAM 使用者指南 中 使用臨時憑證搭配 AWS 資源 中的指示。
IAM	(不建議使用) 使用長期憑證簽署 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 關於 AWS CLI，請參閱 AWS Command Line Interface使用者指南 中的 使用 IAM 使用者憑證進行驗證。 • 關於 AWS SDKs 和工具，請參閱 AWSSDKs 和工具參考指南 中的 使用長期憑證進行驗證。 • 關於 AWS API，請參閱 IAM 使用者指南 中的 管理 IAM 使用者的存取金鑰。

網路和存取

下列主題說明如何設定 WorkSpaces Web 串流執行個體，讓使用者可以連線到這些執行個體。同時也說明如何讓您的 WorkSpaces Web 串流執行個體存取 VPC 資源以及網際網路。

主題

VPC 要求

在建立 WorkSpaces Web 入口網站期間，您會在帳戶中選取 VPC。您也將選擇位於不同可用區域的至少兩個子網路。這些 VPC 和子網路必須符合下列要求：

- VPC 必須具有預設硬體租用。不支援具有專用租用的 VPC。
- 有鑑於可用性，我們至少需要在兩個不同可用區域中建立的子網路。您的子網路必須具有足夠的 IP 位址，才能支援預期的 WorkSpaces Web 流量。請為各個子網路設定子網路遮罩，該遮罩必須具備足夠的用戶端 IP 地址來應付最大同時工作階段數量。如需詳細資訊，請參閱 建立和設定新的 VPC。
- 所有子網路必須與使用者透過 WorkSpaces Web 存取的任何內部內容 (位於AWS 雲端或內部部署) 具有穩定的連線。

在考量到可用性和擴展的情況下我們建議您在不同的可用區域中選擇三個子網路。如需詳細資訊，請參閱 建立和設定新的 VPC。

WorkSpaces Web 不會為串流執行個體指派任何公用 IP 位址來啟用網際網路存取。這將使得使用者可以從網際網路存取您的串流執行個體。因此，任何連接到您公用子網路的串流執行個體都無法存取網際網路。如果您希望入口 WorkSpaces 網站同時存取公用網際網路內容和私人虛擬私人雲端內容，請完成中啟用不受限制的網際網路瀏覽 (建議)的步驟。

建立和設定新的 VPC

本節說明如何使用 VPC 精靈來建立具有公有子網路和一個私有子網路的 VPC。過程中，精靈會建立網際網路閘道和 NAT 閘道，它也會建立與公有子網路相關聯的自訂路由表。接著會更新與私有子網路相關聯的主路由表。會自動在您 VPC 的公有子網路中建立 NAT 閘道。

使用精靈建立 VPC 組態後，您必須新增第二個私有子網路。如需此組態的詳細資訊，請參閱具有公有和私有子網路 (NAT) 的 VPC。

步驟 1：配置彈性 IP 地址

在建立 VPC 之前，您必須在 WorkSpaces Web 區域中配置彈性 IP 位址。配置完成後，您可以將彈性 IP 地址與您的 NAT 閘道建立關聯。透過彈性 IP 地址，您可以快速地將地址重新映射至您 VPC 中的另一個串流執行個體，藉以遮罩串流執行個體的故障。如需詳細資訊，請參閱彈性 IP 地址。

> **Note**
>
> 您可能需要為使用的彈性 IP 地址付費。如需詳細資訊，請參閱彈性 IP 地址定價頁面。

如果您還沒有彈性 IP 地址，請完成以下步驟。若您要使用現有的彈性 IP 地址，您必須先確認它目前並未與其他執行個體或網路界面建立關聯。

配置彈性 IP 地址

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，於 Network & Security (網路與安全) 下方，選擇 Elastic IPs (彈性 IP)。
3. 選擇 Allocate New Address (配置新地址)，然後選擇 Allocate (配置)。
4. 請記下主控台上顯示的彈性 IP 地址。
5. 在彈性 IP 窗格的右上角，按一下 × 圖示來關閉窗格。

步驟 2：建立新的 VPC

請完成下列步驟，以建立具有公有子網路和一個私有子網路的新 VPC。

建立新的 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在導覽窗格中，選擇 VPC dashboard (VPC 儀表板)。
3. 選擇 Launch VPC Wizard (啟動 VPC 精靈)。
4. 在 Step 1: Select a VPC Configuration (步驟 1：選取 VPC 組態) 中，選擇 VPC with Public and Private Subnets (含公有和私有子網路的 VPC)，然後選擇 Select (選取)。
5. 在 Step 2: VPC with Public and Private Subnets (步驟 2：含公有和私有子網路的 VPC)中，按照以下內容設定 VPC：

   - 針對 IPv4 CIDR block (IPv4 CIDR 區塊)，請指定 VPC 的 IPv4 CIDR 區塊。
   - 針對 IPv6 CIDR block (IPv6 CIDR 區塊)，請保留預設值 No IPv6 CIDR Block (無 IPv6 CIDR 區塊)。
   - 針對 VPC 名稱，請輸入 VPC 的專屬名稱。
   - 根據以下內容設定公有子網路：
     - 針對 Public subnet's IPv4 CIDR (公有子網路的 IPv4 CIDR)，請為子網路指定 CIDR 區塊。
     - 針對 Availability Zone (可用區域)，請保留預設值 No Preference (無偏好設定)。
     - 針對公有子網路名稱，輸入子網路的名稱。例如 **`WorkSpaces Web Public Subnet`**。
   - 根據以下內容設定第一個私有子網路：
     - 針對 Private subnet's IPv4 CIDR (私有子網路的 IPv4 CIDR)，請為子網路指定 CIDR 區塊。記下您指定的值。
     - 針對 Availability Zone (可用區域)，請選取特定區域並記下您選取的區域。
     - 針對私有子網路名稱中，輸入子網路名稱。例如 **`WorkSpaces Web Private Subnet1`**。
   - 如果適用，請保留其他欄位的預設值。
   - 針對彈性 IP 配置 ID，請輸入與您建立之彈性 IP 地址對應的值。這個地址會指派至 NAT 閘道。如果您沒有彈性 IP 地址，請在 https://console.aws.amazon.com/vpc/ 使用 Amazon VPC 主控台建立地址。
   - 針對服務端點，如果您的環境需要 Amazon S3 端點，請指定一個。

     如果要指定 Amazon S3 端點，請按照以下步驟操作：

     1. 選擇 Add Endpoint (新增端點)。
     2. 針對服務，請選擇 com.amazonaws.***`Region`***.s3 項目，其中 *`Region`* 是您要在 AWS 區域 中建立 VPC 的位置。
     3. 針對 Subnet (子網路)，選擇 Private subnet (私有子網路)。
     4. 針對 Policy (政策)，請保留預設值 Full Access (完整存取權)。
   - 針對 Enable DNS hostnames (啟用 DNS 主機名稱)，請保留預設值 Yes (是)。

- 針對 Hardware tenancy (硬體租用)，請 保留預設值 Default (預設)。
- 選擇建立 VPC。
- 設定 VPC 需要幾分鐘的時間。建立 VPC 之後，選擇 OK (確定)。

步驟 3：新增第二個私有子網路

在上一個步驟中，您建立了具有一個公有子網路和一個私有子網路的 VPC。請完成以下步驟來新增您的 VPC 的第二個私有子網路。建議您在第一個私有子網路以外的可用區域新增第二個私有子網路。

新增第二個私有子網路

1. 在導覽窗格中，選擇 Subnets (子網)。
2. 選取您在上一個步驟中建立的第一個私有子網路。在 Description (描述) 標籤上 (位在子網路清單下方)，記下此子網路的可用區域。
3. 在子網路窗格的左上角選擇 Create Subnet (建立子網路)。
4. 針對名稱標籤，輸入私有子網路的名稱。例如 **`WorkSpaces Web Private Subnet2`**。
5. 針對 VPC，請選取您在前一個步驟建立的 VPC。
6. 針對可用區域，請選取您為第一個私有子網路使用之可用區域以外的可用區域。選取其他可用區域可提升容錯能力，並協助避免發生容量不足的錯誤。
7. 針對 IPv4 CIDR block (IPv4 CIDR 區塊)，請為新的子網路指定專屬的 CIDR 區塊範圍。舉例來說，如果您第一個私有子網路的 IPv4 CIDR 區塊範圍是 **`10.0.1.0/24`**，可以為第二個私有子網路指定 **`10.0.2.0/24`** 的 CIDR 區塊範圍。
8. 選擇建立。
9. 建立子網路之後，請選擇 Close (關閉)。

步驟 4：確認並為您的子網路路由表命名

在您建立並設定 VPC 後，請完成以下步驟來為您的路由表指定名稱：您需要驗證以下您的路由表詳細資訊是否正確：

- 與您 NAT 閘道所在之子網路關聯的路由表必須包含將網際網路流量指向網際網路閘道的路由。這可確保您的 NAT 閘道可以存取網際網路。
- 與您私有子網路建立關聯的路由表，必須設定為將網際網路流量指向 NAT 閘道。這可讓您私有子網路中的串流執行個體與網際網路通訊。

確認並為您的子網路路由表命名

1. 在導覽窗格中，選擇子網路，並選取您建立的公有子網路。例如，WorkSpaces Web 2.0 公用子網路。
2. 在 Route Table (路由表) 標籤上，請選擇路由表的 ID。例如，rtb-12345678。
3. 選取 路由表。在名稱下，選擇編輯 (鉛筆) 圖示，然後輸入路由表的名稱。例如，輸入名稱 **workspacesweb-public-routetable**。選取打勾記號以儲存名稱。
4. 在已選取公有路由表的情況下，於路由標籤確認本機端流量有兩個路由，且有一個路由會將所有其他流量傳送到 VPC 網際網路閘道。下表說明這兩種路由：

目的地	目標	描述
公有子網路 IPv4 CIDR 區塊 (例如 10.0.0.0/20)	區域	公有子網路 IPv4 CIDR 區塊中，以 IPv4 地址為目標的資源流量。此流量會在 VPC 內進行本機路由傳送。
以所有其他 IPv4 地址 (例如 0.0.0.0/0) 為目標的流量	流出 (igw-ID)	以所有其他 IPv4 地址為目標的流量，都會路由至 VPC 精靈所建立的網際網路閘道 (以 igw-ID 識別)。

5. 在導覽窗格中，選擇 Subnets (子網)。然後，選取您建立的第一個私有子網路 (例如，**WorkSpaces Web Private Subnet1**)。
6. 在路由表標籤上，請選擇路由表的 ID。
7. 選取 路由表。在名稱下，選擇編輯 (鉛筆) 圖示，然後輸入路由表的名稱。例如，輸入名稱 **workspacesweb-private-routetable**。若要儲存名稱，請選擇核取記號。
8. 在 Routes (路由) 標籤上，請確認路由表包含以下路由：

目的地	目標	描述
公有子網路 IPv4 CIDR 區塊 (例如 10.0.0.0/20)	區域	公有子網路 IPv4 CIDR 區塊中，以 IPv4 地址為目標的資源流量都會在 VPC 內進行本機路由。

目的地	目標	描述
以所有其他 IPv4 地址 (例如 0.0.0.0/0) 為目標的流量	流出 (nat-ID)	以所有其他 IPv4 地址為目標的流量，都會路由至 NAT 閘道 (以 nat-ID 識別)。
以 S3 儲存貯體為目標的流量 (如果您指定 S3 端點，則適用)[pl-ID (com.amazonaws.region.s3)]	儲存裝置 (vpce-ID)	以 S3 儲存貯體為目標的流量會路由至 S3 端點 (以 vpce-ID 識別)。

9. 在導覽窗格中，選擇 Subnets (子網)。然後選取您建立的第二個私有子網路 (例如，**WorkSpaces Web Private Subnet2**)。
10. 在路由表標籤上，請確認選定的路由表為私有路由表 (例如，**workspacesweb-private-routetable**)。如果路由表不同，請選擇編輯改為選取您的私有路由表。

啟用不受限制的網際網路瀏覽 (建議)

請依照下列步驟設定具有 NAT 閘道的 VPC，以進行不受限制的網際網路瀏覽。這將授予對公用 WorkSpaces 網際網路上的網站以及託管在 VPC 中或與 VPC 連線的私人網站的 Web 存取權。

設定具有 NAT 閘道的 VPC，以進行不受限制的網際網路瀏覽

如果您希望入口 WorkSpaces 網站同時存取公用網際網路內容和私人虛擬私人雲端內容，請依照下列步驟執行：

> **Note**
>
> 如果您已經設定好 VPC，請完成以下步驟來將 NAT 閘道新增至 VPC。如果您需要建立新的 VPC，請參閱建立和設定新的 VPC。

1. 若要建立 NAT 閘道，請完成建立 NAT 閘道中的步驟。請確定此 NAT 閘道具有公用連線，且位於 VPC 中的公用子網路中。
2. 您必須在不同的可用區域內指定至少兩個私有子網路。將子網路指派給不同的可用區域，有助於確保更好的可用性和容錯能力。如需如何建立第二個私有子網路的資訊，請參閱the section called “步驟 3：新增第二個私有子網路”。

> **Note**
>
> 若要確保每個串流執行個體都具有網際網路存取權，請勿將公用子網路附加至您的入口 WorkSpaces 網站。

3. 更新與您的私有子網路關聯的路由表，將網際網路的流量指向 NAT 閘道。這可讓您私有子網路中的串流執行個體與網際網路通訊。如需有關如何將路由表與私有子網路產生關聯的資訊，請完成設定路由表中的步驟。

啟用受限制的網際網路瀏覽（使用輸出 HTTP 代理）

WorkSpaces Web 入口網站的建議網路設定是使用具有 NAT 閘道的私人子網路，以便入口網站可以同時瀏覽公用網際網路和私人內容。如需詳細資訊，請參閱 the section called “啟用不受限制的網際網路瀏覽 (建議)”。不過，您可能需要使用 Web Proxy 來控制從入口 WorkSpaces 網站到網際網路的輸出通訊。例如，如果您使用 Web Proxy 做為網際網路閘道，您可以實作預防性安全控制，例如網域允許清單和內容篩選。這也可以透過快取經常存取的資源 (例如本機網頁或軟體更新) 來減少頻寬使用量並改善網路效能。對於某些使用案例，您可能擁有只能透過 Web Proxy 存取的私人內容。

您可能已經熟悉在受管理設備上或虛擬環境的映像上設定 Proxy 設定。但是，如果您無法控制裝置 (例如，使用者使用的是非企業擁有或管理的裝置)，或者您需要管理虛擬環境的映像，這會帶來挑戰。透過 WorkSpaces 網頁版，您可以使用網頁瀏覽器內建的 Chrome 政策來設定代理伺服器設定。您可以通過設置 WorkSpaces Web 的 HTTP 出站代理來做到這一點。

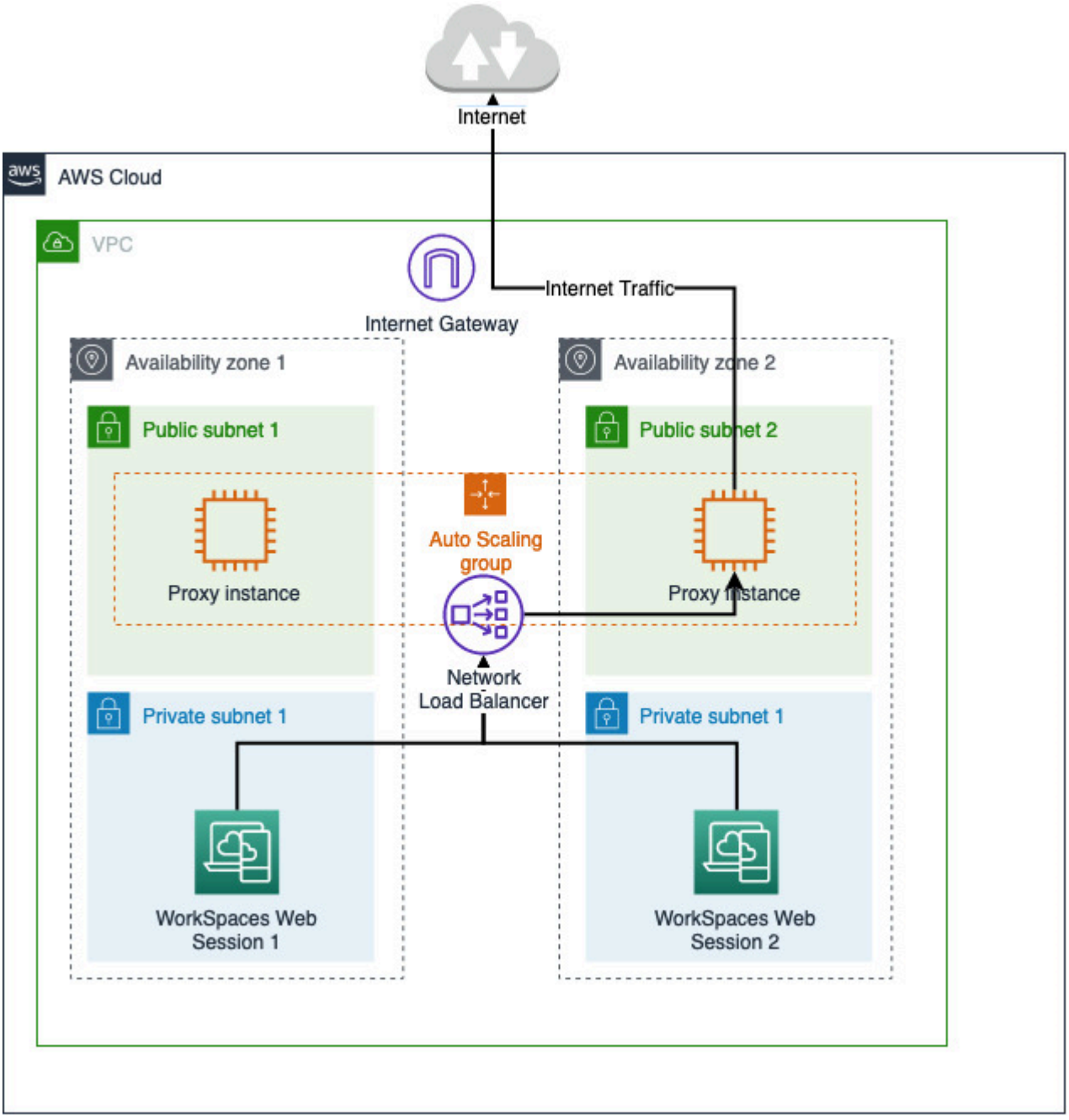
此解決方案是以建議的輸出 VPC Proxy 設定為基礎。代理解決方案是以開放原始碼 HTTP 代理伺服器 Squid 為基礎。然後，它會使用 WorkSpaces 網頁瀏覽器設定，將入口 WorkSpaces 網站設定為連線到 Proxy 端點。如需詳細資訊，請參閱如何使用網域白名單和內容篩選設定輸出 VPC Proxy。

此解決方案為您提供以下優點：

- 輸出代理，其中包含由網路負載平衡器託管的一組 auto-scaling Amazon EC2 執行個體。代理實例位於公共子網中，每個實例都附有彈性 IP，因此可以訪問互聯網。
- 部署到私人子網路的入口網站。 WorkSpaces 您不需要設定 NAT 閘道即可啟用網際網路存取。相反地，您可以設定瀏覽器原則，以便所有網際網路流量都會經過輸出 Proxy。如果您想要使用自己的 Proxy， WorkSpaces Web 入口網站的設定也會類似。

架構

以下是 VPC 中典型 Proxy 設定的範例。代理 Amazon EC2 實例位於公共子網中，並與彈性 IP 相關聯，因此他們可以訪問互聯網。網路負載平衡器主控 Proxy 執行個體的 auto 調整資源調度群組。如此可確保 Proxy 執行個體可以自動擴充，而網路負載平衡器是單一 Proxy 端點，可供 WorkSpaces Web 工作階段使用。



必要條件

開始之前，請確定您符合下列先決條件：

- 您需要已部署的 VPC，其中公有和私有子網路分散在多個可用區域 (AZ)。如需如何設定 VPC 環境的詳細資訊，請參閱預設 V PC。
- 您需要一個可從私有子網路存取的單一 Proxy 端點，其中 WorkSpaces Web 工作階段存取 (例如，網路負載平衡器 DNS 名稱)。如果您想要使用現有的 Proxy，請確定它也有可從您的私有子網路存取的單一端點。

設定網頁的 HTTP 輸出代理伺服 WorkSpaces 器

若要為 WorkSpaces Web 設定 HTTP 輸出代理伺服器，請依照下列步驟執行。

1. 若要將範例輸出 Proxy 部署到您的 VPC，請遵循如何使用網域白名單和內容篩選設定輸出 VPC Proxy 中的步驟進行操作。
   a. 依照「安裝 (一次性設定)」中的步驟，將 CloudFormation範本部署到您的帳戶。請務必選擇正確的 VPC 和子網路做為 CloudFormation 範本參數。
   b. 部署後，找到 CloudFormation 輸出參數OutboundProxyDomain和OutboundProxyPort。這是代理伺服器的 DNS 名稱和連接埠。
   c. 如果您已經擁有自己的代理伺服器，請略過此步驟，並使用 Proxy 的 DNS 名稱和連接埠。
2. 在 WorkSpaces Web 主控台中，選取您的入口網站，然後選擇 [編輯]。
   a. 在 [網路連線詳細資料] 中，選擇可存取 Proxy 的 VPC 和私人子網路。
   b. 在 [原則] 設定中，使用 JSON 編輯器新增下列 ProxySettings原則。此`ProxyServer`欄位應該是您代理伺服器的 DNS 名稱和連接埠。如需有關 ProxySettings 策略的詳細資訊，請參閱ProxySettings。

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
    }
}
```

3. 在您的 WorkSpaces 網絡會話中，您將看到代理已應用於 Chrome 設置 Chrome 正在使用管理員的代理設置。
4. 前往 chrome://政策和 Chrome 政策索引標籤，以確認該政策已套用。
5. 確認您的 WorkSpaces Web 工作階段可成功瀏覽網際網路內容，而不需要 NAT 閘道 在記錄 CloudWatch 檔中，確認是否已記錄 Squid 代理存取記錄檔。

故障診斷

套用 Chrome 政策後，如果您的 WorkSpaces 網頁工作階段仍無法存取網際網路，請依照下列步驟嘗試解決問題：

- 確認 Proxy 端點可從 Web 入口網站所在的 WorkSpaces 私人子網路存取。為此，請在私有子網路中建立 EC2 執行個體，並測試從私有 EC2 執行個體到 Proxy 端點的連線。
- 確認代理伺服器具有網際網路存取權。
- 確認 Chrome 政策是否正確無誤。
  - 確認策略`ProxyServer`欄位的下列格式：`<Proxy DNS name>:<Proxy port>`前綴`https://`中不應該有`http://`或。
  - 在 WorkSpaces 網頁工作階段中，使用 Chrome 瀏覽至 chrome://政策，並確認 ProxySettings 政策已成功套用。

VPC 設定建議

下列建議可協助您更有效率且安全地設定 VPC，

整體 VPC 組態

- 請確定您的 VPC 組態能夠支援擴展需求。
- 請確定您的 WorkSpaces Web 服務配額 (也稱為限制) 足以支援您預期的需求。若要請求增加配額，您可以使用 Service Quotas 主控台，位於 https://console.aws.amazon.com/servicequotas/。如需有關預設 WorkSpaces Web 配額的資訊，請參閱the section called “請求增加服務配額”。
- 如果您打算提供串流工作階段可存取網際網路，建議您在公有子網路中使用 NAT 閘道來設定 VPC。

彈性網路界面

- 在串流期間，每個 WorkSpaces Web 工作階段都需要自己的 elastic network interface。WorkSpaces Web 會建立盡可能多的彈性網路介面 (ENI) 與您的叢集所需的最大容量一樣多。每個區域的 ENI 限制預設為 5000。如需詳細資訊，請參閱網路介面。

  規劃大型部署的容量 (例如，數千個同時串流的工作階段) 時，請考慮尖峰使用量可能需要的 ENI 數量。我們建議您將 ENI 限制保持在或高於您為 Web 入口網站設定的最大同時使用量限制。

子網

- 在制定擴展使用者的計劃時，請記住，每個 WorkSpaces Web 工作階段都需要來自您設定的子網路的唯一用戶端 IP 位址。因此，子網路上設定的用戶端 IP 地址空間大小會決定可同時串流的使用者數量。
- 我們建議為各個子網路設定子網路遮罩，該遮罩必須具備足夠的用戶端 IP 地址來應付預期的最大同時上線使用者數量，此外也要考慮加入額外的 IP 地址來因應帳戶的預期成長。如需詳細資訊，請參閱 VPC 和 IPv4 的子網路大小調整。
- 我們建議您在所需區域中，在 WorkSpaces Web 支援的每個唯一可用區域中設定子網路，以便考量可用性和擴展。如需詳細資訊，請參閱 the section called “建立和設定新的 VPC”。
- 請確保可透過您的子網路存取網路應用程式所需的網路資源。

安全群組

- 使用安全群組來為 VPC 提供額外的存取控制。

  屬於 VPC 的安全群組可讓您控制 WorkSpaces Web 串流執行個體與 Web 應用程式所需的網路資源之間的網路流量。確認安全群組可提供您網路應用程式所需的網路資源存取權。

支援的可用區域

當您建立虛擬私有雲端 (VPC) 以搭配 WorkSpaces Web 使用時，VPC 的子網路必須位於要啟動 Web 的區域中的不同可用區域中。 WorkSpaces 可用區域是代表不同的位置，旨在隔離其他可用區域的故障。藉由在個別的可用區域中啟動執行個體，您就可以保護應用程式免於發生單點故障。各個子網必須完全位於某一可用區域內，不得跨越多個區域。我們建議您為所需區域中每個有支援的可用區域設定子網路，以獲得最大的恢復能力

可用區域以區域代碼加上字母識別符表示；例如 `us-east-1a`。為確保資源分配至區域中的所有可用區域，可用區域會獨立映射至各個 AWS 帳戶的名稱。例如，您 `us-east-1a` 帳戶的可用區域 AWS 與其他 `us-east-1a` 帳戶的 AWS 可能不在同一位置。

為協調各帳戶的可用區域，您必須使用 AZ ID，這是可用區域唯一且一致的識別符。例如，use1-az2 是 us-east-1 區域的 AZ ID，它在每一個 AWS 帳戶的位置都相同。

檢視 AZ ID 能讓您判斷某個帳戶資源在另一個帳戶中的相對位置。例如，如果您與另一個帳戶共享 AZ ID 為 use1-az2 的可用區域子網路，則 AZ ID 也是 use1-az2 之可用區域中的該帳戶就可以使用此子網路。Amazon VPC 主控台會顯示各 VPC 和子網路的 AZ ID。

WorkSpaces Web 可以在每個支援的區域的可用區域子集中使用。下表列出您可用於每個區域的 AZ ID。若要查看帳戶中 AZ ID 與可用區域的對應，請參閱《AWS RAM 使用者指南》中的資源適用的 AZ ID。

區域名稱	區域代碼	支援的 AZ ID
美國東部 (維吉尼亞北部)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
美國西部 (奧勒岡)	us-west-2	usw2-az1, usw2-az2, usw2-az3
亞太區域 (孟買)	ap-south-1	aps1-az1, aps1-az3
亞太區域 (首爾)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
亞太區域 (新加坡)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
亞太區域 (雪梨)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
亞太區域 (東京)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
加拿大 (中部)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
歐洲 (法蘭克福)	eu-central-1	euc1-az2, euc1-az2, euc1-az3

區域名稱	區域代碼	支援的 AZ ID
歐洲 (愛爾蘭)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
歐洲 (倫敦)	eu-west-2	euw2-az1, euw2-az2

如需可用區域和可用區域 ID 的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的區域、可用區域及 Local Zones。

VPC 連線

每個 WorkSpaces Web 串流執行個體都有一個客戶網路介面，可提供 VPC 內資源的連線，以及如果設定了具有 NAT 閘道的私有子網路，則可連線至網際網路。

針對網際網路連線，下列連接埠必須對所有目的地開放。如果您使用修改過或自訂的安全群組，則需要手動新增所需規則。如需詳細資訊，請參閱安全群組規則。

> **Note**
>
> 這適用於出口流量。

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

用戶端/使用者連線

WorkSpaces Web 設定為透過公用網際網路路由串流連線。需要網際網路連線才能驗證使用者並提供 Web 運作所需的 WorkSpaces Web 資產。若要允許此流量，您必須允許 允許的網域 中所列的網域。

下列主題提供如何啟用使用者連線至 WorkSpaces Web 的相關資訊。

主題

- IP 地址和連接埠需求

- 允許的網域

IP 地址和連接埠需求

若要存取 WorkSpaces Web 執行個體，使用者裝置需要下列連接埠的輸出存取權：

- 連接埠 443 (TCP)
  - 連接埠 443 用於在使用網際網路端點時，使用者裝置和串流執行個體之間的 HTTPS 通訊。一般而言，最終使用者在串流工作階段期間瀏覽 Web 時，Web 瀏覽器會隨機選取串流流量高範圍的來源連接埠。您必須確保允許對此連接埠的傳回流量。
  - 此連接埠必須開啟，才能使用 允許的網域 所列的必要網域。
  - AWS以 JSON 格式發佈其目前 IP 位址範圍，包括工作階段閘道和 CloudFront 網域可能解析為的範圍。如需如何下載 .json 檔案及檢視目前範圍的詳細資訊，請參閱 AWSIP 地址範圍。或者，如果您正在使用AWS Tools for Windows PowerShell，則可以使用Get-AWSPublicIpAddressRange PowerShell指令存取相同的資訊。如需詳細資訊，請參閱查詢 AWS 的公有 IP 地址範圍相關文章。
- (選用) 連接埠 53 (UDP)
  - 連接埠 53 用於使用者裝置和您 DNS 伺服器間的通訊。
  - 如果您未使用 DNS 伺服器進行網域名稱解析，則此連接埠為選用。
  - 連接埠必須開放給 DNS 伺服器的 IP 地址，以便解析公有網域名稱。

允許的網域

若要讓使用者能夠從其本機瀏覽器存取 WorkSpaces Web 服務，您必須將下列網域和 IP 位址新增至使用者嘗試存取服務的網路上的允許清單。

以下 *{Region}* 應該替換為操作 AWS 區域 的名稱。例如，若 s3.*{region}*.amazonaws.com 是用於歐洲 (愛爾蘭) (eu-west-1)，則應為 s3.eu-west-1.amazonaws.com。

類別	網域或 IP 位址
WorkSpaces 網路串流資產	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com

類別	網域或 IP 位址
	*.amazonappstream.com *.shortbread.aws.dev
WorkSpaces 網路 WebApp 資產	*.workspaces-web.com
WorkSpaces 網頁驗證	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces 網頁指標和報告	*.execute-api.*{region}*.amazonaws.com unagi-na.amazon.com

根據您設定的身分提供者，您可能也需要允許列出其他網域。檢閱您的 IdP 文件，以確定您需要允許哪些網域清單， WorkSpaces Web 才能使用該提供者。如果您使用的是 IAM Identity Center，請參閱 IAM Identity Center 先決條件以取得更詳細的資訊。

開始使用 Amazon WorkSpaces 網站

請依照下列步驟建立 WorkSpaces Web 入口網站，並讓使用者從現有瀏覽器存取內部和 SaaS 網站。您可以在每個帳戶的任何支援區域建立一個 Web 入口網站。

> **Note**
>
> 若要要求提高多個入口網站的限制，請連絡支援人員，並提供您的 AWS 帳戶 ID、要求的入口網站數量，以及 AWS 區域。

這個作業使用 Web 入口網站建立精靈，通常要 5 分鐘的時間，而入口網站最多還要 15 分鐘的時間才能成為作用中狀態。

設定入口網站不會產生任何相關費用。 WorkSpaces Web 提供 pay-as-you-go定價，包括為積極使用該服務的用戶提供低廉的每月價格。您將無需先預付成本、授權或簽訂長期合約。

> **Important**
>
> 您必須在開始前先完成 Web 入口網站的先決條件。如需 Web 入口網站先決條件的詳細資訊，請參閱 設置 Amazon WorkSpaces 網站。

主題

步驟 1：建立 Web 入口網站

請執行下列步驟以建立 Web 入口網站：

主題

- 進行使用者設定
- 設定身分提供者
- 檢閱和啟動

進行網路設定

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces 網頁]、[入口網站]，然後選擇 [建立入口網站]。
3. 在步驟 1：指定網路連線頁面上，完成下列步驟，將您的 VPC 連線到 Web 入口網站，並且設定您的 VPC 和子網路。

    1. 如需網路詳細資料，請選擇連線到您希望使用者透過 WorkSpaces Web 存取之內容的 VPC。
    2. 選擇最多三個符合下列需求的私有子網路。如需詳細資訊，請參閱 網路和存取。
        - 您必須選擇最少兩個私有子網路，才能建立入口網站。
        - 建議您為 VPC 提供唯一可用區域中最大數量的私有子網路，以確保入口網站的高可用性。
    3. 選擇安全群組。

進行入口網站設定

在步驟 2：進行 Web 入口網站設定頁面上，完成下列步驟，以自訂使用者啟動工作階段時的瀏覽體驗。

1. 在 Web 入口網站詳細資訊底下，針對顯示名稱輸入可識別您入口網站的名稱。
2. 在使用者存取日誌記錄底下，針對 Kinesis 串流 ID，選取您要將資料傳送到哪個 Amazon Kinesis 資料串流。如需詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。
3. 在政策設定下，完成下列操作：

    - 針對選項，請選取視覺化編輯器或 JSON 檔案上傳。您可以使用其中一種方法來提供 Web 入口網站的政策組態詳細資訊。如需詳細資訊，請參閱 the section called “設定或編輯瀏覽器政策”。
        - WorkSpaces 網頁版包含對 Chrome 企業政策的支援。您可以使用視覺化編輯器或手動上傳政策檔案，以新增和管理政策。您可隨時切換使用這兩個選項。
        - 上傳政策檔案時，您可以在主控台中看到可用的政策檔案。但是，您無法在視覺化編輯器中編輯所有政策。主控台會列出您無法在其他 JSON 政策下使用視覺化編輯器編輯的 JSON 檔案政策。您必須用手動編輯的方式，才能更動這些政策。

- (選用) 針對啟動 URL – 選用，輸入當使用者啟動瀏覽器時當成首頁的網域。您的 VPC 必須與此 URL 保持穩定連線。
- 選取或清除隱私瀏覽和刪除歷程記錄，以在使用者工作階段期間開啟或關閉這些功能

> **Note**
>
> 在使用者存取日誌記錄中無法記錄使用隱私瀏覽功能，或在使用者刪除瀏覽器歷程記錄之前造訪的 URL。如需詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。

- 在 [URL 篩選] 底下，您可以設定使用者可以在工作階段期間造訪哪些 URL。如需詳細資訊，請參閱 the section called “設定網址過濾”。
- (選用) 針對瀏覽器書籤 – 選用，針對您要使用者在其瀏覽器中看到的任何書籤，輸入顯示名稱、網域和資料夾。然後，選擇新增書籤。

> **Note**
>
> 網域是瀏覽器書籤的必填欄位。
> Chrome 的使用者可以在書籤工具列的受管理的書籤資料夾中找到受管理的書籤。

- (選用) 為您的入口網站新增標籤。您可以使用標籤來搜尋或篩選資 AWS 源。標籤由金鑰和選用值組成，且與您的入口網站資源相關聯。

4. 在 IP 存取控制 (選用) 底下，選擇是否要限制存取受信任的網路。如需詳細資訊，請參閱 the section called “設定 IP 存取控制 (選用)”。
5. 選擇 Next (下一步) 繼續。

進行使用者設定

在步驟 3：選取使用者設定頁面上完成下列步驟，選擇使用者在工作階段期間可從頂端導覽列存取的功能，然後選擇下一步：

1. 針對使用者許可，請選擇是否啟用單一登入擴充功能。如需詳細資訊，請參閱 the section called “啟用單一登入擴充功能 (選用)”。
2. 針對剪貼簿許可，請選擇停用或啟用。
3. 在檔案傳輸下，選擇停用或啟用。
4. 針對列印至本機端裝置，選擇允許或不允許。

5. 針對使用者工作階段詳細資訊，指定以下內容：

   - 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。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。

設定身分提供者

請使用下列步驟來設定您的身分識別提供者 (IdP)。

主題

- 選擇身分識別提供者類型
- 設定標準驗證類型
- 設定 IAM 身分中心身分驗證類型
- 變更身分識別提供者類型

選擇身分識別提供者類型

WorkSpaces Web 提供了兩種身份驗證類型：標準和 AWS IAM Identity Center. 您可以在 [設定身分識別提供者] 頁面上選擇要搭配入口網站使用的驗證類型。

- 對於標準 (預設選項)，請直接將您的第三方 SAML 2.0 身分識別提供者 (例如 Okta 或 Ping) 與入口網站聯合。如需詳細資訊，請參閱 the section called “設定標準驗證類型”。標準類型支援 SP 起始和 IDP 起始的驗證流程。
- 對於 IAM 身分中心 (進階選項)，請將 IAM 身分中心與入口網站聯合。若要使用此身分驗證類型，您的 IAM 身分中心和 WorkSpaces Web 入口網站必須位於相同的身分驗證類型 AWS 區域。如需詳細資訊，請參閱 the section called “設定 IAM 身分中心身分驗證類型”。

設定標準驗證類型

對於標準 (預設)，請直接將您的第三方 SAML 2.0 身分識別提供者 (例如 Okta 或 Ping) 與入口網站聯盟。

標準身分識別類型可以透過符合 SAML 2.0 標準的 IdP 支援 service-provider-initiated identity-provider-initiated (SP 起始) 和 (IdP 起始) 登入流程。

步驟 1：開始在 WorkSpaces Web 上設定您的身分識別提供者

完成下列步驟來設定您的身分識別提供者：

1. 在建立精靈的設定身分提供者頁面上，選擇標準。
2. 選擇「繼續標準 IdP」。
3. 下載 SP 中繼資料檔案，並保持開啟個別中繼資料值的索引標籤。
   - 如果 SP 中繼資料檔案可用，請選擇「下載中繼資料檔案」以下載服務提供者 (SP) 中繼資料文件，然後在下一個步驟中將服務提供者中繼資料檔案上傳至您的 IdP。如果沒有此功能，使用者將無法登入。
   - 如果您的供應商未上傳 SP 中繼資料檔案，請手動輸入中繼資料值。
4. 在「選擇 SAML 登入類型」下，選擇 SP 起始和 IDP 起始的 SAML 宣告，或者僅限 SP 起始的 SAML 判斷提示。
   - SP 起始和 IDP 起始的 SAML 判斷提示可讓您的入口網站支援這兩種類型的登入流程。支援 IdP 起始流程的入口網站可讓您將 SAML 宣告呈現給服務身分識別聯合端點，而不需要使用者透過造訪入口網站 URL 啟動工作階段。
     - 選擇此選項以允許入口網站接受來路不明的 IDP 起始 SAML 宣告。

- 此選項需要在 SAML 2.0 身分識別提供者中設定預設的轉送狀態。入口網站的轉送狀態參數位於 IdP 起始 SAML 登入之下的主控台中，或者您可以從下的 SP 中繼資料檔案複製它。`<md:IdPInitRelayState>`
- 注意
  - 以下是轉送狀態的格式：`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`。
  - 如果您複製並貼上 SP 中繼資料檔案中的值，請確定您將變更`&amp;` 為`&`。 `&amp;`是 XML 逸出字元。
- 只針對入口網站選擇 SP 起始的 SAML 宣告，以僅支援 SP 起始的登入流程。此選項將拒絕來自 IDP 起始登入流程的來路不明的 SAML 宣告。

> **Note**
>
> 某些協力廠商 IdPs 允許您建立自訂 SAML 應用程式，該應用程式可利用 SP 啟動的流程提供 IdP 起始的驗證體驗。例如，請參閱新增 Okta 書籤應用程式。

5. 選擇是否要對此提供者啟用「簽署 SAML 要求」。SP 啟動的驗證可讓您的 IdP 驗證驗證要求來自入口網站，以防止接受其他第三方要求。
   a. 下載簽署憑證並將其上傳至您的 IdP。相同的簽署憑證可用於單一登出。
   b. 在 IdP 中啟用已簽署的要求。名稱可能會有所不同，具體取決於 IdP。

> **Note**
>
> RSA-SHA256 是唯一支援的要求和預設要求簽章演算法。

6. 選擇是否要啟用「需要加密的 SAML 宣告」。這可讓您加密來自 IdP 的 SAML 判斷提示。它可以防止在 IdP 和 Web 之間的 SAML 判斷提示中攔截資料。 WorkSpaces

> **Note**
>
> 此步驟無法使用加密憑證。它將在您的門戶網站啟動後創建。啟動入口網站之後，請下載加密憑證並將其上傳到您的 IdP。然後，在 IdP 中啟用斷言加密（名稱可能會有所不同，具體取決於 IdP。

7. 選擇是否要啟用「單一登出」。單一登出可讓您的使用者透過單一動作登出其 IdP 和 WorkSpaces Web 工作階段。

   a. 從 WorkSpaces Web 下載簽名證書並將其上傳到您的 IdP。這與上一個步驟中用於「要求簽署」的簽署憑證相同。

   b. 使用單一登出時，您必須在 SAML 2.0 身分識別提供者中設定單一登出 URL。您可以在服務提供者 (SP) 詳細資料下的主控台中找到入口網站的單一登出 URL-顯示個別中繼資料值，或從下<md:SingleLogoutService>的 SP 中繼資料檔案。

   c. 在 IdP 中啟用單一登出。名稱可能會有所不同，具體取決於 IdP。

步驟 2：在您自己的 IdP 上設定您的身分識別提供者

在瀏覽器中開啟新的分頁。然後使用您的 IdP 完成下列步驟：

1. 將入口網站中繼資料新增至您的 SAML IdP。

   將您在上一個步驟中下載的 SP 中繼資料文件上傳至 IdP，或將中繼資料值複製並貼到 IdP 中的正確欄位中。某些供應商不允許檔案上傳。

   此過程的詳細信息可能因提供商而異。如the section called “具體的指導 IdPs”需如何將入口網站詳細資料新增至 IdP 組態的說明，請參閱中的提供者說明文件。

2. 確認您的 SAML 宣告的 NameID。

   請確定您的 SAML IdP 在 SAML 判斷提示中填入使用者電子郵件欄位的 NameID。NameID 和使用者電子郵件用於透過入口網站唯一識別您的 SAML 聯合身分使用者。使用永久性 SAML 名稱識別碼格式。

3. 可選：為 IDP 起始的驗證設定轉送狀態。

   如果您在上一個步驟中選擇了接受 SP 起始和 IDP 起始的 SAML 宣告，請依照步驟 2 中的步驟設定 IdP 應用程式的預設the section called “步驟 1：開始在 WorkSpaces Web 上設定您的身分識別提供者”轉送狀態。

4. 選用性：設定要求簽署。如果您在上一個步驟中選擇「將 SAML 要求簽署給此提供者」，請遵循步驟 3 中的步驟，將簽署憑證上傳the section called “步驟 1：開始在 WorkSpaces Web 上設定您的身分識別提供者”到您的 IdP 並啟用要求簽署。某些 IdPs 例如 Okta 可能要求您的 NameID 屬於「永久」類型才能使用請求簽名。請依照上述步驟確認您的 SAML 判斷提示的 NameID。

5. 選用性：設定宣告加密。如果您選擇需要來自此提供者的加密 SAML 宣告，請等到入口網站建立完成，然後遵循下面「上傳中繼資料」中的步驟 4，將加密憑證上傳至您的 IdP 並啟用宣告加密。

6. 選用性：設定單一登出。如果您選擇「單一登出」，請按照步驟 5 中的步驟將簽署憑證上傳the section called “步驟 1：開始在 WorkSpaces Web 上設定您的身分識別提供者”到 IdP，填寫「單一登出 URL」，然後啟用「單一登出」。
7. 授與 IdP 中的使用者使用 WorkSpaces Web 的存取權。
8. 從您的 IdP 下載中繼資料交換檔案。您將在下一個步驟中將此中繼資料上傳至 WorkSpaces Web。

步驟 3：完成在 WorkSpaces Web 上設定您的身分識別提供者

返回 WorkSpaces Web 主控台。在建立精靈的 [設定身分識別提供者] 頁面上，在 IdP 中繼資料下，上傳中繼資料檔案，或從您的 IdP 輸入中繼資料 URL。入口網站會使用 IdP 中繼資料來建立信任。

1. 若要上載中繼資料檔案，請在 IdP 中繼資料文件下，選擇「選擇檔案」。上傳您在上一個步驟中從 IdP 下載的 XML 格式中繼資料檔案。
2. 若要使用中繼資料 URL，請前往您在上一個步驟中設定的 IdP，並取得其中繼資料 URL。返回 WorkSpaces Web 主控台，然後在 IdP 中繼資料 URL 下，輸入您從 IdP 取得的中繼資料 URL。
3. 完成時請選擇 Next (下一步)。
4. 如果入口網站已啟用「需要來自此提供者的加密 SAML 宣告」選項，您必須從入口網站 IdP 詳細資料區段下載加密憑證，並將其上傳至您的 IdP。然後，您可以在此處啟用該選項。

> **Note**
>
> WorkSpaces 網頁需要在 IdP 的設定中，在 SAML 宣告中對應並設定主旨或 NameID。您的 IdP 可以自動建立這些對映。如果未正確設定這些對映，您的使用者將無法登入 Web 入口網站和啟動工作階段。
>
> WorkSpaces 網路需要在 SAML 回應中出現下列宣告。<Your SP Entity ID><Your SP ACS URL>您可以透過主控台或 CLI 尋找入口網站的服務提供者詳細資料或中繼資料文件，並從中找到。
>
> - 具有將您的 SP 實體 ID 設定為回應目標的`Audience`值的`AudienceRestriction`宣告。範例：
>
> ```
> <saml:AudienceRestriction>
>     <saml:Audience><Your SP Entity ID></saml:Audience>
> </saml:AudienceRestriction>
> ```
>
> - `InResponseTo` 值為原始 SAML 請求 ID 的 `Response` 宣告。範例：
>
> ```
> <samlp:Response ... InResponseTo="<originalSAMLrequestId>">
> ```

- 具有您的 SP ACS 網址`Recipient`值的`SubjectConfirmationData`宣告，以及與原始 SAML 要求識別碼相符的`InResponseTo`值。範例：

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces Web 驗證您的請求參數和 SAML 判斷提示。對於 IdP 起始的 SAML 宣告，請求的詳細資訊必須格式化為 HTTP POST 要求主體中的`RelayState`參數。要求主體也必須包含您的 SAML 判斷提示做為`SAMLResponse`參數。如果您遵循上一個步驟，這兩者都應該存在。

以下是 IdP 起始之 SAML 提供者的範例`POST`主體。

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

具體的指導 IdPs

若要確保您正確設定入口網站的 SAML 聯盟，請參閱下列連結以取得常用 IdPs的說明文件。

IdP	SAML 應用程式設定	使用者管理	IDP 啟動的身份驗證	請求簽署	判斷提示加密	單一登出
Okta	建立 SAML 應用程式整合	使用者管理	應用程式整合精靈 SAML 欄位參考	應用程式整合精靈 SAML 欄位參考	應用程式整合精靈 SAML 欄位參考	應用程式整合精靈 SAML 欄位參考
恩特拉	建立自己的應用程式	快速入門：建立並指派使用者帳戶	啟用企業應用程式的單一登入	SAML 要求簽名驗證	設定 Microsoft 中央 SAML 權杖加密	單一登出 SAML 通訊協定
Ping	新增 SAML 應用程式	使用者	啟用 IDP 起始的單一登入	PingOne 為企業配置	企業版是否 PingOne 支援加密？	單一登出

IdP	SAML 應用程式設定	使用者管理	IDP 啟動的身份驗證	請求簽署	判斷提示加密	單一登出
				身份驗證請求登錄		
一次登入	SAML 客製化連接器 (進階) (4266907)	OneLogin 手動新增使用者	SAML 客製化連接器 (進階) (4266907)	SAML 客製化連接器 (進階) (4266907)	SAML 客製化連接器 (進階) (4266907)	SAML 客製化連接器 (進階) (4266907)
IAM Identity Center	設定您自己的 SAML 2.0 應用程式	設定您自己的 SAML 2.0 應用程式	設定您自己的 SAML 2.0 應用程式	N/A	N/A	N/A

設定 IAM 身分中心身分驗證類型

對於 IAM 身分中心類型 (進階)，您可以將 IAM 身分中心與入口網站聯合。只有在下列情況適用於您時，才選取此選項：

- 您的 IAM 身分中心設定 AWS 區域 為 AWS 帳戶 與您的入口網站相同。
- 如果您使用 AWS Organizations的是管理帳戶。

在建立具有 IAM 身分中心驗證類型的入口網站之前，您必須將 IAM 身分中心設定為獨立提供者。如需詳細資訊，請參閱 IAM 身分識別中心中的一般工作入門。或者，您可以將 SAML 2.0 IdP 連線到身分識別中心。如需詳細資訊，請參閱 Connect 至外部身分識別提供者。否則，您將不會有任何使用者或群組可指派給您的 Web 入口網站。

如果您已在使用 IAM 身分中心，則可以選擇 IAM 身分中心做為提供者類型，然後按照以下步驟從 Web 入口網站新增、檢視或移除使用者或群組。

> **Note**
>
> 若要使用此身分驗證類型，您的 IAM 身分中心必須 AWS 帳戶 與 AWS 區域 您的入口 WorkSpaces 網站位於同一個位置。如果您的 IAM 身分中心位於單獨 AWS 區域， AWS 帳戶 或者請遵循標準身份驗證類型的說明進行操作。如需詳細資訊，請參閱 the section called “設定標準驗證類型”。

如果您使用的是 AWS Organizations，您只能使用管理帳戶建立與 IAM 身分中心整合的入口 WorkSpaces 網站。

使用 IAM Identity Center 來建立 Web 入口網站

1. 在步驟 4：設定身分識別提供者建立入口網站期間，請選擇AWS IAM Identity Center。
2. 選擇「繼續使用 IAM 身分中心」。
3. 在 [指派使用者和群組] 頁面上，選擇使用者和/或群組索引標籤。
4. 核取您要新增至入口網站的使用者或群組旁邊的方塊。
5. 建立入口網站之後，您關聯的使用者可以使用他們的 IAM 身分中心使用者名稱和密碼登入 WorkSpaces Web。

使用 IAM Identity Center 來管理 Web 入口網站

1. 建立入口網站之後，該入口網站會在 IAM 身分中心主控台中列為已設定的應用程式。
2. 若要存取此應用程式的組態設定，請在側邊欄中選擇應用程式，然後尋找名稱與 Web 入口網站顯示名稱相符的已設定應用程式。

> **Note**
>
> 如果您尚未輸入顯示名稱，則會改為顯示入口網站的 GUID。GUID 是您入口網站端點 URL 前置詞的 ID。

將其他使用者和群組新增至現有的 Web 入口網站

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces Web]、[入口網站]、選擇您的入口網站，然後選擇 [編輯]。
3. 選擇身分提供者設定和指派其他使用者和群組。從這裡，您可以將使用者和群組新增至您的 Web 入口網站。

> **Note**
>
> 您無法從 IAM Identity Center 主控台新增使用者或群組。您必須從 WorkSpaces Web 入口網站的編輯頁面執行此操作。

若要檢視或移除 Web 入口網站的使用者和群組

- 您可以使用「已指派的使用者」表格中的可用動作來檢視或移除使用者對此應用程式的存取權限。如需詳細資訊，請參閱管理應用程式的存取權。

> **Note**
>
> 您無法從 WorkSpaces WebPortal 的編輯頁面檢視或移除使用者和群組。您必須從 IAM Identity Center 主控台的編輯頁面執行這個操作。

變更身分識別提供者類型

請依照下列步驟隨時變更入口網站的驗證類型：

- 若要從 IAM 身分中心變更為標準，請遵循中的步驟the section called “設定標準驗證類型”。
- 若要從標準變更為 IAM 身分中心，請遵循中的步驟the section called “設定 IAM 身分中心身分驗證類型”。

身分識別提供者類型的變更最多可能需要 15 分鐘才能部署，而且不會自動終止進行中的工作階段。

您可以透 AWS CloudTrail 過檢查`UpdatePortal`事件來檢視入口網站的身分識別提供者類型變更。該類型在事件的請求和響應有效載荷中可見。

檢閱和啟動

1. 在步驟 5：檢閱和啟動頁面上，檢閱您為 Web 入口網站選取的設定。您可以選擇 編輯，以變更指定部分中的設定。您也可以稍後從主控台的 Web 入口網站標籤變更這些設定。
2. 完成時，請選擇啟動 Web 入口網站。
3. 若要檢視 Web 入口網站的狀態，請選擇 Web 入口網站，選擇您的入口網站，然後選擇檢視詳細資訊。

Web 入口網站有下列其中一個狀態：

- 未完成 – Web 入口網站的組態缺少必要的身分提供者設定。
- 擱置中 – Web 入口網站正在將變更套用至其設定。
- 作用中 – Web 入口網站已準備就緒且可供使用。

4. 請等待最多 15 分鐘，讓您的入口網站變為作用中狀態。

步驟 2：測試您的 Web 入口網站

建立入口網站之後，您可以登入 WorkSpaces Web 端點，以使用者的方式瀏覽連線的網站。

如果您已在 the section called “設定身分提供者” 中完成這些步驟，可跳過本部分並且前往 步驟 3：分發您的 Web 入口網站。

1. 開啟 WorkSpaces 網頁主控台，網址為 https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces Web]、[入口網站]、選擇您的入口網站，然後選擇 [檢視詳細資料
3. 在 Web 入口網站端點下，前往入口網站的指定 URL。Web 入口網站端點是您的使用者在使用針對入口網站設定的身分提供者登入後，啟動 Web 入口網站的存取點。它在網際網路上公開提供，且能夠嵌入到您的網路中。
4. 在 WorkSpaces 網頁登入頁面上，選擇 [登入]、[SAML]，然後輸入您的 SAML 認證。
5. 當您看到 [正在準備您的工作階段] 頁面時，表示您的 WorkSpaces Web 工作階段正在啟動。請勿關閉或離開此頁面。
6. 此時會啟動網頁瀏覽器，並顯示您的啟動 URL，以及透過瀏覽器政策設定所設定的任何其他行為。
7. 您現在可以選擇連結或在網址欄中輸入 URL，以瀏覽已連接的網站。

步驟 3：分發您的 Web 入口網站

當您準備好讓使用者開始使用 WorkSpaces Web 時，您可以從下列選項中選擇散發入口網站：

- 將入口網站新增至 SAML 應用程式閘道，讓使用者直接從其 IdP 啟動工作階段。例如，請參閱建立書籤應用程式整合。
- 將入口網站 URL 新增至您擁有的網站，然後使用瀏覽器重新導向，將使用者導向 Web 入口網站。

- 透過電子郵件傳送入口網站 URL 給您的使用者，或向下推送至您管理的裝置，當成瀏覽器首頁或書籤。

後續步驟

建立第一個 Web 入口網站後，您可以隨時檢視詳細資訊、編輯詳細資訊或刪除 Web 入口網站。如需詳細資訊，請參閱 管理您的 Web 入口網站。

您 AWS 帳戶 可以在每個可用 Web 的 AWS 區域 地方創建一個門戶 WorkSpaces 網站。每個 Web 入口網站可隨時支援多達 25 個使用者連線。若要增加可在區域中建立的入口網站數量，或為入口網站支援更多同時發生的工作階段，請參閱 the section called “請求增加服務配額”。

管理您的 Web 入口網站

設定好 Web 入口網站後，您可以檢視或編輯其詳細資訊，也可以刪除不再需要使用的入口網站。

主題

檢視 Web 入口網站詳細資訊

檢視 Web 入口網站詳細資訊

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces Web]、[入口網站]、選擇您的入口網站，然後選擇 [檢視詳細資料]。

編輯 Web 入口網站

若要編輯 Web 入口網站

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。

2. 選擇 [WorkSpaces Web]、[入口網站]、選擇您的入口網站，然後選擇 [編輯]。

> **Note**
>
> 變更網路設定或逾時設定，會立即結束任何作用中的入口網站工作階段。使用者中斷連線，必須重新連線才能開始新的工作階段。剪貼簿許可、檔案傳輸許可或列印至本機端裝置的變更，會從第一個新的工作階段開始套用。目前作用中的工作階段未中斷連線。連接到作用中工作階段的使用者，在中斷連線並連接到新的工作階段之前不會受到變更的影響。

刪除 Web 入口網站

刪除 Web 入口網站

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces Web]、[入口網站]、選擇您的入口網站，然後選擇 [刪除]。

請求增加服務配額

當您建立 AWS 帳戶時，我們會自動為服務的資源使用量設定預設服 AWS 務配額 (也稱為限制)。WorkSpaces Web 對兩種類型的資源設定配額-入口網站 (每個區域) 和最大同時工作階段 (每個入口網站)。 WorkSpaces Web 目前有下列服務配額限制：

AWS 區域 依帳戶內的預設配額	值
Web 入口網站	1
同時發生工作階段數量上限	25

入口網站是 Web 中的基本資源。 WorkSpaces 它是您的 SAML 2.0 身分提供者，以及您與網際網路和內容的網路連線之間的關聯。您可以在任何可用 Web 的 AWS 區域 地方建立入口 WorkSpaces 網站。請參閱區域資料表，以了解目前的可用性。

同時發生工作階段數量上限是指同時連線至指定 Web 入口網站的最高使用者數量。如果未正確設定最大並行工作階段的服務配額限制，使用者可能會發現其工作階段在登入 WorkSpaces Web 時無法使

用。您還應該確保 VPC 和子網路有足夠的 IP 空間來支援同時發生工作階段數量上限，否則使用者可能無法連線到工作階段。

例如，客戶在美國東部 (維吉尼亞北部) 有兩個 Web 入口網站和 125 個使用者。第一個 Web 入口網站 (入口網站 A) 有 25 個使用者，無需增加服務配額。第二個 Web 入口網站 (入口網站 B) 最多可供 100 位使用者使用。這些使用者分為兩班制，他們的工作時間並不重疊。因此，客戶會需要將入口網站 B 的服務配額提高到同時發生工作階段數量上限為 50 個使用者。

您可以請求提高其中一個服務配額限制。如需詳細資訊，請參閱請求增加配額。

請求增加服務配額

1. 開啟 AWS Support 儀表板。
2. 選擇服務限制提高。

> **Important**
>
> WorkSpaces Web 服務配額一次會影響一個區域。您必須在需要更多資源的每個 AWS 區域申請增加服務配額。如需詳細資訊，請參閱 AWS 服務端點。

3. 在使用案例說明底下輸入下列資訊：
   - 如果您請求增加 Web 入口網站的數量，請指定此資源類型，並且包含您的 AWS 帳戶 ID、要增加的區域及新的限制值。
   - 如果您請求增加同時發生工作階段數量上限，請指定此資源類型，並且包含您的 AWS 帳戶 ID、您想要增加的區域、Web 入口網站 ARN 及新的限制值。
4. (選用) 若要同時請求增加多個服務配額，請完成請求部分中的一個配額增加請求，然後選擇新增其他請求。

控制重新驗證 SAML IdP 權杖的間隔

當使用者造訪 WorkSpaces Web 入口網站時，他們可以登入以啟動串流工作階段。每個工作階段都會從開始頁面開始，除非他們在不到 5 分鐘前登入。入口網站會檢查身分提供者 (IdP) 權杖，以判斷是否在啟動工作階段時提示使用者輸入憑證。未持有有效 IdP 權杖的使用者必須輸入使用者名稱、密碼和選用的多重要素驗證 (MFA)，才能啟動串流工作階段。如果使用者已透過登入其 IdP 或受相同 IdP 保護的應用程式來產生 SAML IdP 權杖，則不會要求他們提供登入憑證。

如果使用者擁有有效的 SAML IdP 權杖，則他們可以存取網 WorkSpaces 頁。您可以控制重新驗證 SAML IdP 權杖所需的間隔。

控制重新驗證 SAML IdP 權杖的間隔

1. 使用您的 SAML IdP 提供者設定 IdP 逾時持續時間。我們建議以使用者完成其工作所需的最短時間來設定 IdP 逾時持續時間。

   - 如需關於 Okta 的詳細資訊，請參閱對所有政策強制執行有限的工作階段存留期。
   - 如需關於 Azure AD 的詳細資訊，請參閱設定驗證工作階段控制項。
   - 如需關於 Ping 的詳細資訊，請參閱工作階段。
   - 如需詳細資訊 AWS IAM Identity Center，請參閱設定工作階段持續時間。

2. 設定入口 WorkSpaces 網站的閒置和閒置逾時值。這些值可控制使用者上次互動與 WorkSpaces Web 工作階段因閒置而結束之間的時間長度。當工作階段結束時，使用者將失去其工作階段狀態 (包括開啟的分頁、未儲存的網頁內容和歷程記錄)，並在下一個工作階段開始時回到最新狀態。如需詳細資訊，請參閱 the section called “步驟 1：建立 Web 入口網站” 中的步驟 5。

   > **Note**
   >
   > 如果使用者的工作階段逾時，但使用者仍有有效的 SAML IdP 權杖，則不需要輸入其使用者名稱和密碼即可啟動新的 WorkSpaces Web 工作階段。請按照上一個步驟中的指南，以控制重新驗證權杖的方式。

設定使用者存取日誌記錄

您可以設定使用者存取日誌記錄，以記錄下列使用者事件：

- 工作階段開始-標記 WorkSpaces Web 工作階段的開始。
- 工作階段結束-標記 WorkSpaces Web 工作階段的結束。
- URL 導覽 – 記錄使用者載入的 URL。

> **Note**
>
> 從瀏覽器歷程記錄記錄 URL 導航日誌。未記錄在瀏覽器歷程記錄中的 URL (以無痕模式造訪或從瀏覽器歷程記錄中刪除) 不會記錄在日誌中。客戶可以決定是否使用瀏覽器政策關閉無痕模式或是刪除歷程記錄。

此外，每個事件還包括以下資訊：

- Event time (事件時間)
- 使用者名稱
- Web 入口網站 ARN

客戶有責任瞭解其使用 WorkSpaces Web 時所產生的潛在法律問題，並確保他們使用 WorkSpaces 網路時遵守所有適用的法律和法規。其中包括規範雇主監控員工使用 WorkSpaces 網路之能力的法律，包括在應用程式中執行的活動。

在 WorkSpaces Web 入口網站上啟用使用者存取日誌可能會產生 Amazon Kinesis Data Streams 的費用。如需定價的詳細資訊，請參閱 Amazon Kinesis Data Streams 定價。

若要在 WorkSpaces Web 主控台中啟用使用者存取記錄，請在使用者存取記錄下，選取您要用來接收資料的 Kinesis Stream ID。記錄的資料將直接傳送到該串流。

如需建立 Amazon Kinesis Data Stream 的詳細資訊，請參閱什麼是 Amazon Kinesis Data Streams？。

> **Note**
>
> 若要從 WorkSpaces 網路接收日誌，您必須擁有一個以「amazon-workspaces-web-*」開頭的 Amazon Kinesis 資料串流。您的 Amazon Kinesis 資料串流必須關閉伺服器端加密，或者必須用 AWS 受管金鑰 於伺服器端加密。
> 如需在 Amazon Kinesis 中設定伺服器端加密的詳細資訊，請參閱如何開始使用伺服器端加密？。

範例日誌

以下是每個可用事件的範例，包括驗證StartSessionVisitPage、、和EndSession。

每個事件都一定有以下欄位：

- timestamp，包含為 epoch 時間 (以毫秒為單位)。
- eventType，為字串。
- details，為另一個 json 物件。
- 除 Validation 外，每個事件都有 portalArn 和 userName。

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

設定或編輯瀏覽器政策

透過 WorkSpaces 網頁版，您可以使用適用於最新穩定版本的 Chrome 政策來設定自訂瀏覽器政策。您可以在 Web 入口網站套用 300 多項政策。如需詳細資訊，請參閱 the section called “設定自訂瀏覽器政策 (範例)” 和 Chrome Enterprise 政策清單。

使用主控台檢視畫面來建立 Web 入口網站，您可以套用以下政策：

- `StartURL`
- 書籤和書籤資料夾
- 開啟和關閉隱私瀏覽
- 刪除歷程記錄
- 使用 `AllowURL` 和 `BlockURL` 篩選 URL

如需有關使用主控台來檢視政策的資訊，請參閱 開始使用 Amazon WorkSpaces 網站。

WorkSpaces Web 會將基準瀏覽器原則組態套用至所有入口網站，以及您指定的任何原則。您可以使用自訂的 JSON 檔案編輯其中部分政策。如需詳細資訊，請參閱 the section called “編輯基準瀏覽器政策”。

主題

- 設定自訂瀏覽器政策 (範例)
- 編輯基準瀏覽器政策

設定自訂瀏覽器政策 (範例)

您可以上傳 JSON 檔案以設定任何支援用於 Linux 的 Chrome 政策。如要進一步了解 Chrome 政策，請參閱 Chrome Enterprise 政策清單，然後選取 Linux 平台。然後，搜尋並檢閱最新穩定版本的政策。

在下例中，您可以建立具有下列政策控制項目的 Web 入口網站：

- 設定書籤
- 設定預設啟動頁面
- 防止使用者安裝其他擴充功能
- 防止使用者刪除歷程記錄

- 防止使用者使用無痕模式
- 為所有工作階段預先安裝 Okta 外掛程式擴充功能。

主題

步驟 1：建立 Web 入口網站

若要上傳您的 Chrome 政策 JSON 檔案，您必須建立 WorkSpaces 網路入口網站。如需詳細資訊，請參閱 the section called “步驟 1：建立 Web 入口網站”。

步驟 2：收集政策

在 Chrome 政策中搜尋並找出您要使用的政策。然後，您可以在下一個步驟中使用政策來建立 JSON 檔案。

1. 前往 Chrome Enterprise 政策清單。
2. 選擇平台 Linux，然後選擇最新的 Chrome 版本。
3. 搜尋您要設定的政策。在此例中，搜尋擴充功能以尋找管理擴充功能的政策。每個政策都包含說明、Linux 偏好設定名稱和範例值。
4. 在搜尋結果中，如果一起使用，則有 3 個符合業務需求的政策：
   - ExtensionSettings – 在啟動瀏覽器時安裝擴充功能。
   - ExtensionInstallBlocklist – 防止安裝特定的擴充功能。
   - ExtensionInstallAllowlist— 允許安裝某些擴充功能。
5. 其他政策滿足其餘要求；
   - ManagedBookmarks— 將書籤新增至網頁。
   - RestoreOnStartupURL — 設定每當啟動新的瀏覽器視窗時，要開啟哪些網頁。
   - AllowDeletingBrowserHistory— 配置用戶是否可以刪除其瀏覽歷史記錄。
   - IncognitoModeAvailability— 配置用戶是否可以訪問隱身模式。

步驟 3：建立自訂的 JSON 政策檔案

使用文字編輯器、範本和您在先前步驟中找到的政策來建立 JSON 檔案。

1. 開啟文字編輯器。
2. 複製下列範本並貼至文字編輯器：

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
```

```
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

步驟 4：將政策加入範本

針對每個業務需求，將您的自訂政策加入範本。

1. 設定書籤 URL。
   a. 為您要加入的每個書籤在 `value` 金鑰下方加入成對的 `name` 和 `url` 金鑰。
   b. 將 `bookmark-url-1` 設定為 `https://www.amazon.com`。
   c. 將 `bookmark-url-2` 設定為 `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`。

```
    "ManagedBookmarks":
        {
```

```
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. 設定啟動 URL。此政策可讓系統管理員設定使用者啟動新瀏覽器視窗時要顯示的網頁。

   a. 將 RestoreOnStartup 設定為 4。這會設定開啟 URL 清單的 RestoreOnStartup 動作。您還可以在啟動 URL 上使用其他動作。如需詳細資訊，請參閱 Chrome Enterprise 政策清單。

   b. 設定 RestoreOnStartupURLs 為 https://www.aboutamazon.com/news。

```
    "RestoreOnStartup":
       {
           "value": 4
       },
   "RestoreOnStartupURLs":
       {
           "value":
           [
               "https://www.aboutamazon.com/news"
           ]
       },
```

3. 若要防止使用者刪除其瀏覽器歷程記錄，請將 AllowDeletingBrowserHistory 設定為 false。

```
    "AllowDeletingBrowserHistory":
       {
           "value": false
       },
```

4. 若要關閉使用者使用無痕模式的權限，請將設定 IncognitoModeAvailability 為 1。

```
"IncognitoModeAvailability":
   {
       "value": 1
   }
```

5. 使用下列政策設定及強制執行 Okta 外掛程式：

   - ExtensionSettings – 在啟動瀏覽器時安裝擴充功能。可從 Okta 外掛程式說明頁面取得擴充功能值。
   - ExtensionInstallBlocklist – 防止安裝特定的擴充功能。預設使用一個 * 值來防止所有擴充功能。管理員可以控制允許在 ExtensionInstallAllowlist 上使用哪些擴充功能。
   - ExtensionInstallAllowlist 允許您安裝某些擴充功能。由於將 ExtensionInstallBlocklist 設定為 *，請在此處加入 Okta 外掛程式值以允許使用它。

   以下顯示開啟 Okta 外掛程式的範例政策：

```
"ExtensionInstallBlocklist": {
    "value": [
        "*",
        ]
},
"ExtensionInstallAllowlist": {
    "value": [
        "glnpjglilkicbckjpbgcfkogebgllemb",
       ]
},
"ExtensionSettings": {
    "value": {
        "glnpjglilkicbckjpbgcfkogebgllemb": {
            "installation_mode": "force_installed",
            "update_url": "https://clients2.google.com/service/update2/crx",
            "toolbar_pin": "force_pinned"
    }
}
```

步驟 5：將您的政策 JSON 檔案上傳到您的 Web 入口網站

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces Web]，然後選擇 [入口網站]。
3. 選擇您的 Web 入口網站，然後選擇編輯。
4. 選擇 政策設定，然後選擇 JSON 檔案上傳。
5. 選擇選擇檔案。導覽至、選取並上傳您的 JSON 檔案。
6. 選擇儲存。

編輯基準瀏覽器政策

為了提供服務， WorkSpaces Web 會將基準瀏覽器原則套用至所有入口網站。除了您從主控台檢視畫面或 JSON 上傳指定的政策之外，還會套用此基準政策。以下是服務套用的 JSON 格式政策清單：

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
```

```
        }
    }
}
```

客戶無法變更下列政策：

- `DefaultDownloadDirectory` – 無法編輯此政策。此服務會覆寫此政策的任何變更。
- `DownloadDirectory` – 無法編輯此政策。此服務會覆寫此政策的任何變更。

客戶可以更新其 Web 入口網站的下列政策：

- `DownloadRestrictions` – 預設是設定成 1，防止 Chrome Safe Browsing 將下載內容辨識成惡意的內容。如需詳細資訊，請參閱防止使用者下載有害檔案。您可以將值從 0 設定成 4。
- 可以使用主控台檢視 URL 篩選功能或 JSON 上傳來擴充 `URLAllowlist` 和 `URLBlocklist` 政策。不過無法覆寫基準線 URL。從您的 Web 入口網站下載的 JSON 檔案中看不到這些政策。不過，如果您在工作階段期間有造訪過「chrome://policy」，遠端瀏覽器會顯示套用的政策。

設定輸入法編輯器 (IME)

終端使用者可以透過輸入法編輯器 (IME) 這項公用工具，選擇使用非 QWERTY 鍵盤的鍵盤配置來輸入語言文字。IME 可以協助使用者用更為龐大複雜的語言集 (例如，日文、中文和韓文) 來輸入文字。WorkSpaces Web 工作階段預設包括 IME 支援。使用者可以從工作階段的 IME 工具列或使用鍵盤快速鍵來選取其他語言。

WorkSpaces Web 的 IME 目前支援下列語言：

- 英文
- 簡體中文 (拼音)
- 繁體中文 (注音符號)
- 日文
- 韓文

請執行下列動作，以從 IME 工具列選取語言：

1. 選取黑色頂端面板列右側的語言選取器下拉清單。選擇器預設顯示英文的 en。
2. 在下拉選單中選擇要使用的語言。

3. 在選擇語言後出現的子選單中，選擇其他語言詳細資訊。

請使用下列鍵盤快速鍵來選取語言：

- 所有 IME
  - 若要向前循環 IME (或向右移動鍵盤配置)，請按 Shift+Control+Left Alt。
- 日文
  - 要選擇平假名，請按 F6。
  - 要選擇片假名，請按 F7。
  - 若要選擇 Latin，請按 F10。
  - 若要選擇 Wide Latin，請按 F9。
  - 要選擇直接輸入，請按 ALT +、ALT + @、全寬半寬。
- 韓文
  - 若要選擇韓文，請按 Shift+Space。
  - 若要選擇漢字，請按 F9。

若要移除 IME 工具列和功能表，或從 WorkSpaces Web 工作階段關閉螢幕鍵盤，請連絡 AWS Support。

設定工作階段內本地化

當使用者啟動工作階段時， WorkSpaces Web 會偵測使用者的本機瀏覽器語言和時區設定，並將其套用至工作階段。這會影響工作階段期間的顯示語言，且有助於確保顯示的時間符合使用者所在位置的當前時間。

下列清單顯示 WorkSpaces Web 目前支援的語言代碼。如果使用者的本機端瀏覽器設定為使用未支援的語言代碼，工作階段會預設為英文 (en-US)。

- 德文
  - de – 德文
  - de-AT – 德文 (奧地利)
  - de-DE – 德文 (德國)
  - de-CH – 德文 (瑞士)
  - de-LI – 德文 (列支敦士登)

- 英文
  - en – 英文
  - en-AU – 英文 (澳洲)
  - en-CA – 英文 (加拿大)
  - en-IN – 英文 (印度)
  - en-NZ – 英文 (紐西蘭)
  - en-ZA – 英文 (非洲南部)
  - en-GB – 英文 (英國)
  - en-US – 英文 (美國)
- 西班牙文
  - es – 西班牙文
  - es-AR – 西班牙文 (阿根廷)
  - es-CL – 西班牙文 (智利)
  - es-CO – 西班牙文 (哥倫比亞)
  - es-CR – 西班牙文 (哥斯大黎加)
  - es-HN – 西班牙文 (洪都拉斯)
  - es-419 – 西班牙文 (拉丁美洲)
  - es-MX – 西班牙文 (墨西哥)
  - es-PE – 西班牙文 (秘魯)
  - es-ES – 西班牙文 (西班牙)
  - es-US – 西班牙文 (美國)
  - es-UY – 西班牙文 (烏拉圭)
  - es-VE – 西班牙文 (委內瑞拉)
- 法文
  - fr – 法文
  - fr-CA – 法文 (加拿大)
  - fr-FR – 法文 (法國)
  - fr-CH – 法文 (瑞士)
- 印尼文
  - id – 印尼文

  - id-ID – 印尼文 (印尼)
- 義大利文
  - it – 義大利文
  - it-IT – 義大利文 (義大利)
  - it-CH – 義大利文 (瑞士)
- 日文
  - ja – 日文
  - ja-JP – 日文 (日本)
- 韓文
  - ko – 韓文
  - ko-KR – 韓文 (韓國)
- 葡萄牙文
  - pt – 葡萄牙文
  - pt-BR – 葡萄牙文 (巴西)
  - pt-PT – 葡萄牙文 (葡萄牙)
- Chinese
  - zh – 中文
  - zh-CN – 中文 (中國)
  - zh-HK – 中文 (香港)
  - zh-TW – 中文 (台灣)

按以下優先順序確定工作階段語言：

1. 入口網站瀏覽器設定中的ForcedLanguages原則。如需詳細資訊，請參閱ForcedLanguages。
2. 終端使用者的本機端瀏覽器語言設定。
3. 預設值為 English (en-US)。

由終端使用者瀏覽器中指定的本地時區設定來確定時區。如果時區設定無效，會使用 UTC。

WorkSpaces Web 支援當地語系化中的下列元件：

- WorkSpaces 網頁登入頁面

- WorkSpaces 入口網站狀態訊息 (包括載入訊息和錯誤)
- Chrome 瀏覽器
- 系統內容選單和另存為視窗

若要設定使用者的本機端瀏覽器設定，請執行下列其中一項操作：

- 在 Chrome 中，選擇設定，選擇語言，然後根據喜好設定語言順序。
- 在 Firefox 中，選擇設定、一般、語言，然後從下拉選單選擇語言。
- 在 Edge 中，選擇設定、選擇語言，然後根據喜好設定語言順序。

設定 IP 存取控制 (選用)

WorkSpaces Web 允許您控制您的門戶網站可以從哪些 IP 地址訪問。使用 IP 存取設定可以定義和管理受信任 IP 地址的群組，並且只允許使用者在連線至受信任網路時存取其入口網站。

根據預設， WorkSpaces Web 允許使用者從任何地方存取其入口網站。IP 存取控制群組充當虛擬防火牆，篩選使用者可用來連線至 Web 入口網站的 IP 地址。當與您的 Web 入口網站建立關聯時，IP 存取設定會在驗證前偵測使用者 IP，以判斷它們是否有資格進行連線。一旦連線， WorkSpaces Web 會持續監控使用者的 IP 位址，以確保它們從受信任的網路保持連線。如果使用者的 IP 變更， WorkSpaces Web 會偵測並終止工作階段。

若要指定 CIDR 地址範圍，請將規則加入 IP 存取控制群組，然後將群組與您的 Web 入口網站建立關聯。您可以將每個 IP 存取設定與一或多個 Web 入口網站建立關聯。若要指定受信任網路的公用 IP 地址和 IP 地址範圍，請將規則加入您的 IP 存取控制群組。如果您的使用者透過 NAT 閘道或 VPN 存取其 Web 入口網站，您必須建立規則，以允許來自 NAT 閘道或 VPN 的公用 IP 地址流量。

> **Note**
>
> 客戶有責任瞭解其使用 WorkSpaces Web 時所產生的潛在法律問題，並且必須確保他們使用 WorkSpaces 網路時符合所有適用的法律和法規。這包括規範雇主監控員工使用 WorkSpaces 網路之能力的法律，包括在應用程式中執行的活動。

建立 IP 存取控制群組

請按照下列步驟來建立 IP 存取控制群組。

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 IP 存取控制。
3. 選擇建立 IP 存取控制群組。
4. 在建立 IP 存取控制群組對話方塊中，輸入群組名稱 (必要) 和描述 (選用)。
5. 輸入將與來源建立關聯的 IP 地址或 CIDR IP 範圍，以及說明 (選用)。
6. 在標籤底下，選擇是否為每個 IP 存取控制群組標記金鑰值配對。
7. 新增規則和標籤完成後，選擇儲存。

將 IP 存取設定與 Web 入口網站建立關聯

若要建立 IP 存取控制群組與現有 Web 入口網站的關聯，請依照下列步驟執行。

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 Web 入口網站。
3. 選取 Web 入口網站，然後選擇編輯。
4. 在 IP 存取控制群組底下，選取 Web 入口網站的 IP 存取控制群組。
5. 選擇儲存。

請依照下列步驟，以便在建立新的 Web 入口網站時建立 IP 存取控制群組的關聯。

1. 完成 the section called “進行入口網站設定” 中的步驟 1 到 4，以存取 IP 存取控制 (選用)。
2. 選擇建立 IP 存取控制。
3. 在建立 IP 群組對話方塊中，輸入群組名稱 (必要) 和描述 (選用)。
4. 輸入將與來源建立關聯的 IP 地址或 CIDR IP 範圍，以及說明 (選用)。
5. 在標籤底下，選擇是否為每個 IP 存取控制群組標記金鑰值配對。
6. 新增規則和標籤完成後，選擇建立 IP 存取控制。
7. 啟動時您的 IP 存取控制群組將與此 Web 入口網站建立關聯。

編輯 IP 存取控制群組

您可以隨時刪除 IP 存取設定中的規則。如果您刪除用來允許連線至 Web 入口網站的規則，任何具有目前工作階段的使用者都會與 Web 入口網站中斷連線。

請按照下列步驟編輯 IP 存取控制群組。

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 IP 存取控制。
3. 選取群組與選擇編輯。
4. 編輯現有規則的來源和說明 (選用)，或加入其他規則。
5. 在標籤底下，選擇是否為每個 IP 存取控制群組標記金鑰值配對。
6. 新增規則和標籤完成後，選擇儲存。
7. 如果您已更新現有的 IP 存取設定，請等待最多 15 分鐘，讓新規則或編輯過的規則生效。

刪除 IP 存取控制群組

您可以隨時刪除 IP 存取控制群組中的規則。如果您刪除用來允許連線至 Web 入口網站的規則，任何具有目前工作階段的使用者都會與 Web 入口網站中斷連線。

請按照下列步驟以刪除 IP 存取控制群組。

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 IP 存取控制群組。
3. 選取群組並選擇刪除。

啟用單一登入擴充功能 (選用)

您可以為終端使用者啟用擴充功能，以獲得更好的入口網站登入體驗。例如，如果您使用 Okta 當成入口網站的 SAML 2.0 身分提供者 (IdP)，並且也將它當成您希望使用者在工作階段期間造訪之網站的 IdP，則可以將 Okta 登入 cookie 傳給具有擴充功能的工作階段。之後使用者造訪需要 Okta 網域 cookie 的網站時，他們無需在工作連線期間登入，便能存取該網站。

Chrome 和 Firefox 瀏覽器支援擴充功能。擴充功能會針對從使用者登入到工作階段所允許的網域啟用 cookie 同步處理。擴充功能無需使用者登入，會在幕後運作以啟用 cookie 同步處理，使用者不用在安裝後採取任何動作。擴充功能不會儲存任何資料。

用戶可以從 Chrome 網上商店將擴展程序添加到其 Chrome 瀏覽器中，也可以從附加組件將擴展程序添加到其 FireFox 瀏覽器中 FireFox。

在 InCognito 視窗中的 Chrome 中未啟用擴充功能。Firefox 有可在隱私瀏覽期間使用擴充功能的設定。如需詳細資訊，請參閱隱私瀏覽中的擴充功能。

您可以更新入口網站現有的使用者設定組態，或是在第一次建立 Web 入口網站時更新。先確定您的 SAML IdP 和網站需要哪些網域。您最多可以加入 10 個網域。

您有責任測試和識別要同步的 Cookie 的適當網域。可能要在 IdP 或網站驗證層級進行變更，以確保單一登入如預期般運作。

若要查看哪些網域搭配最常見的 IdP 使用，請參閱下表：

IdP 和網域

IdP	網域
Okta	okta.com
蔚藍廣告	microsoftonline.com
AWS 身分中心	awsapps.com
一次登入	onelogin.com
Duo	duosecurity.com

接下來，請造訪主控台中的 Web 入口網站。然後允許擴充功能，並加入應同步哪些網域的 cookie。請依照下列步驟建立允許使用擴充功能的新入口網站，或是更新現有入口網站。

若要在建立新的 Web 入口網站時允許擴充功能，請依照下列步驟執行：

1. 請按照 the section called “步驟 1：建立 Web 入口網站” 中的步驟操作，直到到達 the section called “進行使用者設定” 為止。
2. 針對 the section called “進行使用者設定” 的步驟 1，在使用者許可底下選擇允許，以啟用 Web 入口網站的擴充功能。

3. 輸入 cookie 同步的網域，然後選擇新增網域。
4. 完成 the section called “進行使用者設定” 中的步驟和 the section called “步驟 1：建立 Web 入口網站” 的其餘部分，以建立您的 Web 入口網站。

請依照下列步驟執行，以將擴充功能加入現有的 Web 入口網站：

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選取要編輯的 Web 入口網站。
3. 選擇使用者設定、使用者許可和允許，以啟用 Web 入口網站的擴充功能。
4. 輸入 cookie 同步的網域，選擇新增網域。
5. 儲存入口網站變更內容。入口網站會在 15 分鐘內提示使用者安裝擴充功能。

請依照下列步驟編輯網域或移除擴充功能：

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選取要編輯的 Web 入口網站。
3. 選擇使用者設定、使用者許可和不允許以移除 Web 入口網站的擴充功能。
4. 移除或編輯個別網域。
5. 移除之後，工作階段將不再同步 Cookie，即使使用者在瀏覽器中安裝了 WorkSpaces Web 延伸功能也一樣。

如需有關擴充功能使用者體驗的詳細資訊，請參閱 the section called “單一登入擴充功能”。

設定網址過濾

您可以使用 Chrome 政策來篩選使用者可從遠端瀏覽器存取哪些網址。Chrome 政策提供了兩種過濾網址的機制：URL 允許列表和網址阻止列表。您可以使用 WorkSpaces Web 主控台介面將 URL 篩選設定為入口網站設定，或將其新增為自訂 JSON 陳述式的一部分 (無論是在內嵌編輯器中，或作為 JSON 檔案上傳)。

使用主控台設定 URL 篩選

1. 開啟 WorkSpaces Web 主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces Web]、[入口網站]、選擇您的入口網站，然後選擇 [檢視詳細資料]。
3. 對於 URL 篩選，請從下列選項中選擇：

   - 允許存取所有 URL：預設情況下，入口網站允許存取所有 URL。您可以將特定網站新增至 BlockURL 清單，以防止使用者在工作階段期間造訪這些網站。例如，將 www.anycorp.com 添加到塊 URL 列表將阻止用戶在其會話期間導航到 www.anycorp.com。
   - 封鎖對所有 URL 的存取：根據預設，入口網站會封鎖對所有 URL 的存取。您可以將特定網站新增至 URL 允許清單，以組織使用者可以造訪的網站清單，並封鎖任何其他網站的流量。請考慮將每個 URL 新增為書籤，以便在使用者工作階段期間啟用一鍵式存取。
   - 進階設定：選擇此選項可 parallel 時建立 AllowURL 和區塊 URL 清單。URL 允許清單的優先順序高於 URL 封鎖清單。此選項會依路徑啟用 URL 篩選。例如，您可以將 www.anycorp.com 新增至封鎖清單，然後將網站新增至允許清單。這允許用戶訪問我們的網址，但是他們將無法訪問其他網址路徑，例如網址。

如需有關使用封鎖和允許 URL 的詳細指引，請參閱允許或封鎖存取網站。按照 Chrome 的阻止列表過濾器格式將網址添加到這些列表中，以獲得最佳結果。如需詳細資訊，請參閱 URL 封鎖清單篩選格式。

使用 JSON 編輯器或檔案上傳設定 URL 篩選

1. 在 [原則設定] 模組中，選擇 [JSON 編輯器]，並略過 [編輯器] 或 [檔案上傳] 檢視的主控台 UI 模組。

   - 編輯器可讓客戶在主控台內嵌建立自訂政策陳述式。編輯器在策略創建期間突出顯示 JSON 語句中的錯誤。
   - 檔案上傳功能可讓客戶新增在主控台外建立的 JSON 檔案 (例如從現有的 Chrome 瀏覽器匯出)。
2. 請參閱 Chrome 政策詳細資料，瞭解 URL 允許清單和 URL 封鎖清單，以正確格式化入口網站的允許/拒絕 URL 清單。如需詳細資訊，請參閱 URL 允許清單和 URL 封鎖清單。

Amazon WorkSpaces Web 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。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：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。若要了解適用於 Amazon WorkSpaces Web 的合規計畫，請參閱合規計畫的 AWS 服務範圍。
- 雲端內部的安全：您的責任取決於所使用的 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於您資料的法律和法規。

本文件有助於您了解如何在使用 Amazon WorkSpaces Web 時套用共享責任模型。它會示範如何設定 Amazon WorkSpaces Web 以符合您的安全性和合規目標。您也將了解如何使用其他 AWS 服務，幫助您監控並保護 Amazon WorkSpaces Web 資源。

目錄

Amazon WorkSpaces 網絡中的數據保護

AWS共同責任模型適用於 Amazon WorkSpaces Web 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，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，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個人使用者。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 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 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 AWS 時，需要 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 Name (名稱) 欄位。這包括當您使用主控台、API 或 AWS SDK AWS 服務 使用 WorkSpaces Web 或其他工作時。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。

資料加密

Amazon WorkSpaces Web 會收集入口網站自訂資料，例如瀏覽器設定、使用者設定、網路設定、身分提供者資訊、信任存放區資料和信任存放區憑證資料。 WorkSpaces Web 也會收集瀏覽器原則資料、使用者偏好設定 (針對瀏覽器設定) 和工作階段記錄。收集到的資料會存放在 Amazon DynamoDB 和 Amazon S3 中。 WorkSpaces 網絡用AWS Key Management Service於加密。

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 WorkSpaces Web 動作的特定角色。使用 IAM 範本建立完整存取角色或唯讀角色。如需詳細資訊，請參閱 AWS WorkSpaces Web 的受管政策。
- 透過提供客戶管理的金鑰來保護端對端資料，讓 WorkSpaces Web 可以使用您提供的金鑰加密靜態資料。
- 請謹慎共享入口網域和使用者憑證：
  - 管理員必須登入 Amazon WorkSpaces 主控台，且使用者必須登入入口 WorkSpaces 網站。
  - 網際網路上的任何人都可以存取 Web 入口網站，但除非擁有入口網站的有效使用者憑證，否則他們無法啟動工作階段。

- 使用者可以選擇結束工作階段，明確結束工作階段。這會捨棄託管瀏覽器工作階段的執行個體，造成瀏覽器隔離。

WorkSpaces Web 默認情況下通過加密所有敏感數據來保護內容和元數據。AWS KMS它會收集瀏覽器原則和使用者偏好設定，以在 WorkSpaces Web 工作階段期間強制執行原則 如果在套用現有設定時發生錯誤，使用者將無法存取新的工作階段，也無法存取公司的內部網站和 SaaS 應用程式。

靜態加密

預設為靜態加密。 WorkSpaces Web 中使用的客戶特定數據使用AWS KMS加密。 WorkSpaces Web 為您建立的資源提供靜態加密。此服務會在建立資源時接受 AWS KMS 客戶自管金鑰，如果未提供，則會使用 AWS 擁有的金鑰來加密靜態資源。此服務會加密您可以提供的瀏覽器政策文件，以自訂瀏覽器工作階段、身分提供者組態設定，以及入口網站的顯示名稱。這些資訊將使用客戶自管金鑰或 AWS 擁有的金鑰保持加密，同時儲存在我們的後端。

您可以決定建立 WorkSpaces Web 資源時要使用哪個金鑰。如果屬於該資源一部分的資料已加密， WorkSpaces Web 會接受該`customerManagedKeyArn`欄位做為 `create` API 的一部分。提供的金鑰必須是對稱 AWS KMS 金鑰，而使用此金鑰建立資源的管理員必須具有 `kms:Decrypt`、`kms:GenerateDataKey` 和 `kms:CreateGrant` 許可。使用金鑰建立資源之後，即無法移除或變更金鑰。如果您使用客戶自管金鑰，則存取資源的管理員必須具有 `kms:Decrypt` 和 `kms:GenerateDataKey` 許可。如果您在使用主控台時看到有關拒絕存取的錯誤訊息，請確定使用主控台的使用者具有所使用之金鑰的這些許可。

您可以檢查 AWS KMS 授權狀態來排解問題及稽核金鑰使用情況。如需詳細資訊，請參閱在管理授權。在入口網站建立期間， WorkSpaces Web 會建立授權，以允許服務以非同步方式存取金鑰。您可以檢查授權與使用授權時提供的加密內容來檢查金鑰使用狀態。加密內容一律包含有金鑰 `aws:workspaces-web:portal:id` 的項目，以及等於入口網站 ID 的值。對於其他資源，加密內容永遠包含格式 `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` 的項目和對應的資源 ID。

傳輸中加密

WorkSpaces 網頁會透過 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 呼叫傳送要求至 WorkSpaces 。傳輸的要求資料會透過 HTTPS 或 TLS 連線傳送所有資料來進行加密。請求數據可以從AWS控制AWS Command Line Interface台或 AWS SDK 傳輸到 WorkSpaces Web。

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自管 AWS KMS 金鑰來對客戶資訊進行加密。如果您沒有提供， WorkSpaces Web 將使用AWS擁有的金鑰。您可以使用 AWS SDK 設置金鑰。

網際網路流量隱私權

若要保護 WorkSpaces Web 和內部部署應用程式之間的連線，您可以使用 WorkSpaces Web 在自己的 VPC 內啟動瀏覽器工作階段。與內部部署應用程式的連線是在您自己的 VPC 中設定的，不受 WorkSpaces Web 控制。

為了保護帳戶之間的連線安全， WorkSpaces Web 會使用服務連結角色安全地連線至客戶帳戶，並代表客戶執行作業。如需詳細資訊，請參閱 使用 WorkSpaces Web 的服務連結角色。

使用者存取日誌記錄

系統管理員可以記錄 WorkSpaces Web 工作階段事件，包括開始、停止和 URL 造訪。這些日誌經過加密，並且透過 Amazon Kinesis Data Stream 安全交給客戶。不會由 AWS 儲存使用者存取日誌記錄中的瀏覽資訊，也不會在未設定日誌的工作階段中取得。在無痕模式下訪問 URL，或從瀏覽器歷程記錄中刪除的 URL，不會記錄在使用者存取日誌記錄中。

Amazon WorkSpaces 網路的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權。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 Web 資源。IAM 是一種您可以免費使用的 AWS 服務。

主題

物件

根據您在 WorkSpaces Web 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 Web 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 WorkSpaces Web 功能來完成工作時，您可能需要其他權限。瞭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。如果您無法在 WorkSpaces Web 中存取功能，請參閱疑難排解 Amazon WorkSpaces 網路身分和存取。

服務管理員 — 如果您負責公司的 WorkSpaces Web 資源，您可能擁有完整的 WorkSpaces Web 存取權。判斷服務使用者應存取哪些 WorkSpaces Web 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。若要進一步了解貴公司如何將 IAM 與 WorkSpaces Web 搭配使用，請參閱Amazon WorkSpaces 網絡如何與 IAM 一起工作。

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 Web 存取權的詳細資訊。若要檢視可在 IAM 中使用的 WorkSpaces Web 身分型政策範例，請參閱。Amazon 網站的基於身份的政策示例 WorkSpaces

使用身分驗證

身分驗證是使用身分憑證登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證 (登入至 AWS)。

您可以使用透過身分來源 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證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。您 AWS 藉由使用聯合進行存取時，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。如需有關登入至 AWS 的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

如果您是以程式設計的方式存取 AWS，AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。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) 以提高帳戶的安全。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》中的在 AWS 中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。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

最佳實務是要求人類使用者 (包括需要管理員存取權的使用者)搭配身分提供者使用聯合功能，使用暫時憑證來存取 AWS 服務。

聯合身分是來自您企業使用者目錄的使用者、Web 身分供應商、AWS Directory Service、Identity Center 目錄或透過身分來源提供的憑證來存取 AWS 服務 的任何使用者。聯合身分存取 AWS 帳戶時，會擔任角色，並由角色提供暫時憑證。

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來源中的一組使用者和群組，以便在您的所有 AWS 帳戶和應用程式中使用。如需 IAM Identity Center 的相關資訊，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 AWS 帳戶 中的一種身分，具備單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，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。您無法以群組身分登入。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過程變得更為容易。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。如需進一步了解，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 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。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 — 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，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html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。
- 跨帳户存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色作為代理)。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 角色與資源類型政策的差異。
- 跨服務存取 – 有些 AWS 服務 會使用其他 AWS 服務 中的功能。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。
  - 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。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之後，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給 AWS 服務 服務。

- 服務連結角色 – 服務連結角色是一種連結到 AWS 服務 的服務角色類型。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 AWS 帳戶 中，並由該服務所擁有。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 – 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到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暫時憑證。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。

如需了解是否要使用 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

您可以透過建立政策並將其附加到 AWS 身分或資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和身分或資源建立關聯時，便可定義其許可。AWS 會在主體 (使用者、根使用者或角色工作階段) 發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式儲存在 AWS 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。若要授與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。具備該政策的使用者便可以從 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。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。受管政策則是獨立的政策，您可以將這些政策附加到 AWS 帳戶 中的多個使用者、群組和角色。受管政

策包含 AWS 管理政策和客戶管理政策。如需瞭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。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。主體可以包括帳戶、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。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 Simple Storage Service (Amazon S3)、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。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 支援其他較少見的政策類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。如需許可範圍的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可範圍。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 AWS 帳戶。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 AWS 帳戶根使用者。如需組織和 SCP 的更多相關資訊，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。如需更多資訊，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。如需瞭解 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱 IAM 使用者指南中的政策評估邏輯。

Amazon WorkSpaces 網絡如何與 IAM 一起工作

在您使用 IAM 管理 WorkSpaces Web 存取之前，請先了解哪些 IAM 功能可用於 WorkSpaces Web。

您可以搭配 Amazon WorkSpaces 網路使用的 IAM 功能

IAM 功能	WorkSpaces 網路支援
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)	部分
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要深入瞭解 WorkSpaces Web 和其他AWS服務如何搭配大多數 IAM 功能運作，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS服務。

Web 的以身分識別為基礎的原則 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。若要瞭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，因為這會套用至附加的使用者或角色。如要瞭解您在 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。

Web 的身分識別原則範例 WorkSpaces

若要檢視 WorkSpaces Web 身分型原則的範例，請參閱。Amazon 網站的基於身份的政策示例 WorkSpaces

Web 中 WorkSpaces 以資源為基礎的政策

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。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。主體可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

若要啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，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。當主體和資源在不同的 AWS 帳戶 中時，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) 存取資源的許可。其透過將身分型政策附加到實體來授予許可。不過，如果資源型政策會為相同帳戶中的主體授與存取，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。

Web 的政策 WorkSpaces 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。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

若要查看 WorkSpaces Web 動作清單，請參閱服務授權參考中由 Amazon WorkSpaces Web 定義的動作。

WorkSpaces Web 中的原則動作會在動作之前使用下列前置詞：

```
workspaces-web
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

若要檢視 WorkSpaces Web 身分型原則的範例，請參閱。Amazon 網站的基於身份的政策示例 WorkSpaces

Web 的政策 WorkSpaces 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 (例如列出作業)，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 Web 資源類型及其 ARN 的清單，請參閱服務授權參考中由 Amazon WorkSpaces Web 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 網路定義的動作。

若要檢視 WorkSpaces Web 身分型原則的範例，請參閱。Amazon 網站的基於身份的政策示例 WorkSpaces

WorkSpaces Web 的政策條件金鑰

支援服務特定政策條件索引鍵	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。若您為單一條件索引鍵指定多個值，AWS 會使用邏輯 OR 操作評估條件。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與該 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 支援全域條件索引鍵和服務特定的條件索引鍵。若要查看 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 Web 條件金鑰清單，請參閱服務授權參考中的 Amazon WorkSpaces Web 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 Web 定義的動作。

若要檢視 WorkSpaces Web 身分型原則的範例，請參閱。Amazon 網站的基於身份的政策示例 WorkSpaces

網頁版中 WorkSpaces 的存取控制清單 (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。

基於屬性的訪問控制（ABAC）與 Web WorkSpaces

支援 ABAC (政策中的標籤)	部分

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 AWS 中，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)，以及許多 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索引鍵，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索引鍵，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)。

透過 WorkSpaces Web 使用臨時登入資料

支援臨時憑證	是

您使用臨時憑證進行登入時，某些 AWS 服務 無法運作。如需詳細資訊，包括那些 AWS 服務 搭配臨時憑證運作，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

如果您使用使用者名稱和密碼之外的任何方法登入 AWS Management Console，則您正在使用臨時憑證。例如，當您使用公司的單一登入(SSO)連結存取 AWS 時，該程序會自動建立臨時憑證。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)。

您可使用 AWS CLI 或 AWS API，手動建立臨時憑證。接著，您可以使用這些臨時憑證來存取 AWS。AWS 建議您動態產生臨時憑證，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Web 的 WorkSpaces 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 AWS 中執行動作時，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 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。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之後，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 Web 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 Web 的功能。只有在 WorkSpaces Web 提供指引時才編輯服務角色。

Web 的 WorkSpaces 服務連結角色

支援服務連結角色	是

服務連結角色是一種連結到 AWS 服務 的服務角色類型。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 AWS 帳戶 中，並由該服務所擁有。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 網站的基於身份的政策示例 WorkSpaces

根據預設，使用者和角色沒有建立或修改 WorkSpaces Web 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 執行任務。若要授與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。

有關 WorkSpaces Web 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 Web 動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 WorkSpaces Web 主控台
- 允許使用者檢視他們自己的許可

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 Web 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 受管政策並朝向最低權限許可的目標邁進：如需開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。您也可以使用條件來授予對服務動作的存取權，前提是透過特定AWS 服務 (例如 AWS CloudFormation)使用條件。如需更多資訊，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。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多重要素驗證 (MFA)：如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 最佳安全實務。

使用 WorkSpaces Web 主控台

若要存取 Amazon WorkSpaces Web 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許其最基本主控台許可。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。

為確保使用者和角色仍可使用 WorkSpaces Web 主控台，請同時將 WorkSpaces Web `ConsoleAccess` 或`ReadOnly`AWS受管理的策略附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

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上，或是使用 AWS CLI 或 AWS API 透過編寫程式的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": "*"
        }
    ]
}
```

AWS WorkSpaces Web 的受管政策

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自己撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中可用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 服務會維護和更新 AWS 受管政策。您無法更改 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外，AWS 支援跨越多項服務之任務職能的受管政策。例如，ReadOnlyAccess AWS 受管政策提供針對所有 AWS 服務和資源的唯讀存取權限。當服務啟動新功能時，AWS 會為新的操作和資源新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的 AWS 受管政策。

AWS 受管政策：AmazonWorkSpacesWebServiceRolePolicy

您無法將 AmazonWorkSpacesWebServiceRolePolicy 政策附加至 IAM 實體。此政策會連接到服務連結角色，而此角色可讓 WorkSpaces Web 代表您執行動作。如需更多詳細資訊，請參閱 the section called “使用服務連結角色”。

此政策授予管理許可，允許存取 Amazon WorkSpaces Web 使用或管理的 AWS 服務和資源。

許可詳細資訊

此政策包含以下許可：

- WorkSpaces Web – 允許存取 Amazon WorkSpaces Web 使用或管理的 AWS 服務和資源。
- ec2 – 允許主體描述 VPC、子網路和可用區域；建立、標記、描述和刪除網路介面；關聯或取消關聯位址；以及描述路由表、安全群組和 VPC 端點。
- CloudWatch – 允許主體放置量度資料。
- Kinesis-允許主體描述 Kinesis 資料串流的摘要，並將紀錄放入 Kinesis 資料串流中以供使用者存取日誌記錄。如需更多詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
```

```
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

AWS 受管政策：AmazonWorkSpacesWebReadOnly

您可將 AmazonWorkSpacesWebReadOnly 政策連接到 IAM 身分。

此政策會授與唯讀許可，允許透過 AWS 管理主控台、SDK 和 CLI 存取 WorkSpaces Web 及其相依性。此政策不包括使用 IAM_Identity_Center 當成驗證類型與入口網站進行互動所需的許可。若要取得這些許可，請將此政策加上 AWSSSOReadOnly。

許可詳細資訊

此政策包含以下許可。

- WorkSpaces Web – 透過 AWS 管理主控台、SDK 和 CLI，提供對 Amazon WorkSpaces Web 及其相依性的唯讀存取。
- ec2：允許主體描述 VPC、子網路與安全群組。這會在 WorkSpaces Web 的 AWS 管理主控台中使用，以顯示可與服務搭配使用的 VPC、子網路和安全群組。
- Kinesis – 允許主體取得 Kinesis 資料串流的清單。這會在 WorkSpaces Web 的 AWS 管理主控台中使用，以顯示可與服務搭配使用的 Kinesis 資料串流。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
```

```
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces Web 對 AWS 受管政策的更新

檢視自此服務開始追蹤 WorkSpaces Web AWS 受管政策變更以來的更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

變更	描述	日期
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces Web 更新了政策，限制 CreateNetworkInterface 使用 aws:RequestTag/WorkSpacesWebManaged: true 標記，並且作用於子網路和安全群組資源，同時限制 DeleteNetworkInterface 使用 aws:ResourceTag/Wo	2022 年 12 月 15 日

變更	描述	日期
	rkSpacesWebManaged: true 標記的 ENI。	
AmazonWorkSpacesWebReadOnly – 更新的政策	WorkSpaces Web 已更新政策，以納入使用者存取日誌記錄的讀取許可，並且列出 Kinesis 資料串流。如需更多詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。	2022 年 11 月 2 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces Web 已更新政策，以說明 Kinesis 資料串流的摘要，並且將紀錄放入 Kinesis 資料串流中以供使用者存取日誌記錄。如需更多詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。	2022 年 10 月 17 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces Web 更新了政策以在建立 ENI 期間建立標籤。	2022 年 9 月 6 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces Web 已更新政策，將 AWS/Usage 命名空間新增至介面 PutMetricData API 許可。	2022 年 4 月 6 日
AmazonWorkSpacesWebReadOnly – 新政策	WorkSpaces Web 新增了一項新政策，透過 AWS 管理主控台、SDK 和 CLI 提供 Amazon WorkSpaces Web 及其相依性的唯讀存取權。	2021 年 11 月 30 日

變更	描述	日期
AmazonWorkSpacesWebServiceRolePolicy – 新政策	WorkSpaces Web 新增了一項新政策，允許存取 Amazon WorkSpaces Web 使用或管理的 AWS 服務和資源。	2021 年 11 月 30 日
WorkSpaces Web 開始追蹤變更	WorkSpaces Web 已開始追蹤其 AWS 管理的政策的變更。	2021 年 11 月 30 日

疑難排解 Amazon WorkSpaces 網路身分和存取

使用下列資訊可協助您診斷並修正使用 WorkSpaces Web 和 IAM 時可能遇到的常見問題。

主題

- 我沒有在 WorkSpaces Web 中執行操作的權限
- 我沒有授權執行 iam：PassRole
- 我想允許我AWS帳戶以外的人員存取我的 WorkSpaces Web 資源

我沒有在 WorkSpaces Web 中執行操作的權限

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 workspaces-web:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 workspaces-web:*GetWidget* 動作存取 *my-example-widget* 資源。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，您必須更新原則以允許您將角色傳遞至 WorkSpaces Web。

有些 AWS 服務 允許您傳遞現有的角色至該服務，而無須建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者`marymajor`嘗試使用主控台在 WorkSpaces Web 中執行動作時，就會發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想允許我AWS帳戶以外的人員存取我的 WorkSpaces Web 資源

您可以建立一個角色，讓其他帳戶中的使用者或您的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：

- 若要瞭解 WorkSpaces Web 是否支援這些功能，請參閱Amazon WorkSpaces 網絡如何與 IAM 一起工作。
- 如需了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱《IAM 使用者指南》中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 如需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擁有的 AWS 帳戶。
- 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)。
- 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。

使用 WorkSpaces Web 的服務連結角色

WorkSpaces Web 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 WorkSpaces Web 的一種特殊 IAM 角色類型。服務連結角色由 WorkSpaces Web 預先定義，並包含該服務代您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 WorkSpaces Web 更為簡單，因為您不必手動新增必要的許可。WorkSpaces Web 定義其服務連結角色的許可，除非另有定義，否則僅有 WorkSpaces Web 可以擔任其角色。已定義的許可包括信任和許可政策。許可政策無法附加到其他任何 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。如此可保護您 WorkSpaces Web 的資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的 AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

WorkSpaces Web 的服務連結角色許可

WorkSpaces Web 使用名為 AWSServiceRoleForAmazonWorkSpacesWeb 的服務連結角色 – WorkSpaces Web 會使用此服務連結角色存取串流執行個體和 CloudWatch 指標的客戶帳戶 Amazon EC2 資源。

AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色信任下列服務以擔任角色：

- workspaces-web.amazonaws.com

名為 AmazonWorkSpacesWebServiceRolePolicy 的角色許可政策允許 WorkSpaces Web 對指定的資源完成下列動作：如需更多詳細資訊，請參閱 the section called "AmazonWorkSpacesWebServiceRolePolicy"。

- 動作：all AWS resources 上的 ec2:DescribeVpcs
- 動作：all AWS resources 上的 ec2:DescribeSubnets
- 動作：all AWS resources 上的 ec2:DescribeAvailabilityZones
- 動作：在子網路和安全群組資源上具有 aws:RequestTag/WorkSpacesWebManaged: true 的 ec2:CreateNetworkInterface
- 動作：all AWS resources 上的 ec2:DescribeNetworkInterfaces
- 動作：在網路介面上具有 aws:ResourceTag/WorkSpacesWebManaged: true 的 ec2:DeleteNetworkInterface
- 動作：all AWS resources 上的 ec2:DescribeSubnets
- 動作：all AWS resources 上的 ec2:AssociateAddress
- 動作：all AWS resources 上的 ec2:DisassociateAddress

- 動作：all AWS resources 上的 ec2:DescribeRouteTables
- 動作：all AWS resources 上的 ec2:DescribeSecurityGroups
- 動作：all AWS resources 上的 ec2:DescribeVpcEndpoints
- 動作：ec2:CreateNetworkInterface 上的 ec2:CreateTags 使用 aws:TagKeys: ["WorkSpacesWebManaged"] 進行操作
- 動作：all AWS resources 上的 cloudwatch:PutMetricData
- 動作：在名稱開頭為 amazon-workspaces-web- 之 Kinesis 資料串流上的 kinesis:PutRecord
- 動作：在名稱開頭為 amazon-workspaces-web- 之 Kinesis 資料串流上的 kinesis:PutRecords
- 動作：在名稱開頭為 amazon-workspaces-web- 之 Kinesis 資料串流上的 kinesis:DescribeStreamSummary

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 WorkSpaces Web 的服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、AWS CLI 或是 AWS API 中建立第一個入口網站時，WorkSpaces Web 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立第一個入口網站時，WorkSpaces Web 可再次為您建立服務連結角色。

您也可以使用 IAM 主控台，透過 WorkSpaces Web 使用案例建立服務連結角色。在 AWS CLI CLI 或 AWS API 中，建立一個服務名稱為 workspaces-web.amazonaws.com 的服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立服務連結角色。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 WorkSpaces Web 的服務連結角色

WorkSpaces Web 不允許您編輯 AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 WorkSpaces Web 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 若 WorkSpaces Web 服務在您試圖刪除資源時正在使用該角色，刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 AWSServiceRoleForAmazonWorkSpacesWeb 所使用的 WorkSpaces Web 資源

- 選擇下列任一選項：
  - 如果您使用主控台，請刪除主控台上的所有入口網站。
  - 如果您使用 CLI 或 API，請取消所有資源 (包括瀏覽器設定、網路設定、使用者設定、信任存放區和使用者存取日誌記錄設定) 與入口網站的關聯，刪除這些資源，然後刪除入口網站。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、AWS CLI 或 AWS API 來刪除 AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的刪除服務連結角色。

WorkSpaces Web 服務連結角色的支援區域

WorkSpaces Web 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

Amazon WorkSpaces Web 中的事件回應

您可以監控 SessionFailure Amazon CloudWatch 指標以偵測事件。請使用 SessionFailure 指標的 CloudWatch 警示，以接收事件警示。如需更多詳細資訊，請參閱 用 Amazon 監控 Amazon WorkSpaces 網站 CloudWatch。

Amazon WorkSpaces 網站的合規驗證

要瞭解 AWS 服務 是否在特定法規遵循方案範圍內，請參閱法規遵循方案範圍內的 AWS 服務，並選擇您感興趣的法規遵循方案。如需一般資訊，請參閱 AWS 法規遵循方案。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您使用 AWS 服務 時的法規遵循責任取決於資料的敏感度、您的公司的合規目標，以及適用的法律和法規。AWS 提供以下資源協助您處理法規遵循事宜：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心的基準環境的架構考量和步驟。
- Amazon Web Services 的 HIPAA 安全與法規遵循架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規定的應用程式。

> **Note**
>
> 並非全部的 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源：這組手冊和指南可能適用於您的產業和位置。
- AWS 客戶合規指南：透過合規的角度了解共同的責任模式。這份指南橫跨多個架構 (包含國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準組織 (ISO))，總結保護 AWS 服務的最佳實務並將指導方針對應至安全控制。
- AWS Config 開發人員指南中的使用規則評估資源：AWS Config 服務可評估您的資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務 可供您全面檢視 AWS 中的安全狀態。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager – 此 AWS 服務 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。

Amazon WorkSpaces Web 中的復原能力

AWS 全球基礎架構是以 AWS 區域 與可用區域為中心建置的。AWS 區域 提供多個分開且隔離的實際可用區域，並以具備低延遲、高輸送量和高度備援特性的聯網相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，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 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

WorkSpaces Web 目前不支援下列項目：

- 跨可用區域或區域備份內容
- 加密備份
- 加密可用區域或區域之間的傳輸中內容
- 預設或自動備份

若要設定高網際網路可用性，您可以調整 VPC 組態。您可以請求適量的 TPS，以獲得高 API 可用性。

Amazon WorkSpaces Web 的基礎設施安全

Amazon WorkSpaces Web 是一項受管服務，受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您會使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon WorkSpaces Web。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密 (PFS) 的密碼套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

WorkSpaces Web 會將標準 AWS SigV4 驗證和授權套用至所有服務來隔離服務流量。由您的身分提供者保護客戶資源端點 (或 Web 入口網站端點)。您可以使用身分提供者 (IdP) 中的多重要素授權和其他安全機制，進一步隔離流量。

您可以透過設定 VPC、子網路或安全群組等網路設定值，以控制所有網際網路存取。目前不支援多租戶及 VPC 端點 (PrivateLink)。

Amazon WorkSpaces Web 中的組態與漏洞分析

WorkSpaces Web 會視需要代表您 (包括 Chrome 和 Linux) 更新和修補應用程式和平台。您無需進行修補或重建。但是，您有責任根據規格和準則配置 WorkSpaces Web 的組態，並監視使用者的 WorkSpaces Web 使用情況。由 WorkSpaces Web 負責進行所有與服務相關的組態設定和漏洞分析。

您可以要求提高 WorkSpaces Web 資源的限制，例如 Web 入口網站的數量和使用者數量。WorkSpaces Web 可確保服務與 SLA 的可用性。

Amazon WorkSpaces Web 的安全最佳實務

在您開發和執行自己的安全政策時，可考慮使用 Amazon WorkSpaces Web 提供的多種安全功能。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

Amazon WorkSpaces Web 的最佳實務有以下內容：

- 若要偵測與您使用 WorkSpaces Web 相關的潛在安全事件，請使用AWS CloudTrail或 Amazon CloudWatch 來偵測和追蹤存取歷程記錄和流程日誌。如需詳細資訊，請參閱用 Amazon 監控 Amazon WorkSpaces 網站 CloudWatch及使用 AWS CloudTrail 記錄 Amazon WorkSpaces Web API 呼叫。
- 若要執行偵測控制項與識別異常情況，請使用 CloudTrail 日誌和 CloudWatch 指標。如需詳細資訊，請參閱用 Amazon 監控 Amazon WorkSpaces 網站 CloudWatch及使用 AWS CloudTrail 記錄 Amazon WorkSpaces Web API 呼叫。
- 您可以設定使用者存取日誌記錄來記錄使用者事件。如需更多詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。

若要避免發生與您使用 WorkSpaces Web 有關的潛在安全性事件，請遵循下列最佳實務做法：

- 執行最低權限存取，並建立要用於 WorkSpaces Web 動作的特定角色。使用 IAM 範本建立完整存取或唯讀角色。如需更多詳細資訊，請參閱 AWS WorkSpaces Web 的受管政策。
- 請謹慎共享入口網域和使用者憑證。網際網路上的任何人都能存取 Web 入口網站，但除非擁有入口網站的有效使用者憑證，否則他們無法啟動工作階段。請注意您如何、何時以及與誰共用 Web 入口網站憑證。

監控 Amazon WorkSpaces 網站

監控是維護 Amazon WorkSpaces Web 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您的入口 WorkSpaces 網站及其資源、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀表板，以及設定警示，在您指定的指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 CloudTrail、存放和存取日誌檔。 CloudWatch 記錄檔可以監控記錄檔中的資訊，並在符合特定臨界值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。
- 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，以及呼叫發生的時間。如需詳細資訊，請參閱《使用者指南》AWS CloudTrail。

主題

用 Amazon 監控 Amazon WorkSpaces 網站 CloudWatch

您可以使用 CloudWatch收集原始資料並將其處理為可讀且接近即時的指標來監控 Amazon WorkSpaces Web。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AWS/WorkSpacesWeb 命名空間包含下列指標。

CloudWatch Amazon WorkSpaces 網站的指標

指標	描述	維度	統計資料	單位
SessionAttempt	Amazon WorkSpaces 網路工作階段嘗試次數。	PortalId	平均數、總和、上限、下限	計數
SessionSuccess	成功的 Amazon WorkSpaces 網絡會話開始的數量。	PortalId	平均數、總和、上限、下限	計數
SessionFailure	失敗的 Amazon WorkSpaces 網絡會話數量開始。	PortalId	平均數、總和、上限、下限	計數
GlobalCpuPercent	Amazon WorkSpaces 網路工作階段執行個體的 CPU 使用率。	PortalId	平均數、總和、上限、下限	百分比
GlobalMemoryPercent	Amazon WorkSpaces 網路工作階段執行個體的記憶體 (RAM) 使用量。	PortalId	平均數、總和、上限、下限	百分比

> **Note**
>
> 您可以檢視GlobalCpuPercent或GlobalMemoryPercent判斷入口網站上作用中的並行階段作業數目的「SampleCount」測量結果統計資料。每個工作階段每分鐘會發出一次資料點。

使用 AWS CloudTrail 記錄 Amazon WorkSpaces Web API 呼叫

Amazon WorkSpaces Web 已與 AWS CloudTrail 整合，這項服務可提供由使用者、角色或 Amazon WorkSpaces Web 中 AWS 服務所採取之動作的紀錄。CloudTrail 會將 Amazon WorkSpaces Web 的所有 API 呼叫擷取為事件。其中包括從 Amazon WorkSpaces Web 主控台執行的呼叫，以及對 Amazon WorkSpaces Web API 操作發出的程式碼呼叫。如果您建立線索，就可以將 CloudTrail 事件持續交付到 Amazon S3 儲存貯體，包括 Amazon WorkSpaces Web 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。您可以利用 CloudTrail 所收集的資訊來辨別向 Amazon WorkSpaces Web 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 Amazon WorkSpaces Web 資訊

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。在 Amazon WorkSpaces Web 中發生活動時，該活動將與事件歷史紀錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在事件歷史紀錄中檢視、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 事件歷史記錄檢視事件。

若要持續記錄您 AWS 帳戶中正在進行的事件 (包括 Amazon WorkSpaces Web 的事件)，您可以建立追蹤。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Amazon WorkSpaces Web 動作，並記錄在《Amazon WorkSpaces API 參考》中。例如，對 `CreatePortal`、`DeleteUserSettings` 和 `ListBrowserSettings` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生項目。

每一筆事件或日誌項目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：

- 該請求是否使用根或 IAM 使用者憑證提出。

- 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 服務提出。

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

了解 Amazon WorkSpaces Web 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌項目。事件即為來自任何來源的單一請求，其中包含請求動作、動作日期和時間，以及請求參數和其他細節的相關資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 `ListBrowserSettings` 動作的 CloudTrail 日誌項目。


```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
       "sourceIPAddress": "127.0.0.1",
       "userAgent": "[]",
       "requestParameters": null,
       "responseElements": null,
       "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
       "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
       "readOnly": true,
       "eventType": "AwsApiCall",
       "managementEvent": true,
       "recipientAccountId": "111122223333",
       "eventCategory": "Management"
   },
```

```
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```


使用者存取日誌記錄

Amazon WorkSpaces Web 可讓客戶記錄工作階段事件，包括開始、停止和 URL 造訪。這些日誌會傳送到您為 Web 入口網站指定的 Amazon Kinesis Data Stream。如需更多詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。

Amazon WorkSpaces 網絡用戶指南

管理員使用 Amazon WorkSpaces Web 建立連線到公司網站的入口網站，例如內部網站、 software-as-a-service (SAAS) Web 應用程式或網際網路。終端使用者會使用其現有的網頁瀏覽器存取這些入口網站，以啟動工作階段和存取內容。

以下內容可協助指導想要進一步了解如何存取 Amazon WorkSpaces Web、啟動和設定工作階段，以及使用工具列和網頁瀏覽器的使用者。

主題

瀏覽器和裝置相容

Amazon WorkSpaces 網絡由 NICE DCV 網絡瀏覽器客戶端提供支持，該客戶端在網絡瀏覽器中運行，因此無需安裝。網頁瀏覽器用戶端受到 Chrome 和 Firefox 等常見的網頁瀏覽器，以及 Windows、macOS 和 Linux 等主要桌面作業系統的支援。

有關 Web 瀏覽器客戶端支持的最多 up-to-date 詳細信息，請參閱 Web 瀏覽器客戶端。

> **Note**
>
> 目前僅 Google Chrome 和 Microsoft Edge 等採用 Chromium 架構的瀏覽器有支援網路攝影機。目前，蘋果 Safari 瀏覽器和 Mozilla FireFox 不支持網絡攝像頭。

存取 Web 入口網站

您的管理員可以透過下列選項提供您存取 Web 入口網站的權限：

- 您可以從電子郵件或網站選取連結，然後使用您的 SAML 身分憑證登入。

- 您可以登入 SAML 身分提供者 (例如，Okta、Ping 或 Azure)，並且從 SAML 提供者的應用程式首頁 (例如 Okta 終端使用者儀表板或 Azure Myapps 入口網站) 按一下啟動工作階段。

工作階段指引

登入 Web 入口網站之後，您可以啟動工作階段並且在工作階段期間執行各種動作。

主題

啟動工作階段

登入以啟動工作階段後，您會看到啟動工作階段的訊息和進度列。這表明 Amazon WorkSpaces 網絡正在為您創建會話。在幕後，Amazon WorkSpaces Web 正在建立執行個體、啟動受管網頁瀏覽器，以及套用管理員設定和瀏覽器政策。

如果這是您第一次登入 Web 入口網站，您會在工具列中看到藍色的 + 圖示。此圖示表示有提供教學課程，它將帶領說明工具列裡可使用的功能。您可以使用這些圖示以瞭解如何：

- 選取本機端瀏覽器旁邊的鎖定圖示，並將剪貼簿、麥克風和攝影機旁邊的開關切換為開啟，以授予瀏覽器使用麥克風、網路攝影機和剪貼簿的權限。

  > **Note**
  >
  > 當您在第一個工作階段開始時啟用網路攝影機權限，會短暫啟用網路攝影機，且電腦上的指示燈會閃爍。這將使得本機端瀏覽器可以使用網路攝影機。

- 透過選取瀏覽器中的鎖定圖示並選取 [永遠允許快顯視窗] 設定，讓 Amazon WorkSpaces Web 啟動其他監視器視窗。

如果您想要重新啟動教學課程，可以從工具列、說明和啟動教學課程中選擇設定檔。

使用工具列

若要移動工具列，請選取工具列頂部的淺色條，將其拖曳至您想要的位置，然後放開它以放下。

若要收合工具列，請將滑鼠游標暫停在工具列上，然後選取向上箭頭按鈕，或按兩下工具列頂部的淺色條。收合檢視畫面提供更多螢幕空間，按一下即可存取最常用的圖示。

若要將工具列固定在螢幕頂端，請在「工具列」模式下選擇「偏好設定」、「一般」和「停靠」。

下表說明工具列中的所有可用圖示：

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> 除非您的管理員授與這些權限，否則預設隱藏 Clipboard 剪貼簿和 Files 檔案圖示。只有管理員可以啟用或停用 Web 入口網站上的剪貼簿和檔案功能。如果已經隱藏這些圖示，而您需要存取這些圖示，請聯絡您的管理員。

使用瀏覽器

當您啟動工作階段時，瀏覽器會顯示啟動 URL，這是您的管理員所選擇的 URL。如果管理員尚未選擇啟動 URL，您將看到 Google Chrome 瀏覽器中的預設新分頁體驗。

您可以在瀏覽器中開啟分頁、啟動其他瀏覽器視窗 (從 Windows 工具列圖示或瀏覽器的三點功能表)、在 URL 列中輸入 URL 或搜尋 URL，或從受管理的書籤開啟網站。若要存取 Web 入口網站的書籤，請開啟書籤列上的受管理的書籤資料夾 (位於 URL 列下方)，或是從 URL 列右側的三點功能表開啟書籤管理員。

若要調整瀏覽器視窗大小或移動瀏覽器視窗，請向下拖曳 Chrome 分頁列。這樣可以在工作階段期間有更多螢幕空間顯示多個瀏覽器視窗。

> **Note**
>
> 如果您的管理員已經關閉無痕模式等瀏覽器的功能，您的工作階段期間可能無法使用這些功能。

結束工作階段

若要結束工作階段，請選擇設定檔和結束工作階段。工作階段結束後，Amazon WorkSpaces Web 會刪除工作階段中的所有資料。工作階段結束後，將無法使用任何瀏覽器資料，例如開啟的網站或歷程記錄，或是檔案總管裡的檔案或資料。

如果您在使用中的工作階段期間關閉分頁，會在管理員設定的一段時間後結束工作階段。如果您在此逾時生效之前關閉分頁且重新造訪 Web 入口網站，您可以加入目前的工作階段及查看所有先前的工作階段資料，例如開啟的網站和檔案。

故障診斷

我的 Amazon 門戶 WorkSpaces 網站不會讓我登錄。我收到錯誤訊息，指出「尚未設定您的 Web 入口網站。如需進一步協助，請聯絡您的管理員。」

您的管理員必須使用 SAML 2.0 身分提供者來完成建立入口網站，才能讓您登入。如需進一步協助，請聯絡您的管理員。

我的入口網站不會啟動工作階段。我收到錯誤訊息，指出「無法保留工作階段。發生內部錯誤。請再試一次。」

您的 Web 入口網站在啟動工作階段時發生問題。請嘗試再次啟動工作階段。如果繼續發生這個情況，請聯絡您的管理員以尋求協助。

我無法使用剪貼簿、麥克風或網路攝影機。

請選取 URL 旁的鎖定圖示，然後切換剪貼簿、麥克風、攝影機和快顯視窗旁的藍色開關，然後重新導向來開啟這些功能，以允許瀏覽器可以使用這些功能。

> **Note**
>
> 如果您的網頁瀏覽器不支援輸入視訊或音訊，在工具列上將不會出現這些選項。

Amazon WorkSpaces Web 即時音訊視訊 (AV) 會將您的本機網路攝影機視訊和麥克風音訊輸入重新導向至瀏覽器串流工作階段。如此一來，您便能在使用 Google Chrome 或 Microsoft Edge 等 Chromium 架構網頁瀏覽器進行串流工作階段時，透過本機端裝置進行視訊和音訊會議。非 Chromium 架構的瀏覽器目前不支援網路攝影機。

如需如何設定 Google Chrome 瀏覽器的詳細資訊，請參閱使用攝影機和麥克風。

我的 Web 入口網站不會啟動額外的監視器。

如果您嘗試啟動雙監視器，並在頂端瀏覽器的網址列末端看到彈出視窗已封鎖圖示，請選取永遠允許彈出視窗和重新導向旁邊的圖示和圓形按鈕。在允許彈出視窗的情況下，選擇工具欄上的雙監視器圖示以啟動新視窗，重新定位監視器上的視窗，然後將瀏覽器分頁拖到視窗中。

我試著從檔案窗格下載檔案時，沒有任何反應。

如果您嘗試從檔案窗格下載檔案，並在頂端瀏覽器的網址列末端看到彈出視窗已封鎖圖示，請選取永遠允許彈出視窗和重新導向旁邊的圖示和圓形按鈕。在允許彈出視窗的情況下，請嘗試再次下載檔案。

單一登入擴充功能

Amazon WorkSpaces 網絡提供了一個擴展單一登錄與桌面計算機上的 Chrome 和火狐瀏覽器。如果您的管理員有啟用擴充功能，Web 入口網站會在您登入時要求您安裝擴充功能。

Amazon WorkSpaces Web 建置了擴充功能，以便在工作階段期間啟用網站的單一登入功能。例如，如果您使用 Okta 或 Ping 等 SAML 2.0 身分提供者登入 Web 入口網站，並且您在工作階段期間使用相同的身分提供者造訪網站，則該擴充功能可移除其他登入提示讓您更輕鬆地存取網站。

您無需安裝擴展程序即可存取 Web 入口網站，但它可以減少要求您輸入使用者名稱和密碼的次數，讓您有更好的使用體驗。

當您登入時，擴充功能會尋找您的管理員為您的工作階段列出的 cookie。擴充功能找到的所有資料都會在靜態和傳輸期間進行加密。這些資料都不會存在您的本機端瀏覽器中。當您結束工作階段時，會刪除所有工作階段資料 (例如，開啟的分頁、下載的檔案，以及在工作階段期間傳送或建立的 cookie)。

相容性

該擴展功能適用於以下裝置：

- 筆記型電腦
- 桌上型電腦

該擴展功能適用於以下瀏覽器：

- Chrome
- Firefox

安裝

當您登入入口網站時，請依照提示從瀏覽器的網路商店安裝用於 Chrome 或 Firefox 瀏覽器的擴充功能。您只需為每個網頁瀏覽器執行此操作一次。

如果您切換裝置、在同一部裝置上切換使用其他瀏覽器，或從本機端瀏覽器刪除擴充功能，則在您開始下一個工作階段時會看到安裝擴充功能的提示。

為確保擴展功能正常運作，請在普通的瀏覽分頁上使用擴展功能，而非使用無痕模式 (Chrome) 或隱私瀏覽 (Firefox)。

故障診斷

如果您已安裝擴充功能，但仍要求您在工作階段期間登入，請依照下列步驟執行：

1. 確保您在瀏覽器上安裝了 Amazon WorkSpaces 網絡擴展程序。如果您刪除了瀏覽器資料，則可能意外刪除了擴充功能。
2. 確保您不是使用無痕模式 (Chrome) 或隱私瀏覽 (Firefox)。這些模式可能會造成擴充功能發生問題。
3. 如果問題仍然存在，請聯絡入口網站管理員以取得其他協助。

Amazon WorkSpaces 網路使用者指南的文件歷史

下表說明適用於 Amazon WorkSpaces 網路的文件發行版本。

變更	描述	日期
CloudWatch 度量	添加 GlobalCpuPercent 和 GlobalMemoryPercent 指標。	2024年2月26日
設定網址過濾	您可以使用 Chrome 政策來篩選使用者可從遠端瀏覽器存取哪些網址。	2024年2月21 日
IdP 驗證類型	您可以選擇標準或 IAM 身分中心驗證類型。	2024年2月5 日
啟用單一登入的擴充功能	您可以為終端使用者啟用擴充功能，以獲得更好的入口網站登入體驗。	2023 年 8 月 28 日
Amazon WorkSpaces 網站的用戶指南	新增內容可協助引導使用者，以及想要進一步了解如何存取 Amazon WorkSpaces Web、啟動和設定工作階段，以及使用工具列和網頁瀏覽器的使用者。	2023 年 7 月 17 日
IP 存取控制	WorkSpaces Web 允許您控制您的門戶網站可以從哪些 IP 地址訪問。	2023 年 5 月 31 日
受管政策更新	更新的 AmazonWorkSpacesWebReadOnly 受管政策	2023 年 5 月 15 日
設定身分提供者更新	WorkSpaces Web 提供了兩種身份驗證類型：標準和 AWS IAM Identity Center	2023 年 3 月 15 日

瀏覽器政策更新	更新和重組的瀏覽器政策部分	2023 年 1 月 31 日
受管政策更新	更新的 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2022 年 12 月 15 日
允許清單和封鎖清單	指定允許清單和封鎖清單，以指定您的使用者可以存取或無法存取的網域清單。	2022 年 11 月 14 日
受管政策更新	更新的 AmazonWorkSpacesWebReadOnly 受管政策	2022 年 11 月 2 日
受管政策更新	更新的 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2022 年 10 月 24 日
使用者存取日誌記錄	設定使用者存取日誌記錄以記錄使用者事件	2022 年 10 月 17 日
網路更新	「網路和存取」部分的各種更新	2022 年 9 月 22 日
受管政策更新	更新的 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2022 年 9 月 6 日
設定使用者工作階段	設定輸入法編輯器 (IME) 和工作階段內本地化	2022 年 7 月 28 日
網路更新	「網路和存取」部分的各種更新	2022 年 7 月 7 日
連線逾時值	指定中斷連線逾時 (以分鐘為單位) 和閒置中斷連線逾時 (以分鐘為單位)	2022 年 5 月 16 日

已更新受管政策	更新 AmazonWorkSpacesWebServiceRolePolicy 受管理的政策，以將 AWS/ 使用命名空間新增至 API 權限 PutMetricData	2022 年 4 月 6 日
服務連結角色	新的 AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色	2021 年 11 月 30 日
受管政策	新的 AmazonWorkSpacesWebReadOnly 受管理策略	2021 年 11 月 30 日
受管政策	新的 AmazonWorkSpacesWebServiceRolePolicy 受管理策略	2021 年 11 月 30 日
初始版本	《 WorkSpaces 網站管理指南》的初始版本	2021 年 11 月 30 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。