aws

Guía de administración

Amazon WorkSpaces

Amazon WorkSpaces: Guía de administración

Table of Contents

¿Qué es Amazon WorkSpaces?

Amazon WorkSpaces le permite aprovisionar escritorios Microsoft Windows, Amazon Linux o Ubuntu Linux virtuales basados en la nube para sus usuarios, conocidos como WorkSpaces. WorkSpaces elimina la necesidad de adquirir e implementar hardware o instalar software complejo. Puede agregar o eliminar rápidamente a los usuarios en función de las necesidades. Los usuarios tienen acceso a los escritorios virtuales desde diversos dispositivos o navegadores web.

Para obtener más información, consulta Amazon WorkSpaces.

Características

- Elija el sistema operativo (Windows, Amazon Linux, Ubuntu Linux) y seleccione entre una amplia variedad de configuraciones de hardware y software, así como de regiones de AWS. Para obtener más información, consulta Amazon WorkSpaces Bundles ythe section called “Creación de una imagen y un paquete personalizados”.
- Elija su protocolo: PCoIP o WorkSpaces Streaming Protocol (WSP). Para obtener más información, consulte Protocolos para Amazon WorkSpaces.
- Conéctate a tu WorkSpace y continúa desde donde lo dejaste. WorkSpacesproporciona una experiencia de escritorio persistente.
- WorkSpaces ofrece la flexibilidad de facturar mensual o por hora para WorkSpaces. Para obtener más información, consulte WorkSpaces Precios.
- En los escritorios de Windows, puede traer sus propias licencias y aplicaciones, o adquirirlas en AWS Marketplace for Desktop Apps.
- Cree un directorio gestionado independiente para sus usuarios o conéctelo WorkSpaces a su directorio local para que los usuarios puedan utilizar sus credenciales actuales y obtener un acceso sin problemas a los recursos corporativos. Para obtener más información, consulte Directorios.
- Use las mismas herramientas de administración WorkSpaces que usa para administrar los escritorios locales.
- Utilice la autenticación multifactor (MFA) para obtener más seguridad.
- Utilice AWS Key Management Service (AWS KMS) para cifrar los datos en reposo, E/S de disco y las instantáneas de volúmenes.
- Controle las direcciones IP desde las que los usuarios pueden acceder a sus. WorkSpaces

Arquitectura

En Windows y Linux WorkSpaces, cada uno de ellos WorkSpace está asociado a una nube privada virtual (VPC) y a un directorio para almacenar y administrar información para usted WorkSpaces y sus usuarios. Para obtener más información, consulte the section called “Requisitos de la VPC”. Los directorios se administran a través de AWS Directory Service, que ofrece las siguientes opciones: Simple AD, Conector AD o AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD. Para obtener más información, consulte la Guía de administración de AWS Directory Service.

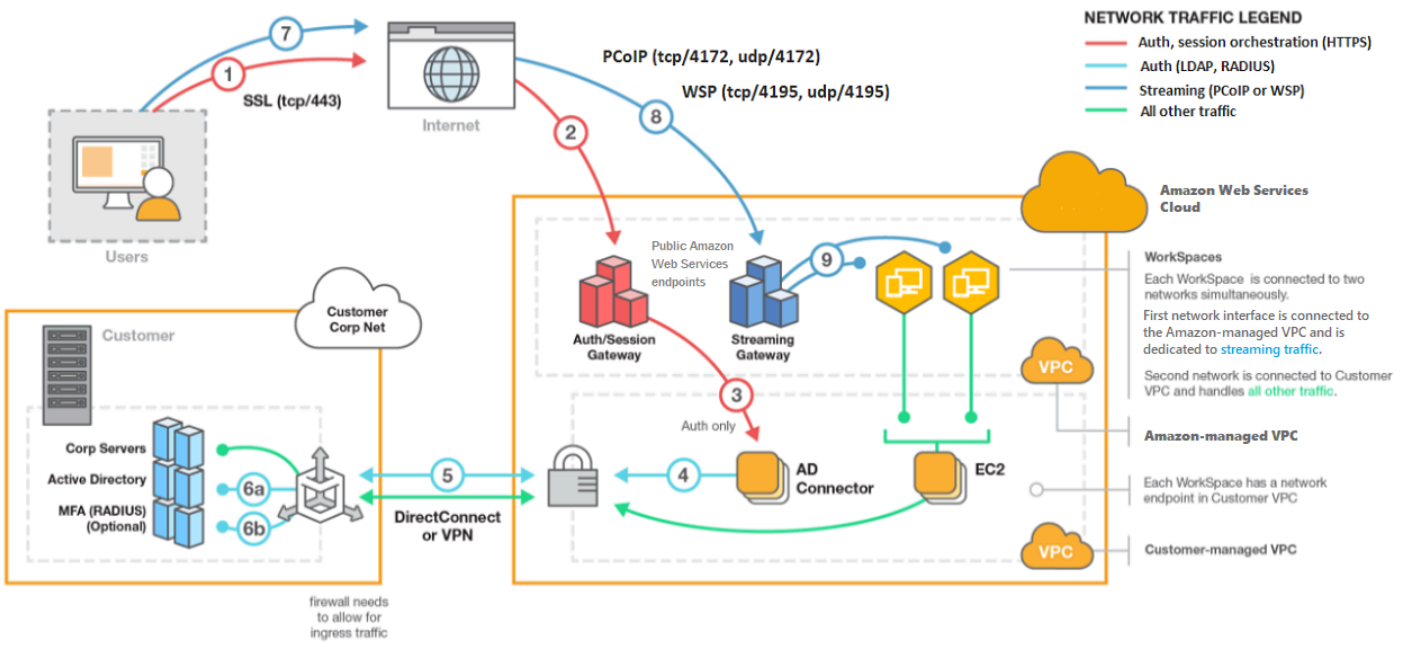
WorkSpaces utiliza el directorio Simple AD, AD Connector o AWS Managed Microsoft AD para autenticar a los usuarios. Los usuarios acceden a ellos WorkSpaces mediante una aplicación cliente desde un dispositivo compatible o, en el caso de Windows WorkSpaces, desde un navegador web, e inician sesión con sus credenciales de directorio. La información de inicio de sesión se envía a una pasarela de autenticación, que reenvía el tráfico al directorio del WorkSpace. Una vez que el usuario está autenticado, se inicia el tráfico de streaming a través de la gateway de transmisión.

Las aplicaciones cliente utilizan HTTPS a través del puerto 443 para todas las sesiones de autenticación y la información relacionada. Las aplicaciones cliente utilizan los puertos 4172 (PCoIP) y 4195 (WSP) para la transmisión de píxeles al puerto y los puertos 4172 WorkSpace y 4195 para comprobar el estado de la red. Para obtener más información, consulte Puertos de aplicaciones cliente.

Cada uno WorkSpace tiene dos interfaces de red elásticas asociadas: una interfaz de red para administración y transmisión (eth0) y una interfaz de red principal (eth1). La interfaz de red principal tiene una dirección IP proporcionada por la VPC, procedente de las mismas subredes que se utilizan en el directorio. Esto garantiza que el tráfico procedente de usted WorkSpace pueda llegar fácilmente al directorio. El acceso a los recursos de la VPC se controla mediante los grupos de seguridad asignados a la interfaz de red principal. Para obtener más información, consulte Interfaces de red.

El siguiente diagrama muestra la arquitectura de WorkSpaces.

Amazon WorkSpaces Architectural Diagram



Acceda a su WorkSpace

Puede conectarse a su WorkSpaces mediante la aplicación cliente de un dispositivo compatible mediante un navegador web compatible en un sistema operativo compatible.

> **Note**
>
> No puede utilizar un navegador web para conectarse a Amazon Linux WorkSpaces.

Hay aplicaciones cliente para las siguientes plataformas y dispositivos:

- Equipos Windows
- Equipos macOS
- Equipos con Ubuntu Linux 18.04
- Chromebooks
- iPads
- Dispositivos Android
- Tabletas Fire

- Dispositivos cliente cero (los dispositivos con cero cliente de Teradici solo son compatibles con PCoIP).

En ordenadores con Windows, macOS y Linux, puede utilizar los siguientes navegadores web para conectarse a Windows y Ubuntu Linux WorkSpaces:

- Chrome 53 y versiones posteriores (solo Windows y macOS)
- Firefox 49 y versiones posteriores

Para obtener más información, consulta WorkSpaces Clientes en la Guía del WorkSpaces usuario de Amazon.

Precios

Una vez que te hayas AWS registrado, podrás empezar de forma WorkSpaces gratuita con la oferta del nivel WorkSpaces gratuito. Para obtener más información, consulta WorkSpaces los precios.

Con WorkSpaces, solo pagas por lo que usas. Se te cobrará en función del paquete y del número de unidades WorkSpaces que lances. El precio WorkSpaces incluye el uso de Simple AD y AD Connector, pero no el uso de AWS Managed Microsoft AD.

WorkSpaces proporciona facturación mensual o por hora para WorkSpaces. Con la facturación mensual, pagas una tarifa fija por un uso ilimitado, lo que es mejor para los usuarios que utilizan su tiempo WorkSpaces completo. Con la facturación por horas, pagas una pequeña cuota mensual fija por hora WorkSpace, además de una tarifa horaria baja por cada hora de WorkSpace funcionamiento. Para obtener más información, consulta WorkSpaces los precios.

Para obtener información sobre las regiones compatibles, consulta WorkSpaces los precios.

Cómo comenzar

Para crear una WorkSpace, prueba uno de los siguientes tutoriales:

- Primeros pasos para la configuración rápida de WorkSpaces
- Lanzamiento de un WorkSpace con AWS Managed Microsoft AD
- Lanzar un escritorio de WorkSpaces con AD sencillo
- Iniciar WorkSpace con el conector AD

- Lanzar escritorios de WorkSpaces usando un dominio de confianza

También puedes explorar estos recursos para obtener más información sobre Amazon WorkSpaces:

- Aprovisionar escritorios en la nube
- Mejores prácticas para implementar Amazon WorkSpaces
- WorkSpaces Recursos de Amazon: incluye documentos técnicos, publicaciones de blog, seminarios web y sesiones de re:Invent
- WorkSpaces Preguntas frecuentes de Amazon

Primeros pasos para la configuración rápida de WorkSpaces

En este tutorial, aprenderá a aprovisionar un escritorio virtual basado en la nube de Microsoft Windows, Amazon Linux o Ubuntu Linux, conocido como WorkSpace, utilizando WorkSpaces y AWS Directory Service.

En este tutorial se utiliza la opción de configuración rápida para lanzar el escritorio WorkSpace. Esta opción solo está disponible si nunca ha lanzado un escritorio de WorkSpaces. Para otras opciones, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

> **Note**
>
> La configuración rápida es compatible únicamente en las siguientes regiones de AWS:
>
> - Este de EE. UU. (Norte de Virginia)
> - Oeste de EE. UU. (Oregón)
> - Europa (Irlanda)
> - Asia-Pacífico (Singapur)
> - Asia Pacífico (Sídney)
> - Asia-Pacífico (Tokio)
>
> Para cambiar su región, consulte Elegir una región.

Tareas

Antes de empezar

Antes de comenzar, asegúrese de que cumple los siguientes requisitos:

- Debe tener una cuenta de AWS para crear o administrar un WorkSpace. Los usuarios no necesitan una cuenta de AWS para conectarse y utilizar los WorkSpaces.
- WorkSpaces no está disponible en todas las regiones. Compruebe las regiones que son compatibles y seleccione una para los WorkSpaces. Para obtener más información sobre las regiones compatibles, consulte Precios de WorkSpaces por región de AWS.

Asimismo, le recomendamos que revise y comprenda lo siguiente antes de seguir:

- Cuando lanza un escritorio de WorkSpaces, debe seleccionar un paquete de WorkSpaces. Para obtener más información, consulte Paquetes de Amazon WorkSpaces y Precios de Amazon WorkSpaces.
- Al iniciar un WorkSpace, debe seleccionar qué protocolo (PCoIP o Protocolo de Streaming de WorkSpaces [WSP]) quiere utilizar con su paquete. Para obtener más información, consulte Protocolos para Amazon WorkSpaces.
- Cuando se inicia un WorkSpace, debe especificar la información de perfil del usuario, incluido un nombre de usuario y una dirección de correo electrónico. Los usuarios completan sus perfiles especificando una contraseña. La información sobre WorkSpaces y los usuarios se almacena en un directorio. Para obtener más información, consulte Directorios.

Qué hace la configuración rápida

La instalación rápida realiza las siguientes tareas:

- Crea un rol de IAM para permitir que el servicio de WorkSpaces cree interfaces de red elásticas y enumere los directorios de WorkSpaces. El nombre de este rol es `workspaces_DefaultRole`.
- Crea una nube virtual privada (VPC). Si, en su lugar, desea utilizar una VPC existente, asegúrese de que cumpla los requisitos que se indican en Configurar una VPC para WorkSpaces, a continuación, siga los pasos de uno de los tutoriales que se enumeran en Lanzar un escritorio virtual utilizando WorkSpaces. Elija el tutorial correspondiente al tipo de Active Directory que desea utilizar.
- Configura un directorio de Simple AD en la VPC y lo habilita para Amazon WorkDocs. Este directorio de Simple AD se utiliza para almacenar información de usuarios y WorkSpace. El primer

Cuenta de AWS que se crea mediante una configuración rápida es su administrador Cuenta de AWS. † El directorio también tiene una cuenta de administrador. Para obtener más información, consulte Qué se crea en la Guía de administración de AWS Directory Service.

- Crea las Cuentas de AWS especificadas y las añade al directorio .
- Crear un espacio de trabajo Cada escritorio de WorkSpaces recibe una dirección IP pública para ofrecer acceso a Internet. El modo de ejecución es AlwaysOn. Para obtener más información, consulte Controlar el modo de ejecución de WorkSpaces.
- Envía los correos electrónicos de invitación a los usuarios especificados. Si sus usuarios no reciben sus correos electrónicos de invitación, consulte Enviar un correo electrónico de invitación.

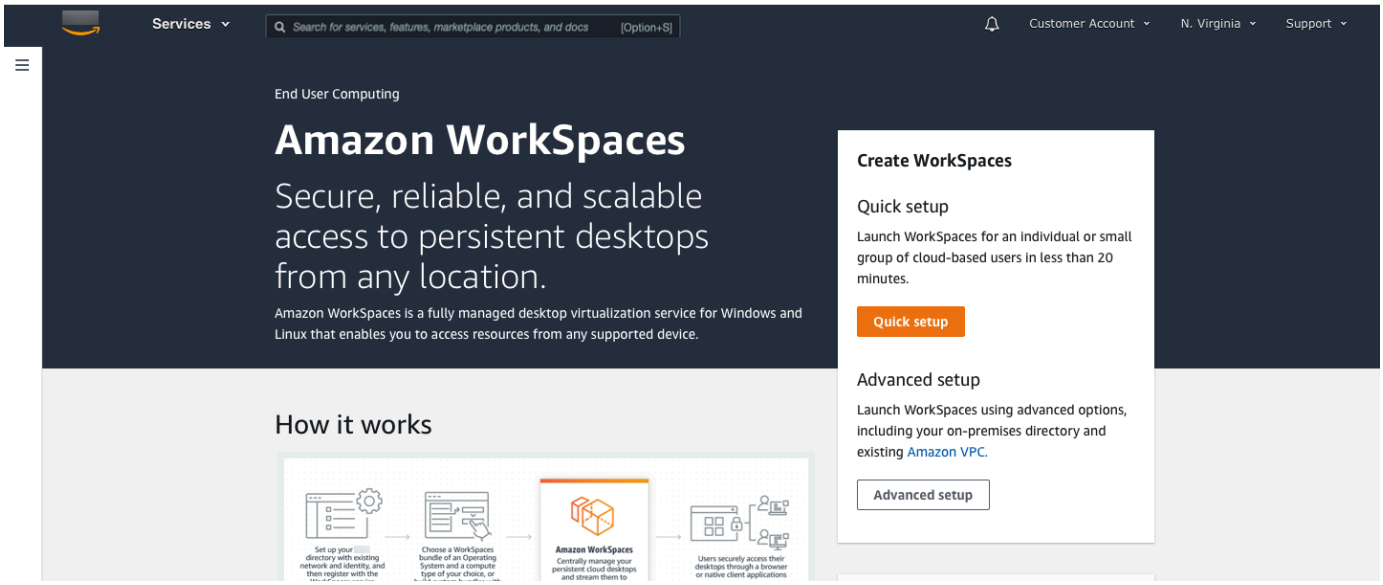
† El primer Cuenta de AWS que se crea mediante una configuración rápida es su administrador Cuenta de AWS. No puede actualizar esta Cuenta de AWS desde la consola de WorkSpaces. No comparta con nadie más la información de esta cuenta. Para invitar a otros usuarios a usar WorkSpaces, cree un nuevo Cuentas de AWS para ellos.

Paso 1: Lanzar el WorkSpace

Con la configuración rápida, puede lanzar el primer WorkSpace en unos minutos.

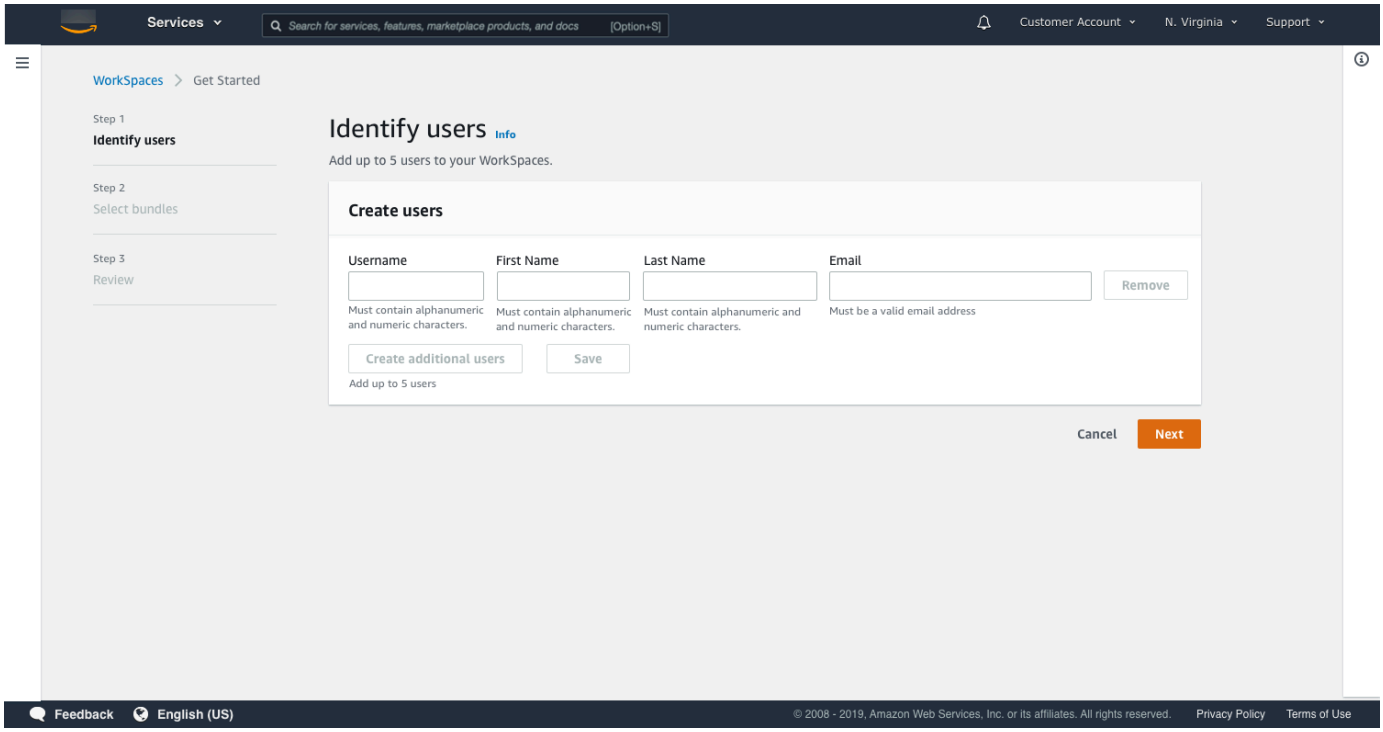
Para lanzar un WorkSpace

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. Elija Quick setup (Configuración rápida). Si no ve este botón, o ya ha iniciado un WorkSpace en esta región o no está utilizando una de las regiones compatibles con la configuración rápida. En este caso, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

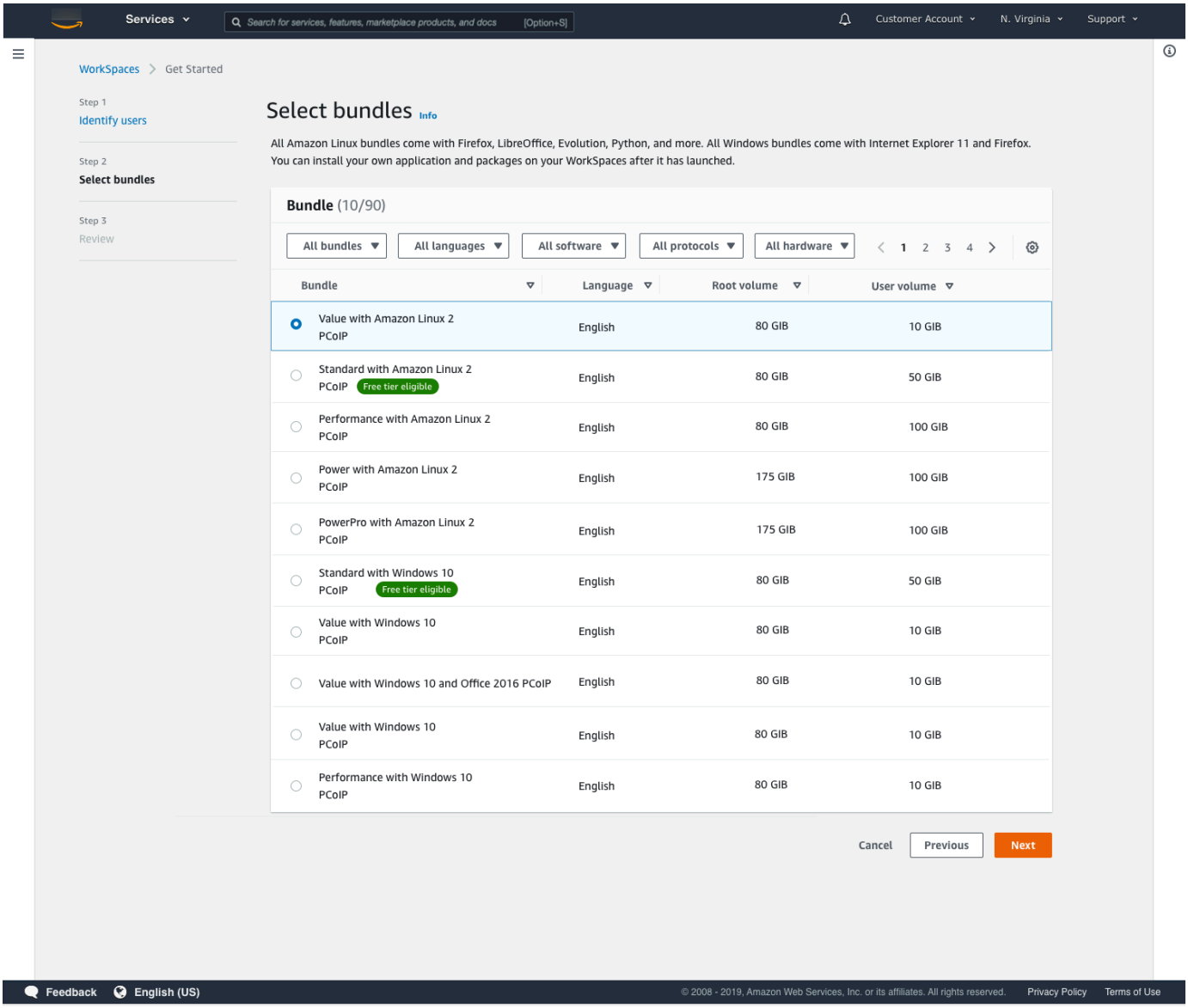


3. En Identificar usuarios, introduzca el nombre de usuario y el nombre. Apellido y correo electrónico. A continuación, elija Next.

> **Note**
>
> Si es la primera vez que utiliza WorkSpaces, le recomendamos que cree un usuario para realizar pruebas.



4. En Paquetes, seleccione un paquete (hardware y software) para el usuario con el protocolo adecuado (PCoIP o WSP). Para obtener más información sobre los distintos paquetes públicos disponibles de Amazon WorkSpaces, consulte Paquetes de Amazon WorkSpaces.



5. Revise su información. A continuación, elija Crear WorkSpace.
6. El WorkSpace tarda unos 20 minutos en iniciarse. Para monitorizar el progreso, vaya al panel de navegación izquierdo y elija Directorios. Verá que se está creando un directorio con un estado inicial de `REQUESTED` y, luego, `CREATING`.

   Una vez que el directorio se haya creado y tenga el estado de`ACTIVE`, puede elegir WorkSpaces en el panel de navegación izquierdo para supervisar el progreso del proceso de inicio de WorkSpace. El estado inicial del WorkSpace es `PENDING`. Cuando el lanzamiento ha terminado, el estado es `AVAILABLE` y se envía una invitación a la dirección de correo electrónico que especificó para el usuario. Si sus usuarios no reciben sus correos electrónicos de invitación, consulte Enviar un correo electrónico de invitación.

Paso 2: Conectarse al WorkSpace

Una vez recibido el correo electrónico de invitación, puede conectarse al WorkSpace utilizando el cliente de su elección. Después de iniciar sesión, el cliente muestra el escritorio de WorkSpaces.

Para conectarse al WorkSpace

1. Si todavía no ha creado las credenciales para el usuario, abra el enlace del correo electrónico de invitación y siga las indicaciones. Recuerde la contraseña que especifique ya que la necesitará para conectarse al WorkSpace.

   > **Note**
   >
   > Las contraseñas distinguen entre mayúsculas y minúsculas y debe tener un mínimo de 8 caracteres y un máximo de 64. Las contraseñas deben contener al menos un carácter de cada una de las siguientes categorías: letras minúsculas (a-z), letras mayúsculas (A-Z), números (0-9) y ~!@#$%^&*_-+=`|(){}[]:;'"<>,.?/.

2. Consulte Clientes de WorkSpaces en la Guía del usuario de Amazon WorkSpaces para obtener más información sobre los requisitos de cada cliente y, a continuación, siga uno de estos procedimientos:

   - Cuando se le solicite, descargue una de las aplicaciones cliente o inicie Acceso web.
   - Si no se le solicita y aún no ha instalado una aplicación cliente, abra https://clients.amazonworkspaces.com/ y descargue una de las aplicaciones cliente o inicie Acceso web.

   > **Note**
   >
   > No puede utilizar un navegador web (Acceso web) para conectarse con los WorkSpaces de Amazon Linux.

3. Inicie el cliente y escriba el código de registro que se incluye en el correo de invitación y elija Register.
4. Cuando se le solicite iniciar sesión, introduzca las credenciales de inicio de sesión y, a continuación, seleccione Iniciar sesión.
5. (Opcional) Cuando se le solicite guardar las credenciales, elija Yes.

Para obtener más información sobre el uso de las aplicaciones cliente, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte Clientes de WorkSpaces y Soporte de dispositivos periféricos en la Guía del usuario de Amazon WorkSpaces.

Paso 3: limpieza (opcional)

Si ha terminado de usar el WorkSpace que ha creado para este tutorial, puede eliminarlo. Para obtener más información, consulte the section called “Eliminar WorkSpaces”.

> **Note**
>
> AD sencillo está disponible de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio de Simple AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.
> Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio de AD sencillo, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

Pasos siguientes

Puede seguir y personalizar el WorkSpace que acaba de crear. Por ejemplo, puede instalar software y, después, crear un paquete personalizado del WorkSpace. También puede realizar varias tareas administrativas para sus WorkSpaces y su directorio de WorkSpaces. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados
- Administre su WorkSpaces
- Administrar directorios para WorkSpaces

Para crear otros WorkSpaces, lleve a cabo alguna de las siguientes operaciones:

- Si desea seguir utilizando la VPC y el directorio de Simple AD que se crearon mediante una configuración rápida, puede añadir WorkSpaces para más usuarios siguiendo los pasos de la sección Paso 2: Crear un espacio de trabajo del tutorial Lanzar un escritorio de WorkSpaces con Simple AD.

- Si necesita usar otro tipo de directorio o si necesita usar un Active Directory existente, consulte el tutorial correspondiente en Lanzar un escritorio virtual utilizando WorkSpaces.

Para obtener más información sobre el uso de las aplicaciones cliente de WorkSpaces, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte Clientes de WorkSpaces y Soporte de dispositivos periféricos en la Guía del usuario de Amazon WorkSpaces.

Primeros pasos para la configuración avanzada de WorkSpaces

En este tutorial, aprenderá a aprovisionar un escritorio virtual basado en la nube de Microsoft Windows, Amazon Linux o Ubuntu Linux, conocido como WorkSpace, utilizando WorkSpaces y AWS Directory Service.

Este tutorial utiliza la opción de de configuración avanzada para lanzar su WorkSpace.

> **Note**
>
> La configuración avanzada está disponible en todas las regiones para WorkSpaces.

Tareas

Antes de empezar

Antes de empezar, asegúrese de que dispone de una cuenta de AWS que puede utilizar para crear o administrar un WorkSpace. Los usuarios no necesitan una cuenta de AWS para conectarse y utilizar sus WorkSpaces.

Revise y comprenda los siguientes conceptos antes de continuar:

- Cuando lanza un escritorio de WorkSpaces, debe seleccionar un paquete de WorkSpaces. Para obtener más información, consulte Paquetes de Amazon WorkSpaces.
- Al iniciar un WorkSpace, debe seleccionar qué protocolo (PCoIP o Protocolo de Streaming de WorkSpaces [WSP]) quiere utilizar con su paquete. Para obtener más información, consulte Protocolos para Amazon WorkSpaces.
- Cuando se inicia un WorkSpace, debe especificar la información de perfil del usuario, incluido un nombre de usuario y una dirección de correo electrónico. Los usuarios completan sus perfiles especificando una contraseña. La información sobre WorkSpaces y los usuarios se almacena en un directorio. Para obtener más información, consulte Directorios.

Uso de la configuración avanzada para iniciar el WorkSpace

Uso de la configuración avanzada para iniciar el WorkSpace:

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. Elija uno de los siguientes tipos de directorio y, a continuación, seleccione Siguiente:
   - AWS Managed Microsoft AD
   - AD sencillo
   - Conector de AD
3. Ingrese la información del directorio.
4. Elija dos subredes en una VPC de dos zonas de disponibilidad diferentes. Para obtener más información, consulte Configurar una VPC con subredes públicas.
5. Revise la información de su directorio y seleccione Crear directorio.

Redes y acceso de WorkSpaces

Como administrador de escritorios de WorkSpaces, debe saber lo siguiente acerca de las redes y el acceso en WorkSpaces.

Contenido

Protocolos para Amazon WorkSpaces

Amazon WorkSpaces admite dos protocolos: PCoIP y WorkSpaces Streaming Protocol (WSP). El protocolo que elija depende de varios factores, como el tipo de dispositivos WorkSpaces desde los que accederán los usuarios, el sistema operativo del que disponga, las condiciones de red a las que se enfrentarán los usuarios y si los usuarios necesitan soporte de vídeo bidireccional. WorkSpaces

Requisitos

Los WSP solo WorkSpaces son compatibles con los siguientes requisitos mínimos.

Requisitos del agente de host:

- Agente de host de Windows (versión 2.0.0.312 o posterior)
- Agente de host de Ubuntu (versión 2.1.0.501 o posterior)
- Agente de host de Amazon Linux 2 (versión 2.0.0.596 o posterior)

Requisitos del cliente:

- Cliente nativo de Windows (versión 5.1.0.329 o posterior)
- Cliente nativo de macOS (versión 5.5.0 o posterior)
- Acceso web

Para obtener más información sobre cómo comprobar la versión de su WorkSpace cliente y la versión del agente de alojamiento, consulte las preguntas frecuentes.

Cuándo se debe usar WSP

- Si necesita una mayor tolerancia a la pérdida/latencia para adaptarse a las condiciones de red de sus usuarios finales. Por ejemplo, hay usuarios que acceden a ellos a WorkSpaces través de distancias globales o utilizan redes poco fiables.
- Si necesita que sus usuarios se autentiquen con tarjetas inteligentes o que las usen durante la sesión.
- Si necesita funciones de compatibilidad con cámaras web durante la sesión.
- Si necesita usar Web Access con el paquete con tecnología Windows Server 2019 WorkSpaces .
- Si necesitas usar Ubuntu. WorkSpaces
- Si necesita usar Windows 11 BYOL WorkSpaces.
- Si necesitas usar paquetes basados en la GPU de Ubuntu (Graphics.G4DN y.g4dn). GraphicsPro
- Si necesita que sus usuarios se autentiquen durante la sesión con autenticadores como Windows Hello. WebAuthn YubiKey

Cuándo se debe usar PCoIP

- Si desea utilizar los clientes de Linux de iPad o Android.
- Si utiliza dispositivos de cliente cero de Teradici.
- Si necesita usar paquetes basados en GPU (Graphics.G4dn, .g4dn, Graphics o). GraphicsPro GraphicsPro
- Si necesita usar un paquete de Linux para casos en los que no se usen tarjetas inteligentes.
-

> **Note**
>
> - Un directorio puede contener una combinación de PCoIP y WSP. WorkSpaces
> - Un usuario puede tener un PCoIP y un WSP WorkSpace siempre que ambos estén ubicados en directorios separados. WorkSpaces El mismo usuario no puede tener un PCoIP y un WorkSpace WSP en el mismo directorio. Para obtener más información sobre la creación de varios WorkSpaces para un usuario, consulte. Crear varios escritorios de WorkSpaces para un usuario
> - Puede migrar a WorkSpace entre los dos protocolos mediante la función de WorkSpaces migración, que requiere una reconstrucción del WorkSpace. Para obtener más información, consulte Migrar un WorkSpace.
> - Si WorkSpace se creó con paquetes de PCoIP, puede modificar el protocolo de transmisión para migrar entre los dos protocolos sin necesidad de volver a compilarlos y, al mismo tiempo, conservar el volumen raíz. Para obtener más información, consulte Modificar protocolos.
> - Para disfrutar de la mejor experiencia con las videoconferencias, le recomendamos que utilice Power o PowerPro paquetes únicamente.

Configurar una VPC para WorkSpaces

WorkSpaces lo lanza WorkSpaces en una nube privada virtual (VPC).

Puede crear una VPC con dos subredes privadas para usted WorkSpaces y una puerta de enlace NAT en una subred pública. Como alternativa, puede crear una VPC con dos subredes públicas

para usted WorkSpaces y asociar una dirección IP pública o una dirección IP elástica a cada una. WorkSpace

Para obtener más información sobre las consideraciones de diseño de las VPC, consulte Prácticas recomendadas para las VPC y redes en las WorkSpaces implementaciones de Amazon y Prácticas recomendadas para la implementación: WorkSpaces diseño de VPC.

Contenido

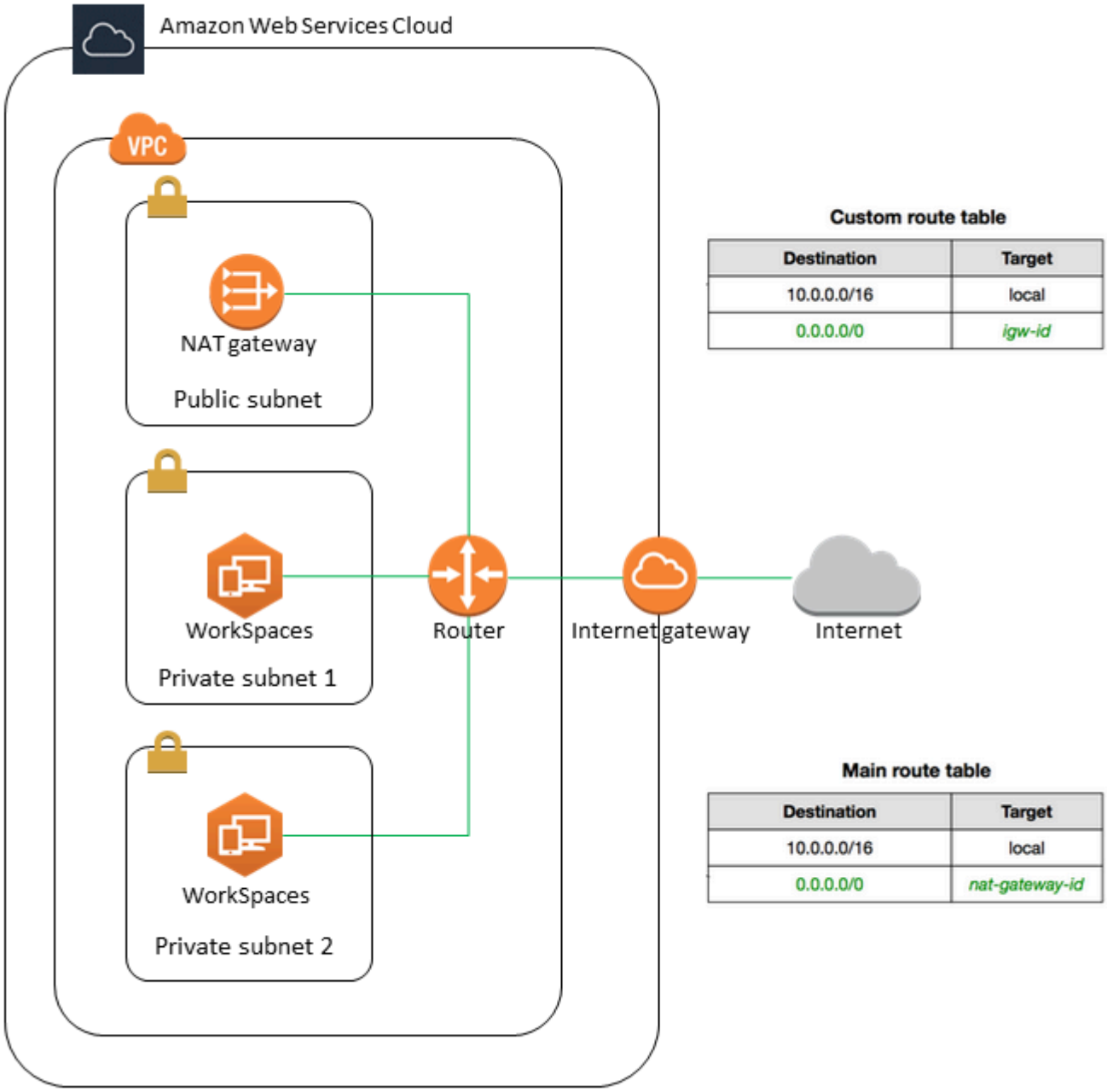
Requisitos

Las subredes de la VPC deben residir en distintas zonas de disponibilidad de la región en la que vaya a realizar el lanzamiento. WorkSpaces Las zonas de disponibilidad son ubicaciones diferentes diseñadas para quedar aisladas en caso de error en otras zonas de disponibilidad. Al lanzar instancias en distintas zonas de disponibilidad, puede proteger sus aplicaciones de los errores que se produzcan en una única ubicación. Cada subred debe residir enteramente en una zona de disponibilidad y no puede abarcar otras zonas.

> **Note**
>
> Amazon WorkSpaces está disponible en un subconjunto de las zonas de disponibilidad de cada región compatible. Para determinar qué zonas de disponibilidad puede usar para las subredes de la VPC WorkSpaces para las que está utilizando, consulte. Zonas de disponibilidad de Amazon WorkSpaces

Configurar una VPC con subredes privadas y una gateway NAT

Si utiliza AWS Directory Service para crear un Microsoft AWS gestionado o un Simple AD, le recomendamos que configure la VPC con una subred pública y dos subredes privadas. Configure su directorio para lanzarlo WorkSpaces en las subredes privadas. Para proporcionar acceso a Internet WorkSpaces en una subred privada, configure una puerta de enlace NAT en la subred pública.



Para crear una VPC con una subred pública y dos subredes privadas

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Crear VPC.
3. En Recursos para crear elija VPC y más.
4. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.

5. Para configurar las subredes, haga lo siguiente:

    a. En Number of Availability Zones (Número de zonas de disponibilidad), elija 1 o 2, según sus necesidades.

    b. Amplíe (Personalizar AZ) y elija sus zonas de disponibilidad. De lo contrario, AWS selecciónelas por usted. Para hacer una selección apropiada, consulte Zonas de disponibilidad de Amazon WorkSpaces.

    c. En Number of public subnets (Número de subredes públicas), asegúrese de tener una subred pública por zona de disponibilidad.

    d. En Number of private subnets (Número de subredes privadas), asegúrese de tener al menos una subred privada por zona de disponibilidad.

    e. Introduzca un bloque CIDR para cada subred. Para obtener más información, consulte Tamaño de subred en la Guía del usuario de Amazon VPC.

6. Para Gateways NAT, elija 1 por AZ.

7. Seleccione Crear VPC.

Bloques CIDR IPv6

Puede asociar bloques de CIDR IPv6 a la VPC y las subredes. Sin embargo, si configura sus subredes para que asignen automáticamente direcciones IPv6 a las instancias lanzadas en la subred, no podrá utilizar los paquetes de Graphics. (Sin embargo, puedes usar Graphics.g4dn, GraphicsPro .g4dn y bundles). GraphicsPro Esta restricción se debe a una limitación de hardware de los tipos de instancia de generaciones anteriores que no son compatibles con IPv6.

Para solucionar este problema, puede deshabilitar temporalmente la configuración de asignación automática de direcciones IPv6 en las WorkSpaces subredes antes de lanzar los paquetes de gráficos y, a continuación, volver a habilitar esta configuración (si es necesario) después de lanzar los paquetes de gráficos para que los demás paquetes reciban las direcciones IP deseadas.

De forma predeterminada, la configuración de asignación automática de direcciones IPv6 está desactivada. Para comprobar esta configuración desde la consola de Amazon VPC, en el panel de navegación, seleccione Subredes. Seleccione la subred y elija Actions (Acciones), Modify auto-assign IP settings (Modificar la configuración de la asignación automática de IP).

Configurar una VPC con subredes públicas

Si lo prefiere, puede crear una VPC con dos subredes públicas. Para proporcionar acceso a Internet a las WorkSpaces subredes públicas, configure el directorio para que asigne direcciones IP elásticas automáticamente o asigne manualmente una dirección IP elástica a cada una de ellas. WorkSpace

Tareas

- Paso 1: Crear una VPC
- Paso 2: Asigne direcciones IP públicas a su WorkSpaces

Paso 1: Crear una VPC

Cree una VPC con una subred pública como se indica a continuación.

Para crear la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Crear VPC.
3. En Recursos para crear elija VPC y más.
4. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.
5. Para configurar las subredes, haga lo siguiente:
    a. Para Número de zonas de disponibilidad, elija 2.
    b. Amplíe Personalizar AZ y elija sus zonas de disponibilidad. De lo contrario, AWS selecciónelas por usted. Para hacer una selección apropiada, consulte Zonas de disponibilidad de Amazon WorkSpaces.
    c. Para Número de subredes públicas, elija 2.
    d. Para Number of private subnets (Número de subredes privadas), elija 0.
    e. Introduzca un bloque CIDR para cada subred pública. Para obtener más información, consulte Tamaño de subred en la Guía del usuario de Amazon VPC.
6. Seleccione Crear VPC.

Bloques CIDR IPv6

Puede asociar un bloque de CIDR IPv6 a la VPC y las subredes. Sin embargo, si configura sus subredes para que asignen automáticamente direcciones IPv6 a las instancias lanzadas en la

subred, no podrá utilizar los paquetes de Graphics. (Sin embargo, puedes usar GraphicsPro paquetes). Esta restricción se debe a una limitación de hardware de los tipos de instancia de generaciones anteriores que no son compatibles con IPv6.

Para solucionar este problema, puede deshabilitar temporalmente la configuración de asignación automática de direcciones IPv6 en las WorkSpaces subredes antes de lanzar los paquetes de gráficos y, a continuación, volver a habilitar esta configuración (si es necesario) después de lanzar los paquetes de gráficos para que los demás paquetes reciban las direcciones IP deseadas.

De forma predeterminada, la configuración de asignación automática de direcciones IPv6 está desactivada. Para comprobar esta configuración desde la consola de Amazon VPC, en el panel de navegación, seleccione Subredes. Seleccione la subred y elija Actions (Acciones), Modify auto-assign IP settings (Modificar la configuración de la asignación automática de IP).

Paso 2: Asigne direcciones IP públicas a su WorkSpaces

Puede asignarle direcciones IP públicas de WorkSpaces forma automática o manual. Para utilizar la asignación automática, consulte the section called “Configurar direcciones IP públicas automáticas”. Para asignar direcciones IP públicas manualmente, utilice el siguiente procedimiento.

Para asignar una dirección IP pública a una de WorkSpace forma manual

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Amplíe la fila (elija el icono de flecha) para WorkSpace y anote el valor de WorkSpace IP. Esta es la dirección IP privada principal del WorkSpace.
4. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
5. En el panel de navegación, elija Direcciones IP elásticas. Si no tiene una dirección IP elástica disponible, elija Asignar dirección IP elástica y, a continuación, Grupo de direcciones IPv4 de Amazon o Grupo de direcciones IPv4 propiedad del cliente. Después, seleccione Asignar. Anote la nueva dirección IP.
6. En el panel de navegación, elija Interfaces de red.
7. Seleccione la interfaz de red para su WorkSpace. Para encontrar la interfaz de red adecuada para usted WorkSpace, introduzca el valor de WorkSpace IP (que ha indicado anteriormente) en el cuadro de búsqueda y, a continuación, pulse Entrar. El valor WorkSpace IP coincide con la dirección IPv4 privada principal de la interfaz de red. Tenga en cuenta que el ID de VPC de la interfaz de red coincide con el ID de su WorkSpaces VPC.

8. Elija Acciones, Administrar direcciones IP. Elija Assign new IP (Asignar nueva IP) y, a continuación, elija Yes, Update (Sí, actualizar). Anote la nueva dirección IP.
9. Elija Actions, Associate Address.
10. En la página Associate Elastic IP Address (Asociar dirección IP elástica), elija una dirección IP elástica en Address (Dirección). En Associate to private IP address (Asociar a dirección IP privada), especifique la nueva dirección IP privada y, a continuación, elija Associate Address (Asociar dirección).

Zonas de disponibilidad de Amazon WorkSpaces

Al crear una nube privada virtual (VPC) para usarla con Amazon WorkSpaces, las subredes de la VPC deben residir en distintas zonas de disponibilidad de la región en la que vaya a realizar el lanzamiento. WorkSpaces Las zonas de disponibilidad son ubicaciones diferentes diseñadas para quedar aisladas en caso de error en otras zonas de disponibilidad. Al lanzar instancias en distintas zonas de disponibilidad, puede proteger sus aplicaciones de los errores que se produzcan en una única ubicación. Cada subred debe residir enteramente en una zona de disponibilidad y no puede abarcar otras zonas.

Una zona de disponibilidad está representada por un código de región seguido de un identificador de letra; por ejemplo, `us-east-1a`. Para garantizar que los recursos se distribuyan entre las zonas de disponibilidad de una región, asignamos las zonas de disponibilidad de forma independiente a los nombres de cada cuenta. AWS Por ejemplo, es posible que la zona `us-east-1a` de disponibilidad de su AWS cuenta no sea la misma ubicación que la `us-east-1a` de otra AWS cuenta.

Para coordinar las zonas de disponibilidad entre cuentas, debe usar el ID de AZ, que es un identificador único y constante de una zona de disponibilidad. Por ejemplo, `use1-az2` es un ID de zona geográfica para la `us-east-1` región y tiene la misma ubicación en todas las AWS cuentas.

La visualización de los ID de zona de disponibilidad le permite determinar la ubicación de los recursos de una cuenta en relación con los recursos de otra cuenta. Por ejemplo, si comparte una subred en la zona de disponibilidad con el ID de AZ `use1-az2` con otra cuenta, esta subred está disponible para dicha cuenta de la zona de disponibilidad cuyo ID de zona de disponibilidad es también `use1-az2`. El ID de zona de disponibilidad para cada VPC y subred aparece en la consola de Amazon VPC.

Amazon solo WorkSpaces está disponible en un subconjunto de las zonas de disponibilidad de cada región compatible. En la siguiente tabla, se enumeran los ID de AZ que puede usar para cada región.

Para ver la asignación de ID de AZ a las zonas de disponibilidad de su cuenta, consulte ID de AZ de sus recursos en la Guía del usuario de AWS RAM .

Nombre de la región	Código de región	ID de AZ admitidos
Este de EE. UU. (Norte de Virginia)	us-east-1	use1-az2, use1-az4, use1-az6
Oeste de EE. UU. (Oregón)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asia-Pacífico (Bombay)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
Asia-Pacífico (Seúl)	ap-northeast-2	apne2-az1 , apne2-az3
Asia-Pacífico (Singapur)	ap-southeast-1	apse1-az1 , apse1-az2
Asia-Pacífico (Sídney)	ap-southeast-2	apse2-az1 , apse2-az3
Asia-Pacífico (Tokio)	ap-northeast-1	apne1-az1 , apne1-az4
Canadá (centro)	ca-central-1	cac1-az1, cac1-az2
Europa (Fráncfort)	eu-central-1	euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (Londres)	eu-west-2	euw2-az2, euw2-az3
América del Sur (São Paulo)	sa-east-1	sae1-az1, sae1-az3
África (Ciudad del Cabo)	af-south-1	afs1-az1, afs1-az2, afs1-az3
Israel (Tel Aviv)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3

Nombre de la región	Código de región	ID de AZ admitidos
AWS GovCloud (EE. UU.-Oeste)	`us-gov-west-1`	`usgw1-az1` , `usgw1-az2` , `usgw1-az3`
AWS GovCloud (EEUU-Este)	`us-gov-east-1`	`usge1-az1` , `usge1-az2` , `usge1-az3`

Para obtener más información sobre las zonas de disponibilidad y los ID de zona de disponibilidad, consulte Regiones, zonas de disponibilidad y zonas locales en la Guía del usuario de Amazon EC2.

Requisitos de dirección IP y puerto para WorkSpaces

Para conectarse a la suya WorkSpaces, la red a la que estén conectados sus WorkSpaces clientes debe tener ciertos puertos abiertos a los rangos de direcciones IP de los distintos AWS servicios (agrupados en subconjuntos). Estos rangos de direcciones varían en función de la región de AWS. Estos puertos también deben estar abiertos en los firewalls que se ejecuten en el cliente. Para obtener más información sobre los intervalos de direcciones IP de AWS en diferentes regiones, consulte Intervalos de direcciones IP de AWS en la Referencia general de Amazon Web Services.

Para ver un diagrama de arquitectura, consulte WorkSpaces Arquitectura. Para ver diagramas de arquitectura adicionales, consulte Best Practices for Deplying Amazon WorkSpaces.

Puertos de aplicaciones cliente

La aplicación WorkSpaces cliente requiere acceso saliente en los siguientes puertos:

Puerto 53 (UDP)

> Este puerto se utiliza para acceder a los servidores DNS. Debe estar abierto para las direcciones IP del servidor DNS, de modo que el cliente pueda resolver los nombres de dominio público. Si no se utilizan servidores DNS para resolver nombres de dominio, este puerto es opcional.

Puerto 443 (TCP)

> Este puerto se utiliza para las actualizaciones, el registro y la autenticación de las aplicaciones cliente. Las aplicaciones cliente de escritorio pueden usar un servidor proxy para el tráfico del puerto 443 (HTTPS). Para habilitar el uso de un servidor proxy, abra la aplicación cliente, elija

Advanced Settings, seleccione Use Proxy Server, especifique la dirección y el puerto del servidor proxy, y elija Save.

Este puerto debe estar abierto para los siguientes intervalos de direcciones IP:

- El subconjunto `AMAZON` de la región `GLOBAL`.
- El `AMAZON` subconjunto de la región en la que WorkSpace se encuentra.
- El subconjunto `AMAZON` de la región `us-east-1`.
- El subconjunto `AMAZON` de la región `us-west-2`.
- El subconjunto `S3` de la región `us-west-2`.

Puerto 4172 (UDP y TCP)

Este puerto se utiliza para transmitir el WorkSpace escritorio y comprobar el estado del WorkSpaces PCoIP. Este puerto debe estar abierto a la puerta de enlace PCoIP y a los servidores de comprobación de estado de la región en la que se encuentra. WorkSpace Para obtener más información, consulte Servidores de comprobación de estado y Servidores de puerta de enlace PCoIP.

En el caso del PCoIP WorkSpaces, las aplicaciones cliente de escritorio no admiten el uso de un servidor proxy ni el descifrado ni la inspección mediante TLS del tráfico del puerto 4172 en UDP (para el tráfico de escritorio). Necesitan una conexión directa a los puertos 4172.

Puerto 4195 (UDP y TCP)

Este puerto se utiliza para transmitir el WorkSpace escritorio y comprobar el estado del Streaming Protocol (WSP WorkSpaces). WorkSpaces Este puerto debe estar abierto a los rangos de direcciones IP de WSP Gateway y a los servidores de comprobación de estado de la región en la que WorkSpace se encuentra. Para obtener más información, consulte Servidores de comprobación de estado y Servidores de puerta de enlace WSP.

Para WSP WorkSpaces, la aplicación cliente WorkSpaces Windows (versión 5.1 y superior) y la aplicación cliente macOS (versión 5.4 y superior) admiten el uso de servidores proxy HTTP para el tráfico TCP del puerto 4195, pero no se recomienda el uso de un proxy. No se admiten el descifrado ni la inspección por TLS. Para obtener más información, consulte Configurar los ajustes del servidor proxy del dispositivo para el acceso a Internet en Windows WorkSpaces WorkSpaces, Amazon Linux y Ubuntu WorkSpaces.

> **Note**
>
> - Si el firewall utiliza filtros con estado, los puertos efímeros (también conocidos como puertos dinámicos) se abren automáticamente para permitir la comunicación de retorno. Si el firewall utiliza filtros sin estado, debe abrir los puertos efímeros explícitamente para permitir la comunicación de retorno. El intervalo de puertos efímeros que debe abrirse variará en función de la configuración.
> - La característica de servidor proxy no es compatible con el tráfico UDP. Si eliges usar un servidor proxy, las llamadas a la API que la aplicación cliente realiza a los WorkSpaces servicios de Amazon también se envían mediante proxy. Tanto las llamadas a la API como el tráfico de escritorio deben pasar por el mismo servidor proxy.

Puertos para Acceso web

WorkSpaces El acceso web requiere acceso saliente a los siguientes puertos:

Puerto 53 (UDP)

Este puerto se utiliza para acceder a los servidores DNS. Debe estar abierto para las direcciones IP del servidor DNS, de modo que el cliente pueda resolver los nombres de dominio público. Si no se utilizan servidores DNS para resolver nombres de dominio, este puerto es opcional.

Puerto 80 (UDP y TCP)

Este puerto se utiliza para las conexiones iniciales a `https://clients.amazonworkspaces.com` y, a continuación, cambia a HTTPS. Debe estar abierto a todos los rangos de direcciones IP del `EC2` subconjunto de la región en la que WorkSpace se encuentra.

Puerto 443 (UDP y TCP)

Este puerto se utiliza para el registro y la autenticación a través de HTTPS. Debe estar abierto a todos los rangos de direcciones IP del `EC2` subconjunto de la región en la que WorkSpace se encuentra.

Puerto 4195 (UDP y TCP)

Si WorkSpaces están configurados para el Protocolo de WorkSpaces Transmisión (WSP), este puerto se usa para transmitir el tráfico de WorkSpaces escritorio. Este puerto debe estar abierto

para los siguientes intervalos de direcciones IP de la puerta de enlace de WSP. Para obtener más información, consulte Servidores de puerta de enlace WSP.

El acceso web WSP admite el uso de un servidor proxy para el tráfico TCP del puerto 4195, pero no se recomienda. Para obtener más información, consulte Configurar los ajustes del servidor proxy del dispositivo para el acceso a Internet en Windows WorkSpaces WorkSpaces, Amazon Linux y Ubuntu WorkSpaces.

> **Note**
>
> Si el firewall utiliza filtros con estado, los puertos efímeros (también conocidos como puertos dinámicos) se abren automáticamente para permitir la comunicación de retorno. Si el firewall utiliza filtros sin estado, debe abrir los puertos efímeros explícitamente para permitir la comunicación de retorno. El intervalo de puertos efímeros que debe abrirse variará en función de la configuración.

Por lo general, el navegador web selecciona aleatoriamente un puerto de origen en el rango alto para usarlo como tráfico de streaming. WorkSpaces Web Access no controla el puerto que selecciona el navegador. Debe asegurarse de que el tráfico de retorno a este puerto esté permitido.

Dominios y direcciones IP para agregar a la lista de permitidos

Para que la aplicación WorkSpaces cliente pueda acceder al WorkSpaces servicio, debe agregar los siguientes dominios y direcciones IP a la lista de dominios permitidos en la red desde la que el cliente intenta acceder al servicio.

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Dominio o dirección IP
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	• https://d2td7dqidlhjx7.cloudfront.net/ • En la región AWS GovCloud (EE. UU. Oeste): https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ 64.xml WorkSpacesAppCastx

Categoría	Dominio o dirección IP
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/

Categoría	Dominio o dirección IP
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominios: • https://.us-east-1.amazonaws.com skylight-client-ds • skylight-client-dshttps://.us-west-2.amazonaws.com • skylight-client-dshttps://.ap-south-1.amazonaws.com • skylight-client-dshttps://.ap-northeast-2.amazonaws.com • skylight-client-dshttps://.ap-southeast-1.amazonaws.com • skylight-client-dshttps://.ap-southeast-2.amazonaws.com • skylight-client-dshttps://.ap-northeast-1.amazonaws.com • skylight-client-dshttps://.ca-central-1.amazonaws.com • skylight-client-dshttps://.eu-central-1.amazonaws.com • skylight-client-dshttps://.eu-west-1.amazonaws.com • skylight-client-dshttps://.eu-west-2.amazonaws.com • skylight-client-dshttps://.sa-east-1.amazonaws.com • skylight-client-dshttps://.af-south-1.amazonaws.com • skylight-client-dshttps://.il-central-1.amazonaws.com • En la región (EE. UU.-Oeste): AWS GovCloud

Categoría	Dominio o dirección IP
	https://skylight-client-ds. us-gov-west-1.amazonaws.com • En la región AWS GovCloud (este de EE. UU.): https://skylight-client-ds. us-gov-east-1.amazonaws.com

Categoría	Dominio o dirección IP
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o superior) WorkSpaces	Dominios: • https://.us-east-1.amazonaws.com ws-client-service • ws-client-servicehttps://.us-west-2.amazonaws.com • ws-client-servicehttps://.ap-south-1.amazonaws.com • ws-client-servicehttps://.ap-northeast-2.amazonaws.com • ws-client-servicehttps://.ap-southeast-1.amazonaws.com • ws-client-servicehttps://.ap-southeast-2.amazonaws.com • ws-client-servicehttps://.ap-northeast-1.amazonaws.com • ws-client-servicehttps://.ca-central-1.amazonaws.com • ws-client-servicehttps://.eu-central-1.amazonaws.com • ws-client-servicehttps://.eu-west-1.amazonaws.com • ws-client-servicehttps://.eu-west-2.amazonaws.com • ws-client-servicehttps://.sa-east-1.amazonaws.com • ws-client-servicehttps://.af-south-1.amazonaws.com • ws-client-servicehttps://.il-central-1.amazonaws.com • En la región (EE. UU.-Oeste): AWS GovCloud

Categoría	Dominio o dirección IP
	https://ws-client-service. us-gov-west-1.amazonaws.com • En la región AWS GovCloud (este de EE. UU.): https://ws-client-service. us-gov-east-1.amazonaws.com

Categoría	Dominio o dirección IP
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/*<región>*/*<ID del directorio>* Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • Heredado: https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> • Este de EE. UU. (Norte de Virginia): https://d2h1yryv1jxiq.cloudfront.net/ • Oeste de EE. UU. (Oregón): https://d1fq42e1gi7rtq.cloudfront.net/ • Asia-Pacífico (Bombay): https://d1ctsk4u02kky7.cloudfront.net/ • Asia-Pacífico (Seúl): https://dyoj3cw6iktvg.cloudfront.net • Asia-Pacífico (Singapur): https://d1525ef92caquk.cloudfront.net/ • Asia-Pacífico (Sídney): https://dodwxjr2amr8p.cloudfront.net/

Categoría	Dominio o dirección IP
	• Asia-Pacífico (Tokio): https://d3v7kcib8ir2e1.cloudfront.net/ • Canadá (centro): https://d1ebdk07rro1qy.cloudfront.net/ • UE (Fráncfort): https://d39q4y7cndearu.cloudfront.net/ • UE (Irlanda): https://d2127w6wvrc6l3.cloudfront.net/ • Europa (Londres): https://df4ahgpxbxqy2.cloudfront.net/ • América del Sur (São Paulo): https://d2nezqurrjvain.cloudfront.net/ • África (Ciudad del Cabo): https://dr6ry0pwaoy23.cloudfront.net • Israel (Tel Aviv) — https://d2kmf63k5sit88.cloudfront.net Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Este de EE. UU. (Norte de Virginia): https://d32i4gd7pg4909.cloudfront.net/ • Oeste de EE. UU. (Oregón): https://d18af777lco7lp.cloudfront.net/ • Asia-Pacífico (Bombay): https://d78hovzzqqtsb.cloudfront.net/

Categoría	Dominio o dirección IP
	• Asia-Pacífico (Seúl): https://dtyv4uwoh7ynt.cloudfront.net/ • Asia-Pacífico (Singapur): https://d3qzmd7y07pz0i.cloudfront.net/ • Asia-Pacífico (Sídney): https://dwcpoxuuza83q.cloudfront.net/ • Asia-Pacífico (Tokio): https://d2c2t8mxjhq5z1.cloudfront.net/ • Canadá (centro): https://d2wfbsypmqjmog.cloudfront.net/ • UE (Fráncfort): https://d1whcm49570jjw.cloudfront.net/ • UE (Irlanda): https://d3pgffbf39h4k4.cloudfront.net/ • Europa (Londres): https://d16q6638mh01s7.cloudfront.net/ • América del Sur (São Paulo): https://d2lh2qc5bdoq4b.cloudfront.net/ • África (Ciudad del Cabo): https://di5ygl2cs0mrh.cloudfront.net/ • Israel (Tel Aviv) — https://d1a3pnge9on3sx.cloudfront.net En AWS GovCloud la región (EEUU-Oeste): • Configuración de directorios de clientes: https://s3.amazonaws.com/ /prod/pdt/workspaces-client-properties <directory ID> • Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente:

Categoría	Dominio o dirección IP
	https://.s3- -1.amazonaws.com workspace-client-assets-pdt us-gov-west • Archivo CSS para el estilo de las páginas de inicio de sesión: workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css • JavaScript archivo para las páginas de inicio de sesión: No aplicable En la región AWS GovCloud (EE. UU.-Este): • Configuración de directorios de clientes: https://s3.amazonaws.com/ /prod/osu/ workspaces-client-properties <directory ID> • Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: https://.s3- -1.amazonaws.com workspace-client-assets-pdt us-gov-east • Archivo CSS para el estilo de las páginas de inicio de sesión: workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css • JavaScript archivo para las páginas de inicio de sesión: No aplicable
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Dominio o dirección IP
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin. amazonaws-us-gov.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente) En las regiones AWS GovCloud (EE. UU. Oeste) y AWS GovCloud (EE. UU. Este): https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(donde está el dominio del cliente)

Categoría	Dominio o dirección IP
Agente de WS	Dominios: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com • ws-broker-servicehttps://.ap-south-1.amazonaws.com • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com • ws-broker-servicehttps://.ca-central-1.amazonaws.com • ws-broker-servicehttps://.eu-central-1.amazonaws.com • ws-broker-servicehttps://.eu-west-1.amazonaws.com • ws-broker-servicehttps://.eu-west-2.amazonaws.com • ws-broker-servicehttps://.sa-east-1.amazonaws.com • ws-broker-servicehttps://.af-south-1.amazonaws.com

Categoría	Dominio o dirección IP
	• ws-broker-servicehttps://.il-central-1.amazonaws.com • httpsws-broker-service://. us-gov-west-1.amazonaws.com • https://. ws-broker-service-fips us-gov-west-1.amazonaws.com • https://. ws-broker-service us-gov-east-1.amazonaws.com • https://. ws-broker-service-fips us-gov-east-1.amazonaws.com

Categoría	Dominio o dirección IP
WorkSpaces Puntos finales de la API	Dominios: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

Categoría	Dominio o dirección IP
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com

Categoría	Dominio o dirección IP
WorkSpaces Puntos de conexión para el inicio de sesión único (SSO) de SAML	Dominios: • euc-sso-smhttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-east-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-sm-fipshttps://.us-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-southeast-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.ap-northeast-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-central-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.eu-west-2.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.af-south-1.amazonaws.com/v1/report-heartbeat • euc-sso-smhttps://.il-central-1.amazonaws.com/v1/report-heartbeat • httpseuc-sso-sm://. us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://. euc-sso-sm-fips us-gov-west-1.amazonaws.com/v1/report-heartbeat

Categoría	Dominio o dirección IP
	• https://. euc-sso-sm us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://. euc-sso-sm-fips us-gov-east-1.amazonaws.com/v1/report-heartbeat

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Dominio o dirección IP
Gateway de sesión PCoIP (PSG)	Servidores de puerta de enlace PCoIP
Agente de sesiones (PCM)	Dominios: • https://skylight-cm.us-east-1.amazonaws.com • https://.us-east-1.amazonaws.com skylight-cm-fips • https://skylight-cm.us-west-2.amazonaws.com • skylight-cm-fipshttps://.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

Categoría	Dominio o dirección IP
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm. us-gov-west-1.amazonaws.com • https://. skylight-cm-fips us-gov-west-1.amazonaws.com • https://skylight-cm. us-gov-east-1.amazonaws.com • https://. skylight-cm-fips us-gov-east-1.amazonaws.com

Categoría	Dominio o dirección IP
Servidores TURN de Acceso web para PCoIP	Servidores: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Acceso web no está disponible actualmente en la región Asia Pacífico (Bombay) • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • El acceso a la web no está disponible actualmente en la región de África (Ciudad del Cabo) • El acceso a la web no está disponible actualmente en la región de Israel (Tel Aviv).

Dominios y direcciones IP para añadir a tu lista de dominios permitidos para el Protocolo de WorkSpaces Transmisión (WSP)

Categoría	Dominio o dirección IP
Puerta de enlace de sesión WSP (WSG)	Servidores de puerta de enlace WSP
Servidores TURN de Acceso web para WSP	Servidores de puerta de enlace WSP

Servidores de comprobación de estado

Las aplicaciones WorkSpaces cliente realizan comprobaciones de estado en los puertos 4172 y 4195. Estas comprobaciones validan si el tráfico TCP o UDP fluye desde los WorkSpaces servidores a las aplicaciones cliente. Para que estas comprobaciones se realicen correctamente, las políticas de firewall deben permitir el tráfico saliente a las direcciones IP de los siguientes servidores regionales de comprobación de estado.

Región	El nombre del host de comprobación de estado	Direcciones IP
Este de EE. UU. (Norte de Virginia)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
Oeste de EE. UU. (Oregón)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
Asia-Pacífico (Bombay)	drp-bom.amazonworkspaces.com	13.127.57.82 13,234250,73
Asia-Pacífico (Seúl)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105

Región	El nombre del host de comprobación de estado	Direcciones IP
		52.78.44.253 52.79.54.102
Asia-Pacífico (Singapur)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
Asia-Pacífico (Sídney)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
Asia-Pacífico (Tokio)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
Canadá (Centro)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
Europa (Fráncfort)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227

Región	El nombre del host de comprobación de estado	Direcciones IP
Europa (Irlanda)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
Europa (Londres)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
América del Sur (São Paulo)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
África (Ciudad del Cabo)	drp-cpt.amazonworkspaces.com/	13,244128155 13,245,205255 13,245216116
Israel (Tel Aviv)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51,17109231 51,16190,43

Región	El nombre del host de comprobación de estado	Direcciones IP
AWS GovCloud (US-Oeste)	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88
AWS GovCloud (EE. UU.-Este)	drp-osu.amazonworkspaces.com	18.253,251,70 18,254,0118

Servidores de puerta de enlace PCoIP

WorkSpaces usa PCoIP para transmitir la sesión de escritorio a los clientes a través del puerto 4172. Para sus servidores de puerta de enlace PCoIP, WorkSpaces utiliza un pequeño rango de direcciones IPv4 públicas de Amazon EC2. Esto permite establecer políticas de firewall más detalladas para los dispositivos que obtienen acceso a WorkSpaces. Tenga en cuenta que los WorkSpaces clientes no admiten direcciones IPv6 como opción de conectividad en este momento.

Región	Intervalo de direcciones IP públicas
Este de EE. UU. (Norte de Virginia)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
Oeste de EE. UU. (Oregón)	35.80.88.0 - 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255

Región	Intervalo de direcciones IP públicas
Asia-Pacífico (Bombay)	13126,243,0 - 13126,243,255
Asia-Pacífico (Seúl)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
Asia-Pacífico (Singapur)	18.141.152,0 - 18.141.152.255 18.141.154,0 - 18.141.155.255 52.76.127.0 - 52.76.127.255
Asia-Pacífico (Sídney)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
Asia-Pacífico (Tokio)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
Canadá (Centro)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
Europa (Fráncfort)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
Europa (Irlanda)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255

Región	Intervalo de direcciones IP públicas
Europa (Londres)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
América del Sur (São Paulo)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
África (Ciudad del Cabo)	13,246,120,0 - 13,246,123255
Israel (Tel Aviv)	51,17,28,0-51,17,31,255
AWS GovCloud (US-Oeste)	52.61.193.0 - 52.61.193.255
AWS GovCloud (EE. UU.-Este)	18.254.140.0 - 18.254.143.255

Servidores de puerta de enlace WSP

> **Important**
>
> A partir de junio de 2020, WorkSpaces transmite la sesión de escritorio de WSP WorkSpaces a los clientes a través del puerto 4195 en lugar del puerto 4172. Si desea utilizar WSP WorkSpaces, asegúrese de que el puerto 4195 esté abierto al tráfico.

WorkSpaces utiliza un pequeño rango de direcciones IPv4 públicas de Amazon EC2 para sus servidores de puerta de enlace WSP. Esto permite establecer políticas de firewall más detalladas para los dispositivos que obtienen acceso a WorkSpaces. Tenga en cuenta que los WorkSpaces clientes no admiten direcciones IPv6 como opción de conectividad en este momento.

Región	Intervalo de direcciones IP públicas
Este de EE. UU. (Norte de Virginia)	• 3.227.4.0/22

Región	Intervalo de direcciones IP públicas
	• 4420984,0/22
Oeste de EE. UU. (Oregón)	34,223,96,0/22
Asia-Pacífico (Bombay)	65,1156,0/22
Asia-Pacífico (Seúl)	3,35,160,0/22
Asia-Pacífico (Singapur)	13,212.132,0/22
Asia-Pacífico (Sídney)	3,25248,0/22
Asia-Pacífico (Tokio)	3,114,164,0/22
Canadá (Centro)	3,97,20,0/22
Europa (Fráncfort)	18,192216,0/22
Europa (Irlanda)	3,248,176,0/22
Europa (Londres)	18,3468,0/22
América del Sur (São Paulo)	15228,64,0/22
África (Ciudad del Cabo)	13,246,6108,0/22
Israel (Tel Aviv)	5117,72,0/22
AWS GovCloud (Estados Unidos-Oeste)	• 3.32.139,0/24 • 3,30129,0/24 • 3,30,130,0/23
AWS GovCloud (Este de EE. UU.)	18,254.148,0/22

Nombres de dominio de la puerta de enlace WSP

La siguiente tabla muestra los nombres de dominio de la WorkSpace puerta de enlace WSP. Estos dominios deben ser accesibles para que la aplicación WorkSpaces cliente pueda acceder al servicio WorkSpace WSP.

Región	Dominio
Este de EE. UU. (Norte de Virginia)	*.prod.us-east-1.highlander.aws.a2z.com
Oeste de EE. UU. (Oregón)	*.prod.us-west-2.highlander.aws.a2z.com
Asia-Pacífico (Bombay)	*.prod.ap-south-1.highlander.aws.a2z.com
Asia-Pacífico (Seúl)	*.prod.ap-northeast-2.highlander.aws.a2z.com
Asia-Pacífico (Singapur)	*.prod.ap-southeast-1.highlander.aws.a2z.com
Asia-Pacífico (Sídney)	*.prod.ap-southeast-2.highlander.aws.a2z.com
Asia-Pacífico (Tokio)	*.prod.ap-northeast-1.highlander.aws.a2z.com
Canadá (Centro)	*.prod.ca-central-1.highlander.aws.a2z.com
Europa (Fráncfort)	*.prod.eu-central-1.highlander.aws.a2z.com
Europa (Irlanda)	*.prod.eu-west-1.highlander.aws.a2z.com
Europa (Londres)	*.prod.eu-west-2.highlander.aws.a2z.com
América del Sur (São Paulo)	*.prod.sa-east-1.highlander.aws.a2z.com
África (Ciudad del Cabo)	*.prod.af-south-1.highlander.aws.a2z.com
Israel (Tel Aviv)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud (US-Oeste)	*.prod. us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud (Este de EE. UU.)	*.prod. us-gov-east-1.highlander.aws.a2z.com

Interfaces de red

Cada uno tiene las siguientes interfaces de red: WorkSpace

- La interfaz de red principal (eth1) proporciona conectividad a los recursos de la VPC y de Internet, y se utiliza para unirlos al WorkSpace directorio.
- La interfaz de red de administración (eth0) se conecta a una red de administración segura de WorkSpaces. Se utiliza para la transmisión interactiva del WorkSpace escritorio a WorkSpaces los clientes y para WorkSpaces permitir la administración del. WorkSpace

WorkSpaces selecciona la dirección IP para la interfaz de red de administración entre varios rangos de direcciones, según la región en la que WorkSpaces se hayan creado. Cuando se registra un directorio, WorkSpaces comprueba el CIDR de la VPC y las tablas de enrutamiento de la VPC para determinar si estos rangos de direcciones crean un conflicto. Si se encuentra un conflicto en todos los rangos de direcciones disponibles en la región, se muestra un mensaje de error y el directorio no se registra. Si cambia las tablas de ruteo en la VPC después de registrar el directorio, puede provocar un conflicto.

> **Warning**
>
> No modifique ni elimine ninguna de las interfaces de red que están conectadas a un. WorkSpace Si lo hace, podría resultar inalcanzable o perder el acceso a Internet. WorkSpace Por ejemplo, si ha habilitado la asignación automática de direcciones IP elásticas a nivel de directorio, se le asignará una dirección IP elástica (del grupo proporcionado por Amazon) WorkSpace cuando se lance. Sin embargo, si asocias una dirección IP elástica de tu propiedad a una y WorkSpace, posteriormente, desasocias esa dirección IP elástica de la WorkSpace, WorkSpace pierde su dirección IP pública y no obtiene automáticamente una nueva del grupo proporcionado por Amazon.
> Para asociar una nueva dirección IP pública del grupo proporcionado por Amazon al WorkSpace, debes volver a crear el. WorkSpace Si no quiere volver a crear el WorkSpace, debe asociar otra dirección IP elástica de su propiedad al. WorkSpace

Intervalos de IP de la interfaz de administración

En la siguiente tabla se muestran los rangos de direcciones IP para la interfaz de red de administración.

Note

- Si utiliza Bring Your Own License (BYOL) en Windows WorkSpaces, no se aplican los rangos de direcciones IP de la siguiente tabla. En su lugar, el BYOL de PCoIP WorkSpaces utiliza el rango de direcciones IP 54.239.224.0/20 para el tráfico de la interfaz de administración en todas las regiones. AWS Para Windows WSP BYOL, los rangos de direcciones IP 54.239.224.0/20 y WorkSpaces 10.0.0.0/8 se aplican en todas las regiones. AWS (Estos rangos de direcciones IP se utilizan además del bloque CIDR /16 que se selecciona para administrar el tráfico de su BYOL). WorkSpaces
- Si utiliza un WSP WorkSpaces creado a partir de paquetes públicos, el rango de direcciones IP 10.0.0.0/8 también se aplica al tráfico de la interfaz de administración en todas AWS las regiones, además de los rangos PCoIP/WSP que se muestran en la siguiente tabla.

Región	Rango de direcciones IP
Este de EE. UU. (Norte de Virginia)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 WSP: 10.0.0.0/8
Oeste de EE. UU. (Oregón)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 y 198.19.0.0/16 WSP: 10.0.0.0/8
Asia-Pacífico (Bombay)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
Asia-Pacífico (Seúl)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Asia-Pacífico (Singapur)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Región	Rango de direcciones IP
Asia-Pacífico (Sídney)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 y 198.19.0.0/16 WSP: 10.0.0.0/8
Asia-Pacífico (Tokio)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Canadá (Centro)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Fráncfort)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Irlanda)	PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 y 198.19.0.0/16 WSP: 10.0.0.0/8
Europa (Londres)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
América del Sur (São Paulo)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
África (Ciudad del Cabo)	PCoIP/WSP: 172.31.0.0/16 y 198.19.0.0/16 WSP: 10.0.0.0/8
Israel (Tel Aviv)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Región	Rango de direcciones IP
AWS GovCloud (EE. UU.-Oeste)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8 y 192.169.0.0/16
AWS GovCloud (EE. UU.-Este)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

Puertos de la interfaz de administración

Todos WorkSpaces los puertos siguientes deben estar abiertos en la interfaz de red de administración:

- TCP de entrada en el puerto 4172. Se utiliza para establecer la conexión de streaming en el protocolo PCoIP.
- UDP de entrada en el puerto 4172. Se usa para transmitir las entradas del usuario en el protocolo PCoIP.
- TCP de entrada en el puerto 4489. Se usa para el acceso mediante el cliente web.
- TCP de entrada en el puerto 8200. Se utiliza para la administración y configuración del WorkSpace.
- TCP de entrada en los puertos 8201 a 8250. Estos puertos se utilizan para establecer la conexión de streaming y para transmitir las entradas del usuario en el protocolo WSP.
- UDP de entrada en el puerto 8220. Este puerto se utiliza para establecer la conexión de streaming y para transmitir las entradas del usuario en el protocolo WSP
- TCP de salida en los puertos 8443 y 9997. Se usa para el acceso mediante el cliente web.
- UDP de salida en los puertos 3478, 4172 y 4195. Se usa para el acceso mediante el cliente web.
- UDP de salida en los puertos 50002 y 55002. Se utiliza para streaming. Si el firewall utiliza filtrado con estado, se abre automáticamente los puertos efímeros 50002 y 55002 para permitir la comunicación de retorno. Si el firewall utiliza filtros sin estado, debe abrir los puertos efímeros 49152 - 65535 para permitir la comunicación de retorno.
- El TCP saliente del puerto 80, tal como se define en los rangos de IP de la interfaz de administración, a la dirección IP 169.254.169.254 para acceder al servicio de metadatos de EC2. Cualquier proxy HTTP que se le asigne también debe excluir 169.254.169.254. WorkSpaces

- TCP de salida en el puerto 1688 a direcciones IP 169.254.169.250 y 169.254.169.251 para permitir el acceso a la activación de Microsoft KMS for Windows para los Workspaces basados en paquetes públicos. Si utiliza Bring Your Own License (BYOL) para Windows WorkSpaces, debe permitir el acceso a sus propios servidores KMS para la activación de Windows.
- TCP saliente en el puerto 1688 a la dirección IP 54.239.236.220 para permitir el acceso a Microsoft KMS para la activación de Office para BYOL. WorkSpaces

  Si usa Office a través de uno de los paquetes WorkSpaces públicos, la dirección IP para la activación de Microsoft KMS for Office varía. Para determinar esa dirección IP, busque la dirección IP de la interfaz de administración del y WorkSpace, a continuación, sustituya los dos últimos octetos por. `64.250` Por ejemplo, si la dirección IP de la interfaz de administración es 192.168.3.5, la dirección IP para la activación de Microsoft KMS Office es 192.168.64.250.
- Dirección TCP a IP de salida 127.0.0.2 para WSP WorkSpaces cuando el WorkSpace host está configurado para usar un servidor proxy.
- Las comunicaciones se originan en la dirección de bucle invertido 127.0.01.

En circunstancias normales, el WorkSpaces servicio configura estos puertos para usted. WorkSpaces Si se instala algún software de seguridad o firewall WorkSpace que bloquee alguno de estos puertos, es WorkSpace posible que no funcione correctamente o que no se pueda acceder a ellos.

Puertos de interfaces principales

Independientemente del tipo de directorio que tenga, los siguientes puertos deben estar abiertos en la interfaz de red principal de todos ellos: WorkSpaces

- Para la conectividad a Internet, los siguientes puertos deben estar abiertos de salida a todos los destinos y de entrada desde la WorkSpaces VPC. Debe añadirlos manualmente a su grupo de seguridad WorkSpaces si quiere que tengan acceso a Internet.
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- Para comunicarse con los controladores de directorio, los siguientes puertos deben estar abiertos entre la WorkSpaces VPC y los controladores de directorio. Para un directorio de AD sencillo, estos puertos estarán configurados correctamente en el grupo de seguridad creado por AWS Directory Service. En el caso de un directorio con Conector AD, es posible que tenga que ajustar el grupo de seguridad predeterminado de la VPC para abrir estos puertos.

- TCP/UDP 53: DNS
- TCP/UDP 88: autenticación de Kerberos
- UDP 123: NTP
- TCP 135: RPC
- UDP 137-138: Netlogon
- TCP 139: Netlogon
- TCP/UDP 389: LDAP
- TCP/UDP 445: SMB
- TCP/UDP 636: LDAPS (LDAP sobre TLS/SSL)
- TCP 1024-65535: puertos dinámicos para RPC

Si se instala algún software de seguridad o firewall WorkSpace que bloquee alguno de estos puertos, es posible que no funcione correctamente o que no se WorkSpace pueda acceder a ellos.

Requisitos de puertos y direcciones IP por región

Este de EE. UU. (Norte de Virginia)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.us-east-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.us-east-1.amazonaws.com ws-client-service

Categoría	Detalles
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Este de EE. UU. (Norte de Virginia): https://d32i4gd7pg4909.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Detalles
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.us-east-1.signin.aws
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominios: • ws-broker-servicehttps://.us-east-1.amazonaws.com • ws-broker-service-fipshttps://.us-east-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominios: https://workspaces.us-east-1.amazonaws.com
Agente de sesiones (PCM)	Dominios: • https://skylight-cm.us-east-1.amazonaws.com • https://.us-east-1.amazonaws.com skylight-cm-fips
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.us-east-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-iad.amazonworkspaces.com

Categoría	Detalles
Direcciones IP de la comprobación de estado	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	• 3.227.4.0/22 • 4420984,0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.us-east-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Oeste de EE. UU. (Oregón)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio:

Categoría	Detalles
	https://.us-west-2.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.us-west-2.amazonaws.com ws-client-service

Categoría	Detalles
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Oeste de EE. UU. (Oregón): https://d18af777lco7lp.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Detalles
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.us-west-2.signin.aws
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominios: • ws-broker-servicehttps://.us-west-2.amazonaws.com • ws-broker-service-fipshttps://.us-west-2.amazonaws.com
WorkSpaces Puntos finales de la API	Dominios: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
Agente de sesiones (PCM)	Dominios: • https://skylight-cm.us-west-2.amazonaws.com • https://.us-west-2.amazonaws.com skylight-cm-fips
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.us-west-2.rdn.amazonaws.com

Categoría	Detalles
El nombre del host de comprobación de estado	drp-pdx.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	34,223,96,0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.us-west-2.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16, 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia-Pacífico (Bombay)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/

Categoría	Detalles
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ap-south-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ap-south-1.amazonaws.com ws-client-service

Categoría	Detalles
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Asia-Pacífico (Bombay): https://d78hovzzqqtsb.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Detalles
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.ap-south-1 .amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.ap-south-1.amazon aws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ap-south-1.amazo naws.com
Servidores TURN de Acceso web para PCoIP	Acceso web no está disponible actualmente en la región Asia Pacífico (Bombay)
El nombre del host de comprobación de estado	drp-bom.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 13.12757,82 • 13,234250,73
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	13126,243,0 - 13126,243,255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	65,1156,0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace WSP	*.prod.ap-south-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

Asia-Pacífico (Seúl)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Métricas de dispositivos (para aplicaciones cliente de versiones superiores a la versión 1.0 y 2.0) WorkSpaces	https://-2.amazon.com/ device-metrics-us
Métricas de clientes (para aplicaciones cliente de 3.0 WorkSpaces o más)	Dominio: https://.ap-northeast-2.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o superior) WorkSpaces	Dominio: https://.ap-northeast-2.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio>

Categoría	Detalles
	Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Asia-Pacífico (Seúl): https://dtyv4uwoh7ynt.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com

Categoría	Detalles
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.ap-northeast-2.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.ap-northeast-2.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ap-northeast-2.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.ap-northeast-2.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-icn.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	3.35.160.0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace WSP	*.prod.ap-northeast-2.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia-Pacífico (Singapur)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ap-southeast-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o superior) WorkSpaces	Dominio: https://.ap-southeast-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/

Categoría	Detalles
	Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Asia-Pacífico (Singapur): https://d3qzmd7y07pz0i.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)

Categoría	Detalles
Agente de WS	Dominio: • ws-broker-servicehttps://.ap-southeast-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.ap-southeast-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ap-southeast-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.ap-southeast-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-sin.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 18.141.152,0 - 18.141.152.255 • 18.141.154,0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	13.212.132.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.ap-southeast-1.highlander.aws.a2z.com

Categoría	Detalles
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia-Pacífico (Sídney)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ap-southeast-2.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o superior) WorkSpaces	Dominio: https://.ap-southeast-2.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes:

Categoría	Detalles
	• https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Asia-Pacífico (Sídney): https://dwcpoxuuza83q.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.ap-southeast-2.signin.aws
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)

Categoría	Detalles
Agente de WS	Dominio: • ws-broker-servicehttps://.ap-southeast-2.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.ap-southeast-2.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ap-southeast-2.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.ap-southeast-2.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-syd.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 3.24.11.127 • 13.237.232.125
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	3.25.248.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.ap-southeast-2.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 y 198.19.0.0/16 • WSP: 10.0.0.0/8

Asia-Pacífico (Tokio)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ap-northeast-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o superior) WorkSpaces	Dominio: https://.ap-northeast-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente:

Categoría	Detalles
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Asia-Pacífico (Tokio): https://d2c2t8mxjhq5z1.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.ap-northeast-1.signin.aws
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.ap-northeast-1.amazonaws.com

Categoría	Detalles
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.ap-northeast-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ap-northeast-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.ap-northeast-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-nrt.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 18.178.102.247 • 54.64.174.128
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	3.114.164.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.ap-northeast-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Canadá (Centro)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ca-central-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.ca-central-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente:

Categoría	Detalles
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Canadá (centro): https://d2wfbsypmqjmog.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.ca-central-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.ca-central-1.amazonaws.com

Categoría	Detalles
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ca-central-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.ca-central-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-yul.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	3.97.20.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.ca-central-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Fráncfort)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

Categoría	Detalles
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.eu-central-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.eu-central-1.amazonaws.com ws-client-service

Categoría	Detalles
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • UE (Fráncfort): https://d1whcm49570jjw.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Detalles
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.eu-central-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.eu-central-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.eu-central-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.eu-central-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-fra.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227

Categoría	Detalles
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	18.192.216.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.eu-central-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Irlanda)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.eu-west-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.eu-west-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace

Categoría	Detalles
	• https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • UE (Irlanda): https://d3pgffbf39h4k4.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado

Categoría	Detalles
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.eu-west-1.signin.aws
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.eu-west-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.eu-west-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.eu-west-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.eu-west-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-dub.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255

Categoría	Detalles
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	3.248.176.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.eu-west-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• PCoIP/WSP: 172.31.0.0/16, 192.168.0.0/16 y 198.19.0.0/16 • WSP: 10.0.0.0/8

Europa (Londres)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.eu-west-2.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.eu-west-2.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio>

Categoría	Detalles
	Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Europa (Londres): https://d16q6638mh01s7.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com

Categoría	Detalles
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.eu-west-2.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.eu-west-2.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.eu-west-2.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.eu-west-2.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-lhr.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	18.134.68.0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace WSP	*.prod.eu-west-2.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• 198.19.0.0/16 • WSP: 10.0.0.0/8

América del Sur (São Paulo)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.sa-east-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.sa-east-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/

Categoría	Detalles
	Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • América del Sur (São Paulo): https://d2lh2qc5bdoq4b.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)

Categoría	Detalles
Agente de WS	Dominio: • ws-broker-servicehttps://.sa-east-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.sa-east-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.sa-east-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turn:*.sa-east-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-gru.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	15.228.64.0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.sa-east-1.highlander.aws.a2z.com

Categoría	Detalles
Intervalos de direcciones IP de la interfaz de administración	• 198.19.0.0/16 • WSP: 10.0.0.0/8

África (Ciudad del Cabo)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.af-south-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.af-south-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes:

Categoría	Detalles
	• https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://d1cbg795sa4g1u.cloudfront.net/prod/<región>/<ID del directorio> Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • África (Ciudad del Cabo): https://di5ygl2cs0mrh.cloudfront.net/
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)

Categoría	Detalles
Agente de WS	Dominio: • ws-broker-servicehttps://.af-south-1 .amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.af-south-1.amazon aws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.af-south-1.amazo naws.com
El nombre del host de comprobación de estado	drp-cpt.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 13,246,120,0 - 13,246,13255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	15228,64,0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.af-south-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• 172.31.0.0/16 y 198.19.0.0/16 • WSP: 10.0.0.0/8

Israel (Tel Aviv)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.il-central-1.amazonaws.com skylight-client-ds
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://.il-central-1.amazonaws.com ws-client-service
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://d21ui22avrxoh6.cloudfront.net/prod/<región>/<ID del directorio> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente:

Categoría	Detalles
	• Archivo CSS para el estilo de las páginas de inicio de sesión: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript archivo para las páginas de inicio de sesión: • Israel (Tel Aviv); —
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://<ID del directorio>.awsapps.com/ (donde <ID del directorio> es el dominio del cliente)
Agente de WS	Dominio: • ws-broker-servicehttps://.il-central-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces.il-central-1.amazonaws.com

Categoría	Detalles
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.il-central-1.amazonaws.com
Servidores TURN de Acceso web para PCoIP	Servidor: • turno: *.il-central-1.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-tlv.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 51.17.52.90 • 51,17109231 • 51,16190,43
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 51,17,28,0-51,17,31,255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	5117,72,0/22
Nombre de dominio de la puerta de enlace WSP	*.prod.il-central-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud Región (EE. UU.-Oeste)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

Categoría	Detalles
Actualización automática del cliente	https://s3.amazonaws.com/ workspaces-client-updates /prod/pdt/windows/ .xml WorkSpaces AppCast
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://. skylight-client-ds us-gov-west-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 WorkSpaces o más)	Dominio: https://ws-client-service. us-gov-west-1.amazonaws.com

Categoría	Detalles
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://s3.amazonaws.com/ workspaces-client-assets /prod/pdt/ <directory ID> Archivo CSS para el estilo de las páginas de inicio de sesión: • workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css JavaScript archivo para las páginas de inicio de sesión: • No aplicable
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Detalles
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.signin. amazonaws-us-gov.com
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(donde está el dominio del cliente)
Agente de WS	Dominio: • https://. ws-broker-service us-gov-west-1.amazonaws.com • https://. ws-broker-service-fips us-gov-west-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces. us-gov-west-1.amazonaws.com • https://workspaces-fips. us-gov-west-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm. us-gov-west-1.amazonaws.com • https://. skylight-cm-fips us-gov-west-1.amazonaws.com
El nombre del host de comprobación de estado	drp-pdt.amazonworkspaces.com

Categoría	Detalles
Direcciones IP de la comprobación de estado	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 52.61.193.0 - 52.61.193.255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	• 3.32.139,0/24 • 3,30129,0/24 • 3,30,130,0/23
Nombre de dominio de la puerta de enlace WSP	*.prod. us-gov-west-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• 198.19.0.0/16 • WSP: 10.0.0.0/8 y 192.169.0.0/16

AWS GovCloud Región (EE. UU.-Este)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
Actualización automática del cliente	https://s3.amazonaws.com/ workspaces-client-updates /prod/osu/windows/ .xml WorkSpaces AppCast
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/

Categoría	Detalles
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://. skylight-client-ds us-gov-east-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 WorkSpaces o más)	Dominio: https://ws-client-service. us-gov-east-1.amazonaws.com

Categoría	Detalles
Configuración de directorios	Autenticación del cliente en el directorio de clientes antes de iniciar sesión en: WorkSpace • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS: • https://d32i4gd7pg4909.cloudfront.net/ Configuración de directorios de clientes: • https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: • https://s3.amazonaws.com/ workspaces-client-assets /prod/osu/ <directory ID> Archivo CSS para el estilo de las páginas de inicio de sesión: • workspaces-clients-csshttps://s3.amazonaws.com/ /workspaces_v2.css JavaScript archivo para las páginas de inicio de sesión: • No aplicable
Servicio de registro de Forrester	https://fls-na.amazon.com/

Categoría	Detalles
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.signin. amazonaws-us-gov.com
Dependencia de registro (para Acceso web y Teradici PCoIP Zero Clients)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://login. us-gov-home<directory id>.awsapps.com/directory/<directory id>/(donde está el dominio del cliente)
Agente de WS	Dominio: • https://. ws-broker-service us-gov-east-1.amazonaws.com • https://. ws-broker-service-fips us-gov-east-1.amazonaws.com
WorkSpaces Puntos finales de la API	Dominio: • https://workspaces. us-gov-east-1.amazonaws.com • https://workspaces-fips. us-gov-east-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm. us-gov-east-1.amazonaws.com • https://. skylight-cm-fips us-gov-east-1.amazonaws.com
El nombre del host de comprobación de estado	drp-osu.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 18.253,251,70 • 18,254,0118

Categoría	Detalles
Intervalo de direcciones IP públicas del servidor de la puerta de enlace de PCoIP	• 18,254,1400,0 - 18,254,143,255
Intervalo de direcciones IP de los servidores de puerta de enlace de WSP	18,254.148,0/22
Nombre de dominio de la puerta de enlace WSP	*.prod. us-gov-east-1.highlander.aws.a2z.com
Intervalos de direcciones IP de la interfaz de administración	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Requisitos de red de clientes de Amazon WorkSpaces

Los usuarios de WorkSpaces pueden conectarse a los WorkSpaces mediante la aplicación cliente de un dispositivo compatible. De forma alternativa, pueden usar un navegador web para conectarse a los WorkSpaces que admiten esta forma de acceso. Para obtener una lista de WorkSpaces que son compatibles con el acceso mediante navegador web, consulte «¿Qué paquetes de Amazon WorkSpaces son compatibles con el acceso web?» en Acceso de clientes, Acceso web y Experiencia de usuario.

> **Note**
>
> No se puede utilizar un navegador web para conectarse con los WorkSpaces de Amazon Linux.

> **Important**
>
> A partir del 1 de octubre de 2020, los clientes ya no podrán usar el cliente Acceso web de Amazon WorkSpaces para conectarse a WorkSpaces del tipo personalizado o «traiga su propia licencia (BYOL)» de Windows 7.

Para proporcionar a los usuarios una buena experiencia con los escritorios de WorkSpaces, compruebe que sus dispositivos cliente cumplen los siguientes requisitos de red:

- El dispositivo cliente debe tener una conexión a Internet de banda ancha. Recomendamos planificar un mínimo de 1 Mbps por usuario simultáneo que vea una ventana de vídeo de 480p. En función de los requisitos de calidad de usuario para la resolución de vídeo, es posible que se requiera más ancho de banda.
- La red a la que está conectado el dispositivo cliente y cualquier firewall que esté en el propio dispositivo cliente deben tener abiertos determinados puertos en los rangos de direcciones IP de diversos servicios de AWS. Para obtener más información, consulte Requisitos de dirección IP y puerto para WorkSpaces.
- Para un rendimiento óptimo de PCoIP, el tiempo de ida y vuelta (RTT) de la red del cliente a la región en la que están los espacios de trabajo debe ser inferior a 100 ms. Si el RTT está entre 100 ms y 200 ms, el usuario puede obtener acceso al WorkSpace, pero el rendimiento se reduce. Si el RTT está entre 200 ms y 375 ms, el rendimiento se degrada. Si el RTT supera los 375 ms, se interrumpe la conexión del cliente de WorkSpaces.

  Para obtener el mejor rendimiento del protocolo WorkSpaces Streaming Protocol (WSP), el RTT desde la red del cliente hasta la región en la que se encuentran los WorkSpaces debe ser inferior a Para un rendimiento óptimo de PCoIP, el tiempo de ida y vuelta (RTT) de la red del cliente a la región en la que están los espacios de trabajo debe ser inferior a 250 ms. Si el RTT está entre 250 ms y 400 ms, el usuario puede obtener acceso al WorkSpace, pero el rendimiento se reduce.

  Para comprobar el RTT a las distintas regiones de AWS desde su ubicación, utilice la comprobación de estado de conexión de Amazon WorkSpaces.
- Para utilizar cámaras web con WSP, recomendamos un ancho de banda de carga mínimo de 1,7 megabits por segundo.
- Si los usuarios van a obtener acceso a un WorkSpace a través de una red privada virtual (VPN), la conexión debe permitir una unidad de transmisión máxima (MTU) de 1.200 bytes como mínimo.

> **Note**
>
> No se puede acceder a WorkSpaces a través de una VPN conectada a la nube virtual privada (VPC). Para acceder a WorkSpaces mediante una VPN, se requiere conectividad a Internet (a través de las direcciones IP públicas de la VPN), tal como se describe en Requisitos de dirección IP y puerto para WorkSpaces.

- Los clientes requieren acceso HTTPS a los recursos de WorkSpaces alojados en el servicio y en Amazon Simple Storage Service (Amazon S3). Los clientes no admiten el redireccionamiento proxy en el nivel de aplicaciones. Se requiere acceso HTTPS para que los usuarios puedan completar correctamente el registro y obtener acceso a los WorkSpaces.
- Para permitir el acceso desde dispositivos de cliente cero PCoIP, debe utilizar un paquete de protocolos PCoIP para WorkSpaces. También debe habilitar el protocolo de tiempo de red (NTP) en Teradici. Para obtener más información, consulte Configuración del cliente de PCoIP Zero para WorkSpaces.
- Para clientes 3.0 o posterior, si utiliza el inicio de sesión único (SSO) para Amazon WorkDocs debe seguir las instrucciones de la sección Inicio de sesión único de la Guía de administración de AWS Directory Service.

Puede verificar si un dispositivo cliente satisface los requisitos de red como sigue.

Para verificar los requisitos de red para clientes 3.0+

1. Abra el cliente de WorkSpaces. Si es la primera vez que abra el cliente, se le pedirá que introduzca el código de registro que recibió en el email de invitación.
2. En función del cliente que esté utilizando, realice una de las siguientes acciones.

Si utiliza...	Haga lo siguiente
Clientes Windows o Linux	En la esquina superior derecha de la aplicación cliente, seleccione el icono Network (Red) .
Cliente para macOS	Elija Connections (Conexiones), Network (Red).

   La aplicación cliente prueba la conexión de red, los puertos y el tiempo de ida y vuelta y notifica los resultados de estas pruebas.
3. Cierre el cuadro de diálogo Network (Red) para volver a la página de inicio de sesión.

Para verificar los requisitos de red para clientes 1.0+ y 2.0+

1. Abra el cliente de WorkSpaces. Si es la primera vez que abra el cliente, se le pedirá que introduzca el código de registro que recibió en el email de invitación.
2. Elija Network (Red) en la esquina inferior derecha de la aplicación cliente. La aplicación cliente prueba la conexión de red, los puertos y el tiempo de ida y vuelta y notifica los resultados de estas pruebas.
3. Elija Dismiss para volver a la página de inicio de sesión.

Restrinja el WorkSpaces acceso a dispositivos de confianza

De forma predeterminada, los usuarios pueden acceder a ellos WorkSpaces desde cualquier dispositivo compatible que esté conectado a Internet. Si su empresa limita el acceso a los datos corporativos a los dispositivos de confianza (también conocidos como dispositivos gestionados), puede restringir el WorkSpaces acceso a los dispositivos de confianza con certificados válidos.

Al habilitar esta función, WorkSpaces utiliza la autenticación basada en certificados para determinar si un dispositivo es de confianza. Si la aplicación WorkSpaces cliente no puede comprobar que un dispositivo es de confianza, bloquea los intentos de iniciar sesión o volver a conectarse desde el dispositivo.

Para cada directorio, puede importar hasta dos certificados raíz. Si importa dos certificados raíz, WorkSpaces preséntelos al cliente y este encontrará el primer certificado válido que coincida con alguno de los certificados raíz.

Clientes compatibles

- Android, que se ejecuta en sistemas Android o Chrome OS compatibles con Android
- macOS
- Windows

> **Important**
>
> Esta característica solo se admite en los siguientes clientes:
>
> - WorkSpaces aplicaciones cliente para Linux o iPad

- Clientes de terceros, incluidos, entre otros, Teradici PCoIP, clientes RDP y aplicaciones de escritorio remoto.

> **Note**
>
> Cuando habilites el acceso para clientes específicos, asegúrate de bloquear el acceso a otros tipos de dispositivos que no necesites. Para obtener más información sobre cómo hacerlo, consulta el paso 3.7 que aparece a continuación.

Paso 1: Crear los certificados

Esta característica requiere dos tipos de certificados: certificados raíz generados por una entidad de certificación (CA) interna y certificados de cliente que se encadenan hasta un certificado raíz.

Requisitos

- Los certificados raíz deben ser archivos de certificado codificados en Base64, con formato CRT, CERT o PEM.
- Los certificados raíz deben cumplir con el siguiente patrón de expresiones regulares, lo que significa que cada línea codificada, además de la última, debe tener exactamente 64 caracteres: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`.
- Los certificados deben incluir un nombre común.
- Los certificados de dispositivo deben incluir las siguientes extensiones: `Key Usage: Digital Signature` y `Enhanced Key Usage: Client Authentication`.
- Todos los certificados de la cadena, desde el certificado del dispositivo hasta la entidad emisora de certificados raíz de confianza, deben estar instalados en el dispositivo cliente.
- La longitud máxima que se admite para una cadena de certificados es 4.
- WorkSpaces actualmente no admite mecanismos de revocación de dispositivos, como las listas de revocación de certificados (CRL) o el Protocolo de estado de certificados en línea (OCSP), para los certificados de clientes.
- Utilice un algoritmo de cifrado sólido. Recomendamos SHA256 con RSA, SHA256 con ECDSA, SHA384 con ECDSA o SHA512 con ECDSA.

- Para macOS, si el certificado del dispositivo está en el llavero del sistema, le recomendamos que autorice a la aplicación WorkSpaces cliente a acceder a esos certificados. De lo contrario, los usuarios tendrán que escribir las credenciales de llavero cuando inician sesión o vuelven a conectarse.

Paso 2: Implementar certificados de cliente en los dispositivos de confianza

En los dispositivos de confianza de sus usuarios, debe instalar un paquete de certificados que incluya todos los certificados de la cadena, desde el certificado del dispositivo hasta la autoridad de certificación raíz de confianza. Puede utilizar la solución que prefiera para instalar los certificados en la flota de dispositivos cliente, por ejemplo, System Center Configuration Manager (SCCM) o Mobile Device Management (MDM). Tenga en cuenta que, si lo desea, SCCM y MDM pueden realizar una evaluación del nivel de seguridad para determinar si los dispositivos cumplen las políticas corporativas de acceso. WorkSpaces

Las aplicaciones WorkSpaces cliente buscan los certificados de la siguiente manera:

- Android: vaya a Ajustes, seleccione Seguridad y ubicación, Credenciales y, a continuación, Instalar desde una tarjeta SD.
- Sistemas Chrome OS compatibles con Android: abra los ajustes de Android y seleccione Seguridad y ubicación, Credenciales y, a continuación, Instalar desde una tarjeta SD.
- macOS: busca certificados de cliente en el llavero.
- Windows: busca certificados de cliente en los almacenes de certificados de usuario y raíz.

Paso 3: Configurar la restricción

Una vez que ha implementado los certificados de cliente en los dispositivos de confianza, puede permitir el acceso restringido en el nivel de directorio. Esto requiere que la aplicación WorkSpaces cliente valide el certificado en un dispositivo antes de permitir que el usuario inicie sesión en un WorkSpace.

Para configurar la restricción

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y después elija Actions, Update Details.

4. Amplíe Access Control Options.
5. En Para cada tipo de dispositivo, especifique los dispositivos a los que puede acceder WorkSpaces y seleccione Dispositivos de confianza.
6. Importe hasta dos certificados raíz. Con cada certificado raíz, haga lo siguiente:
   a. Seleccione Importar.
   b. Copie el cuerpo del certificado en el formulario.
   c. Seleccione Importar.
7. Especifique si otros tipos de dispositivos tienen acceso a WorkSpaces.
   a. Desplácese hacia abajo hasta la sección Other platforms (Otras plataformas). De forma predeterminada, los clientes WorkSpaces Linux están deshabilitados y los usuarios pueden acceder a ellos WorkSpaces desde sus dispositivos iOS, dispositivos Android, Web Access, Chromebooks y dispositivos de cliente cero de PCoIP.
   b. Seleccione los tipos de dispositivo que va a habilitar y deseleccione los que va a deshabilitar.
   c. Para bloquear el acceso de todos los tipos dispositivos seleccionados, elija Block.
8. Elija Update and Exit.

Integración de WorkSpaces con SAML 2.0

La integración de SAML 2.0 con la autenticación de sesiones de escritorio de WorkSpaces permite a los usuarios usar sus credenciales del proveedor de identidades (IdP) de SAML 2.0 y los métodos de autenticación existentes a través de su navegador web predeterminado. Al usar su IdP para autenticar a los usuarios de WorkSpaces, puede proteger los WorkSpaces con las características del IdP, como la autenticación multifactor y las políticas de acceso contextual.

Flujo de trabajo de autenticación

En las siguientes secciones se describe el flujo de trabajo de autenticación iniciado por la aplicación cliente de WorkSpaces, WorkSpaces Acceso web y un proveedor de identidades (IdP) de SAML 2.0:

- Cuando el IdP inicia el flujo. Por ejemplo, cuando los usuarios eligen una aplicación en el portal de usuarios del IdP en un navegador web.

- Cuando el cliente de WorkSpaces inicia el flujo. Por ejemplo, cuando los usuarios abren la aplicación cliente e inician sesión.
- Cuando el cliente de WorkSpaces inicia el flujo. Por ejemplo, cuando los usuarios abren Acceso web en un navegador e inician sesión.

En estos ejemplos, los usuarios acceden a `user@example.com` para iniciar sesión en el IdP. El IdP tiene una aplicación de proveedor de servicios SAML 2.0 configurada para un directorio de WorkSpaces y los usuarios están autorizados para usar la aplicación SAML 2.0 de WorkSpaces. Los usuarios crean un escritorio de WorkSpaces para sus nombres de usuario, `user`, en un directorio que está habilitado para la autenticación SAML 2.0. Además, los usuarios instalan la aplicación cliente WorkSpaces en sus dispositivos o utilizan Acceso web en un navegador web.

Flujo iniciado por el proveedor de identidades (IdP) con la aplicación cliente

El flujo iniciado por el IdP permite a los usuarios registrar automáticamente la aplicación cliente de WorkSpaces en sus dispositivos sin tener que introducir un código de registro de WorkSpaces. Los usuarios no inician sesión en sus WorkSpaces mediante el flujo iniciado por el IdP. La autenticación de WorkSpaces debe originarse en la aplicación cliente.

1. Con su navegador web, los usuarios inician sesión en el IdP.
2. Tras iniciar sesión en el IdP, los usuarios eligen la aplicación WorkSpaces en el portal de usuario del IdP.
3. Los usuarios son redirigidos a esta página en el navegador y la aplicación cliente WorkSpaces se abre automáticamente.

4. La aplicación cliente de WorkSpaces ya está registrada y los usuarios pueden seguir iniciando sesión haciendo clic en Seguir para iniciar sesión en WorkSpaces.

Flujo iniciado por el proveedor de identidades (IdP) con Acceso web

El flujo de Acceso web iniciado por el IdP permite a los usuarios registrar automáticamente la aplicación cliente de WorkSpaces en sus dispositivos sin tener que introducir un código de registro de WorkSpaces. Los usuarios no inician sesión en sus WorkSpaces mediante el flujo iniciado por el IdP. La autenticación de WorkSpaces debe originarse en Acceso web.

1. Con su navegador web, los usuarios inician sesión en el IdP.
2. Tras iniciar sesión en el IdP, los usuarios hacen clic en la aplicación WorkSpaces en el portal de usuario del IdP.
3. Los usuarios son redirigidos a esta página en el navegador. Para abrir WorkSpaces, elija Amazon WorkSpaces en el navegador.

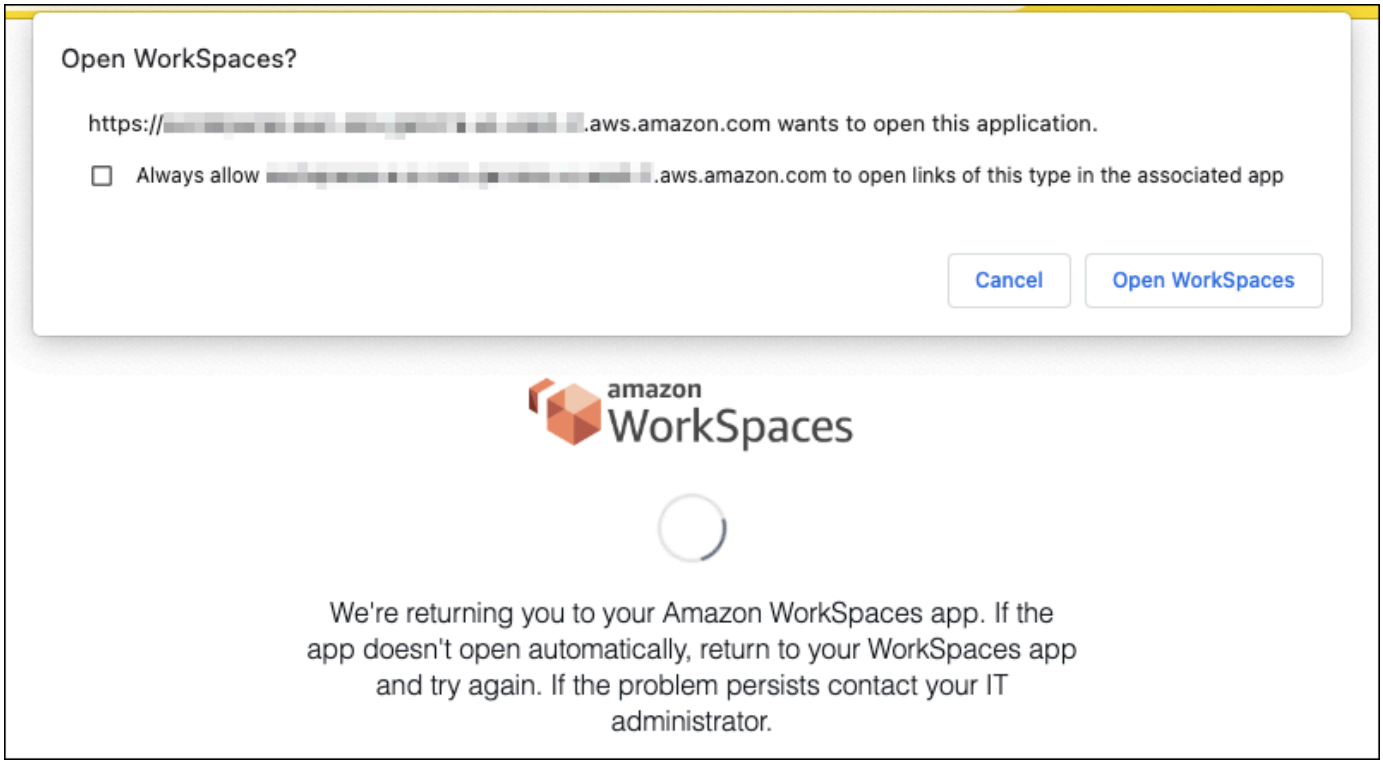
4. La aplicación cliente de WorkSpaces ya está registrada y los usuarios pueden seguir iniciando sesión a través de WorkSpaces Acceso web.

Flujo iniciado por el cliente de WorkSpaces

El flujo iniciado por el cliente permite a los usuarios iniciar sesión en sus WorkSpaces después de iniciar sesión en un IdP.

1. Los usuarios inician la aplicación cliente de WorkSpaces (si aún no se está ejecutando) y hacen clic en Seguir para iniciar sesión en WorkSpaces.

2. Los usuarios son redirigidos a su navegador web predeterminado para iniciar sesión en el IdP. Si los usuarios ya han iniciado sesión en el IdP en su navegador, no necesitan volver a iniciar sesión y se saltarán este paso.
3. Una vez que hayan iniciado sesión en el IdP, los usuarios son redirigidos a una ventana emergente. Siga las instrucciones para permitir que su navegador web abra la aplicación cliente.



4. Los usuarios son redirigidos a la aplicación cliente de WorkSpaces para completar el inicio de sesión en su WorkSpace. Los nombres de usuario de WorkSpaces se rellenan automáticamente a partir de la aserción SAML 2.0 del IdP. Al utilizar la autenticación basada en certificados (CBA), los usuarios inician sesión automáticamente.
5. Los usuarios han iniciado sesión en su escritorio de WorkSpaces.

Flujo iniciado por WorkSpaces Acceso web

El flujo iniciado por Acceso web permite a los usuarios iniciar sesión en sus WorkSpaces después de iniciar sesión en un IdP.

1. Los usuarios inician WorkSpaces Acceso web y eligen Iniciar sesión.
2. En la misma pestaña del navegador, los usuarios son redirigidos al portal de IdP. Si los usuarios ya han iniciado sesión en el IdP en su navegador, no necesitan volver a iniciar sesión y se saltarán este paso.

3. Una vez que han iniciado sesión en el IdP, se redirige a los usuarios a esta página en el navegador, donde hacen clic en Iniciar sesión en WorkSpaces.
4. Los usuarios son redirigidos a la aplicación cliente de WorkSpaces para completar el inicio de sesión en su WorkSpace. Los nombres de usuario de WorkSpaces se rellenan automáticamente a partir de la aserción SAML 2.0 del IdP. Al utilizar la autenticación basada en certificados (CBA), los usuarios inician sesión automáticamente.
5. Los usuarios han iniciado sesión en su escritorio de WorkSpaces.

Configuración de SAML 2.0

Habilite el registro de las aplicaciones WorkSpaces cliente y el inicio de sesión WorkSpaces para sus usuarios mediante sus credenciales de proveedor de identidad (IdP) de SAML 2.0 y sus métodos de autenticación configurando la federación de identidades mediante SAML 2.0. Para configurar la federación de identidades mediante SAML 2.0, usa un rol de IAM y una URL de estado de retransmisión para configurar tu IdP y habilitarlo. AWS Esto permite a los usuarios federados acceder a un directorio. WorkSpaces El estado de retransmisión es el punto final del WorkSpaces directorio al que se redirige a los usuarios después de iniciar AWS sesión correctamente.

Contenido

Requisitos

- La autenticación SAML 2.0 está disponible en las siguientes regiones:
  - Región del este de EE. UU. (Norte de Virginia)
  - Región del oeste de EE. UU (Oregón)

  - Región África (Ciudad del Cabo)
  - Asia Pacific (Mumbai) Region
  - Asia Pacific (Seoul) Region
  - Región de Asia-Pacífico (Singapur)
  - Región de Asia-Pacífico (Sídney)
  - Asia Pacífico (Tokio)
  - Región de Canadá (centro)
  - Región de Europa (Fráncfort)
  - Región de Europa (Irlanda)
  - Región de Europa (Londres)
  - Región de América del Sur (São Paulo)
  - Región Israel (Tel Aviv)
  - AWS GovCloud (EE. UU.-Oeste)
  - AWS GovCloud (EE. UU.-Este)
- Para utilizar la autenticación SAML 2.0 con WorkSpaces, el IdP debe admitir el SSO iniciado por un IdP no solicitado con un recurso de destino de enlace profundo o una URL de punto final de estado de retransmisión. Algunos ejemplos IdPs son ADFS, Azure AD, Duo Single Sign-On, Okta y. PingFederate PingOne Para obtener más información, consulte la documentación de su IdP.
- La autenticación SAML 2.0 funcionará si se WorkSpaces inicia con Simple AD, pero no se recomienda porque Simple AD no se integra con SAML 2.0. IdPs
- La autenticación SAML 2.0 se admite en los siguientes clientes. WorkSpaces Otras versiones de los clientes no son compatibles con la autenticación SAML 2.0. Abre Amazon WorkSpaces Client Downloads para encontrar las versiones más recientes:
  - Aplicación cliente de Windows (versión 5.1.0.3029 o posterior)
  - Cliente para macOS (versión 5.x o posterior)
  - Cliente Linux para Ubuntu 22.04 versión 2024.1 o posterior, Ubuntu 20.04 versión 24.1 o posterior
  - Acceso web

  Las demás versiones de cliente no podrán conectarse a la autenticación WorkSpaces habilitada para SAML 2.0 a menos que se habilite la opción alternativa. Para obtener más información, consulte Habilitar la autenticación SAML 2.0 en el directorio. WorkSpaces

Para step-by-step obtener instrucciones sobre cómo integrar SAML 2.0 WorkSpaces con ADFS, Azure AD, Duo Single Sign-On, Okta PingFederate y PingOne para empresas, consulte la OneLogin Guía de implementación de la autenticación de Amazon WorkSpaces SAML.

Requisitos previos

Complete los siguientes requisitos previos antes de configurar la conexión del proveedor de identidad (IdP) de SAML 2.0 a un directorio. WorkSpaces

1. Configure su IdP para integrar las identidades de usuario del Microsoft Active Directory que se utiliza con el WorkSpaces directorio. En el caso de un usuario con un WorkSpace, los atributos de correo electrónico AccountName y sAM del usuario de Active Directory y los valores de notificación de SAML deben coincidir para que el usuario inicie sesión WorkSpaces con el iDP. Para obtener más información sobre la integración de Active Directory con el IdP, consulte la documentación del IdP.
2. Configure el IdP para establecer una relación de confianza con AWS.
   - Consulte Integrar proveedores de soluciones SAML de terceros AWS para obtener más información sobre la configuración de la federación. AWS Los ejemplos relevantes incluyen la integración del IdP con AWS IAM para acceder a la AWS consola de administración.
   - Use su IdP para generar y descargar un documento de metadatos de federación que describa su organización como proveedor de identidades. Este documento XML firmado se utiliza para establecer la relación de confianza. Guarde este archivo en una ubicación a la que pueda acceder desde la consola de IAM en otro momento.
3. Cree o registre un directorio WorkSpaces mediante la consola de WorkSpaces administración. Para obtener más información, consulte Administrar directorios para WorkSpaces. La autenticación SAML 2.0 para WorkSpaces se admite en los siguientes tipos de directorios:
   - Conector de AD
   - AWS Microsoft AD gestionado
4. Cree una WorkSpace para un usuario que pueda iniciar sesión en el IdP mediante un tipo de directorio compatible. Puede crear una WorkSpace mediante la consola WorkSpaces de administración o AWS CLI la WorkSpaces API. Para obtener más información, consulte Lanzar un escritorio virtual mediante WorkSpaces.

Paso 1: Crear un proveedor de identidades SAML en IAM AWS

En primer lugar, cree un IdP de SAML en IAM. AWS Este IdP define la relación entre el IDP y la AWS confianza de su organización mediante el documento de metadatos generado por el software de IdP de su organización. Para obtener más información, consulte Creación y administración de un proveedor de identidades de SAML (consola de administración de Amazon Web Services). Para obtener información sobre cómo trabajar con SAML IdPs en AWS GovCloud (EE. UU. Oeste) y AWS GovCloud (EE. UU. Este), consulte AWS Identity and Access Management.

Paso 2: crear un rol de IAM de federación de SAML 2.0

A continuación, creará un rol de IAM de federación de SAML 2.0. Este paso se establece una relación de confianza entre IAM y el proveedor de identidades de su organización, que identifica el proveedor de identidades como una entidad de confianza para la federación.

Para crear un rol de IAM para el IdP de SAML

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Roles > Crear rol.
3. Para Tipo de rol, seleccione Federación con SAML 2.0.
4. Para Proveedor de SAML, seleccione el IdP de SAML que ha creado.

   > **Important**
   >
   > No elija ninguno de los dos métodos de acceso de SAML 2.0 (Permitir solo acceso mediante programación o Permitir acceso mediante programación y mediante la consola de administración de Amazon Web Services).

5. Para Attribute, elija SAML:sub_type.
6. En Valor, ingrese `persistent`. Este valor restringe el acceso del rol a solicitudes de streaming de usuario de SAML que incluyan una aserción de tipo de sujeto de SAML con un valor de persistente. Si el SAML:sub_type es persistente, su IdP envía el mismo valor único para el elemento NameID en todas las solicitudes de SAML desde un usuario particular. Para obtener más información sobre la afirmación SAML:sub_type, consulta la sección Cómo identificar de forma exclusiva a los usuarios en la federación basada en SAML en Cómo utilizar la federación basada en SAML para el acceso a la API. AWS
7. Revise su información de confianza de SAML 2.0, confirmando la entidad de confianza y la condición correctas y, a continuación, elija Siguiente: Permisos.

8. En la página Asociar políticas de permisos, seleccione Siguiente: Etiquetas.
9. (Opcional) Especifique una clave y un valor para cada etiqueta que desee añadir. Para obtener más información, consulte Etiquetado de usuarios y roles de IAM.
10. Cuando haya terminado, seleccione Siguiente: Revisar. Posteriormente, creará e incrustará una política en línea para este rol.
11. En Nombre del rol, introduzca un nombre de rol que le sea útil para identificar su propósito. Dado que múltiples entidades pueden hacer referencia al rol, no se puede editar el nombre del rol una vez que se haya creado.
12. (Opcional) En Descripción del rol, escriba una descripción para el nuevo rol.
13. Revise los detalles del rol y seleccione Crear rol.
14. Añada el permiso sts: TagSession a la política de confianza de su nueva función de IAM. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS. En la página de detalles del nuevo rol de IAM, seleccione la pestaña Relaciones de confianza y, a continuación, seleccione Editar la relación de confianza. Cuando se abra el editor de políticas de Editar relaciones de confianza, añada el permiso sts: TagSession * de la siguiente manera:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
    }]
}
```

Sustituya `IDENTITY-PROVIDER` por el nombre del IdP de SAML que ha creado en el paso 1. A continuación, seleccione Actualizar la política de confianza.

Paso 3: incrustar una política en línea para el rol de IAM

A continuación, incruste una política de IAM en línea para el rol que ha creado. Al incrustar una política en línea, los permisos en la política no se pueden asociar de forma accidental a una entidad principal incorrecta. La política en línea proporciona a los usuarios federados acceso al WorkSpaces directorio.

> **Important**
>
> Esta acción no admite políticas de IAM para gestionar el acceso en AWS función de la IP de origen. `workspaces:Stream` Para administrar los controles de acceso IP WorkSpaces, utilice los grupos de control de acceso IP. Además, al usar la autenticación SAML 2.0, puede usar políticas de control de acceso IP si están disponibles en su IdP de SAML 2.0.

1. En los detalles del rol de IAM que ha creado, seleccione la pestaña Permisos y, a continuación, añada los permisos necesarios a la política de permisos del rol. Se inicia el Asistente de creación de políticas.
2. En Crear política, elija la pestaña JSON.
3. Copie y pegue la siguiente política JSON en la ventana de JSON. A continuación, modifique el recurso introduciendo el código de AWS región, el identificador de cuenta y el identificador de directorio. En la siguiente política, `"Action": "workspaces:Stream"` es la acción que proporciona a WorkSpaces los usuarios permisos para conectarse a sus sesiones de escritorio en el WorkSpaces directorio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
```

```
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

`REGION-CODE`Sustitúyala por la AWS región en la que se encuentra tu WorkSpaces directorio. `DIRECTORY-ID`Sustitúyalo por el identificador del WorkSpaces directorio, que se encuentra en la consola WorkSpaces de administración. Para los recursos en AWS GovCloud (EE. UU. Oeste) o AWS GovCloud (EE. UU. Este), utilice el siguiente formato para el ARN:. `arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID`

4. Cuando haya terminado, elija Revisar política. El validador de políticas notificará los errores de sintaxis.

Paso 4: configurar el proveedor de identidades de SAML 2.0

A continuación, en función del IdP de SAML 2.0, es posible que tengas que actualizar manualmente tu IdP para que sea AWS confiable como proveedor de servicios cargando `saml-metadata.xml` el archivo en https://signin.aws.amazon.com/static/saml-metadata.xml a tu IdP. En este paso se actualizan los metadatos de su proveedor de identidades. En el caso de algunos IdPs, es posible que la actualización ya esté configurada. En tal caso, continúe en el paso siguiente.

Si esta actualización aún no está configurada en su IdP, revise la documentación facilitada por su proveedor de identidad para obtener información acerca de cómo actualizar los metadatos. Algunos proveedores ofrecen la opción de escribir la URL y de que el IdP obtenga e instale el archivo automáticamente. Otros requieren que descargue el archivo de la URL y, a continuación, lo proporcione como archivo local.

> **Important**
>
> En este momento, también puede autorizar a los usuarios de su IdP a acceder a la WorkSpaces aplicación que ha configurado en su IdP. A los usuarios que están autorizados a acceder a la WorkSpaces aplicación de su directorio no se les WorkSpace crea automáticamente una. Del mismo modo, los usuarios que hayan WorkSpace creado una para ellos no están autorizados automáticamente a acceder a la WorkSpaces aplicación. Para

conectarse correctamente a una autenticación WorkSpace mediante SAML 2.0, el IdP debe autorizar al usuario y tener WorkSpace un creado.

Paso 5: crear declaraciones para la respuesta de autenticación SAML

A continuación, configure la información que su IdP envía AWS como atributos de SAML en su respuesta de autenticación. Según su IdP, ya está configurado, omita este paso y continúe con el Paso 6: configurar el estado de retransmisión de su federación.

Si esta información no está configurada en su IdP, proporcione lo siguiente:

- SAML Subject NameID: el identificador único del usuario que está iniciando sesión. El valor debe coincidir con el nombre WorkSpaces de usuario y, por lo general, es el AccountName atributo sAM del usuario de Active Directory.
- SAML Subject Type (con un valor establecido en `persistent`): al configurar el valor como `persistent` se garantiza que su proveedor de identidades envíe el mismo valor único para el elemento `NameID` en todas las solicitudes de SAML de un usuario particular. Asegúrese de que su política de IAM incluya una condición para permitir solo las solicitudes de SAML con un SAML sub_type configurado como `persistent`, tal como se describe en Paso 2: crear un rol de IAM de federación de SAML 2.0.
- Elemento **`Attribute`** con el atributo **`Name`** configurado como **`https://aws.amazon.com/SAML/Attributes/Role`**: este elemento contiene uno o más elementos `AttributeValue` que enumera el rol de IAM y el IdP de SAML a los que el usuario está asignado mediante su IdP. El rol y el proveedor de identidades se especifican como un par de ARN separados por comas. Un ejemplo del valor esperado es `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`.
- **`Attribute`**elemento con el **`Name`** atributo establecido en`https://aws.amazon.com/SAML/Attributes/RoleSessionName`: este elemento contiene un `AttributeValue` elemento que proporciona un identificador para las credenciales AWS temporales que se emiten para el SSO. El valor del elemento `AttributeValue` debe tener entre 2 y 64 caracteres, solo puede contener caracteres alfanuméricos, guiones bajos y los siguientes caracteres: _ . : / = + - @. No puede contener espacios. Normalmente, el valor es una dirección de correo electrónico o un nombre principal de un usuario (UPN). No debe ser un valor que contenga un espacio, como el nombre visible de un usuario.
- Elemento **`Attribute`** con el atributo **`Name`** configurado como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`**: este elemento contiene un elemento

`AttributeValue` que proporciona la dirección de correo electrónico del usuario. El valor debe coincidir con la dirección de correo electrónico del WorkSpaces usuario tal como se define en el WorkSpaces directorio. Los valores de las etiquetas pueden incluir combinaciones de caracteres , letras, números, espacios y caracteres _ . : / = + - @. Para obtener más información, consulte Reglas para etiquetar en IAM y AWS STS en la Guía del usuario de IAM.

- Elemento **`Attribute`** con el atributo **`Name`** configurado como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** (opcional): este elemento contiene un elemento `AttributeValue` que proporciona el `userPrincipalName` de Active Directory del usuario que inicia sesión. El formato del valor que proporcione debe ser `username@domain.com`. Este parámetro se usa con la autenticación basada en certificados como nombre alternativo del sujeto en el certificado del usuario final. Para obtener más información, consulte Autenticación basada en certificados.
- Elemento **`Attribute`** con el atributo **`Name`** configurado como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** (opcional): este elemento contiene un elemento que proporciona el identificador de seguridad (SID) de Active Directory del usuario que inicia sesión. Este parámetro se usa con la autenticación basada en certificados para permitir una asignación firme con el usuario de Active Directory. Para obtener más información, consulte Autenticación basada en certificados.
- Elemento **`Attribute`** con el atributo **`Name`** configurado como **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** (opcional): este elemento contiene un elemento `AttributeValue` que proporciona un formato de nombre de usuario alternativo. Utilice este atributo si tiene casos de uso que requieren formatos de nombre de usuario como `corp\username`corp.example.com\username, o `username@corp.example.com` para iniciar sesión con el WorkSpaces cliente. Las claves y los valores de las etiquetas puede incluir cualquier combinación de letras, números, espacios y los caracteres _ : / . + = @ -. Para obtener más información, consulte Reglas para etiquetar en IAM y AWS STS en la Guía del usuario de IAM. Para reclamar los formatos `corp\username` o `corp.example.com\username`, sustituya \ por / en la aserción SAML.
- **`Attribute`**elemento con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/Attributes/:Domain PrincipalTag (opcional): este elemento contiene un elemento `AttributeValue` que proporciona el nombre de dominio completo (FQDN) de DNS de Active Directory para que los usuarios inicien sesión. Este parámetro se usa con la autenticación basada en certificados cuando el `userPrincipalName` de Active Directory del usuario contiene un sufijo alternativo. El valor debe proporcionarse en `domain.com`, incluidos los subdominios.

- **`Attribute`**elemento con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/ Attributes/ SessionDuration (opcional): este elemento contiene un `AttributeValue` elemento que especifica el tiempo máximo que una sesión de streaming federada de un usuario puede permanecer activa antes de que sea necesario volver a autenticarse. El valor predeterminado es de 3600 segundos (60 minutos). Para obtener más información, consulte la `SessionDurationAttribute` de SAML.

  > **Note**
  >
  > Aunque `SessionDuration` es un atributo opcional, se recomienda incluirlo en la respuesta de SAML. Si no especificas este atributo, la duración de la sesión se establece en un valor predeterminado de 3600 segundos (60 minutos). WorkSpaces Las sesiones de escritorio se desconectan una vez expirada la duración de la sesión.

Para obtener más información acerca de cómo configurar estos elementos, consulte Configuración de aserciones SAML para la respuesta de autenticación en la Guía del usuario de IAM. Para obtener información sobre los requisitos de configuración específicos de su IdP, consulte la documentación de su IdP.

Paso 6: configurar el estado de retransmisión de la federación

A continuación, utilice su IdP para configurar el estado de retransmisión de su federación para que apunte a la URL del estado de retransmisión del WorkSpaces directorio. Tras la correcta autenticación AWS, se dirige al usuario al punto final del WorkSpaces directorio, definido como el estado de retransmisión en la respuesta de autenticación SAML.

Este es el formato de la URL del estado de retransmisión:

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

Cree la URL del estado de retransmisión a partir del código de registro del WorkSpaces directorio y el punto final del estado de retransmisión asociado a la región en la que se encuentra el directorio. El código de registro se encuentra en la consola WorkSpaces de administración.

Si lo prefiere, si utiliza la redirección entre regiones WorkSpaces, puede sustituir el código de registro por el nombre de dominio completo (FQDN) asociado a los directorios de las regiones principal

y de conmutación por error. Para obtener más información, consulta Redireccionamiento entre regiones para Amazon. WorkSpaces Cuando se utiliza el redireccionamiento entre regiones y la autenticación SAML 2.0, los directorios principal y de conmutación por error deben estar habilitados para la autenticación SAML 2.0 y configurarse de forma independiente con el IdP, mediante el punto de conexión de estado de retransmisión asociado a cada región. Esto permitirá configurar correctamente el FQDN cuando los usuarios registren sus aplicaciones WorkSpaces cliente antes de iniciar sesión, y permitirá a los usuarios autenticarse durante un evento de conmutación por error.

En la siguiente tabla se enumeran los puntos finales del estado de retransmisión de las regiones en las que está disponible la autenticación WorkSpaces SAML 2.0.

Regiones en las que está WorkSpaces disponible la autenticación SAML 2.0

Región	Punto de conexión del estado de retransmisión
Región del este de EE. UU. (Norte de Virginia)	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
Región del oeste de EE. UU (Oregón)	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
Región África (Ciudad del Cabo)	workspaces.euc-sso.us-east-1.aws.amazon.com
Región de Asia-Pacífico (Bombay)	workspaces.euc-sso.ap-south-1.aws.amazon.com
Región de Asia-Pacífico (Seúl)	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
Región de Asia-Pacífico (Singapur)	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
Región de Asia-Pacífico (Sídney)	workspaces.euc-sso.ap-southeast-1.aws.amazon.com

Región	Punto de conexión del estado de retransmisión
Asia Pacífico (Tokio)	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
Región de Canadá (centro)	workspaces.euc-sso.us-east-1.aws.amazon.com
Región de Europa (Fráncfort)	workspaces.euc-sso.eu-central-1.aws.amazon.com
Región de Europa (Irlanda)	workspaces.euc-sso.eu-west-1.aws.amazon.com
Región de Europa (Londres)	workspaces.euc-sso.eu-west-1.aws.amazon.com
Región de América del Sur (São Paulo)	workspaces.euc-sso.sa-east-1.aws.amazon.com
Región Israel (Tel Aviv)	workspaces.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud (EE. UU.-Oeste)	• workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** Para obtener más información, consulta la Guía del usuario WorkSpaces de AmazonAWS GovCloud (EE. UU.).

Región	Punto de conexión del estado de retransmisión
AWS GovCloud (Este de EE. UU.)	• workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** Para obtener más información, consulta la Guía del usuario WorkSpaces de AmazonAWS GovCloud (EE. UU.).

Paso 7: Habilita la integración con SAML 2.0 en tu directorio WorkSpaces

Puede usar la WorkSpaces consola para habilitar la autenticación SAML 2.0 en el WorkSpaces directorio.

Para activar la integración con SAML 2.0

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija el ID de directorio para su WorkSpaces.
4. En Autenticación, elija Editar.
5. Seleccione Editar proveedor de identidad de SAML 2.0.
6. Seleccione Habilitar la autenticación SAML.
7. En URL de acceso del usuario y Nombre del parámetro de enlace profundo del IdP, introduzca los valores aplicables a su IdP y a la aplicación que ha configurado en el paso 1. El valor predeterminado del nombre del parámetro de enlace profundo del IdP es RelayState «» si se omite este parámetro. En la siguiente tabla se enumeran las URL de acceso de los usuarios y los nombres de los parámetros que son exclusivos de los distintos proveedores de identidad de las aplicaciones.

Dominios y direcciones IP para agregar a la lista de permitidos

Proveedor de identidades	Parámetro	URL de acceso del usuario
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`
Okta	`RelayState`	`https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml`
OneLogin	`RelayState`	`https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>`
JumpCloud	`RelayState`	`https://sso.jumpcloud.com/saml2/<app-id>`
Auth0	`RelayState`	`https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>`

Proveedor de identidades	Parámetro	URL de acceso del usuario
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>`
PingOne para Enterprise	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

El proveedor suele definir la URL de acceso del usuario para el SSO iniciado por un IdP no solicitado. Un usuario puede introducir esta URL en un navegador web para federarse directamente con la aplicación SAML. Para probar la URL de acceso del usuario y los valores de los parámetros de su IdP, elija Probar. Copie y pegue la URL de prueba en una ventana privada de su navegador actual o de otro navegador para probar el inicio de sesión con SAML 2.0 sin interrumpir la sesión actual de la consola AWS de administración. Cuando se abra el flujo iniciado por el IdP, podrá registrar a su WorkSpaces cliente. Para obtener más información, consulte Flujo iniciado por el proveedor de identidades (IdP).

8. Para administrar la configuración alternativa, active o desactive Permitir que los clientes que no sean compatibles con SAML 2.0 inicien sesión. Active esta configuración para seguir proporcionando a sus usuarios el acceso al WorkSpaces uso de tipos de clientes o versiones que no sean compatibles con SAML 2.0 o si los usuarios necesitan tiempo para actualizar a la última versión del cliente.

> **Note**
>
> Esta configuración permite a los usuarios omitir SAML 2.0 e iniciar sesión mediante la autenticación de directorio con versiones de cliente anteriores.

9. Para usar SAML con el cliente web, habilite Acceso web. Para obtener más información, consulte Habilitar y configurar Amazon WorkSpaces Web Access.

> **Note**
>
> Acceso web no admite PCoIP con SAML.

10. Seleccione Guardar. Su WorkSpaces directorio ahora está habilitado con la integración de SAML 2.0. Puede utilizar los flujos iniciados por el IdP y por la aplicación cliente para registrar las aplicaciones WorkSpaces cliente e iniciar sesión en ellas. WorkSpaces

Autenticación basada en certificados

Puede utilizar la autenticación basada en certificados WorkSpaces para eliminar la solicitud de usuario de la contraseña del dominio de Active Directory. Al usar la autenticación basada en certificados con su dominio de Active Directory, puede:

- Confiar en su proveedor de identidades SAML 2.0 para autenticar al usuario y proporcionar declaraciones de SAML que coincidan con las del usuario de Active Directory.
- Crear una experiencia de inicio de sesión único con menos solicitudes al usuario.
- Habilitar los flujos de autenticación sin contraseña con su proveedor de identidades SAML 2.0.

La autenticación basada en certificados utiliza los AWS Private CA recursos de su cuenta. AWS AWS Private CA permite la creación de jerarquías de autoridades de certificación (CA) privadas, incluidas las CA raíz y subordinadas. Con él AWS Private CA, puede crear su propia jerarquía de entidades de certificación y emitir certificados con ella para autenticar a los usuarios internos. Para obtener más información, consulte la Guía del usuario de AWS Private Certificate Authority.

Cuando se utilice AWS Private CA para la autenticación basada en certificados, WorkSpaces solicitará los certificados para sus usuarios automáticamente durante la autenticación de la sesión. Autentica a los usuarios en Active Directory con una tarjeta inteligente virtual proporcionada con los certificados.

La autenticación basada en certificados es compatible con los paquetes de Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) que utilizan las aplicaciones cliente de WorkSpaces Web Access, Windows y macOS más recientes. Abre las descargas de Amazon WorkSpaces Client para encontrar las versiones más recientes:

- Cliente de Windows (versión 5.5.0 o posterior)

- Cliente para macOS (versión 5.6.0 o posterior)

Para obtener más información sobre la configuración de la autenticación basada en certificados con Amazon WorkSpaces, consulte Cómo configurar la autenticación basada en certificados para Amazon WorkSpaces y Consideraciones de diseño en entornos altamente regulados para la autenticación basada en certificados con 2.0 y. AppStream WorkSpaces

Requisitos previos

Realice los siguientes pasos antes de habilitar la autenticación basada en certificados.

1. Configure su WorkSpaces directorio con la integración de SAML 2.0 para utilizar la autenticación basada en certificados. Para obtener más información, consulte WorkSpacesIntegración con SAML 2.0.
2. Configurar el atributo `userPrincipalName` en su declaración de SAML. Para obtener más información, consulte Crear declaraciones para la respuesta de autenticación SAML.
3. Configurar el atributo `0bjectSid` en su declaración de SAML. Esto es opcional para realizar un mapeo fuerte al usuario de Active Directory. La autenticación basada en certificados fallará si el atributo no coincide con el identificador de seguridad (SID) de Active Directory para el usuario especificado en SAML_Subject `NameID`. Para obtener más información, consulte Crear declaraciones para la respuesta de autenticación SAML.
4. Añada el TagSession permiso sts: a la política de confianza de roles de IAM utilizada con su configuración de SAML 2.0 si aún no está presente. Este permiso es necesario para usar la autenticación basada en certificados. Para obtener más información, consulte Crear un rol de IAM de federación SAML 2.0..
5. Cree una autoridad de certificación (CA) privada utilizando AWS Private CA si no tiene ninguna configurada en su Active Directory. AWS Private CA es necesario para utilizar la autenticación basada en certificados. Para obtener más información, consulte Planear la AWS Private CA implementación y siga las instrucciones para configurar una CA para la autenticación basada en certificados. Los siguientes AWS Private CA ajustes son los más comunes para los casos de uso de la autenticación basada en certificados:
   a. Opciones de tipo de CA
      i. Modo de uso de CA con certificados de corta duración (se recomienda si la CA solo emite certificados de usuario final para la autenticación basada en certificados)
      ii. Jerarquía de un solo nivel con una CA raíz (también puede elegir una CA subordinada si quiere integrarla con una jerarquía de CA existente)

b. Opciones de algoritmos de clave: RSA 2048

c. Opciones de nombre distintivo por asunto: utilice la combinación de opciones más adecuada para identificar la CA en el almacén de entidades emisoras de certificados raíz de confianza de Active Directory.

d. Opciones de revocación de certificados: distribución de CRL

> **Note**
>
> La autenticación basada en certificados requiere un punto de distribución de CRL en línea al que se pueda acceder tanto desde los escritorios como desde el controlador de dominio. Esto requiere un acceso no autenticado al depósito de Amazon S3 configurado para las entradas privadas de la CRL de CA o a una CloudFront distribución que tendrá acceso al depósito de S3 si bloquea el acceso público. Para obtener más información sobre estas opciones, consulte Planificación de una lista de revocación de certificados (CRL).

6. Etiquete su CA privada con una clave `euc-private-ca` que permita designar la CA para su uso con la autenticación basada en certificados. Esta clave no requiere ningún valor. Para obtener más información, consulte Administrar las etiquetas de su CA privada.

7. La autenticación basada en certificados utiliza tarjetas inteligentes virtuales para iniciar sesión. Siguiendo las directrices para habilitar el inicio de sesión con tarjetas inteligentes con entidades emisoras de certificados de terceros en Active Directory, lleve a cabo los siguientes pasos:

   - Configure los controladores de dominio con un certificado de controlador de dominio para autenticar a los usuarios de tarjetas inteligentes. Si tiene una CA empresarial de Active Directory Certificate Services configurada en su Active Directory, los controladores de dominio se inscriben automáticamente con certificados para permitir el inicio de sesión con tarjeta inteligente. Si no tiene los Servicios de certificados de Active Directory, consulte Requirements for domain controller certificates from a third-party CA. Puede crear un certificado de controlador de dominio con AWS Private CA. Si lo hace, no utilice una CA privada configurada para certificados de corta duración.

> **Note**
>
> Si lo está utilizando AWS Managed Microsoft AD, puede configurar los servicios de certificación en una instancia EC2 para cumplir con el requisito de los certificados de controlador de dominio. Consulte, AWS Launch Wizardpor ejemplo, las

implementaciones de servicios de certificados AWS Managed Microsoft AD configurados con Active Directory. AWS La CA privada se puede configurar como una entidad subordinada a la CA de los servicios de certificados de Active Directory o se puede configurar como su propia raíz cuando se utiliza. AWS Managed Microsoft AD Una tarea de configuración adicional con AWS Managed Microsoft AD los Servicios de certificados de Active Directory consiste en crear reglas de salida desde el grupo de seguridad de VPC del controlador hasta la instancia EC2 que ejecuta los Servicios de certificados, lo que permite que los puertos TCP 135 y 49152-65535 habiliten la inscripción automática de certificados. Además, la instancia EC2 en ejecución también debe permitir el acceso entrante a estos mismos puertos desde las instancias de dominio, incluidos los controladores de dominio. Para obtener más información sobre la ubicación del grupo de seguridad, AWS Managed Microsoft AD consulte Configurar las subredes y grupos de seguridad de la VPC.

- En la AWS Private CA consola o mediante el SDK o la CLI, seleccione su CA y, en el certificado de CA, exporte el certificado privado de CA. Para obtener más información, consulte Exportación de un certificado privado.
- Publique la CA en Active Directory. Inicie sesión en un controlador de dominio o en una máquina asociada a un dominio. Copie el certificado de CA privado en cualquier `<path>\<file>` y ejecute los siguientes comandos como administrador de dominio. También puede usar la política de grupo y la herramienta PKI Health Tool (PKIView) de Microsoft para publicar la CA. Para obtener más información, consulte Configuration instructions.

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

Asegúrese de que los comandos se completen correctamente y, a continuación, elimine el archivo de certificado privado. Según la configuración de replicación de Active Directory, la CA puede tardar varios minutos en publicar en los controladores de dominio y en las instancias de escritorio.

> **Note**
>
> - Es necesario que Active Directory distribuya la CA a las autoridades emisoras de certificados raíz de confianza y Enterprise NTauth las almacena automáticamente para los WorkSpaces escritorios cuando se unen al dominio.

- Los controladores de dominio de Active Directory deben estar en modo de compatibilidad para que la aplicación estricta de los certificados admita la autenticación basada en certificados. Para obtener más información, consulte KB5014754: cambios en la autenticación basada en certificados en los controladores de dominio de Windows en la documentación de Microsoft Support. Si utiliza Microsoft AD AWS administrado, consulte Configurar los ajustes de seguridad de los directorios para obtener más información.

Habilitación de la autenticación basada en certificados

Realice los siguientes pasos antes de habilitar la autenticación basada en certificados.

1. Abra la WorkSpaces consola enhttps://console.aws.amazon.com/workspaces.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija el ID de directorio para su WorkSpaces.
4. En Autenticación, haga clic en Editar.
5. Haga clic en Editar la autenticación basada en certificados.
6. Elija Habilitar la autenticación basada en certificados.
7. Confirme que su ARN de CA privada esté asociado a la lista. La CA privada debe estar en la misma AWS cuenta y Región de AWS debe estar etiquetada con una clave euc-private-ca que pueda aparecer en la lista.
8. Haga clic en Save Changes (Guardar cambios). Ya está habilitada la autenticación basada en certificados.
9. Reinicie los paquetes de Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) para que los cambios surtan efecto. Para obtener más información, consulte Reiniciar un. WorkSpace
10. Tras el reinicio, cuando los usuarios se autentiquen mediante SAML 2.0 mediante un cliente compatible, ya no se les solicitará la contraseña del dominio.

> **Note**
>
> Cuando la autenticación basada en certificados está habilitada para iniciar sesión WorkSpaces, no se solicita a los usuarios la autenticación multifactor (MFA) aunque esté habilitada en el Directorio. Al usar la autenticación basada en certificados, la MFA se puede habilitar a través de su proveedor de identidad SAML 2.0. Para obtener más información

sobre la AWS Directory Service MFA, consulte Autenticación multifactorial (AD Connector) o Habilitar la autenticación multifactorial para. AWS Managed Microsoft AD

Administración de la autenticación basada en certificados

Certificado de entidad de certificación

En una configuración típica, el certificado de CA privada tiene un período de validez de 10 años. Consulte Administración del ciclo de vida de entidad de certificación privada para obtener más información sobre cómo reemplazar una CA privada con un certificado vencido o cómo volver a emitir la CA privada con un nuevo período de validez.

Certificados de usuario final

Los certificados de usuario final emitidos AWS Private CA por la autenticación WorkSpaces basada en certificados no requieren renovación ni revocación. Estos certificados son de corta duración. WorkSpacesemite automáticamente un nuevo certificado cada 24 horas. Estos certificados de usuario final tienen un período de validez más corto que una distribución AWS Private CA CRL típica. Como resultado, no es necesario revocar los certificados de usuario final y no aparecerán en una CRL.

Informes de auditoría

Puede crear un informe de auditoría para mostrar todos los certificados que la CA privada ha emitido o revocado. Para obtener más información, consulte Using audit reports with your private CA.

Registro y supervisión

Se pueden utilizar AWS CloudTrailpara grabar las llamadas a la API a AWS Private CA by WorkSpaces. Para obtener más información, consulte Uso CloudTrail. En el historial de CloudTrail eventos, puede ver `GetCertificate` los nombres de los `IssueCertificate` `acm-pca.amazonaws.com` eventos de la fuente de eventos creados por el nombre WorkSpaces `EcmAssumeRoleSession` de usuario. Estos eventos se registrarán para cada solicitud de autenticación basada en certificados de EUC.

Habilite el uso compartido de PCA entre cuentas

Al utilizar el uso compartido entre cuentas de CA privada, puede conceder permisos a otras cuentas para usar una CA centralizada, lo que elimina la necesidad de una CA privada en todas las

cuentas. La CA puede generar y emitir certificados mediante AWS Resource Access Manager para administrar los permisos. El uso compartido entre cuentas privadas de CA se puede utilizar con la autenticación WorkSpaces basada en certificados (CBA) dentro de la misma región. AWS

Para utilizar un recurso de CA privada compartido con la CBA WorkSpaces

1. Configure la CA privada para la CBA en una cuenta centralizada AWS . Para obtener más información, consulte Autenticación basada en certificados.
2. Comparta la CA privada con las AWS cuentas de recursos en las que WorkSpaces los recursos utilizan la CBA siguiendo los pasos de Cómo usar la AWS RAM para compartir una cuenta cruzada de ACM Private CA. No necesita completar el paso 3 para crear un certificado. Puede compartir la CA privada con AWS cuentas individuales o compartirla a través de AWS Organizations. Para compartir con cuentas individuales, debe aceptar la CA privada compartida en su cuenta de recursos mediante la consola Resource Access Manager (RAM) o las API. Al configurar el recurso compartido, confirme que el recurso compartido de RAM de la CA privada de la cuenta de recursos utiliza la plantilla de permisos `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` gestionados. Esta plantilla se alinea con la plantilla de PCA que utiliza el rol de WorkSpaces servicio al emitir los certificados CBA.
3. Una vez que el intercambio se haya realizado correctamente, podrá ver la CA privada compartida mediante la consola de CA privada de la cuenta de recursos.
4. Utilice la API o la CLI para asociar el ARN de CA privado con el CBA en las propiedades de su WorkSpaces directorio. En este momento, la WorkSpaces consola no admite la selección de ARN de CA privados compartidos. Ejemplos de comandos CLI:

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

Utilizar tarjetas inteligentes para la autenticación

Los paquetes de Windows y Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) permiten el uso de tarjetas inteligentes Common Access Card (CAC) y Personal Identity Verification (PIV) para la autenticación.

Amazon WorkSpaces admite el uso de tarjetas inteligentes tanto para la autenticación previa a la sesión como para la autenticación durante la sesión. La autenticación previa a la sesión se refiere

a la autenticación con tarjeta inteligente que se realiza mientras los usuarios inician sesión en su cuenta. WorkSpaces La autenticación durante la sesión se refiere al proceso que se realiza después de iniciar sesión.

Por ejemplo, los usuarios pueden usar tarjetas inteligentes para la autenticación durante la sesión cuando trabaja con navegadores web y aplicaciones. También pueden usar tarjetas inteligentes para aquellas acciones que requieran permisos administrativos. Por ejemplo, si el usuario tiene permisos administrativos en su sistema Linux WorkSpace, puede usar tarjetas inteligentes para autenticarse cuando ejecuta comandos `sudo` y `sudo -i` ejecuta.

Contenido

Requisitos

- Se requiere un directorio de Active Directory Connector (Conector AD) para la autenticación previa a la sesión. Conector AD utiliza la autenticación Mutual Transport Layer Security (mutual TLS) basada en certificados para autenticar a los usuarios en Active Directory mediante certificados de tarjetas inteligentes basados en hardware o software. Para obtener más información acerca de cómo configurar el Conector AD y el directorio local, consulte Configuración del directorio:.
- Para usar una tarjeta inteligente con Windows o Linux WorkSpace, el usuario debe usar el cliente Amazon WorkSpaces Windows versión 3.1.1 o posterior o el cliente WorkSpaces macOS versión 3.1.5 o posterior. Para obtener más información sobre el uso de tarjetas inteligentes con los clientes de Windows y macOS, consulte Smart Card Support en la Guía del WorkSpaces usuario de Amazon.
- El CA raíz y los certificados de tarjeta inteligente deben cumplir ciertos requisitos. Para obtener más información, consulte Habilitar la autenticación mTLS en Conector AD para usarla con tarjetas inteligentes en la Guía de administración de AWS Directory Service y Requisitos de certificados en la documentación de Microsoft.

  Además de estos requisitos, los certificados de usuario empleados para la autenticación con tarjetas inteligentes en Amazon WorkSpaces deben incluir los siguientes atributos:

  - El nombre del usuario de AD userPrincipalName (UPN) en el campo subjectAltName (SAN) del certificado. Recomendamos emitir certificados de tarjeta inteligente para el UPN predeterminado del usuario.
  - El atributo de uso extendido de claves (EKU) de autenticación de cliente (1.3.6.1.5.5.7.3.2).
  - El atributo EKU de inicio de sesión con tarjeta inteligente (1.3.6.1.4.1.311.20.2.2).
- Para la autenticación previa a la sesión, se requiere el Protocolo de estado de certificados en línea (OCSP) para verificar la revocación de certificados. Para la autenticación durante la sesión, se recomienda el OCSP, pero no es obligatorio.

Limitaciones

- Actualmente, solo la aplicación cliente WorkSpaces Windows versión 3.1.1 o posterior y la aplicación cliente macOS versión 3.1.5 o posterior son compatibles actualmente con la autenticación con tarjeta inteligente.
- La aplicación cliente de WorkSpaces Windows 3.1.1 o posterior solo admite tarjetas inteligentes cuando el cliente se ejecuta en una versión de 64 bits de Windows.
- Actualmente, Ubuntu WorkSpaces no admite la autenticación con tarjeta inteligente.
- Actualmente, solo se admiten los directorios de Conector AD para la autenticación con tarjeta inteligente.
- La autenticación durante la sesión está disponible en todas las regiones donde el WSP sea compatible. La autenticación previa a la sesión está disponible en las siguientes regiones:
  - Región de Asia-Pacífico (Sídney)
  - Región de Asia-Pacífico (Tokio)
  - Región de Europa (Irlanda)
  - AWS GovCloud Región (EE. UU.-Este)
  - AWS GovCloud Región (EE. UU.-Oeste)
  - Región del este de EE. UU. (Norte de Virginia)
  - Región del oeste de EE. UU (Oregón)
- Para la autenticación durante la sesión y la autenticación previa a la sesión en Linux o Windows WorkSpaces, actualmente solo se permite una tarjeta inteligente a la vez.
- Para la autenticación previa a la sesión, actualmente no se permite habilitar la autenticación con tarjeta inteligente y la autenticación de inicio de sesión en el mismo directorio.

- Por el momento, solo se admiten las tarjetas CAC y PIV. Es posible que haya otros tipos de tarjetas inteligentes basadas en hardware o software que también funcionen, pero su uso no se ha probado de forma exhaustiva con WSP.

Configuración del directorio:

Para habilitar la autenticación con tarjeta inteligente, debe configurar el directorio de Conector AD y el directorio en las instalaciones de la siguiente manera.

Configuración del directorio de Conector AD

Antes de empezar, asegúrese de que el directorio de Conector AD se ha configurado tal y como se describe en los requisitos previos de Conector AD en la Guía de administración de AWS Directory Service . En particular, asegúrese de haber abierto los puertos necesarios en el firewall.

Para terminar de configurar el directorio de Conector AD, siga las instrucciones de Habilitar la autenticación mTLS en Conector AD para usarla con tarjetas inteligentes en la Guía de administración de AWS Directory Service .

> **Note**
>
> La autenticación con tarjeta inteligente requiere la delegación restringida de Kerberos (KCD) para funcionar correctamente. KCD requiere que la parte del nombre de usuario de la cuenta de servicio AD Connector coincida con el AccountName SaM del mismo usuario. Un SaM no AccountName puede superar los 20 caracteres.

Configuración de directorios en las instalaciones

Además de configurar su directorio de Conector AD, también debe asegurarse de que los certificados que se emiten a los controladores de dominio para su directorio en las instalaciones tengan configurado el uso de clave extendida (EKU) de «Autenticación de KDC». Para ello, utilice la plantilla de certificado de autenticación Kerberos predeterminada de Active Directory Domain Services (AD DS). No utilice una plantilla de certificado de controlador de dominio ni una plantilla de certificado de autenticación de controlador de dominio porque esas plantillas no contienen la configuración necesaria para la autenticación con tarjetas inteligentes.

Habilite las tarjetas inteligentes para Windows WorkSpaces

Para obtener instrucciones generales sobre cómo habilitar la autenticación con tarjeta inteligente en Windows, consulte Directrices para habilitar el inicio de sesión de tarjeta inteligente con entidades de certificación de terceros en la documentación de Microsoft.

Para detectar la pantalla de bloqueo de Windows y desconectar la sesión

Para permitir a los usuarios desbloquear las ventanas WorkSpaces que están habilitadas para la autenticación previa a la sesión con tarjetas inteligentes cuando la pantalla está bloqueada, puede habilitar la detección de la pantalla de bloqueo de Windows en las sesiones de los usuarios. Cuando se detecta la pantalla de bloqueo de Windows, la WorkSpace sesión se desconecta y el usuario puede volver a conectarse desde el WorkSpaces cliente mediante su tarjeta inteligente.

Puede habilitar la desconexión de la sesión cuando se detecte la pantalla de bloqueo de Windows mediante la configuración de la política de grupo. Para obtener más información, consulte Activar o desactivar la sesión de desconexión en el bloqueo de pantalla para WSP.

Para habilitar la autenticación durante o antes de la sesión

De forma predeterminada, Windows WorkSpaces no admite el uso de tarjetas inteligentes para la autenticación previa o durante la sesión. Si es necesario, puede habilitar la autenticación durante y antes de la sesión para Windows WorkSpaces mediante la configuración de la política de grupo. Para obtener más información, consulte Activar o desactivar el redireccionamiento de tarjeta inteligente para WSP.

Para usar la autenticación previa a la sesión, además de actualizar la configuración de la política de grupo, también debe habilitar la autenticación previa a la sesión a través de la configuración del directorio de Conector AD. Para obtener más información, siga las instrucciones de Habilitar la autenticación mTLS en Conector AD para usarla con tarjetas inteligentes en la Guía de administración de AWS Directory Service .

Para permitir a los usuarios utilizar tarjetas inteligentes en un navegador

Si los usuarios utilizan Chrome como navegador, no es necesaria ninguna configuración especial para utilizar tarjetas inteligentes.

Si los usuarios utilizan Firefox como navegador, puede permitir que usen tarjetas inteligentes en Firefox mediante la política de grupo. Puedes usar estas plantillas de políticas de grupo de Firefox en. GitHub

Por ejemplo, puede instalar la versión de 64 bits de OpenSC para Windows para que sea compatible con PKCS #11 y, a continuación, usar la siguiente configuración de política de grupo, donde *NAME_OF_DEVICE* es el valor que desee usar para identificar PKCS #11, por ejemplo `OpenSC`, y donde *PATH_TO_LIBRARY_FOR_DEVICE* es la ruta al módulo PKCS #11. Esta ruta debe apuntar a una biblioteca con la extensión.DLL, como `C:\Program Files\OpenSC Project\OpenSC \pkcs11\onepin-opensc-pkcs11.dll`.

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

Si utiliza OpenSC, también puedes cargar el módulo `pkcs11` de OpenSC en Firefox ejecutando el programa. `pkcs11-register.exe`. Para ejecutar este programa, haga doble clic en `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` en el archivo o abra una ventana de línea de comandos y ejecute el siguiente comando:

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

Para verificar que el módulo `pkcs11` de OpenSC se cargó en Firefox, haga lo siguiente:

1. Si Firefox ya se está ejecutando, debe cerrarlo.
2. Abra Firefox. Seleccione el botón de menú

   ,

   en la esquina superior derecha, y seleccione Opciones.
3. En la página about:preferences, en el panel de navegación de la izquierda, seleccione Privacidad y seguridad.
4. En Certificados, seleccione Dispositivos de seguridad.
5. En el cuadro de diálogo del Administrador de dispositivos, debería aparecer OpenSC smartcard framework (0.21) en el menú de navegación izquierdo. Al seleccionarlo, tendrá los siguientes valores:

   Módulo: `OpenSC smartcard framework (0.21)`

Ruta: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

Solución de problemas

Para obtener información sobre la solución de problemas de tarjetas inteligentes, consulte Problemas de certificado y configuración en la documentación de Microsoft.

Algunos errores comunes que pueden causar problemas:

- Asignación incorrecta de slots a los certificados.
- Tener varios certificados en la tarjeta inteligente que puedan coincidir con los del usuario. Los certificados se comparan según los siguientes criterios:
  - La CA raíz del certificado.
  - Los campos <EKU> y <KU> del certificado.
  - El UPN del asunto del certificado.
- Tener varios certificados que incluyan `<EKU>msScLogin` en su clave el uso.

En general, es mejor tener un solo certificado para la autenticación con tarjeta inteligente que esté asignado al primer slot de la tarjeta inteligente.

Las herramientas para administrar los certificados y las claves de la tarjeta inteligente (como quitar o reasignar los certificados y las claves) pueden ser específicas del fabricante. Para obtener más información, consulte la documentación facilitada por el fabricante de sus tarjetas inteligentes.

Habilita las tarjetas inteligentes para Linux WorkSpaces

Note

Actualmente, Linux WorkSpaces en WSP tiene las siguientes limitaciones:

- No se admiten el portapapeles, la entrada de audio, la entrada de vídeo ni el redireccionamiento de zona horaria.
- No se admiten varios monitores.

- Debe usar la aplicación cliente de WorkSpaces Windows para conectarse a Linux WorkSpaces en WSP.

Para habilitar el uso de tarjetas inteligentes en Linux WorkSpaces, debe incluir un archivo de certificado de CA raíz en formato PEM en la WorkSpace imagen.

Para obtener el certificado de CA raíz

Puede obtener su certificado de CA raíz de varias maneras:

- Puede utilizar un certificado de CA raíz gestionado por una entidad emisora de certificados externa.
- Puede exportar su propio certificado CA raíz utilizando el sitio web de registro, ya sea `http://`*`ip_address`*`/certsrv` o `http://`*`fqdn`*`/certsrv`, donde *`ip_address`* y *`fqdn`* son la dirección IP y el nombre de dominio completo (FQDN) del servidor de CA de certificación raíz. Para obtener más información sobre el uso del sitio web de registro, consulte Exportación del certificado de entidad de certificación raíz en la documentación de Microsoft.
- Puede usar el siguiente procedimiento para exportar el certificado de CA raíz desde un servidor de certificación de CA raíz que ejecute Active Directory Certificate Services (AD CS). Para obtener información sobre la instalación de AD CS, consulte Instalar la entidad de certificación en la documentación de Microsoft.

  1. Inicie sesión en el servidor de CA raíz con una cuenta de administrador.
  2. En el menú Inicio de Windows, abra una ventana de línea de comandos (Inicio > Sistema Windows > Símbolo del sistema).
  3. Utilice el siguiente comando para exportar el certificado de CA raíz a un nuevo archivo, donde *`rootca`*`.cer` aparece el nombre del nuevo archivo:

     ```
     certutil -ca.cert rootca.cer
     ```

     Para obtener más información acerca de cómo ejecutar certutil, consulte certutil en la documentación de Microsoft.
  4. Utilice el siguiente comando OpenSSL para convertir el certificado de CA raíz exportado del formato DER al formato PEM, donde *`rootca`* es el nombre del certificado. Para obtener más información acerca de OpenSSL, consulte http://www.openssl.org/.

```
openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
```

Para añadir el certificado de CA raíz a su Linux WorkSpaces

Para ayudarle a habilitar las tarjetas inteligentes, hemos añadido el script `enable_smartcard` a nuestros paquetes Amazon Linux WSP. Este script realiza las siguientes acciones:

- Importa su certificado de CA raíz a la base de datos de Network Security Services (NSS).
- Instala el módulo `pam_pkcs11` para la autenticación del módulo de autenticación conectable (PAM).
- Realiza una configuración predeterminada, que incluye la activación `pkinit` durante el WorkSpace aprovisionamiento.

El siguiente procedimiento explica cómo usar el `enable_smartcard` script para agregar el certificado de CA raíz a su Linux WorkSpaces y habilitar las tarjetas inteligentes para su Linux. WorkSpaces

1. Cree un nuevo Linux WorkSpace con el protocolo WSP activado. Al iniciar el WorkSpace en la WorkSpaces consola de Amazon, en la página Select Bundles, asegúrese de seleccionar WSP para el protocolo y, a continuación, seleccione uno de los paquetes públicos de Amazon Linux 2.
2. En la nueva versión WorkSpace, ejecute el siguiente comando como root, donde *pem-path* está la ruta al archivo de certificado raíz de CA en formato PEM.

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path
   ```

   > **Note**
   >
   > Linux WorkSpaces supone que los certificados de las tarjetas inteligentes se emiten para el nombre principal de usuario (UPN) predeterminado del usuario, por ejemplo, si *domain* es un nombre de dominio completo (FQDN). *sAMAccountName*@*domain*
   > Si quiere utilizar sufijos UPN alternativos, consulte `run /usr/lib/skylight/enable_smartcard --help` para obtener más información. La asignación de sufijos UPN alternativos es exclusiva de cada usuario. Por lo tanto, ese mapeo debe realizarse de forma individual en el de cada usuario. WorkSpace

3. (Opcional) De forma predeterminada, todos los servicios están habilitados para usar la autenticación con tarjeta inteligente en Linux WorkSpaces. Para limitar la autenticación con tarjetas inteligentes solo a servicios específicos, debe editar `/etc/pam.d/system-auth`. Elimine los comentarios de la línea `auth` de `pam_succeed_if.so` y edite la lista de servicios según sea necesario.

   Una vez eliminados los comentarios de la línea `auth`, para permitir que un servicio utilice la autenticación con tarjetas inteligentes, debe agregarlo a la lista. Para hacer que un servicio utilice únicamente la autenticación mediante contraseña, debe quitarlo de la lista.

4. Realice cualquier personalización adicional en el WorkSpace. Por ejemplo, es posible que desee añadir una política para todo el sistema que permita a los usuarios usar tarjetas inteligentes en Firefox. (Los usuarios de Chrome deben habilitar ellos mismos las tarjetas inteligentes en sus clientes. Para obtener más información, consulte Smart Card Support en la Guía del WorkSpaces usuario de Amazon.)
5. Cree una WorkSpace imagen y un paquete personalizados a partir de WorkSpace.
6. Utilice el nuevo paquete personalizado para lanzarlo WorkSpaces para sus usuarios.

Para permitir a los usuarios utilizar tarjetas inteligentes en Firefox

Puedes permitir que tus usuarios usen tarjetas inteligentes en Firefox añadiendo una SecurityDevices política a tu WorkSpace imagen de Linux. Para obtener más información sobre cómo añadir políticas para todo el sistema a Firefox, consulta las plantillas de políticas de Mozilla en. GitHub

1. En el archivo WorkSpace que estés usando para crear la WorkSpace imagen, crea un nuevo archivo con el nombre `policies.json` in. `/usr/lib64/firefox/distribution/`
2. En el archivo JSON, agrega la siguiente SecurityDevices política, donde *`NAME_OF_DEVICE`* está el valor que quieras usar para identificar el `pkcs` módulo. Por ejemplo, es posible que desee usar un valor como `"OpenSC"`:

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

Solución de problemas

Para solucionar problemas, recomendamos agregar la función `pkcs11-tools`. Le permite realizar las siguientes acciones:

- Enumerar cada tarjeta inteligente.
- Enumerar los slots de cada tarjeta inteligente.
- Enumerar los certificados de cada tarjeta inteligente.

Algunos errores comunes que pueden causar problemas:

- Asignación incorrecta de slots a los certificados.
- Tener varios certificados en la tarjeta inteligente que puedan coincidir con los del usuario. Los certificados se comparan según los siguientes criterios:
  - La CA raíz del certificado.
  - Los campos <EKU> y <KU> del certificado.
  - El UPN del asunto del certificado.
- Tener varios certificados que incluyan <EKU>`msScLogin` en su clave el uso.

En general, es mejor tener un solo certificado para la autenticación con tarjeta inteligente que esté asignado al primer slot de la tarjeta inteligente.

Las herramientas para administrar los certificados y las claves de la tarjeta inteligente (como quitar o reasignar los certificados y las claves) pueden ser específicas del fabricante. Otras herramientas que puede usar para trabajar con tarjetas inteligentes son:

- `opensc-explorer`
- `opensc-tool`
- `pkcs11_inspect`
- `pkcs11_listcerts`
- `pkcs15-tool`

Para habilitar el registro de depuración

Para solucionar los problemas de configuración de `pam_pkcs11` y `pam-krb5`, puede activar el registro de depuración.

1. En el archivo `/etc/pam.d/system-auth-ac`, edite la acción `auth` y cambie el parámetro `nodebug` de `pam_pksc11.so` a `debug`.
2. En el archivo `/etc/pam_pkcs11/pam_pkcs11.conf`, cambie `debug = false;` por `debug = true;`. La opción `debug` se aplica por separado a cada módulo del mapeador, por lo que puede que tenga que cambiarla directamente en la sección `pam_pkcs11` y en la sección del mapeador correspondiente (de forma predeterminada, `mapper generic`)
3. En el archivo `/etc/pam.d/system-auth-ac`, edite la acción `auth` y cambie el parámetro `debug` o `debug_sensitive` a `pam_krb5.so`.

Una vez activado el registro de depuración, el sistema imprime los mensajes de depuración de `pam_pkcs11` directamente en el terminal activo. Los mensajes de `pam_krb5` se registran en `/var/log/secure`.

Para comprobar el nombre de usuario al que se asigna un certificado de tarjeta inteligente, utilice el siguiente comando `pklogin_finder`:

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

Cuando se le solicite, escriba el PIN de la tarjeta inteligente. `pklogin_finder` muestra en `stdout` el nombre de usuario que figura en el certificado de la tarjeta inteligente del formulario *`NETBIOS`*`\`*`username`*. Este nombre de usuario debe coincidir con el WorkSpace nombre de usuario.

En Active Directory Domain Services (AD DS), el nombre de dominio de NetBIOS es el nombre de dominio anterior a Windows 2000. Normalmente (pero no siempre), el nombre de dominio de NetBIOS es el subdominio del nombre de dominio del sistema de nombres de dominio (DNS). Por ejemplo, si el nombre de dominio de DNS es `example.com`, normalmente el dominio de NetBIOS será `EXAMPLE`. Si el nombre de dominio de DNS es `corp.example.com`, normalmente el dominio de NetBIOS será `CORP`.

Por ejemplo, para el usuario `mmajor` del dominio `corp.example.com`, el resultado de `pklogin_finder` es `CORP\mmajor`.

> **Note**
>
> Si recibe el mensaje `"ERROR:pam_pkcs11.c:504: verify_certificate() failed"`, significa que `pam_pkcs11` ha encontrado un certificado en la tarjeta inteligente que coincide con los criterios del nombre de usuario, pero que no está vinculado a un certificado de CA raíz reconocido por la máquina. Si esto ocurre, `pam_pkcs11` muestra el mensaje anterior y,

a continuación, prueba con el siguiente certificado. Solo permite la autenticación si encuentra un certificado que coincide con el nombre de usuario y se vincula a un certificado de CA raíz reconocido.

Para solucionar los problemas de la configuración de `pam_krb5`, puede invocar `kinit` manualmente en el modo de depuración con el siguiente comando:

```
KRB5_TRACE=/dev/stdout kinit -V
```

Este comando debería obtener correctamente un ticket de concesión de Kerberos (TGT). Si se produce un error, intente añadir el nombre principal correcto de Kerberos de forma explícita al comando. Por ejemplo, para el usuario `mmajor` del dominio `corp.example.com`, utilice este comando:

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

Si este comando se ejecuta correctamente, lo más probable es que el problema se deba a la asignación del WorkSpace nombre de usuario al nombre principal de Kerberos. Consulte la sección `[appdefaults]/pam/mappings` del archivo `/etc/krb5.conf`.

Si este comando no funciona, pero sí un comando `kinit` basado en contraseña, compruebe las configuraciones relacionadas con `pkinit_` en el archivo `/etc/krb5.conf`. Por ejemplo, si la tarjeta inteligente contiene más de un certificado, es posible que deba realizar cambios en `pkinit_cert_match`.

Proporcione acceso a Internet desde su WorkSpace

WorkSpaces Debe tener acceso a Internet para poder instalar actualizaciones del sistema operativo e implementar aplicaciones. Puede utilizar una de las siguientes opciones para permitir el WorkSpaces acceso a Internet desde una nube privada virtual (VPC).

Opciones

- WorkSpaces Inicie sus subredes privadas y configure una puerta de enlace NAT en una subred pública de su VPC.
- Lance sus WorkSpaces subredes públicas y asigne direcciones IP públicas a las suyas de forma automática o manual. WorkSpaces

Para obtener más información sobre estas opciones, consulte las secciones correspondientes de Configurar una VPC para WorkSpaces.

Con cualquiera de estas opciones, debe asegurarse de que su grupo de seguridad WorkSpaces permita el tráfico saliente en los puertos 80 (HTTP) y 443 (HTTPS) hacia todos los destinos (`0.0.0.0/0`).

Biblioteca de extras de Amazon Linux

Si utiliza el repositorio de Amazon Linux, su Amazon Linux WorkSpaces debe tener acceso a Internet o debe configurar los puntos de enlace de VPC para este repositorio y para el repositorio principal de Amazon Linux. Para obtener más información, consulte la sección que muestra el ejemplo sobre habilitación de acceso a repositorios de la AMI de Amazon Linux AMI en Puntos de conexión de Amazon S3. Los repositorios de AMI de Amazon Linux son buckets de Amazon S3 en cada región. Si desea que las instancias de su VPC obtengan acceso a los repositorios a través de un punto de enlace, puede crear una política de puntos de enlace que permita el acceso a estos buckets. La siguiente política permite obtener acceso a los repositorios de Amazon Linux.

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

Grupos de seguridad para su WorkSpaces

Al registrar un directorio WorkSpaces, se crean dos grupos de seguridad, uno para los controladores de directorio y otro para WorkSpaces el directorio. El grupo de seguridad de los controladores de directorio tiene un nombre que consta del identificador de directorio seguido de _controllers (por

ejemplo, d-12345678e1_controllers). El grupo de seguridad para WorkSpaces tiene un nombre que consiste en el identificador del directorio seguido de _WorkspacesMembers (por ejemplo, D-123456FC11_WorkspacesMembers).

> **Warning**
>
> Evite modificar, eliminar o separar los grupos de seguridad _controllers y _WorkspacesMembers. Tenga cuidado al modificar o eliminar estos grupos de seguridad, ya que no podrá volver a crearlos ni volver a agregarlos después de haberlos modificado o eliminado. Para obtener más información, consulte Grupos de seguridad de Amazon EC2 para instancias de Linux o Grupos de seguridad de Amazon EC2 para instancias de Windows.

Puede agregar un grupo de seguridad predeterminado a un directorio WorkSpaces . Después de asociar un nuevo grupo de seguridad a un WorkSpaces directorio, el nuevo grupo de seguridad WorkSpaces que inicie o el existente WorkSpaces que regenere tendrá el nuevo grupo de seguridad. También puede agregar este nuevo grupo de seguridad predeterminado a los existentes WorkSpaces sin volver a crearlos, como se explica más adelante en este tema.

Al asociar varios grupos de seguridad a un WorkSpaces directorio, las reglas de cada grupo de seguridad se agregan de manera efectiva para crear un conjunto de reglas. Recomendamos condensar las reglas de grupo de seguridad tanto como sea posible.

Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.

Para agregar un grupo de seguridad a un WorkSpaces directorio

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions, Update Details.
4. Amplíe Security Group y seleccione un grupo de seguridad.
5. Elija Update and Exit.

Para añadir un grupo de seguridad a uno existente WorkSpace sin volver a crearlo, asigne el nuevo grupo de seguridad a la elastic network interface (ENI) del WorkSpace.

Para agregar un grupo de seguridad a un grupo existente WorkSpace

1. Busque la dirección IP de cada uno de ellos WorkSpace que necesite actualizarse.
   a. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
   b. Amplíe cada una WorkSpace y registre su dirección WorkSpace IP.
2. Busque el ENI de cada uno WorkSpace y actualice su asignación de grupo de seguridad.
   a. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   b. En Red y seguridad, elija Interfaces de red.
   c. Busque la primera dirección IP que registró en el paso 1.
   d. Seleccione el ENI asociado a la dirección IP, elija Acciones, y, a continuación, elija Cambiar grupos de seguridad.
   e. Seleccione el nuevo grupo de seguridad y elija Guardar.
   f. Repita este proceso según sea necesario para cualquier otro WorkSpaces.

Grupos de control de acceso a direcciones IP para los escritorios de WorkSpaces

Amazon WorkSpaces le permite controlar las direcciones IP desde las que se puede acceder a sus WorkSpaces. Al usar grupos de control basados en direcciones IP, puede definir y administrar grupos de direcciones IP de confianza y solo permitir que los usuarios accedan a sus WorkSpaces cuando están conectados a una red de confianza.

Un grupo de control de acceso a direcciones IP actúa como un firewall virtual que controla las direcciones IP desde las que los usuarios pueden tener acceso a sus escritorios de WorkSpaces. Para especificar los rangos de direcciones del CIDR, añada reglas a su grupo de control de acceso de IP y, a continuación, asocie el grupo a su directorio. Puede asociar cada grupo de control de acceso a direcciones IP a uno o varios directorios. Puede crear hasta 100 grupos de control de acceso a direcciones IP por cada cuenta de AWS. Sin embargo, solo puede asociar un máximo de 25 grupos de control de acceso a direcciones IP a cada directorio.

Hay un grupo de control de acceso a direcciones IP predeterminado asociado a cada directorio. Este grupo predeterminado incluye una regla predeterminada que permite a los usuarios acceder a sus WorkSpaces desde cualquier lugar. No puede modificar el grupo de control de acceso a direcciones IP predeterminado de su directorio. Si no asocia un grupo de control de acceso a direcciones IP

a su directorio, se utilizará el grupo predeterminado. Si asocia un grupo de control de acceso a direcciones IP a un directorio, se desvincula el grupo predeterminado.

Para especificar las direcciones IP públicas y los intervalos de direcciones IP para sus redes de confianza, añada reglas a sus grupos de control de acceso a direcciones IP. Si los usuarios tienen acceso a los WorkSpaces a través de una gateway NAT o VPN, debe crear reglas que permitan el tráfico desde las direcciones IP públicas para la gateway NAT o VPN.

> **Note**
>
> - Los grupos de control de acceso IP no permiten utilizar direcciones IP dinámicas con NAT. Si utiliza una NAT, configúrela para que use una dirección IP estática en lugar de una dinámica. Asegúrese de que la NAT direcciona todo el tráfico UDP a través de la misma dirección IP estática mientras dura la sesión de WorkSpaces.
> - Los grupos de control de acceso a direcciones IP controlan las direcciones IP desde las que los usuarios pueden conectar sus sesiones de streaming a WorkSpaces. Los usuarios pueden seguir ejecutando funcionalidades, como reiniciar entornos, volver a crearlos o cerrarlos, desde cualquier dirección IP mediante las API públicas de Amazon WorkSpaces.

Puede utilizar esta característica con Acceso web, clientes cero de PCoIP y las aplicaciones cliente de macOS X, iPad, Windows, Chromebook y Android.

Cree un grupo de control de acceso a direcciones IP

Puede crear un grupo de control de acceso a direcciones IP como sigue. Cada grupo de control de acceso a direcciones IP puede contener hasta 10 reglas.

Para crear un grupo de control de acceso a direcciones IP

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione IP Access Controls (Controles de acceso a direcciones IP).
3. Elija Create IP Group (Crear grupo de IP).
4. En el cuadro de diálogo Create IP Group (Crear grupo de IP), introduzca un nombre y una descripción para el grupo, y elija Create (Crear).
5. Seleccione el grupo y elija Edit (Editar).

6. Para cada dirección IP, elija Add Rule (Añadir regla). En Source (Origen), introduzca la dirección IP o el intervalo de direcciones IP. En Description (Descripción), escriba una descripción. Cuando haya acabado de añadir reglas, elija Save (Guardar).

Asociar un grupo de control de acceso a direcciones IP a un directorio

Puede asociar un grupo de control de acceso a direcciones IP a un directorio para asegurarse de que solo se tenga acceso a los escritorios de WorkSpaces desde redes de confianza.

Si asocia un grupo de control de acceso a direcciones IP que no tiene reglas a un directorio, se bloquea todo el acceso a todos los escritorios de WorkSpaces.

Para asociar un grupo de control de acceso a direcciones IP a un directorio

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions, Update Details.
4. Expanda IP Access Control Groups (Grupos de control de acceso a direcciones IP) y seleccione uno o varios grupos.
5. Elija Update and Exit.

Copiar un grupo de control de acceso a direcciones IP

Puede utilizar un grupo de control de acceso a direcciones IP existente como punto de partida para crear un nuevo grupo de control de acceso a direcciones IP.

Para crear un grupo de control de acceso a direcciones IP a partir de uno existente

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione IP Access Controls (Controles de acceso a direcciones IP).
3. Seleccione el grupo y elija Actions (Acciones), Copy to New (Copiar en nuevo).
4. En el cuadro de diálogo Copy IP Group (Copiar grupo de IP), escriba un nombre y una descripción para el nuevo grupo, y elija Copy Group (Copiar grupo).
5. (Opcional) Para modificar las reglas copiadas del grupo original, seleccione el nuevo grupo y elija Edit (Editar). Añada, actualice o elimine reglas según sea necesario. Seleccione Save.

Elimine un grupo de control de acceso de IP

Puede eliminar una regla de un grupo de control de acceso a direcciones IP en cualquier momento. Si elimina una regla que se utilizó para permitir una conexión a un escritorio de WorkSpaces, el usuario se desconecta del escritorio de WorkSpaces.

Para poder eliminar un grupo de control de acceso a direcciones IP, debe desvincularlo de todos los directorios.

Para eliminar un grupo de control de acceso a direcciones IP

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Para cada directorio asociado al grupo de control de acceso a direcciones IP, seleccione el directorio y haga clic en Actions (Acciones), Update Details (Actualizar detalles). Expanda IP Access Control Groups (Grupos de control de acceso a direcciones IP), desactive la casilla del grupo de control de acceso a direcciones IP y, a continuación, seleccione Update and Exit (Actualizar y salir).
4. En el panel de navegación, seleccione IP Access Controls (Controles de acceso a direcciones IP).
5. Seleccione el grupo y elija Actions (Acciones), Delete IP Group (Eliminar grupo de IP).

Configuración del cliente de PCoIP Zero para WorkSpaces

Los clientes cero PCoIP solo son compatibles con los paquetes WorkSpaces que utilizan el protocolo PCoIP.

Si el dispositivo de cliente cero tiene firmware versión 6.0.0 o posterior, los usuarios pueden conectarse a sus WorkSpaces directamente. Cuando los usuarios se conectan directamente a sus WorkSpaces utilizando un dispositivo de cliente cero, recomendamos utilizar la autenticación multifactor (MFA) con el directorio de WorkSpaces. Para más información sobre el uso de MFA con su directorio, consulte la siguiente documentación:

- AWS Managed Microsoft AD: Habilite la autenticación multifactor para AWS Managed Microsoft AD in the Guía de administración de AWS Directory Service
- Conector AD: Habilite la autenticación multifactor para el Conector AD en la Guía de administración de AWS Directory Service y Autenticación multifactor (Conector AD)

- Dominios de confianza: Habilite la autenticación multifactor para AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service
- AD sencillo: La autenticación multifactor no está disponible para AD sencillo.

A partir del 13 de abril de 2021, ya no se admite el uso de PCoIP Connection Manager con versiones de firmware de dispositivos cliente cero comprendidas entre las versiones 4.6.0 y 6.0.0. Si el firmware de su cliente cero no es de la versión 6.0.0 o posterior, puede obtener el firmware más reciente mediante una suscripción a https://www.teradici.com/desktop-access.

> **Important**
>
> - En la Administrative Web Interface (AWI, interfaz web administrativa) de Teradici PCoIP o en la Management Console (MC, consola de administración) de Teradici PCoIP, asegúrese de habilitar el Network Time Protocol (NTP, protocolo de tiempo en redes). Para el nombre DNS del host NTP, utilice **`pool.ntp.org`** y establezca el puerto host NTP como 123. Si NTP no está habilitado, los usuarios del cliente cero PCoIP podrían recibir errores de certificado, como “El certificado suministrado no es válido debido a la marca temporal”.
> - A partir de la versión 20.10.4 del agente PCoIP, Amazon WorkSpaces deshabilita el redireccionamiento USB de forma predeterminada a través del registro de Windows. Esta configuración de registro afecta al comportamiento de los periféricos USB cuando los usuarios utilizan dispositivos cliente cero PCoIP para conectarse a sus WorkSpaces. Para obtener más información, consulte Las impresoras USB y otros periféricos USB no funcionan para los clientes cero PCoIP.

Para obtener información acerca de cómo configurar y conectar con un dispositivo de cliente cero PCoIP, consulte Cliente cero de PCoIP en la Guía del usuario de Amazon WorkSpaces. Para obtener una lista de los dispositivos de cliente cero PCoIP aprobados, consulte Clientes cero de PCoIP en el sitio web de Teradici.

Configurar Android para Chromebooks

La versión 2.4.13 es la versión final de la aplicación cliente Amazon WorkSpaces Chromebook. Como Google está eliminando gradualmente la compatibilidad con las aplicaciones de Chrome, no habrá más actualizaciones en la aplicación cliente de WorkSpaces Chromebook y no se admite su uso.

En el caso de los Chromebooks que admiten la instalación de aplicaciones de Android, te recomendamos que utilices en su lugar la aplicación cliente de Android. WorkSpaces

Algunos Chromebooks lanzados antes de 2019 deben estar habilitados para instalar aplicaciones Android antes de que los usuarios puedan instalar la aplicación cliente Amazon WorkSpaces Android. Para obtener más información, consulte Chrome OS Systems Supporting Android Apps.

Para administrar de forma remota la habilitación para que los Chromebooks de los usuarios instalen aplicaciones Android, consulte Set up Android on Chrome devices.

Habilitar y configurar Amazon WorkSpaces Web Access

La mayoría WorkSpaces de los paquetes son compatibles con Amazon WorkSpaces Web Access. Para ver una lista de los paquetes de Amazon WorkSpaces compatibles con el acceso a navegadores web, consulta «¿Qué WorkSpaces paquetes de Amazon admiten el acceso web?» en Acceso de clientes, Acceso web y Experiencia de usuario.

> **Note**
>
> - El acceso web con WSP para Windows y Ubuntu WorkSpaces es compatible en todas las regiones en las que WSP WorkSpaces esté disponible. WSP para Amazon Linux solo WorkSpaces está disponible en AWS GovCloud (EE. UU. al oeste).
> - Recomendamos encarecidamente utilizar Web Access con WSP WorkSpaces para obtener la mejor calidad de streaming y la mejor experiencia de usuario. Las siguientes son limitaciones al utilizar Web Access con WorkSpaces PCoIP:
>   - El acceso a la web con PCoIP no es compatible en Asia Pacífico (Bombay), África (Ciudad del Cabo) e Israel (Tel Aviv) AWS GovCloud (US) Regions
>   - El acceso web con PCoIP solo es compatible con Windows WorkSpaces, no con Amazon Linux. WorkSpaces
>   - El acceso web no está disponible para algunos Windows 10 WorkSpaces que utilizan el protocolo PCoIP. Si su PCoIP funciona con Windows Server 2019 o 2022, el acceso web no WorkSpaces está disponible.
> - No puedes usar un navegador web para conectarte a un dispositivo con GPU. WorkSpaces
> - Si utilizas macOS en una VPN y utilizas el navegador web Firefox, el navegador web no admitirá la transmisión de PCoIP WorkSpaces mediante WorkSpaces Web Access. Esto se debe a una limitación en la implementación del protocolo WebRTC en Firefox.

> **Important**
>
> A partir del 1 de octubre de 2020, los clientes ya no podrán usar el cliente Amazon WorkSpaces Web Access para conectarse a Windows 7 custom WorkSpaces o a Windows 7 Bring Your Own License (BYOL) WorkSpaces.

Paso 1: Habilite el acceso web a su WorkSpaces

Usted controla el acceso web WorkSpaces a su directorio. Para cada directorio WorkSpaces que contenga y al que desee permitir el acceso de los usuarios a través del cliente de acceso web, lleve a cabo los siguientes pasos.

Para habilitar el acceso web a su WorkSpaces

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. En la columna ID de directorio, seleccione el ID del directorio para el que desea habilitar el acceso web.
4. En la página Detalles del directorio, desplácese hasta la sección Otras plataformas y seleccione Editar.
5. Elija Acceso web.
6. Seleccione Guardar.

> **Note**
>
> Después de activar el acceso web, reinicie el suyo WorkSpace para que se aplique el cambio.

Paso 2: Configurar el acceso de entrada y salida a los puertos para Acceso web

Amazon WorkSpaces Web Access requiere acceso entrante y saliente a determinados puertos. Para obtener más información, consulte Puertos para Acceso web.

Paso 3: Configurar las políticas de grupo y de seguridad para que los usuarios puedan iniciar sesión

Amazon WorkSpaces se basa en una configuración de pantalla de inicio de sesión específica para permitir a los usuarios iniciar sesión correctamente desde su cliente de acceso web.

Para permitir que los usuarios de Web Access inicien sesión en su cuenta WorkSpaces, debe configurar una política de grupo y tres ajustes de política de seguridad. Si estas opciones no están configuradas correctamente, es posible que los usuarios experimenten tiempos de inicio de sesión prolongados o pantallas negras cuando intenten iniciar sesión en su WorkSpaces Para configurar estas opciones, utilice los procedimientos siguientes.

Puede usar los objetos de política de grupo (GPO) para aplicar la configuración y administrar Windows WorkSpaces o los usuarios que forman parte de su directorio de Windows WorkSpaces . Se recomienda crear una unidad organizativa para los objetos de WorkSpaces equipo y una unidad organizativa para los objetos WorkSpaces de usuario.

Para obtener más información sobre el uso de las herramientas de administración de Active Directory para trabajar con GPO, consulte Instalación de las herramientas de administración de Active Directory en la Guía de administración de AWS Directory Service .

Para permitir que el agente de WorkSpaces inicio de sesión cambie de usuario

En la mayoría de los casos, cuando un usuario intenta iniciar sesión en un WorkSpace, el campo del nombre de usuario se rellena previamente con el nombre de ese usuario. Sin embargo, si un administrador ha establecido una conexión RDP con el WorkSpace para realizar tareas de mantenimiento, el campo del nombre de usuario se rellena con el nombre del administrador.

Para evitar este problema, deshabilite la opción de política de grupo Hide entry points for Fast User Switching (Ocultar los puntos de entrada para cambiar rápido de usuario). Al deshabilitar esta configuración, el agente de inicio de WorkSpaces sesión puede usar el botón Cambiar de usuario para rellenar el campo del nombre de usuario con el nombre correcto.

1. Abra la herramienta de administración de políticas de grupo (gpmc.msc) y busque y seleccione un GPO en el nivel de dominio o controlador de dominio del directorio que usa para su. WorkSpaces (Si tiene la plantilla administrativa de política de WorkSpaces grupo instalada en su dominio, puede usar el WorkSpaces GPO para las cuentas de sus WorkSpaces máquinas).
2. Elija Action, Edit en el menú principal.

3. En el editor de administración de políticas de grupo, elija Computer Configuration (Configuración de equipo), Policies (Políticas), Administrative Templates (Plantillas administrativas), System (Sistema) y Logon (Inicio de sesión).
4. Abra la configuración de Hide entry points for Fast User Switching (Ocultar los puntos de entrada para cambiar rápido de usuario).
5. En el cuadro de diálogo Hide entry points for Fast User Switching (Ocultar los puntos de entrada para cambiar rápido de usuario), elija Disabled (Deshabilitado) y, a continuación, elija OK (Aceptar).

Para ocultar el último nombre de usuario que ha iniciado sesión

De forma predeterminada, se muestra la lista de los últimos usuarios que han iniciado sesión en lugar del botón Switch User (Cambiar usuario). Según la configuración del WorkSpace, es posible que la lista no muestre el icono Otros usuarios. Cuando se produce esta situación, si el nombre de usuario rellenado previamente no es correcto, el agente de inicio de WorkSpaces sesión no podrá rellenar el campo con el nombre correcto.

Para evitar este problema, active la opción Interactive logon: Don't display last signed-in (Inicio de sesión interactivo: no mostrar el último inicio de sesión) o Interactive logon: Do not display last user name (Inicio de sesión interactivo: no mostrar el último nombre de usuario) (según cuál sea la versión de Windows que utilice) de la política de seguridad.

1. Abra la herramienta de administración de políticas de grupo (gpmc.msc) y busque y seleccione un GPO en el nivel de dominio o controlador de dominio del directorio que usa para su. WorkSpaces (Si tiene la plantilla administrativa de política de WorkSpaces grupo instalada en su dominio, puede usar el WorkSpaces GPO para las cuentas de sus WorkSpaces máquinas).
2. Elija Action, Edit en el menú principal.
3. En el editor de administración de políticas de grupo, elija Computer Configuration (Configuración del equipo), Windows Settings (Configuración de Windows), Security Settings (Configuración de seguridad), Local Policies (Políticas locales) y Security Options (Opciones de seguridad).
4. Abra una de las siguientes opciones de configuración:
   - En Windows 7: Inicio de sesión interactivo: No mostrar el último inicio de sesión
   - En Windows 10: Inicio de sesión interactivo: No mostrar el último nombre de usuario
5. En el cuadro de diálogo Properties (Propiedades) de la configuración, elija Enabled (Habilitado) y, a continuación, elija OK (Aceptar).

Para que sea obligatorio que los usuarios pulsen CTRL+ALT+SUPR con el fin de iniciar sesión

Para acceder a la WorkSpaces web, debe exigir a los usuarios que presionen CTRL+ALT+DEL para poder iniciar sesión. Requerir que los usuarios pulsen CTRL+ALT+SUPR con el fin de iniciar sesión garantiza que utilicen una ruta de acceso de confianza al introducir sus contraseñas.

1. Abra la herramienta de administración de políticas de grupo (gpmc.msc) y busque y seleccione un GPO en el nivel de dominio o controlador de dominio del directorio que utiliza para su. WorkSpaces (Si tiene la plantilla administrativa de política de WorkSpaces grupo instalada en su dominio, puede usar el WorkSpaces GPO para las cuentas de sus WorkSpaces máquinas).
2. Elija Action, Edit en el menú principal.
3. En el editor de administración de políticas de grupo, elija Computer Configuration (Configuración del equipo), Windows Settings (Configuración de Windows), Security Settings (Configuración de seguridad), Local Policies (Políticas locales) y Security Options (Opciones de seguridad).
4. Abra la opción Interactive logon: Do not require CTRL+ALT+DEL (Inicio de sesión interactivo: no requerir CTRL+ALT+SUPR).
5. En la pestaña Local Security Setting (Opción de seguridad local), elija Disabled (Deshabilitado) y, a continuación, seleccione OK (Aceptar).

Para mostrar la información de dominio y usuario cuando la sesión está bloqueada

El agente de WorkSpaces inicio de sesión busca el nombre y el dominio del usuario. Después de configurar esta opción, la pantalla de bloqueo mostrará el nombre completo del usuario (si se ha especificado en Active Directory), su nombre de dominio y su nombre de usuario.

1. Abra la herramienta de administración de políticas de grupo (gpmc.msc) y navegue hasta un GPO en el nivel de dominio o controlador de dominio del directorio que utilice para el suyo y selecciónelo. WorkSpaces (Si tiene la plantilla administrativa de política de WorkSpaces grupo instalada en su dominio, puede usar el WorkSpaces GPO para las cuentas de sus WorkSpaces máquinas).
2. Elija Action, Edit en el menú principal.
3. En el editor de administración de políticas de grupo, elija Computer Configuration (Configuración del equipo), Windows Settings (Configuración de Windows), Security Settings (Configuración de seguridad), Local Policies (Políticas locales) y Security Options (Opciones de seguridad).
4. Abra el parámetro Interactive logon: Display user information when the session is locked (Inicio de sesión interactivo: mostrar información del usuario cuando la sesión está bloqueada).

5. En la pestaña Local Security Setting (Configuración de seguridad local) elija User display name, domain and user names (Nombre para mostrar de usuario, nombres de dominio y de usuario) y, a continuación, elija OK (Aceptar).

Para aplicar los cambios de configuración de política de grupo y política de seguridad

Los cambios en la configuración de la política de grupo y la política de seguridad se aplican después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de política de grupo y política de seguridad de los procedimientos anteriores, siga uno de estos procedimientos:

- Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
- En el símbolo del sistema administrativo, introduzca gpupdate /force.

Configurar Amazon WorkSpaces para obtener la autorización FedRAMP o la conformidad DoD SRG.

Para cumplir con el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP) o la Guía de requisitos de seguridad de informática en la nube (SRG)del Departamento de Defensa (DoD), debe configurar Amazon WorkSpaces para utilizar el cifrado de punto de conexión de los Estándares Federales de Procesamiento de Información (FIPS) en el nivel de directorio. También debe utilizar una región de AWS de EE. UU. que cuente con autorización FedRAMP o que sea conforme con la SRG del DoD.

El nivel de autorización FedRAMP (moderado o alto) o el nivel de impacto de la SRG del DoD (2, 4 o 5) depende de la región de AWS de EE.UU. en la que se utilice Amazon WorkSpaces. Para conocer los niveles de autorización de FedRAMP y conformidad con DoD SRG que se aplican a cada región, consulte Servicios de AWS en el ámbito del programa de conformidad.

> **Note**
>
> Además de utilizar el cifrado del punto de conexión FIPS, también puede cifrar sus WorkSpaces. Para obtener más información, consulte Cifrado WorkSpaces.

Requisitos de

- Debe crear sus WorkSpaces en una región de AWS de EE. UU. que tenga autorización del FedRAMP o que cumpla con la SRG del DoD.
- El directorio de WorkSpaces debe configurarse para utilizar el modo validado FIPS 140-2 para el cifrado de puntos de enlace.

> **Note**
>
> Para utilizar la configuración FIPS 140-2 Validated Mode (Modo validado de FIPS 140-2), el directorio de WorkSpaces debe ser nuevo o todos los WorkSpaces existentes del directorio deben utilizar FIPS 140-2 Validated Mode (Modo validado FIPS 140-2) para el cifrado de puntos de enlace. De lo contrario, no puede utilizar esta configuración y, por lo tanto, los WorkSpaces que cree no cumplirán con los requisitos de seguridad del FedRAMP o DoD.

- Los usuarios deben obtener acceso a sus escritorios de WorkSpaces desde una de las siguientes aplicaciones cliente de WorkSpaces:
  - Windows 2.4.3 o posterior
  - macOS 2.4.3 o posterior
  - Linux: 3.0.0 o posterior
  - iOS 2.4.1 o posterior
  - Android: 2.4.1 o posterior
  - Fire Tablet: 2.4.1 o posterior
  - ChromeOS: 2.4.1 o posterior
  - Acceso web

Para utilizar el cifrado de punto de enlace de FIPS

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Compruebe que el directorio en el que desea crear escritorios de WorkSpaces autorizados por FedRAMP y compatibles con la SRG del DoD no tiene ningún WorkSpaces asociado. Si hay escritorios de WorkSpaces asociados al directorio y el directorio aún no está habilitado para utilizar el modo validado FIPS 140-2, termine los WorkSpaces o cree un nuevo directorio.

4. Elija el directorio que cumpla los criterios anteriores y, a continuación, elija Actions (Acciones),Update Details(Actualizar detalles).
5. En la página Update Directory Details(Actualizar detalles del directorio) elija la flecha para ampliar la sección Access Control Options (Acceder a las opciones de control) .
6. En Endpoint Encryption, elija FIPS 140-2 Validated Mode en lugar de TLS Encryption Mode (Standard).
7. Elija Update and Exit.
8. Ahora puede crear escritorios de WorkSpaces desde este directorio que estén autorizados por FedRAMP y que cumplan con la SRG del DoD. Para obtener acceso a estos espacios de trabajo, los usuarios deben utilizar una de las aplicaciones cliente de WorkSpaces indicadas anteriormente en la sección Requisitos .

Habilita las conexiones SSH para tu Linux WorkSpaces

Si usted o sus usuarios desean conectarse a Amazon Linux WorkSpaces mediante la línea de comandos, pueden habilitar las conexiones SSH. Puede habilitar las conexiones SSH para todos los miembros WorkSpaces de un directorio o para personas de WorkSpaces un directorio.

Para habilitar las conexiones SSH, crea un nuevo grupo de seguridad o actualiza un grupo de seguridad existente y añade una regla para permitir el tráfico de entrada con este fin. Los grupos de seguridad actúan como firewall para las instancias asociadas al controlar el tráfico entrante y saliente en el ámbito de la instancia. Tras crear o actualizar el grupo de seguridad, los usuarios y otras personas pueden usar PuTTY u otros terminales para conectarse desde sus dispositivos a Amazon Linux. WorkSpaces Para obtener más información, consulte the section called “Grupos de seguridad”.

Para ver un tutorial en vídeo, consulta ¿Cómo puedo conectarme a mi Amazon Linux WorkSpaces mediante SSH? en el Centro de AWS Conocimiento.

Contenido

Requisitos previos para las conexiones SSH a Amazon Linux WorkSpaces

- Habilitar el tráfico SSH entrante en un WorkSpace : para añadir una regla que permita el tráfico SSH entrante a uno o más Amazon Linux WorkSpaces, asegúrese de tener las direcciones IP públicas o privadas de los dispositivos que requieren conexiones SSH con su. WorkSpaces Por ejemplo, puede especificar las direcciones IP públicas de los dispositivos fuera de su nube privada virtual (VPC) o la dirección IP privada de otra instancia de EC2 en la misma VPC que la suya. WorkSpace

  Si planea conectarse a una WorkSpace desde su dispositivo local, puede utilizar la frase de búsqueda «cuál es mi dirección IP» en un navegador de Internet o utilizar el siguiente servicio: Check IP.
- Conexión a un WorkSpace : se requiere la siguiente información para iniciar una conexión SSH desde un dispositivo a Amazon Linux. WorkSpace
  - El nombre NetBIOS del dominio de Active Directory al que está conectado.
  - Su nombre WorkSpace de usuario.
  - La dirección IP pública o privada a la WorkSpace que desea conectarse.

    Privada: si su VPC está conectada a una red corporativa y tiene acceso a esa red, puede especificar la dirección IP privada de la. WorkSpace

    Pública: si WorkSpace tiene una dirección IP pública, puede usar la WorkSpaces consola para buscar la dirección IP pública, tal y como se describe en el siguiente procedimiento.

Para encontrar las direcciones IP de Amazon Linux a las que WorkSpace desea conectarse y su nombre de usuario

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. En la lista de WorkSpaces, elige WorkSpace aquella a la que deseas habilitar las conexiones SSH.
4. En la columna Modo de ejecución, confirme que el WorkSpace estado es Disponible.
5. Haga clic en la flecha situada a la izquierda del WorkSpace nombre para ver el resumen integrado y anote la siguiente información:

   - La WorkSpace IP. Esta es la dirección IP privada del WorkSpace.

La dirección IP privada es necesaria para obtener la interfaz de red elástica asociada a WorkSpace. La interfaz de red es necesaria para recuperar información como el grupo de seguridad o la dirección IP pública asociada al WorkSpace.

- El WorkSpace nombre de usuario. Es el nombre de usuario que se especifica para conectarse al WorkSpace.

6. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
7. En el panel de navegación, elija Network Interfaces.
8. En el cuadro de búsqueda, escriba la WorkSpace IP que anotó en el paso 5.
9. Seleccione la interfaz de red asociada a la WorkSpaceIP.
10. Si WorkSpace tiene una dirección IP pública, aparecerá en la columna IP pública de IPv4. Anote esta dirección IP pública, si procede.

Para encontrar el nombre NetBIOS del dominio de Active Directory al que está conectado

1. Abra la AWS Directory Service consola en https://console.aws.amazon.com/directoryservicev2/.
2. En la lista de directorios, haga clic en el enlace del ID de directorio del directorio correspondiente al WorkSpace.
3. En la sección Directory details (Detalles del directorio), anote el Directory NetBIOS name (Nombre NetBIOS del directorio).

Habilite las conexiones SSH a todos los Amazon Linux WorkSpaces de un directorio

Para habilitar las conexiones SSH a todos los Amazon Linux WorkSpaces de un directorio, haga lo siguiente.

Para crear un grupo de seguridad con una regla que permita el tráfico SSH entrante a todos los Amazon Linux de un WorkSpaces directorio

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Elija Crear grupo de seguridad.
4. Escriba un nombre y, de forma opcional, una descripción para su grupo de seguridad.

5. Para la VPC, elija la VPC que contiene la VPC a la WorkSpaces que desea habilitar las conexiones SSH.
6. En la pestaña Inbound (Entrada), elija Add Rule (Añadir regla) y haga lo siguiente:
   - En Tipo, seleccione SSH.
   - En Protocol (Protocolo), TCP se especifica automáticamente al elegir SSH.
   - En Port Range (Rango de puertos), 22 se especifica automáticamente al elegir SSH.
   - En Source, especifique el rango CIDR de las direcciones IP públicas de las computadoras que los usuarios utilizarán para conectarse a las suyas. WorkSpaces Por ejemplo, una red corporativa o una red doméstica.
   - En Description (Descripción) (opcional), escriba una descripción para la regla.
7. Seleccione Crear.

Autenticación basada en contraseñas en Amazon Linux 2 WorkSpaces

Amazon Linux 2 WorkSpaces lanzado antes del 10 de noviembre de 2023 tiene habilitada la autenticación mediante contraseña SSH de forma predeterminada. Para Amazon Linux 2 WorkSpaces lanzado después del 10 de noviembre. 2023, la autenticación de contraseña SSH está deshabilitada de forma predeterminada.

Para deshabilitar la autenticación con contraseña en las WorkSpaces instancias de Amazon Linux 2 existentes

1. Inicie el WorkSpaces cliente e inicie sesión en su WorkSpace.
2. Abra Terminal (Aplicación > Herramientas del sistema > Terminal de MATE).
3. En la ventana Terminal, ejecute el siguiente comando.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

Para habilitar la autenticación con contraseña en las WorkSpaces instancias de Amazon Linux 2 recién creadas

1. Inicie el WorkSpaces cliente e inicie sesión en su WorkSpace.
2. Abra Terminal (Aplicación > Herramientas del sistema > Terminal de MATE).
3. En la ventana Terminal, ejecute el siguiente comando.

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

A diferencia de Ubuntu WorkSpaces, Amazon Linux 2 no conserva de forma WorkSpaces predeterminada la configuración de autenticación mediante contraseña SSH en las imágenes personalizadas. Si desea habilitar la autenticación por contraseña SSH de forma predeterminada en Amazon Linux 2 WorkSpaces aprovisionada a partir de una imagen personalizada, además de habilitar la autenticación por contraseña, también debe cambiar el `/etc/cloud/cloud.cfg` archivo para eliminar la línea que contiene `ssh_pwauth` al crear una imagen personalizada. Para cambiar el archivo `/etc/cloud/cloud.cfg` ejecute el siguiente comando:

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

Habilitar conexiones SSH a un Amazon Linux específico WorkSpace

Para habilitar las conexiones SSH a un Amazon Linux específico WorkSpace, haga lo siguiente.

Para añadir una regla a un grupo de seguridad existente para permitir el tráfico SSH entrante a un Amazon Linux específico WorkSpace

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Network & Security (Red y seguridad), seleccione Network Interfaces (Interfaces de red).
3. En la barra de búsqueda, escriba la dirección IP privada a la WorkSpace que desea habilitar las conexiones SSH.
4. En la columna Security groups (Grupos de seguridad), haga clic en el enlace para el grupo de seguridad.
5. En la pestaña Inbound (Entrada), seleccione Edit (Editar).
6. Elija Add Rule (Añadir regla) y, a continuación, haga lo siguiente:

   - En Tipo, seleccione SSH.
   - En Protocol (Protocolo), TCP se especifica automáticamente al elegir SSH.
   - En Port Range (Rango de puertos), 22 se especifica automáticamente al elegir SSH.
   - En Source (Fuente), elija My IP (Mi IP) o Custom (Personalizado) y especifique una sola dirección IP o un rango de direcciones IP en notación CIDR. Por ejemplo, si su dirección IPv4 es `203.0.113.25`, especifique `203.0.113.25/32` para mostrar la dirección IPv4 única en

notación CIDR. Si su empresa asigna direcciones de un rango, especifíquelo; por ejemplo, `203.0.113.0/24`.

- En Description (Descripción) (opcional), escriba una descripción para la regla.

7. Elija Guardar.

Conéctate a Amazon Linux WorkSpace mediante Linux o PuTTY

Tras crear o actualizar el grupo de seguridad y añadir la regla necesaria, los usuarios y otras personas pueden utilizar Linux o PuTTY para conectarse desde sus dispositivos al suyo. WorkSpaces

> **Note**
>
> Antes de completar cualquiera de los siguientes procedimientos, asegúrese de que tiene lo siguiente:
>
> - El nombre NetBIOS del dominio de Active Directory al que está conectado.
> - El nombre de usuario que utiliza para conectarse al WorkSpace.
> - La dirección IP pública o privada de la WorkSpace que desea conectarse.
>
> Para obtener instrucciones sobre cómo obtener esta información, consulte «Requisitos previos para las conexiones SSH a Amazon Linux WorkSpaces», que aparece anteriormente en este tema.

Para conectarse a Amazon Linux WorkSpace mediante Linux

1. Abra el símbolo del sistema como administrador e introduzca el siguiente comando. Para el *nombre, el nombre de usuario y la WorkSpace IP de NetBIOS*, introduzca los valores aplicables.

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   A continuación, mostramos un ejemplo del comando SSH donde:

   - El *NetBIOS_NAME* es AnyCompany
   - El *Nombre de usuario* es janedoe

- La *WorkSpace IP es 203.0.113.25*

```
ssh "anycompany\janedoe"@203.0.113.25
```

2. Cuando se le pida, introduzca la misma contraseña que utilizó al autenticarse con el WorkSpaces cliente (su contraseña de Active Directory).

Para conectarse a Amazon Linux WorkSpace mediante PuTTY

1. Abra PuTTY.
2. En el cuadro de diálogo PuTTY Configuration (Configuración de PuTTY), haga lo siguiente:
   - En Host Name (or IP address) [Nombre de host (o dirección IP)], escriba el siguiente comando. Sustituya los valores por el nombre NetBIOS del dominio de Active Directory al que está conectado, el nombre de usuario que utiliza para conectarse y la dirección IP del dominio al WorkSpace que desea conectarse. WorkSpace

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

   - En Puerto, escriba **22**.
   - En Connection type (Tipo de conexión), elija SSH.

   Para ver un ejemplo del comando SSH, consulte el paso 1 en el procedimiento anterior.
3. Elija Open.
4. Cuando se le pida, introduzca la misma contraseña que utilizó al autenticarse con el WorkSpaces cliente (su contraseña de Active Directory).

Componentes de configuración y servicio necesarios para WorkSpaces

Como WorkSpace administrador, debe comprender lo siguiente acerca de los componentes de configuración y servicio necesarios.

- the section called “Configuración de la tabla de enrutamiento”
- the section called “Componentes para Windows”

- the section called “Componentes para Linux”
- the section called “Componentes para Ubuntu”

Configuración necesaria de la tabla de ruteo

Se recomienda no modificar la tabla de enrutamiento a nivel del sistema operativo para un. WorkSpace El WorkSpaces servicio requiere las rutas preconfiguradas de esta tabla para monitorear el estado del sistema y actualizar los componentes del sistema. Si su organización requiere cambios en la tabla de enrutamiento, póngase en contacto con AWS Support o con el equipo de su AWS cuenta antes de aplicar cualquier cambio.

Componentes de servicio necesarios para Windows

En Windows WorkSpaces, los componentes de servicio se instalan en las siguientes ubicaciones. No elimine, cambie, bloquee o ponga en cuarentena estos objetos. Si lo hace, no WorkSpace funcionará correctamente.

Si hay un software antivirus instalado en el WorkSpace, asegúrese de que no interfiera con los componentes de servicio instalados en las siguientes ubicaciones.

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

Agente PCoIP de 32 bits

A partir del 29 de marzo de 2021, actualizamos el agente PCoIP de 32 bits a 64 bits. En el caso de Windows WorkSpaces que utilice el protocolo PCoIP, esto significa que la ubicación de los archivos de Teradici ha cambiado de a. `C:\Program Files (x86)\Teradici` `C:\Program Files\Teradici` Como actualizamos los agentes PCoIP durante los períodos de mantenimiento habituales, es WorkSpaces posible que algunos de ustedes hayan utilizado el agente de 32 bits durante más tiempo que otros durante la transición.

Si ha configurado reglas de cortafuegos, exclusiones de software antivirus (en el lado del cliente y en el lado del host), ajustes de objetos de política de grupo (GPO) o ajustes para Microsoft System Center Configuration Manager (SCCM), Microsoft Endpoint Configuration Manager o herramientas de gestión de configuración similares basadas en la ruta completa al agente de 32 bits, también debe añadir la ruta completa al agente de 64 bits a esos ajustes.Traducción realizada con la versión gratuita del traductor www.DeepL.com/Translator

Si está filtrando las rutas a cualquier componente PCoIP de 32 bits, asegúrese de añadir las rutas a las versiones de 64 bits de los componentes. Como es WorkSpaces posible que no estén todos actualizados al mismo tiempo, no sustituya la ruta de 32 bits por la de 64 bits, ya que algunas de las suyas podrían no funcionar. WorkSpaces Por ejemplo, si basa sus exclusiones o filtros de comunicación en `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`, también debe añadir `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`. Por ejemplo, si está basando sus exclusiones o filtros de comunicación en `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe`, también debe añadir `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe`.

Cambio en el servicio de arbitraje de PCoIP: tenga en cuenta que el servicio de árbitro de PCoIP (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) se eliminará cuando se actualice para utilizar el agente de 64 WorkSpaces bits.

Clientes PCoIP cero y dispositivos USB: a partir de la versión 20.10.4 del agente PCoIP, WorkSpaces Amazon deshabilita la redirección USB de forma predeterminada a través del registro de Windows. Esta configuración de registro afecta al comportamiento de los periféricos USB cuando los usuarios utilizan dispositivos PCoIP sin cliente para conectarse a sus dispositivos. WorkSpaces Para obtener más información, consulte Las impresoras USB y otros periféricos USB no funcionan para los clientes cero PCoIP.

Componentes de servicio necesarios para Linux

En Amazon Linux WorkSpaces, los componentes del servicio se instalan en las siguientes ubicaciones. No elimine, cambie, bloquee o ponga en cuarentena estos objetos. Si lo hace, no WorkSpace funcionará correctamente.

> **Note**
>
> Hacer cambios en los archivos de otro tipo `/etc/pcoip-agent/pcoip-agent.conf` puede provocar que deje de funcionar y que tenga que volver a construirlos. WorkSpaces

Para obtener información sobre cómo modificar `/etc/pcoip-agent/pcoip-agent.conf`, consulte Administre su Amazon Linux WorkSpaces.

- `/etc/dhcp/dhclient.conf`
- `/etc/logrotate.d/pcoip-agent`
- `/etc/logrotate.d/pcoip-server`
- `/etc/os-release`
- `/etc/pam.d/pcoip`
- `/etc/pam.d/pcoip-session`
- `/etc/pcoip-agent`
- `/etc/profile.d/system-restart-check.sh`
- `/etc/X11/default-display-manager`
- `/etc/yum/pluginconf.d/halt_os_update_check.conf`
- `/etc/systemd/system/euc-analytic-agent.service`
- `/lib/systemd/system/pcoip.service`
- `/lib/systemd/system/pcoip-agent.service`
- `/lib64/security/pam_self.so`
- `/usr/bin/pcoip-fne-view-license`
- `/usr/bin/pcoip-list-licenses`
- `/usr/bin/pcoip-validate-license`
- `/usr/bin/euc-analytics-agent`
- `/usr/lib/firewalld/services/pcoip-agent.xml`
- `/usr/lib/modules-load.d/usb-vhci.conf`
- `/usr/lib/pcoip-agent`
- `/usr/lib/skylight`
- `/usr/lib/systemd/system/pcoip.service`
- `/usr/lib/systemd/system/pcoip.service.d/`
- `/usr/lib/systemd/system/skylight-agent.service`
- `/usr/lib/tmpfiles.d/pcoip-agent.conf`
- `/usr/lib/yum-plugins/halt_os_update_check.py`

- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Componentes de servicio necesarios para Ubuntu

En Ubuntu WorkSpaces, los componentes del servicio se instalan en las siguientes ubicaciones. No elimine, cambie, bloquee o ponga en cuarentena estos objetos. Si lo hace, no WorkSpace funcionará correctamente.

- /etc/X11/default-display-manager
- /etc/X11/xorg.conf
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /etc/systemd/system/euc-analytic-agent.service

- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

Administrar directorios para WorkSpaces

WorkSpaces utiliza un directorio para almacenar y administrar la información de sus WorkSpaces y usuarios. Puede utilizar una de las siguientes opciones:

- Conector AD: Use el Microsoft Active Directory local existente. Los usuarios pueden iniciar sesión en los escritorios de WorkSpaces con sus credenciales locales y tener acceso a los recursos locales de los escritorios de WorkSpaces.
- AWS Managed Microsoft AD: Cree un Microsoft Active Directory alojado en AWS.
- AD sencillo: Cree un directorio compatible con Microsoft Active Directory, activado por Samba 4 y alojado en AWS.
- Confianza cruzada: Cree una relación de confianza entre su directorio de Microsoft AD administrado por AWS Managed Microsoft AD cree una relación de confianza entre el directorio de Microsoft AD y el dominio en las instalaciones.

Para encontrar tutoriales sobre cómo configurar estos directorios y lanzar WorkSpaces, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

> **Tip**
>
> Para obtener información detallada sobre las consideraciones de diseño de directorio y nube privada virtual (VPC) para diferentes escenarios de implementación, consulte Prácticas recomendadas para implementar Amazon WorkSpaces.

Después de crear un directorio, llevará a cabo la mayoría de las tareas administrativas del directorio con herramientas como las herramientas de administración de Active Directory. Puede realizar algunas tareas de administración de directorios utilizando la consola de WorkSpaces y otras tareas utilizando la política de grupo. Para obtener más información acerca de la administración de usuarios y grupos, consulte Administrar usuarios de WorkSpaces y Configurar las herramientas de administración de Active Directory para WorkSpaces.

> **Note**
>
> - Los directorios compartidos no son compatibles actualmente con Amazon WorkSpaces.

- Si configura su directorio de Microsoft AD administrado por AWS para la reproducción en varias regiones, solo se podrá registrar el directorio de la región principal para utilizarlo con Amazon WorkSpaces. Los intentos de registrar el directorio en una región duplicada para su uso con Amazon WorkSpaces fallarán. No se admite la replicación multirregional con AWS Managed Microsoft AD para su uso con Amazon WorkSpaces dentro de las regiones replicadas.
- Tanto AD sencillo como el conector AD están disponibles de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio AD sencillo o conector AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.

  Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio AD sencillo o conector AD, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

Contenido

Registrar un directorio en WorkSpaces

Para permitir que WorkSpaces utilice un directorio existente de AWS Directory Service, debe registrarlo con WorkSpaces. Después de registrar un directorio, puede lanzar en él escritorios de WorkSpaces.

Requisitos

Para registrar un directorio para su uso con WorkSpaces, debe cumplir el siguiente requisito:

- Si utiliza AWS Managed Microsoft AD o AD Sencillo, su directorio puede estar en una subred privada dedicada, siempre y cuando el directorio tenga acceso a la VPC en la que se encuentran los WorkSpaces.

Para obtener más información sobre el diseño de directorios y VPC, consulte el documento técnico Mejores prácticas para implementar Amazon WorkSpaces.

> **Note**
>
> Tanto AD sencillo como el conector AD están disponibles de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio AD sencillo o conector AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.
> Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio AD sencillo o conector AD, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

Para anular el registrar de un directorio

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio.
4. Elija Actions, Register.

> **Note**
>
> - Los directorios compartidos no son compatibles actualmente con Amazon WorkSpaces.
> - Si su directorio AWS Managed Microsoft AD se ha configurado para la reproducción en varias regiones, solo se podrá registrar el directorio de la región principal para utilizarlo con Amazon WorkSpaces. Los intentos de registrar el directorio en una región duplicada para su uso con Amazon WorkSpaces fallarán. No se admite la

replicación multirregional con AWS Managed Microsoft AD para su uso con Amazon WorkSpaces dentro de las regiones replicadas.

5. Seleccione dos subredes de su VPC que no sean de la misma zona de disponibilidad. Estas subredes se utilizarán para lanzar sus WorkSpaces. Para obtener más información, consulte Zonas de disponibilidad de Amazon WorkSpaces.

> **Note**
>
> Si no sabe qué subredes elegir, seleccione Sin preferencia.

6. En Enable Self Service Permissions (Habilitar permisos de autoservicio), elija Yes (Sí) para permitir a los usuarios que reconstruyan sus WorkSpaces, cambien el tamaño del volumen, tipo de computación y modo de ejecución. Habilitar puede afectar la cantidad que paga por Amazon WorkSpaces. En caso contrario, elija No.
7. En Habilitar Amazon WorkDocs, elija Sí para registrar el directorio para su uso con Amazon WorkDocs o No en caso contrario.

> **Note**
>
> Esta opción solo se muestra si Amazon WorkDocs está disponible en la región y si no utiliza AWS Managed Microsoft AD. Si utiliza AWS Managed Microsoft AD, termine de registrar su directorio y, a continuación, consulte Habilitar Amazon WorkDocs para Microsoft AD administrado por AWS.

8. Elija Register. Inicialmente el valor de Registered es `REGISTERING`. Una vez completado el registro, el valor es `Yes`.

Cuando termine de utilizar el directorio con WorkSpaces, puede darlo de baja. Tenga en cuenta que debe anular el registro de un directorio si quiere eliminarlo. Si desea anular el registro y eliminar un directorio, primero debe buscar y suprimir todas las aplicaciones y los servicios que están registrados en el directorio. Para obtener más información, consulte Eliminar su directorio en la Guía de administración de AWS Directory Service.

Para anular el registro de un directorio

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.

2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio.
4. Elija Actions, Deregister.
5. Cuando se le pida que confirme, elija Deregister. Una vez hecha la anulación, el valor de Registered es No.

Actualice los detalles del directorio de su WorkSpaces

Puede realizar las siguientes tareas de administración de directorios mediante la WorkSpaces consola.

Tareas

- Seleccionar una unidad organizativa
- Configurar direcciones IP públicas automáticas
- Controlar el acceso de los dispositivos
- Administrar los permisos de administrador local
- Actualizar la cuenta del Conector AD (Conector AD)
- Autenticación multifactor (Conector AD)

Seleccionar una unidad organizativa

WorkSpace las cuentas de máquina se colocan en la unidad organizativa (OU) predeterminada del WorkSpaces directorio. En principio, las cuentas de la máquina se guardan en la unidad organizativa Computers del directorio al que está conectado el directorio de Conector AD. Puede seleccionar otras unidades organizativas del directorio o directorio conectado, o bien especificar una en un dominio de destino independiente. Tenga en cuenta que solo puede seleccionar una unidad organizativa por directorio.

Tras seleccionar una nueva unidad organizativa, las cuentas de máquina de todas las WorkSpaces que se creen o reconstruyan se colocan en la unidad organizativa recién seleccionada.

Para seleccionar una unidad organizativa

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).

3. Elija su directorio.
4. En Dominio y unidad organizativa de destino, selecciona Editar.
5. Para buscar una OU, en Destino y unidad organizativa, puede empezar a escribir todo o parte del nombre de la OU y elegir la OU que desee usar.
6. (Opcional) Elija un nombre distintivo para sobrescribir la OU seleccionada por una unidad organizativa personalizada.
7. Seleccione Guardar.
8. (Opcional) Reconstruya la existente WorkSpaces para actualizar la OU. Para obtener más información, consulte Reconstruir un WorkSpace.

Configurar direcciones IP públicas automáticas

Tras activar la asignación automática de direcciones IP públicas, a cada una de las direcciones IP WorkSpace que lances se le asigna una dirección IP pública del conjunto de direcciones públicas proporcionado por Amazon. WorkSpace En una subred pública, puede acceder a Internet a través de la puerta de enlace de Internet si tiene una dirección IP pública. WorkSpaces las que ya existían antes de activar la asignación automática no reciben direcciones públicas hasta que las reconstruya.

Tenga en cuenta que no necesita habilitar la asignación automática de direcciones públicas si WorkSpaces se encuentra en subredes privadas y configuró una puerta de enlace NAT para la nube privada virtual (VPC), o si WorkSpaces se encuentra en subredes públicas y les asignó direcciones IP elásticas. Para obtener más información, consulte Configurar una VPC para WorkSpaces.

> **Warning**
>
> Si asocias una dirección IP elástica de tu propiedad a una y WorkSpace, posteriormente, desasocias esa dirección IP elástica de la WorkSpace, WorkSpace pierde su dirección IP pública y no obtiene automáticamente una nueva del grupo proporcionado por Amazon. Para asociar una nueva dirección IP pública del grupo proporcionado por Amazon al WorkSpace, debes volver a crear el. WorkSpace Si no quiere volver a crearla WorkSpace, debe asociar otra dirección IP elástica de su propiedad a la. WorkSpace

Para configurar direcciones IP elásticas

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.

2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio para su WorkSpaces.
4. Elija Actions, Update Details.
5. Amplíe Access to Internet y seleccione Enable o Disable.
6. Seleccione Actualizar.

Controlar el acceso de los dispositivos

Puede especificar los tipos de dispositivos a los que tiene acceso WorkSpaces. Además, puede restringir el acceso WorkSpaces a dispositivos de confianza (también conocidos como dispositivos gestionados).

Para controlar el acceso de los dispositivos a WorkSpaces

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija su directorio.
4. En Opciones de control de acceso, selecciona Editar.
5. En Dispositivos de confianza, especifica los tipos de dispositivos a los que se puede acceder WorkSpaces seleccionando Permitir todo, Dispositivos de confianza o Denegar todo. Para obtener más información, consulte Restrinja el WorkSpaces acceso a dispositivos de confianza.
6. Seleccione Save (Guardar).

Administrar los permisos de administrador local

Puede especificar si los usuarios son administradores locales WorkSpaces, lo que les permite instalar la aplicación y modificar su configuración WorkSpaces. Los usuarios son los administradores locales de forma predeterminada. Si modifica esta configuración, el cambio se aplicará a todas las nuevas WorkSpaces que cree y a todas las WorkSpaces que reconstruya.

Para modificar los permisos de administrador local

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija su directorio.

4. En Configuración de administrador local, selecciona Editar.
5. Para asegurarse de que los usuarios son administradores locales, seleccione Habilitar la configuración de administrador local.
6. Seleccione Guardar.

Actualizar la cuenta del Conector AD (Conector AD)

Puede actualizar la cuenta de AD Connector que se usa para leer usuarios y grupos y unir cuentas de WorkSpaces máquinas a su directorio de AD Connector.

Para actualizar la cuenta de Conector AD

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione su directorio y, a continuación, elija Ver detalles.
4. En la cuenta del conector AD, selecciona Editar.
5. Introduzca las credenciales de inicio de sesión de la nueva cuenta.
6. Seleccione Guardar.

Autenticación multifactor (Conector AD)

Puede habilitar la autenticación multifactor (MFA) para el directorio del Conector AD. Para obtener más información sobre el uso de la autenticación multifactor con AWS Directory Service, consulte Habilitar la autenticación multifactor para el Conector y los requisitos previos del Conector AD.

> **Note**
>
> - Su servidor RADIUS puede estar alojado en AWS o en las instalaciones.
> - Los nombres de usuario deben coincidir entre Active Directory y su servidor RADIUS.

Para habilitar la autenticación multifactor

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).

3. Seleccione el directorio y después elija Actions, Update Details.
4. Amplíe Multi-Factor Authentication y, a continuación, seleccione Enable Multi-Factor Authentication.
5. En RADIUS server IP address(es), escriba las direcciones IP de los puntos de enlace del servidor RADIUS separadas por comas o escriba la dirección IP del balanceador de carga del servidor RADIUS.
6. En Port, escriba el puerto que el servidor RADIUS utiliza para las comunicaciones. La red en las instalaciones debe permitir el tráfico entrante a través del puerto predeterminado del servidor RADIUS (UDP:1812) desde el Conector AD.
7. En Shared secret code y Confirm shared secret code, escriba del código secreto compartido del servidor RADIUS.
8. En Protocol, elija el protocolo del servidor RADIUS.
9. En Server timeout, escriba el tiempo, en segundos, que hay que esperar a que el servidor RADIUS responda. Este valor debe estar entre 1 y 50.
10. En Max retries, escriba el número de veces que se intenta la comunicación con el servidor RADIUS. Este valor debe estar entre 0 y 10.
11. Elija Update and Exit.

La autenticación multifactor está disponible cuando RADIUS status está Enabled. Mientras se configura la autenticación multifactorial, los usuarios no pueden iniciar sesión en su WorkSpaces.

Actualizar los servidores de DNS para Amazon WorkSpaces

Si necesita actualizar las direcciones IP del servidor DNS de su Active Directory después de lanzar sus WorkSpaces, también debe actualizar sus WorkSpaces con la nueva configuración del servidor DNS.

Puede actualizar sus WorkSpaces con la nueva configuración DNS de una de las siguientes maneras:

- Actualice la configuración DNS en los WorkSpaces antes de actualizar la configuración DNS para Active Directory.
- Reconstruya los WorkSpaces después de actualizar la configuración DNS para Active Directory.

Recomendamos actualizar la configuración DNS en los WorkSpaces antes de actualizar la configuración DNS en Active Directory (como se explica en el Paso 1 del siguiente procedimiento).

Si, en su lugar, desea volver a crear los WorkSpaces, actualice una de las direcciones IP del servidor DNS de Active Directory (Paso 2) y, a continuación, siga el procedimiento indicado en Reconstruir un WorkSpace para volver a crear los WorkSpaces. Después de volver a crear sus WorkSpaces, siga el procedimiento del Paso 3 para probar las actualizaciones de su servidor DNS. Tras completar ese paso, actualice la dirección IP del segundo servidor DNS en Active Directory y, a continuación, vuelva a crear los WorkSpaces. Asegúrese de seguir el procedimiento del Paso 3 para probar la actualización de su segundo servidor DNS. Como se indica en la sección Prácticas recomendadas, le recomendamos que actualice las direcciones IP de sus servidores DNS de una en una.

Prácticas recomendadas

Cuando actualice la configuración del servidor DNS, le recomendamos las siguientes prácticas recomendadas:

- Para evitar desconexiones e inaccesibilidad de los recursos del dominio, le recomendamos encarecidamente que realice las actualizaciones del servidor DNS durante las horas de menor actividad o durante un periodo de mantenimiento planificado.
- No inicie nuevos WorkSpaces durante los 15 minutos anteriores y los 15 minutos posteriores al cambio de configuración del servidor DNS.
- Al actualizar la configuración del servidor DNS, cambie una dirección IP del servidor DNS al mismo tiempo. Compruebe que la primera actualización es correcta antes de actualizar la segunda dirección IP. Se recomienda realizar el siguiente procedimiento (Paso 1, Paso 2 y Paso 3) dos veces para actualizar las direcciones IP de una en una.

Paso 1: Actualizar la configuración del servidor de DNS en sus WorkSpaces

En el siguiente procedimiento, los valores actuales y nuevos de la dirección IP del servidor DNS se denominan de la siguiente manera:

- Direcciones IP DNS actuales: *OldIP1*, *OldIP2*
- Nuevas direcciones IP DNS: *NewIP1*, *NewIP2*

> **Note**
>
> Si es la segunda vez que realiza este procedimiento, sustituya *OldIP1* por *OldIP2* y *NewIP1* por *NewIP2*.

Actualizar la configuración del servidor DNS para Windows WorkSpaces

Si tiene varios WorkSpaces, puede implementar la siguiente actualización del registro en los WorkSpaces aplicando un objeto de directiva de grupo (GPO) en la OU de Active Directory para sus WorkSpaces. Para obtener más información sobre cómo trabajar con GPO, consulte Administre su Windows WorkSpaces.

Puede realizar estas actualizaciones mediante el Editor del Registro o mediante Windows PowerShell. En esta sección se describen ambos procedimientos.

Para actualizar la configuración del registro DNS mediante el Editor del registro

1. En su Windows WorkSpace, abra el cuadro de búsqueda de Windows e introduzca **registry editor** para abrir el Editor del registro (regedit.exe).
2. Cuando se le pregunte "¿Desea permitir que esta aplicación realice cambios en su dispositivo?", elija Sí.
3. En el Editor del registro, navegue hasta la siguiente entrada de registro:

   HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ SkyLight
4. Abra la clave de registro DomainJoinDNS. Actualice ***OldIP1*** con ***NewIP1*** y a continuación, seleccione OK.
5. Cierre el editor de registro.
6. Reinicie el WorkSpace, o reinicie el servicio SkyLightWorkspaceConfigService.

   > **Note**
   >
   > Tras reiniciar el servicio SkylightWorkspaceConfigService, el adaptador de red puede tardar hasta 1 minuto en reflejar el cambio.
7. Continúe con el Paso 2 y actualice la configuración del servidor DNS en Active Directory para reemplazarlo *OldIP1* por *NewIP1*.

Para actualizar la configuración del registro DNS mediante PowerShell

El siguiente procedimiento utiliza comandos de PowerShell para actualizar el registro y reiniciar el servicio SkylightWorkspaceConfigService.

1. En su WorkSpace para Windows, abra el cuadro de búsqueda de Windows e introduzca **`powershell`**. Elija Ejecutar como administrador.
2. Cuando se le pregunte "¿Desea permitir que esta aplicación realice cambios en su dispositivo?", elija Sí.
3. En la ventana de PowerShell, ejecute el siguiente comando para recuperar las direcciones IP actuales del servidor DNS.

   ```
   Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
   ```

   Debería obtener el siguiente resultado.

   ```
   DomainJoinDns : OldIP1,OldIP2
   PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon\SkyLight
   PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
   \Amazon
   PSChildName   : SkyLight
   PSDrive       : HKLM
   PSProvider    : Microsoft.PowerShell.Core\Registry
   ```

4. En una ventana de PowerShell, ejecute el siguiente comando para cambiar *`OldIP1`* a *`NewIP1`*: Asegúrese de dejar *`OldIP2`* como está.

   ```
   Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
    "NewIP1,OldIP2"
   ```

5. Ejecute el siguiente comando para reiniciar el servicio SkylightWorkspaceConfigService.

   ```
   restart-service -Name SkyLightWorkspaceConfigService
   ```

   > **Note**
   >
   > Tras reiniciar el servicio SkylightWorkspaceConfigService, el adaptador de red puede tardar hasta 1 minuto en reflejar el cambio.

6. Continúe con el Paso 2 y actualice la configuración del servidor DNS en Active Directory para reemplazarlo *OldIP1* por *NewIP1*.

Actualizar la configuración del servidor DNS en WorkSpaces para Linux

Si tiene más de un WorkSpace para Linux, se recomienda que utilice una solución de administración de configuración para distribuir y aplicar la política. Por ejemplo, puede utilizar AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise o Ansible.

Para actualizar la configuración del servidor DNS en WorkSpaces para Linux

1. En su WorkSpace para Linux, abra una ventana de terminal (Aplicaciones > Herramientas del sistema > Terminal MATE).
2. Utilice el siguiente comando para editar el archivo `/etc/dhcp/dhclient.conf`. Debe tener privilegios de usuario raíz para editar este archivo. Para obtener estos privilegios, puede usar el comando `sudo -i` o ejecutar todos los comandos con `sudo` como se indica.

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   En el archivo `/etc/dhcp/dhclient.conf`, verá el siguiente comando `prepend`, donde *OldIP1* y *OldIP2* son las direcciones IP de sus servidores DNS.

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```
3. Reemplace *OldIP1* por *NewIP1* y deje *OldIP2* como está.
4. Guarde los cambios en `/etc/dhcp/dhclient.conf`.
5. Reinicie el WorkSpace.
6. Continúe con el Paso 2 y actualice la configuración del servidor DNS en Active Directory para reemplazarlo *OldIP1* por *NewIP1*.

Paso 2: actualizar la configuración del servidor de DNS para Active Directory

En este paso, actualice la configuración del servidor de DNS para Active Directory. Como se indica en la sección Prácticas recomendadas, le recomendamos que actualice las direcciones IP de sus servidores DNS de una en una.

Para actualizar la configuración del servidor DNS para Active Directory, consulte la siguiente documentación en la Guía de administración de AWS Directory Service:

- Conector AD: Actualice la dirección de DNS del Conector AD
- AWS Managed Microsoft AD: Configure programas de envío condicionales DNS para su dominio local
- Simple AD: configure el DNS

Después de actualizar la configuración de su servidor DNS, continúe con el paso 3.

Paso 3: probar la configuración del servidor de DNS actualizada

Tras completar el Paso 1 y el Paso 2, utilice el siguiente procedimiento para comprobar que la configuración actualizada del servidor DNS funciona según lo previsto.

En el siguiente procedimiento, los valores actuales y nuevos de la dirección IP del servidor DNS se denominan de la siguiente manera:

- Direcciones IP DNS actuales: *OldIP1*, *OldIP2*
- Nuevas direcciones IP DNS: *NewIP1*, *NewIP2*

> **Note**
>
> Si es la segunda vez que realiza este procedimiento, sustituya *OldIP1* por *OldIP2* y *NewIP1* por *NewIP2*.

Probar la nueva configuración del servidor DNS en WorkSpaces para Windows

1. Apague el servidor DNS de *OldIP1*.
2. Inicie sesión en un WorkSpace para Windows.
3. En el menú Inicio de Windows, elija Sistema de Windows, y, a continuación, elija Símbolo del sistema.
4. Ejecute el siguiente comando, donde *AD_Name* es el nombre de su Active Directory (por ejemplo, `corp.example.com`).

```
nslookup AD_Name
```

El comando `nslookup` debe devolver lo siguiente. (Si es la segunda vez que realiza este procedimiento, debería ver *NewIP2* en lugar de *OldIP2*).

```
Server:  Full_AD_Name
Address:  NewIP1

Name:    AD_Name
Addresses:  OldIP2
          NewIP1
```

5. Si el resultado no es el esperado o si recibe algún error, repita el Paso 1.
6. Espere una hora y confirme que los usuarios no hayan informado de ningún problema. Compruebe que *NewIP1* recibe consultas de DNS y ofrece respuestas.
7. Tras comprobar que el primer servidor DNS funciona correctamente, repita el Paso 1 para actualizar el segundo servidor DNS, esta vez sustituyendo *OldIP2* por *NewIP2*. A continuación, repita los pasos 2 y 3.

Probar la nueva configuración del servidor DNS en WorkSpaces para Linux

1. Apague el servidor DNS de *OldIP1*.
2. Inicie sesión en un WorkSpace para Linux.
3. En su WorkSpace para Linux, abra una ventana de terminal (Aplicaciones > Herramientas del sistema > Terminal MATE).
4. Las direcciones IP del servidor DNS devueltas en la respuesta de DHCP se escriben en el archivo local `/etc/resolv.conf` en el WorkSpace. Ejecute el siguiente comando para mostrar el contenido del archivo `/etc/resolv.conf` .

```
cat /etc/resolv.conf
```

Debería ver los siguientes datos de salida. (Si es la segunda vez que realiza este procedimiento, debería ver *NewIP2* en lugar de *OldIP2*).

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
```

```
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> Si realiza modificaciones manuales en el archivo `/etc/resolv.conf`, esos cambios se pierden al reiniciar WorkSpace.

5. Si el resultado no es el esperado o si recibe algún error, repita el Paso 1.
6. Las direcciones IP reales del servidor DNS se almacenan en el archivo `/etc/dhcp/dhclient.conf`. Para ver el contenido del archivo, ejecute el siguiente comando.

```
sudo cat /etc/dhcp/dhclient.conf
```

Debería ver los siguientes datos de salida. (Si es la segunda vez que realiza este procedimiento, debería ver *NewIP2* en lugar de *OldIP2*).

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. Espere una hora y confirme que los usuarios no hayan informado de ningún problema. Compruebe que *NewIP1* recibe consultas de DNS y ofrece respuestas.
8. Tras comprobar que el primer servidor DNS funciona correctamente, repita el Paso 1 para actualizar el segundo servidor DNS, esta vez sustituyendo *OldIP2* por *NewIP2*. A continuación, repita los pasos 2 y 3.

Eliminar el directorio de los escritorios WorkSpaces

Puede eliminar el directorio de los WorkSpaces si ya no lo utilizan otros WorkSpaces ni otras aplicaciones, como Amazon WorkDocs, Amazon WorkMail o Amazon Chime. Tenga en cuenta que debe anular el registro de un directorio si quiere eliminarlo.

> **Note**
>
> Tanto AD sencillo como el conector AD están disponibles de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio AD sencillo o conector AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.
> Si elimina su directorio AD sencillo o conector AD, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

¿Qué sucede cuando se elimina un directorio?

Qué ocurre cuando se elimina un directorioCuando se elimina un directorio de AD sencillo o de AWS Directory Service for Microsoft Active Directory, todos los datos y las instantáneas del directorio se eliminan y no se pueden recuperar. Una vez eliminado el directorio, las instancias de Amazon EC2 unidas al directorio permanecen intactas. No se puede, sin embargo, utilizar las credenciales del directorio para iniciar sesión en estas instancias. Debe registrarse en estas instancias con una cuenta de AWS que sea local para la instancia.

Cuando se elimina un directorio del conector AD, su directorio local permanece intacto. Las instancias de Amazon EC2 unidas al directorio también permanecen intactas y siguen unidas al directorio en las instalaciones. Puede seguir utilizando las credenciales del directorio para iniciar sesión en estas instancias.

Para eliminar un directorio

1. Elimine todos los WorkSpaces del directorio. Para obtener más información, consulte Eliminar WorkSpaces.
2. Busque y elimine todas las aplicaciones y servicios que están registrados en el directorio. Para obtener más información, consulte Eliminar su directorio en la Guía de administración de AWS Directory Service.
3. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
4. En el panel de navegación, elija Directories (Directorios).
5. Seleccione el directorio y elija Actions, Deregister.
6. Cuando se le pida que confirme, elija Deregister.
7. Seleccione el directorio de nuevo y elija Actions, Delete.

8. Cuando se le pida confirmación, elija Delete (Eliminar).

> **Note**
>
> La eliminación de asignaciones de aplicaciones a veces puede llevar más tiempo del esperado. Si recibe el siguiente mensaje de error, compruebe que ha quitado todas las asignaciones de aplicaciones y, a continuación, espere entre 30 y 60 minutos antes de intentar eliminar el directorio de nuevo:
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (Opcional) Después de eliminar todos los recursos de la nube virtual privada (VPC) para el directorio, puede eliminarla y liberar la dirección IP elástica utilizada para la gateway NAT. Para obtener más información, consulte Eliminar su VPC y Uso de direcciones IP elásticas en la Guía del usuario de Amazon VPC.
10. (Opcional) Para eliminar paquetes e imágenes personalizados que no vaya a volver a usar, consulte Eliminar un WorkSpaces paquete o una imagen personalizados.

Habilitar Amazon WorkDocs para Microsoft AD administrado por AWS

Si utiliza Microsoft AD administrado por AWS con Amazon WorkSpaces, puede habilitar Amazon WorkDocs para su directorio a través de la consola de Amazon WorkDocs o de la consola de AWS Directory Service.

> **Note**
>
> Amazon WorkDocs no está disponible en todas las regiones de AWS regiones en las que está disponible Amazon WorkSpaces. Para obtener más información, consulte Precios de Amazon WorkDocs.

Para habilitar WorkDocs a través de la consola de Amazon WorkDocs

1. Abra la consola de Amazon WorkDocs en https://console.aws.amazon.com/zocalo/.

2. Elija Crear un nuevo sitio de WorkDocs.
3. En Standard Setup, elija Launch.
4. Seleccione el directorio y cree el nombre del sitio.
5. Especifique el usuario que administrará el sitio de WorkDocs. Puede utilizar el administrador o cualquier usuario creado en el directorio.

Para obtener más información, consulte Introducción a Microsoft AD administrado por AWS en la Guía de administración de Amazon WorkDocs.

Para habilitar WorkDocs a través de la consola AWS Directory Service

1. Abra la consola de AWS Directory Service en https://console.aws.amazon.com/directoryservicev2/.
2. En el panel de navegación, elija Directories (Directorios).
3. En la página Directories (Directorios), elija el directorio.
4. En la página Directory details (Detalles del directorio), seleccione la pestaña Application management (Administración de aplicaciones).
5. En la sección Application access URL (URL de acceso a aplicaciones), si no se ha asignado una URL de acceso al directorio, se mostrará el botón Create (Crear). Escriba un alias de directorio y elija Create (Crear). Para obtener más información, consulte Creación de una URL de acceso en la Guía de administración.
6. En la sección Application access URL (URL de acceso a la aplicación), elija Enable (Habilitar) para habilitar el inicio de sesión único para Amazon WorkDocs. Para obtener más información, consulte Inicio de sesión único en la Guía de administración.

Configurar las herramientas de administración de Active Directory para WorkSpaces

Llevará a cabo la mayoría de las funciones administrativas del directorio WorkSpaces con herramientas de administración de directorios, como las herramientas de administración de Active Directory. Sin embargo, utilizará la consola de WorkSpaces para realizar algunas tareas relacionadas con el directorio. Para obtener más información, consulte Administrar directorios para WorkSpaces.

Si crea un directorio con AWS Managed Microsoft AD o Simple AD que incluya cinco o más WorkSpaces, le recomendamos que centralice la administración en una instancia de Amazon EC2.

Aunque puede instalar las herramientas de administración de directorios en un WorkSpace, utilizar una instancia de Amazon EC2 es una solución más sólida.

Configurar las herramientas de administración de Active Directory

1. Lance una instancia de Amazon EC2 para Windows y asóciela al directorio de WorkSpaces mediante una de las siguientes opciones:

   - Si aún no tiene una instancia de Amazon EC2 para Windows, puede asociar la instancia al dominio de su directorio al lanzarla. Para obtener más información, consulte Unión fluida de una instancia de EC2 de Windows en la Guía de administración de AWS Directory Service.
   - Si ya tiene una instancia de Amazon EC2 para Windows, puede unirla a su directorio manualmente. Para obtener más información, consulte Añadir manualmente una instancia de Windows en la Guía de administración de AWS Directory Service.

2. Instale las herramientas de administración de Active Directory en la instancia de Amazon EC2 para Windows. Para obtener más información, consulte Instalar las herramientas de administración de Active Directory en la Guía de administración de AWS Directory Service.

   > **Note**
   >
   > Al instalar las herramientas de administración de Active Directory, asegúrese de seleccionar también la administración de políticas de grupo para instalar la herramienta del editor de administración de políticas de grupo (gpmc.msc).

   Cuando finalice la instalación de la característica, las herramientas de Active Directory estarán disponibles en el menú Inicio de Windows, en Herramientas administrativas de Windows.

3. Ejecute las herramientas como administrador del directorio del modo siguiente:

   a. En el menú Inicio de Windows, abra Herramientas administrativas de Windows.

   b. Mantenga pulsada la tecla Mayús, haga clic con el botón derecho en el acceso directo de la herramienta que quiera usar y seleccione Run as different user.

   c. Introduzca las credenciales de inicio de sesión del administrador. Con Simple AD, el nombre de usuario es **`Administrator`** y con AWS Microsoft AD, el administrador es **`Admin`**.

A partir de ahora, puede realizar las tareas de administración de directorios con las herramientas de Active Directory que ya conoce. Por ejemplo, puede utilizar la herramienta de Usuarios y equipos

de Active Directory para añadir y eliminar usuarios, promocionar un usuario a administrador del directorio o restablecer una contraseña de usuario. Tenga en cuenta que debe haber iniciado sesión en la instancia de Windows como un usuario con permisos para administrar usuarios en el directorio.

Para promocionar un usuario a administrador del directorio

> **Note**
>
> Este procedimiento solo se aplica a los directorios creados con Simple AD, no a los de AWS Managed AD. Para ver los directorios creados con AWS Managed AD, consulte Administrar usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.

1. Abra la herramienta Usuarios y equipos de Active Directory.
2. Vaya a la carpeta Users del dominio y seleccione el usuario que desea promocionar.
3. Elija Action, Properties.
4. En el cuadro de diálogo Propiedades de ***`nombre de usuario`***, elija Miembro de.
5. Añada el usuario a los siguientes grupos y seleccione OK.
   - Administradores
   - Administradores de dominio
   - Administradores de empresas
   - Propietarios del creador de políticas de grupo
   - Administradores de esquemas

Para agregar o eliminar usuarios

Puede crear nuevos usuarios desde la consola de Amazon WorkSpaces únicamente durante el proceso de inicio de WorkSpace, pero no puede eliminar usuarios a través de la consola de Amazon WorkSpaces. La mayoría de las tareas de administración de usuarios, incluida la administración de grupos de usuarios, deben realizarse a través del directorio.

> **Important**
>
> Tenga en cuenta que antes de eliminar a un usuario, debe eliminar el escritorio de WorkSpaces asignado a ese usuario. Para obtener más información, consulte Eliminar WorkSpaces.

El proceso que utilice para administrar usuarios y grupos depende del tipo de directorio que utilice.

- Si utiliza AWS Managed Microsoft AD, consulte Administración de usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
- Si utiliza Simple AD, consulte Administración de usuarios y grupos en Simple AD en la Guía de administración de AWS Directory Service.
- Si utiliza Microsoft Active Directory a través de Conector AD o una relación de confianza, puede administrar los usuarios y grupos utilizando el módulo de Active Directory.

Para restablecer una contraseña de usuario

Cuando restablezca la contraseña de un usuario, no configure User must change password at next logon. Si lo hace, los usuarios no podrán conectarse a los escritorios de WorkSpaces. En lugar de eso, asigne una contraseña temporal segura a cada usuario y pídales que la cambien manualmente desde el espacio de trabajo la próxima vez que inicie sesión.

> **Note**
>
> Si utiliza Conector AD o si sus usuarios se encuentran en la región AWS GovCloud (Oeste de EE. UU.), no podrán restablecer sus propias contraseñas. (La opción ¿Olvidó la contraseña? de la pantalla de inicio de sesión de la aplicación cliente de WorkSpaces no estará disponible).

Lanzar un escritorio virtual utilizando WorkSpaces

WorkSpaces le permite poner a disposición de los usuarios escritorios virtuales basados en la nube de Microsoft Windows, Amazon Linux o Ubuntu Linux, conocidos como WorkSpaces.

> **Note**
>
> El valor de nombre de equipo que se muestra para un WorkSpace en la consola de Amazon WorkSpaces varía en función del tipo de WorkSpace que haya lanzado (Amazon Linux, Ubuntu o Windows). El nombre del equipo para un WorkSpace puede estar en uno de estos formatos:
>
> - Amazon Linux: A- *xxxxxxxxxxxxx*
> - ***Ubuntu: U-xxxxxxxxxxxxx***
> - Windows *: IP-C xxxxxx o WSAMZN- xxxxxxx o EC2AMAZ- xxxxxxx*
>
> En Windows WorkSpaces, el formato del nombre del equipo viene determinado por el tipo de paquete y, en el caso de los WorkSpaces creados a partir de paquetes públicos o de paquetes personalizados basados en imágenes públicas, por el momento en que se crearon las imágenes públicas.
> A partir del 22 de junio de 2020, los Windows WorkSpaces lanzados desde paquetes públicos tienen el formato WSAMZN-*xxxxxxx* para los nombres de sus equipos en lugar del formato IP-C*xxxxxx*.
> Para los paquetes personalizados basados en una imagen pública, si la imagen pública se creó antes del 22 de junio de 2020, los nombres de los equipos tienen el formato EC2AMAZ-*xxxxxxx*. Si la imagen pública se creó a partir del 22 de junio de 2020, los nombres de ordenador tienen el formato WSAMZN-*xxxxxxx*.
> Para los paquetes "Traiga su propia licencia" (BYOL), se utiliza de forma predeterminada el formato DESKTOP-*xxxxxxx* o el formato EC2AMAZ-*xxxxxxx* para los nombres de los equipos.
> Si ha especificado un formato personalizado para los nombres de equipo en sus paquetes personalizados o BYOL, su formato personalizado anula estos valores predeterminados.
> Para especificar un formato personalizado, consulte Crea una WorkSpaces imagen y un paquete personalizados.

Importante: Si cambia el nombre del equipo para un WorkSpace a través de la configuración del sistema Windows, ya no podrá acceder al WorkSpace.

WorkSpaces utiliza un directorio para almacenar y administrar la información de sus WorkSpaces y usuarios. Puede elegir cualquiera de las opciones siguientes:

- Cree un directorio de AD sencillo.
- Crear un AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD.
- Conectarse con un Microsoft Active Directory existente a través del conector de Active Directory.
- Crear una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio local.

Note

- Los directorios compartidos no son compatibles actualmente con Amazon WorkSpaces.
- Si configura su directorio de Microsoft AD administrado por AWS para la reproducción en varias regiones, solo se podrá registrar el directorio de la región principal para utilizarlo con Amazon WorkSpaces. Los intentos de registrar el directorio en una región duplicada para su uso con Amazon WorkSpaces fallarán. No se admite la replicación multirregional con AWS Managed Microsoft AD para su uso con Amazon WorkSpaces dentro de las regiones replicadas.
- Tanto AD sencillo como el conector AD están disponibles de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio AD sencillo o conector AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.

  Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio AD sencillo o conector AD, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

En los siguientes tutoriales se muestra cómo lanzar un WorkSpace mediante las opciones de servicio de directorio compatibles.

Tutoriales

- Lanzamiento de un WorkSpace con AWS Managed Microsoft AD
- Lanzar un escritorio de WorkSpaces con AD sencillo
- Iniciar WorkSpace con el conector AD
- Lanzar escritorios de WorkSpaces usando un dominio de confianza

Lanzamiento de un WorkSpace con AWS Managed Microsoft AD

WorkSpaces le permite proporcionar a sus usuarios escritorios virtuales Windows y Linux basados en la nube, conocidos como WorkSpaces.

WorkSpaces utiliza directorios para almacenar y administrar la información de sus WorkSpaces y usuarios. Para el directorio, puede elegir entre Simple AD, Conector AD o AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD. Además, puede establecer una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio local.

En este tutorial, se lanza un WorkSpace que utiliza AWS Managed Microsoft AD. Para encontrar tutoriales que utilicen las otras opciones, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

Tareas

- Antes de empezar
- Paso 1: crear un directorio de AWS Managed Microsoft AD
- Paso 2: Crear un espacio de trabajo
- Paso 3: Conectarse al WorkSpace
- Pasos siguientes

Antes de empezar

- WorkSpaces no está disponible en todas las regiones. Compruebe las regiones que son compatibles y seleccione una para los WorkSpaces. Para obtener más información sobre las regiones compatibles, consulte Precios de WorkSpaces por región de AWS.
- Cuando lanza un escritorio de WorkSpaces, debe seleccionar un paquete de WorkSpaces. Un paquete es una combinación de un sistema operativo, capacidad informática, almacenamiento y recursos de software. Para obtener más información, consulte Paquetes de Amazon WorkSpaces.

- Cuando cree un directorio con AWS Directory Service o lance un WorkSpace, debe crear o seleccionar una nube virtual privada configurada con una subred pública y dos subredes privadas. Para obtener más información, consulte Configurar una VPC para WorkSpaces.

Paso 1: crear un directorio de AWS Managed Microsoft AD

Primero cree un directorio de AWS Managed Microsoft AD. AWS Directory Service crea dos servidores de directorios, uno en cada una de las subredes privadas de la VPC. Tenga en cuenta que en el directorio no hay usuarios inicialmente. En el siguiente paso agregará un usuario cuando lance el escritorio de WorkSpaces.

> **Note**
>
> - Los directorios compartidos no son compatibles actualmente con Amazon WorkSpaces.
> - Si su directorio de Microsoft AD administrado por AWS se ha configurado para la reproducción en varias regiones, solo se podrá registrar el directorio de la región principal para utilizarlo con Amazon WorkSpaces. Los intentos de registrar el directorio en una región duplicada para su uso con Amazon WorkSpaces fallarán. No se admite la replicación multirregional con AWS Managed Microsoft AD para su uso con Amazon WorkSpaces dentro de las regiones replicadas.

Para crear un directorio de AWS Managed Microsoft AD

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Set up Directory, Create Microsoft AD.
4. Configure el directorio del modo siguiente:

   a. En Organization name (Nombre de la organización), escriba un nombre para el directorio que sea único en la organización (por ejemplo, «mi-directorio-de-demostración»). Este nombre debe tener al menos cuatro caracteres, incluir caracteres alfanuméricos y guiones (-), y comenzar o terminar por un carácter distinto de un guion.

   b. En Directory DNS (DNS de directorio), escriba el nombre completo del directorio (por ejemplo, «workspaces.demo.com»).

> **Important**
>
> Si necesita actualizar su servidor DNS después de lanzar sus WorkSpaces, siga el procedimiento indicado en Actualizar los servidores de DNS para Amazon WorkSpaces para asegurarse de que sus WorkSpaces se actualizan correctamente.

c. En NetBIOS name (Nombre de NetBIOS), escriba un nombre abreviado para el directorio (por ejemplo, «workspaces»).

d. En Admin password (Contraseña de administrador) y Confirm password (Confirmar contraseña), escriba una contraseña para la cuenta del administrador del directorio. Para obtener más información sobre los requisitos de las contraseñas, consulte Crear su directorio de Managed Microsoft AD por AWS en la Guía de administración de AWS Directory Service.

e. (Opcional) En Description (Descripción), escriba una descripción del directorio.

f. En VPC, seleccione la VPC que ha creado.

g. En Subnets, seleccione las dos subredes privadas (con los bloques CIDR `10.0.1.0/24` y `10.0.2.0/24`).

h. Elija Next Step (Paso siguiente).

5. Seleccione Create Microsoft AD.
6. Seleccione Done (Listo). El estado inicial del directorio es `Creating`. Cuando la creación del directorio se completa, el estado cambia a `Active`.

Paso 2: Crear un espacio de trabajo

Ahora que ha creado un directorio de AWS Managed Microsoft AD, ya puede crear un WorkSpace.

Para crear un escritorio WorkSpace

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Elija Launch WorkSpaces.
4. En la página Seleccionar un directorio, elija el directorio que ha creado y, a continuación, elija Pasos siguientes. WorkSpaces registra su directorio.
5. En la página Identify Users, agregue un nuevo usuario al directorio del modo siguiente:

a. Complete Username, First Name, Last Name y Email. Utilice una dirección de correo electrónico a la que tenga acceso.

b. Seleccione Create Users.

c. Elija Next Step (Paso siguiente).

6. En la página Select Bundle, seleccione un paquete y después elija Next Step.

> **Note**
>
> Revise los usos recomendados y las especificaciones de cada paquete para asegurarse de que selecciona el que mejor se adapta a sus usuarios. Para obtener más información sobre cada caso de uso, consulte Paquetes de Amazon WorkSpaces. Para obtener más información sobre las especificaciones de los paquetes, los usos recomendados y los precios, consulte Precios de Amazon WorkSpaces.

7. En la página WorkSpaces Configuration, elija un modo de ejecución y después elija Next Step.

8. En la página Review & Launch WorkSpaces, elija Launch WorkSpaces. El estado inicial del WorkSpace es `PENDING`. Cuando el lanzamiento ha terminado, el estado es `AVAILABLE` y se envía una invitación a la dirección de correo electrónico que especificó para el usuario.

> **Note**
>
> Los correos electrónicos de invitación no se envían si el usuario ya existe en Active Directory. Para ello, envíe manualmente al usuario un correo electrónico de invitación. Para obtener más información, consulte Enviar un correo electrónico de invitación.

9. (Opcional) Si Amazon WorkDocs está disponible en la región, puede habilitar Amazon WorkDocs para todos los usuarios del directorio. Para obtener más información, consulte Habilitar Amazon WorkDocs para Microsoft AD administrado por AWS. Para obtener más información sobre Amazon WorkDocs, consulte Amazon WorkDocs Drive en la Guía de administración de Amazon WorkDocs.

Paso 3: Conectarse al WorkSpace

Después de recibir el correo electrónico de invitación, puede conectarse al WorkSpace utilizando el cliente de su elección. Después de iniciar sesión, el cliente muestra el escritorio de WorkSpaces.

Para conectarse al WorkSpace

1. Abra el enlace del correo electrónico de invitación. Cuando se le solicite, especifique una contraseña y active el usuario. Recuerde esta contraseña, ya que la necesitará para iniciar sesión en el WorkSpace.

   > **Note**
   >
   > Las contraseñas distinguen entre mayúsculas y minúsculas y debe tener un mínimo de 8 caracteres y un máximo de 64. Las contraseñas deben contener al menos un carácter de cada una de las siguientes categorías: letras minúsculas (a-z), letras mayúsculas (A-Z), números (0-9) y ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/.

2. Consulte Clientes de WorkSpaces en la Guía del usuario de Amazon WorkSpaces para obtener más información sobre los requisitos de cada cliente y, a continuación, siga uno de estos procedimientos:

   - Cuando se le solicite, descargue una de las aplicaciones cliente o inicie Acceso web.
   - Si no se le solicita y aún no ha instalado una aplicación cliente, abra https://clients.amazonworkspaces.com/ y descargue una de las aplicaciones cliente o inicie Acceso web.

   > **Note**
   >
   > No puede utilizar un navegador web (Acceso web) para conectarse con los WorkSpaces de Amazon Linux.

3. Inicie el cliente y escriba el código de registro que se incluye en el correo de invitación y elija Register.
4. Cuando se le solicite iniciar sesión, introduzca las credenciales de inicio de sesión del usuario y, a continuación, seleccione Iniciar sesión.
5. (Opcional) Cuando se le solicite guardar las credenciales, elija Yes.

Pasos siguientes

Puede seguir y personalizar el WorkSpace que acaba de crear. Por ejemplo, puede instalar software y, después, crear un paquete personalizado del WorkSpace. También puede realizar varias tareas

administrativas para sus WorkSpaces y su directorio de WorkSpaces. Si ya ha terminado con él, puede eliminarlo. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados
- Administre su WorkSpaces
- Administrar directorios para WorkSpaces
- Eliminar WorkSpaces

Para obtener más información sobre el uso de las aplicaciones cliente de WorkSpaces, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte Clientes de WorkSpaces y Soporte de dispositivos periféricos en la Guía del usuario de Amazon WorkSpaces.

Lanzar un escritorio de WorkSpaces con AD sencillo

WorkSpaces le permite proporcionar escritorios virtuales de Microsoft Windows y Linux basados en la nube para sus usuarios, conocidos como WorkSpaces.

WorkSpaces utiliza directorios para almacenar y administrar la información de sus WorkSpaces y usuarios. Para el directorio, puede elegir entre Simple AD, Conector AD o AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD. Además, puede establecer una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio local.

En este tutorial, se lanza un escritorio de WorkSpaces que utiliza AD sencillo. Para encontrar tutoriales que utilicen las otras opciones, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

Tareas

- Antes de empezar
- Paso 1: Crear el directorio AD sencillo
- Paso 2: Crear un espacio de trabajo
- Paso 3: Conectarse al WorkSpace
- Pasos siguientes

Antes de empezar

- AD sencillo no está disponible en todas las regiones. Compruebe las regiones que son compatibles y seleccione una región para su directorio de AD sencillo. Para obtener más información sobre las regiones compatibles con AD sencillo, consulte Disponibilidad regional para Directory Service deAWS.
- WorkSpaces no está disponible en todas las regiones. Compruebe las regiones que son compatibles y seleccione una para los WorkSpaces. Para obtener más información sobre las regiones compatibles, consulte Precios de WorkSpaces por región de AWS.
- Cuando lanza un escritorio de WorkSpaces, debe seleccionar un paquete de WorkSpaces. Un paquete es una combinación de un sistema operativo, capacidad informática, almacenamiento y recursos de software. Para obtener más información, consulte Paquetes de Amazon WorkSpaces.
- Cuando cree un directorio con AWS Directory Service o lance un WorkSpace, debe crear o seleccionar una nube virtual privada configurada con una subred pública y dos subredes privadas. Para obtener más información, consulte Configurar una VPC para WorkSpaces.

Paso 1: Crear el directorio AD sencillo

Cree un directorio de Simple AD. AWS Directory Service crea dos servidores de directorios, uno en cada una de las subredes privadas de la VPC. Tenga en cuenta que en el directorio no hay usuarios inicialmente. Agregará un usuario en el siguiente paso al crear el escritorio de WorkSpaces.

> **Note**
>
> AD sencillo está disponible de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio de Simple AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.
> Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio de AD sencillo, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

Para crear un directorio de AD sencillo

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.

2. En el panel de navegación, elija Directories (Directorios).
3. Elija Crear un directorio, AD sencillo y Siguiente.
4. Configure el directorio del modo siguiente:

   a. En Organization name (Nombre de la organización), escriba un nombre para el directorio que sea único en la organización (por ejemplo, mi-directorio-de-ejemplo). Este nombre debe tener al menos cuatro caracteres, incluir caracteres alfanuméricos y guiones (-), y comenzar o terminar por un carácter distinto de un guion.

   b. En Nombre del directorio DNS, introduzca el nombre completo del directorio (por ejemplo, ejemplo.com).

   > **Important**
   >
   > Si necesita actualizar su servidor DNS después de lanzar sus WorkSpaces, siga el procedimiento indicado en Actualizar los servidores de DNS para Amazon WorkSpaces para asegurarse de que sus WorkSpaces se actualizan correctamente.

   c. En NetBIOS name (Nombre de NetBIOS), escriba un nombre abreviado para el directorio (por ejemplo, «ejemplo»).

   d. En Admin password (Contraseña de administrador) y Confirm password (Confirmar contraseña), escriba una contraseña para la cuenta del administrador del directorio. Para obtener más información sobre los requisitos de contraseña, consulte Cómo crear un directorio de Microsoft AD en la Guía de administración de AWS Directory Service.

   e. (Opcional) En Description (Descripción), escriba una descripción del directorio.

   f. En Tamaño del directorio, elija Pequeño.

   g. En VPC, seleccione la VPC que ha creado.

   h. En Subnets, seleccione las dos subredes privadas (con los bloques CIDR `10.0.1.0/24` y `10.0.2.0/24`).

   i. Elija Next (Siguiente).

5. Elija Create directory.
6. El estado inicial del directorio es `Requested` y luego `Creating`. Cuando se complete la creación del directorio (puede tardar unos minutos), el estado será `Active`.

Qué ocurre durante la creación del directorio

WorkSpaces realiza las siguientes tareas en su nombre:

- Crea un rol de IAM para permitir que el servicio de WorkSpaces cree interfaces de red elásticas y enumere los directorios de WorkSpaces. El nombre de este rol es `workspaces_DefaultRole`.
- Establece un directorio de AD sencillo en la VPC que se usa para almacenar la información de los usuarios y de los WorkSpaces. El directorio tiene una cuenta de administrador con el nombre de usuario Administrator y la contraseña especificada.
- Crea dos grupos de seguridad: uno para los controladores del directorio y otro para los WorkSpaces del directorio.

Paso 2: Crear un espacio de trabajo

Ahora ya puede lanzar el WorkSpace.

Para crear un WorkSpace para un usuario

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Elija Launch WorkSpaces.
4. En la página Select a Directory, haga lo siguiente:
   a. En Directory, elija el directorio que ha creado.
   b. En Habilitar los permisos de autoservicio, elija Sí o No e introduzca una descripción.
   c. En Enable Amazon WorkDocs, seleccione Yes.

      > **Note**
      >
      > Esta opción solo está disponible si Amazon WorkDocs está disponible en la región seleccionada.

   d. Elija Next Step (Paso siguiente). WorkSpaces registra su directorio AD sencillo.
5. En la página Identify Users, agregue un nuevo usuario al directorio del modo siguiente:
   a. Complete Username, First Name, Last Name y Email. Utilice una dirección de correo electrónico a la que tenga acceso.

b. Seleccione Create Users.

c. Elija Next Step (Paso siguiente).

6. En la página Select Bundle, seleccione un paquete y después elija Next Step.

> **Note**
>
> Revise los usos recomendados y las especificaciones de cada paquete para asegurarse de que selecciona el que mejor se adapta a sus usuarios. Para obtener más información sobre cada caso de uso, consulte Paquetes de Amazon WorkSpaces. Para obtener más información sobre las especificaciones de los paquetes, los usos recomendados y los precios, consulte Precios de Amazon WorkSpaces.

7. En la página WorkSpaces Configuration, elija un modo de ejecución y después elija Next Step.

8. En la página Review & Launch WorkSpaces, elija Launch WorkSpaces. El estado inicial del WorkSpace es `PENDING`. WhUna vez finalizado el lanzamiento (que puede tardar hasta 20 minutos), el estado será `AVAILABLE` y se envía una invitación a la dirección de correo electrónico que especificó para el usuario.

> **Note**
>
> Los correos electrónicos de invitación no se envían si el usuario ya existe en Active Directory. Para ello, envíe manualmente al usuario un correo electrónico de invitación. Para obtener más información, consulte Enviar un correo electrónico de invitación.

Paso 3: Conectarse al WorkSpace

Después de recibir el correo electrónico de invitación, puede conectarse al WorkSpace utilizando el cliente de su elección. Después de iniciar sesión, el cliente muestra el escritorio de WorkSpaces.

Para conectarse al WorkSpace

1. Abra el enlace del correo electrónico de invitación. Cuando se lo soliciten, escriba una contraseña y active el usuario. Recuerde esta contraseña, ya que la necesitará para iniciar sesión en el WorkSpace.

> **Note**
>
> Las contraseñas distinguen entre mayúsculas y minúsculas y debe tener un mínimo de 8 caracteres y un máximo de 64. Las contraseñas deben contener al menos un carácter de cada una de las siguientes categorías: letras minúsculas (a-z), letras mayúsculas (A-Z), números (0-9) y ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/.

2. Consulte Clientes de WorkSpaces en la Guía del usuario de Amazon WorkSpaces para obtener más información sobre los requisitos de cada cliente y, a continuación, siga uno de estos procedimientos:

   - Cuando se le solicite, descargue una de las aplicaciones cliente o inicie Acceso web.
   - Si no se le solicita y aún no ha instalado una aplicación cliente, abra https://clients.amazonworkspaces.com/ y descargue una de las aplicaciones cliente o inicie Acceso web.

   > **Note**
   >
   > No puede utilizar un navegador web (Acceso web) para conectarse con los WorkSpaces de Amazon Linux.

3. Inicie el cliente y escriba el código de registro que se incluye en el correo de invitación y elija Register.
4. Cuando se le solicite iniciar sesión, introduzca las credenciales de inicio de sesión del usuario y, a continuación, seleccione Iniciar sesión.
5. (Opcional) Cuando se le solicite guardar las credenciales, elija Yes.

Pasos siguientes

Puede seguir y personalizar el WorkSpace que acaba de crear. Por ejemplo, puede instalar software y, después, crear un paquete personalizado del WorkSpace. También puede realizar varias tareas administrativas para sus WorkSpaces y su directorio de WorkSpaces. Si ya ha terminado con él, puede eliminarlo. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados

- Administre su WorkSpaces
- Administrar directorios para WorkSpaces
- Eliminar WorkSpaces

Para obtener más información sobre el uso de las aplicaciones cliente de WorkSpaces, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte Clientes de WorkSpaces y Soporte de dispositivos periféricos en la Guía del usuario de Amazon WorkSpaces.

Iniciar WorkSpace con el conector AD

WorkSpaces le permite proporcionar escritorios virtuales de Microsoft Windows y Linux basados en la nube para sus usuarios, conocidos como WorkSpaces.

WorkSpaces utiliza directorios para almacenar y administrar la información de sus WorkSpaces y usuarios. Para el directorio, puede elegir entre Simple AD, Conector AD o AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD. Además, puede establecer una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio local.

En este tutorial, se lanza un escritorio de WorkSpaces que utiliza Conector AD. Para encontrar tutoriales que utilicen las otras opciones, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

Tareas

- Antes de empezar
- Paso 1: Crear un Conector AD
- Paso 2: Crear un espacio de trabajo
- Paso 3: Conectarse al WorkSpace
- Pasos siguientes

Antes de empezar

- WorkSpaces no está disponible en todas las regiones. Compruebe las regiones que son compatibles y seleccione una para los WorkSpaces. Para obtener más información sobre las regiones compatibles, consulte Precios de WorkSpaces por región de AWS.

- Cuando lanza un escritorio de WorkSpaces, debe seleccionar un paquete de WorkSpaces. Un paquete es una combinación de un sistema operativo, capacidad informática, almacenamiento y recursos de software. Para obtener más información, consulte Paquetes de Amazon WorkSpaces.
- Cree una cloud virtual privada al menos con dos subredes privadas. Para obtener más información, consulte Configurar una VPC para WorkSpaces. La VPC debe estar conectada a la red local a través de una conexión de red privada virtual (VPN) o de AWS Direct Connect. Para obtener más información, consulte Requisitos previos del conector AD en la Guía de administración de AWS Directory Service.
- Proporcione acceso a Internet desde el WorkSpace. Para obtener más información, consulte Proporcione acceso a Internet desde su WorkSpace.

Paso 1: Crear un Conector AD

> **Note**
>
> El conector AD está disponible de forma gratuita para su uso con WorkSpaces. Si no se utiliza ningún WorkSpaces con su directorio del conector AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service. Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio del conector AD, siempre puede crear uno nuevo cuando quiera volver a utilizar WorkSpaces.

Para crear una instancia de Conector AD

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Set up Directory, Create Conector AD.
4. En Organization name (Nombre de la organización), escriba un nombre para el directorio que sea único en la organización (por ejemplo, mi-directorio-de-ejemplo). Este nombre debe tener al menos cuatro caracteres, incluir caracteres alfanuméricos y guiones (-), y comenzar o terminar por un carácter distinto de un guion.
5. En Connected directory DNS (DNS de directorio conectado), escriba el nombre completo del directorio local (por ejemplo, «ejemplo.com»).

6. En Connected directory NetBIOS name (Nombre de NetBIOS de directorio conectado), escriba el nombre abreviado del directorio local (por ejemplo, «ejemplo»).
7. En Connector account username (Nombre de usuario de cuenta de conector), escriba el nombre de usuario de un usuario del directorio local. El usuario debe tener permisos para leer usuarios y grupos, crear objetos del equipo y unir equipos al dominio.
8. En Contraseña de la cuenta del conector y en Confirmar contraseña, introduzca la contraseña del usuario local.
9. En DNS address (Dirección DNS), escriba la dirección IP de al menos un servidor DNS del directorio local.

> **Important**
>
> Si necesita actualizar la dirección IP de su servidor DNS después de lanzar sus WorkSpaces, siga el procedimiento indicado en Actualizar los servidores de DNS para Amazon WorkSpaces para asegurarse de que sus WorkSpaces se actualicen correctamente.

10. (Opcional) En Description (Descripción), escriba una descripción del directorio.
11. Mantenga Size en Small.
12. En VPC, seleccione la VPC.
13. En Subnets, seleccione las subredes. Los servidores DNS que especifique deben ser accesibles desde cada subred.
14. Elija Next Step (Paso siguiente).
15. Elija Create Conector AD. Se tarda unos minutos en conectar a su directorio. El estado inicial del directorio es `Requested` y luego `Creating`. Cuando la creación del directorio se completa, el estado cambia a `Active`.

Paso 2: Crear un espacio de trabajo

Ahora ya puede lanzar WorkSpaces para uno o varios usuarios del directorio local.

Para iniciar un espacio de trabajo para un usuario existente

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.

3. Elija Launch WorkSpaces.
4. En Directory, elija el directorio que ha creado.
5. (Opcional) Si es la primera vez que lanza WorkSpace en este directorio y Amazon WorkDocs es compatible en la región, puede habilitar o deshabilitar Amazon WorkDocs para todos los usuarios del directorio. Para obtener más información sobre Amazon WorkDocs, consulte Amazon WorkDocs Drive en la Guía de administración de Amazon WorkDocs.
6. Elija Next (Siguiente). WorkSpaces registra el conector AD.
7. Seleccione uno o varios usuarios existentes en su directorio local. No añada nuevos usuarios a un directorio local a través de la consola de WorkSpaces.

   Para buscar a los usuarios que va a seleccionar, escriba todo o parte del nombre del usuario y elija Search (Buscar) o Show All Users (Mostrar todos los usuarios). Tenga en cuenta que no puede seleccionar un usuario que no tenga dirección de correo electrónico.

   Después de seleccionar a los usuarios, elija Add Selected y, a continuación, elija Next Step.
8. En Select Bundle, elija el paquete de WorkSpace predeterminado que se utilizará para los WorkSpaces. En Assign WorkSpace Bundles, puede elegir otro paquete distinto para un WorkSpace individual, si es necesario. Cuando haya terminado, seleccione Next Step.

   > **Note**
   >
   > Revise los usos recomendados y las especificaciones de cada paquete para asegurarse de que selecciona el que mejor se adapta a sus usuarios. Para obtener más información sobre cada caso de uso, consulte Paquetes de Amazon WorkSpaces. Para obtener más información sobre las especificaciones de los paquetes, los usos recomendados y los precios, consulte Precios de Amazon WorkSpaces.
9. Elija un modo de ejecución para los Workspaces y después, Next Step. Para obtener más información, consulte Controlar el modo de ejecución de WorkSpaces.
10. Elija Launch WorkSpaces. El estado inicial del WorkSpace es `PENDING`. Cuando el lanzamiento se completa, el estado cambia a `AVAILABLE`.
11. Envíe invitaciones a la dirección de correo electrónico de cada usuario. (Estas invitaciones no se envían automáticamente si se utiliza Conector AD). Para obtener más información, consulte Enviar un correo electrónico de invitación.

Paso 3: Conectarse al WorkSpace

Puede conectarse al escritorio WorkSpace utilizando el cliente de su elección. Después de iniciar sesión, el cliente muestra el escritorio de WorkSpaces.

Para conectarse al WorkSpace

1. Abra el enlace del correo electrónico de invitación.
2. Consulte Clientes de WorkSpaces en la Guía del usuario de Amazon WorkSpaces para obtener más información sobre los requisitos de cada cliente y, a continuación, siga uno de estos procedimientos:
   - Cuando se le solicite, descargue una de las aplicaciones cliente o inicie Acceso web.
   - Si no se le solicita y aún no ha instalado una aplicación cliente, abra https://clients.amazonworkspaces.com/ y descargue una de las aplicaciones cliente o inicie Acceso web.

   > **Note**
   >
   > No puede utilizar un navegador web (Acceso web) para conectarse con los WorkSpaces de Amazon Linux.

3. Inicie el cliente y escriba el código de registro que se incluye en el correo de invitación y elija Register.
4. Cuando se le solicite iniciar sesión, introduzca las credenciales de inicio de sesión del usuario y, a continuación, seleccione Iniciar sesión.
5. (Opcional) Cuando se le solicite guardar las credenciales, elija Yes.

> **Note**
>
> Como está utilizando Conector AD, los usuarios no podrán restablecer sus propias contraseñas. (La opción ¿Olvidó la contraseña? de la pantalla de inicio de sesión de la aplicación cliente de WorkSpaces no estará disponible). Para obtener información acerca de cómo restablecer las contraseñas de usuario, consulte Configurar las herramientas de administración de Active Directory para WorkSpaces.

Pasos siguientes

Puede seguir y personalizar el WorkSpace que acaba de crear. Por ejemplo, puede instalar software y, después, crear un paquete personalizado del WorkSpace. También puede realizar varias tareas administrativas para sus WorkSpaces y su directorio de WorkSpaces. Si ya ha terminado con él, puede eliminarlo. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados
- Administre su WorkSpaces
- Administrar directorios para WorkSpaces
- Eliminar WorkSpaces

Para obtener más información sobre el uso de las aplicaciones cliente de WorkSpaces, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte Clientes de WorkSpaces y Soporte de dispositivos periféricos en la Guía del usuario de Amazon WorkSpaces.

Lanzar escritorios de WorkSpaces usando un dominio de confianza

WorkSpaces le permite proporcionar a sus usuarios escritorios virtuales basados en la nube de Microsoft Windows, Amazon Linux o Ubuntu Linux, conocidos como WorkSpaces.

WorkSpaces utiliza directorios para almacenar y administrar la información de sus WorkSpaces y usuarios. Para el directorio, puede elegir entre Simple AD, Conector AD o AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD. Además, puede establecer una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio local.

En este tutorial, se lanza un escritorio WorkSpace que utiliza una relación de confianza. Para encontrar tutoriales que utilicen las otras opciones, consulte Lanzar un escritorio virtual utilizando WorkSpaces.

Tareas

- Antes de empezar
- Paso 1: Establecer una relación de confianza
- Paso 2: Crear un espacio de trabajo
- Paso 3: Conectarse al WorkSpace

- Pasos siguientes

Antes de empezar

- El lanzamiento de WorkSpaces con cuentas de Cuentas de AWS en un dominio de confianza independiente funciona con AWS Managed Microsoft AD cuando está configurado mediante una relación de confianza con el directorio en las instalaciones. Sin embargo, WorkSpaces que utiliza AD sencillo o el conector AD no puede lanzar WorkSpaces para usuarios desde un dominio de confianza.
- WorkSpaces no está disponible en todas las regiones. Compruebe las regiones que son compatibles y seleccione una para los WorkSpaces. Para obtener más información sobre las regiones compatibles, consulte Precios de WorkSpaces por región de AWS.
- Cuando lanza un escritorio de WorkSpaces, debe seleccionar un paquete de WorkSpaces. Un paquete es una combinación de capacidad informática, almacenamiento y recursos de software. Para obtener más información, consulte Paquetes de Amazon WorkSpaces.
- Cuando cree un directorio con AWS Directory Service o lance un WorkSpace, debe crear o seleccionar una nube virtual privada configurada con una subred pública y dos subredes privadas. Para obtener más información, consulte Configurar una VPC para WorkSpaces.

Paso 1: Establecer una relación de confianza

Para establecer la relación de confianza

1. Configure AWS Managed Microsoft AD en la nube virtual privada (VPC). Para obtener más información, consulte Creación del Microsoft AD administrado por AWS en la Guía de administración de AWS Directory Service.

   > **Note**
   >
   > - Los directorios compartidos no son compatibles actualmente con Amazon WorkSpaces.
   > - Si su directorio de Microsoft AD administrado por AWS se ha configurado para la reproducción en varias regiones, solo se podrá registrar el directorio de la región principal para utilizarlo con Amazon WorkSpaces. Los intentos de registrar el directorio en una región duplicada para su uso con Amazon WorkSpaces fallarán. No se admite

la replicación multirregional con AWS Managed Microsoft AD para su uso con Amazon WorkSpaces dentro de las regiones replicadas.

2. Cree una relación de confianza entre AWS Managed Microsoft AD y el dominio local. Asegúrese de que la confianza se configura de manera bidireccional. Para obtener más información, consulte Tutorial: Crear una relación de confianza entre Microsoft AD administrado por AWS y el dominio en las instalaciones en la Guía de administración de Directory Service deAWS Directory Service.

Se puede utilizar una relación de confianza unidireccional o bidireccional para administrar y autenticar con WorkSpaces, y para que WorkSpaces se pueda aprovisionar a usuarios y grupos en las instalaciones. Para obtener más información, consulte Implementación de Amazon WorkSpaces mediante un dominio de recursos de confianza unidireccional con Directory Service de AWS.

> **Note**
>
> Ubuntu WorkSpaces utiliza System Security Services Daemon (SSSD) para la integración con Active Directory, y SSSD no admite la confianza forestal. En su lugar, configure la confianza externa. Se recomienda la confianza bidireccional para Amazon Linux y Ubuntu WorkSpaces.

Paso 2: Crear un espacio de trabajo

Después de establecer una relación de confianza entre AWS Managed Microsoft AD y el dominio local de Microsoft Active Directory, puede aprovisionar WorkSpaces para los usuarios en el dominio local.

Tenga en cuenta que deberá asegurarse de que la configuración de GPO se replique en todos los dominios antes de poder aplicarla a los WorkSpaces.

Para iniciar espacios de trabajos para usuarios en un dominio local de confianza

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Elija Launch WorkSpaces.

4. En la página Select a Directory, elija el directorio que acaba de registrar y, a continuación, elija Next Step.
5. En la página Identify Users, haga lo siguiente:
   a. En Select trust from forest, seleccione la relación de confianza que ha creado.
   b. Seleccione los usuarios del dominio local y, a continuación, elija Add Selected.
   c. Elija Next Step (Paso siguiente).
6. Seleccione el paquete que se va a utilizar para WorkSpaces y, a continuación, elija Next Step.

   > **Note**
   >
   > Revise los usos recomendados y las especificaciones de cada paquete para asegurarse de que selecciona el que mejor se adapta a sus usuarios. Para obtener más información sobre cada caso de uso, consulte Paquetes de Amazon WorkSpaces. Para obtener más información sobre las especificaciones de los paquetes, los usos recomendados y los precios, consulte Precios de Amazon WorkSpaces.

7. Elija el modo de ejecución, elija la configuración de cifrado y configure las etiquetas. Cuando haya terminado, seleccione Next Step.
8. Elija Launch WorkSpaces. Tenga en cuenta que los espacios de trabajo podrían tardar hasta 20 minutos en estar disponibles y hasta 40 minutos si está habilitado el cifrado. El estado inicial del WorkSpace es `PENDING`. Cuando el lanzamiento se completa, el estado cambia a `AVAILABLE`.
9. Envíe invitaciones a la dirección de correo electrónico de cada usuario. (Estas invitaciones no se envían automáticamente si se utiliza una relación de confianza). Para obtener más información, consulte Enviar un correo electrónico de invitación.

Paso 3: Conectarse al WorkSpace

Una vez recibido el correo electrónico de invitación, puede conectarse al WorkSpace. Los usuarios pueden introducir los nombres de usuario como username, corp\username o corp.example.com\username).

Para conectarse al WorkSpace

1. Abra el enlace del correo electrónico de invitación. Cuando se lo soliciten, escriba una contraseña y active el usuario. Recuerde esta contraseña, ya que la necesitará para iniciar sesión en el WorkSpace.

> **Note**
>
> Las contraseñas distinguen entre mayúsculas y minúsculas y debe tener un mínimo de 8 caracteres y un máximo de 64. Las contraseñas deben contener al menos un carácter de cada una de las siguientes categorías: letras minúsculas (a-z), letras mayúsculas (A-Z), números (0-9) y ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/.

2. Consulte Clientes de WorkSpaces en la Guía del usuario de Amazon WorkSpaces para obtener más información sobre los requisitos de cada cliente y, a continuación, siga uno de estos procedimientos:

   - Cuando se le solicite, descargue una de las aplicaciones cliente o inicie Acceso web.
   - Si no se le solicita y aún no ha instalado una aplicación cliente, abra https://clients.amazonworkspaces.com/ y descargue una de las aplicaciones cliente o inicie Acceso web.

   > **Note**
   >
   > No puede utilizar un navegador web (Acceso web) para conectarse con los WorkSpaces de Amazon Linux.

3. Inicie el cliente y escriba el código de registro que se incluye en el correo de invitación y elija Register.
4. Cuando se le solicite iniciar sesión, introduzca las credenciales de inicio de sesión del usuario y, a continuación, seleccione Iniciar sesión.
5. (Opcional) Cuando se le solicite guardar las credenciales, elija Yes.

Pasos siguientes

Puede seguir y personalizar el WorkSpace que acaba de crear. Por ejemplo, puede instalar software y, después, crear un paquete personalizado del WorkSpace. También puede realizar varias tareas administrativas para sus WorkSpaces y su directorio de WorkSpaces. Si ya ha terminado con él, puede eliminarlo. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados

- Administre su WorkSpaces
- Administrar directorios para WorkSpaces
- Eliminar WorkSpaces

Para obtener más información sobre el uso de las aplicaciones cliente de WorkSpaces, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte Clientes de WorkSpaces y Soporte de dispositivos periféricos en la Guía del usuario de Amazon WorkSpaces.

Administración de usuarios de WorkSpace

Cada escritorio de WorkSpaces se asigna a un único usuario y no se puede compartir entre varios usuarios. De forma predeterminada, solo se permite un escritorio de WorkSpaces por usuario y directorio.

Contenido

Administrar usuarios de WorkSpaces

Como administrador de WorkSpaces, puede realizar las siguientes tareas para administrar los usuarios de WorkSpaces.

Edición de la información de usuario

Puede utilizar la consola WorkSpaces para editar la información de usuario de un WorkSpace.

> **Note**
>
> Esta característica solo está disponible si utiliza Microsoft AD administrado por AWS o AD sencillo. Si utiliza Microsoft Active Directory a través de Conector AD o una relación de confianza, puede administrar los usuarios y grupos utilizando el módulo de Active Directory.

Para editar la información de usuario

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione un usuario y elija Acciones, Editar usuarios.

4. Actualice First Name, Last Name, Email según sea necesario.
5. Elija Actualizar.

Adición o eliminación de usuarios

Puede crear usuarios desde la consola de Amazon WorkSpaces únicamente durante el proceso de inicio de WorkSpace, pero no puede eliminar usuarios a través de la consola de Amazon WorkSpaces. La mayoría de las tareas de administración de usuarios, incluida la administración de grupos de usuarios, deben realizarse a través del directorio.

Para añadir o eliminar usuarios y grupos

Para poder añadir, eliminar o administrar usuarios y grupos, debe hacerlo a través del directorio. Llevará a cabo la mayoría de las funciones administrativas del directorio WorkSpaces con herramientas de administración de directorios, como las herramientas de administración de Active Directory. Para obtener más información, consulte Configurar las herramientas de administración de Active Directory para WorkSpaces.

> **Important**
>
> Tenga en cuenta que antes de eliminar a un usuario, debe eliminar el escritorio de WorkSpaces asignado a ese usuario. Para obtener más información, consulte Eliminar WorkSpaces.

El proceso que utilice para administrar usuarios y grupos depende del tipo de directorio que utilice.

- Si utiliza AWS Managed Microsoft AD, consulte Administración de usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
- Si utiliza Simple AD, consulte Administración de usuarios y grupos en Simple AD en la Guía de administración de AWS Directory Service.
- Si utiliza Microsoft Active Directory a través de un conector AD o una relación de confianza, puede administrar usuarios y grupos utilizando el módulo de Active Directory.

Enviar un correo electrónico de invitación

Puede enviar un correo electrónico de invitación a un usuario manualmente si es necesario.

> **Note**
>
> Si utiliza el conector AD o un dominio de confianza, los correos electrónicos de invitación no se envían automáticamente a los usuarios, por lo que debe enviarlos manualmente. Los correos electrónicos de invitación tampoco se envían automáticamente si el usuario ya existe en Active Directory.

Para volver a enviar un correo electrónico de invitación

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. En la página WorkSpaces utilice el cuadro de búsqueda para buscar el usuario al que desea enviar una invitación y, a continuación, seleccione el WorkSpace correspondiente en los resultados de la búsqueda. Solo puede seleccionar un WorkSpace a la vez.
4. Seleccione Acciones, Invitar usuario.
5. En la página Invitar a los usuarios al WorkSpace, seleccione Enviar invitación.

Crear varios escritorios de WorkSpaces para un usuario

De forma predeterminada, solo puede crear un escritorio de WorkSpaces por usuario y directorio. Sin embargo, si es necesario, puede crear más de un escritorio de WorkSpaces para un usuario, dependiendo de la configuración del directorio.

- Si solo tiene un directorio para sus WorkSpaces, cree varios nombres de usuario para el usuario. Por ejemplo, un usuario llamado Mary Major puede tener como nombres de usuario mmajor1, mmajor2, etc. Cada nombre de usuario está asociado a un WorkSpace diferente en el mismo directorio, pero los WorkSpaces tienen el mismo código de registro, siempre y cuando los WorkSpaces se creen todos en el mismo directorio en la misma región de AWS.
- Si tiene varios directorios para su escritorio de WorkSpaces, cree los escritorios de WorkSpaces para el usuario en directorios distintos. Puede utilizar el mismo nombre de usuario en los directorios, o puede utilizar diferentes nombres de usuario en los directorios. Los escritorios de WorkSpaces tendrán códigos de registro diferentes.

> **Tip**
>
> Para poder localizar fácilmente todos los WorkSpaces creados para un usuario, utilice el mismo nombre de usuario base para cada WorkSpace.
> Por ejemplo, si tiene un usuario llamado Mary Major con el nombre de usuario de Active Directory mmajor, cree WorkSpaces para ella con nombres de usuario como mmajor, mmajor1, mmajor2, mmajor3, u otras variantes, como mmajor_windows o mmajor_linux. Si todos los WorkSpaces tienen el mismo nombre de usuario base inicial (mmajor), puedes ordenar el nombre de usuario en tu consola de WorkSpaces para agrupar todos los WorkSpaces de ese usuario.

> **Important**
>
> - Un usuario puede tener un WorkSpace con WSP y PCoIP siempre que los dos WorkSpaces estén ubicados en directorios independientes. El mismo usuario no puede tener un PCoIP y un WorkSpace con WSP en el mismo directorio.
> - Si está configurando varios WorkSpaces para usarlos con el redireccionamiento entre regiones, debe configurar los WorkSpaces en diferentes directorios de diferentes regiones de AWS y debe utilizar los mismos nombres de usuario en cada directorio. Para obtener más información sobre el redireccionamiento entre regiones, consulte Redirección entre regiones para Amazon WorkSpaces.

Para cambiar de un escritorio de WorkSpaces a otro, el usuario inicia sesión con el nombre de usuario y el código de registro asociados a un escritorio de WorkSpaces concreto. Si el usuario está utilizando la versión 3.0 o posterior de las aplicaciones cliente de WorkSpaces para Windows, macOS o Linux, puede asignar nombres diferentes a los escritorios de WorkSpaces yendo a Configuración, Administrar la información de inicio de sesión en la aplicación cliente.

Personalice la forma en que los usuarios inician sesión en sus WorkSpaces

Personalice el acceso de sus usuarios WorkSpaces mediante identificadores uniformes de recursos (URI) para ofrecer una experiencia de inicio de sesión simplificada que se integre con los flujos de

trabajo existentes en su organización. Por ejemplo, puede generar automáticamente URI de inicio de sesión que registren a sus usuarios mediante su WorkSpaces código de registro. Como resultado:

- Los usuarios pueden omitir el proceso de registro manual.
- Sus nombres de usuario se introducen automáticamente en la página de inicio de sesión del WorkSpaces cliente.
- Si en la organización se utiliza la autenticación multifactor (MFA), sus nombres de usuario y códigos MFA se introducen automáticamente en la página de inicio de sesión del cliente.

El acceso URI funciona tanto con códigos de registro basados en regiones (por ejemplo, `WSpdx+ABC12D`) como con códigos de registro basados en nombres de dominio completos (FQDN) (por ejemplo, `desktop.example.com`). Para obtener más información sobre la creación y el uso de códigos de registro basados en FQDN, consulte Redirección entre regiones para Amazon WorkSpaces.

Puede configurar el acceso mediante URI a WorkSpaces las aplicaciones cliente en los siguientes dispositivos compatibles:

- Equipos Windows
- Equipos macOS
- Ordenadores con Ubuntu Linux 18.04, 20.04 y 22.04
- iPads
- Dispositivos Android

Para usar los URI para acceder a sus dispositivos WorkSpaces, los usuarios primero deben instalar la aplicación cliente para su dispositivo abriendo https://clients.amazonworkspaces.com/ https://s3.us-iso-eastus-isob-east

El acceso a la URI se admite en los navegadores Firefox y Chrome en ordenadores Windows y macOS, en el navegador Firefox en ordenadores Ubuntu Linux 18.04, 20.04 y 22.04, y en los navegadores Internet Explorer y Microsoft Edge en ordenadores Windows. Para obtener más información sobre WorkSpaces los clientes, consulta WorkSpaces Clientes en la Guía del WorkSpaces usuario de Amazon.

> **Note**
>
> En los dispositivos Android, el acceso de URI solo funciona con el navegador Firefox, no con el navegador Google Chrome.

Para configurar el acceso mediante URI WorkSpaces, utilice cualquiera de los formatos de URI que se describen en la siguiente tabla.

> **Note**
>
> Si el componente de datos de su URI incluye cualquiera de los siguientes caracteres reservados, le recomendamos que utilice la codificación de porcentaje en el componente de datos para evitar la ambigüedad:
> `@ : / ? & =`
> Por ejemplo, si tiene nombres de usuario que incluyen alguno de estos caracteres, debe codificarlos porcentualmente en su URI. Para obtener más información, consulte Uniform Resource Identifier (URI): Generic Syntax.

Sintaxis admitida	Descripción
workspaces://	Abre la aplicación WorkSpaces cliente. (Nota: la aplicación cliente de Linux no permite utilizar el propio directorio workspaces://).
workspaces://@registrationcode	Registra un usuario mediante su código WorkSpaces de registro. También muestra la página de inicio de sesión del cliente.
workspaces://username@registrationcode	Registra un usuario mediante su código WorkSpaces de registro. También escribe automáticamente el nombre de usuario en el campo nombre de usuario de la página de inicio de sesión del cliente.
workspaces://username@registrationcode?MFACode=mfa	Registra un usuario mediante su código WorkSpaces de registro. También rellena automáticamente el nombre de usuario en el campo username (nombre de usuario) y el

Sintaxis admitida	Descripción
	código de multi-factor authentication (MFA) en el campo MFA code (Código MFA) de la página de inicio de sesión del cliente.
workspaces://@registrationcode?MFACode=mfa	Registra un usuario mediante su código WorkSpaces de registro. También rellena automáticamente el código de multi-factor authentication (MFA) en el campo MFA code (Código MFA) de la página de inicio de sesión del cliente.

> **Note**
>
> Si los usuarios abren un enlace URI cuando ya están conectados a un cliente WorkSpace de Windows, se abre una nueva WorkSpaces sesión y la WorkSpaces sesión original permanece abierta. Si los usuarios abren un enlace URI cuando están conectados a un cliente WorkSpace de macOS, iPad o Android, no se abre ninguna sesión nueva; solo permanece abierta la WorkSpaces sesión original.

Habilite las capacidades de WorkSpace administración de autoservicio para sus usuarios

En WorkSpaces, puede habilitar las capacidades de WorkSpace administración de autoservicio para que sus usuarios tengan más control sobre su experiencia. También puede reducir la carga de trabajo del personal de soporte de TI para WorkSpaces. Al habilitar las funciones de autoservicio, los usuarios pueden realizar una o más de las siguientes tareas directamente desde su WorkSpaces cliente:

- Almacene en caché sus credenciales en su cliente. Esto les permite volver a conectarse a ellos WorkSpace sin tener que volver a introducir sus credenciales.
- Reinicie (reinicie) sus. WorkSpace
- Aumente el tamaño de los volúmenes raíz y de usuario de sus WorkSpace.
- Cambie el tipo de procesamiento (paquete) de sus WorkSpace.
- Cambie el modo de ejecución de sus WorkSpace.

- Reconstruye sus WorkSpace.

Clientes compatibles

- Android, que se ejecuta en sistemas Android o Chrome OS compatibles con Android
- Linux
- macOS
- Windows

Para habilitar capacidades de gestión de autoservicio para sus usuarios

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija el directorio en el que desee habilitar las capacidades de administración de autoservicio.
4. Desplázate hacia abajo hasta Permisos de autoservicio y selecciona Editar. Active o desactive las siguientes opciones según sea necesario para determinar las tareas WorkSpace de administración que los usuarios pueden realizar desde su cliente:

    - Recordarme: los usuarios pueden elegir si almacenar en caché sus credenciales en su cliente seleccionando la casilla de verificación Recordarme o Mantenerme conectado en la pantalla de inicio de sesión. Las credenciales se almacenan en caché solo en RAM. Cuando los usuarios eligen almacenar sus credenciales en caché, pueden volver a conectarse a ellas WorkSpaces sin tener que volver a escribirlas. Para controlar el tiempo que los usuarios pueden almacenar en caché sus credenciales, consulte Establecer la duración máxima de un ticket de Kerberos.
    - Reiniciar WorkSpace desde el cliente: los usuarios pueden reiniciar (reiniciar) sus. WorkSpace Al reiniciar, se desconecta al usuario del suyo WorkSpace, se apaga y se reinicia. Esto no afecta a los datos de usuario, el sistema operativo y la configuración del sistema.
    - Aumente el tamaño del volumen: los usuarios pueden ampliar sus volúmenes raíz y de usuario WorkSpace hasta un tamaño específico sin ponerse en contacto con el soporte de TI. Los usuarios pueden aumentar el tamaño del volumen raíz (para Windows, la unidad C:; para Linux,/) hasta 175 GB y el tamaño del volumen de usuario (para Windows, la unidad D:; para Linux, /home) hasta 100 GB. WorkSpace Los volúmenes raíz y de usuario vienen agrupados en conjuntos que no se pueden cambiar. Los grupos disponibles son [Raíz (GB),

Usuario (GB)]: [80, 10], [80, 50], [80, 100], [de 175 a 2000, de 100 a 2000]. Para obtener más información, consulte Modificar un WorkSpace.

En el caso de las unidades recién creadas WorkSpace, los usuarios deben esperar 6 horas antes de poder aumentar el tamaño de estas unidades. Después de eso, solo podrán hacerlo una vez en un periodo de 6 horas. Mientras se está incrementando el tamaño del volumen, los usuarios pueden realizar la mayoría de las tareas en sus dispositivos WorkSpace. Las tareas que no pueden realizar son: cambiar su tipo de WorkSpace cómputo, cambiar su modo de WorkSpace ejecución, reiniciarlo o reconstruirlo. WorkSpace WorkSpace Cuando finalice el proceso, es WorkSpace necesario reiniciarlo para que los cambios surtan efecto. Este proceso puede tardar hasta una hora.

> **Note**
>
> Si los usuarios aumentan el tamaño del volumen en sus WorkSpace servidores, esto aumenta su tarifa de facturación. WorkSpace

- Cambiar el tipo de cómputo: los usuarios pueden cambiar de un tipo de cómputo a otro (paquetes). WorkSpace En el caso de un paquete recién creado WorkSpace, los usuarios deben esperar 6 horas antes de poder cambiar a un paquete diferente. Después de eso, pueden cambiar a un paquete más grande solo una vez en un periodo de 6 horas, o bien a un paquete más pequeño una vez en un periodo de 30 días. Cuando se está produciendo un cambio en el tipo de WorkSpace procesamiento, los usuarios se desconectan del suyo WorkSpace y no pueden usarlo ni cambiarlo WorkSpace. WorkSpace Se reinicia automáticamente durante el proceso de cambio de tipo de cómputo. Este proceso puede tardar hasta una hora.

  > **Note**
  >
  > Si los usuarios cambian su tipo de WorkSpace procesamiento, esto cambia la tarifa de facturación de sus usuarios. WorkSpace

- Cambiar el modo de funcionamiento: los usuarios pueden cambiar WorkSpace entre el modo de AutoStopfuncionamiento AlwaysOny el modo de funcionamiento. Para obtener más información, consulte Controlar el modo de ejecución de WorkSpaces.

> **Note**
>
> Si los usuarios cambian su modo de funcionamiento WorkSpace, esto cambia su tarifa de facturación WorkSpace.

- Reconstruir WorkSpace desde el cliente: los usuarios pueden reconstruir el sistema operativo de a WorkSpace a a su estado original. Cuando WorkSpace se reconstruye a, el volumen de usuario (unidad D: unidad) se vuelve a crear a partir de la última copia de seguridad. Como las copias de seguridad se completan cada 12 horas, los datos de los usuarios pueden tener una antigüedad máxima de 12 horas. En el caso de una nueva creación WorkSpace, los usuarios deben esperar 12 horas antes de poder volver a crear la suya WorkSpace. Cuando se está WorkSpace realizando una reconstrucción, los usuarios se desconectan de las WorkSpace suyas y no pueden utilizarlas ni realizar cambios en las suyas WorkSpace. Este proceso puede tardar hasta una hora.
- Cargas de registros de diagnóstico: los usuarios pueden cargar los archivos de registro del WorkSpaces cliente directamente WorkSpaces para solucionar problemas sin interrumpir el uso del cliente. WorkSpaces Si habilitas la carga de registros de diagnóstico para tus usuarios o dejas que los usuarios lo hagan ellos mismos, los archivos de registro se enviarán automáticamente. WorkSpaces Puedes activar la carga de los registros de diagnóstico antes o durante una sesión de WorkSpaces streaming.

5. Elija Guardar.

Habilitar la optimización de audio de Amazon Connect para sus usuarios

En la consola de administración de WorkSpaces, puede habilitar la optimización de audio del Panel de control de contactos (CCP) de Amazon Connect para sus flotas de WorkSpaces a fin de mejorar la seguridad y habilitar el audio con calidad nativa. Tras habilitar la optimización del audio del CCP, los puntos de conexión del cliente procesarán el audio del CCP, mientras que los usuarios de WorkSpaces pueden interactuar con el CCP desde sus WorkSpaces.

La optimización de audio del panel de control de contactos (CCP) de Amazon Connect funciona con:

- El cliente WorkSpaces para Windows.
- Amazon Linux y WorkSpaces para Windows.

- WorkSpaces que utilizan PCoIP o WSP.

Requisitos

- Debe estar configurado con Amazon Connect.
- Puede crear un CCP personalizado con la API de Amazon Connect Stream mediante la creación de un CCP sin medios para la señalización de llamadas. De esta forma, el contenido multimedia se maneja en el escritorio local utilizando el CCP estándar y la señalización y los controles de llamada se gestionan en la conexión remota con el CCP sin contenido multimedia. Para obtener más información sobre la API de Amazon Connect Streams, consulte el repositorio GitHub en https://github.com/aws/amazon-connect-streams. El CCP personalizado que cree es el CCP que utilizarán sus agentes de Amazon Connect en sus WorkSpaces.
- Debe tener un navegador web instalado en los puntos de conexión del cliente de WorkSpaces que sean compatibles con Amazon Connect. Para ver la lista de navegadores compatibles, consulte Navegadores compatibles con Amazon Connect.

> **Note**
>
> Si sus usuarios utilizan navegadores no compatibles, se les pedirá que descarguen uno compatible cuando intenten iniciar sesión en el CCP.

Habilitar la optimización de audio de Amazon Connect

Para habilitar la optimización de audio de Amazon Connect para sus usuarios:

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions, Update Details.
4. Despliegue la opción Optimización de audio de Amazon Connect.

> **Note**
>
> Antes de realizar la configuración con Amazon Connect, seleccione Actualizar para guardar los cambios no guardados realizados anteriormente en la consola de administración.

5. Seleccione Configurar Amazon Connect.
6. Introduzca un nombre para el panel de control de contactos (CCP) de Amazon Connect.

> **Note**
>
> El nombre que le dé a su CCP se utilizará en el menú de complementos de usuario. Elija un nombre que sea significativo para sus usuarios.

7. Introduzca la URL del panel de control de contactos de Amazon Connect generada por Amazon Connect. Consulte Proporcionar acceso al panel de control de contactos para obtener más información sobre cómo obtener la URL.
8. Elija Crear Amazon Connect.

Actualizar los detalles de optimización de audio de Amazon Connect del directorio

Para actualizar los detalles de optimización de audio de Amazon Connect del directorio:

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions, Update Details.
4. Despliegue la opción Optimización de audio de Amazon Connect.

> **Note**
>
> Antes de realizar la configuración con Amazon Connect, seleccione Actualizar para guardar los cambios no guardados realizados anteriormente en la consola de administración.

5. Seleccione Configurar Amazon Connect.

6. Elija Edit (Editar).
7. Seleccione el directorio y elija Actions, Update Details.
8. Actualice el nombre y la URL del panel de control de contactos de Amazon Connect.
9. Seleccione Save.

Eliminar los detalles de optimización de audio de Amazon Connect del directorio

Para eliminar los detalles de optimización de audio de Amazon Connect del directorio:

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions, Update Details.
4. Despliegue la opción Optimización de audio de Amazon Connect.

> **Note**
>
> Antes de realizar la configuración con Amazon Connect, seleccione Actualizar para guardar los cambios no guardados realizados anteriormente en la consola de administración.

5. Seleccione Configurar Amazon Connect.
6. Seleccione Eliminar Amazon Connect.

Para obtener más información, consulte la Guía de formación de agentes.

Habilitar las cargas de registros de diagnóstico

Para solucionar problemas con los WorkSpaces clientes, habilite la carga automática de registros de diagnóstico. Actualmente, esto es compatible con los clientes de Windows, macOS, Linux y Web Access.

> **Note**
>
> La función de carga de registros de diagnóstico del WorkSpaces cliente no está disponible actualmente en la región AWS GovCloud (EE. UU. Oeste).

Cargas de registros de diagnóstico

Con las cargas de registros de diagnóstico, puede cargar los archivos de registro del WorkSpaces cliente directamente WorkSpaces a para solucionar problemas sin interrumpir el uso del cliente. WorkSpaces Si habilita la carga de registros de diagnóstico para sus usuarios o permite que los usuarios lo hagan ellos mismos, los archivos de registro se enviarán automáticamente. WorkSpaces Puedes activar la carga de los registros de diagnóstico antes o durante una sesión de WorkSpaces streaming.

Para cargar automáticamente los registros de diagnóstico desde los dispositivos gestionados, instala un WorkSpaces cliente que admita la carga de diagnósticos. La carga de registros está habilitada de forma predeterminada. Puede modificar la configuración de cualquiera de las siguientes formas:

Opción 1: usar la consola AWS

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija el nombre del directorio para el que desea habilitar el registro de diagnóstico.
4. Desplácese hacia abajo hasta Permisos de autoservicio
5. Seleccione Ver detalles
6. Elija Editar.
7. Seleccione Cargas de registros de diagnóstico
8. Seleccione Guardar.

Opción 2: usar una llamada a la API

Puede editar la configuración del directorio para habilitar o deshabilitar el cliente de WorkSpaces Windows, macOS y Linux para que cargue los registros de diagnóstico automáticamente mediante una llamada a la API. Si está habilitada, cuando se produce un problema con el cliente, los registros se envían WorkSpaces sin la interacción del usuario. Para obtener más información, consulta la referencia WorkSpaces de la API.

También puede permitir que los usuarios elijan si desean habilitar las cargas de registros de diagnóstico automáticas después de instalar el cliente. Para obtener más información, consulte Aplicación cliente WorkSpaces Windows, aplicación cliente WorkSpaces macOS y Aplicación cliente WorkSpaces Linux.

> **Note**
>
> - Los registros de diagnóstico no contienen información confidencial. Puede deshabilitar las cargas de registros de diagnóstico automáticas a nivel de directorio o permitir que los usuarios deshabiliten estas características ellos mismos.
> - Para acceder a la función de carga de registros de diagnóstico, debe instalar las siguientes versiones de los WorkSpaces clientes:
>   - 5.4.0 o posterior del cliente de Windows
>   - 5.8.0 o posterior del cliente macOS
>   - 2023.1 del cliente Ubuntu 22.04
>   - 2023.1 del cliente Ubuntu 20.04
>   - También puede acceder a la función de carga del registro de diagnóstico con el cliente Web Access

Administre su WorkSpaces

Puede administrarlos WorkSpaces mediante la WorkSpaces consola.

Para realizar tareas de administración de directorios, consulte the section called “Configurar la administración del directorio”.

> **Note**
>
> - Asegúrese de actualizar los controladores de dependencia de la red, como los controladores ENA, NVMe y PV, en su WorkSpaces ordenador. Debe hacerlo al menos una vez cada 6 meses. Para obtener más información, consulte Instalar o actualizar el controlador Elastic Network Adapter (ENA) Controladores NVMe de AWS para instancias de Windows y Actualizar los controladores PV en instancias de Windows.
> - Asegúrese de actualizar periódicamente los agentes de EC2Config, EC2Launch y EC2Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada 6 meses. Para obtener más información, consulte Actualizar EC2Config y EC2Launch.

Contenido

- Reconstruir un WorkSpace
- Restaurar un espacio de trabajo
- Traiga su propia licencia (BYOL) de Microsoft 365
- Actualice Windows BYOL WorkSpaces
- Migrar un WorkSpace
- Eliminar WorkSpaces

Administre su Windows WorkSpaces

Puede usar los objetos de política de grupo (GPO) para aplicar la configuración y administrar Windows WorkSpaces o los usuarios que forman parte de su WorkSpaces directorio de Windows.

> **Note**
>
> Las instancias de Linux no cumplen la política de grupo. Para obtener información sobre la administración de Amazon Linux WorkSpaces, consulteAdministre su Amazon Linux WorkSpaces.

Le recomendamos que cree una unidad organizativa para sus objetos WorkSpaces informáticos y una unidad organizativa para sus objetos WorkSpaces de usuario.

Para utilizar la configuración de política de grupo específica de Amazon WorkSpaces, debe instalar la plantilla administrativa de política de grupo para el protocolo o los protocolos que utilice, ya sea PCoIP o WorkSpaces Streaming Protocol (WSP).

> **Warning**
>
> La configuración de la política de grupo puede afectar a la experiencia de los WorkSpace usuarios de la siguiente manera:
>
> - La implementación de un mensaje de inicio de sesión interactivo para mostrar un banner de inicio de sesión impide que los usuarios puedan acceder a sus mensajes. WorkSpaces El PCoIP no admite actualmente la configuración de la política de grupo de los mensajes de inicio de sesión interactivos. WorkSpaces El mensaje de inicio de sesión es compatible con WSP WorkSpaces y los usuarios deben volver a iniciar sesión después de aceptar el banner de inicio de sesión.

- Deshabilitar el almacenamiento extraíble a través de la configuración de la política de grupo provoca un error de inicio de sesión que hará que los usuarios inicien sesión en perfiles de usuario temporales sin acceso a la unidad D.
- Eliminar usuarios del grupo local de usuarios de escritorio remoto mediante la configuración de la política de grupo impide que esos usuarios puedan autenticarse a través de las aplicaciones cliente. WorkSpaces Para obtener más información acerca de esta configuración de directiva de grupo, consulte Permitir inicio de sesión a través de Servicios de Escritorio remoto en la documentación de Microsoft.
- Si elimina el grupo de usuarios integrado de la política de seguridad Permitir el inicio de sesión local, WorkSpaces los usuarios de PCoIP no podrán conectarse a él a WorkSpaces través de las WorkSpaces aplicaciones cliente. Su PCoIP WorkSpaces tampoco recibirá actualizaciones del software del agente de PCoIP. Las actualizaciones del agente de PCoIP pueden contener correcciones de seguridad y de otro tipo, o pueden habilitar nuevas funciones para usted. WorkSpaces Para obtener más información sobre cómo trabajar con esta política de seguridad, consulte Permitir el inicio de sesión local en la documentación de Microsoft.
- La configuración de la política de grupo se puede usar para restringir el acceso de unidad. Si configura la política de grupo para restringir el acceso a la unidad C o a la unidad D, los usuarios no podrán acceder a las suyas. WorkSpaces Para que no se produzca este problema, asegúrese de que sus usuarios pueden tener acceso a la unidad C y a la unidad D.
- La función de entrada de WorkSpaces audio requiere el acceso de inicio de sesión local dentro de la. WorkSpace La función de entrada de audio está habilitada de forma predeterminada en Windows. WorkSpaces Sin embargo, si tienes una configuración de política de grupo que restringe el inicio de sesión local de los usuarios WorkSpaces, la entrada de audio no funcionará en la tuya. WorkSpaces Si eliminas esa configuración de política de grupo, la función de entrada de audio se habilitará tras el siguiente reinicio del. WorkSpace Para obtener más información sobre la configuración de esta política de grupo, consulte Permitir el inicio de sesión local en la documentación de Microsoft.

  Para obtener más información acerca de cómo habilitar o deshabilitar el redireccionamiento de entrada de audio, consulte o Activar o desactivar el redireccionamiento de entrada de audio para PCoIP o Activar o desactivar el redireccionamiento de entrada de audio para WSP.
- Si utilizas una política de grupo para configurar el plan de energía de Windows en equilibrado o en modo de ahorro de energía, es posible que te WorkSpaces quedes

dormido cuando no estén funcionando. Recomendamos encarecidamente utilizar una política de grupo para configurar el plan de energía de Windows en un nivel de alto rendimiento. Para obtener más información, consulte Mi Windows WorkSpace entra en modo de suspensión cuando está inactivo.

- Algunas configuraciones de políticas de grupo obligan a los usuarios a cerrar sesión cuando se desconectan de una sesión. Todas las aplicaciones que los usuarios tengan abiertas WorkSpaces están cerradas.
- Actualmente, WSP WorkSpaces no admite la opción «Establecer un límite de tiempo para las sesiones de Servicios de Escritorio Remoto activas pero inactivas». Evite usarlo durante las sesiones de WSP, ya que provoca una desconexión incluso cuando hay actividad y la sesión no está inactiva.

Para obtener información sobre el uso de las herramientas de administración de Active Directory para trabajar con GPO, consulte Configurar las herramientas de administración de Active Directory para WorkSpaces.

Contenido

- Requisitos previos
- Cree la clave de registro en un host de Windows WorkSpaces
- Resolución de problemas

Instale los archivos de plantillas administrativas de políticas de grupo para el Protocolo de WorkSpaces transmisión (WSP)

Para usar la configuración de política de grupo específica del Protocolo de WorkSpaces transmisión (WSP), debe agregar la plantilla administrativa de la política de grupo `wsp.admx` y `wsp.adml` los archivos del WSP al almacén central del controlador de dominio de su directorio. WorkSpaces WorkSpaces Para obtener más información sobre cómo trabajar con archivos `.admx` y `.adml`, consulte Cómo crear y administrar el almacén central de plantillas administrativas de políticas de grupo en Windows.

En el siguiente procedimiento se describe cómo crear el almacén central y agregarle los archivos de plantilla administrativa. Realice el siguiente procedimiento en una instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su WorkSpaces directorio.

Para instalar la plantilla administrativa de política de grupo para WSP

1. Desde un sistema Windows en ejecución WorkSpace, haga una copia de los `wsp.adml` archivos `wsp.admx` y del `C:\Program Files\Amazon\WSP` directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra el Explorador de archivos de Windows y, en la barra de direcciones, introduzca el nombre de dominio completo (FQDN) de su organización, como. `\\example.com`
3. Abra la carpeta `sysvol`.
4. Abra la carpeta con el nombre *`FQDN`*.
5. Abra la carpeta `Policies`. Debería acceder a `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies`.
6. Si no existe, cree una carpeta llamada `PolicyDefinitions`.
7. Abra la carpeta `PolicyDefinitions`.
8. Copie el archivo `wsp.admx` en la carpeta `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions`.
9. Cree una carpeta denominada `en-US` dentro de la carpeta `PolicyDefinitions`.
10. Abra la carpeta `en-US`.

11. Copie el archivo `wsp.adml` en la carpeta `\\FQDN\sysvol\FQDN\Policies\PolicyDefinitions\en-US`.

Para comprobar que los archivos de plantilla administrativa están instalados correctamente

1. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
2. Amplíe el bosque (bosque: ***FQDN***).
3. Amplíe Dominios.
4. Amplíe su FQDN (por ejemplo, `example.com`).
5. Elija Objetos de política de grupo.
6. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, debe crear y vincular el GPO en el contenedor de dominios que tiene los privilegios delegados.
>
> Al crear un directorio con AWS Managed Microsoft AD, AWS Directory Service crea una unidad organizativa (OU) *yourdomainname* en la raíz del dominio. El nombre de esta OU se basa en el nombre NetBIOS que escribió cuando creó el directorio. Si no especificó un nombre NetBIOS, este será de forma predeterminada la primera parte del nombre de DNS del directorio (por ejemplo, en el caso de `corp.example.com`, el nombre NetBIOS sería `corp`).
>
> Para crear su GPO, en lugar de seleccionar la política de dominio predeterminada, seleccione la unidad organizativa *sunombrededominio* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí.
>
> Para obtener más información sobre la OU de *sunombrededominio*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

7. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.

8. Ahora puede usar este objeto de política de grupo de WSP para modificar la configuración de la política de grupo específica de WSP WorkSpaces .

Administre la configuración de la política de grupo para el Protocolo WorkSpaces de transmisión (WSP)

Utilice la configuración de la política de grupo para administrar las ventanas WorkSpaces que utilizan WSP.

Configurar la compatibilidad con impresoras para WSP

De forma predeterminada, WorkSpaces habilita la impresión remota básica, que ofrece capacidades de impresión limitadas porque utiliza un controlador de impresora genérico en el servidor para garantizar una impresión compatible.

La impresión remota avanzada para clientes de Windows (no disponible para WSP) le permite utilizar características específicas de su impresora, como la impresión a doble cara, pero necesita que se instale el controlador de impresora compatible en el lado del host.

La impresión remota se implementa como un canal virtual. La impresión remota no funciona si los canales virtuales están deshabilitados.

WorkSpacesEn Windows, puede usar la configuración de la política de grupo para configurar la compatibilidad con la impresora según sea necesario.

Para configurar la compatibilidad con impresoras

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.

7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la configuración de Configure remote printing.
10. En el cuadro de diálogo Configure remote printing (Configurar impresión remota), realice una de las acciones siguientes:
    - Para habilitar el redireccionamiento de impresoras locales, seleccione Activado y, a continuación, en Opciones de impresión, elija Básico. Para utilizar de forma automática la impresora predeterminada actual del ordenador del cliente, seleccione Establecer automáticamente la impresora predeterminada.
    - Para deshabilitar la impresión, seleccione Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Configure la redirección del portapapeles (copiar/pegar) para WSP

De forma predeterminada, WorkSpaces admite la redirección bidireccional del portapapeles (copiar/pegar). WorkSpacesEn Windows, puede usar la configuración de la política de grupo

para deshabilitar esta función o configurar la dirección en la que se permite la redirección del portapapeles.

Para configurar la redirección del portapapeles para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la configuración Configure clipboard redirection.
10. En el cuadro de diálogo Configurar el redireccionamiento del portapapeles, seleccione Activado o Desactivado.

    Si la opción Configurar el redireccionamiento del portapapeles está habilitada, aparecerán las siguientes opciones de redireccionamiento del portapapeles:

- Seleccione Copiar y pegar para permitir el redireccionamiento bidireccional de copiar y pegar en el portapapeles.
- Seleccione Copiar solo para que se puedan copiar datos del portapapeles del servidor únicamente al portapapeles del cliente.
- Seleccione Pegar solo para que se puedan pegar datos del portapapeles del servidor únicamente al portapapeles del cliente.

11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Limitación conocida

Con la redirección del portapapeles habilitada WorkSpace, si copia contenido de más de 890 KB de una aplicación de Microsoft Office, la aplicación podría ralentizarse o dejar de responder durante un máximo de 5 segundos.

Establezca el tiempo de espera de reanudación de la sesión para WSP

Cuando pierde la conectividad de red, la sesión de WorkSpaces cliente activa se desconecta. WorkSpaces las aplicaciones cliente para Windows y macOS intentan volver a conectar la sesión automáticamente si se restablece la conectividad de red en un período de tiempo determinado. El tiempo de espera predeterminado para WorkSpaces reanudar la sesión es de 20 minutos (1200 segundos), pero puede modificar ese valor si lo controla la configuración de la política de grupo de su dominio.

Para establecer el valor del tiempo de espera para reanudar la sesión automático

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.

2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar la reconexión automática.
10. En el cuadro de diálogo Activar/desactivar la reconexión automática, seleccione Activada y, a continuación, indique los segundos deseados en el campo Tiempo de espera de reconexión (segundos).
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activar o desactivar el redireccionamiento de entrada de audio para WSP

De forma predeterminada, WorkSpaces admite la redirección de datos desde una cámara local. Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitar o deshabilitar la redirección de entrada de vídeo para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar el redireccionamiento de entrada de vídeo.
10. En el cuadro de diálogo Activar/desactivar el redireccionamiento de entrada de vídeo, seleccione Activado o Desactivado.

11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activar o desactivar el redireccionamiento de entrada de audio para WSP

De forma predeterminada, WorkSpaces admite la redirección de datos desde un micrófono local. Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitar o deshabilitar la redirección de entrada de audio en Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***`FQDN`***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con

el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *sunombrededominio*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar el redireccionamiento de entrada de audio.
10. En el cuadro de diálogo Activar/desactivar el redireccionamiento de entrada de vídeo, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activar o desactivar el redireccionamiento de salida de audio para WSP

De forma predeterminada, WorkSpaces redirige los datos a un altavoz local. Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitar o deshabilitar la redirección de salida de audio en Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN. Por ejemplo, `example.com`.

6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *sunombrededominio* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *sunombrededominio*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar el redireccionamiento de salida de audio.
10. En el cuadro de diálogo Activar/desactivar el redireccionamiento de salida de audio, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

    - Reinicie el. WorkSpace En la WorkSpaces consola de Amazon, selecciona y WorkSpace, a continuación, selecciona Acciones > Reiniciar WorkSpaces.
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Desactivar el redireccionamiento de zona horaria para WSP

De forma predeterminada, la hora de un espacio de trabajo está configurada para reflejar la zona horaria del cliente que se utiliza para conectarse al WorkSpace. Este comportamiento se controla mediante el redireccionamiento de zona horaria. Es posible que desee desactivar el redireccionamiento de zona horaria por diversas razones: Por ejemplo:

- Su empresa quiere que todos los empleados trabajen en la misma zona horaria (aunque algunos empleados estén en otras zonas horarias).

- Ha programado tareas en una WorkSpace que están destinadas a ejecutarse a una hora determinada y en una zona horaria específica.
- Sus usuarios, que viajan mucho, desean mantener su WorkSpaces zona horaria única para mantener la coherencia y mantener sus preferencias personales.

Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para deshabilitar la redirección de zona horaria en Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar el redireccionamiento de zona horaria.

10. En el cuadro de diálogo Activar/desactivar el redireccionamiento de zona horaria, seleccione Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.
13. Configura la zona horaria en WorkSpaces la zona horaria deseada.

La zona horaria de ahora WorkSpaces es estática y ya no refleja la zona horaria de las máquinas cliente.

Establecer la configuración de seguridad de WSP

En el caso de WSP, los datos en tránsito se cifran mediante encriptación TLS 1.2. De forma predeterminada, se permiten todos los siguientes cifrados para el cifrado, y el cliente y el servidor negocian qué cifrado utilizar:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

WorkSpacesEn Windows, puede usar la configuración de la política de grupo para modificar el modo de seguridad TLS y agregar nuevos conjuntos de cifrado o bloquear determinados conjuntos de cifrado. Encontrará una explicación detallada de estos parámetros y de los conjuntos de cifrado compatibles en el cuadro de diálogo Configurar los ajustes de seguridad de la política de grupo.

Para configurar los ajustes de seguridad de WSP

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN. Por ejemplo, `example.com`.
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .
8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra Configurar los ajustes de seguridad.
10. En el cuadro de diálogo Configurar los ajustes de seguridad, seleccione Activado. Agregue los conjuntos de cifrado que desee permitir y elimine los conjuntos de cifrado que desee bloquear. Para obtener más información sobre estos ajustes, consulte las descripciones que aparecen en el cuadro de diálogo Configurar los ajustes de seguridad.
11. Seleccione Aceptar.

12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la WorkSpace política de grupo y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

    - Para reiniciar WorkSpace, en la WorkSpaces consola de Amazon, selecciona y, a continuación WorkSpace, selecciona Acciones, Reiniciar WorkSpaces.
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Configurar las extensiones para WSP

De forma predeterminada, la compatibilidad WorkSpaces con las extensiones está deshabilitada. Si es necesario, puede WorkSpace configurar sus extensiones de las siguientes maneras:

- Servidor y cliente: habilite las extensiones tanto para el servidor como para el cliente
- Solo servidor: habilite las extensiones solo para el servidor
- Solo cliente: habilite las extensiones solo para el cliente

WorkSpacesEn Windows, puede usar la configuración de la política de grupo para configurar el uso de extensiones.

Para configurar las extensiones para WSP

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***`FQDN`***).
4. Amplíe Dominios.
5. Amplíe su FQDN. Por ejemplo, `example.com`
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *sunombrededominio* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *sunombrededominio*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Configurar extensiones.
10. En el cuadro de diálogo Configurar extensiones, seleccione Activado y, a continuación, defina la opción de soporte que desee. Seleccione Solo cliente, Servidor y cliente o Solo servidor.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo para la WorkSpace sesión WorkSpace y después de reiniciarla. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

    - Reinicie el WorkSpace. En la WorkSpaces consola de Amazon, selecciona y WorkSpace, a continuación, selecciona Acciones, Reiniciar WorkSpaces.
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activar o desactivar el redireccionamiento de tarjeta inteligente para WSP

De forma predeterminada, Amazon no WorkSpaces está habilitado para admitir el uso de tarjetas inteligentes ni para la autenticación previa a la sesión ni para la autenticación durante la sesión. La autenticación previa a la sesión se refiere a la autenticación con tarjeta inteligente que se realiza mientras los usuarios inician sesión en su cuenta. WorkSpaces La autenticación durante la sesión se refiere al proceso que se realiza después de iniciar sesión.

Si es necesario, puede habilitar la autenticación previa y durante la sesión para Windows WorkSpaces mediante la configuración de la política de grupo. La autenticación previa a la sesión también debe habilitarse a través de la configuración del directorio de AD Connector mediante la

acción de la EnableClientAuthentication API o el enable-client-authentication AWS CLI comando. Para obtener más información, consulte Habilitación de la autenticación con tarjeta inteligente para Conector AD en la Guía de administración de AWS Directory Service .

> **Note**
>
> Para habilitar el uso de tarjetas inteligentes con Windows WorkSpaces, se requieren pasos adicionales. Para obtener más información, consulte Utilizar tarjetas inteligentes para la autenticación.

Para habilitar o deshabilitar la redirección de tarjetas inteligentes para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar el redireccionamiento de tarjetas inteligentes.
10. En el cuadro de diálogo Activar/desactivar el redireccionamiento de tarjetas inteligentes, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto una vez WorkSpace reiniciada la sesión. Para aplicar el cambio de política de grupo, reinicie WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, reinicie WorkSpaces).

Habilite o deshabilite la redirección WebAuthn (FIDO2) para WSP

De forma predeterminada, Amazon WorkSpaces habilita el uso de WebAuthn autenticadores para la autenticación durante la sesión. La autenticación durante la sesión se refiere a la WebAuthn autenticación que se realiza después de iniciar sesión y que es solicitada por las aplicaciones web que se ejecutan en la sesión.

Requisitos

WebAuthn La redirección (FIDO2) para WSP requiere lo siguiente:

- Agente host WSP, versión 2.0.0.1425 o superior
- WorkSpaces clientes:
  - Linux Ubuntu 22.04 2023.3 o superior
  - Windows 5.19.0 o superior
  - Cliente Mac 5.19.0 o superior
- Navegadores web instalados en los WorkSpaces que ejecuta la extensión de WebAuthn redireccionamiento Amazon DCV:
  - Google Chrome 116+
  - Microsoft Edge 116+

Habilitar o deshabilitar la redirección WebAuthn (FIDO2) para Windows WorkSpaces

Si es necesario, puede habilitar o deshabilitar la compatibilidad con la autenticación durante la sesión con WebAuthn autenticadores para Windows WorkSpaces mediante la configuración de la política

de grupo. Si habilita o no configura esta opción, se habilitará la WebAuthn redirección y los usuarios podrán utilizar los autenticadores locales del control remoto. WorkSpace

Cuando la función está habilitada, todas WebAuthn las solicitudes del navegador de la sesión se redirigen al cliente local. Los usuarios pueden usar Windows Hello o dispositivos de seguridad conectados localmente, como YubiKey otros autenticadores compatibles con FIDO2, para completar el proceso de autenticación.

Para habilitar o deshabilitar la redirección WebAuthn (FIDO2) para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la configuración de habilitar/deshabilitar WebAuthn la redirección.

10. En el cuadro de diálogo Activar/desactivar el WebAuthn redireccionamiento, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto una vez reiniciada la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. A continuación, selecciona Acciones, Reiniciar WorkSpaces).

Instalación de la extensión de WebAuthn redireccionamiento de Amazon DCV

Los usuarios deberán instalar la extensión de WebAuthn redireccionamiento Amazon DCV para utilizarla WebAuthn después de habilitar la función mediante una de las siguientes acciones:

- Se les pedirá a sus usuarios que habiliten la extensión de navegador en sus navegadores.

> **Note**
>
> Se trata de un mensaje del navegador que se solicita una sola vez. Sus usuarios recibirán la notificación cuando actualice la versión del agente WSP a la 2.0.0.1425 o superior. Si sus usuarios finales no necesitan la WebAuthn redirección, simplemente pueden eliminar la extensión del navegador. También puedes bloquear el mensaje de instalación de la extensión de WebAuthn redireccionamiento mediante la siguiente política de GPO.

- Puede forzar la instalación de la extensión de redireccionamiento para sus usuarios mediante la siguiente política de GPO. Si habilita la política de GPO, la extensión se instalará automáticamente cuando los usuarios inicien los navegadores compatibles con acceso a Internet.
- Los usuarios pueden instalar la extensión manualmente con los complementos de Microsoft Edge o la Chrome Web Store.

Administra e instala la extensión del navegador mediante la política de grupo

Puede instalar la extensión de WebAuthn redireccionamiento Amazon DCV mediante una política de grupo, ya sea de forma centralizada desde su dominio para los hosts de sesión que estén unidos a un dominio de Active Directory (AD) o mediante el editor de políticas de grupo local para cada host de sesión. Este proceso cambiará en función del navegador que utilice.

Para Microsoft Edge

1. Descargue e instale la plantilla administrativa de Microsoft Edge.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.
8. Elija la configuración del equipo, las plantillas administrativas, Microsoft Edge y las extensiones
9. Abra Configurar los ajustes de administración de extensiones y configúrelo en Habilitado.
10. En Configurar los ajustes de administración de extensiones, introduzca lo siguiente:

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo se aplica después de reiniciar la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. A continuación, selecciona Acciones, Reiniciar WorkSpaces).

> **Note**
>
> Puede bloquear la instalación de la extensión aplicando el siguiente ajuste de administración de la configuración:
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

Para Google Chrome

1. Descarga e instala la plantilla administrativa de Google Chrome. Para obtener más información, consulta Cómo configurar las políticas del navegador Chrome en los PC gestionados.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.
8. Elija la configuración del ordenador, las plantillas administrativas, Google Chrome y las extensiones
9. Abre Configurar los ajustes de administración de extensiones y configúralo como Habilitado.
10. En Configurar los ajustes de administración de extensiones, introduzca lo siguiente:

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo se aplica después de reiniciar la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. A continuación, selecciona Acciones, Reiniciar WorkSpaces).

> **Note**
>
> Puede bloquear la instalación de la extensión aplicando el siguiente ajuste de administración de la configuración:

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"blocked","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

Activar o desactivar la sesión de desconexión en el bloqueo de pantalla para WSP

Si es necesario, puede desconectar WorkSpaces las sesiones de los usuarios cuando se detecte la pantalla de bloqueo de Windows. Para volver a conectarse desde el WorkSpaces cliente, los usuarios pueden usar sus contraseñas o sus tarjetas inteligentes para autenticarse, en función del tipo de autenticación que tengan habilitado. WorkSpaces

Este ajuste de la política de grupo está deshabilitado de forma predeterminada. Si es necesario, puede habilitar la desconexión de la sesión cuando se detecte la pantalla de bloqueo de Windows para Windows WorkSpaces mediante la configuración de la política de grupo.

> **Note**
>
> - Esta configuración de política de grupo se aplica tanto a las sesiones autenticadas con contraseña como a las autenticadas con tarjeta inteligente.
> - Para habilitar el uso de tarjetas inteligentes con Windows WorkSpaces, se requieren pasos adicionales. Para obtener más información, consulte Utilizar tarjetas inteligentes para la autenticación.

Para habilitar o deshabilitar la sesión de desconexión mediante el bloqueo de pantalla para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.

5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Activar/desactivar la sesión de desconexión en el bloqueo de pantalla.
10. En el cuadro de diálogo Activar/desactivar la sesión de desconexión en el bloqueo de pantalla, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activa o desactiva el controlador de pantalla indirecta (IDD) para WSP

De forma predeterminada, WorkSpaces admite el uso del controlador de pantalla indirecta (IDD). Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitar o deshabilitar el controlador de pantalla indirecta (IDD) para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una instancia de administración de directorios WorkSpace o de Amazon Elastic Compute Cloud que esté unida a tu WorkSpaces directorio, abre la herramienta de administración de políticas de grupo (gpmc.msc).
3. Amplíe el bosque (forest:FQDN).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione la política de dominio predeterminada, abra el contexto haciendo clic con el botón derecho en el menú y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un directorio AWS administrado de Microsoft AD, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad `yourdomainname` organizativa (OU) o cualquier OU con ese nombre de dominio, abra el contexto haciendo clic con el botón derecho en el menú y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información acerca de la `yourdomainname` OU, consulte Qué se crea en la Guía de administración de AWS Directory Service.

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la configuración Habilitar el controlador de pantalla AWS indirecta.
10. En el cuadro de diálogo Habilitar el controlador de pantalla AWS indirecta, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

a. Reinicie el WorkSpace (en la WorkSpaces consola, seleccione y, a continuación WorkSpace, elija Acciones, reinicie WorkSpaces).

b. En el símbolo del sistema administrativo, introduzca `gpupdate /force`.

Configurar los ajustes de visualización para WSP

WorkSpaces permite configurar varios ajustes de visualización diferentes, como la velocidad de fotogramas máxima, la calidad de imagen mínima, la calidad de imagen máxima y la codificación YUV. Ajuste estos ajustes en función de la calidad de imagen, la capacidad de respuesta y la precisión del color que necesite.

De forma predeterminada, el valor máximo de velocidad de fotogramas es 25. El valor de velocidad de fotogramas máxima especifica el número máximo de fotogramas por segundo (fps) permitido. El valor 0 indica que no hay ningún límite.

De forma predeterminada, el valor mínimo de calidad de imagen es 30. La calidad de imagen mínima se puede optimizar para obtener la mejor capacidad de respuesta o la mejor calidad de imagen. Para obtener la mejor capacidad de respuesta, reduzca la calidad mínima. Para obtener la mejor calidad, aumente la calidad mínima.

- Los valores ideales para una mejor capacidad de respuesta están entre 30 y 90.
- Los valores ideales para una mejor capacidad de respuesta están entre 60 y 90.

De forma predeterminada, el valor mínimo de calidad de imagen es 80. La calidad de imagen máxima no afecta a la capacidad de respuesta ni a la calidad de la imagen, pero establece un máximo para limitar el uso de la red.

De forma predeterminada, la codificación de la imagen está establecida en YUV420. Al seleccionar Activar la codificación YUV444, se activa la codificación YUV444 para obtener una alta precisión de color.

WorkSpacesEn Windows, puede usar la configuración de la política de grupo para configurar los valores de velocidad de fotogramas máxima, calidad de imagen mínima y calidad de imagen máxima.

Para configurar los ajustes de pantalla de Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .
8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Configurar los ajustes de visualización.
10. En el cuadro de diálogo Configurar los ajustes de visualización, seleccione Activado y, a continuación, indique los valores deseados en los campos Velocidad de fotogramas máxima (fps), Calidad de imagen mínima y Calidad de imagen máxima.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo para la WorkSpace sesión WorkSpace y después de

reiniciarla. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

- Reinicia la WorkSpace WorkSpaces consola de Amazon, selecciona y, a continuación WorkSpace, selecciona Acciones, Reiniciar WorkSpaces
- En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Habilite o deshabilite VSync para el controlador AWS virtual de solo pantalla para WSP

De forma predeterminada, WorkSpaces admite el uso de la función VSync para el controlador de solo pantalla virtual. AWS Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitar o deshabilitar VSync para Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. En una instancia de administración de directorios WorkSpace o de Amazon Elastic Compute Cloud que esté unida a tu WorkSpaces directorio, abre la herramienta de administración de políticas de grupo (gpmc.msc).
3. Amplíe el bosque (forest:FQDN).
4. Amplíe Dominios.
5. Amplíe su FQDN (por ejemplo, `example.com`).
6. Elija Objetos de política de grupo.
7. Seleccione la política de dominio predeterminada, abra el contexto haciendo clic con el botón derecho en el menú y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un directorio AWS administrado de Microsoft AD, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, elija la unidad `yourdomainname` organizativa (OU) o cualquier OU que esté bajo ese nombre de dominio, abra el contexto haciendo clic con el botón derecho del ratón en el menú y seleccione Crear un GPO en este dominio y vincularlo aquí. Para obtener

más información acerca de la `yourdomainname` OU, consulte Qué se crea en la Guía de administración de AWS Directory Service.

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la función Habilitar VSync de la configuración del controlador de pantalla AWS virtual únicamente.
10. En la función Habilitar VSync del cuadro de diálogo del controlador de pantalla AWS virtual únicamente, seleccione Activado o Desactivado.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios en la política de grupo, haga lo siguiente:

    a. Reinicie el WorkSpace mediante una de las siguientes acciones:

        i. Opción 1: en la WorkSpaces consola, selecciona la WorkSpace que deseas reiniciar. Luego, elige Acciones, Reiniciar WorkSpaces.

        ii. Opción 2: En una línea de comandos administrativa, introduzcagpupdate `/force`.

    b. Vuelva a conectarse WorkSpace al para aplicar la configuración.

    c. Vuelva a reiniciar el espacio de trabajo.

Configure la verbosidad del registro para WSP

De forma predeterminada, el nivel de detalle del registro de WSP WorkSpaces está establecido en Información. Puede configurar los niveles de registro en niveles de verbosidad que vayan desde el menos detallado hasta el más detallado, como se detalla aquí:

- Error: menos detallado
- Advertencia
- Información: predeterminado
- Depuración: más detallado

WorkSpacesEn Windows, puede usar la configuración de la política de grupo para configurar los niveles de verbosidad del registro.

Para configurar los niveles de verbosidad de los registros en Windows WorkSpaces

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para WSP esté instalada en el almacén central del controlador de dominio de su directorio. WorkSpaces
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
3. Amplíe el bosque (bosque: ***FQDN***).
4. Amplíe Dominios.
5. Amplíe su FQDN. Por ejemplo, `example.com`.
6. Elija Objetos de política de grupo.
7. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

   > **Note**
   >
   > Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí. Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

8. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y WSP.
9. Abra la opción Configurar la verbosidad del registro.
10. En el cuadro de diálogo Configurar la verbosidad del registro, seleccione Habilitado y, a continuación, establezca el nivel de verbosidad del registro en depuración, error, información o advertencia.
11. Seleccione Aceptar.
12. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo para la WorkSpace sesión WorkSpace y después de

reiniciarla. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

- Reinicie el WorkSpace. En la WorkSpaces consola de Amazon, selecciona y WorkSpace, a continuación, selecciona Acciones, Reiniciar WorkSpaces.
- En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Instalación de la plantilla administrativa de la política de grupo para PCoIP

Para utilizar la configuración de política de grupo específica de Amazon WorkSpaces cuando utilice el protocolo PCoIP, debe añadir la plantilla administrativa de política de grupo adecuada a la versión del agente de PCoIP (de 32 o 64 bits) que se utilice para su. WorkSpaces

> **Note**
>
> Si tiene una combinación de agentes de WorkSpaces 32 y 64 bits, puede usar las plantillas administrativas de políticas de grupo para los agentes de 32 bits y la configuración de la política de grupo se aplicará a los agentes de 32 y 64 bits. Cuando todos usen el agente de 64 bits, pueden cambiar a la plantilla administrativa para los agentes de 64 bits. WorkSpaces

Para determinar si WorkSpaces tiene el agente de 32 bits o el agente de 64 bits

1. Inicie sesión en un WorkSpace administrador de tareas y ábralo seleccionando Ver, Enviar Ctrl + Alt + Eliminar o haciendo clic con el botón derecho en la barra de tareas y seleccionando Administrador de tareas.
2. En el Administrador de tareas, vaya a la pestaña Detalles, haga clic con el botón derecho en los encabezados de las columnas y elija Seleccionar columnas.
3. En el cuadro de diálogo Seleccionar columnas, seleccione Plataforma y, a continuación, pulse Aceptar.
4. En la pestaña Detalles, busque `pcoip_agent.exe` y compruebe su valor en la columna Plataforma para determinar si el agente de PCoIP es de 32 o 64 bits. (Es posible que vea una combinación de WorkSpaces componentes de 32 y 64 bits; esto es normal).

Instalación de la plantilla administrativa de la política de grupo para PCoIP (32 bits)

Para usar la configuración de política de grupo específica para WorkSpaces el uso del protocolo PCoIP con el agente PCoIP de 32 bits, debe instalar la plantilla administrativa de política de grupo para PCoIP. Realice el siguiente procedimiento en una instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su directorio.

Para obtener más información sobre cómo trabajar con archivos.adm, consulte Recomendaciones para administrar los archivos de plantilla administrativa (.adm) de directiva de grupo en la documentación de Microsoft.

Para instalar la plantilla administrativa de la política de grupo para PCoIP

1. Desde un sistema Windows en ejecución WorkSpace, haga una copia del `pcoip.adm` archivo en el `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` directorio.
2. En una instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y navegue hasta la unidad organizativa de su dominio que contiene las cuentas de su WorkSpaces máquina.
3. Abra el menú contextual (haga clic con el botón derecho) de la unidad organizativa de la cuenta de la máquina y elija Create a GPO in this domain, and link it here.
4. En el cuadro de diálogo Nuevo GPO, introduzca un nombre descriptivo para el GPO, como políticas de WorkSpaces máquina, y deje el GPO inicial de origen establecido en (ninguno). Seleccione Aceptar.
5. Abra el menú contextual (con el botón derecho del ratón) del nuevo GPO y elija Editar.
6. En el editor de administración de políticas de grupo, elija Computer Configuration, Policies y Administrative Templates. Elija Action, Add/Remove Templates en el menú principal.
7. En el cuadro de diálogo Add/Remove Templates, elija Add, seleccione el archivo `pcoip.adm` copiado previamente y elija Open, Close.
8. Cierre el editor de administración de políticas de grupo. Ahora puede usar este GPO para modificar la configuración de la política de grupo específica de. WorkSpaces

Para comprobar que el archivo de plantilla administrativa está instalado correctamente

1. En una instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo

(gpmc.msc) y navegue hasta el WorkSpaces GPO de las cuentas de su WorkSpaces máquina y selecciónelo. Elija Action, Edit en el menú principal.

2. En el editor de administración de políticas de grupo, elija Computer Configuration, Policies, Administrative Templates, Classic Administrative Templates y PCoIP Session Variables.
3. Ahora puede utilizar este objeto de política de grupo de variables de sesión de PCoIP para modificar la configuración de política de grupo específica de Amazon WorkSpaces cuando utiliza PCoIP.

> **Note**
>
> Para permitir que el usuario pueda anular la configuración, seleccione Valores predeterminados de administración anulables; para no permitirlo, seleccione Valores predeterminados de administración no anulables.

Instalación de la plantilla administrativa de la política de grupo para PCoIP (64 bits)

Para utilizar la configuración de política de grupo específica del protocolo PCoIP, debe añadir la plantilla administrativa de la política de grupo `PCoIP.admx` y los `PCoIP.adml` archivos de PCoIP al almacén central del controlador de dominio de su directorio. WorkSpaces WorkSpaces Para obtener más información sobre cómo trabajar con archivos `.admx` y `.adml`, consulte Cómo crear y administrar el almacén central de plantillas administrativas de políticas de grupo en Windows.

En el siguiente procedimiento se describe cómo crear el almacén central y agregarle los archivos de plantilla administrativa. Realice el siguiente procedimiento en una instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su WorkSpaces directorio.

Para instalar los archivos de la plantilla administrativa de la política de grupo para PCoIP

1. Desde un sistema Windows en ejecución WorkSpace, haga una copia de los `PCoIP.adml` archivos `PCoIP.admx` y del `C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions` directorio. El archivo `PCoIP.adml` se encuentra en la subcarpeta `en-US` de ese directorio.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra el Explorador de archivos de Windows y, en la barra de direcciones, introduzca el nombre de dominio completo (FQDN) de su organización, como. `\ \example.com`
3. Abra la carpeta `sysvol`.

4. Abra la carpeta con el nombre *FQDN*.
5. Abra la carpeta `Policies`. Debería acceder a `\\FQDN\sysvol\FQDN\Policies`.
6. Si no existe, cree una carpeta llamada `PolicyDefinitions`.
7. Abra la carpeta `PolicyDefinitions`.
8. Copie el archivo `PCoIP.admx` en la carpeta `\\FQDN\sysvol\FQDN\Policies\PolicyDefinitions`.
9. Cree una carpeta denominada `en-US` dentro de la carpeta `PolicyDefinitions`.
10. Abra la carpeta `en-US`.
11. Copie el archivo `PCoIP.adml` en la carpeta `\\FQDN\sysvol\FQDN\Policies\PolicyDefinitions\en-US`.

Para comprobar que los archivos de plantilla administrativa están instalados correctamente

1. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
2. Amplíe el bosque (bosque: ***FQDN***).
3. Amplíe Dominios.
4. Amplíe su FQDN (por ejemplo, `example.com`).
5. Elija Objetos de política de grupo.
6. Seleccione Política de dominio predeterminada, abra el menú contextual (haga clic con el botón derecho) y elija Editar.

> **Note**
>
> Si el dominio que respalda WorkSpaces es un AWS Managed Microsoft AD directorio, no puede usar la política de dominio predeterminada para crear su GPO. En su lugar, debe crear y vincular el GPO en el contenedor de dominios que tiene los privilegios delegados.
>
> Al crear un directorio con AWS Managed Microsoft AD, AWS Directory Service crea una unidad organizativa (OU) *yourdomainname* en la raíz del dominio. El nombre de esta OU se basa en el nombre NetBIOS que escribió cuando creó el directorio. Si no especificó un nombre NetBIOS, este será de forma predeterminada la primera parte

del nombre de DNS del directorio (por ejemplo, en el caso de `corp.example.com`, el nombre NetBIOS sería `corp`).
Para crear su GPO, en lugar de seleccionar la política de dominio predeterminada, seleccione la unidad organizativa *`sunombrededominio`* (o cualquier unidad organizativa incluida en esa unidad organizativa), abra el menú contextual (haga clic con el botón derecho) y elija Crear un GPO en este dominio y vincularlo aquí.
Para obtener más información sobre la OU de *`sunombrededominio`*, consulte Qué se crea en la Guía de administración de AWS Directory Service .

7. En el editor de administración de políticas de grupo, elija Computer Configuration, Policies, Administrative Templates y PCoIP Session Variables.
8. Ahora puede usar este objeto de política de grupo de variables de sesión de PCoIP para modificar la configuración de la política de grupo específica al WorkSpaces usar PCoIP.

> **Note**
>
> Para permitir que el usuario pueda anular la configuración, seleccione Valores predeterminados de administración anulables; para no permitirlo, seleccione Valores predeterminados de administración no anulables.

Administre la configuración de políticas de grupo para PCoIP

Utilice la configuración de la política de grupo para administrar las ventanas WorkSpaces que utilizan PCoIP.

Configurar la compatibilidad con impresoras para PCoIP

De forma predeterminada, WorkSpaces habilita la impresión remota básica, que ofrece capacidades de impresión limitadas porque utiliza un controlador de impresora genérico en el servidor para garantizar una impresión compatible.

La impresión remota avanzada para clientes de Windows le permite utilizar características específicas de su impresora, como la impresión a doble cara, pero necesita que se instale el controlador de impresora compatible en el lado del host.

La impresión remota se implementa como un canal virtual. La impresión remota no funciona si los canales virtuales están deshabilitados.

WorkSpacesEn Windows, puede usar la configuración de la política de grupo para configurar la compatibilidad con la impresora según sea necesario.

Para configurar la compatibilidad con impresoras

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la configuración de Configure remote printing.
4. En el cuadro de diálogo Configure remote printing (Configurar impresión remota), realice una de las acciones siguientes:
   - Para habilitar la impresión remota avanzada, seleccione Enabled (Habilitada) y, a continuación, en Options (Opciones), Configure remote printing (Configurar impresión remota), seleccione Basic and Advanced printing for Windows clients (Impresión básica y avanzada para clientes de Windows). Para utilizar de forma automática la impresora predeterminada actual del ordenador del cliente, seleccione Automatically set default printer (Establecer automáticamente la impresora predeterminada).
   - Para deshabilitar la impresión, seleccione Enabled (Habilitada) y, a continuación, en Options (Opciones), Configure remote printing (Configurar impresión remota), elija Printing disabled (Impresión deshabilitada).
5. Seleccione Aceptar.
6. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo de la sesión WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

De forma predeterminada, el redireccionamiento automático a la impresora local está deshabilitado. Puedes usar la configuración de la política de grupo para habilitar esta función, de modo que tu

impresora local esté configurada como la impresora predeterminada cada vez que te conectes a la tuya WorkSpace.

> **Note**
>
> La redirección de impresoras locales no está disponible para Amazon Linux. WorkSpaces

Para habilitar el redireccionamiento automático a la impresora local

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la configuración de Configure remote printing.
4. Seleccione Activado y, a continuación, en Opciones, Configurar impresión remota, elija una de las siguientes opciones:
   - Impresión básica y avanzada para clientes de Windows
   - Impresión básica
5. Seleccione Establecer automáticamente la impresora predeterminada y, a continuación, elija Aceptar.
6. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo de la sesión WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activa o desactiva la redirección del portapapeles (copiar/pegar) para PCoIP

De forma predeterminada, admite la redirección del portapapeles. WorkSpaces Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitar o deshabilitar el redireccionamiento del portapapeles

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la configuración Configure clipboard redirection.
4. En el cuadro de diálogo Configure clipboard redirection (Configurar redirección del portapapeles), elija Enabled (Habilitado) y, a continuación, elija una de las siguientes opciones de configuración para determinar la dirección en la que se permite el redireccionamiento al portapapeles. Elija OK (Aceptar) cuando haya terminado.

   - Deshabilitado en ambas direcciones
   - El agente está habilitado solo para el cliente (WorkSpace para el ordenador local)
   - Habilitado solo entre el cliente y el agente (desde el equipo local WorkSpace)
   - Habilitado en ambas direcciones
5. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Limitación conocida

Con la redirección del portapapeles habilitada WorkSpace, si copia contenido de más de 890 KB de una aplicación de Microsoft Office, la aplicación podría ralentizarse o dejar de responder durante un máximo de 5 segundos.

Establezca el tiempo de espera de reanudación de la sesión para PCoIP

Cuando pierde la conectividad de red, la sesión de WorkSpaces cliente activa se desconecta. WorkSpaces las aplicaciones cliente para Windows y macOS intentan volver a conectar la sesión automáticamente si se restablece la conectividad de red en un período de tiempo determinado. El tiempo de espera predeterminado para WorkSpaces reanudar la sesión es de 20 minutos, pero puede modificar ese valor si lo controla la configuración de la política de grupo de su dominio.

Para establecer el valor del tiempo de espera para reanudar la sesión automático

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la configuración Configure Session Automatic Reconnection Policy.
4. En el cuadro de diálogo Configure Session Automatic Reconnection Policy, elija Enabled, establezca la opción Configure Session Automatic Reconnection Policy en el tiempo de espera deseado, en minutos, y elija Aceptar.
5. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo de la sesión WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Activar o desactivar el redireccionamiento de entrada de audio para PCoIP

De forma predeterminada, Amazon WorkSpaces admite la redirección de datos desde un micrófono local. Si es necesario para Windows WorkSpaces, puedes usar la configuración de la política de grupo para deshabilitar esta función.

> **Note**
>
> Si tienes una configuración de política de grupo que restringe el inicio de sesión local de los usuarios WorkSpaces, la entrada de audio no funcionará en la tuya. WorkSpaces Si eliminas esa configuración de política de grupo, la función de entrada de audio se habilitará tras el siguiente reinicio del. WorkSpace Para obtener más información sobre la configuración de esta política de grupo, consulte Permitir el inicio de sesión local en la documentación de Microsoft.

Para habilitar o deshabilitar el redireccionamiento de entrada de audio

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la opción Activar/desactivar el audio en la sesión de PCoIP.
4. En el cuadro de diálogo Activar/desactivar el audio en la sesión PCoIP, seleccione Activado o Desactivado.
5. Seleccione Aceptar.
6. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo de la sesión WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Deshabilitar el redireccionamiento de zona horaria para PCoIP

De forma predeterminada, la hora de un espacio de trabajo está configurada para reflejar la zona horaria del cliente que se utiliza para conectarse al WorkSpace. Este comportamiento se

controla mediante el redireccionamiento de zona horaria. Es posible que desee desactivar el redireccionamiento de zona horaria por diversas razones:

- Su empresa quiere que todos los empleados trabajen en la misma zona horaria (aunque algunos empleados estén en otras zonas horarias).
- Ha programado tareas en una WorkSpace que están destinadas a ejecutarse a una hora determinada y en una zona horaria específica.
- Sus usuarios, que viajan mucho, desean mantener su WorkSpaces zona horaria única para mantener la coherencia y mantener sus preferencias personales.

Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para deshabilitar el redireccionamiento de zona horaria

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la opción Configure clipboard redirection.
4. En el cuadro de diálogo Configurar el redireccionamiento de zonas horarias, seleccione Desactivado.
5. Seleccione Aceptar.
6. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo de la sesión WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.
7. Configura la zona horaria en WorkSpaces la zona horaria deseada.

La zona horaria de ahora WorkSpaces es estática y ya no refleja la zona horaria de las máquinas cliente.

Configurar opciones de seguridad de PCoIP

En el caso de los PCoIP, los datos en tránsito se cifran mediante encriptación TLS 1.2 y firma de solicitud SigV4. El protocolo PCOIP utiliza tráfico UDP cifrado, con cifrado AES, para la transmisión de píxeles. La conexión de streaming, que utiliza el puerto 4172 (TCP y UDP), se cifra mediante los cifrados AES-128 y AES-256, pero el cifrado predeterminado es de 128 bits. Puede cambiar este valor predeterminado a 256 bits mediante la configuración de política de grupo Configurar los ajustes de seguridad de PCoIP.

También puede usar esta configuración de política de grupo para modificar el modo de seguridad TLS y bloquear determinados conjuntos de cifrado. Encontrará una explicación detallada de estos parámetros y de los conjuntos de cifrado compatibles en la sección Configurar los ajustes de seguridad de PCoIP .

Para configurar los ajustes de seguridad de PCoIP

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra el menú Configurar parámetros de seguridad PCoIP.
4. En el cuadro de diálogo Configurar los ajustes de seguridad del PCoIP, seleccione Activado. Para establecer el cifrado predeterminado para el tráfico de streaming en 256 bits, acceda a la opción PCoIP Data Encryption Ciphers, y seleccione AES-256-GCM only.
5. (Opcional) Ajuste la configuración del Modo de seguridad TLS y, a continuación, enumere los conjuntos de cifrado que desee bloquear. Para obtener más información sobre estos ajustes, consulte las descripciones que aparecen en el cuadro de diálogo Configurar los ajustes de seguridad del PCoIP.
6. Seleccione Aceptar.
7. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo de la sesión WorkSpace y después de que se reinicie

la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

- Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
- En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Habilita la redirección USB para YubiKey U2F

> **Note**
>
> WorkSpaces Actualmente, Amazon solo admite la redirección USB para YubiKey U2F. Es posible que se redirijan otros tipos de dispositivos USB, pero no son compatibles y es posible que no funcionen correctamente.

Para habilitar la redirección USB para U2F YubiKey

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCoIP (64 bits) más reciente.
2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Abra la opción Activar/desactivar USB en la sesión de PCoIP.
4. Seleccione Habilitada y, a continuación, elija OK.
5. Abra la opción configuración de reglas de dispositivos permitidos y no permitidos de PCoIP USB.
6. Seleccione Habilitado y, en Introducir la tabla de autorización USB (máximo diez reglas), configure las reglas de la lista de dispositivos USB permitidos.

    - Regla de autorización: 110500407 Este valor es una combinación de un ID de proveedor (VID) y un ID de producto (PID). El formato de una combinación VID/PID es 1xxxxyyyy, donde xxxx es el VID en formato hexadecimal e yyyy es el PID en formato hexadecimal. Para este ejemplo, 1050 es el VID, y 0407 es el PID. Para obtener más valores de YubiKey USB, consulte Valores de ID de YubiKey USB.

7. En Introducir la tabla de autorización USB (máximo diez reglas), configure las reglas de la lista de bloqueo de dispositivos USB.

   - Para Regla de desautorización, establezca una cadena vacía. Esto significa que solo se permiten los dispositivos USB de la lista de autorización.

   > **Note**
   >
   > Puede definir un máximo de 10 reglas de autorización USB y un máximo de 10 reglas de desautorización USB. Utilice el carácter de barra vertical (|) para separar varias reglas. Para obtener información detallada sobre las reglas de autorización/no autorización, consulte Agente Teradici PCoIP Standard para Windows..

8. Seleccione Aceptar.
9. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

   - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Una vez que la configuración surta efecto, todos los dispositivos USB compatibles se pueden redirigir a, a WorkSpaces menos que se establezcan restricciones mediante la configuración de las reglas de los dispositivos USB.

Establecer la duración máxima de un ticket de Kerberos

Si no ha desactivado la función Recordarme de Windows WorkSpaces, WorkSpace los usuarios pueden utilizar las casillas Recordarme o Mantener la sesión iniciada en su aplicación WorkSpaces cliente para guardar sus credenciales. Esta función permite a los usuarios conectarse fácilmente a ella WorkSpaces mientras la aplicación cliente sigue ejecutándose. Como máximo, las credenciales se guardarán en caché de forma segura durante el período de vida máximo de los tickets de Kerberos.

Si WorkSpace utiliza un directorio AD Connector, puede modificar la duración máxima de los tickets de Kerberos para sus WorkSpaces usuarios mediante la política de grupo siguiendo los pasos de Duración máxima de un ticket de usuario en la documentación de Microsoft Windows.

Para habilitar o deshabilitar la función Remember Me (Recordarme) consulte Habilite las capacidades de WorkSpace administración de autoservicio para sus usuarios.

Configurar los ajustes del servidor proxy del dispositivo para acceder a Internet

De forma predeterminada, las aplicaciones WorkSpaces cliente utilizan el servidor proxy que se especifica en la configuración del sistema operativo del dispositivo para el tráfico HTTPS (puerto 443). Las aplicaciones WorkSpaces cliente de Amazon utilizan el puerto HTTPS para las actualizaciones, el registro y la autenticación.

> **Note**
>
> No se admiten los servidores proxy que requieren autenticación con credenciales de inicio de sesión.

Puede configurar los ajustes del servidor proxy del dispositivo para su Windows WorkSpaces mediante la política de grupo siguiendo los pasos que se indican en Configurar el proxy del dispositivo y los ajustes de conectividad a Internet en la documentación de Microsoft.

Para obtener más información sobre la configuración del proxy en la aplicación cliente de WorkSpaces Windows, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Para obtener más información sobre cómo configurar los ajustes del proxy en la aplicación cliente de WorkSpaces macOS, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Para obtener más información sobre cómo configurar los ajustes del proxy en la aplicación cliente WorkSpaces Web Access, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Cómo utilizar el proxy del tráfico de escritorio

En el caso de PCoIP WorkSpaces, las aplicaciones cliente de escritorio no admiten el uso de un servidor proxy ni el descifrado ni la inspección mediante TLS del tráfico del puerto 4172 en UDP (para el tráfico de escritorio). Necesitan una conexión directa a los puertos 4172.

Para WSP WorkSpaces, la aplicación cliente WorkSpaces Windows (versión 5.1 y superior) y la aplicación cliente macOS (versión 5.4 y superior) admiten el uso de servidores proxy HTTP para el tráfico TCP del puerto 4195. No se admiten el descifrado ni la inspección por TLS.

WSP no es compatible con el uso de proxy para el tráfico de escritorios a través de UDP. Solo las aplicaciones cliente de escritorio de WorkSpaces Windows y macOS y el acceso web WSP admiten el uso de proxy para el tráfico TCP.

> **Note**
>
> Si opta por utilizar un servidor proxy, las llamadas a la API que la aplicación cliente realiza a los WorkSpaces servicios también se envían mediante proxy. Tanto las llamadas a la API como el tráfico de escritorio deben pasar por el mismo servidor proxy.

Recomendación sobre el uso de servidores proxy

No recomendamos el uso de un servidor proxy con el tráfico de WorkSpaces escritorio.

El tráfico WorkSpaces de escritorio de Amazon ya está cifrado, por lo que los proxies no mejoran la seguridad. Un proxy representa un salto adicional en la ruta de la red que, al introducir latencia, podría afectar a la calidad de la transmisión. Los proxies también podrían reducir el rendimiento si un proxy no tiene el tamaño adecuado para gestionar el tráfico de streaming de escritorio. Además, la mayoría de los proxies no están diseñados para soportar conexiones de larga duración WebSocket (TCP) y pueden afectar a la calidad y estabilidad de la transmisión.

Si debe usar un proxy, ubique su servidor proxy lo más cerca posible del WorkSpace cliente, preferiblemente en la misma red, para evitar añadir latencia a la red, lo que podría afectar negativamente a la calidad y la capacidad de respuesta de la transmisión.

Habilite la compatibilidad con el complemento multimedia Amazon WorkSpaces for Zoom Meeting

Zoom admite una comunicación optimizada en tiempo real para WSP y PCoIP basados en Windows WorkSpaces, con el complemento Zoom VDI. La comunicación directa con el cliente permite que las videollamadas pasen por alto el escritorio virtual basado en la nube y proporcionen una experiencia de Zoom similar a la local cuando la reunión se lleva a cabo en casa del usuario. WorkSpace

Habilite el complemento multimedia Zoom Meeting para WSP

Antes de instalar los componentes de Zoom VDI, actualice la WorkSpaces configuración para que sea compatible con la optimización de Zoom.

Requisitos previos

Antes de usar el complemento, asegúrese de que se cumplen los siguientes requisitos.

- WorkSpaces Cliente de Windows versión 5.10.0+ con el complemento Zoom VDI versión 5.17.10+
- Dentro de su cliente Zoom VDI Meeting, versión WorkSpaces 5.17.10+

Antes de empezar

1. Habilite la configuración de la política de grupo de extensiones. Para obtener más información, consulte Configurar las extensiones para WSP.
2. Deshabilite la configuración de la política de grupo de reconexión automática. Para obtener más información, consulte Establezca el tiempo de espera de reanudación de la sesión para WSP.

Instalación de los componentes de Zoom

Para habilitar la optimización de Zoom, instale dos componentes, proporcionados por Zoom, en su Windows WorkSpaces. Para obtener más información, consulte Uso de Zoom para Amazon Web Services.

1. Instale el cliente Zoom VDI Meeting, versión 5.12.6+, en su. WorkSpace
2. Instale la versión 5.12.6+ del complemento Zoom VDI (Windows Universal Installer) en el cliente en el que está instalado WorkSpace
3. Compruebe que el complemento esté optimizando el tráfico de Zoom confirmando que el estado del complemento de VDI aparece como Conectado en el cliente de Zoom VDI. Para obtener más información, consulta Cómo confirmar la WorkSpaces optimización de Amazon.

Habilite el complemento multimedia Zoom Meeting para PCoIP

Los usuarios con permisos administrativos para Active Directory pueden generar una clave de registro mediante su objeto de política de grupo (GPO). Esto permite a los usuarios enviar la clave de registro a todos los Windows WorkSpaces de su dominio mediante una actualización forzada. Como

alternativa, los usuarios con derechos administrativos también pueden instalar las claves de registro de forma individual en su WorkSpaces host.

Requisitos previos

Antes de usar el complemento, asegúrese de que se cumplen los siguientes requisitos.

- WorkSpaces Cliente de Windows versión 5.4.0+ con el complemento Zoom VDI versión 5.12.6+.
- Dentro de su cliente Zoom VDI Meeting WorkSpaces , versión 5.12.6+.

Cree la clave de registro en un host de Windows WorkSpaces

Complete el siguiente procedimiento para crear una clave de registro en un WorkSpaces host de Windows. La clave de registro es necesaria para utilizar Zoom en Windows WorkSpaces.

1. Abra el Editor del Registro de Windows como administrador.
2. Vaya a `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`.
3. Si la clave Extensión no existe, haga clic con el botón derecho del ratón y seleccione Nueva > Clave. A continuación, escriba el nombre Extensión.
4. En la nueva clave Extensión, haga clic con el botón derecho del ratón y seleccione Nuevo > DWORD y escriba activar. El nombre debe estar en minúsculas.
5. Elija el nuevo DWORD y cambie el valor a 1.
6. Reinicie el ordenador para completar el proceso.
7. En su WorkSpaces host, descargue e instale el último cliente VDI de Zoom. En su WorkSpaces cliente (5.4 o superior), descargue e instale el complemento de cliente Zoom VDI más reciente para Amazon WorkSpaces. Para obtener más información, consulte las versiones y descargas de VDI en el sitio web de soporte de Zoom.

Abra Zoom para iniciar la videollamada.

Resolución de problemas

Realice las siguientes acciones para solucionar los problemas de Zoom en Windows. WorkSpaces

- Confirme que la clave de registro se activó y se aplicó correctamente.
- Vaya a `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`. Debería aparecer `wse_core_dll`.

- Asegúrese de que las versiones del host y de los clientes sean correctas y de que coincidan.

Si sigue teniendo dificultades, póngase en contacto con nosotros a AWS Support través del AWS Support Centro.

Puede utilizar los siguientes ejemplos para aplicar un GPO como administrador de su directorio.

- WSE.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

Administre su Amazon Linux WorkSpaces

Al igual que en Windows WorkSpaces, Amazon Linux WorkSpaces está unido a un dominio, por lo que puede usar los usuarios y grupos de Active Directory para:

- Administre su Amazon Linux WorkSpaces
- Proporcione acceso a ellos a WorkSpaces los usuarios

Dado que las instancias de Linux no cumplen la política de grupo, recomendamos que utilice una solución de administración de la configuración para distribuir y aplicar la política. Por ejemplo, puede utilizar AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise o Ansible.

> **Note**
>
> La redirección de impresoras locales no está disponible para Amazon Linux. WorkSpaces

Controle el comportamiento del Protocolo de WorkSpaces transmisión (WSP) en Amazon Linux WorkSpaces

El comportamiento de WSP se controla mediante la configuración del archivo `wsp.conf`, que se encuentra en el directorio `/etc/wsp/`. Para implementar y aplicar cambios en la política, utilice una solución de administración de la configuración que sea compatible con Amazon Linux. Los cambios surtirán efecto cuando se inicie el agente.

> **Note**
>
> - Si realiza cambios incorrectos o incompatibles en el `wsp.conf` archivo, es posible que los cambios de política no se apliquen a las conexiones recién establecidas en su archivo. WorkSpace
> - Los paquetes de Amazon Linux WorkSpaces en WSP tienen actualmente las siguientes limitaciones:
>   - Actualmente, solo están disponibles en (EE. UU. Oeste) y AWS GovCloud (EE. UU. Este AWS GovCloud).
>   - No se admite la entrada de vídeo.

- No se admite la desconexión de la sesión al bloquear la pantalla.

En las secciones siguientes, se describe cómo activar o desactivar determinadas funciones.

Configurar la redirección del portapapeles para WSP Amazon Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección del portapapeles. Utilice el archivo de configuración WSP para configurar esta característica, si es necesario. Esta configuración se aplica al desconectar y volver a conectar el. WorkSpace

Para configurar la redirección del portapapeles para WSP Amazon Linux WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2.
```
clipboard = X
```

Donde los valores posibles de *X* son:

`enabled`: el redireccionamiento del portapapeles está habilitado en ambas direcciones (opción predeterminada)

`disabled`: el redireccionamiento del portapapeles está desactivado en ambas direcciones

`paste-only`: el redireccionamiento del portapapeles está habilitado, pero solo permite copiar el contenido del dispositivo cliente local y pegarlo en el escritorio del host remoto

`copy-only`: el redireccionamiento del portapapeles está habilitado, pero solo permite copiar el contenido del escritorio del host remoto y pegarlo en el dispositivo cliente local

Habilitar o deshabilitar la redirección de entrada de audio para WSP Amazon Linux WorkSpaces

De forma predeterminada, admite la redirección de entrada de audio WorkSpaces . Utilice el archivo de configuración WSP para desactivar esta característica, si es necesario. Esta configuración se aplica al desconectarse y volver a conectarse al. WorkSpace

Para habilitar o deshabilitar la redirección de entrada de audio para WSP Amazon Linux WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Añada la siguiente línea al final del archivo.

   ```
   audio-in = X
   ```

   Donde los valores posibles de *X* son:

   `enabled`: el redireccionamiento de entrada de audio está habilitado (de forma predeterminada)

   `disabled`: el redireccionamiento de entrada de audio está desactivado

Habilitar o deshabilitar la redirección de zona horaria para WSP Amazon Linux WorkSpaces

De forma predeterminada, la hora de un espacio de trabajo está configurada para reflejar la zona horaria del cliente que se utiliza para conectarse al. WorkSpace Este comportamiento se controla mediante el redireccionamiento de zona horaria. Es posible que desee desactivar el redireccionamiento de zona horaria por diversas razones:

- Su empresa quiere que todos los empleados trabajen en la misma zona horaria (aunque algunos empleados estén en otras zonas horarias).
- Ha programado tareas en una WorkSpace que están destinadas a ejecutarse a una hora determinada y en una zona horaria específica.
- Sus usuarios, que viajan mucho, desean mantener su zona horaria WorkSpaces en una sola zona horaria para mantener la coherencia y mantener sus preferencias personales.

Utilice el archivo de configuración WSP para configurar esta característica, si es necesario. Esta configuración surtirá efecto después de desconectarse y volver a conectarse al WorkSpace.

Para habilitar o deshabilitar la redirección de zona horaria para WSP Amazon Linux WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
   ```

2. Añada la siguiente línea al final del archivo.

   ```
   timezone_redirect= X
   ```

   Donde los valores posibles de *X* son:

   habilitado: el redireccionamiento de zona horaria está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento de zona horaria está deshabilitado

Controle el comportamiento del agente PCoIP en Amazon Linux WorkSpaces

El comportamiento del agente de PCoIP se controla mediante la configuración del archivo `pcoip-agent.conf`, que se encuentra en el directorio `/etc/pcoip-agent/`. Para implementar y aplicar cambios en la política, utilice una solución de administración de la configuración que sea compatible con Amazon Linux. Los cambios surtirán efecto cuando se inicie el agente. Al reiniciar el agente, finalizarán las conexiones abiertas y se reiniciará el administrador de ventanas. Para aplicar cualquier cambio, se recomienda reiniciar el. WorkSpace

> **Note**
>
> Si realizas cambios incorrectos o incompatibles en el `pcoip-agent.conf` archivo, es posible que dejes de WorkSpace funcionar. Si el tuyo WorkSpace deja de funcionar, puede que tengas que conectarte a tu red WorkSpace mediante SSH para deshacer los cambios, o puede que tengas que volver a crearlos. WorkSpace

En las secciones siguientes, se describe cómo activar o desactivar determinadas funciones. Para obtener una lista completa de los ajustes disponibles, `man pcoip-agent.conf` ejecútelos desde el terminal de cualquier Amazon Linux WorkSpace.

Configurar la redirección del portapapeles para PCoIP Amazon Linux WorkSpaces

De forma predeterminada, admite la redirección del WorkSpaces portapapeles. Utilice el agente de PCoIP conf para deshabilitar esta característica si es necesario. Esta configuración se aplica al reiniciar el. WorkSpace

Para configurar la redirección del portapapeles para PCoIP (Amazon Linux) WorkSpaces

1. Abra el archivo `pcoip-agent.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Añada la siguiente línea al final del archivo.

   ```
   pcoip.server_clipboard_state = X
   ```

   Donde los valores posibles de *X* son:

   0: el redireccionamiento del portapapeles está desactivado en ambas direcciones

   1: el redireccionamiento del portapapeles está habilitado en ambas direcciones

   2: el redireccionamiento del portapapeles solo está habilitado de cliente a agente (solo permite copiar y pegar desde el dispositivo cliente local al escritorio del host remoto).

   3: el redireccionamiento del portapapeles solo está habilitado de agente a cliente (solo permite copiar y pegar desde el escritorio del host remoto al dispositivo cliente local).

> **Note**
>
> El redireccionamiento del portapapeles se implementa como un canal virtual. Si los canales virtuales están deshabilitados, el redireccionamiento del portapapeles no funciona. Para

habilitar los canales virtuales, consulte Canales virtuales PCoIP en la documentación de Teradici.

Habilitar o deshabilitar la redirección de entrada de audio para PCoIP Amazon Linux WorkSpaces

De forma predeterminada, admite la redirección de entrada de audio. WorkSpaces Utilice el agente de PCoIP conf para deshabilitar esta característica si es necesario. Esta configuración se aplica al reiniciar el. WorkSpace

Para habilitar o deshabilitar la redirección de entrada de audio para PCoIP en Amazon Linux WorkSpaces

1. Abra el archivo `pcoip-agent.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Añada la siguiente línea al final del archivo.

   ```
   pcoip.enable_audio = X
   ```

   Donde los valores posibles de *X* son:

   0: el redireccionamiento de entrada de audio está desactivado

   1: el redireccionamiento de entrada de audio está habilitado

Habilitar o deshabilitar la redirección de zonas horarias para PCoIP | Amazon Linux WorkSpaces

De forma predeterminada, la hora de un espacio de trabajo está configurada para reflejar la zona horaria del cliente que se utiliza para conectarse al. WorkSpace Este comportamiento se controla mediante el redireccionamiento de zona horaria. Es posible que desee desactivar el redireccionamiento de zona horaria por diversas razones:

- Su empresa quiere que todos los empleados trabajen en la misma zona horaria (aunque algunos empleados estén en otras zonas horarias).
- Ha programado tareas en una WorkSpace que están destinadas a ejecutarse a una hora determinada y en una zona horaria específica.
- Sus usuarios, que viajan mucho, desean mantener su zona horaria WorkSpaces en una sola zona horaria para mantener la coherencia y mantener sus preferencias personales.

Si es necesario para Linux WorkSpaces, puede usar la configuración del agente PCoIP para deshabilitar esta función. Esta configuración se aplica al reiniciar el. WorkSpace

Para activar o desactivar la redirección de zonas horarias para PCoIP | Amazon Linux WorkSpaces

1. Abra el archivo `pcoip-agent.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. Añada la siguiente línea al final del archivo.

   ```
   pcoip.enable_timezone_redirect= X
   ```

   Donde los valores posibles de *X* son:

   0: el redireccionamiento de zonas horarias está deshabilitado

   1: el redireccionamiento de zonas horarias está habilitado

Otorgue acceso SSH a los administradores de Amazon Linux WorkSpaces

De forma predeterminada, solo los usuarios y las cuentas asignados en el grupo de administradores de dominio pueden conectarse a Amazon Linux WorkSpaces mediante SSH.

Le recomendamos que cree un grupo de administradores dedicado para los WorkSpaces administradores de Amazon Linux en Active Directory.

Para habilitar el acceso sudo para los miembros del grupo de Active Directory Linux_WorkSpaces_Admins

1. Edite el archivo `sudoers` mediante `visudo`, como se muestra en el siguiente ejemplo.

```
[example\username@workspace-id ~]$ sudo visudo
```

2. Añada la siguiente línea.

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Después de crear el grupo de administradores dedicado, siga los pasos que se indican a continuación para habilitar el inicio de sesión para los miembros de dicho grupo.

Para habilitar el inicio de sesión para los miembros del grupo Active Directory Linux_ WorkSpaces _Admins

1. Edite `/etc/security/access.conf` con privilegios elevados.

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Añada la siguiente línea.

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

Para obtener más información sobre la activación de conexiones SSH, consulte Habilita las conexiones SSH para tu Linux WorkSpaces.

Anular el shell predeterminado de Amazon Linux WorkSpaces

Para anular el shell predeterminado de Linux WorkSpaces, le recomendamos que edite el archivo del `~/.bashrc` usuario. Por ejemplo, para utilizar `Z shell` en lugar del shell de `Bash`, añada las siguientes líneas a /home/*username*/`.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Tras realizar este cambio, debe reiniciar WorkSpace o cerrar la sesión WorkSpace (no solo desconectarse) y, a continuación, volver a iniciarla para que el cambio surta efecto.

Proteger los repositorios personalizados de accesos no autorizados

Para controlar el acceso a los repositorios personalizados, le recomendamos que utilice las características de seguridad integradas en Amazon Virtual Private Cloud (VPC) en lugar de utilizar contraseñas. Por ejemplo, utilice las listas de control de acceso (ACL) y los grupos de seguridad. Para obtener más información sobre estas características, consulte Seguridad en la Guía del usuario de Amazon VPC.

Si tiene que utilizar contraseñas para proteger sus repositorios, asegúrese de crear sus archivos de definición del repositorio de `yum` tal y como se muestra en los Archivos de definición del repositorio en la documentación de Fedora.

Utilice el repositorio de la biblioteca de extras de Amazon Linux

Con Amazon Linux, permite utilizar la biblioteca de extras para instalar actualizaciones de software y de aplicaciones en sus instancias. Para obtener más información sobre el uso de la biblioteca de extras, consulte Biblioteca de extras (Amazon Linux) en la Guía del usuario de Amazon EC2 para instancias de Linux.

> **Note**
>
> Si utiliza el repositorio de Amazon Linux, su Amazon Linux WorkSpaces debe tener acceso a Internet o debe configurar los puntos de enlace de la nube privada virtual (VPC) para este repositorio y para el repositorio principal de Amazon Linux. Para obtener más información, consulte Proporcione acceso a Internet desde su WorkSpace.

Utilice tarjetas inteligentes para la autenticación en Linux WorkSpaces

Los paquetes de Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) permiten el uso de tarjetas inteligentes Common Access Card (CAC) y Personal Identity Verification (PIV) para

la autenticación. Para obtener más información, consulte Utilizar tarjetas inteligentes para la autenticación.

Configurar los ajustes del servidor proxy del dispositivo para acceder a Internet

De forma predeterminada, las aplicaciones WorkSpaces cliente utilizan el servidor proxy que se especifica en la configuración del sistema operativo del dispositivo para el tráfico HTTPS (puerto 443). Las aplicaciones WorkSpaces cliente de Amazon utilizan el puerto HTTPS para las actualizaciones, el registro y la autenticación.

> **Note**
>
> No se admiten los servidores proxy que requieren autenticación con credenciales de inicio de sesión.

Puede configurar los ajustes del servidor proxy del dispositivo para su Linux WorkSpaces mediante la política de grupo siguiendo los pasos que se indican en Configurar el proxy del dispositivo y los ajustes de conectividad a Internet en la documentación de Microsoft.

Para obtener más información sobre la configuración del proxy en la aplicación cliente de WorkSpaces Windows, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Para obtener más información sobre cómo configurar los ajustes del proxy en la aplicación cliente de WorkSpaces macOS, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Para obtener más información sobre cómo configurar los ajustes del proxy en la aplicación cliente WorkSpaces Web Access, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Cómo utilizar el proxy del tráfico de escritorio

En el caso de PCoIP WorkSpaces, las aplicaciones cliente de escritorio no admiten el uso de un servidor proxy ni el descifrado ni la inspección mediante TLS del tráfico del puerto 4172 en UDP (para el tráfico de escritorio). Necesitan una conexión directa a los puertos 4172.

Para WSP WorkSpaces, la aplicación cliente WorkSpaces Windows (versión 5.1 y superior) y la aplicación cliente macOS (versión 5.4 y superior) admiten el uso de servidores proxy HTTP para el tráfico TCP del puerto 4195. No se admiten el descifrado ni la inspección por TLS.

WSP no es compatible con el uso de proxy para el tráfico de escritorios a través de UDP. Solo las aplicaciones cliente de escritorio de WorkSpaces Windows y macOS y el acceso web WSP admiten el uso de proxy para el tráfico TCP.

> **Note**
>
> Si opta por utilizar un servidor proxy, las llamadas a la API que la aplicación cliente realiza a los WorkSpaces servicios también se envían mediante proxy. Tanto las llamadas a la API como el tráfico de escritorio deben pasar por el mismo servidor proxy.

Recomendación sobre el uso de servidores proxy

No recomendamos el uso de un servidor proxy con el tráfico de WorkSpaces escritorio.

El tráfico WorkSpaces de escritorio de Amazon ya está cifrado, por lo que los proxies no mejoran la seguridad. Un proxy representa un salto adicional en la ruta de la red que, al introducir latencia, podría afectar a la calidad de la transmisión. Los proxies también podrían reducir el rendimiento si un proxy no tiene el tamaño adecuado para gestionar el tráfico de streaming de escritorio. Además, la mayoría de los proxies no están diseñados para soportar conexiones de larga duración WebSocket (TCP) y pueden afectar a la calidad y estabilidad de la transmisión.

Si debe usar un proxy, ubique su servidor proxy lo más cerca posible del WorkSpace cliente, preferiblemente en la misma red, para evitar añadir latencia a la red, lo que podría afectar negativamente a la calidad y la capacidad de respuesta de la transmisión.

Administra tu Ubuntu WorkSpaces

Al igual que Windows y Amazon Linux WorkSpaces, Ubuntu WorkSpaces está unido a un dominio, por lo que puede usar Usuarios y grupos de Active Directory para:

- Administra tu Ubuntu WorkSpaces
- Proporcione acceso a ellos a WorkSpaces los usuarios

Puede administrar Ubuntu WorkSpaces con una política de grupo mediante AdSys. Para obtener más información, consulte Ubuntu Active Directory integration FAQ. También puede utilizar otras soluciones de configuración y administración, como Landscape y Ansible.

Controle el comportamiento del Protocolo de WorkSpaces Transmisión (WSP) en Ubuntu WorkSpaces

El comportamiento de WSP se controla mediante la configuración del archivo `wsp.conf`, que se encuentra en el directorio `/etc/wsp/`. Para implementar y aplicar cambios en la política, utilice una solución de administración de la configuración que sea compatible con Ubuntu. Los cambios surtirán efecto cuando se inicie el agente.

> **Note**
>
> Si realiza cambios incorrectos o no compatibles en las `wsp.conf` políticas, es posible que no se apliquen a las nuevas conexiones establecidas con su cuenta. WorkSpace

En las secciones siguientes, se describe cómo activar o desactivar determinadas funciones.

Habilita o deshabilita la redirección del portapapeles para Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección del portapapeles. Utilice el archivo de configuración WSP para desactivar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección del portapapeles en Ubuntu WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Añada la siguiente línea al final del grupo `[policies]`.

   ```
   clipboard = X
   ```

   Donde los valores posibles de *X* son:

   habilitado: el redireccionamiento del portapapeles está habilitado en ambas direcciones (opción predeterminada)

   deshabilitado: el redireccionamiento del portapapeles está desactivado en ambas direcciones

solo pegar: el redireccionamiento del portapapeles está habilitado, pero solo permite copiar el contenido del dispositivo cliente local y pegarlo en el escritorio del host remoto

solo copiar: el redireccionamiento del portapapeles está habilitado, pero solo permite copiar el contenido del escritorio del host remoto y pegarlo en el dispositivo cliente local

Habilita o deshabilita la redirección de entrada de audio en Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de audio. Utilice el archivo de configuración WSP para desactivar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de entrada de audio en Ubuntu WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Añada la siguiente línea al final del grupo `[policies]`.

```
audio-in = X
```

Donde los valores posibles de *X* son:

habilitado: el redireccionamiento de entrada de audio está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de entrada de audio está desactivado

Habilita o deshabilita la redirección de entrada de vídeo en Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de vídeo. Utilice el archivo de configuración WSP para desactivar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de entrada de vídeo en Ubuntu WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Añada la siguiente línea al final del grupo `[policies]`.

```
video-in = X
```

Donde los valores posibles de *X* son:

habilitado: el redireccionamiento de entrada de vídeo está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de entrada de vídeo está desactivado

Habilita o deshabilita la redirección de zona horaria en Ubuntu WorkSpaces

De forma predeterminada, la hora de un espacio de trabajo está configurada para reflejar la zona horaria del cliente que se utiliza para conectarse al WorkSpace. Este comportamiento se controla mediante el redireccionamiento de zona horaria. Es posible que desee desactivar el redireccionamiento de zona horaria por diversas razones:

- Su empresa quiere que todos los empleados trabajen en la misma zona horaria (aunque algunos empleados estén en otras zonas horarias).
- Ha programado tareas en una WorkSpace que deben ejecutarse a una hora determinada y en una zona horaria específica.
- Sus usuarios viajan mucho y quieren mantener su WorkSpaces zona horaria única para mantener la coherencia y mantener sus preferencias personales.

Utilice el archivo de configuración WSP para configurar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de zona horaria en Ubuntu WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. Añada la siguiente línea al final del grupo `[policies]`.

```
timezone-redirection = X
```

Donde los valores posibles de *X* son:

habilitado: el redireccionamiento de zona horaria está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de zona horaria está deshabilitado

Habilita o deshabilita la redirección de impresoras para Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de impresoras. Utilice el archivo de configuración WSP para desactivar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de impresoras en Ubuntu WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Añada la siguiente línea al final del grupo `[policies]`.

   ```
   remote-printing = X
   ```

   Donde los valores posibles de *X* son:

   habilitado: el redireccionamiento a la impresora está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento a la impresora está deshabilitado

Activar o desactivar la sesión de desconexión en el bloqueo de pantalla para WSP

Habilite la desconexión de la sesión en el bloqueo de pantalla para que los usuarios puedan finalizar su WorkSpaces sesión cuando se detecte la pantalla de bloqueo. Para volver a conectarse desde

el WorkSpaces cliente, los usuarios pueden usar sus contraseñas o sus tarjetas inteligentes para autenticarse, según el tipo de autenticación que tengan habilitado. WorkSpaces

De forma predeterminada, WorkSpaces no admite la desconexión de la sesión al bloquear la pantalla. Utilice el archivo de configuración WSP para activar esta característica, si es necesario.

Para activar o desactivar la sesión de desconexión mediante el bloqueo de pantalla en Ubuntu WorkSpaces

1. Abra el archivo `wsp.conf` en un editor con privilegios elevados mediante el siguiente comando.

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. Añada la siguiente línea al final del grupo `[policies]`.

   ```
   disconnect-on-lock = X
   ```

   Donde los valores posibles de *X* son:

   habilitado: la desconexión al bloquear la pantalla está activada

   deshabilitado: la desconexión al bloquear la pantalla está desactivada (de forma predeterminada)

Conceda acceso SSH a los administradores de Ubuntu WorkSpaces

De forma predeterminada, solo los usuarios y cuentas asignados en el grupo de administradores de dominio pueden conectarse a Ubuntu WorkSpaces mediante SSH. Para permitir que otros usuarios y cuentas se conecten a Ubuntu WorkSpaces mediante SSH, le recomendamos que cree un grupo de administradores dedicado para sus administradores de Ubuntu en Active WorkSpaces Directory.

Para habilitar el acceso sudo para los miembros del grupo de Active Directory **`Linux_WorkSpaces_Admins`**

1. Edite el archivo `sudoers` mediante `visudo`, como se muestra en el siguiente ejemplo.

   ```
   [username@workspace-id ~]$ sudo visudo
   ```

2. Añada la siguiente línea.

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

Después de crear el grupo de administradores dedicado, siga los pasos que se indican a continuación para habilitar el inicio de sesión para los miembros de dicho grupo.

Para habilitar el inicio de sesión para los miembros del grupo de Active Directory **`Linux_WorkSpaces_Admins`**

1. Edite `etc/security/access.conf` con privilegios elevados.

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. Añada la siguiente línea.

```
+:(Linux_WorkSpaces_Admins):ALL
```

Con Ubuntu WorkSpaces , no es necesario añadir un nombre de dominio al especificar el nombre de usuario para la conexión SSH y, de forma predeterminada, la autenticación por contraseña está deshabilitada. Para conectarte a través de SSH, debes añadir tu clave pública SSH `$HOME/.ssh/authorized_keys` en Ubuntu WorkSpace o editarla `/etc/ssh/sshd_config` para configurarla. PasswordAuthentication `yes` Para obtener más información sobre cómo habilitar las conexiones SSH, consulta Habilitar las conexiones SSH para Linux. WorkSpaces

Anule el shell predeterminado para Ubuntu WorkSpaces

Para anular el shell predeterminado de Ubuntu WorkSpaces, te recomendamos que edites el archivo del `~/.bashrc` usuario. Por ejemplo, para utilizar `Z shell` en lugar del shell de `Bash`, añada las siguientes líneas a `/home/username/.bashrc`.

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> Tras realizar este cambio, debe reiniciar WorkSpace o cerrar la sesión WorkSpace (no solo desconectarse) y volver a iniciarla para que el cambio surta efecto.

Configurar los ajustes del servidor proxy del dispositivo para acceder a Internet

De forma predeterminada, las aplicaciones WorkSpaces cliente utilizan el servidor proxy que se especifica en la configuración del sistema operativo del dispositivo para el tráfico HTTPS (puerto 443). Las aplicaciones WorkSpaces cliente de Amazon utilizan el puerto HTTPS para las actualizaciones, el registro y la autenticación.

> **Note**
>
> No se admiten los servidores proxy que requieren autenticación con credenciales de inicio de sesión.

Puede configurar los ajustes del servidor proxy del dispositivo para su Ubuntu WorkSpaces mediante la política de grupo siguiendo los pasos que se indican en Configurar el proxy del dispositivo y los ajustes de conectividad a Internet en la documentación de Microsoft.

Para obtener más información sobre la configuración del proxy en la aplicación cliente de WorkSpaces Windows, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Para obtener más información sobre cómo configurar los ajustes del proxy en la aplicación cliente de WorkSpaces macOS, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Para obtener más información sobre la configuración del proxy en la aplicación cliente WorkSpaces Web Access, consulte Proxy Server en la Guía del WorkSpaces usuario de Amazon.

Cómo utilizar el proxy del tráfico de escritorio

En el caso de PCoIP WorkSpaces, las aplicaciones cliente de escritorio no admiten el uso de un servidor proxy ni el descifrado ni la inspección mediante TLS del tráfico del puerto 4172 en UDP (para el tráfico de escritorio). Necesitan una conexión directa a los puertos 4172.

Para WSP WorkSpaces, la aplicación cliente WorkSpaces Windows (versión 5.1 y superior) y la aplicación cliente macOS (versión 5.4 y superior) admiten el uso de servidores proxy HTTP para el tráfico TCP del puerto 4195. No se admiten el descifrado ni la inspección por TLS.

WSP no es compatible con el uso de proxy para el tráfico de escritorios a través de UDP. Solo las aplicaciones cliente de escritorio de WorkSpaces Windows y macOS y el acceso web WSP admiten el uso de proxy para el tráfico TCP.

> **Note**
>
> Si opta por utilizar un servidor proxy, las llamadas a la API que la aplicación cliente realiza a los WorkSpaces servicios también se envían mediante proxy. Tanto las llamadas a la API como el tráfico de escritorio deben pasar por el mismo servidor proxy.

Recomendación sobre el uso de servidores proxy

No recomendamos el uso de un servidor proxy con el tráfico de WorkSpaces escritorio.

El tráfico WorkSpaces de escritorio de Amazon ya está cifrado, por lo que los proxies no mejoran la seguridad. Un proxy representa un salto adicional en la ruta de la red que, al introducir latencia, podría afectar a la calidad de la transmisión. Los proxies también podrían reducir el rendimiento si un proxy no tiene el tamaño adecuado para gestionar el tráfico de streaming de escritorio. Además, la mayoría de los proxies no están diseñados para soportar conexiones de larga duración WebSocket (TCP) y pueden afectar a la calidad y estabilidad de la transmisión.

Si debe usar un proxy, ubique su servidor proxy lo más cerca posible del WorkSpace cliente, preferiblemente en la misma red, para evitar añadir latencia a la red, lo que podría afectar negativamente a la calidad y la capacidad de respuesta de la transmisión.

Optimice Amazon WorkSpaces para una comunicación en tiempo real

Amazon WorkSpaces ofrece una amplia gama de técnicas para facilitar el despliegue de aplicaciones de comunicación unificada (UC), como Microsoft Teams, Zoom, Webex y otras. En los entornos de aplicaciones actuales, la mayoría de las aplicaciones de comunicaciones unificadas constan de una variedad de funciones, entre las que se incluyen salas de chat individuales, canales de chat grupales colaborativos, almacenamiento e intercambio de archivos sin problemas, eventos en directo, seminarios web, transmisiones, funciones interactivas de control y uso compartido de la pantalla, pizarra y funciones de mensajería de audio y vídeo sin conexión. La mayoría de estas funciones están disponibles sin problemas WorkSpaces como características estándar, sin necesidad de ajustes o mejoras adicionales. Sin embargo, cabe señalar que los elementos de comunicación en tiempo real, especialmente las one-on-one convocatorias y las reuniones grupales colectivas, representan una excepción a esta regla. La incorporación exitosa de esta funcionalidad a menudo exige una concentración y una planificación específicas durante el proceso de WorkSpaces implementación.

Al planificar la implementación de las funcionalidades de comunicación en tiempo real de las aplicaciones de UC en Amazon WorkSpaces, tiene tres modos de configuración de comunicación en tiempo real (RTC) distintos entre los que elegir. La selección de estos depende de la aplicación o aplicaciones específicas que desee proporcionar a sus usuarios y de los dispositivos cliente que vaya a utilizar.

Este documento se centra en optimizar la experiencia del usuario para las aplicaciones de UC más comunes en Amazon WorkSpaces. Para obtener información sobre las optimizaciones específicas de WorkSpaces Core, consulte la documentación específica del socio.

Temas

Descripción general de los modos de optimización multimedia

A continuación se muestran las opciones de optimización multimedia disponibles.

Opción 1: Comunicación en tiempo real optimizada para medios (RTC optimizada para medios)

En este modo, las aplicaciones UC y VoIP de terceros se ejecutan de forma remota WorkSpace, mientras que su estructura multimedia se transfiere al cliente compatible para la comunicación directa. Las siguientes aplicaciones de comunicaciones unificadas utilizan este enfoque en Amazon WorkSpaces:

- Zoom Meetings
- Reuniones de Cisco Webex

Para que funcione el modo RTC optimizado para medios, el proveedor de aplicaciones de UC debe desarrollar la integración WorkSpaces utilizando uno de los kits de desarrollo de software (SDK) disponibles, como el SDK de extensión DCV. Este modo requiere que los componentes de UC estén instalados en el dispositivo cliente.

Para obtener más información sobre la configuración de este modo, consulte Configure el RTC optimizado para medios.

Opción 2: comunicación en tiempo real optimizada durante la sesión (RTC optimizada durante la sesión)

En este modo, la aplicación UC inalterada se ejecuta en el dispositivo cliente WorkSpace y canaliza el tráfico de audio y vídeo a través del protocolo de WorkSpaces transmisión. El audio local del micrófono y la transmisión de vídeo de una cámara web se redirigen al WorkSpace, donde son consumidos por la aplicación UC. Este modo proporciona una amplia compatibilidad de aplicaciones y entrega de manera eficiente la aplicación de UC desde una plataforma remota WorkSpace a una variedad de plataformas cliente. No es necesario implementar los componentes de la aplicación de comunicaciones unificadas en el dispositivo cliente.

Para obtener más información sobre la configuración de este modo, consulte Configure el RTC optimizado durante la sesión.

Opción 3: comunicación directa en tiempo real (RTC directo)

En este modo, la aplicación que opera dentro de la WorkSpace toma el control del teléfono físico o virtual ubicado en el escritorio del usuario o en el sistema operativo cliente. Esto hace que el tráfico de audio pase directamente del teléfono físico de la estación de trabajo del usuario o del teléfono

virtual del dispositivo cliente al interlocutor remoto. Algunos ejemplos notables de aplicaciones que funcionan en este modo son:

- Optimización de Amazon Connect para Amazon WorkSpaces
- Asistente multimedia WebRTC Genesys Cloud
- Puerta de enlace SIP de Microsoft Teams
- Teléfonos y pantallas de escritorio de Microsoft Teams
- Participa en audioconferencias a través de las funciones de acceso telefónico o «marca mi teléfono» de la aplicación UC.

Para obtener más información sobre la configuración de este modo, consulte Configurar Direct RTC.

¿Qué modo de optimización RTC utilizar?

Se pueden emplear diferentes modos de optimización del RTC simultáneamente o configurarlos para que se complementen entre sí como alternativa. Por ejemplo, considere la posibilidad de habilitar el RTC optimizado para los medios de comunicación para las reuniones de Cisco Webex. Esta configuración garantiza que los usuarios disfruten de una comunicación optimizada cuando accedan a WorkSpace través de un cliente de escritorio. Sin embargo, en situaciones en las que se accede a Webex desde un quiosco de Internet compartido que carece de componentes de optimización de comunicaciones unificadas, Webex pasará sin problemas al modo RTC optimizado durante la sesión para mantener la funcionalidad. Cuando los usuarios utilizan varias aplicaciones de comunicaciones unificadas, los modos de configuración del RTC pueden variar en función de sus requisitos únicos.

La siguiente tabla representa las funciones comunes de las aplicaciones de UC y define qué modo de configuración RTC ofrece el mejor resultado.

Característica	RTC directo	RTC multimedia optimizado	RTC optimizado durante la sesión
Chat uno a uno	No requiere configuración RTC		
Salas de chat grupales	No requiere configuración RTC		
Audioconferencias grupales	Óptima	Óptima	Buena

Característica	RTC directo	RTC multimedia optimizado	RTC optimizado durante la sesión
Videoconferencias grupales	Buena	Óptima	Buena
Llamadas de audio individuales	Óptima	Óptima	Buena
Videollamadas individuales	Buena	Óptima	Buena
Pizarra	No requiere configuración RTC		
Clips de audio/vídeo/mensajería	No aplicable	Buena	Óptima
Uso compartido de archivos	No aplicable	Depende de la aplicación UC	Óptima
Control y uso compartido de la pantalla	No aplicable	Depende de la aplicación UC	Óptima
Seminarios web/eventos de difusión	No aplicable	Buena	Óptima

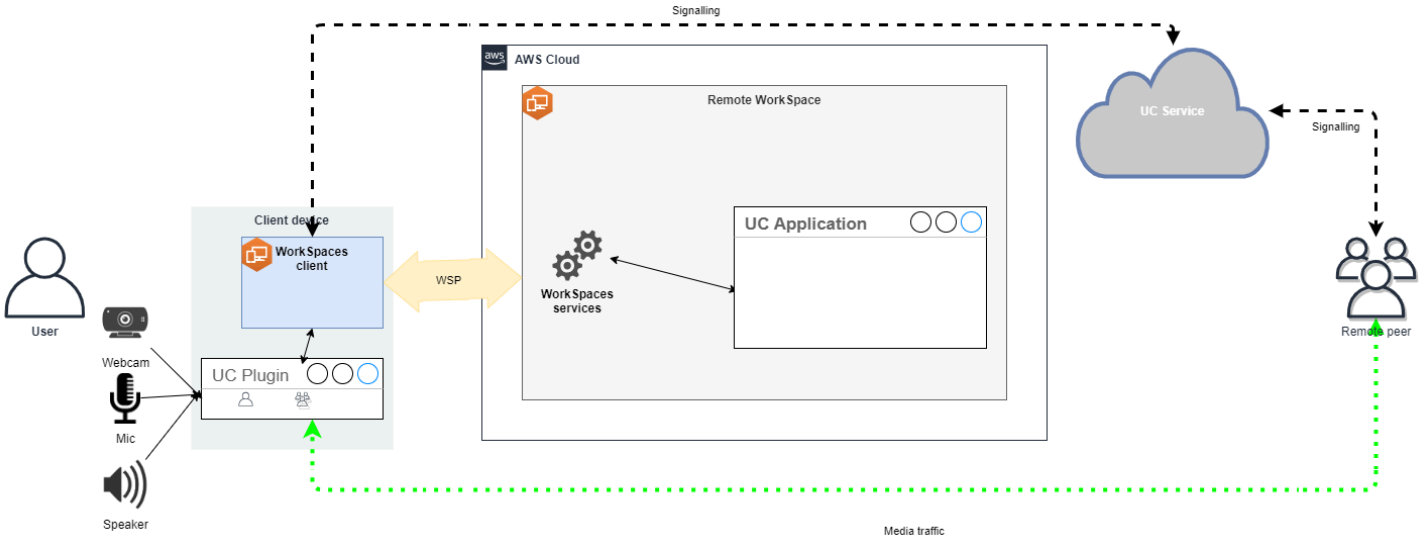
Guía de optimización de RTC

Configure el RTC optimizado para medios

El modo RTC optimizado para medios es posible gracias al uso de los SDK proporcionados por Amazon por parte del fabricante de aplicaciones de comunicaciones unificadas. La arquitectura requiere que el proveedor de UC desarrolle un complemento o extensión específico para UC y lo implemente en el cliente.

El SDK, que incluye opciones disponibles públicamente, como el SDK de extensión DCV y versiones privadas personalizadas, establece un canal de control entre el módulo de aplicaciones de comunicaciones unificadas que funciona en WorkSpace él y un complemento del lado del

cliente. Normalmente, este canal de control indica a la extensión de cliente que inicie o se una a una llamada. Una vez que la llamada se establece a través de la extensión del lado del cliente, el complemento UC captura el audio del micrófono y el vídeo de la cámara web, que luego se transmiten directamente a la nube de UC o al interlocutor de la llamada. El audio entrante se reproduce localmente y el vídeo se superpone en la interfaz de usuario remota del cliente. El canal de control es responsable de comunicar el estado de la llamada.



WorkSpaces Actualmente, Amazon admite las siguientes aplicaciones con el modo RTC optimizado para medios:

- Reuniones con Zoom (para PCoIP y WSP) WorkSpaces
- Reuniones de Cisco Webex (solo para WSP) WorkSpaces

Si utiliza una aplicación que no figura en la lista, se recomienda contactar con el proveedor de la aplicación y solicitar asistencia para WorkSpaces Media Optimized RTC. Para agilizar este proceso, anímelos a ponerse en contacto con aws-av-offloading@amazon .com.

Si bien el modo RTC optimizado para medios mejora el rendimiento de las llamadas y minimiza la utilización de los WorkSpace recursos, presenta ciertas limitaciones:

- La extensión de cliente UC debe estar instalada en el dispositivo cliente.
- La extensión de cliente UC requiere una administración y actualizaciones independientes.
- Es posible que las extensiones de cliente UC no estén disponibles en determinadas plataformas de cliente, como las plataformas móviles o los clientes web.

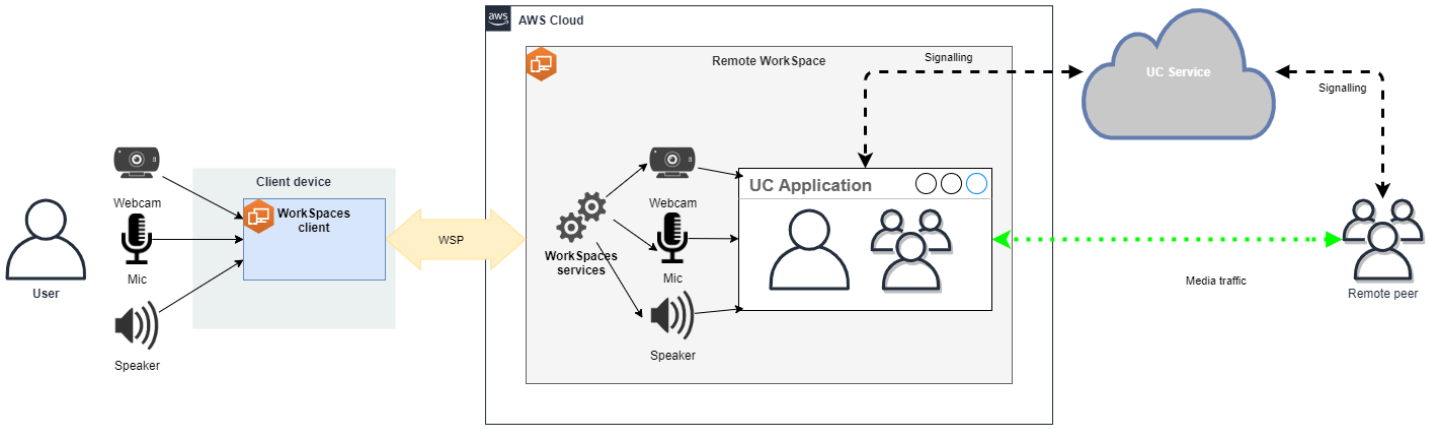
- Algunas funcionalidades de las aplicaciones de comunicaciones unificadas podrían estar restringidas en este modo; por ejemplo, el comportamiento de uso compartido de la pantalla podría ser diferente.
- Es posible que el uso de extensiones del lado del cliente no sea adecuado en situaciones como la de traer su propio dispositivo (BYOD) o quioscos compartidos.

Si el modo RTC optimizado para contenido multimedia resulta inadecuado para su entorno o si algunos usuarios no pueden instalar la extensión de cliente, se recomienda configurar el modo RTC optimizado durante la sesión como opción alternativa.

Configure el RTC optimizado durante la sesión

En el modo RTC optimizado durante la sesión, la aplicación UC funciona WorkSpace sin modificaciones, lo que proporciona una experiencia similar a la local. Las transmisiones de audio y vídeo generadas por la aplicación son capturadas por el Protocolo de WorkSpaces Transmisión (WSP) y transmitidas al lado del cliente. En el cliente, las señales del micrófono (tanto en el WSP como en el PCoIP WorkSpaces) y de la cámara web (solo en el WSP WorkSpaces) se capturan, se redirigen de nuevo a la aplicación UC y se transmiten sin problemas a la WorkSpace aplicación UC.

En particular, esta opción garantiza una compatibilidad excepcional, incluso con aplicaciones antiguas, y ofrece una experiencia de usuario coherente, independientemente del origen de la aplicación. La optimización durante la sesión también funciona con el cliente web.



WorkSpaces El protocolo de transmisión (WSP) se ha optimizado meticulosamente para mejorar el rendimiento del modo RTC remoto. Las medidas de optimización incluyen:

- Utilización de un transporte QUIC adaptativo basado en UDP, que garantiza una transmisión de datos eficiente.

- Establecimiento de una ruta de audio de baja latencia, lo que facilita la entrada y salida rápidas de audio.
- Implementación de códecs de audio optimizados para voz para mantener la calidad del audio y reducir el uso de la CPU y la red.
- Redirección de cámaras web, que permite la integración de las funcionalidades de las cámaras web.
- Configuración de la resolución de la cámara web para optimizar el rendimiento.
- Integración de códecs de pantalla adaptables para equilibrar la velocidad y la calidad visual.
- Corrección de la fluctuación del audio, lo que garantiza una transmisión de audio fluida.

En conjunto, estas optimizaciones contribuyen a una experiencia sólida y fluida en el modo RTC remoto.

Recomendaciones de tamaño

Para admitir eficazmente el modo RTC remoto, es fundamental garantizar el tamaño adecuado de Amazon. WorkSpaces El mando a distancia WorkSpace debe cumplir o superar los requisitos del sistema de la aplicación de comunicación unificada (UC) correspondiente. En la siguiente tabla se describen las WorkSpaces configuraciones mínimas admitidas y recomendadas para las aplicaciones de comunicaciones unificadas más populares cuando se utilizan para videollamadas y llamadas de audio:

			Videollamadas		Llamadas de audio		
Aplicación	Requisitos de CPU para la aplicación RTC	Requisitos de RAM para la aplicación RTC	Mínimamente compatible WorkSpace	Recomendado WorkSpace	Mínimamente compatible WorkSpace	Recomendado WorkSpace	Referencia
Microsoft Teams	Se requieren 2 núcleos, se recomiend	4.0 GB DE RAM	Power (4 vCPU, 16 GB de memoria)	PowerPro (8 vCPU, 32 GB de memoria)	Performance (2 vCPU, 8 GB de memoria)	Power (4 vCPU, 16 GB de memoria)	Requisitos de hardware para

			Videollamadas		Llamadas de audio		
Aplicación	Requisitos de CPU para la aplicación RTC	Requisitos de RAM para la aplicación RTC	Mínimamente compatible WorkSpace	Recomendado WorkSpace	Mínimamente compatible WorkSpace	Recomendado WorkSpace	Referencia
	an 4 núcleos						Microsoft Teams
Zoom	Se requieren 2 núcleos, se recomiendan 4 núcleos	4.0 GB DE RAM	Power (4 vCPU, 16 GB de memoria)	PowerPro (8 vCPU, 32 GB de memoria)	Performance (2 vCPU, 8 GB de memoria)	Power (4 vCPU, 16 GB de memoria)	Requisitos del sistema Zoom: Windows, macOS, Linux
Webex	Se requieren 2 núcleos	4.0 GB DE RAM	Power (4 vCPU, 16 GB de memoria)	PowerPro (8 vCPU, 32 GB de memoria)	Performance (2 vCPU, 8 GB de memoria)	Power (4 vCPU, 16 GB de memoria)	Requisitos del sistema para los servicios de Webex

Es importante tener en cuenta que las videoconferencias implican un uso significativo de recursos para la codificación y decodificación de vídeo. En situaciones de máquinas físicas, estas tareas se transfieren a la GPU. En sistemas que no son de GPU WorkSpaces, estas tareas se realizan en la CPU en paralelo con la codificación de protocolos remotos. Por lo tanto, se recomienda encarecidamente a los usuarios que realizan videollamadas o retransmisiones de vídeo de forma habitual, optar por esta PowerPro configuración.

El uso compartido de la pantalla también consume recursos considerables, ya que el consumo de recursos aumenta con resoluciones más altas. Como resultado, en dispositivos que no utilizan

una GPU WorkSpaces, el uso compartido de la pantalla suele estar limitado a una velocidad de fotogramas más baja.

Aproveche el transporte QUIC basado en UDP con el Protocolo de WorkSpaces Transmisión (WSP)

El transporte UDP es especialmente adecuado para transmitir aplicaciones RTC. Para maximizar la eficiencia, asegúrese de que su red esté configurada para utilizar el transporte QUIC para WSP. Tenga en cuenta que el transporte basado en UDP solo está disponible con clientes nativos.

Configure la aplicación UC para WorkSpaces

Para mejorar las capacidades de procesamiento de vídeo, como el desenfoque del fondo, los fondos virtuales, las reacciones o la organización de eventos en directo, WorkSpace es fundamental optar por una GPU para lograr un rendimiento óptimo.

La mayoría de las aplicaciones de comunicaciones unificadas proporcionan instrucciones para deshabilitar el procesamiento de vídeo avanzado a fin de reducir el uso de la CPU en dispositivos que no utilizan GPU. WorkSpaces

Para obtener más información, consulte los siguientes recursos:

- Microsoft Teams: equipos para una infraestructura de escritorios virtualizados
- Zoom Meetings: gestión de la experiencia del usuario para complementos de VDI incompatibles
- Webex: Guía de implementación de la aplicación Webex para infraestructura de escritorio virtual (VDI): administre y solucione problemas de la aplicación Webex para VDI [Webex App]
- Google Meet: uso de VDI

Habilite el redireccionamiento bidireccional de audio y cámara web

Amazon admite de WorkSpaces forma inherente la entrada y salida de audio y la redirección de cámara a través de la entrada de vídeo de forma predeterminada. Sin embargo, si estas funciones se han deshabilitado por algún motivo específico, puede seguir las instrucciones proporcionadas para volver a habilitar el redireccionamiento. Para obtener más información, consulte Habilitar o deshabilitar la redirección de entrada de vídeo para WSP en la Guía de administración de Amazon. WorkSpaces Los usuarios deben seleccionar la cámara que desean usar en la sesión después de conectarse. Para obtener más información, los usuarios deben consultar las cámaras web y otros dispositivos de vídeo en la Guía del WorkSpaces usuario de Amazon.

Limite la resolución máxima de la cámara web

Para los usuarios que utilizan Power o PowerPro WorkSpaces para realizar videoconferencias, se recomienda encarecidamente restringir la resolución máxima de las cámaras web redirigidas. En este caso PowerPro, la resolución máxima recomendada es de 640 píxeles de ancho por 480 píxeles de alto. En el caso de Power, la resolución máxima recomendada es de 320 píxeles de ancho por 240 píxeles de alto.

Complete los siguientes pasos para configurar la resolución máxima de la cámara web.

1. Abra el Editor del Registro de Windows.
2. Vaya a la siguiente ruta del registro:

   ```
   HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
   ```

3. Cree un valor de cadena con un nombre `max-resolution` y configúrelo en la resolución deseada en el formato `(X,Y)`, donde `X` representa el recuento de píxeles horizontales (ancho) y `Y` el recuento de píxeles verticales (altura). Por ejemplo, especifique `(640,480)`) para representar una resolución de 640 píxeles de ancho y 480 píxeles de alto.

Habilite la configuración de audio optimizada por voz

De forma predeterminada, WorkSpaces están configurados para ofrecer audio 7.1 de alta fidelidad WorkSpaces al cliente, lo que garantiza una calidad de reproducción de música superior. Sin embargo, si su uso principal son las conferencias de audio o vídeo, modificar el perfil del códec de audio a una configuración optimizada para la voz puede ahorrar recursos de la CPU y la red.

Complete los siguientes pasos para configurar el perfil de audio como de voz optimizado.

1. Abra el Editor del Registro de Windows.
2. Vaya a la siguiente ruta del registro:

   ```
   HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
   ```

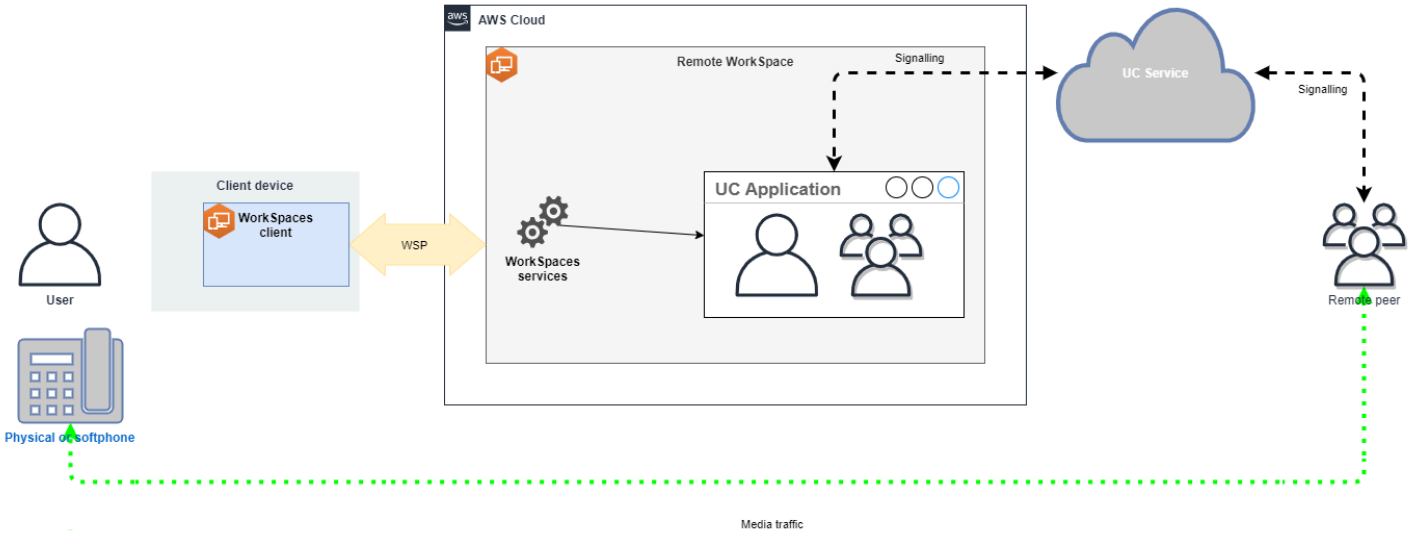
3. Cree un nombre de valor de cadena `default-profile` y configúrelo en `voice`.

Utilice auriculares de buena calidad para las llamadas de audio y vídeo

Para mejorar la experiencia de audio y evitar el eco, es fundamental utilizar auriculares de alta calidad. El uso de altavoces de escritorio puede provocar problemas de eco en la parte remota de la llamada.

Configurar Direct RTC

La configuración del modo RTC directo depende de la aplicación de comunicación unificada (UC) específica y no requiere ningún cambio en la configuración. WorkSpaces La siguiente lista ofrece una recopilación no exhaustiva de las optimizaciones para diversas aplicaciones de UC.



- Microsoft Teams
  - Plan para SIP Gateway
  - Audioconferencias en Microsoft 365
  - Planificar tu solución de voz para Teams
- Reuniones por Zoom:
  - Activación o desactivación de los números de llamadas telefónicas
  - Uso del control de llamadas de un teléfono de escritorio
  - Modo complementario de teléfono de escritorio
- Webex
  - Aplicación Webex | Realice llamadas con su teléfono de escritorio
  - Aplicación Webex | Opciones de llamada compatibles
- BlueJeans:

  - Llamar a una reunión desde un teléfono de escritorio
- Genesys:
  - Asistente multimedia WebRTC Genesys Cloud
- Amazon Connect
  - Optimización de Amazon Connect para Amazon WorkSpaces
- Google Meet:
  - Usa un teléfono para escuchar audio en una videoconferencia

Controlar el modo de ejecución de WorkSpaces

El modo de ejecución de un WorkSpace determina su disponibilidad inmediata y el modo de pago (mensual o por horas). Puede elegir entre los siguientes modos de ejecución cuando cree el Workspace:

- AlwaysOn – se utiliza cuando se paga una tarifa mensual fija por el uso ilimitado de los WorkSpaces. Este modo es la mejor opción para los usuarios que utilizan su espacio de trabajo a tiempo completo como escritorio principal.
- AutoStop – se utiliza cuando los WorkSpaces se pagan por horas. Con este modo, su WorkSpace se detiene tras un periodo determinado de inactividad y se guarda el estado de las aplicaciones y los datos.

Para obtener más información, consulte Precios de WorkSpaces.

Parada automática de los WorkSpaces

Para configurar la hora de parada automática, seleccione el WorkSpace en la consola de Amazon WorkSpaces, elija Acciones, Modificar propiedades del modo de ejecución y, a continuación, configure el tiempo de parada automática (horas). De forma predeterminada, el tiempo de parada automática (horas) se establece en 1 hora, lo que significa que el WorkSpace se detiene automáticamente una hora después de que el WorkSpace se desconecte.

Una vez desconectado un WorkSpace y transcurrido el período de tiempo de parada automática, es posible que el WorkSpace tarde varios minutos más en detenerse automáticamente. Sin embargo, la facturación se detiene tan pronto como vence el período de tiempo de parada automática, y no se le cobra por ese tiempo adicional.

Cuando sea posible, el estado del escritorio se guarda en el volumen raíz del espacio de trabajo. El Workspace se reanuda cuando un usuario inicia sesión, y todos los documentos abiertos y los programas en ejecución se mantienen en el estado en que se guardaron.

Los WorkSpaces de parada automática Graphics.g4dn, GraphicsPro.g4dn, Graphics y GraphicsPro no conservan el estado de los datos y programas cuando se detienen. Para estos WorkSpaces de parada automática, le recomendamos que guarde su trabajo cada vez que termine de utilizarlos.

En el caso de los WorkSpaces de parada automática traiga su propia licencia (BYOL), un gran número de inicios de sesión simultáneos podría provocar un aumento significativo del tiempo de disponibilidad de los WorkSpaces. Si espera que varios usuarios inicien sesión en sus WorkSpaces BYOL AutoStop al mismo tiempo, consulte a su administrador de cuentas para obtener asesoramiento.

> **Important**
>
> Los WorkSpaces de parada automática se detienen automáticamente solo si se desconectan los WorkSpaces.

Un WorkSpace solo se desconecta en las siguientes circunstancias:

- Si el usuario se desconecta manualmente del WorkSpace o cierra la aplicación cliente de Amazon WorkSpaces.
- Si el dispositivo cliente está apagado.
- Si no hay conexión entre el dispositivo cliente y el WorkSpace durante más de 20 minutos.

Como práctica recomendada, los usuarios de WorkSpace de parada automática deben desconectarse manualmente de sus WorkSpaces cuando terminen de utilizarlos cada día. Para desconectarse manualmente, seleccione Desconectar WorkSpace o Salir de Amazon WorkSpaces en el menú de Amazon WorkSpaces en las aplicaciones cliente de WorkSpaces para Linux, macOS o Windows. Para Android o iPad, seleccione Desconectar en el menú de la barra lateral.

Es posible que los WorkSpaces de tipo AutoStop no se detengan automáticamente en las siguientes situaciones:

- Si el dispositivo cliente solo está bloqueado, en reposo o inactivo (por ejemplo, la tapa del portátil está cerrada) en lugar de apagarse, es posible que la aplicación WorkSpaces siga ejecutándose

en segundo plano. Mientras la aplicación WorkSpaces siga ejecutándose, es posible que el WorkSpace no se desconecte y, por lo tanto, que el WorkSpace no se detenga automáticamente.

- WorkSpaces solo puede detectar la desconexión cuando los usuarios utilizan clientes de WorkSpaces. Si los usuarios utilizan clientes de terceros, es posible que WorkSpaces no detecte inactividad y, por lo tanto, puede que el escritorio de WorkSpaces no se detenga automáticamente y no se suspenda la medición.

Modificar el modo de ejecución

Puede cambiar el modo de ejecución en cualquier momento.

Para modificar el modo de ejecución de un escritorio de WorkSpaces

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione el escritorio de WorkSpaces que se va a modificar y elija Acciones, Modificar propiedades del modo de ejecución.
4. Seleccione el nuevo modo de ejecución, AlwaysOn o AutoStop y, a continuación, elija Guardar.

Para modificar el modo de ejecución de un escritorio de WorkSpaces con la AWS CLI

Utilice el comando modify-workspace-properties.

Comenzar y detener un WorkSpace de tipo AutoStop

Cuando los WorkSpaces de tipo AutoStop se desconectan, se detienen automáticamente tras un periodo determinado de desconexión y se suspende la facturación por horas. Para optimizar aún más los costes, puede suspender manualmente los cargos por hora asociados a los WorkSpaces de tipo AutoStop. El escritorio de WorkSpaces se detiene y se guardan todas las aplicaciones y los datos para la próxima vez que un usuario inicie sesión en el escritorio de WorkSpaces.

Cuando un usuario vuelve a conectarse a un espacio de trabajo parado, se reanuda donde se haya quedado, normalmente en menos de 90 segundos.

Puede reiniciar los WorkSpaces de tipo AutoStop que están disponibles o en un estado de error.

Para parar un espacio de trabajo de tipo AutoStop

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione el escritorio de WorkSpaces que se va a detener y elija Acciones, Detener WorkSpaces.
4. Cuando se le pida que confirme, elija Detener WorkSpace.

Para iniciar un espacio de trabajo de tipo AutoStop

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione los que desea iniciar y elija Acciones, Iniciar WorkSpaces.
4. Cuando se le pida que confirme, elija Iniciar WorkSpaces.

Para eliminar los costos fijos de la infraestructura asociados a los escritorios de WorkSpaces AutoStop, elimine el escritorio de WorkSpaces de su cuenta. Para obtener más información, consulte Eliminar WorkSpaces.

Para comenzar y detener un WorkSpace de tipo AutoStop con la AWS CLI

Utilice los comandos stop-WorkSpaces y start-WorkSpaces.

Administración de aplicaciones

Tras lanzar un WorkSpace, podrá ver la lista de todos los paquetes de aplicaciones que están asociados al suyo WorkSpace en la WorkSpaces consola.

Para ver la lista de todos los paquetes de aplicaciones asociados a su WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación izquierdo, elija WorkSpaces.
3. Seleccione WorkSpace y elija Ver detalles.
4. En Aplicaciones, busque la lista de aplicaciones asociadas a esto WorkSpace, junto con su estado de instalación.

Puede actualizar los paquetes de aplicaciones de su cuenta de WorkSpace las siguientes maneras:

- Instale paquetes de aplicaciones en su WorkSpace
- Desinstale los paquetes de aplicaciones de su WorkSpace
- Instale paquetes de aplicaciones y desinstale un conjunto diferente de paquetes de aplicaciones en su WorkSpace

> **Note**
>
> - Para actualizar los paquetes de aplicaciones, el estado WorkSpace debe ser o. `AVAILABLE` `STOPPED`
> - Administrar aplicaciones solo está disponible para Windows WorkSpaces.
> - Administrar aplicaciones solo está disponible para los paquetes de aplicaciones a los que se haya suscrito mediante AWS.

Paquetes compatibles para Administrar aplicaciones

Administrar aplicaciones le permite instalar y desinstalar las siguientes aplicaciones en su WorkSpaces. En el caso del paquete Microsoft Office 2016 y Microsoft Office 2019, solo puedes desinstalarlo.

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Estándar LTSC de Microsoft Visio 2021
- Estándar de Microsoft Project 2021

En la siguiente tabla se muestra la lista de combinaciones de aplicaciones y sistemas operativos compatibles y no compatibles:

	Microsoft Office Professional Plus 2016 (32 bits)	Microsoft Office Professional Plus 2019 (64 bits)	Microsoft LTSC Office Professional Plus / Standard 2021 (64 bits)	Microsoft Project Professional / Standard 2021 (64 bits)	Microsoft LTSC Visio Professional / Standard 2021 (64 bits)
Windows Server 2016	Desinstalación	No admitido	No admitido	No admitido	No admitido
Windows Server 2019	No compatible	Desinstalación	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar
Windows Server 2022	No compatible	Desinstalación	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar
Windows 10	Desinstalación	Desinstalación	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar
Windows 11	Desinstalación	Desinstalación	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar

Important

- Estas aplicaciones deben seguir las mismas ediciones. Por ejemplo, no se pueden mezclar aplicaciones de las versiones Standard con aplicaciones de las versiones Professional.
- Estas aplicaciones deben seguir las mismas ediciones. Por ejemplo, no se pueden mezclar aplicaciones de 2019 con aplicaciones de 2021.
- Microsoft Office/Visio/Project 2021 Standard/Professional no son compatibles con Value, Graphics ni paquetes. GraphicsPro WorkSpaces

- Al desinstalar el paquete de aplicaciones Plus para Microsoft Office 2016 de su WorkSpaces cuenta, perderá el acceso a todas las soluciones de Trend Micro incluidas como parte de ese WorkSpaces paquete de Amazon. Si desea seguir utilizando las soluciones de Trend Micro con su Amazon WorkSpaces, puede adquirirlas por separado en el AWS mercado.
- Para instalar o desinstalar aplicaciones de Microsoft 365, debe incorporar sus propias herramientas e instaladores. Administrar el flujo de trabajo de aplicaciones no puede instalar/desinstalar aplicaciones de Microsoft 365.
- No puede crear una imagen personalizada WorkSpaces con las aplicaciones instaladas mediante Gestionar aplicaciones, pero sí puede crear una imagen personalizada a WorkSpaces partir de la cual desinstalar los paquetes de aplicaciones mediante Gestionar aplicaciones.
- La resolución de DNS debe estar habilitada para usar Administrar aplicaciones.
- En el caso de las regiones que permiten la suscripción, como África (Ciudad del Cabo), la conexión WorkSpaces a Internet debe estar habilitada a nivel de directorio.

Para actualizar los paquetes de aplicaciones en un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione WorkSpace y elija Acciones, Administrar aplicaciones.
4. En Aplicaciones actuales, verá una lista de los paquetes de aplicaciones que ya están instalados WorkSpace y, en Elegir aplicaciones, verá una lista de los paquetes de aplicaciones que están disponibles para instalar en ella. WorkSpace
5. Para instalar paquetes de aplicaciones en este sitio: WorkSpace
   a. Seleccione el paquete de aplicaciones que desee instalar en él y elija Asociar. WorkSpace
   b. Repita el paso anterior para instalar otros paquetes de aplicaciones.
   c. Mientras se instalan los paquetes de aplicaciones, los verá en Aplicaciones actuales con el estado `Pending install deployment`.
6. Para desinstalar paquetes de aplicaciones desde aquí WorkSpace:

a. En Elegir aplicaciones, seleccione el paquete de aplicaciones que desee desinstalar y elija Desasociar.

b. Repita el paso anterior para desinstalar otros paquetes de aplicaciones.

c. Mientras se desinstalan los paquetes de aplicaciones, los verá en Aplicaciones actuales con el estado `Pending uninstall deployment`.

7. Para revertir la instalación o el estado de instalación de los paquetes, realice una de las siguientes acciones.

   - Si desea revertir el estado `Pending uninstall deployment` de los paquetes, seleccione la aplicación que desee revertir y, a continuación, seleccione Asociar.
   - Si desea revertir los paquetes desde el estado `Pending install deployment`, seleccione la aplicación que desea revertir y, a continuación, seleccione Desasociar.

8. Cuando los paquetes de aplicaciones que eligió instalar o desinstalar estén en estado pendiente, elija Implementar aplicaciones.

   > **Important**
   >
   > Tras seleccionar Implementar aplicaciones, la sesión del usuario final finalizará y no se podrá acceder WorkSpaces a ella mientras se estén instalando o desinstalando las aplicaciones.

9. Para confirmar sus acciones, escriba Confirmar. Seleccione forzar para instalar o desinstalar los paquetes de aplicaciones que estén en estado de error.

10. Para monitorizar el progreso de sus paquetes de aplicaciones:

    a. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.

    b. En el panel de navegación, elija WorkSpaces. Puede ver el estado en Estado, que incluye lo siguiente.

       - ACTUALIZANDO: la actualización del paquete de aplicaciones está en curso.
       - DISPONIBLE O DETENIDO: la actualización del paquete de aplicaciones ha finalizado y ha vuelto a su estado original. WorkSpace

    c. Para supervisar el estado de instalación o desinstalación de los paquetes de aplicaciones, seleccione WorkSpace y elija Ver detalles. En Aplicaciones, puede ver el estado en Estado, que incluye `Pending install`, `Pending uninstall` y `Installed`.

> **Note**
>
> Si los usuarios observan que los paquetes de aplicaciones recién instalados a través de Managed Applications no están activados con licencia, puede realizar un reinicio manual. WorkSpace Los usuarios pueden empezar a utilizar esas aplicaciones tras un reinicio. Para obtener asistencia adicional, ponte en contacto con el soporte de AWS.

Administrar las WorkSpaces modificaciones mediante Administrar aplicaciones

Tras instalar o desinstalar los paquetes de aplicaciones en su ordenador WorkSpaces, las siguientes acciones pueden afectar a las configuraciones existentes.

- Restaurar a WorkSpace: la restauración de WorkSpace a recrea tanto el volumen raíz como el volumen de usuarios, en función de las instantáneas más recientes de estos volúmenes que se crearon cuando estaba en buen estado. WorkSpace Se toman WorkSpace instantáneas completas cada 12 horas. Para obtener más información, consulte Restaurar un WorkSpace. Asegúrese de esperar al menos 12 horas antes de restaurar las WorkSpaces que se modificaron mediante Administrar aplicaciones. Si se restaura WorkSpaces antes de la siguiente instantánea completa, que se modificó mediante Administrar aplicaciones, se obtendrá lo siguiente:
  - Los paquetes de aplicaciones que se le instalaron WorkSpaces mediante el flujo de trabajo Administrar aplicaciones se eliminarán de su servidor, WorkSpaces pero la licencia seguirá activa y se le WorkSpaces facturarán esas aplicaciones. Para recuperar esos paquetes de aplicaciones, WorkSpaces debe volver a ejecutar el flujo de trabajo de gestión de aplicaciones, desinstalar la aplicación para empezar de cero y, a continuación, volver a instalarla.
  - Los paquetes de aplicaciones que se eliminaron al WorkSpaces utilizar el flujo de trabajo Gestionar aplicaciones volverán a estar en su servidor. WorkSpaces Sin embargo, esos paquetes de aplicaciones no funcionarán correctamente porque faltará la activación de la licencia. Para deshacerte de esos paquetes de aplicaciones, ejecuta una desinstalación manual de esos paquetes de aplicaciones desde tu. WorkSpaces
- Reconstruir a WorkSpace: al reconstruir a se WorkSpace recrea el volumen raíz. Para obtener más información, consulte Reconstruir un WorkSpace. La reconstrucción de WorkSpaces las que se modificaron mediante Administrar aplicaciones tendrá como resultado lo siguiente:

  - Los paquetes de aplicaciones que se instalaron en usted WorkSpaces mediante el flujo de trabajo Administrar aplicaciones se eliminarán y desactivarán de su servidor. WorkSpaces Para recuperar esas aplicaciones, WorkSpaces debe volver a ejecutar el flujo de trabajo de gestión de aplicaciones.
  - Los paquetes de aplicaciones que se eliminaron de su flujo de trabajo WorkSpaces mediante la gestión de aplicaciones se instalarán y activarán en su WorkSpaces servidor. Para eliminar esos paquetes de aplicaciones de su cuenta WorkSpaces, debe volver a ejecutar el flujo de trabajo de gestión de aplicaciones.
- Migrar a WorkSpace: el proceso de migración recrea el WorkSpace mediante un nuevo volumen raíz de la imagen del paquete de destino y el volumen de usuario de la última instantánea disponible del original. WorkSpace Se crea WorkSpace uno nuevo con un WorkSpace ID nuevo. Para obtener más información, consulte WorkSpaceMigración de una aplicación modificada mediante Administrar WorkSpaces aplicaciones. La migración tendrá como resultado lo siguiente:
  - Se eliminará y WorkSpaces desactivará todo el paquete de aplicaciones de la fuente. El nuevo destino WorkSpaces heredará las aplicaciones del paquete de destino WorkSpaces . Los paquetes de WorkSpaces aplicaciones de origen se facturarán durante todo el mes, pero los paquetes de aplicaciones del paquete de destino tendrán una factura prorrateada.

Modificar un WorkSpace

Tras lanzar un WorkSpace, puede modificar su configuración de tres maneras:

- Puede cambiar el tamaño de su volumen raíz (para Windows, unidad C; para Linux, /) y su volumen de usuario (para Windows, unidad D; para Linux /home).
- Puede cambiar su tipo de computación para seleccionar un nuevo paquete.
- Puede modificar el protocolo de streaming mediante la AWS CLI o la WorkSpaces API de Amazon si WorkSpace se creó con paquetes de PCoIP.

Para ver el estado de modificación actual de un WorkSpace, seleccione la flecha para ver más detalles al respecto. WorkSpace Los valores posibles de State (Estado) son Modifying Compute (Modificación del equipo), Modifying Storage (Modificación del almacenamiento) y None (Ninguno).

Si desea modificar un WorkSpace, debe tener el estado `AVAILABLE` o`STOPPED`. No puede cambiar el tamaño del volumen y el tipo de computación al mismo tiempo.

Si se cambia el tamaño del volumen o el tipo de cálculo de un, WorkSpace se modificará la tarifa de facturación del WorkSpace.

Para permitir que los usuarios puedan modificar sus volúmenes y tipos de cálculo por sí mismos, consulte Habilite las capacidades de WorkSpace administración de autoservicio para sus usuarios.

Modificar los tamaños de los volúmenes

Puede aumentar el tamaño de los volúmenes raíz y de usuario hasta 2000 GB cada uno. WorkSpace WorkSpace los volúmenes raíz y de usuario vienen agrupados en conjuntos que no se pueden cambiar. Los grupos disponibles son:

[Raíz (GB), Usuario (GB)]
[80, 10]
[80, 50]
[80, 100]
[de 175 a 2000, de 100 a 2000]

Puede expandir los volúmenes raíz y de usuario si están cifrados o no cifrados y puede expandir ambos volúmenes una vez en un período de 6 horas. Sin embargo, no puede aumentar el tamaño de los volúmenes raíz y de usuario al mismo tiempo. Para obtener más información, consulte Limitaciones para aumentar volúmenes.

> **Note**
>
> Al expandir un volumen para un WorkSpace, amplía WorkSpaces automáticamente la partición del volumen en Windows o Linux. Cuando finalice el proceso, debe reiniciarlo WorkSpace para que los cambios surtan efecto.

Para garantizar la conservación de los datos, no puede reducir el tamaño de los volúmenes raíz o de usuarios después de lanzar un WorkSpace. En su lugar, asegúrese de especificar los tamaños mínimos de estos volúmenes al lanzar un WorkSpace. Puede lanzar un Value, Standard, Performance, Power o PowerPro WorkSpace con un mínimo de 80 GB para el volumen raíz y 10 GB para el volumen de usuario. Puede lanzar un archivo Graphics.G4dn, GraphicsPro .g4dn, Graphics o

GraphicsPro WorkSpace con un mínimo de 100 GB para el volumen raíz y 100 GB para el volumen de usuario.

Mientras se está incrementando WorkSpace el tamaño del disco, los usuarios pueden realizar la mayoría de las tareas en sus discos. WorkSpace Sin embargo, no pueden cambiar su tipo de WorkSpace cómputo, cambiar el modo de WorkSpace ejecución, reconstruirlo o reiniciarlo (reiniciar) el suyo WorkSpace. WorkSpace

> **Note**
>
> Si desea que sus usuarios puedan utilizarlos WorkSpaces mientras se produce el aumento de tamaño del disco, asegúrese de que WorkSpaces tengan el estado de en `AVAILABLE` lugar de `STOPPED` antes de cambiar el tamaño de los volúmenes del WorkSpaces. Si es así`STOPPED`, no se pueden iniciar mientras se esté incrementando el tamaño del disco. WorkSpaces

En la mayoría de los casos, el proceso de aumento del tamaño del disco puede tardar hasta dos horas. Sin embargo, si va a modificar los tamaños de los volúmenes para un gran número de WorkSpaces ellos, el proceso puede tardar bastante más. Si tiene que modificar un gran número de ellos, le recomendamos WorkSpaces que se ponga en contacto con nosotros AWS Support para obtener ayuda.

Limitaciones para aumentar los volúmenes

- Solo se puede cambiar el tamaño de los volúmenes SSD.
- Al lanzar un WorkSpace, debe esperar 6 horas antes de poder modificar los tamaños de sus volúmenes.
- No se puede aumentar el tamaño de los volúmenes raíz y de usuario al mismo tiempo. Para aumentar el volumen raíz, primero debe cambiar el volumen de usuario a 100 GB. Después de realizar ese cambio, puede actualizar el volumen raíz a cualquier valor entre 175 y 2000 GB. Después de cambiar el volumen raíz a cualquier valor entre 175 y 2000 GB, puede actualizar el volumen del usuario a cualquier valor entre 100 y 2000 GB.

  > **Note**
  >
  > Si desea aumentar ambos volúmenes, debe esperar entre 20 y 30 minutos para que finalice la primera operación antes de poder comenzar la segunda operación.

- A menos que WorkSpace sea un Graphics.G4dn, GraphicsPro .g4dn, Graphics o GraphicsPro WorkSpace, el volumen raíz no puede ser inferior a 175 GB cuando el volumen de usuario es de 100 GB. Graphics.g4dn, GraphicsPro .g4dn y Graphics pueden tener los volúmenes raíz y de usuario configurados en 100 GB como mínimo. GraphicsPro WorkSpaces
- Si el volumen de usuario es de 50 GB, no podrá actualizar el volumen raíz a un tamaño distinto de 80 GB. Si el volumen raíz es de 80 GB, el volumen de usuario solo puede ser de 10, 50 o 100 GB.

Para modificar el volumen raíz de un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione WorkSpace y elija Acciones, Modificar el volumen raíz. .
4. En Tamaños de volumen raíz, elija un tamaño de volumen o elija Personalizado para introducir un tamaño de volumen personalizado.
5. Elija Guardar cambios.
6. Cuando finalice el aumento del tamaño del disco, debe reiniciarlo WorkSpace para que los cambios surtan efecto. Para evitar la pérdida de datos, asegúrese de que el usuario guarde todos los archivos abiertos antes de reiniciar el WorkSpace.

Para modificar el volumen de usuarios de un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione WorkSpace y elija Acciones, Modificar el volumen de usuarios. .
4. En Tamaños de volumen de usuario, elija un tamaño de volumen o Personalizado para introducir un tamaño de volumen personalizado.
5. Elija Guardar cambios.
6. Cuando finalice el aumento del tamaño del disco, debe reiniciarlo WorkSpace para que los cambios surtan efecto. Para evitar la pérdida de datos, asegúrese de que el usuario guarde todos los archivos abiertos antes de reiniciar el WorkSpace.

Para cambiar los tamaños de volumen de un WorkSpace

Utilice el modify-workspace-propertiescomando con la `UserVolumeSizeGib` propiedad `RootVolumeSizeGib` o.

Modificar tipo de computación

Puede cambiar WorkSpace entre los tipos Estándar, Potencia, Rendimiento y PowerPro cómputo. Para obtener más información sobre estos tipos de procesamiento, consulte Amazon WorkSpaces Bundles.

> **Note**
>
> - Puede cambiar el tipo de cómputo de Graphics.g4dn a .g4dn o de GraphicsPro .g4dn a Graphics.g4dn. GraphicsPro No puedes cambiar el tipo de procesamiento de GraphicsPro Graphics.g4dn y .g4dn por ningún otro valor.
> - El paquete de Graphics dejará de ser compatible a partir del 30 de noviembre de 2023. Te recomendamos migrar tu paquete a Graphics.G4DN. WorkSpaces Para obtener más información, consulte Migrar un WorkSpace.
> - No puedes cambiar el tipo de procesamiento de los gráficos ni a ningún otro valor. GraphicsPro

Cuando solicite un cambio de cálculo, WorkSpaces reinicie el sistema WorkSpace con el nuevo tipo de cálculo. WorkSpaces conserva la configuración del sistema operativo, las aplicaciones, los datos y el almacenamiento del WorkSpace.

Puede solicitar un tipo de computación más grande una vez cada 6 horas o un paquete más pequeño una vez cada 30 días. En el caso de los recién lanzados WorkSpace, debe esperar 6 horas antes de solicitar un tipo de procesamiento más grande.

Cuando se está produciendo un cambio en el tipo de WorkSpace procesamiento, los usuarios se desconectan del suyo WorkSpace y no pueden usarlo ni cambiarlo WorkSpace. WorkSpace Se reinicia automáticamente durante el proceso de cambio de tipo de cómputo.

> **Important**
>
> Para evitar la pérdida de datos, asegúrese de que los usuarios guarden los documentos abiertos y otros archivos de la aplicación antes de cambiar el tipo de WorkSpace procesamiento.

El proceso para cambiar el tipo de cálculo puede tardar hasta una hora.

Para cambiar el tipo de procesamiento de un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione WorkSpace y elija Acciones, Modificar el tipo de cálculo.
4. En Tipo de computación, elija un tipo de computación.
5. Elija Guardar cambios.

Para cambiar el tipo de procesamiento de un WorkSpace

Utilice el modify-workspace-propertiescomando con la `ComputeTypeName` propiedad.

Modificar protocolos

Si los ha creado con paquetes PCoIP, puede modificar su protocolo de streaming mediante la AWS CLI o la API de Amazon. WorkSpace WorkSpaces Esto le permite migrar el protocolo utilizando el existente WorkSpace sin utilizar la WorkSpace función de migración. Esto también le permite utilizar el Protocolo de WorkSpaces transmisión (WSP) y mantener su volumen raíz sin volver a crear el PCoIP existente WorkSpaces durante el proceso de migración.

- Solo puede modificar su protocolo si se WorkSpace creó con paquetes de PCoIP.
- Antes de modificar el protocolo a WSP, asegúrese de que WorkSpace cumple los siguientes requisitos para un WSP. WorkSpace
  - Su WorkSpaces cliente es compatible con WSP
  - La región en la que WorkSpace está desplegado es compatible con WSP
  - Los requisitos de dirección IP y puerto para el WSP están abiertos. Para obtener más información, consulte los requisitos de dirección IP y puerto para WorkSpaces.
  - Asegúrese de que su paquete actual está disponible con WSP.
  - Para disfrutar de la mejor experiencia con las videoconferencias, te recomendamos que utilices Power o PowerPro paquetes únicamente.

> **Note**
>
> - Te recomendamos encarecidamente que pruebes con un dispositivo que no sea de producción WorkSpaces antes de empezar a cambiar el protocolo.
> - Si modifica el protocolo de PCoIP a WSP y, a continuación, lo modifica de nuevo a PCoIP, no podrá conectarse a través de Web Access. WorkSpaces

Para cambiar el protocolo de un WorkSpace

1. [Opcional] Reinicie el protocolo WorkSpace y espere a que esté en ese `AVAILABLE` estado antes de modificar el protocolo.
2. [Opcional] Usa el `describe-workspaces` comando para enumerar las WorkSpace propiedades. Asegúrese de que está en estado `AVAILABLE` y de que su actual `Protocol` es correcto.
3. Utilice el comando `modify-workspace-properties` y modifique la propiedad `Protocols` de `PCOIP` a `WSP`, o al revés.

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> La propiedad `Protocols` distingue entre mayúsculas y minúsculas. Asegúrese de que utiliza `PCOIP` o. `WSP`

4. Tras ejecutar el comando, puede tardar hasta 20 minutos en reiniciarse y completar las configuraciones necesarias. WorkSpace
5. Vuelva a utilizar el `describe-workspaces` comando para enumerar WorkSpace las propiedades y comprobar que se encuentra en un `AVAILABLE` estado y que la `Protocols` propiedad actual se ha cambiado al protocolo correcto.

> **Note**
>
> - La modificación WorkSpace del protocolo no actualizará la descripción del paquete en la consola. La descripción del paquete de lanzamiento no cambiará.
> - Si WorkSpace permanece en ese `UNHEALTHY` estado después de 20 minutos, reinícielo WorkSpace en la consola.

6. Ahora puede conectarse a su WorkSpace.

Personaliza la WorkSpace marca

Amazon te WorkSpaces permite crear una WorkSpaces experiencia familiar para tus usuarios mediante el uso de las API para personalizar la apariencia de tu página de inicio WorkSpace de sesión con el logotipo de tu marca, información de soporte de TI, enlace de contraseña olvidada y mensaje de inicio de sesión. Tu marca se mostrará a tus usuarios en su página de inicio de WorkSpace sesión y no en la WorkSpaces marca predeterminada.

Se admiten los siguientes caracteres:

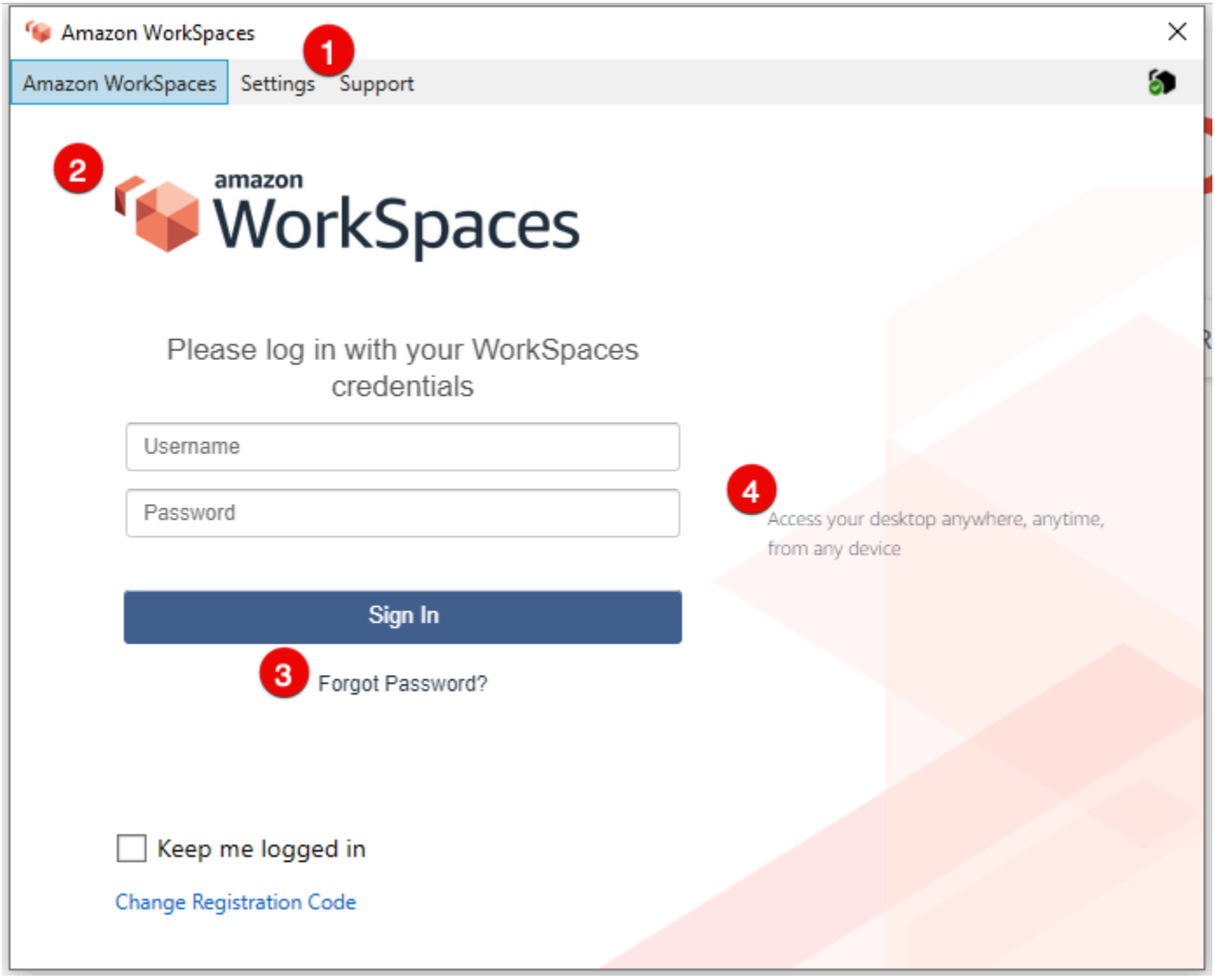
- Windows
- Linux
- Android
- MacOS
- iOS
- Acceso web

> **Note**
>
> Para modificar los elementos de la marca mediante las ClientBranding API deAWS GovCloud (US) Region, utilice una versión de WorkSpaces cliente que sea la 5.10.0.

Importe una marca personalizada

Para importar la personalización de la marca de tu cliente, usa la acción`ImportClientBranding`, que incluye los siguientes elementos. Consulte la referencia ImportClientBranding de la API para obtener más información.

> **Important**
>
> Los atributos de la marca del cliente están orientados al público. Asegúrese de no incluir información confidencial.



1. Support link

2. Logo
3. Código de contraseña olvidada
4. Mensaje de inicio de sesión

Elementos de marca personalizados

Elemento de marca	Descripción	Requisitos y recomendaciones
Support link	Permite especificar un enlace de correo electrónico de soporte al que puedan contactar los usuarios para obtener ayuda con su WorkSpaces. Puede usar el `SupportEmail` atributo o proporcionar un enlace a su página de soporte mediante el `SupportLink` atributo.	• Para cada tipo de plataforma, los `SupportLink` parámetros `SupportEmail` y se excluyen mutuamente. Puede especificar un parámetro único para cada tipo de plataforma, pero no ambos. • El correo electrónico predeterminado es `workspaces-feedback@amazon.com` . • Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Logo	Le permite personalizar el logotipo de su organización mediante el `Logo` atributo.	• El único formato de imagen aceptado es un objeto de datos binarios que se convierte a partir de un `.png` archivo.
		• Resoluciones recomendadas:
		  • Android: 978 x 190
		  • Escritorio: 319 x 55
		  • iOS @2x: 110 x 200

Elemento de marca	Descripción	Requisitos y recomendaciones
		• iOS @3x: 1650 x 300
Código de contraseña olvidada	Permite añadir una dirección web mediante el ForgotPas swordLink atributo al que pueden acceder los usuarios si olvidan su contraseña WorkSpace.	Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.
Mensaje de inicio de sesión	Permite personalizar un mensaje mediante el `LoginMessage` atributo de la pantalla de inicio de sesión.	• Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 2000 caracteres para la integración con etiquetas HTML y diferentes tamaños de fuente. En los casos predeterminados sin etiquetas HTML, se recomienda mantener el mensaje de inicio de sesión en menos de 600 caracteres. • Etiquetas HTML compatibles: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

Los siguientes son ejemplos de fragmentos de código para su uso. ImportClientBranding

AWSCLI versión 2

> **Warning**
>
> La importación de una marca personalizada sobrescribe los atributos, dentro de esa plataforma, que especifique con sus datos personalizados. También sobrescribe los atributos que no especifiques con los valores predeterminados de los atributos de marca personalizados. Debe incluir los datos de cualquier atributo que no desee sobrescribir.

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

El archivo JSON de importación debe tener el siguiente aspecto:

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

El siguiente fragmento de código Java de ejemplo convierte la imagen del logotipo en una cadena codificada en base64:

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
```

```
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

El siguiente fragmento de código de Python de ejemplo convierte la imagen del logotipo en una cadena codificada en base64:

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> La importación de una marca personalizada sobrescribe los atributos, dentro de esa plataforma, que especifique con sus datos personalizados. También sobrescribe los atributos que no especifiques con los valores predeterminados de los atributos de marca personalizados. Debe incluir los datos de cualquier atributo que no desee sobrescribir.

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();
```

```
// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> La importación de una marca personalizada sobrescribe los atributos, dentro de esa plataforma, que especifique con sus datos personalizados. También sobrescribe los atributos que no especifiques con los valores predeterminados de los atributos de marca personalizados. Debe incluir los datos de cualquier atributo que no desee sobrescribir.

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
```

```
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

Para obtener una vista previa de la página de inicio de sesión, inicie la WorkSpaces aplicación o la página de inicio de sesión web.

> **Note**
>
> Los cambios pueden tardar hasta 1 minuto en aparecer.

Describe la marca personalizada

Para ver los detalles de la personalización de la marca del cliente que tienes actualmente, usa la acción`DescribeCustomBranding`. El siguiente es un ejemplo de script para su uso DescribeClientBranding. Consulte la referencia de la DescribeClientBranding API para obtener más información.

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

Eliminar la marca personalizada

Para eliminar la personalización de la marca de tu cliente, usa la acción`DeleteCustomBranding`. El siguiente es un ejemplo de script para su uso DeleteClientBranding. Consulte la referencia de la DeleteClientBranding API para obtener más información.

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> Los cambios pueden tardar hasta 1 minuto en aparecer.

Etiquetado de recursos de WorkSpaces

Puede organizar y administrar los recursos de WorkSpaces asignando sus propios metadatos a cada recurso en forma de etiquetas. Especificará una clave y un valor para cada etiqueta. Una clave puede ser una categoría general, como "proyecto", "propietario" o "entorno", con valores específicos asociados. El uso de las etiquetas es una forma sencilla y potente para administrar los recursos de AWS y organizar los datos, incluidos los datos de facturación.

Cuando agrega etiquetas a un recurso existente, esas etiquetas no aparecen en el informe de asignación de costos hasta el primer día del mes siguiente. Por ejemplo, si agrega etiquetas a un escritorio de WorkSpace existente el 15 de julio, las etiquetas no aparecerán en el informe de asignación de costos hasta el 1 de agosto. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

> **Note**
>
> Para ver las etiquetas de recursos de WorkSpaces en Explorador de costos, debe activar las etiquetas que ha aplicado a los recursos de WorkSpaces siguiendo las instrucciones que encontrará en Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario de AWS Billing.
> Aunque las etiquetas aparecen 24 horas después de su activación, los valores asociados a dichas etiquetas pueden tardar de 4 a 5 días en aparecer en el Explorador de costos.

Además, para que aparezcan y proporcionen datos de costos en Explorador de costos, los recursos de WorkSpaces que se hayan etiquetado deben incurrir en cargos durante ese tiempo. Explorador de costos solo muestra datos de costos desde el momento en que se activaron las etiquetas en adelante. No hay datos históricos disponibles en este momento.

Recursos que puede etiquetar

- Puede etiquetar los siguientes recursos en el momento de su creación: WorkSpaces, imágenes importadas y grupos de control de acceso de IP.
- Puede añadir etiquetas a los recursos existentes de los siguientes tipos: WorkSpaces, directorios registrados, paquetes personalizados, imágenes y grupos de control de acceso de IP.

Restricciones de las etiquetas

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 127 caracteres Unicode
- Longitud máxima del valor: 255 caracteres Unicode
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @. No utilice espacios iniciales ni finales.
- No utilice los prefijos `aws:` o `aws:workspaces:` en los nombres o valores de sus etiquetas porque están reservados para uso de AWS. Los nombres y valores de etiquetas que tienen estos prefijos no se pueden editar.

Actualización de las etiquetas de un recurso existente mediante la consola (directorios, WorkSpaces o grupos de control de acceso de IP)

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione uno de los siguientes tipos de recursos: directorios, WorkSpaces o controles de acceso de IP.
3. Seleccione el recurso para abrir su página de detalles.
4. Realice una o más de las siguientes acciones:
   - Para actualizar una etiqueta, modifique los valores Key y Value.

- Para agregar una etiqueta, elija Add Tag y, a continuación, modifique los valores Key y Value.
- Para eliminar una etiqueta, elija el icono de eliminación (X) situado junto a la etiqueta.

5. Cuando termine de actualizar las etiquetas, elija Save.

Para actualizar las etiquetas de un recurso existente desde la consola (imágenes o paquetes)

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione uno de los siguientes tipos de recursos: Paquetes o Imágenes.
3. Elija el recurso para abrir su página de detalles.
4. En Tags (Etiquetas), elija Manage tags (Administrar etiquetas).
5. Realice una o más de las siguientes acciones:

   - Para actualizar una etiqueta, modifique los valores Key y Value.
   - Para agregar una etiqueta, seleccione Agregar nueva etiqueta y, a continuación, edite los valores de Clave y Valor.
   - Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.

6. Cuando termine de actualizar las etiquetas, seleccione Guardar cambios.

Para actualizar las etiquetas de un recurso existente desde la AWS CLI

Utilice los comandos create-tags y delete-tags.

Mantenimiento de escritorios de WorkSpaces

Le recomendamos que realice el mantenimiento de sus WorkSpaces con regularidad. WorkSpaces programa periodos de mantenimiento de forma predeterminada para sus WorkSpaces. Durante el periodo de mantenimiento, el WorkSpace instala actualizaciones importantes de Amazon WorkSpaces y se reinicia según sea necesario. Si están disponibles, las actualizaciones del sistema operativo también se instalan desde el servidor de actualización del sistema operativo que se han configurado en el escritorio de WorkSpaces. Durante el mantenimiento, puede que sus escritorios de WorkSpaces no estén disponibles.

De forma predeterminada, los escritorios de WorkSpaces en Windows están configurados para recibir actualizaciones de Windows Update. Para configurar sus propios mecanismos de

actualización automática para Windows, consulte la documentación de Windows Server Update Services (WSUS) y Configuration Manager.

Requisito

Sus WorkSpaces deben obtener acceso a Internet para que pueda instalar las actualizaciones en el sistema operativo e implementar las aplicaciones. Para obtener más información, consulte the section called “Acceso a Internet”.

Periodos de mantenimiento para escritorios de WorkSpaces AlwaysOn

Para los escritorios de WorkSpaces AlwaysOn, el periodo de mantenimiento se determina en función de la configuración del sistema operativo. La opción predeterminada es un periodo de cuatro horas, desde las 12 de la noche hasta las 4 de la madrugada, en la zona horaria del WorkSpace, todos los domingos por la mañana. De forma predeterminada, la zona horaria de un espacio de trabajo AlwaysOn es la zona horaria de la región de AWS para el WorkSpace. Sin embargo, si se conecta desde otra región y el redireccionamiento de zona horaria está habilitada, y después se desconecta, la zona horaria del escritorio de WorkSpaces se actualiza a la zona horaria de la región desde la que se ha conectado.

Puede deshabilitar el redireccionamiento de zona horaria en Windows WorkSpaces mediante la política de grupo. Puede deshabilitar el redireccionamiento de zona horaria para los WorkSpaces Linux mediante la configuración del agente de PCoIP.

En las áreas de trabajo (WorkSpaces) de Windows, puede configurar el periodo de mantenimiento a través de la política de grupo; consulte Configuración de directivas de grupo para actualizaciones automáticas. No puede configurar el periodo de mantenimiento para escritorios de WorkSpaces de Linux.

Periodos de mantenimiento para escritorios de WorkSpaces AutoStop

Los escritorios de WorkSpaces AutoStop se inician automáticamente una vez al mes para instalar las actualizaciones importantes. A partir del tercer lunes del mes y durante un máximo de dos semanas, el periodo de mantenimiento comienza cada día desde las 12 de la noche hasta las 5 de la madrugada, en la zona horaria de la región de AWS del WorkSpace. Se puede realizar el mantenimiento de los escritorios de WorkSpaces cualquier día dentro del periodo de mantenimiento. Durante este período, solo se mantienen los WorkSpaces con más de 7 días de antigüedad.

Durante el periodo de tiempo en el que WorkSpace está en proceso de mantenimiento, el estado de WorkSpace se establece en `MAINTENANCE`.

Aunque no puede modificar la zona horaria utilizada para mantener el escritorio de WorkSpaces AutoStop, puede desactivar el periodo de mantenimiento del escritorio de WorkSpaces AutoStop de la siguiente manera. Si deshabilita el modo de mantenimiento, sus escritorios de WorkSpaces no se reiniciarán y no pasarán al estado `MAINTENANCE`.

Para deshabilitar el modo de mantenimiento

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions, Update Details.
4. Amplíe Maintenance Mode.
5. Para habilitar las actualizaciones automáticas, elija Enabled. Si prefiere administrar las actualizaciones de forma manual, elija Disabled (Deshabilitadas).
6. Elija Update and Exit.

Mantenimiento manual

Si lo prefiere, puede mantener sus escritorios de WorkSpaces siguiendo su propia programación. Cuando realice tareas de mantenimiento, le recomendamos que cambie el estado del WorkSpace a Mantenimiento. Cuando haya terminado, cambie el estado del WorkSpace a Disponible.

Cuando un WorkSpace se encuentra en estado de Mantenimiento, se producen los siguientes comportamientos:

- El escritorio de WorkSpaces no responde a las solicitudes reiniciar, detener, iniciar o volver a compilar.
- Los usuarios no pueden iniciar sesión en el escritorio de WorkSpaces.
- Un escritorio de WorkSpaces AutoStop no entra en modo de hibernación.

Para cambiar el estado del escritorio de WorkSpaces mediante la consola

> **Note**
>
> Para cambiar el estado de un WorkSpace, éste debe estar en estado Disponible. La opción Modificar estado no está disponible cuando el WorkSpace no está en estado Disponible

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione su WorkSpace, y elija Acciones, Modificar estado.
4. En Modificar estado, elija Disponible o Mantenimiento.
5. Seleccione Save.

Para cambiar el estado del escritorio de WorkSpaces mediante la AWS CLI

Utilice el comando modify-workspace-state.

Cifrado WorkSpaces

WorkSpaces está integrado con AWS Key Management Service (AWS KMS). Esto le permite cifrar los volúmenes de almacenamiento WorkSpaces mediante AWS KMS Key. Al iniciar un WorkSpace, puede cifrar el volumen raíz (para Microsoft Windows, la unidad C; para Linux,/) y el volumen de usuario (para Windows, la unidad D; para Linux, /home). De este modo, se garantiza el cifrado de los datos almacenados en reposo, la E/S de disco en el volumen y las instantáneas creadas a partir de los volúmenes.

> **Note**
>
> Además de cifrar su dispositivo WorkSpaces, también puede utilizar el cifrado FIPS para terminales en determinadas regiones de EE. UU. AWS Para obtener más información, consulte Configurar Amazon WorkSpaces para obtener la autorización FedRAMP o la conformidad DoD SRG..

Contenido

- Ver cifrado WorkSpaces

Requisitos previos

Necesita una AWS KMS clave antes de poder iniciar el proceso de cifrado. Esta clave de KMS puede ser la clave de KMS AWS administrada para Amazon WorkSpaces (aws/workspaces) o una clave de KMS simétrica administrada por el cliente.

- AWS Claves de KMS gestionadas: la primera vez que lanzas una clave de KMS no cifrada WorkSpace desde la WorkSpaces consola de una región, Amazon crea WorkSpaces automáticamente una clave de KMS AWS gestionada (aws/workspaces) en tu cuenta. Puede seleccionar esta clave de KMS AWS administrada para cifrar sus volúmenes de usuario y raíz. WorkSpace Para obtener más detalles, consulte Descripción general del WorkSpaces cifrado mediante AWS KMS.

  Puede ver esta clave de KMS AWS administrada, incluidas sus políticas y concesiones, y puede realizar un seguimiento de su uso en AWS CloudTrail los registros, pero no puede usar ni administrar esta clave de KMS. Amazon WorkSpaces crea y administra esta clave de KMS. Solo Amazon WorkSpaces puede usar esta clave de KMS y solo WorkSpaces puede usarla para cifrar WorkSpaces los recursos de su cuenta.

  AWS Las claves KMS gestionadas, incluida la que WorkSpaces admite Amazon, se rotan cada tres años. Para obtener más información, consulte la AWS KMS clave giratoria en la guía para AWS Key Management Service desarrolladores.
- Clave de KMS gestionada por el cliente: también puede seleccionar una clave de KMS simétrica gestionada por el cliente que haya creado con AWS KMS ella. Puede consultar, usar y administrar esta clave de KMS, incluida la configuración de sus políticas. Para obtener más información sobre la creación de claves KMS, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service . Para obtener más información sobre la creación de claves de KMS mediante la AWS KMS API, consulte Cómo trabajar con claves en la Guía para AWS Key Management Service desarrolladores.

  Las claves KMS administradas por el cliente no se rotan automáticamente a menos que decida habilitar la rotación automática de claves. Para obtener más información, consulte Rotación de AWS KMS claves en la guía para AWS Key Management Service desarrolladores.

> **Important**
>
> Al rotar manualmente las claves KMS, debe mantener habilitadas tanto la clave KMS original como la nueva clave KMS para AWS KMS poder descifrar la WorkSpaces clave KMS original cifrada. Si no quiere mantener habilitada la clave KMS original, debe volver a crearla WorkSpaces y cifrarla con la nueva clave KMS.

Debe cumplir los siguientes requisitos para poder utilizar una AWS KMS clave para cifrar la suya: WorkSpaces

- La clave debe ser simétrica. Amazon WorkSpaces no admite claves KMS asimétricas. Para obtener información sobre cómo distinguir entre CMK simétricas y asimétricas, consulte Identificar clave KMS simétricas y asimétricas en la Guía para desarrolladores de AWS Key Management Service .
- La clave debe estar habilitada. Para determinar si una clave KMS está habilitada, consulte Mostrar detalles de clave KMS en la Guía para desarrolladores de AWS Key Management Service .
- Debe contar con los permisos y políticas correctos asociados a la clave. Para obtener más información, consulte Parte 2: Conceder a WorkSpaces los administradores permisos adicionales mediante una política de IAM.

Límites

- No puedes cifrar una existente. WorkSpace Debe cifrar un WorkSpace cuando lo inicie.
- No se admite la creación de una imagen personalizada a partir de una imagen WorkSpace cifrada.
- Actualmente, no se admite la desactivación del cifrado para un cifrado WorkSpace .
- WorkSpaces si se ejecuta con el cifrado del volumen raíz activado, el aprovisionamiento puede tardar hasta una hora.
- Para reiniciar o reconstruir una clave cifrada WorkSpace, primero asegúrese de que la AWS KMS clave esté habilitada; de lo contrario, WorkSpace quedará inutilizable. Para determinar si una clave KMS está habilitada, consulte Mostrar detalles de clave KMS en la Guía para desarrolladores de AWS Key Management Service .

Descripción general del WorkSpaces cifrado mediante AWS KMS

Cuando crea WorkSpaces con volúmenes cifrados, WorkSpaces utiliza Amazon Elastic Block Store (Amazon EBS) para crear y gestionar esos volúmenes. Amazon EBS cifra el volumen con una clave de datos que utiliza el algoritmo estándar de la industria AES-256. Tanto Amazon EBS como Amazon WorkSpaces utilizan su clave de KMS para trabajar con los volúmenes cifrados. Para obtener más información sobre el cifrado de volúmenes de EBS, consulte Amazon EBS Encryption en la Guía del usuario de Amazon EC2.

Cuando se lanza WorkSpaces con volúmenes cifrados, el end-to-end proceso funciona de la siguiente manera:

1. Debe especificar la clave de KMS que se va a utilizar para el cifrado, así como el usuario y el directorio del WorkSpace. Esta acción crea una concesión que permite WorkSpaces utilizar la clave KMS únicamente para este fin, es WorkSpace decir, únicamente para la WorkSpace asociada al usuario y al directorio especificados.
2. WorkSpaces crea un volumen de EBS cifrado para el volumen WorkSpace y especifica la clave de KMS que se va a utilizar, así como el usuario y el directorio del volumen. Esta acción crea una concesión que permite a Amazon EBS usar su clave de KMS solo para este WorkSpace volumen, es decir, solo para los WorkSpace asociados al usuario y directorio especificados y solo para el volumen especificado.
3. Amazon EBS solicita una clave de datos de volumen cifrada en su clave de KMS y especifica el identificador de seguridad (SID) y el ID de directorio de AWS Directory Service Active Directory del WorkSpace usuario, así como el ID de volumen de Amazon EBS como contexto de cifrado.
4. AWS KMS crea una clave de datos nueva, la cifra con su clave de KMS y, a continuación, envía la clave de datos cifrada a Amazon EBS.
5. WorkSpaces utiliza Amazon EBS para adjuntar el volumen cifrado a su WorkSpace. Amazon EBS envía la clave de datos cifrados a AWS KMS con una `Decrypt`solicitud y especifica el SID del WorkSpace usuario, el ID del directorio y el ID del volumen, que se utilizan como contexto de cifrado.
6. AWS KMS utiliza su clave de KMS para descifrar la clave de datos y, a continuación, envía la clave de datos de texto sin formato a Amazon EBS.
7. Amazon EBS utiliza la clave de datos en texto no cifrado para cifrar todos los datos que se envían a los volúmenes cifrados y se reciben de ellos. Amazon EBS mantiene la clave de datos de texto sin formato en la memoria mientras el volumen esté conectado al WorkSpace.

8. Amazon EBS almacena la clave de datos cifrada (recibida enStep 4) junto con los metadatos del volumen para utilizarla en el futuro en caso de que reinicie o reconstruya el WorkSpace.
9. Cuando utilizas la AWS Management Console para eliminar una WorkSpace (o utilizas la `TerminateWorkspaces`acción en la WorkSpaces API) WorkSpaces y Amazon EBS retira las concesiones que le permitían usar tu clave de KMS para ello WorkSpace.

WorkSpaces contexto de cifrado

WorkSpaces no usa su clave KMS directamente para operaciones criptográficas (como `Encrypt`,, `DecryptGenerateDataKey`, etc.), lo que significa que WorkSpaces no envía solicitudes AWS KMS que incluyan un contexto de cifrado. Sin embargo, cuando Amazon EBS solicita una clave de datos cifrada para los volúmenes cifrados de su WorkSpaces (Step 3en elDescripción general del WorkSpaces cifrado mediante AWS KMS) y cuando solicita una copia en texto plano de esa clave de datos (Step 5), incluye el contexto de cifrado en la solicitud.

El contexto de cifrado proporciona datos autenticados (AAD) adicionales que se AWS KMS utilizan para garantizar la integridad de los datos. El contexto de cifrado también se escribe en los archivos de AWS CloudTrail registro, lo que puede ayudarle a entender por qué se utilizó una clave KMS determinada. Amazon EBS usa lo siguiente para el contexto de cifrado:

- El identificador de seguridad (SID) del usuario de Active Directory que está asociado al WorkSpace
- El ID de AWS Directory Service directorio del directorio que está asociado a WorkSpace
- El ID de volumen de Amazon EBS del volumen cifrado

El siguiente ejemplo muestra una representación JSON del contexto de cifrado que usa Amazon EBS:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

Conceda WorkSpaces permiso para usar una clave KMS en su nombre

Puede proteger sus WorkSpace datos con la clave de KMS AWS administrada para WorkSpaces (aws/workspaces) o con una clave de KMS administrada por el cliente. Si usa una clave KMS

administrada por el cliente, debe conceder WorkSpaces permiso para usar la clave KMS en nombre de los WorkSpaces administradores de su cuenta. La clave KMS AWS administrada WorkSpaces tiene los permisos necesarios de forma predeterminada.

Para preparar la clave KMS administrada por el cliente para usarla con WorkSpaces ella, utilice el siguiente procedimiento.

1. Agregue a sus WorkSpaces administradores a la lista de usuarios clave de la política de claves de la clave KMS
2. Otorgue a sus WorkSpaces administradores permisos adicionales con una política de IAM

Sus WorkSpaces administradores también necesitan permiso para WorkSpaces utilizarla. Para obtener más información acerca de estos permisos, consulte Gestión de identidades y accesos para WorkSpaces.

Parte 1: Añadir WorkSpaces administradores a usuarios clave

Para conceder a WorkSpaces los administradores los permisos que necesitan, puede utilizar la API AWS Management Console o la AWS KMS API.

Para añadir WorkSpaces administradores como usuarios clave de una clave KMS (consola)

1. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija el alias o el ID de clave de la clave KMS administrada por el cliente que prefiera.
5. Seleccione la pestaña Key policy (Política de claves). En Key Users (Usuarios de claves), elija Add (Agregar).
6. En la lista de usuarios y roles de IAM, seleccione los usuarios y roles que corresponden a sus WorkSpaces administradores y, a continuación, elija Agregar.

Para añadir WorkSpaces administradores como usuarios clave de una clave de KMS (API)

1. Utilice la operación GetKeyPolítica para obtener la política clave existente y, a continuación, guarde el documento de política en un archivo.

2. Abra el documento de políticas en el editor de textos que prefiera. Agregue los usuarios y funciones de IAM que correspondan a sus WorkSpaces administradores a las declaraciones de política que otorgan permisos a los usuarios clave. A continuación, guarde el archivo.
3. Utilice la operación PutKeyPolítica para aplicar la política clave a la clave KMS.

Parte 2: Conceder a WorkSpaces los administradores permisos adicionales mediante una política de IAM

Si selecciona una clave de KMS gestionada por el cliente para utilizarla en el cifrado, debe establecer políticas de IAM que permitan WorkSpaces a Amazon utilizar la clave de KMS en nombre de un usuario de IAM de su cuenta que lance la clave de KMS. WorkSpaces Ese usuario también necesita permiso para usar Amazon WorkSpaces. Para obtener más información sobre la creación y edición de políticas de usuario de IAM, consulte Administración de políticas de IAM en la Guía del usuario de IAM y Gestión de identidades y accesos para WorkSpaces.

WorkSpaces el cifrado requiere un acceso limitado a la clave KMS. A continuación, se muestra una política de claves de ejemplo que puede utilizar. Esta política separa a las entidades principales que pueden administrar la clave de AWS KMS de aquellas que pueden usarla. Antes de utilizar esta política de claves de ejemplo, reemplace el ID de la cuenta de ejemplo y el nombre de usuario de IAM por valores reales de su cuenta.

La primera declaración coincide con la política de AWS KMS claves predeterminada. Le da permiso a su cuenta para usar políticas de IAM para controlar el acceso a la clave KMS. La segunda y la tercera sentencia definen qué AWS directores pueden administrar y usar la clave, respectivamente. La cuarta afirmación permite que AWS los servicios que están integrados AWS KMS utilicen la clave en nombre del principal especificado. Esta instrucción permite a los servicios de AWS crear y administrar concesiones. La declaración utiliza un elemento de condición que limita las concesiones de la clave KMS a las concedidas por los AWS servicios en nombre de los usuarios de su cuenta.

> **Note**
>
> Si sus WorkSpaces administradores la utilizan AWS Management Console para crear WorkSpaces con volúmenes cifrados, necesitan permiso para enumerar los alias y las claves (`"kms:ListKeys"`los `"kms:ListAliases"` y los permisos). Si tus WorkSpaces administradores utilizan únicamente la WorkSpaces API de Amazon (no la consola), puedes omitir los `"kms:ListKeys"` permisos `"kms:ListAliases"` y.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
```

```
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

La política de IAM para un usuario o rol que esté cifrando WorkSpace debe incluir los permisos de uso de la clave de KMS administrada por el cliente, así como el acceso a. WorkSpaces Para conceder WorkSpaces permisos a un usuario o rol de IAM, puede adjuntar el siguiente ejemplo de política al usuario o rol de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

El usuario requiere la siguiente política de IAM para usar AWS KMS. Proporciona al usuario acceso de solo lectura a la clave KMS junto con la capacidad de crear concesiones.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Si desea especificar la clave KMS en su política, utilice una política de IAM similar a la siguiente. Reemplace el ARN de la clave KMS de ejemplo por uno válido.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Cifra un WorkSpace

Para cifrar un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. Seleccione Iniciar WorkSpaces y complete los tres primeros pasos.
3. Para el paso WorkSpaces de configuración, haga lo siguiente:

a. Seleccione los volúmenes que se van a cifrar: volumen raíz, volumen de usuarios o ambos.

b. En Clave de cifrado, seleccione una AWS KMS clave, ya sea la clave de KMS AWS gestionada creada por Amazon WorkSpaces o una clave de KMS que haya creado usted. La clave KMS que utilice debe ser simétrica. Amazon WorkSpaces no admite claves KMS asimétricas.

c. Elija Paso siguiente.

4. Selecciona Launch WorkSpaces.

Ver cifrado WorkSpaces

Para ver qué volúmenes WorkSpaces y cuáles se han cifrado desde la WorkSpaces consola, seleccione una opción en la barra WorkSpacesde navegación de la izquierda. La columna Cifrado de volúmenes muestra si cada uno de ellos WorkSpace tiene el cifrado activado o desactivado. Para ver qué volúmenes específicos se han cifrado, expanda la WorkSpace entrada para ver el campo Volúmenes cifrados.

Reiniciar un WorkSpace

Ocasionalmente, es posible que necesite reiniciar (reiniciar) a WorkSpace manualmente. Al reiniciar a, WorkSpace se desconecta al usuario y, a continuación, se apaga y se reinicia el. WorkSpace Para evitar la pérdida de datos, asegúrese de que el usuario guarde todos los documentos abiertos y otros archivos de la aplicación antes de reiniciar el. WorkSpace Esto no afecta a los datos de usuario, el sistema operativo y la configuración del sistema.

> **Warning**
>
> Para reiniciar un archivo cifrado WorkSpace, primero asegúrese de que la AWS KMS clave esté habilitada; de lo contrario, WorkSpace quedará inutilizable. Para determinar si una clave KMS está habilitada, consulte Mostrar detalles de clave KMS en la Guía para desarrolladores de AWS Key Management Service.

Para reiniciar un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.

2. En el panel de navegación, elija WorkSpaces.
3. Seleccione la opción WorkSpaces para reiniciar y elija Acciones, Reiniciar WorkSpaces.
4. Cuando se le solicite la confirmación, elija Reiniciar WorkSpaces.

Para reiniciar un WorkSpace mediante AWS CLI

Utilice el comando reboot-workspaces.

Para reiniciar de forma masiva WorkSpaces

Usa el amazon-workspaces-admin-module.

Reconstruir un WorkSpace

Al reconstruir a, WorkSpace se recrea el volumen raíz de la imagen más reciente del paquete desde el que WorkSpace se lanzó, su volumen de usuario y su interfaz de red elástica principal. Al reconstruir un WorkSpace se eliminan más datos que al restaurar uno WorkSpace, pero solo es necesario disponer de una instantánea del volumen de usuarios. Para restaurar un WorkSpace, consulteRestaurar un espacio de trabajo.

Si se WorkSpace reconstruye a, se produce lo siguiente:

- El volumen raíz (para Microsoft Windows, unidad C; para Linux,/) se actualiza con la imagen más reciente del paquete desde el que WorkSpace se creó. Se pierden todas las aplicaciones que se instalaron o la configuración del sistema que WorkSpace se modificó después de su creación.
- El volumen de usuario (para Microsoft Windows, la unidad D; para Linux, /home) se vuelve a crear a partir de la instantánea más reciente. El contenido actual del volumen de usuario se sobrescribe.

  Las instantáneas automáticas para su uso al reconstruir un WorkSpace se programan cada 12 horas. Estas instantáneas del volumen de usuarios se toman independientemente del estado del. WorkSpace Al seleccionar Acciones, Reconstruir o Restaurar WorkSpace, se muestran la fecha y la hora de la instantánea más reciente.

  Al reconstruir una WorkSpace, también se toman nuevas instantáneas poco después de finalizar la reconstrucción (normalmente en 30 minutos).
- Se vuelve a crear la interfaz de red elástica principal. WorkSpace Recibe una nueva dirección IP privada.

> **Important**
>
> Después del 14 de enero de 2020, los WorkSpaces productos creados a partir de un paquete público de Windows 7 ya no se podrán reconstruir. Es posible que desee considerar la posibilidad de migrar su Windows 7 WorkSpaces a Windows 10. Para obtener más información, consulte Migrar un WorkSpace.

Puede reconstruir un WorkSpace solo si se cumplen las siguientes condiciones:

- WorkSpace Debe tener un estado de`AVAILABLE`, `ERRORUNHEALTHY`,`STOPPED`, o`REBOOTING`. Para volver a crear un WorkSpace `REBOOTING` estado, debe usar la operación de RebuildWorkspacesAPI o el comando AWS CLI rebuild-workspaces.
- Debe existir una instantánea del volumen de usuario.

Para reconstruir un WorkSpace

> **Warning**
>
> Para reconstruir un cifrado WorkSpace, primero asegúrese de que la AWS KMS clave esté habilitada; de lo contrario, WorkSpace quedará inutilizable. Para determinar si una clave KMS está habilitada, consulte Mostrar detalles de clave KMS en la Guía para desarrolladores de AWS Key Management Service .

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione la WorkSpace que desea reconstruir y elija Acciones, Reconstruir o Restaurar WorkSpace.
4. En Instantánea, seleccione la marca de tiempo de la instantánea.
5. Elija Rebuild.

Para reconstruir un WorkSpace mediante el AWS CLI

Utilice el comando rebuild-workspaces.

Resolución de problemas

Si regenera un WorkSpace después de cambiar el atributo de nombre de AccountName usuario SaM del usuario en Active Directory, es posible que reciba el siguiente mensaje de error:

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

Para solucionar este problema, vuelva al atributo de nombre de usuario original y, a continuación, reinicie la reconstrucción o cree uno nuevo WorkSpace para ese usuario.

Restaurar un espacio de trabajo

La restauración de un WorkSpace vuelve a crear tanto el volumen raíz como el volumen de usuario, basándose en las instantáneas más recientes de estos volúmenes que se crearon cuando el WorkSpace estaba en buen estado. Al restaurar un WorkSpace se borran menos datos que al reconstruirlo. Sin embargo, es necesario tener instantáneas tanto del volumen raíz como del volumen de usuario, mientras que para reconstruir un WorkSpace solo se necesita una instantánea del volumen de usuario. Para reconstruir un WorkSpace, consulte Reconstruir un WorkSpace.

La restauración de un espacio de trabajo tiene las siguientes consecuencias:

- El volumen raíz (para Microsoft Windows, unidad C; para Linux,/) se restaura a la instantánea más reciente. Se perderán todas las aplicaciones que se instalaron o la configuración del sistema que se modificó después de crear la instantánea más reciente.
- El volumen de usuario (para Microsoft Windows, la unidad D; para Linux, /home) se vuelve a crear a partir de la instantánea más reciente. El contenido actual del volumen de usuario se sobrescribe.

Cuando hay que hacer instantáneas

Las instantáneas del volumen raíz y de usuario se toman de la siguiente manera. Cuando se selecciona Acciones, Reconstruir / Restaurar WorkSpace, se muestran la fecha y la hora de las instantáneas más recientes.

- Tras la creación de un WorkSpace: Normalmente, las instantáneas iniciales de los volúmenes raíz y de usuario se toman poco después de la creación de un WorkSpace (a menudo en 30 minutos). En algunas regiones de AWS, es posible que se tarden varias horas en tomar las instantáneas iniciales después de crear un WorkSpace.

Si un WorkSpace deja de funcionar correctamente antes de tomar las instantáneas iniciales, el WorkSpace no se podrá restaurar. En ese caso, puede intentar reconstruir el WorkSpace o ponerse en contacto con el soporte de AWS para obtener ayuda.

- Durante el uso regular: las instantáneas automáticas para restaurar un WorkSpace se programan cada 12 horas. Si el escritorio de WorkSpaces está en buen estado, las instantáneas del volumen raíz y del volumen de usuario se crean al mismo tiempo. Si el WorkSpace no está en buen estado, se crean instantáneas solo para el volumen de usuario.
- Después de restaurar un WorkSpace: Cuando restaura un WorkSpace, se toman nuevas instantáneas poco después de finalizar la restauración (normalmente en 30 minutos). En algunas regiones de AWS, es posible que se tarden varias horas en tomar estas instantáneas después de restaurar un WorkSpace.

  Después de restaurar un WorkSpace, si este deja de estar en buen estado antes de que se puedan tomar nuevas instantáneas, el WorkSpace no se podrá restaurar de nuevo. En ese caso, puede intentar reconstruir el WorkSpace o ponerse en contacto con el soporte de AWS para obtener ayuda.

Solo se puede restaurar un WorkSpace si se cumplen las siguientes condiciones:

- El estado del WorkSpace debe ser `AVAILABLE`, `ERROR`, `UNHEALTHY`, o `STOPPED`.
- Deben existir instantáneas de los volúmenes raíz y de usuario.

Para restaurar un WorksSpace

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione el WorkSpace a restaurar y elija Acciones, Reconstruir/Restaurar WorkSpaces.
4. En Instantánea, seleccione la marca de tiempo de la instantánea.
5. Elija Restore (Restaurar).

Para restaurar un espacio de trabajo mediante la AWS CLI

Utilice el comando restore-workspace.

Traiga su propia licencia (BYOL) de Microsoft 365

Amazon te WorkSpaces permite traer tus propias licencias de Microsoft 365 si cumplen con los requisitos de licencia de Microsoft. Estas licencias le permiten instalar y activar aplicaciones de Microsoft 365 para software empresarial WorkSpaces que funcione con los siguientes sistemas operativos:

- Windows 10 (Traiga su propia licencia)
- Windows 10 (Traiga su propia licencia)
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Para usar Microsoft 365 Apps for Enterprise en WorkSpaces, debes tener una suscripción a Microsoft 365 E3/E5, Microsoft 365 A3/A5 o Microsoft 365 Business Premium.

En Amazon, WorkSpaces puedes usar tus licencias de Microsoft 365 para instalar y activar las aplicaciones de Microsoft 365 para empresas, incluidas las siguientes:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

Para obtener más información, consulte la lista completa de aplicaciones de Microsoft 365 para empresas.

También puede instalar aplicaciones de Microsoft no incluidas en Microsoft 365, como Microsoft Project, Microsoft Visio y Microsoft Power Automate, WorkSpaces pero necesita incorporar sus propias licencias adicionales.

Puede instalar y usar Microsoft 365 y otras aplicaciones de Microsoft en la versión principal WorkSpaces y en la conmutación por error WorkSpaces mediante Multi-Region Resilience.

Contenido

Cree WorkSpaces con Microsoft 365 Apps para empresas

Para crear WorkSpaces con Microsoft 365 Apps for enterprise, debe crear una imagen personalizada con las aplicaciones instaladas y utilizarla para crear un paquete personalizado. Puede usar el paquete para lanzar nuevas aplicaciones WorkSpaces que tengan las aplicaciones instaladas. WorkSpaces no proporciona paquetes públicos con Microsoft 365 Apps para empresas.

Para crear WorkSpaces con Microsoft 365 Apps para empresas:

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. Inicie una WorkSpace que desee usar como imagen para otra aplicación de Microsoft WorkSpaces. Aquí es donde instalará las aplicaciones de Microsoft. Para obtener más información sobre el lanzamiento de un WorkSpace, consulte Iniciar un escritorio virtual mediante WorkSpaces.
3. Inicie la aplicación cliente en https://clients.amazonworkspaces.com/, introduzca el código de registro que aparece en el correo electrónico de invitación y seleccione Registrar.
4. Cuando se le solicite iniciar sesión, introduzca las credenciales de inicio de sesión del usuario y, a continuación, seleccione Iniciar sesión.
5. Instala y configura tus aplicaciones de Microsoft 365 para empresas.
6. Cree una imagen personalizada a partir WorkSpace de y úsela para crear un paquete personalizado. Para obtener más información sobre la creación de imágenes y paquetes personalizados, consulte Crear una WorkSpaces imagen y un paquete personalizados.
7. WorkSpaces Lánzalo con el paquete personalizado que has creado. WorkSpaces Tienen instaladas las aplicaciones Microsoft 365 para empresas.

Migre sus aplicaciones actuales WorkSpaces para usar Microsoft 365 Apps para empresas

Si WorkSpaces no tiene una licencia de Microsoft OfficeAWS, puede instalar y configurar Microsoft 365 Apps for Enterprise en su WorkSpaces.

Si ya WorkSpaces tiene una licencia de Microsoft OfficeAWS, primero debe anular el registro de su licencia de Microsoft Office antes de instalar Microsoft 365 Apps for enterprise.

> **Important**
>
> La desinstalación de aplicaciones de Microsoft Office WorkSpaces no anula el registro de las licencias. Para evitar que se le cobren las licencias de Microsoft Office, anule el registro de las aplicaciones de WorkSpaces Microsoft Office AWS mediante una de las siguientes acciones:
>
> - Administrar aplicaciones (recomendado): puede desinstalar Microsoft Office 2016 y 2019 de su WorkSpaces. Para obtener más información, consulte Administrar aplicaciones. Tras la desinstalación, puede instalar Microsoft 365 Apps for Enterprise en su WorkSpaces.
> - Migrar un WorkSpace: puedes migrar un WorkSpace paquete a otro sin perder los datos del volumen de usuarios.
>   - Migre su paquete WorkSpaces a una imagen que no tenga una suscripción a Microsoft Office. Una vez completada la migración, puede instalar Microsoft 365 Apps for Enterprise en su WorkSpaces.
>   - O bien, cree una WorkSpaces imagen y un paquete personalizados que ya tengan Microsoft 365 Apps for Enterprise instaladas en la imagen y, a continuación, migre WorkSpaces los suyos a este nuevo paquete personalizado. Una vez completada la migración, WorkSpaces los usuarios pueden empezar a usar Microsoft 365 Apps for Enterprise.
>   - Para obtener más información sobre cómo migrar WorkSpaces, consulte Migrar un WorkSpace.

Actualice sus aplicaciones de Microsoft 365 para empresas en WorkSpaces

De forma predeterminada, los WorkSpaces que ejecutan el sistema operativo Microsoft Windows están configurados para recibir actualizaciones de Windows Update. Sin embargo, las actualizaciones de las aplicaciones de Microsoft 365 para empresas no están disponibles con Windows Update. Configure las actualizaciones para que se ejecuten automáticamente desde la CDN de Office o utilice Windows Server Update Services (WSUS) junto con Microsoft Configuration Manager para actualizar las aplicaciones de Microsoft 365 para empresas. Para obtener más información, consulte Administrar las actualizaciones de las aplicaciones de Microsoft 365 con Microsoft Configuration Manager. Para establecer la frecuencia de las actualizaciones de las

aplicaciones de Microsoft 365, especifique un canal de actualización y configúrelo en Current o Monthly Enterprise para cumplir con la política de WorkSpaces licencias de Microsoft 365.

Actualice Windows BYOL WorkSpaces

En su licencia Windows Bring Your Own License (BYOL) WorkSpaces, puede actualizar a una versión más reciente de Windows mediante el proceso de actualización local. Siga las instrucciones de este tema para hacerlo.

El proceso de actualización local se aplica únicamente a Windows 10 y 11 BYOL. WorkSpaces

> **Important**
>
> No ejecute Sysprep en una versión actualizada. WorkSpace Si lo hace, podría producirse un error que impide que Sysprep termine. Si planea ejecutar Sysprep, hágalo únicamente en un sistema WorkSpace que no se haya actualizado.

> **Note**
>
> Puede usar este proceso para actualizar Windows 10 y 11 WorkSpaces a una versión más reciente. Sin embargo, este proceso no se puede utilizar para actualizar Windows 10 WorkSpaces a Windows 11.

Contenido

Requisitos previos

- Si has aplazado o pausado las actualizaciones de Windows 10 y 11 mediante una política de grupo o System Center Configuration Manager (SCCM), habilita las actualizaciones del sistema operativo para Windows 10 y 11. WorkSpaces
- Si WorkSpace es una AutoStop WorkSpace, cámbiela por una AlwaysOn WorkSpace anterior al proceso de actualización local para que no se detenga automáticamente mientras se aplican las actualizaciones. Para obtener más información, consulte Modificar el modo de ejecución. Si prefieres mantener el tiempo WorkSpace establecido AutoStop, cambia el AutoStop tiempo a tres horas o más mientras se lleva a cabo la actualización.
- El proceso de actualización in situ vuelve a crear el perfil de usuario realizando una copia de un perfil especial denominado Default User (Usuario predeterminado) (`C:\Users\Default`). No utilice este perfil de usuario predeterminado para realizar personalizaciones. Se recomienda realizar cualquier personalización en el perfil de usuario a través de objetos de política de grupo (GPO) en su lugar. Las personalizaciones realizadas a través de los GPO se pueden modificar o revertir de forma sencilla y son menos propensas a errores.
- El proceso de actualización local sólo permite realizar una copia de seguridad y volver a crear un perfil de usuario. Si tiene varios perfiles de usuario en la unidad D, elimine todos los perfiles excepto el que necesita.

Consideraciones

El proceso de actualización local utiliza dos scripts de registro (`enable-inplace-upgrade.ps1yupdate-pvdrivers.ps1`) para realizar los cambios necesarios WorkSpaces que permitan la ejecución del proceso de Windows Update. Estos cambios implican la creación de un perfil de usuario (temporal) en la unidad C en lugar de en la unidad D. Si ya existe un perfil de usuario en la unidad D, los datos de ese perfil de usuario original permanecen en la unidad D.

De forma predeterminada, WorkSpaces crea el perfil de usuario en`D:\Users\%USERNAME%`. El script `enable-inplace-upgrade.ps1` configura Windows para crear un nuevo perfil de usuario en `C:\Users\%USERNAME%` y redirige las carpetas del shell de usuario a `D:\Users\%USERNAME%`. Este nuevo perfil de usuario se crea cuando un usuario se registra por primera vez.

Después de la actualización local, tiene la opción de dejar sus perfiles de usuario en la unidad C para permitir a los usuarios utilizar el proceso de Windows Update para actualizar sus equipos en el futuro. Sin embargo, tenga en cuenta que WorkSpaces los perfiles almacenados en la unidad C no

se pueden reconstruir ni migrar sin perder todos los datos del perfil del usuario, a menos que haga una copia de seguridad de esos datos y los restaure usted mismo. Si decide dejar los perfiles en la unidad C, puede utilizar la clave de UserShellFoldersRedirectionregistro para redirigir las carpetas del shell de usuario a la unidad D, como se explica más adelante en este tema.

Para asegurarse de que puede reconstruir o migrar sus carpetas WorkSpaces y evitar posibles problemas con la redirección de carpetas del shell de usuario, le recomendamos que devuelva sus perfiles de usuario a la unidad D tras la actualización inmediata. Para ello, utilice la clave de registro PostUpgradeRestoreProfileOnD, tal y como se explica más adelante en este tema.

Limitaciones conocidas

- El cambio de ubicación del perfil de usuario de la unidad D a la unidad C no se produce durante las WorkSpace recompilaciones o migraciones. Si realiza una actualización local en una BYOL de Windows 10 u 11 WorkSpace y, a continuación, la reconstruye o migra, la nueva WorkSpace tendrá el perfil de usuario en la unidad D.

  > **Warning**
  >
  > Si deja el perfil de usuario en la unidad C después de la actualización local, los datos del perfil de usuario almacenados en la unidad C se perderán cuando se vuelvan a crear o migrar los escritorios a no ser que haga una copia de seguridad manual de los datos del perfil de usuario antes de realizar estas operaciones y, a continuación, restaure manualmente los datos del perfil de usuario después de volver a crear o migrar los escritorios.

- Si el paquete BYOL predeterminado contiene una imagen basada en una versión anterior de Windows 10 y 11, debe volver a realizar la actualización local una vez reconstruida o migrada. WorkSpace

Resumen de la configuración de la clave del Registro

Para habilitar el proceso de actualización local y especificar dónde desea que se encuentre el perfil de usuario después de la actualización, debe establecer una serie de claves de registro.

Ruta de registro: HKL M:\Software\Amazon\WorkSpacesConfig\ .ps1 enable-inplace-upgrade

Clave del Registro	Tipo	Valores
Enabled (Habilitado)	DWORD	0: (opción predeterminada) Desactiva la actualización local 1: Habilita la actualización local
PostUpgradeRestoreProfileOnD	DWORD	0: (opción predeterminada) No intenta restaurar la ruta del perfil de usuario tras la actualización local 1 — Restaura la ruta del perfil de usuario (ProfileImagePath) tras la actualización in situ
UserShellFoldersRedirection	DWORD	0: No habilita el redirecci onamiento de carpetas de intérprete de comandos de usuario 1: (opción predeterminada) Habilita el redireccionamiento de las carpetas del intérpret e de comandos de usuario a `D:\Users\%USERNAME%` que el perfil de usuario se regenere en `C:\Users\%USERNAME%`
NoReboot	DWORD	0: (opción predeterminada) Le permite controlar cuándo se produce un reinicio tras modificar el registro del perfil de usuario.

Clave del Registro	Tipo	Valores
		1 — No permite que el script se reinicie WorkSpace tras modificar el registro del perfil de usuario

Ruta de registro: HKL M:\Software\Amazon\WorkSpacesConfig\ update-pvdrivers.ps1

Clave del Registro	Tipo	Valores
Enabled (Habilitado)	DWORD	0: (predeterminado) Desactiva la actualización de los controladores fotovoltaicos AWS 1 — Permite la actualización de los controladores AWS fotovoltaicos

Realizar una actualización local

Para habilitar las actualizaciones locales de Windows en su BYOL WorkSpaces, debe configurar determinadas claves de registro, tal y como se describe en el siguiente procedimiento. También debe configurar determinadas claves del registro para indicar la unidad (C o D) en la que desea que se encuentren los perfiles de usuario una vez finalizadas las actualizaciones locales.

Puede realizar estos cambios en el Registro manualmente. Si tiene varias que WorkSpaces actualizar, puede usar la política de grupo o SCCM para insertar un script. PowerShell Para ver un ejemplo de PowerShell script, consulteActualice el WorkSpace registro mediante un script PowerShell .

Para realizar una actualización local de Windows 10 y 11

1. Anote qué versión de Windows se está ejecutando actualmente en el BYOL de Windows 10 y 11 WorkSpaces que está actualizando y, a continuación, reinícielo.

2. Actualice las siguientes claves del Registro del sistema de Windows para cambiar los datos del valor de Habilitado de 0 a 1. Estos cambios en el registro permiten actualizar in situ el. WorkSpace

   - HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ update-pvdrivers.ps1 WorkSpacesConfig

   > **Note**
   >
   > Si estas claves no existen, reinicie el. WorkSpace Las claves deben añadirse cuando se reinicia el sistema.

   (Opcional) Si utiliza un flujo de trabajo administrado como secuencias de tareas de SCCM para realizar la actualización, establezca el siguiente valor de clave en 1 para evitar que el equipo se reinicie:

   HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. Determine en qué unidad desea que se encuentren los perfiles de usuario tras el proceso de actualización local (para obtener más información, consulte Consideraciones) y configure las claves de registro como se indica a continuación:

   - Configuración si desea el perfil de usuario en la unidad C después de la actualización:

     HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     Nombre clave PostUpgradeRestoreProfileOn: D

     Valor de la clave: 0

     Nombre de clave: UserShellFoldersRedirection

     Valor de la clave: 1

   - Configuración si desea el perfil de usuario en la unidad D después de la actualización:

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

Nombre clave PostUpgradeRestoreProfileOn: D

Valor de la clave: 1

Nombre de clave: UserShellFoldersRedirection

Valor de la clave: 0

4. Tras guardar los cambios en el registro, reinícielo de WorkSpace nuevo para que se apliquen los cambios.

> **Note**
>
> - Tras el reinicio, al iniciar sesión se WorkSpace crea un nuevo perfil de usuario. Es posible que vea iconos de marcador de posición en el menú Inicio. Este comportamiento se resuelve automáticamente después de que se haya completado la actualización in situ.
> - Espere 10 minutos para asegurarse de que WorkSpace está desbloqueado.

(Opcional) Confirme que el siguiente valor clave esté establecido en 1, lo que desbloquea la actualización WorkSpace :

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ Eliminado WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. Realice la actualización in situ. Puede utilizar el método que prefiera; por ejemplo, SCCM, ISO o Windows Update (WU). En función de la versión original de Windows 10 y 11 y del número de aplicaciones instaladas, este proceso puede tardar entre 40 y 120 minutos.

> **Note**
>
> El proceso de actualización local puede tardar al menos una hora. Es posible que el estado de la WorkSpace instancia aparezca igual que `UNHEALTHY` durante la actualización.

6. Una vez finalizado el proceso de actualización, confirme que la versión de Windows se ha actualizado.

   > **Note**
   >
   > Si se produce un error en la actualización local, Windows vuelve a utilizar automáticamente la versión de Windows 10 y 11 que estaba vigente antes de iniciar la actualización. Para obtener más información sobre solución de problemas, consulte la documentación de Microsoft.

   (Opcional) Para confirmar que los scripts de actualización se han ejecutado correctamente, verifique que el valor de la clave siguiente se ha establecido en 1:

   HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. Si modificó el modo de ejecución configurándolo AlwaysOn o WorkSpace cambiando el período de AutoStop tiempo para que el proceso de actualización in situ pudiera ejecutarse sin interrupciones, devuelva el modo de ejecución a su configuración original. Para obtener más información, consulte Modificar el modo de ejecución.

Si no ha establecido la clave de registro PostUpgradeRestoreProfileOnD en 1, Windows regenera el perfil de usuario y lo coloca `C:\Users\%USERNAME%` después de la actualización local, de modo que no tenga que volver a realizar los pasos anteriores para futuras actualizaciones in situ de Windows 10 y 11. De forma predeterminada, el script `enable-inplace-upgrade.ps1` redirige las siguientes carpetas del shell a la unidad D:

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts`

- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

Si redirige las carpetas del shell a otras ubicaciones de su ordenador WorkSpaces, lleve a cabo las operaciones necesarias WorkSpaces después de las actualizaciones locales.

Solución de problemas

Si se produce algún problema con la actualización, puede comprobar los siguientes elementos para solucionarlo:

- Logs de Windows, que se encuentran, de forma predeterminada, en las ubicaciones siguientes:

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`
- Visor de eventos de Windows

  Registros de Windows > Aplicación > Fuente: Amazon WorkSpaces

> **Tip**
>
> Durante el proceso de actualización in situ, si observa que algunos atajos de iconos en el escritorio ya no funcionan, es porque WorkSpaces mueve los perfiles de usuario ubicados en la unidad D a la unidad C para preparar la actualización. Cuando finalice la actualización, los accesos directos funcionarán según lo previsto.

Actualice el WorkSpace registro mediante un script PowerShell

Puede utilizar el siguiente PowerShell script de ejemplo para actualizar el registro y WorkSpaces permitir las actualizaciones locales. Siga las instruccionesRealizar una actualización local, pero utilice este script para actualizar el registro de cada una de ellas WorkSpace.

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
```

```
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

Migrar un WorkSpace

> **Note**
>
> Si desea cancelar la suscripción o desinstalar las licencias de las versiones de Microsoft Office AWS desde su cuenta WorkSpace, le recomendamos que utilice Administrar aplicaciones.

Puede migrar un WorkSpace paquete a otro y, al mismo tiempo, conservar los datos del volumen de usuarios. A continuación se presentan algunos ejemplos:

- Puede migrar WorkSpaces de la experiencia de escritorio de Windows 7 a la experiencia de escritorio de Windows 10.
- Puede migrar WorkSpaces del protocolo PCoIP al Protocolo de WorkSpaces Transmisión (WSP).
- Puede migrar WorkSpaces del paquete de 32 bits con tecnología Microsoft Office en Windows Server 2016 a los WorkSpaces paquetes con tecnología Microsoft Office en Windows Server 2019 y Windows Server 2022 de 64 bits. WorkSpaces
- Puede migrar WorkSpaces de un paquete público o personalizado a otro. Por ejemplo, puedes migrar desde una versión con GPU (Graphics.G4DN). GraphicsProLos paquetes.g4dn, Graphics y GraphicsPro) a paquetes no compatibles con la GPU, o en la otra dirección.
- Puede migrar WorkSpaces del BYOL de Windows 10 al BYOL de Windows 11, pero no se admite la migración de Windows 11 a Windows 10.
- Los paquetes de valores no son compatibles con Windows 11. Para migrar tu paquete económico de Windows 7 o 10 WorkSpaces a Windows 11, primero debes cambiar tu paquete Value WorkSpaces a un paquete más grande.

- Antes WorkSpaces de migrar de Windows 7 a Windows 11, debes migrarlo a Windows 10. Inicie sesión en Windows 10 al WorkSpace menos una vez antes de migrarlo a Windows 11. No se admite la migración de Windows 7 WorkSpaces directamente a Windows 11.
- Puede migrar los Windows WorkSpaces que utilizan Microsoft Office AWS a un WorkSpaces paquete personalizado con aplicaciones de Microsoft 365. Tras la migración, WorkSpaces se cancelará la suscripción a Microsoft Office.
- Puede migrar los Windows WorkSpaces que utilizan Microsoft Office AWS a un WorkSpaces paquete sin suscripción a Office 2016/2019. Tras la migración, WorkSpaces se cancelará la suscripción a Microsoft Office.

Para obtener más información sobre los WorkSpaces paquetes de Amazon, consultaWorkSpace paquetes e imágenes.

El proceso de migración recrea el volumen raíz WorkSpace utilizando un nuevo volumen raíz de la imagen del paquete de destino y el volumen de usuario de la última instantánea disponible del original. WorkSpace Se genera un nuevo perfil de usuario durante la migración para una mejor compatibilidad. Se cambia el nombre del perfil de usuario antiguo y, a continuación, ciertos archivos del perfil de usuario antiguo se transfieren al nuevo perfil de usuario. (Para obtener más información sobre lo que se transfiere, consulte Qué ocurre durante la migración.)

El proceso de migración tarda hasta una hora cada WorkSpace uno. Al iniciar el proceso de migración, WorkSpace se crea uno nuevo. Si se produce un error que impide que la migración WorkSpace se realice correctamente, el original se recupera y vuelve a su estado original, y el nuevo WorkSpace finaliza.

Contenido

Límites de migración

- No puede migrar a un paquete de experiencia de escritorio de Windows 7 público o personalizado. Tampoco puede migrar a paquetes de Windows 7 Bring Your Own License (BYOL).
- WorkSpaces Solo puede migrar BYOL a otros paquetes de BYOL. Para migrar un BYOL WorkSpace de PCoIP a WSP, primero debe crear un paquete BYOL con el protocolo WSP. A continuación, puede migrar su BYOL de PCoIP a ese paquete BYOL de WSP. WorkSpaces
- No puede migrar un paquete WorkSpace creado a partir de paquetes públicos o personalizados a un paquete BYOL.
- Por el momento, Graphics.g4dn, GraphicsPro .g4dn, Graphics y los GraphicsPro bundles solo están disponibles para el protocolo PCoIP, por lo que Graphics.g4dn, .g4dn y Graphics no se pueden migrar a WSP todavía. GraphicsPro GraphicsPro WorkSpaces
- Actualmente WorkSpaces , no se admite la migración de Linux.
- En AWS las regiones que admiten más de un idioma, puede migrar WorkSpaces entre paquetes de idiomas.
- Los paquetes de origen y destino deben ser diferentes. (Sin embargo, en las regiones que admiten más de un idioma, puede migrar al mismo paquete de Windows 10 siempre que los idiomas sean diferentes). Si quiere actualizar el paquete WorkSpace con el mismo paquete, reconstruya el paquete WorkSpace en su lugar.
- No puede migrar de una WorkSpaces región a otra.
- En algunos casos, si la migración no puede realizarse correctamente, es posible que no reciba un mensaje de error y que parezca que el proceso de migración no se inició. Si el WorkSpace paquete permanece igual una hora después de intentar la migración, la migración no se realizará correctamente. Póngase en contacto con el Centro de AWS Support para obtener ayuda.

Escenarios de migración

En la siguiente tabla se muestran las situaciones de migración disponibles:

SO de origen	SO de destino	¿Disponible?
Paquete público o personalizado de Windows 7	Paquete público o personalizado de Windows 10	Sí

SO de origen	SO de destino	¿Disponible?
Paquete personalizado de Windows 7	Paquete público de Windows 7	No
Paquete personalizado de Windows 7	Paquete personalizado de Windows 7	No
Paquete público de Windows 7	Paquete personalizado de Windows 7	No
Paquete público o personalizado de Windows 10	Paquete público o personalizado de Windows 7	No
Paquete público o personalizado de Windows 10	Paquete personalizado de Windows 10	Sí
Paquete BYOL de Windows 7	Paquete BYOL de Windows 7	No
Paquete BYOL de Windows 7	Paquete BYOL de Windows 10	Sí
Paquete BYOL de Windows 10	Paquete BYOL de Windows 7	No
Paquete BYOL de Windows 10	Paquete BYOL de Windows 10	Sí
Paquete público de Windows 10 con Windows Server 2016	Paquete público de Windows 10 con Windows Server 2019 	Sí
Paquete público de Windows 10 con Windows Server 2019 	Paquete público de Windows 10 con Windows Server 2016	Sí

SO de origen	SO de destino	¿Disponible?
Paquete BYOL de Windows 10	Paquete BYOL de Windows 11	Sí
Paquete BYOL de Windows 11	Paquete BYOL de Windows 10	No
Paquete personalizado de Windows 10 con Windows Server 2016	Paquete público de Windows 10 con Windows Server 2019	Sí
Paquete personalizado de Windows 10 con Windows Server 2016	Paquete público de Windows 10 con Windows Server 2022	Sí
Paquete personalizado de Windows 10 con Windows Server 2019	Paquete público de Windows 10 con Windows Server 2022	Sí

Note

El acceso web no está disponible para la versión PCoIP del paquete público de Windows 10 con Windows Server 2019.

Important

El paquete público de Windows 10 plus con Windows Server 2016 incluye Microsoft Office 2016 y Trend Micro Worry-Free Business Security Services. El paquete público de Windows 10 plus con Windows Server 2019 incluye Microsoft Office 2019, pero no incluye Trend Micro Worry-Free Business Security Services.

Qué ocurre durante la migración

Durante la migración, se conservan los datos del volumen de usuario (unidad D), pero se pierden todos los datos del volumen raíz (unidad C). Esto significa que no se conserva ninguna de las aplicaciones, configuraciones ni cambios instalados en el registro. Se cambia el nombre de la carpeta de perfil de usuario anterior con el sufijo `.NotMigrated` y se crea un nuevo perfil de usuario.

El proceso de migración vuelve a crear la unidad D basándose en la última instantánea del volumen de usuario original. Durante el primer arranque del nuevo WorkSpace, el proceso de migración mueve la `D:\Users\%USERNAME%` carpeta original a una carpeta denominada`D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. El nuevo sistema operativo genera una nueva carpeta `D:\Users\%USERNAME%\`.

Después de crear el nuevo perfil de usuario, los archivos de las siguientes carpetas de shell de usuario se mueven del perfil antiguo `.NotMigrated` al nuevo perfil:

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

Important

El proceso de migración intenta transferir los archivos del perfil de usuario antiguo al nuevo perfil. Los archivos que no se transfirieron durante la migración permanecen en la carpeta `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Si la migración se realiza correctamente, puede ver qué archivos se transfirieron en `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. Puede transferir manualmente cualquier archivo que no se haya movido automáticamente.

De forma predeterminada, los paquetes públicos tienen deshabilitada la indexación de búsquedas locales. Si lo habilita, el valor predeterminado es buscar `C:\Users` y no `D:\Users`, por lo que también debe ajustarlo. Si ha configurado la indexación de búsqueda local específicamente para `D:\Users\`*`username`* y no para `D:\Users`, es

posible que la indexación de búsqueda local no funcione después de la migración para los archivos de usuario que estén en la carpeta `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`.

Todas las etiquetas asignadas a la original se WorkSpace conservan durante la migración y WorkSpace se conserva el modo de ejecución de la. Sin embargo, el nuevo WorkSpace recibe un WorkSpace identificador, un nombre de equipo y una dirección IP nuevos.

Prácticas recomendadas

Antes de migrar un WorkSpace, haga lo siguiente:

- Realice una copia de seguridad de los datos importantes de la unidad C en otra ubicación. Todos los datos de la unidad C se borrarán durante la migración.
- Asegúrese de WorkSpace que la migración tenga al menos 12 horas de antigüedad para asegurarse de que se ha creado una instantánea del volumen de usuarios. En la WorkSpaces página Migrate de la WorkSpaces consola de Amazon, puedes ver la hora de la última instantánea. Los datos creados después de la última instantánea se pierden durante la migración.
- Para evitar una posible pérdida de datos, asegúrate de que tus usuarios cierren la sesión WorkSpaces y no la vuelvan a iniciar hasta que finalice el proceso de migración. Tenga en cuenta que WorkSpaces no se pueden migrar cuando están en `ADMIN_MAINTENANCE` modo.
- Asegúrese de que el estado que WorkSpaces desea migrar sea `AVAILABLE`, `STOPPED`, o`ERROR`.
- Asegúrese de tener suficientes direcciones IP para la WorkSpaces que está migrando. Durante la migración, se asignarán nuevas direcciones IP a. WorkSpaces
- Si utiliza scripts para migrar WorkSpaces, migre los archivos en lotes de no más de 25 WorkSpaces a la vez.

Solución de problemas

- Si los usuarios le informan de que faltan archivos después de la migración, compruebe si sus archivos de perfil de usuario no se movieron durante el proceso de migración. Puede ver qué archivos se han movido en `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`. Los archivos que no se han movido se ubicarán en la carpeta `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`. Puede transferir manualmente cualquier archivo que no se haya movido automáticamente.

- Si utilizas la API para migrar WorkSpaces y la migración no se realiza correctamente, no se utilizará el WorkSpace ID de destino devuelto por la API y se WorkSpace conservará el WorkSpace ID original.
- Si una migración no se finaliza correctamente, compruebe el Active Directory para ver si se limpió en consecuencia. Es posible que tengas WorkSpaces que eliminar manualmente lo que ya no necesitas.

Cómo se ve afectada la facturación

Durante el mes en que se produce la migración, se le cobrarán importes prorrateados tanto para la nueva como para la original WorkSpaces. Por ejemplo, si migra WorkSpace A a WorkSpace B el 10 de mayo, se le cobrará por WorkSpace A del 1 al 10 de mayo y se le cobrará por WorkSpace B del 11 al 30 de mayo.

> **Note**
>
> Si va a migrar WorkSpace A a un tipo de paquete diferente (por ejemplo, de rendimiento a potencia o económico a estándar), el tamaño del volumen raíz (unidad C) y del volumen de usuarios (unidad D) podría aumentar durante el proceso de migración. Si es necesario, el volumen raíz aumenta para que coincida con el tamaño predeterminado del volumen raíz para el nuevo paquete. Sin embargo, si ya había especificado un tamaño diferente (mayor o menor) para el volumen de usuario que el predeterminado para el paquete original, ese mismo tamaño de volumen de usuario se conservará durante el proceso de migración. De lo contrario, el proceso de migración utiliza el volumen de WorkSpace usuarios de origen que sea mayor y el tamaño de volumen de usuarios predeterminado para el nuevo paquete.

Migración de un WorkSpace

Puedes migrar WorkSpaces a través de la WorkSpaces consola de Amazon, la AWS CLI o la WorkSpaces API de Amazon.

Para migrar un WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione su WorkSpace y elija Acciones, Migrar WorkSpaces.

4. En Paquetes, selecciona el paquete al que quieres WorkSpace migrar.

> **Note**
>
> Para migrar un BYOL WorkSpace de PCoIP a WSP, primero debe crear un paquete BYOL con el protocolo WSP. A continuación, puede migrar su BYOL de PCoIP a ese paquete BYOL de WSP. WorkSpaces

5. WorkSpacesElija Migrar.

   `PENDING`Aparece una nueva WorkSpace con el estado de en la WorkSpaces consola de Amazon. Cuando finaliza la migración, la original WorkSpace finaliza y el estado de la nueva WorkSpace se establece en`AVAILABLE`.

6. (Opcional) Para eliminar los paquetes e imágenes personalizados que ya no necesite, consulte Eliminar un WorkSpaces paquete o una imagen personalizados.

Para migrar WorkSpaces a través deAWS CLI, utilice el comando migrate-workspace. Para migrar WorkSpaces a través de la WorkSpaces API de Amazon, consulta MigrateWorkSpacela referencia de la WorkSpaces API de Amazon.

Eliminar WorkSpaces

Cuando ya no necesite una WorkSpace, puede eliminarlo. También puede eliminar los recursos relacionados.

> **Warning**
>
> Eliminar un WorkSpace es una acción permanente y no se puede deshacer. Los datos del usuario del Workspace no se conservan y se destruyen. Para obtener ayuda para realizar el backup de los datos de usuario, póngase en contacto con AWS Support.

> **Note**
>
> Tanto AD sencillo como Conector AD están disponibles de forma gratuita para su uso con WorkSpaces. Si no se utiliza WorkSpaces con su directorio AD sencillo o conector AD durante 30 días consecutivos, este directorio se dará de baja automáticamente para su

uso con Amazon WorkSpaces, y se le cobrará por este directorio según las condiciones de precios de AWS Directory Service.
Para eliminar directorios vacíos, consulte Eliminar el directorio de los escritorios WorkSpaces. Si elimina su directorio AD sencillo o conector AD, siempre puede crear uno nuevo cuando desee volver a utilizar WorkSpaces.

Para eliminar WorkSpaces

Puede eliminar un WorkSpace que se encuentre en cualquier estado excepto Suspendido.

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, seleccione WorkSpaces.
3. Seleccione su WorkSpace y seleccione Eliminar.
4. Cuando se le pida confirmación, elija Eliminar WorkSpace. Eliminar un WorkSpace tarda aproximadamente 5 minutos. Durante la eliminación, el estado del WorkSpace se establece en Terminando. Cuando se complete la eliminación, el WorkSpace desaparecerá de la consola.
5. (Opcional) Para eliminar paquetes e imágenes personalizados que no vaya a volver a usar, consulte Eliminar un WorkSpaces paquete o una imagen personalizados.
6. (Opcional) Una vez eliminados todos los escritorios WorkSpaces de un directorio, puede eliminar el directorio. Para obtener más información, consulte Eliminar el directorio de los escritorios WorkSpaces.
7. (Opcional) Después de eliminar todos los recursos de la nube virtual privada (VPC) para el directorio, puede eliminarla y liberar la dirección IP elástica utilizada para la gateway NAT. Para obtener más información, consulte Eliminar su VPC y Uso de direcciones IP elásticas en la Guía del usuario de Amazon VPC.

Para eliminar un WorkSpace con la AWS CLI

Utilice el comando terminate-workspaces.

WorkSpace paquetes e imágenes

Un WorkSpace paquete es una combinación de un sistema operativo y recursos de almacenamiento, cómputo y software. Al lanzar un paquete WorkSpace, selecciona el paquete que mejor se adapte a sus necesidades. Los paquetes predeterminados para los que están disponibles WorkSpaces se denominan paquetes públicos. Para obtener más información sobre los distintos paquetes públicos disponibles WorkSpaces, consulta Amazon WorkSpaces Bundles.

Si has lanzado un Windows o Linux WorkSpace y lo has personalizado, puedes crear una imagen personalizada a partir de él. WorkSpace

Una imagen personalizada contiene solo el sistema operativo, el software y la configuración del WorkSpace. Un paquete personalizado es una combinación de esa imagen personalizada y del hardware desde el que se WorkSpace puede lanzar una.

Tras crear una imagen personalizada, puede crear un paquete personalizado que combine la WorkSpace imagen personalizada y la configuración de almacenamiento e informática subyacente que seleccione. A continuación, puede especificar este paquete personalizado al lanzar un nuevo paquete WorkSpaces para garantizar que el nuevo WorkSpaces tenga la misma configuración uniforme (hardware y software).

Si necesitas realizar actualizaciones de software o instalar software adicional en el tuyo WorkSpaces, puedes actualizar tu paquete personalizado y usarlo para reconstruirlo WorkSpaces.

WorkSpaces es compatible con varios sistemas operativos (SO), protocolos de streaming y paquetes diferentes. La siguiente tabla proporciona información sobre las licencias, los protocolos de transmisión y los paquetes compatibles con cada sistema operativo.

Sistema operativo	Licencias	Protocolos de transmisión	Paquetes compatibles	Política de ciclo de vida o fecha de jubilación
Windows Server 2016	Incluido	WSP, PCoIP	Valor, estándar, rendimiento, potencia, gráficos (obsoletos) PowerPro, gráficos. G4dn, GraphicsPro .g4dn GraphicsPro	12 de enero de 2027

Sistema operativo	Licencias	Protocolos de transmisión	Paquetes compatibles	Política de ciclo de vida o fecha de jubilación
Windows Server 2019	Incluido	WSP, PCoIP	Valor, estándar, rendimiento, potencia, gráficos (obsoletos) PowerPro, gráficos. G4dn, GraphicsPro .g4dn GraphicsPro	9 de enero de 2029
Windows Server 2022	Incluido	WSP, PCoIP	Estándar, rendimiento, potencia, gráficos (obsoletos) PowerPro, gráficos. G4dn, GraphicsPro .g4dn GraphicsPro	14 de octubre de 2013
Windows 10	Traiga su propia licencia (BYOL)	WPS, PCoIP	Valor, estándar, rendimiento, potencia, gráficos (obsoletos) PowerPro, gráficos. G4dn, GraphicsPro .g4dn GraphicsPro	¿En soporte
Windows 11	Traiga su propia licencia (BYOL)	AVISPA	Estándar, rendimiento, potencia, PowerPro	En apoyo
Amazon Linux 2	Incluido	WSP, PCoIP	Valor, estándar, rendimiento, potencia, PowerPro	30 de junio de 2025
Ubuntu 22.04 LTS	Incluido	AVISPA	Valor, estándar, rendimiento, potencia, gráficos. G4dn PowerPro, .g4dn GraphicsPro	Junio de 2032

> **Note**
>
> - No se garantiza que las versiones del sistema operativo que el vendedor ya no admite funcionen ni cuentan con AWS soporte técnico.
> - Para WorkSpaces ejecutarse en el sistema operativo Windows, los paquetes de gráficos solo admiten el protocolo de transmisión PCoIP.

Contenido

Opciones de paquete

Antes de seleccionar un paquete, asegúrese de que el paquete que desea seleccionar sea compatible con el protocolo, el sistema operativo, la red y el tipo de procesamiento de sus WorkSpaces. Para obtener más información, consulte Protocolos de Amazon WorkSpaces. Para obtener más información sobre las redes, consulte los requisitos de redes de los clientes de Amazon WorkSpaces.

> **Note**
>
> - Recomendamos no superar la latencia de red máxima de 250 ms para los WorkSpaces de PCoIP. Para obtener la mejor experiencia de usuario de PCoIP WorkSpaces, recomendamos mantener la latencia de la red por debajo de 100 ms. Cuando el tiempo de ida y vuelta (RTT) supere los 375 ms, la conexión del cliente de WorkSpaces se apagará. Para obtener la mejor experiencia de usuario del WorkSpaces Streaming Protocol (WSP), recomendamos mantener el RTT por debajo de 250 ms. Si el RTT está entre

250 ms y 400 ms, el usuario puede acceder al WorkSpace, pero el rendimiento disminuirá significativamente.

- Recomendamos probar el rendimiento de los paquetes que desee elegir en un entorno de prueba mediante la ejecución y el uso de aplicaciones que repliquen las tareas diarias de los usuarios.

Important

- El paquete de Graphics dejará de ser compatible a partir del 30 de noviembre de 2023. Recomendamos cambiar al paquete Graphics.g4dn para WorkSpaces mediante el paquete Graphics.
- Los paquetes Graphics y GraphicsPro no están disponibles actualmente en la región Asia-Pacífico (Mumbai).

A continuación se indican los paquetes que ofrece WorkSpaces. Para obtener más información sobre los paquetes disponibles en WorkSpaces, consulte Paquetes de Amazon WorkSpaces.

Paquete de valor

Este paquete está especialmente indicado para lo siguiente:

- Edición básica de texto y entrada de datos
- Navegación web con poco uso
- Mensajería instantánea

Este paquete no se recomienda para el procesamiento de textos, las conferencias de audio y vídeo, el uso compartido de pantalla, las herramientas de desarrollo de software, las aplicaciones de inteligencia empresarial y las aplicaciones gráficas.

Paquete estándar

Este paquete está especialmente indicado para lo siguiente:

- Edición básica de texto y entrada de datos
- Navegación web

- Mensajería instantánea
- Email

Este paquete no se recomienda para las conferencias de audio y vídeo, el uso compartido de pantalla, el procesamiento de textos, las herramientas de desarrollo de software, las aplicaciones de inteligencia empresarial y las aplicaciones gráficas.

Paquete de rendimiento

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Mensajería instantánea
- Email
- Hojas de cálculo
- Procesamiento de audio
- Material didáctico

Este paquete no se recomienda para las conferencias de vídeo, el uso compartido de pantalla, las herramientas de desarrollo de software, las aplicaciones de inteligencia empresarial y las aplicaciones gráficas.

Paquete de energía

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Email
- Mensajería instantánea
- Hojas de cálculo
- Procesamiento de audio
- Desarrollo de software (entorno de desarrollo integrado (IDE)
- Introducción al procesamiento de datos de nivel medio

- Conferencias de audio y vídeo

Este paquete no se recomienda para el uso compartido de pantalla, las herramientas de desarrollo de software, las aplicaciones de inteligencia empresarial y las aplicaciones gráficas.

Paquete PowerPro

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Email
- Mensajería instantánea
- Hojas de cálculo
- Procesamiento de audio
- Desarrollo de software (entorno de desarrollo integrado (IDE)
- Almacenes de datos
- Aplicaciones de inteligencia empresarial
- Conferencias de audio y vídeo

Este paquete no se recomienda para el machine learning, el entrenamiento de modelos y las aplicaciones gráficas.

Paquete GraphicsPro

Este paquete ofrece un nivel básico de rendimiento gráfico y un alto nivel de rendimiento de CPU y memoria para sus WorkSpaces. Está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Email
- Mensajería instantánea
- Hojas de cálculo
- Conferencias de audio
- Desarrollo de software (entorno de desarrollo integrado (IDE)

- Almacenes de datos
- Aplicaciones de inteligencia empresarial
- Diseño gráfico
- Procesamiento de imágenes

Este paquete no se recomienda para las conferencias de audio y vídeo, la renderización 3D y el diseño fotorrealista

Paquete Graphics.G4DN

Este paquete ofrece un nivel alto de rendimiento gráfico y un nivel moderado de rendimiento de CPU y memoria para sus WorkSpaces. Está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Email
- Hojas de cálculo
- Mensajería instantánea
- Conferencias de audio
- Desarrollo de software (entorno de desarrollo integrado (IDE)
- Introducción al procesamiento de datos de nivel medio
- Almacenes de datos
- Aplicaciones de inteligencia empresarial
- Diseño gráfico
- CAD/CAM (diseño asistido por ordenador/fabricación asistida por ordenador)

Este paquete no se recomienda para las conferencias de audio y vídeo, la renderización 3D, el diseño fotorrealista y el entrenamiento de modelos de machine learning.

GraphicsPro.g4dn

Paquete GraphicsPro.g4dn

Este paquete ofrece un nivel alto de rendimiento gráfico, rendimiento de CPU y memoria para sus WorkSpaces. Está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Email
- Hojas de cálculo
- Mensajería instantánea
- Conferencias de audio
- Desarrollo de software (entorno de desarrollo integrado (IDE)
- Introducción al procesamiento de datos de nivel medio
- Almacenes de datos
- Aplicaciones de inteligencia empresarial
- Diseño gráfico
- CAD/CAM (diseño asistido por ordenador/fabricación asistida por ordenador)
- Transcodificación de video
- Renderización 3D
- Diseño fotorrealista
- Streaming de videojuegos
- Entrenamiento con modelos de machine learning e inferencia de machine learning

Este paquete no se recomienda para las conferencias de audio y vídeo.

Crea una WorkSpaces imagen y un paquete personalizados

Si has lanzado un sistema Windows o Linux WorkSpace y lo has personalizado, puedes crear una imagen personalizada y paquetes personalizados a partir de ahí WorkSpace.

Una imagen personalizada contiene solo el sistema operativo, el software y la configuración del WorkSpace. Un paquete personalizado es una combinación de esa imagen personalizada y del hardware desde el que se WorkSpace puede lanzar una.

> **Note**
>
> Asegúrese de esperar al menos 2 horas después de eliminar un paquete antes de crear uno nuevo con el mismo nombre.

Después de crear una imagen personalizada, puede crear un paquete personalizado que combine la imagen personalizada y la configuración de computación y almacenamiento subyacente que seleccione. A continuación, puede especificar este paquete personalizado al lanzar un nuevo paquete WorkSpaces para garantizar que el nuevo WorkSpaces tenga la misma configuración coherente (hardware y software).

Puede utilizar la misma imagen personalizada para crear varios grupos personalizados seleccionando diferentes opciones de computación y almacenamiento para cada grupo.

Important

- Si piensa crear una imagen desde un sistema Windows 10 WorkSpace, tenga en cuenta que la creación de imágenes no es compatible con los sistemas Windows 10 que se hayan actualizado de una versión de Windows 10 a una versión más reciente de Windows 10 (una actualización de una característica o versión de Windows). Sin embargo, el proceso de creación de WorkSpaces imágenes admite las actualizaciones acumulativas o de seguridad de Windows.
- Después del 14 de enero de 2020, no se pueden crear imágenes desde paquetes públicos de Windows 7. Es posible que desee considerar la posibilidad de migrar su Windows 7 WorkSpaces a Windows 10. Para obtener más información, consulte Migrar un WorkSpace.
- El paquete de Graphics dejará de ser compatible a partir del 30 de noviembre de 2023. Te recomendamos migrar tu paquete a WorkSpaces Graphics.G4DN. Para obtener más información, consulte Migrar un WorkSpace.
- Los gráficos y los GraphicsPro paquetes no están disponibles actualmente en la región Asia Pacífico (Bombay).
- Los volúmenes de almacenamiento en paquetes personalizados no pueden ser más pequeños que los volúmenes de almacenamiento de imágenes.

Los paquetes personalizados cuestan igual que los paquetes públicos desde los que se crean. Para obtener más información sobre los precios, consulta Amazon WorkSpaces Pricing.

Contenido

- Prácticas recomendadas
- (Opcional) Paso 1: especificar un formato de nombre de equipo personalizado para la imagen
- Paso 2: ejecutar el comprobador de imágenes
- Paso 3: crear una imagen personalizada y un paquete personalizado
- ¿Qué se WorkSpaces incluye con las imágenes personalizadas de Windows
- ¿Qué se incluye con las imágenes WorkSpace personalizadas de Linux

Requisitos para crear imágenes personalizadas de Windows

> **Note**
>
> Actualmente, Windows define 1 GB como 1.073.741.824 bytes. Los clientes deberán asegurarse de tener más de 12.884.901.888 bytes (o 12 GiB) libres en la unidad C y de que el perfil de usuario sea inferior a 10.737.418.240 bytes (o 10 GiB) para crear una imagen de un. WorkSpace

- El estado de debe estar disponible y su estado de modificación debe ser Ninguno. WorkSpace
- Todas las aplicaciones y los perfiles de usuario de WorkSpaces las imágenes deben ser compatibles con Microsoft Sysprep.
- Todas las aplicaciones que se van a incluir en la imagen deben estar instaladas en la unidad C.
- Para Windows 7 WorkSpaces, su tamaño total (archivos y datos) debe ser inferior a 10 GB.
- Para Windows 7 WorkSpaces, la C unidad debe tener al menos 12 GB de espacio disponible.
- Todos los servicios de aplicaciones que se ejecuten en el WorkSpace deben usar una cuenta de sistema local en lugar de las credenciales de usuario del dominio. Por ejemplo, no puede haber una instalación de Microsoft SQL Server Express en ejecución con las credenciales de un usuario del dominio.
- No WorkSpace deben estar cifrados. Actualmente, no WorkSpace se admite la creación de imágenes a partir de un archivo cifrado.
- Los siguientes componentes son necesarios en una imagen. Sin estos componentes, lo WorkSpaces que inicie desde la imagen no funcionará correctamente. Para obtener más información, consulte the section called “Configuración necesaria”.
  - Windows PowerShell versión 3.0 o posterior

- Servicios de Escritorio remoto
- AWS Controladores PV
- Administración remota de Windows (WinRM)
- Agentes y controladores de Teradici PCoIP
- Agentes y controladores de STXHD
- AWS y WorkSpaces certificados
- Agente de Skylight

Requisitos para crear imágenes personalizadas de Linux

- El estado del WorkSpace debe estar disponible y su estado de modificación debe ser Ninguno.
- Todas las aplicaciones que se incluyen en la imagen deben estar instaladas fuera del volumen de usuario (el directorio `/home`).
- El volumen raíz (/) no puede estar más lleno del 97%.
- No WorkSpace debe estar cifrado. Actualmente, no WorkSpace se admite la creación de imágenes a partir de un archivo cifrado.
- Los siguientes componentes son necesarios en una imagen. Sin estos componentes, lo WorkSpaces que inicie desde la imagen no funcionará correctamente:
  - Cloud-init
  - Agentes y controladores de Teradici PCoIP o WSP
  - Agente de Skylight

Prácticas recomendadas

Antes de crear una imagen a partir de un WorkSpace, haga lo siguiente:

- Utilice una VPC independiente que no esté conectada al entorno de producción.
- Implemente el WorkSpace en una subred privada y utilice una instancia de NAT para el tráfico saliente.
- Utilice un directorio Simple AD pequeño.
- Utilice el tamaño de volumen más pequeño para la fuente y WorkSpace, a continuación, ajústelo según sea necesario al crear el paquete personalizado.

- Instale todas las actualizaciones del sistema operativo (excepto las actualizaciones de las características y versiones de Windows) y todas las actualizaciones de las aplicaciones en el. WorkSpace Para obtener más información, consulte la nota importante al principio de este tema.
- Elimine los datos en caché de los WorkSpace que no deberían incluirse en el paquete (por ejemplo, el historial del navegador, los archivos en caché y las cookies del navegador).
- Elimine los ajustes de configuración WorkSpace que no deberían incluirse en el paquete (por ejemplo, los perfiles de correo electrónico).
- Cambie a la configuración de direcciones IP dinámicas que utiliza DHCP.
- Asegúrate de no haber superado el límite de WorkSpace imágenes permitido en una región. De forma predeterminada, se permiten 40 WorkSpace imágenes por región. Si ha alcanzado esta cuota, los nuevos intentos de crear una imagen producirán un error. Para solicitar un aumento de cuota, utiliza el formulario de WorkSpaces límites.
- Asegúrese de no intentar crear una imagen a partir de un archivo cifrado WorkSpace. Actualmente, no WorkSpace se admite la creación de imágenes a partir de un archivo cifrado.
- Si tienes instalado algún software antivirus en el WorkSpace, desactívalo mientras intentas crear una imagen.
- Si tienes un firewall activado WorkSpace, asegúrate de que no bloquee ningún puerto necesario. Para obtener más información, consulte Requisitos de dirección IP y puerto para WorkSpaces.
- En el caso de Windows WorkSpaces, no configure ningún objeto de política de grupo (GPO) antes de crear la imagen.
- WorkSpacesEn Windows, no personalice el perfil de usuario predeterminado (`C:\Users \Default`) antes de crear una imagen. Se recomienda realizar personalizaciones en el perfil de usuario a través de los GPO y aplicarlas después de la creación de la imagen. Los GPO se pueden modificar o revertir de manera sencilla y, por lo tanto, son menos propensos a errores que las personalizaciones realizadas en el perfil de usuario predeterminado.
- Para Linux WorkSpaces, consulte también el documento técnico «Mejores prácticas para preparar sus imágenes de Amazon WorkSpaces para Linux».
- Si desea utilizar tarjetas inteligentes en Linux WorkSpaces con el Protocolo de WorkSpaces transmisión (WSP) habilitado, consulte Utilizar tarjetas inteligentes para la autenticación las personalizaciones que debe realizar en su Linux WorkSpace antes de crear la imagen.
- Asegúrese de actualizar los controladores de dependencia de la red, como los controladores ENA, NVMe y PV, en su ordenador. WorkSpaces Debe hacerlo al menos una vez cada 6 meses. Para obtener más información, consulte Instalar o actualizar el controlador Elastic Network Adapter

(ENA)Controladores NVMe de AWS para instancias de Windows y Actualizar los controladores PV en instancias de Windows.

- Asegúrese de actualizar periódicamente los agentes de EC2Config, EC2Launch y EC2Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada 6 meses. Para obtener más información, consulte Actualizar EC2Config y EC2Launch.

(Opcional) Paso 1: especificar un formato de nombre de equipo personalizado para la imagen

En el caso de las imágenes WorkSpaces lanzadas desde una versión personalizada o con licencia propia (BYOL), puede especificar un prefijo personalizado para el formato del nombre del equipo en lugar de utilizar el formato de nombre del equipo predeterminado. Para especificar un prefijo personalizado, siga el procedimiento adecuado para el tipo de imagen.

Para especificar un formato de nombre de equipo personalizado para las imágenes personalizadas

> **Note**
>
> De forma predeterminada, el formato del nombre del equipo para Windows 10 WorkSpaces es `DESKTOP-XXXXX` y para Windows 11 WorkSpaces,. `WORKSPA-XXXXX`

1. En el WorkSpace que estés usando para crear tu imagen personalizada, ábrelo en el Bloc de notas o `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` en otro editor de texto. Para obtener más información sobre cómo trabajar con el archivo `Unattend.xml`, consulte Archivos de respuesta (unattend.xml) en la documentación de Microsoft.

   > **Note**
   >
   > Para acceder a la unidad C: desde el explorador de archivos de Windows de tu ordenador WorkSpace, introduce **`C:\`** en la barra de direcciones.

2. En la sección `<settings pass="specialize">`, asegúrese de que `<ComputerName>` esté configurada con un asterisco (`*`). Si `<ComputerName>` se establece en cualquier otro valor, se ignorará la configuración personalizada del nombre de su equipo. Para obtener más información

acerca de la <ComputerName> configuración, consulte ComputerNamela documentación de Microsoft.

3. En la sección <settings pass="specialize">, defina <RegisteredOrganization> y <RegisteredOwner> según los valores que prefiera.

   Durante Sysprep, los valores que especifique para <RegisteredOwner> y <RegisteredOrganization> se concatenarán, y los primeros 7 caracteres de la cadena combinada se utilizarán para crear el nombre del equipo. *Por ejemplo, si especifica* ***Amazon.com*** *para <RegisteredOrganization> y* ***EC2*** *para<RegisteredOwner>, los nombres de equipo que se WorkSpaces creen a partir del paquete personalizado comenzarán por EC2AMAZ-xxxxxxx.*

   > **Note**
   >
   > Sysprep ignora los valores <RegisteredOrganization> y <RegisteredOwner> de la sección <settings pass="oobeSystem">.

4. Guarde los cambios en el archivo Unattend.xml.

Para especificar un formato de nombre de equipo personalizado para las imágenes BYOL

1. Si utiliza Windows 10, abra C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml en el Bloc de notas o en otro editor de texto. Si usa Windows 11, abra C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml.
2. En la sección <settings pass="specialize">, quite la marca de comentario de <ComputerName>*</ComputerName> y asegúrese de que <ComputerName> se haya definido como un asterisco (*). Si <ComputerName> se establece en cualquier otro valor, se ignorará la configuración personalizada del nombre de su equipo. Para obtener más información acerca de la <ComputerName> configuración, consulte ComputerNamela documentación de Microsoft.
3. En la sección <settings pass="specialize">, defina <RegisteredOrganization> y <RegisteredOwner> según los valores que prefiera.

   Durante Sysprep, los valores que especifique para <RegisteredOwner> y <RegisteredOrganization> se concatenarán, y los primeros 7 caracteres de la cadena combinada se utilizarán para crear el nombre del equipo. *Por ejemplo, si especifica* ***Amazon.com*** *para <RegisteredOrganization> y* ***EC2*** *para<RegisteredOwner>,*

los nombres de equipo que se WorkSpaces creen a partir del paquete personalizado comenzarán por EC2AMAZ-xxxxxxx.

> **Note**
>
> Sysprep ignora los valores `<RegisteredOrganization>` y `<RegisteredOwner>` de la sección `<settings pass="oobeSystem">`.

4. Si utiliza Windows 10, guarde los cambios en el archivo `Sysprep2008.xml`. Si utiliza Windows 11, guarde los cambios en `OOBE_unattend.xml`.

Paso 2: ejecutar el comprobador de imágenes

> **Note**
>
> El verificador de imágenes solo está disponible para Windows. WorkSpaces Si va a crear una imagen desde un sistema Linux WorkSpace, vaya aPaso 3: crear una imagen personalizada y un paquete personalizado.

Para confirmar que su Windows WorkSpace cumple los requisitos para la creación de imágenes, le recomendamos que ejecute el Comprobador de imágenes. El comprobador de imágenes realiza una serie de pruebas en la imagen WorkSpace que desee utilizar para crear la imagen y proporciona instrucciones sobre cómo resolver cualquier problema que encuentre.

> **Important**
>
> - WorkSpace Debe superar todas las pruebas realizadas por el Image Checker antes de poder utilizarlo para la creación de imágenes.
> - Antes de ejecutar el comprobador de imágenes, compruebe que las últimas actualizaciones acumulativas y de seguridad de Windows estén instaladas en su dispositivo. WorkSpace

Para obtener el comprobador de imágenes, realice una de las siguientes acciones:

- Reinicie su. WorkSpace El comprobador de imágenes se descarga automáticamente durante el reinicio y se instala en `C:\Program Files\Amazon\ImageChecker.exe`.
- Descarga Amazon WorkSpaces Image Checker desde https://tools.amazonworkspaces.com/ImageChecker .zip y extrae el archivo. `ImageChecker.exe` Copie este archivo en `C:\Program Files\Amazon\`.

Para ejecutar el comprobador de imágenes

1. Abra el archivo `C:\Program Files\Amazon\ImageChecker.exe`.
2. En el cuadro de diálogo Amazon WorkSpaces Image Checker, seleccione Ejecutar.
3. Tras completarse cada prueba, puede ver el estado de la prueba.

   Para cualquier prueba con el estado FAILED (Error), elija Info (Información) para mostrar información sobre cómo resolver el problema que provocó el error. Para obtener más información acerca de cómo resolver estos problemas, consulte Sugerencias para resolver problemas detectados por el comprobador de imágenes.

   Si alguna prueba muestra el estado WARNING (Advertencia), elija el botón Fix all Warnings (Solucionar todos los mensajes de advertencia).

   La herramienta genera un archivo de registro de salida en el mismo directorio donde está ubicado el comprobador de imágenes. De forma predeterminada, este archivo se encuentra en `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

   > **Tip**
   >
   > No elimine este archivo de registro. Si se produce un problema, este archivo de registro puede ser útil para solucionar problemas.

4. Si procede, resuelva cualquier problema que provoque errores y advertencias en las pruebas y repita el proceso de ejecutar el Image Checker hasta que supere todas las pruebas. WorkSpace Todos los errores y advertencias deben resolverse antes de poder crear una imagen.
5. Una vez WorkSpace superadas todas las pruebas, aparecerá el mensaje de validación correcta. Ahora está listo para crear un paquete personalizado.

Sugerencias para resolver problemas detectados por el comprobador de imágenes

Además de consultar las siguientes sugerencias para resolver los problemas detectados por el comprobador de imágenes, asegúrese de revisar el archivo de registro del comprobador de imágenes en `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`.

PowerShell debe estar instalada la versión 3.0 o posterior

Instale la versión más reciente de Microsoft Windows PowerShell.

> **Important**
>
> La política de PowerShell ejecución de a WorkSpace debe estar configurada para permitir los RemoteSignedscripts. Para comprobar la política de ejecución, ejecute el ExecutionPolicy PowerShell comando Get-. Si la política de ejecución no está establecida en Sin restricciones RemoteSigned, ejecute el ExecutionPolicy RemoteSigned comando Set- ExecutionPolicy — para cambiar el valor de la política de ejecución. La RemoteSignedconfiguración permite la ejecución de scripts en Amazon WorkSpaces, lo cual es necesario para crear una imagen.

Solo las unidades C y D pueden estar presentes

Solo las `D` unidades `C` and pueden estar presentes en una unidad WorkSpace que se utilice para la generación de imágenes. Elimine todas las demás unidades, incluidas las unidades virtuales.

No se puede detectar ningún reinicio pendiente debido a las actualizaciones de Windows

- El proceso Crear imagen no se puede ejecutar hasta que se haya reiniciado Windows para finalizar la instalación de actualizaciones acumulativas o de seguridad. Reinicie Windows para aplicar estas actualizaciones y asegúrese de que no sea necesario instalar otras actualizaciones acumulativas o de seguridad de Windows pendientes.
- La creación de imágenes no es compatible con los sistemas de Windows 10 que se han actualizado de una versión de Windows 10 a otra más reciente (una actualización de características o de versión de Windows). Sin embargo, el proceso de WorkSpaces creación de imágenes admite las actualizaciones acumulativas o de seguridad de Windows.

El archivo Sysprep debe existir y no puede estar en blanco

Si hay problemas con su archivo Sysprep, póngase en contacto con el Centro de AWS Support para reparar su EC2Config o EC2Launch.

El tamaño del perfil de usuario debe ser inferior a 10 GB

Para Windows 7 WorkSpaces, el perfil de usuario (`D:\Users\username`) debe tener menos de 10 GB en total. Elimine los archivos según sea necesario para reducir el tamaño del perfil de usuario.

La unidad C debe tener suficiente espacio libre

Para Windows 7 WorkSpaces, debe tener al menos 12 GB de espacio libre en el disco`C`. Elimine los archivos según sea necesario para liberar espacio en la unidad `C`. En Windows 10 WorkSpaces, omítelo si recibe un `FAILED` mensaje y el espacio en disco es superior a 2 GB.

No se puede ejecutar ningún servicio en una cuenta de dominio

Para ejecutar el proceso de creación de imagen, ningún servicio de la misma WorkSpace puede ejecutarse en una cuenta de dominio. Todos los servicios deben ejecutarse en una cuenta local.

Para ejecutar servicios en una cuenta local

1. Abra `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` y busque la lista de servicios que se ejecutan en una cuenta de dominio.
2. En el cuadro de búsqueda de Windows, escriba **`services.msc`** para abrir el Administrador de servicios de Windows.
3. En Iniciar sesión como, busque los servicios que se ejecutan en cuentas de dominio. (Los servicios que se ejecutan como Sistema local, Servicio local o Servicio de red no interfieren con la creación de imágenes).
4. Seleccione un servicio que se esté ejecutando en una cuenta de dominio y, a continuación, elija Acción, Propiedades.
5. Abra la pestaña Iniciar sesión. En Iniciar sesión como, elija Cuenta de sistema local.
6. Seleccione Aceptar.

WorkSpace Debe estar configurado para usar DHCP

Debe configurar todos los adaptadores de red del WorkSpace para que utilicen DHCP en lugar de direcciones IP estáticas.

Para configurar todos los adaptadores de red para utilizar DHCP

1. En el cuadro de búsqueda de Windows, escriba **`control panel`** para abrir el Panel de control.
2. Elija Redes e Internet.
3. Elija Centro de redes y recursos compartidos.
4. Elija Cambiar configuración del adaptador y seleccione un adaptador.
5. Elija Cambiar la configuración de esta conexión.
6. En la pestaña Redes seleccione Protocolo de Internet versión 4 (TCP/IPv4) y, a continuación, elija Propiedades.
7. En el cuadro de diálogo Propiedades del Protocolo de Internet versión 4 (TCP/IPv4), seleccione Obtener una dirección IP automáticamente.
8. Seleccione Aceptar.
9. Repita este proceso para todos los adaptadores de red del WorkSpace.

Los servicios de Escritorio remoto deben estar habilitados

El proceso Crear imagen requiere que los servicios de Escritorio remoto estén habilitados.

Para habilitar Servicios de Escritorio remoto

1. En el cuadro de búsqueda de Windows, escriba **`services.msc`** para abrir el Administrador de servicios de Windows.
2. En la columna Nombre, busque Servicios de Escritorio remoto.
3. Seleccione Servicios de Escritorio remoto y, a continuación, elija Acción, Propiedades.
4. En la pestaña General, para Tipo de inicio, elija Manual o Automático.
5. Seleccione Aceptar.

Debe existir un perfil de usuario

El WorkSpace que utilices para crear imágenes debe tener un perfil de usuario (`D:\Users\`*`username`*). Si esta prueba produce un error, póngase en contacto con el Centro de AWS Support para obtener ayuda.

La ruta de la variable de entorno debe estar configurada correctamente

Faltan entradas para System32 y Windows PowerShell en la ruta de la variable de entorno de la máquina local. Estas entradas son necesarias para que se ejecute Crear imagen.

Para configurar la ruta de la variable de entorno

1. En el cuadro de búsqueda de Windows, escriba **`environment variables`** y después elija Editar las variables de entorno del sistema.
2. En el cuadro de diálogo Propiedades del sistema, abra la pestaña Avanzadas y elija Variables de entorno.
3. En el cuadro de diálogo Variables de entorno, en Variables de sistema, seleccione la entrada Ruta y, a continuación, elija Editar.
4. Elija Nueva y agregue la siguiente ruta:

   ```
   C:\Windows\System32
   ```
5. Vuelva a elegir Nueva y agregue la siguiente ruta:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. Seleccione Aceptar.
7. Reinicie el WorkSpace.

> **Tip**
>
> El orden en que aparecen los elementos en la ruta de la variable de entorno es importante. Para determinar el orden correcto, puede que desee comparar la ruta de su variable de entorno WorkSpace con la de una instancia de Windows recién creada WorkSpace o nueva.

El instalador de módulos de Windows debe estar habilitado

El proceso Crear imagen requiere que el servicio Instalador de módulos de Windows esté habilitado.

Para habilitar el servicio Instalador de módulos de Windows

1. En el cuadro de búsqueda de Windows, escriba **`services.msc`** para abrir el Administrador de servicios de Windows.

2. En la columna Nombre, busque Instalador de módulos de Windows.
3. Seleccione Instalador de módulos de Windows y, a continuación, elija Acción, Propiedades.
4. En la pestaña General, para Tipo de inicio, elija Manual o Automático.
5. Seleccione Aceptar.

El agente de Amazon SSM debe estar deshabilitado

El proceso Crear imagen requiere que el servicio del agente de Amazon SSM esté deshabilitado.

Para desactivar el servicio del agente de Amazon SSM

1. En el cuadro de búsqueda de Windows, escriba **`services.msc`** para abrir el Administrador de servicios de Windows.
2. En la columna Nombre, busque Agente de Amazon SSM.
3. Seleccione Agente de Amazon SSM y, a continuación, elija Acción, Propiedades.
4. En la pestaña General, para Tipo de inicio, elija Deshabilitado.
5. Seleccione Aceptar.

SSL3 y TLS versión 1.2 deben estar habilitados

Para configurar SSL/TLS para Windows, consulte Habilitación de TLS 1.2 en la documentación de Microsoft Windows.

Solo puede existir un perfil de usuario en la WorkSpace

Solo puede haber un perfil WorkSpaces de usuario (`D:\Users\`*`username`*) en el WorkSpace que estás utilizando para crear las imágenes. Elimine cualquier perfil de usuario que no pertenezca al usuario previsto del WorkSpace.

Para que la creación de imágenes funcione, solo WorkSpace puede tener tres perfiles de usuario:

- El perfil de usuario del usuario previsto de WorkSpace (`D:\Users\`*`username`*)
- El perfil de usuario predeterminado (también conocido como perfil predeterminado)
- El perfil de usuario administrador

Si hay perfiles de usuario adicionales, puede eliminarlos a través de las propiedades avanzadas del sistema en el Panel de control de Windows.

Para eliminar un perfil de usuario

1. Para acceder a las propiedades avanzadas del sistema, siga uno de estos procedimientos:
   - Pulse tecla de Windows+Pausa Inter y, a continuación, elija Configuración avanzada del sistema en el panel izquierdo del cuadro de diálogo Panel de control > Sistema y seguridad > Sistema.
   - En el cuadro de búsqueda de Windows, escriba **`control panel`**. En el Panel de control, elija Sistema y seguridad después elija Sistema y, a continuación, elija Configuración avanzada del sistema en el panel izquierdo del cuadro de diálogo Panel de control > Sistema y seguridad > Sistema.
2. En el cuadro de diálogo Propiedades del sistema, en la pestaña Avanzadas, elija Configuración en Perfiles de usuario.
3. Si aparece algún perfil distinto del perfil de administrador, el perfil predeterminado y el perfil del WorkSpaces usuario previsto, seleccione ese perfil adicional y pulse Eliminar.
4. Cuando se le pregunte si desea eliminar el perfil, elija Sí.
5. Si es necesario, repita los pasos 3 y 4 para eliminar cualquier otro perfil que no pertenezca al WorkSpace.
6. Elija Aceptar dos veces y cierre el Panel de control.
7. Reinicie el WorkSpace.

Ningún paquete de AppX puede estar en un estado por etapas

Uno o más paquetes de AppX están en un estado por etapas. Esto puede provocar un error de Sysprep durante la creación de la imagen.

Para eliminar todos los paquetes de AppX por etapas

1. En el cuadro de búsqueda de Windows, escriba **`powershell`**. Seleccione Ejecutar como administrador.
2. Cuando se le pregunte "¿Desea permitir que esta aplicación realice cambios en su dispositivo?", elija Sí.
3. En la PowerShell ventana de Windows, introduzca los siguientes comandos para obtener una lista de todos los paquetes de AppX preparados y pulse Entrar después de cada uno de ellos.

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                ($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                $_.PackageUserInformation -like "*Staged*")
                                }
```

4. Escriba el siguiente comando para eliminar todos los paquetes de AppX por etapas y pulse Intro.

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Vuelva a ejecutar el comprobador de imágenes. Si esta prueba sigue produciendo un error, escriba los siguientes comandos para eliminar todos los paquetes de AppX y pulse Intro después de cada uno.

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows no se debe haber actualizado desde una versión anterior

La creación de imágenes no se admite en los sistemas de Windows que se han actualizado de una versión de Windows 10 a otra más reciente (una actualización de características o de versión de Windows).

Para crear imágenes, utilice una WorkSpace que no haya sido objeto de una actualización de características o versión de Windows.

El recuento de rearmados de Windows no debe ser 0

La característica "rearmar" le permite ampliar el periodo de activación de la versión de prueba de Windows. El proceso Crear imagen requiere que el recuento de rearmados sea un valor distinto de 0.

Para comprobar el recuento de rearmados de Windows

1. En el menú Inicio de Windows, elija Sistema de Windows, y, a continuación, elija Símbolo del sistema.
2. En la ventana del símbolo del sistema, escriba el siguiente comando y, a continuación, pulse Intro.

   ```
   cscript C:\Windows\System32\slmgr.vbs /dlv
   ```

Para restablecer el recuento de rearmados en un valor distinto de 0, consulte Ejecutar Sysprep (Generalize) en una instalación de Windows en la documentación de Microsoft Windows.

Sugerencias adicionales para la solución de problemas

Si WorkSpace superas todas las pruebas realizadas por el Image Checker, pero sigues sin poder crear una imagen a partir de él WorkSpace, comprueba los siguientes problemas:

- Asegúrese de que WorkSpace no esté asignado a un usuario de un grupo de invitados del dominio. Para comprobar si hay cuentas de dominio, ejecuta el siguiente PowerShell comando.

  ```
  Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
  $env:USERDOMAIN*" }
  ```

- WorkSpaces Solo para Windows 7: si se producen problemas al copiar el perfil de usuario durante la creación de la imagen, compruebe los siguientes problemas:
  - Las rutas de perfil largas pueden provocar errores de creación de imágenes. Asegúrese de que las rutas de acceso de todas las carpetas dentro del perfil de usuario tienen menos de 261 caracteres.
  - Asegúrese de conceder permisos completos en la carpeta de perfil al sistema y a todos los paquetes de aplicaciones.
  - Si algún archivo del perfil de usuario está bloqueado por un proceso o se está utilizando durante la creación de la imagen, es posible que se produzca un error al copiar el perfil.
- Algunos objetos de política de grupo (GPO) restringen el acceso a la huella digital del certificado RDP cuando lo solicitan el servicio EC2Config o los scripts EC2Launch durante la configuración de la instancia de Windows. Antes de intentar crear una imagen, WorkSpace muévala a una nueva unidad organizativa (OU) con una herencia bloqueada y sin ningún GPO aplicado.
- Asegúrese de que el servicio Administración remota de Windows (WinRM) está configurado para iniciarse automáticamente. Haga lo siguiente:

1. En el cuadro de búsqueda de Windows, escriba **`services.msc`** para abrir el Administrador de servicios de Windows.
2. En la columna Nombre, busque Administración remota de Windows (WS-Management).
3. Seleccione Administración remota de Windows (WS-Management) y, a continuación, elija Acción y Propiedades.
4. En la pestaña General, para Tipo de inicio, elija Automático.
5. Seleccione Aceptar.

Paso 3: crear una imagen personalizada y un paquete personalizado

Una vez validada WorkSpace la imagen, puede continuar con la creación de la imagen y el paquete personalizados.

Para crear una imagen personalizada y un grupo personalizado

1. Si todavía está conectado a WorkSpace, desconéctese seleccionando Amazon WorkSpaces y Disconnect en la aplicación WorkSpaces cliente.
2. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
3. En el panel de navegación, elija WorkSpaces.
4. Seleccione WorkSpace para abrir su página de detalles y elija Crear imagen. Si el estado de WorkSpace es Detenido, debe iniciarlo primero (elija Acciones, Iniciar WorkSpaces) antes de poder elegir Acciones, Crear imagen.

   > **Note**
   >
   > Para crear una imagen mediante programación, usa la acción de la CreateWorkspaceImage API. Para obtener más información, consulta CreateWorkspaceImagela referencia de la WorkSpaces API de Amazon.

5. Aparece un mensaje en el que se le pide que reinicie (reinicie) la suya WorkSpace antes de continuar. Al reiniciar, se WorkSpace actualiza el WorkSpaces software de Amazon a la última versión.

   Reinicie el suyo WorkSpace cerrando el mensaje y siguiendo los pasos que se indican. Reiniciar un WorkSpace Cuando haya terminado, repita el Step 4 de este procedimiento, pero esta vez

elija Siguiente cuando aparezca el mensaje de reinicio. Para crear una imagen, el estado de la imagen WorkSpace debe estar disponible y su estado de modificación debe ser Ninguno.

6. Escriba un nombre y una descripción de la imagen que le ayuden a identificarla y, a continuación, elija Create Image (Crear imagen). Mientras se crea la imagen, el estado de WorkSpace es Suspendido y no WorkSpace está disponible.

> **Note**
>
> Al introducir la descripción de una imagen, asegúrate de no utilizar el carácter especial «-» o aparecerá un error.

7. En el panel de navegación, elija Images. La imagen estará completa cuando el estado de la imagen WorkSpace cambie a Disponible (esto puede tardar hasta 45 minutos).
8. Seleccione la imagen y elija Acciones, Crear paquete.

> **Note**
>
> Para eliminar un paquete mediante programación, utilice la acción de la API CreateWorkspaceBundle. Para obtener más información, consulta CreateWorkspaceBundlela referencia de la WorkSpaces API de Amazon.

9. Introduzca un nombre y una descripción para el paquete y, a continuación, haga lo siguiente:

   - Para el tipo de hardware del paquete, elija el hardware que se utilizará al lanzar WorkSpaces desde este paquete personalizado.
   - En Configuración de almacenamiento, seleccione una de las combinaciones predeterminadas para el volumen raíz y el tamaño del volumen de usuario, o seleccione Personalizado y, a continuación, introduzca valores (hasta 2000 GB) para el Tamaño del volumen raíz y Tamaño del volumen de usuario.

     Las combinaciones de tamaños disponibles predeterminados para el volumen raíz (para Microsoft Windows, la unidad `C`, para Linux, /) y el volumen de usuario (para Windows, la unidad `D`, para Linux, /home) son los siguientes:

     - Raíz: 80 GB, Usuario: 10 GB, 50 GB o 100 GB
     - Raíz: 175 GB, Usuario: 100 GB
     - Para gráficos. G4dn, GraphicsPro .g4dn, gráficos y GraphicsPro WorkSpaces solo: raíz: 100 GB, usuario: 100 GB

Puede ampliar los volúmenes raíz y de usuario hasta un máximo de 2000 GB cada uno.

> **Note**
>
> Para garantizar que sus datos se conserven, no puede reducir el tamaño de los volúmenes raíz o de usuarios después de lanzar un. WorkSpace En su lugar, asegúrese de especificar los tamaños mínimos de estos volúmenes al lanzar un WorkSpace. Puede lanzar un Value, Standard, Performance, Power o PowerPro WorkSpace con un mínimo de 80 GB para el volumen raíz y 10 GB para el volumen de usuario. Puede lanzar un archivo Graphics.G4dn, GraphicsPro .g4dn, Graphics o GraphicsPro WorkSpace con un mínimo de 100 GB para el volumen raíz y 100 GB para el volumen de usuario.

10. Elija Crear paquete.
11. Para confirmar que el paquete se ha creado, seleccione Paquetes y compruebe que el paquete aparezca en la lista.

¿Qué se WorkSpaces incluye con las imágenes personalizadas de Windows

Al crear una imagen desde un dispositivo Windows 7, Windows 10 o Windows 11 WorkSpace, se incluye todo el contenido de la `C` unidad.

En Windows 10 u 11 WorkSpaces, el perfil de usuario no `D:\Users\`*`username`* está incluido en la imagen personalizada.

En `D:\Users\`*`username`* Windows 7 WorkSpaces, se incluye todo el contenido del perfil de usuario, excepto lo siguiente:

- Contactos
- Descargas
- Música
- Imágenes
- Juegos guardados
- Videos

- Podcasts
- Máquinas virtuales
- .virtualbox
- Tracing
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

¿Qué se incluye con las imágenes WorkSpace personalizadas de Linux

Al crear una imagen desde Amazon Linux WorkSpace, se elimina todo el contenido del volumen de usuario (/home). Se incluye el contenido del volumen raíz (/), excepto las siguientes carpetas y claves correspondientes, que se eliminan:

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /inicio
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/ /users AccountsService

Las claves siguientes se destruyen durante la creación de la imagen personalizada:

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

Actualizar un paquete de WorkSpaces personalizado

Puede actualizar un paquete de escritorios de WorkSpaces personalizado modificando un escritorio de WorkSpaces basado en el paquete, creando una imagen del escritorio de WorkSpaces y actualizando el paquete con la nueva imagen. Puede lanzar escritorios de WorkSpaces nuevos usando el paquete actualizado.

> **Important**
>
> Los WorkSpaces existentes no se actualizan automáticamente al actualizar el paquete en el que se basan. Para actualizar WorkSpaces existentes basados en un paquete que ha actualizado, debe volver a generar los WorkSpaces o eliminarlos y volver a crearlos.

Para actualizar un paquete mediante la consola

1. Conéctese a un escritorio de WorkSpaces basado en el paquete y realice los cambios que desee. Por ejemplo, puede aplicar las revisiones más recientes del sistema operativo y las aplicaciones, así como instalar otras aplicaciones.

   También puede crear un escritorio de WorkSpaces nuevo con el mismo paquete de software de referencia (Plus o Standard) como la imagen utilizada para crear el paquete y hacer cambios.
2. Si sigue conectado al WorkSpace, desconéctese seleccionando Amazon WorkSpaces y Desconectar en la aplicación cliente de WorkSpaces.
3. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
4. En el panel de navegación, seleccione WorkSpaces.
5. Seleccione el WorkSpace y elija Actions, Create Image. Si el estado del WorkSpace es `STOPPED`, primero debe iniciarlo (elija Acciones, Iniciar WorkSpaces) antes de seleccionar Acciones, Crear imagen.

6. Escriba un nombre y una descripción para la imagen y, a continuación, elija Create Image (Crear imagen). El escritorio de WorkSpaces no está disponible mientras se crea la imagen. Para obtener información detallada sobre el proceso de creación de imágenes, consulte Crea una WorkSpaces imagen y un paquete personalizados.
7. En el panel de navegación, elija Bundles.
8. Seleccione el paquete para abrir su página de detalles y, a continuación, en Imagen de origen, seleccione Editar.
9. En la página Actualizar imagen de origen, seleccione la imagen que ha creado y elija Actualizar paquete.
10. Según sea necesario, actualice los WorkSpaces existentes que se basen en el paquete volviéndolos a generar o elimínelos y vuelva a crearlos. Para obtener más información, consulte Reconstruir un WorkSpace.

Para actualizar un paquete mediante programación

Para eliminar un paquete mediante programación, utilice la acción de la API UpdateWorkspaceBundle. Para obtener más información, consulte UpdateWorkspaceBundle en la Referencia de la API de Amazon WorkSpaces.

Copiar una imagen personalizada de WorkSpaces

Puede copiar una imagen personalizada de WorkSpaces en una misma región de AWS o entre regiones. La copia de una imagen produce una imagen idéntica con su propio identificador único.

Puede copiar una imagen Bring Your Own License (BYOL) en otra región siempre que la región de destino esté habilitada para BYOL. Asegúrese de que BYOL está habilitado para todas las cuentas y regiones implicadas.

> **Note**
>
> En la región de China (Ningxia), solop puede copiar imágenes dentro de la misma región.
> En AWS GovCloud (US) Region, para copiar imágenes desde y hacia otras regiones de AWS, póngase en contacto con el soporte de AWS.
> En regiones registradas, para copiar imágenes a otras regiones, póngase en contacto con el soporte de AWS. Para obtener más información sobre las regiones registradas, consulte Regiones disponibles.

También puede copiar una imagen que haya sido compartida con usted por otra cuenta de AWS. Para obtener más información sobre las imágenes compartidas, consulte Compartir o dejar de compartir una imagen personalizada de WorkSpaces.

No hay cargos adicionales por copiar una imagen dentro o entre regiones. Sin embargo, se aplica la cuota del número de imágenes en la región de destino. Para obtener más información sobre las cuotas de Amazon WorkSpaces, consulte WorkSpaces Cuotas de Amazon.

Permisos de IAM para copiar una imagen

Permisos de IAM para copiar una imagenSi utiliza un usuario de IAM para copiar una imagen, el usuario debe tener permisos para `workspaces:DescribeWorkspaceImages` y `workspaces:CopyWorkspaceImage`.

La siguiente política de ejemplo permite al usuario copiar la imagen indicada en la cuenta indicada en la región indicada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

Si va a crear una política de IAM para copiar imágenes compartidas para cuentas que no son propietarias de las imágenes, no puede especificar un ID de cuenta en el ARN. En su lugar, debe utilizar * para el ID de cuenta, como se muestra en la siguiente directiva de ejemplo.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Puede especificar un ID de cuenta en el ARN solo cuando esa cuenta es la propietaria de las imágenes que se van a copiar.

Para obtener más información acerca de cómo trabajar con IAM, consulte Gestión de identidades y accesos para WorkSpaces.

Copia en bloque de imágenes

Puede copiar imágenes una por una mediante la consola. Para copiar imágenes en bloque, utilice la operación de la API CopyWorkspaceImage API o el comando copy-workspace-image en la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte CopyWorkspaceImage en la Referencia de la API de Amazon WorkSpaces o consulte copy-workspace-image en la AWS CLI Referencia de los comandos.

Important

Antes de copiar una imagen compartida, asegúrese de que se ha compartido desde la cuenta de AWS correcta. Para determinar si una imagen se ha compartido y ver el ID de la cuenta de AWS propietaria de una imagen, utilice las operaciones de la API DescribeWorkSpaceImages y DescribeWorkspaceImagePermissions o los comandos describe-workspace-images y describe-workspace-image-permissions en la AWS CLI.

Para copiar una imagen mediante la consola

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.

2. En el panel de navegación, elija Images.
3. Seleccione la imagen y elija Acciones, Copiar imagen.
4. En Seleccionar destino, seleccione la región AWS en la que desee copiar la imagen.
5. En Nombre de la copia, introduzca el nuevo nombre de la imagen copiada y, en Descripción, introduzca una descripción para la imagen copiada.
6. (Opcional) En Etiquetas, introduzca las etiquetas de la imagen copiada. Para obtener más información, consulte Etiquetado de recursos de WorkSpaces.
7. Elija Copiar imagen.

Compartir o dejar de compartir una imagen personalizada de WorkSpaces

Puede compartir imágenes de WorkSpaces personalizadas entre cuentas de AWS en la misma región de AWS. Después de compartir una imagen, la cuenta del destinatario puede copiar la imagen en otras regiones de AWS según sea necesario. Para obtener más información sobre cómo copiar imágenes, consulte Copiar una imagen personalizada de WorkSpaces.

> **Note**
>
> En la región de China (Ningxia), solo puede copiar imágenes dentro de la misma región. En las AWS GovCloud (US) Region, para copiar imágenes desde y hacia otras regiones de AWS, póngase en contacto con el soporte de AWS.

No se aplican cargos adicionales por compartir una imagen. Sin embargo, se aplica la cuota del número de imágenes en la región de AWS. Una imagen compartida no se tiene en cuenta para la cuota de la cuenta del destinatario hasta que el destinatario no copie la imagen. Para obtener más información sobre las cuotas de Amazon WorkSpaces, consulte WorkSpaces Cuotas de Amazon.

Para eliminar una imagen compartida, debe detener el uso compartido de la imagen antes de poder eliminarla.

Comparta imágenes de traiga su propia licencia

Puede compartir imágenes de traiga su propia licencia (BYOL) con cuentas de AWS que estén habilitadas para BYOL. La cuenta de AWS con la que desea compartir imágenes BYOL también debe formar parte de su organización (en la misma cuenta de pagador).

> **Note**
>
> En este momento, no se puede compartir imágenes BYOL entre cuentas de AWS en las regiones AWS GovCloud (Oeste de EE. UU.) y AWS GovCloud (Este de EE. UU.). Para compartir imágenes BYOL entre cuentas de AWS en las regiones AWS GovCloud (Oeste de EE. UU.) y GovCloud (Este de EE. UU.), póngase en contacto con el servicio de soporte de AWS.

Imágenes compartidas con usted

Si las imágenes se comparten con usted, puede copiarlas. A continuación, puede usar las copias de las imágenes para crear paquetes para lanzar nuevos escritorios de WorkSpaces.

> **Important**
>
> Antes de copiar una imagen compartida, asegúrese de que se ha compartido desde la cuenta de AWS correcta. Para determinar mediante programación si una imagen se ha compartido, utilice las operaciones de API DescribeWorkspaceImages y DescribeWorkspaceImagePermissions o los comandos describe-workspace-images y describe-workspace-image-permissions de la interfaz de línea de comandos (CLI) de AWS.

La fecha de creación que se muestra para una imagen que se ha compartido con usted es la fecha en que se creó originalmente la imagen, no la fecha en que se compartió.

Si se ha compartido una imagen con usted, no podrá seguir compartiéndola con otras cuentas.

Para compartir una imagen

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Images.
3. Elija la imagen para abrir la página de detalles.
4. En la página de detalles de la imagen, en la sección Cuentas compartidas, elija Agregar cuenta.
5. En la página Agregar cuenta, en Agregar cuenta con la que compartir, introduzca el ID de la cuenta con la que quiera compartir la imagen.

> **Important**
>
> Antes de compartir una imagen, confirme que el ID de la cuenta de AWS sea correcto.

6. Elija Share Image (Compartir imagen).

> **Note**
>
> Para usar la imagen compartida, la cuenta del destinatario primero debe copiar la imagen. La cuenta del destinatario puede usar la copia de la image compartida para crear paquetes para lanzar nuevos escritorios de WorkSpaces.

Para dejar de compartir una imagen

1. Abra la consola de WorkSpaces en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Images.
3. Elija la imagen para abrir la página de detalles.
4. En la página de detalles de la imagen, en la sección Cuentas compartidas, seleccione la cuenta de AWS con la que quiere dejar de compartir y, a continuación, elija Dejar de compartir.
5. Cuando se le pida que confirme que quiere dejar de compartir la imagen, seleccione Dejar de compartir.

> **Note**
>
> Si quiere eliminar la imagen después de dejar de compartirla, primero debe dejar de compartirla en todas las cuentas con las que se haya compartido.

Cuando deje de compartir una imagen, la cuenta del destinatario no podrá hacer copias de la imagen. Sin embargo, las copias de imágenes compartidas que ya están en la cuenta del destinatario permanecen en esa cuenta y los nuevos escritorios de WorkSpaces se pueden lanzar desde esas copias.

Para compartir o dejar de compartir imágenes mediante programación

Para compartir o dejar de compartir imágenes mediante programación, utilice la operación de la API UpdateWorkspaceImagePermission o el comando update-workspace-image-permission AWS Command Line Interface (AWS CLI). Para determinar si se ha compartido una imagen, utilice la operación de la API DescribeWorkspaceImagePermissions o el comando describe-workspace-image-permissions de la CLI.

Eliminar un WorkSpaces paquete o una imagen personalizados

Es posible eliminar los paquetes personalizados o las imágenes personalizadas que no se utilicen.

Eliminar un paquete

Para eliminar un paquete, primero debes eliminar todos los WorkSpaces que estén basados en el paquete.

Para eliminar un paquete utilizando la consola

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Bundles.
3. Seleccione el paquete y elija Eliminar.
4. Cuando se le pida confirmación, elija Eliminar.

Para eliminar un paquete de forma programada

Para eliminar un paquete mediante programación, utilice la acción de la API DeleteWorkspaceBundle. Para obtener más información, consulta DeleteWorkspaceBundlela referencia de la WorkSpaces API de Amazon.

> **Note**
>
> Asegúrese de esperar al menos 2 horas después de eliminar un paquete antes de crear uno nuevo con el mismo nombre.

Eliminar una imagen

Después de eliminar un paquete personalizado, puede eliminar la imagen que usó para crearlo o actualizarlo.

Para eliminar una imagen, primero debe eliminar los paquetes asociados a ella o actualizarlos para que utilicen otra imagen de origen. También debe anular el uso compartido de la imagen si está compartida con otras cuentas. La imagen tampoco puede estar en estado Pendiente o Validando.

Para eliminar una imagen utilizando la consola

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Images.
3. Seleccione la imagen y elija Eliminar.
4. Cuando se le pida confirmación, elija Eliminar.

Para eliminar una imagen de forma programada

Para eliminar una imagen de forma programada, utilice la acción de la API DeleteWorkspaceImage. Para obtener más información, consulta DeleteWorkspaceImagela referencia de la WorkSpaces API de Amazon.

Utilizar sus propias licencias de escritorio de Windows

Si su acuerdo de licencia con Microsoft lo permite, puede llevar e implementar su escritorio Windows 10 u 11 en su WorkSpaces. Para ello, debe traer su propia licencia (BYOL) y proporcionar una licencia de Windows 10 u 11 que cumpla con los siguientes requisitos. Para obtener más información sobre el AWS uso del software de Microsoft en Amazon Web Services y Microsoft.

Para cumplir con los términos de licencia de Microsoft, AWS ejecuta tu BYOL WorkSpaces en un hardware dedicado a ti en la AWS nube. Si trae su licencia, podrá ofrecer una experiencia uniforme a los usuarios. Para obtener más información, consulta los WorkSpaces precios.

> **Important**
>
> La creación de imágenes no es compatible con los sistemas Windows 10 u 11 que se hayan actualizado de una versión de Windows 10 u 11 a una versión más reciente de Windows 10 u 11 (una actualización de una característica o versión de Windows). Sin embargo, el proceso de creación de WorkSpaces imágenes admite las actualizaciones acumulativas o de seguridad de Windows.

Contenido

Requisitos

Antes de comenzar, verifique lo siguiente:

- El acuerdo de licencia de Microsoft permite que Windows se ejecute en un entorno de alojamiento virtual.
- Si va a utilizar paquetes no compatibles con la GPU (paquetes distintos de Graphics.G4dn, GraphicsPro .g4dn, Graphics y), compruebe que utilizará un mínimo de 100 por región. GraphicsPro WorkSpaces Estos 100 pueden ser cualquier combinación de y. WorkSpaces AlwaysOn AutoStop WorkSpaces El uso de un mínimo de 100 WorkSpaces por región es un requisito para WorkSpaces ejecutar un hardware dedicado. Es necesario ejecutar su WorkSpaces hardware dedicado para cumplir con los requisitos de licencia de Microsoft. El hardware dedicado se aprovisiona de forma AWS lateral, por lo que su VPC puede permanecer en el arrendamiento predeterminado.

  Si planea usar paquetes con GPU (Graphics.G4dn, GraphicsPro .g4dn, Graphics y GraphicsPro), compruebe que va a ejecutar un mínimo de 4 o 20 unidades con GPU habilitadas en una región al mes en hardware dedicado. AlwaysOn AutoStop WorkSpaces

Note

- Los gráficos. G4dn, .g4dn, gráficos y paquetes solo se pueden crear para el protocolo PCoIP en este momento. GraphicsPro GraphicsPro
- El paquete de Graphics dejará de ser compatible a partir del 30 de noviembre de 2023. Te recomendamos migrar tu paquete a WorkSpaces Graphics.g4dn. Para obtener más información, consulte Migrar un WorkSpace.
- Los gráficos y los GraphicsPro paquetes no están disponibles actualmente en la región de Asia Pacífico (Bombay).
- Graphics.g4dn, GraphicsPro .g4dn, Graphics y los GraphicsPro paquetes no están disponibles actualmente en la región de África (Ciudad del Cabo).
- Para ejecutar tu versión WorkSpaces en la región de África (Ciudad del Cabo), debes ejecutar un mínimo de 400 WorkSpaces en la región de África (Ciudad del Cabo).
- Los paquetes de Windows 11 solo se pueden crear para el protocolo WSP.
- Los paquetes Graphics.g4dn y GraphicsPro .g4dn no están disponibles actualmente para Windows 11.
- Los gráficos y los paquetes no son compatibles con Windows 11. GraphicsPro
- Los paquetes Value no están disponibles para Windows 11. Para obtener más información sobre la migración de su paquete WorkSpaces de valor existente, consulte. Migrar un WorkSpace
- Para disfrutar de la mejor experiencia de videoconferencia, le recomendamos que utilice Power o paquetes PowerPro
- Windows 11 requiere el modo de arranque de la Interfaz Unificada de Firmware Extensible (UEFI) para funcionar. Asegúrese de especificar el `--boot-mode` parámetro opcional como UEFI para importar correctamente la máquina virtual.

- WorkSpaces puede usar una interfaz de administración en el rango de direcciones IP de /16. La interfaz de administración está conectada a una red de WorkSpaces administración segura que se utiliza para la transmisión interactiva. Esto le WorkSpaces permite administrar su WorkSpaces. Para obtener más información, consulte Interfaces de red. Para este fin, debe reservar una máscara de red /16 en al menos uno de los siguientes intervalos de direcciones IP:
  - 10.0.0.0/8
  - 100.64.0.0/10

- 172.16.0.0/12
- 192.168.0.0/16
- 198.18.0.0/15

> **Note**
>
> - A medida que adopta el WorkSpaces servicio, los rangos de direcciones IP de la interfaz de administración disponibles cambian con frecuencia. Para determinar qué rangos están disponibles actualmente, ejecute el comando list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI).
> - Además del bloque CIDR /16 que seleccione, el rango de direcciones IP 54.239.224.0/20 se utiliza para el tráfico de la interfaz de administración en todas las regiones. AWS

- Asegúrese de haber abierto los puertos de interfaz de administración necesarios para la activación de Microsoft Windows y Microsoft Office KMS para BYOL WorkSpaces. Para obtener más información, consulte Puertos de la interfaz de administración.
- Tiene una máquina virtual (VM) que ejecuta una versión de 64 bits compatible de Windows. Para obtener una lista de versiones compatibles, consulte la siguiente sección de este tema, Versiones de Windows compatibles con BYOL. La máquina virtual también debe cumplir los requisitos siguientes:
  - El sistema operativo Windows debe activarse en los servidores de administración clave.
  - El sistema operativo Windows debe tener English (United States) [Inglés (Estados Unidos)] como idioma principal.
  - No se puede instalar en la máquina virtual ningún software más allá de lo que se incluye con Windows. Puede agregar software adicional, como una solución antivirus, al crear una imagen personalizada más adelante.
  - No personalice el perfil de usuario predeterminado (`C:\Users\Default`) ni realice otras personalizaciones antes de crear una imagen. Todas las personalizaciones deben realizarse después de la creación de la imagen. Se recomienda realizar cualquier personalización en el perfil de usuario a través de objetos de política de grupo (GPO) y aplicarlos después de la creación de la imagen. Esto se debe a que las personalizaciones realizadas a través de los GPO se pueden modificar o revertir de forma sencilla y son menos propensas a errores que las personalizaciones realizadas en el perfil de usuario predeterminado.

  - Debe crear una cuenta WorkSpaces_BYOL con acceso de administrador local antes de compartir la imagen. La contraseña de esta cuenta puede ser necesaria más adelante, así que anótela.
  - La máquina virtual debe estar en un solo volumen con un tamaño máximo de 70 GB y al menos 10 GB de espacio libre. Si también planea suscribirse a Microsoft Office para su imagen BYOL, la máquina virtual debe estar en un solo volumen con un tamaño máximo de 70 GB y al menos 20 GB de espacio libre. El disco en el que se encuentra el volumen raíz no puede superar los 70 GB.
  - La máquina virtual debe ejecutar la PowerShell versión 4 o posterior de Windows.
- Asegúrese de haber instalado los parches (revisiones) más recientes de Microsoft Windows antes de ejecutar la secuencia de comandos del verificador de BYOL en Paso 3: Ejecute el PowerShell script BYOL Checker en una máquina virtual Windows.

> **Note**
>
> - En el caso de BYOL AutoStop WorkSpaces, un gran número de inicios de sesión simultáneos podría aumentar considerablemente el tiempo de disponibilidad WorkSpaces . Si espera que varios usuarios inicien sesión en su BYOL AutoStop WorkSpaces al mismo tiempo, consulte a su administrador de cuentas para que le aconseje.
> - Las AMI cifradas no se admiten en el proceso de importación. Asegúrese de deshabilitar la instancia utilizada para crear la AMI de EC2 con cifrado EBS. El cifrado se puede activar después de aprovisionar el cifrado final WorkSpaces .

Versiones de Windows compatibles con BYOL

Su máquina virtual debe ejecutar una de las siguientes versiones de Windows:

- Windows 10 versión 21H2 (actualización de diciembre 2021)
- Windows 10 versión 22H2 (actualización de noviembre de 2022)
- Windows 10 Enterprise LTSC 2019 (1809)
- Windows 10 Enterprise LTSC 2021 (21H2)
- Windows 11 Enterprise 23H2 (versión de octubre de 2023)
- Windows 11 Enterprise 22H2 (versión de octubre de 2022)

Todas las versiones de sistema operativo compatibles admiten todos los tipos de procesamiento disponibles en la AWS región en la que se esté utilizando. WorkSpaces No se garantiza que las versiones de Windows que ya no son compatibles con Microsoft funcionen y Support tampoco las AWS admite.

> **Note**
>
> Las versiones Windows 10 N y Windows 11 N no son compatibles con BYOL en este momento.

Añada Microsoft Office a su imagen BYOL

Durante el proceso de ingesta de imágenes BYOL, si utiliza Windows 10, tiene la opción de suscribirse a Microsoft Office Professional desde 2016 (32 bits) o 2019 (64 bits) hasta Microsoft. AWS Si utilizas Windows 11, puedes suscribirte a Microsoft Office Professional 2019 (64 bits). Si elige una de estas opciones, Microsoft Office viene preinstalado en la imagen BYOL y se incluye en cualquier imagen WorkSpaces que inicie desde esta imagen.

Si decides suscribirte a Office a través de AWS, se aplicarán cargos adicionales. Para obtener más información, consulta WorkSpaces los precios.

> **Important**
>
> - Si Microsoft Office ya está instalado en la máquina virtual que está utilizando para crear la imagen BYOL, debe desinstalarla de la máquina virtual si desea suscribirse a Office a través AWS de ella.
> - Si planea suscribirse a Office a través de AWS, asegúrese de que la máquina virtual tenga al menos 20 GB de espacio libre en disco.
> - Durante la importación de imágenes, puede suscribirse a Office 2016 o 2019, pero no a Office 2021. Para Office 2021 y otras aplicaciones, como Microsoft Visio 2021 y Microsoft Project 2021, consulte Administrar aplicaciones.
> - Para llevar tus propias licencias de Microsoft 365 para aplicaciones de escritorio y de navegador a Amazon WorkSpaces, instala las aplicaciones de Microsoft 365 en tu imagen BYOL una vez finalizado el proceso de ingesta de imágenes BYOL.

> **Note**
>
> Las imágenes BYOL de Graphics.g4dn GraphicsPro y.g4dn solo son compatibles con Office 2019 y no con Office 2016.

Si decide suscribirse a Office, el proceso de ingesta de imágenes BYOL tarda un mínimo de 3 horas.

Para obtener más información sobre cómo suscribirse a Office durante el proceso de ingesta BYOL, consulte Paso 6: Cree una imagen BYOL mediante la consola WorkSpaces .

Configuración de idioma de Office

Elegimos el idioma de tu suscripción a Office en función de la AWS región en la que vayas a realizar la ingesta de imágenes BYOL. Por ejemplo, si realiza la ingesta de imágenes BYOL en la región Asia-Pacífico (Tokio), el idioma de su suscripción de Office es el japonés.

De forma predeterminada, instalamos en tu ordenador varios paquetes de idiomas de Office de uso frecuente. WorkSpaces Si el paquete de idioma que desea no está instalado, puede descargar paquetes de idioma adicionales de Microsoft. Para obtener más información, consulte Paquete accesorio de idioma para Microsoft 365 en la documentación de Microsoft.

Para cambiar el idioma de Office, tiene varias opciones:

Opción 1: permitir que los usuarios individuales personalicen la configuración de idioma de Office

Los usuarios individuales pueden ajustar la configuración de idioma de Office en sus propios idiomas WorkSpaces. Para obtener más información, consulte Agregue un idioma de edición o establezca preferencias de idioma en Office en la documentación de Microsoft.

Opción 2: utilice las plantillas administrativas de GPO (.admx/.adml) para aplicar la configuración de idioma predeterminada de Office a todos los usuarios WorkSpaces

Puede usar la configuración de objetos de política de grupo (GPO) para aplicar la configuración de idioma de Office predeterminada a sus usuarios. WorkSpaces

> **Note**
>
> Sus WorkSpaces usuarios no podrán anular la configuración de idioma impuesta mediante el GPO.

Para obtener más información sobre el uso de GPO para establecer el idioma de Office, consulte Personalizar la instalación y la configuración de idioma de Office en la documentación de Microsoft. Office 2016 y Office 2019 usan la misma configuración de GPO (etiquetada con Office 2016).

Para trabajar con los GPO, debe instalar las herramientas de administración de Active Directory. Para obtener información sobre el uso de las herramientas de administración de Active Directory para trabajar con GPO, consulte Configurar las herramientas de administración de Active Directory para WorkSpaces.

Antes de poder configurar las políticas de Office 2016 u Office 2019, debe descargar los archivos de plantilla administrativa (.admx/.adml) de Office desde el Centro de descarga de Microsoft. Tras descargar los archivos de plantilla administrativa, debe añadir los `office16.adml` archivos `office16.admx` y al almacén central del controlador de dominio de su WorkSpaces directorio. (Los archivos `office16.admx` y `office16.adml` se aplican tanto a Office 2016 como a Office 2019). Para obtener más información sobre cómo trabajar con archivos `.admx` y `.adml`, consulte Cómo crear y administrar el almacén central de plantillas administrativas de políticas de grupo en Windows en la documentación de Microsoft.

En el siguiente procedimiento se describe cómo crear el almacén central y agregarle los archivos de plantilla administrativa. Realice el siguiente procedimiento en una instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su WorkSpaces directorio.

Para instalar los archivos de plantilla administrativa de política de grupo para Office

1. Descargue los archivos de plantillas administrativas (.admx/.adml) para Office desde el Centro de descarga de Microsoft.
2. En una administración de directorios WorkSpace o en una instancia de Amazon EC2 que esté unida a su WorkSpaces directorio, abra el Explorador de archivos de Windows y, en la barra de direcciones, introduzca el nombre de dominio completo (FQDN) de su organización, como. `\\example.com`
3. Abra la carpeta `SYSVOL`.
4. Abra la carpeta con el nombre *`FQDN`*.
5. Abra la carpeta `Policies`. Debería acceder a `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies`.
6. Si no existe, cree una carpeta llamada `PolicyDefinitions`.
7. Abra la carpeta `PolicyDefinitions`.
8. Copie el archivo `office16.admx` en la carpeta `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions`.

9. Cree una carpeta denominada `en-US` dentro de la carpeta `PolicyDefinitions`.
10. Abra la carpeta `en-US`.
11. Copie el archivo `office16.adml` en la carpeta `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`.

Para configurar los ajustes de idioma del GPO para Office

1. En la instancia de administración de directorios WorkSpace o Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo ()gpmc.msc.
2. Amplíe el bosque (bosque: ***FQDN***).
3. Amplíe Dominios.
4. Amplíe su FQDN (por ejemplo, `example.com`).
5. Seleccione su FQDN, abra el menú contextual (clic con el botón derecho) o abra el menú Acción y elija Crear un GPO en este dominio y vincularlo aquí.
6. Asigne un nombre a su GPO (por ejemplo, **`Office`**).
7. Seleccione su GPO, abra el menú contextual (clic con el botón derecho) o abra el menú Acción y elija Editar.
8. En el Editor de administración de políticas de grupo, seleccione Configuración de usuario, Políticas, Definiciones de políticas de plantillas administrativas (archivos ADMX) recuperadas del ordenador local, Microsoft Office 2016 y Preferencias de idioma.

   > **Note**
   >
   > Office 2016 y Office 2019 usan la misma configuración de GPO (etiquetada con Office 2016). Si no ve Definiciones de políticas de plantillas administrativas (archivos ADMX) recuperadas del ordenador local en Configuración de usuario, Políticas, los archivos `office16.admx` y `office16.adml` no están instalados correctamente en el controlador de dominio.

9. En Preferencias de idioma, especifique el idioma que desea para la siguiente configuración. Asegúrese de establecer cada configuración en Habilitada y, a continuación, en Opciones, seleccione el idioma que desee. Seleccione Aceptar para guardar la configuración.

   - Idioma de visualización > Mostrar ayuda en
   - Idioma de visualización > Mostrar menús y cuadros de diálogo en

- Idiomas de edición > Idioma de edición principal

10. Cierre la herramienta de administración de políticas de grupo cuando termine.
11. Los cambios en la configuración de la política de grupo se aplican después de la siguiente actualización de la política de grupo WorkSpace y después de que se reinicie la WorkSpace sesión. Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:

    - Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).
    - En el símbolo del sistema administrativo, introduzca gpupdate /force.

Opción 3: actualice la configuración del registro de idiomas de Office en su WorkSpaces

Para establecer la configuración de idioma de Office a través del registro, actualice la siguiente configuración del registro:

- HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Office\ 16.0\ Common\\ UILanguage LanguageResources
- HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Office\ 16.0\ Common\\ LanguageResources HelpLanguage

Para esta configuración, añada un valor de clave DWORD con el ID de configuración regional de Office (LCID) correspondiente. Por ejemplo, el LCID para inglés (EE. UU.) es 1033. Como los LCID son valores decimales, debe establecer la opción Base para el valor DWORD en Decimal. Para obtener una lista de los LCID de Office, consulte Identificadores de idioma y valores de OptionState ID en Office 2016 en la documentación de Microsoft.

Puede aplicar esta configuración de registro a su cuenta mediante la configuración de GPO o WorkSpaces mediante un script de inicio de sesión.

Para obtener más información sobre el uso de GPO para establecer el idioma de Office, consulte Personalizar la instalación y la configuración de idioma de Office en la documentación de Microsoft.

Agregue Office a su BYOL existente WorkSpaces

También puedes añadir una suscripción a Office a tu BYOL actual de la WorkSpaces siguiente manera.

- Administrar aplicaciones (recomendado): puedes instalar y configurar Microsoft Office, Microsoft Visio o Microsoft Project 2021 en las existentes WorkSpaces. Para obtener más información, consulte Administrar aplicaciones.
- Migrar un WorkSpace paquete BYOL con Office instalado, puedes usar la función de WorkSpaces migración para migrar tu BYOL actual WorkSpaces al paquete BYOL suscrito a Office. Para obtener más información, consulte Migrar un WorkSpace.

> **Note**
>
> La opción administrar aplicaciones está disponible para instalar Microsoft Office 2021 y otras aplicaciones, como Microsoft Visio 2021 y Microsoft Project 2021, en su WorkSpaces dispositivo. Para instalar Microsoft Office 2016 o 2019 en su dispositivo WorkSpaces, utiliceMigrar un WorkSpace.

Migre entre versiones de Microsoft Office

Para migrar de una versión de Microsoft Office a otra, tiene las siguientes opciones:

- Administrar aplicaciones (recomendado): puedes desinstalar la versión original de Office e instalar Office 2021 y otras aplicaciones, como Microsoft Visio 2021 y Microsoft Project 2021, en la existente WorkSpaces. Por ejemplo, para migrar de Microsoft Office 2019 a Microsoft Office 2021, utilice el flujo de trabajo de administración de aplicaciones para desinstalar Microsoft Office 2019 e instalar Microsoft Office 2021. Para obtener más información, consulte Administrar aplicaciones.
- Migrar un WorkSpace: para migrar de Microsoft Office 2016 a Microsoft Office 2019 o de Microsoft Office 2019 a Microsoft Office 2016, debe crear un paquete BYOL que esté suscrito a la versión de Office a la que desee migrar. A continuación, utilice la función de WorkSpaces migración para migrar los BYOL actuales WorkSpaces que estén suscritos a Office al paquete BYOL suscrito a la versión de Office a la que desee migrar. Por ejemplo, para migrar de Microsoft Office 2016 a Microsoft Office 2019, cree un paquete BYOL suscrito a Microsoft Office 2019. A continuación, utilice la función de WorkSpaces migración para migrar los BYOL actuales WorkSpaces que estén suscritos a Office 2016 al paquete BYOL suscrito a Office 2019. Para obtener más información, consulte Migrar un. WorkSpace

Puede usar estas opciones para migrar las aplicaciones WorkSpaces que están suscritas a Microsoft Office AWS a las aplicaciones de Microsoft 365. Sin embargo, administrar aplicaciones se limita a

desinstalar Microsoft Office de su WorkSpace. Debe traer sus propias herramientas e instaladores para instalar las aplicaciones de Microsoft 365 en su WorkSpaces.

> **Note**
>
> Mediante la administración de aplicaciones, puede instalar o desinstalar Microsoft Office, Microsoft Visio o MicrosoftProject 2021 en su WorkSpaces. Para las versiones de Microsoft Office 2016 o 2019, solo puedes eliminarlas de tu WorkSpaces. Para instalar Microsoft Office 2016 o 2019 en su WorkSpaces, migre un WorkSpace.

Para obtener información sobre el proceso de migración, consulte Migrar un WorkSpace.

Cancelar suscripción a Office

Para cancelar su suscripción a Office, tiene las siguientes opciones.

- Administrar aplicaciones (recomendado): puede desinstalar Microsoft Office y otras aplicaciones, como Microsoft Visio y Microsoft Project, de su WorkSpaces. Para obtener más información, consulte Administrar aplicaciones.
- Migrar a WorkSpace: puede crear un paquete BYOL que no esté suscrito a Office. A continuación, utilice la función de WorkSpaces migración para migrar el BYOL existente WorkSpaces al paquete BYOL que no esté suscrito a Office. Para obtener más información, consulte Migrar un WorkSpace.

Actualizaciones de Office

Si te has suscrito a Office mediante AWS, las actualizaciones de Office se incluyen como parte de las actualizaciones habituales de Windows. Para estar al día de todos los parches y actualizaciones de seguridad, te recomendamos que actualices periódicamente tus imágenes base de BYOL.

Paso 1: Comprueba si tu cuenta es apta para BYOL mediante la consola de Amazon WorkSpaces

Para poder habilitar su cuenta para BYOL, debe pasar por un proceso de verificación para confirmar que cumple los requisitos correspondientes. Hasta que no realices este proceso, la opción Habilitar BYOL no estará disponible en tu WorkSpaces consola de Amazon.

> **Note**
>
> El proceso de verificación tarda al menos un día laborable. Si desea aplicar el rango CIDR y las configuraciones BYOL de una AWS cuenta existente a otra diferente, puede vincularlas para usar el mismo hardware subyacente. Para vincular sus AWS cuentas, no necesita enviar un ticket de soporte. Puedes usar API, por ejemplo, CreateAccountLinkInvitationsy AcceptAccountLinkInvitationpara conectar tus AWS cuentas. Para obtener más información, consulte Vincule cuentas BYOL.

Para comprobar si tu cuenta es apta para BYOL mediante la consola de Amazon WorkSpaces

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, selecciona Configuración de la cuenta y, a continuación, en Traiga su propia licencia (BYOL), elija Ver la configuración de WorkSpaces BYOL. Si su cuenta no cumple actualmente los requisitos de BYOL, un mensaje proporciona orientación sobre los siguientes pasos. Para empezar, ponte en contacto con tu gestor de AWS cuentas o con tu representante de ventas, o ponte en contacto con el AWS Support Centro. Su contacto verificará su elegibilidad para BYOL.

   Para determinar si reúne los requisitos para BYOL, su contacto necesitará cierta información suya. Por ejemplo, es posible que se le pida que responda a las preguntas siguientes.

   - ¿Ha revisado y aceptado los requisitos de BYOL enumerados anteriormente?
   - ¿En qué AWS regiones necesita que su cuenta esté habilitada para BYOL?
   - ¿Cuántos BYOL planea implementar por AWS región WorkSpaces ?
   - ¿Cuál es su plan de puesta en marcha?
   - ¿Va a comprar WorkSpaces a un distribuidor?
   - ¿Qué tipos de paquetes necesita para BYOL?
   - ¿Su organización tiene otras AWS cuentas habilitadas para el BYOL en la misma región? En caso afirmativo, ¿desea vincular estas cuentas para que usen el mismo hardware subyacente?

     Si las cuentas están vinculadas, el número total de cuentas WorkSpaces desplegadas en estas cuentas se suma para determinar su aptitud para el BYOL. Si la respuesta a estas dos preguntas es afirmativa, puede vincular sus cuentas entre sí. Puedes usar las API, por ejemplo, CreateAccountLinkInvitationsy AcceptAccountLinkInvitationpara conectar tus AWS

cuentas. Si quieres vincular otras cuentas compatibles con BYOL, pero quieres usar una configuración de BYOL diferente (rango e imagen CIDR), ponte en contacto con AWS Support para habilitar tu nueva cuenta para BYOL.

3. Una vez que se confirme tu aptitud para BYOL, puedes continuar con el siguiente paso, en el que habilitas BYOL para tu cuenta en la consola de Amazon WorkSpaces .

Paso 2: Activa BYOL para tu cuenta de BYOL mediante la consola de Amazon WorkSpaces

Para habilitar BYOL para su cuenta, debe especificar una interfaz de red de administración. Esta interfaz está conectada a una red de WorkSpaces administración segura de Amazon. Se utiliza para la transmisión interactiva del WorkSpace escritorio a los WorkSpaces clientes de Amazon y para permitir que Amazon WorkSpaces administre el WorkSpace.

> **Note**
>
> Solo tiene que realizar los pasos de este procedimiento una vez por región para activar BYOL en su cuenta.

Para habilitar BYOL en tu cuenta mediante la consola de Amazon WorkSpaces

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, selecciona Configuración de la cuenta y, a continuación, en Traiga su propia licencia (BYOL), elija Ver la configuración de WorkSpaces BYOL.
3. En la página Configuraciones de la cuenta, en Traiga su propia licencia (BYOL), seleccione Habilitar BYOL.

   Si no aparece la opción Habilitar BYOL, significa que su cuenta no cumple los requisitos para utilizar esta opción. Para obtener más información, consulte Paso 1: Comprueba si tu cuenta es apta para BYOL mediante la consola de Amazon WorkSpaces .
4. En Bring Your Own License (BYOL) (Traiga su propia licencia), en el área Management network interface IP address range (Rango de direcciones IP de interfaz de red de administración), elija un rango de direcciones IP y, a continuación, elija Display available CIDR blocks (Mostrar bloques de CIDR disponibles).

Amazon WorkSpaces busca y muestra los rangos de direcciones IP disponibles como bloques de enrutamiento entre dominios sin clase (CIDR) IPv4, dentro del rango que especifique. Si requiere un rango de direcciones IP específico, puede editar el rango de búsqueda.

> **Important**
>
> Después de especificar un intevalo de direcciones IP, no puede modificarlo. Asegúrese de especificar un intervalo de direcciones IP que no entre en conflicto con los intervalos que utiliza su red interna. Si tiene alguna duda sobre qué rango debe especificar, póngase en contacto con su gerente de AWS cuentas o representante de ventas, o póngase en contacto con el AWS Support Centro antes de continuar.

5. Elija el bloque de CIDR que desee en la lista de resultados y, a continuación, elija Enable BYOL (Habilitar BYOL).

   Este proceso puede tardar varias horas. Mientras WorkSpaces habilita su cuenta para BYOL, continúe con el siguiente paso.

Paso 3: Ejecute el PowerShell script BYOL Checker en una máquina virtual Windows

Después de habilitar BYOL para su cuenta, debe confirmar que su máquina virtual cumple los requisitos para BYOL. Para ello, lleve a cabo estos pasos para descargar y ejecutar el script WorkSpaces BYOL Checker. PowerShell El script realiza una serie de pruebas sobre la máquina virtual que tiene previsto usar para crear su imagen.

> **Important**
>
> La máquina virtual debe superar todas las pruebas antes de que pueda usarla para BYOL.

Para descargar el script de comprobador de BYOL

Antes de que descargue y ejecute el script de comprobador de BYOL, verifique que las últimas actualizaciones de seguridad de Windows están instaladas en su máquina virtual. Mientras se ejecuta este script, deshabilita el servicio Windows Update.

1. Descargue el archivo.zip del script BYOL Checker desde https://tools.amazonworkspaces.com/BYOLChecker.zip a su carpeta. `Downloads`
2. En la carpeta `Downloads`, cree una carpeta `BYOL`.
3. Extraiga los archivos de `BYOLChecker.zip` y cópielos en la carpeta `Downloads\BYOL`.
4. Elimine la carpeta `Downloads\BYOLChecker.zip` para que solo queden los archivos extraídos.

Siga estos pasos para ejecutar el script de comprobador de BYOL.

Para ejecutar el script de comprobador de BYOL

1. Desde el escritorio de Windows, abra Windows. PowerShell Pulse el botón Inicio de Windows, haga clic con el botón derecho en Windows PowerShell y seleccione Ejecutar como administrador. Si el Control de cuentas de usuario le pide que elija si desea PowerShell realizar cambios en el dispositivo, seleccione Sí.
2. En la PowerShell línea de comandos, vaya al directorio en el que se encuentra el script BYOL Checker. Por ejemplo, si el script está ubicado en el directorio `Downloads\BYOL`, escriba los comandos siguientes y pulse Intro:

   ```
   cd C:\Users\username\Downloads\BYOL
   ```
3. Introduzca el siguiente comando para actualizar la política de PowerShell ejecución en el equipo. Esto le permite que el script de comprobador de BYOL ejecute:

   ```
   Set-ExecutionPolicy AllSigned
   ```
4. Cuando se le pida que confirme si desea cambiar la política de PowerShell ejecución, introduzca A para especificar Sí a todas.
5. Escriba el comando siguiente para ejecutar el script de comprobador de BYOL:

   ```
   .\BYOLChecker.ps1
   ```
6. Si aparece una notificación de seguridad, pulse la tecla R para ejecutar una vez.
7. En el cuadro de diálogo de validación de WorkSpaces imágenes, seleccione Comenzar pruebas.
8. Tras completarse cada prueba, puede ver el estado de la prueba. Para cualquier prueba con el estado FAILED (Error), elija Info (Información) para mostrar información sobre cómo resolver el problema que provocó el error. Si alguna prueba muestra el estado WARNING (Advertencia), elija el botón Fix all Warnings (Solucionar todos los mensajes de advertencia).

9. Si procede, resuelva los problemas que provoquen errores y advertencias de prueba y repita los pasos Step 7 y Step 8 hasta que la máquina virtual supere todas las pruebas. Deben resolverse todos los errores y advertencias antes de que exporte la máquina virtual.
10. El comprobador del script de BYOL genera dos archivos de registro, `BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` y `ImageInfo.text`. Estos archivos se encuentran en el directorio que contiene los archivos de script del comprobador de BYOL.

    > **Tip**
    >
    > No elimine estos archivos. Si se produce un problema, es posible que resulten útiles para solucionarlo.

11. Después de que su máquina virtual pase todas las pruebas, aparecerá el mensaje Validation Successful (Validación exitosa). Revise los ajustes de configuración regional de la máquina virtual que se muestran en la herramienta. Para actualizar los ajustes de configuración regionales, siga estas instrucciones en la documentación de Microsoft y ejecute de nuevo el script del comprobador de BYOL.
12. Apague la máquina virtual y cree una instantánea de la misma.
13. Vuelva a iniciar la máquina virtual. Elija Run Sysprep (Ejecutar Sysprep). Si Sysprep se ejecuta correctamente, la máquina virtual que exportó después de Step 12 podrá importarse en Amazon Elastic Compute Cloud (Amazon EC2). De lo contrario, revise los registros de Sysprep, vuelva a la instantánea tomada en Step 12, resuelva los problemas notificados, realice una nueva instantánea y vuelva a ejecutar el script del comprobador de BYOL.

    El motivo más común por el que se produce un error en Sysprep es que no están desinstalados los Modern AppX Packages para todos los usuarios. Utilice el Remove-AppxPackage PowerShell cmdlet para eliminar los paquetes de AppX.
14. Una vez que haya creado correctamente la imagen, puede eliminar la cuenta _BYOL. WorkSpaces

Lista de mensajes de error y correcciones de errores

La importación de BYOL requiere Powershell 4.0 o una versión posterior. La versión instalada de no PowerShell es compatible.

PowerShell debe estar instalada la versión 4.0 o posterior. Para obtener más información, consulte Microsoft Windows PowerShell.

La importación BYOL no admite sistemas con Microsoft Office activo instalado.

Microsoft Office debe desinstalarse antes de la importación. Para obtener más información, consulte Desinstalar Office de un equipo PC.

La importación de BYOL requiere un sistema sin un agente PCoIP.

Desinstale el agente PCoIP. Para obtener información sobre la desinstalación del agente PCoIP, consulte cómo desinstalar el cliente de software PCoIP de Teradici para Mac

La importación de BYOL requiere que las actualizaciones de Windows estén deshabilitadas.

Deshabilite las actualizaciones de Windows siguiendo estos pasos:

1. Pulse la tecla Windows + R. Escriba `services.msc` y, a continuación, pulse Intro.
2. Haga clic con el botón derecho en Windows Update y, a continuación, seleccione Propiedades.
3. En la pestaña General, defina el Tipo de inicio como Desactivado.
4. Elija Detener.
5. Elija Aplicar y, después, Aceptar.
6. Reinicie el equipo.

La importación de BYOL requiere que la opción Montaje automático esté activada.

Debe activar la opción Montaje automático. Abra PowerShell como administrador y ejecute el siguiente comando:

```
C:\> diskpart
DISKPART> automount enable
```

Se ha activado el montaje automático de nuevos volúmenes.

La importación BYOL requiere que la cuenta WorkSpaces _BYOL esté habilitada

WorkSpacesLa cuenta _BYOL debe estar habilitada. Para obtener más información, consulta Cómo habilitar BYOL en tu cuenta para BYOL mediante la consola de Amazon WorkSpaces .

La importación de BYOL requiere que la interfaz de red utilice DHCP para asignar automáticamente una dirección IP. La interfaz de red utiliza una dirección IP estática.

Se debe cambiar la interfaz de red para utilizar DHCP. Para obtener más información, consulte Cambiar la configuración de TCP/IP.

La importación de BYOL requiere más de 20 GB de espacio en el disco local.

El disco local debe tener suficiente espacio y requiere que libere 20 GB o más.

La importación de BYOL requiere sistemas con 1 unidad local. Hay unidades locales, extraíbles o de red adicionales.

Solo las unidades C y D pueden estar presentes en una WorkSpace que se utilice para importar una imagen. Elimine todas las demás unidades, incluidas las unidades virtuales.

La importación de BYOL requiere Windows 10 o Windows 11.

Utilice un sistema operativo Windows 10 o Windows 11.

La importación de BYOL requiere que los sistemas que no estén unidos a un dominio de AD.

El sistema debe estar separado del dominio AD. Para obtener más información, consulte las preguntas frecuentes sobre la administración de dispositivos de Azure Active Directory.

La importación de BYOL requiere que los sistemas que no estén unidos a un dominio de Azure.

El sistema debe estar separado del dominio de Azure. Para obtener más información, consulte las preguntas frecuentes sobre la administración de dispositivos de Azure Active Directory.

La importación de BYOL requiere que el firewall público de Windows esté desactivado.

El perfil de firewall público debe estar deshabilitado. Para obtener más información, consulte Activar o desactivar el Firewall de Microsoft Defender.

La importación de BYOL requiere un sistema sin VMware Tools.

Debe desinstalar VMware Tools. Para obtener más información, consulte Desinstalar e instalar VMware Tools manualmente en VMware Fusion (1014522).

La importación de BYOL requiere que el disco local sea inferior a 80 GB.

El archivo debe tener un tamaño inferior a 80 GB. Reduzca el tamaño del disco.

La importación de BYOL requiere menos de 2 particiones en la unidad local. Además, todas las particiones de Windows 10 deben estar particionadas en MBR y todas las particiones de Windows 11 deben estar particionadas en GPT.

Los volúmenes deben estar particionados en MBR para Windows 10 y GPT en Windows 11. Para obtener más información, consulte Administración de discos.

La importación de BYOL requiere que se hayan completado todas las actualizaciones pendientes que requieran reinicios.

Instale todas las actualizaciones y reinicie el sistema operativo.

La importación BYOL requiere que AutoLogon esté deshabilitada.

Para deshabilitar el AutoLogon registro:

1. Pulse la tecla Windows + R y escriba `Regedit.exe` en la línea de comandos.
2. Desplácese hasta `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`.
3. Añada un valor para `DontDisplayLastUserName`.
4. En Tipo, escriba `REG_SZ`.
5. En Valor, introduzca `0`.

> **Note**
>
> - El valor `DontDisplayLastUserName` determina si el cuadro de diálogo de inicio de sesión muestra el nombre de usuario del último usuario que inició sesión en el PC.
> - El nombre no existe por defecto. Si existe, debe configurarlo en `0` o el valor de se `DefaultUser` borrará y AutoLogon fallará.

La importación mediante BYOL debe estar habilitada **`RealTimeIsUniversal`**.

RealTimeUniversal La clave de registro debe estar habilitada. Para obtener más información, consulte Configuración de hora para Windows Server 2008 y posterior.

La importación de BYOL requiere un sistema con una partición de arranque.

El número de particiones de arranque no debe ser superior a una.

Para eliminar particiones adicionales

1. Pulsa el logotipo de Windows + las teclas R para abrir el cuadro Ejecutar. Introduzca `msconfig` y pulse la tecla Intro del teclado para abrir la ventana de configuración del sistema.
2. Seleccione la pestaña de arranque en la ventana y compruebe si el sistema operativo que desea utilizar está configurado como Sistema operativo actual; Sistema operativo predeterminado. Si no está configurado, elija el sistema operativo que desee en la ventana y elija Definir por defecto en la misma ventana.
3. Para eliminar otra partición, selecciónela y, a continuación, seleccione Eliminar, Aplicar y Aceptar.

Si el error persiste, arranque el ordenador desde el disco de instalación o reparación y siga estos pasos.

1. Omita la pantalla de idiomas inicial y, a continuación, seleccione Reparar el equipo en la pantalla principal de instalación.
2. En la pantalla Elija una opción, seleccione Solucionar problemas.
3. En la pantalla Opciones avanzadas, seleccione Símbolos del sistema.
4. En el símbolo del sistema, escriba `bootrec.exe /fixmbr` y, a continuación, pulse Intro.

La importación de BYOL requiere un sistema de 64 bits.

Debe utilizarse una imagen del sistema operativo de 64 bits. Para obtener más información, consulte Versiones de Windows compatibles con BYOL.

La importación de BYOL requiere un sistema que no se haya rearmado.

El recuento de imágenes rearmadas no debe ser 0. La característica "rearmar" le permite ampliar el periodo de activación de la versión de prueba de Windows. El proceso Crear imagen requiere que el recuento de rearmados sea un valor distinto de 0.

Para comprobar el recuento de rearmados de Windows

1. En el menú Inicio de Windows, elija Sistema de Windows, y, a continuación, elija Símbolo del sistema.
2. En el símbolo del sistema, escriba `cscript C:\Windows\System32\slmgr.vbs /dlv` y pulse Intro.
3. Para restablecer el recuento de rearme a un valor distinto de 0. Para obtener más información, consulte Ejecutar Sysprep (Generalize) en una instalación de Windows.

La importación de BYOL requiere un sistema que no se haya actualizado in situ. Este sistema se ha actualizado in situ.

Windows no se debe haber actualizado desde una versión anterior.

La importación mediante BYOL requiere que no haya ningún antivirus instalado en el sistema.

Debe desinstalar el software antivirus. Ejecute BYOLChecker para obtener los detalles del software antivirus que va a desinstalar.

La importación mediante BYOL requiere que los sistemas Windows 10 tengan un modo de arranque antiguo.

La BIOS antigua BootMode debe usarse en Windows 10. Para obtener más información, consulte Modos de arranque.

Paso 4: exportar la máquina virtual desde su entorno de virtualización

Para crear una imagen para BYOL, primero debe exportar la máquina virtual desde su entorno de virtualización. La máquina virtual debe estar en un solo volumen con un tamaño máximo de 70 GB y al menos 10 GB de espacio libre. Para obtener más información, consulte la documentación para su entorno de virtualización y Exportar la máquina virtual desde el entorno de virtualización en la Guía del usuario de VM Import/Export.

Windows 11 establece nuevos requisitos de hardware para la interfaz de firmware extensible unificada (UEFI), el módulo de plataforma segura (TPM) 2.0 y la compatibilidad con el arranque seguro. Exclusivo de las importaciones de Windows 11, VM Import/Export habilita automáticamente el arranque seguro de UEFI mediante claves de Microsoft y NitroTPM. Para obtener más información, consulte Cómo transferir la imagen de Windows 11 a AWS con VM Import/Export.

Paso 5: importar la máquina virtual como imagen en Amazon EC2

Después de exportar su máquina virtual, revise los requisitos de importación de sistemas operativos Windows desde una máquina virtual. Realice las acciones necesarias. Para obtener más información, consulte Requisitos de VM Import/Export.

> **Note**
>
> No se admite la importación de una máquina virtual con un disco cifrado. Si ha optado por el cifrado predeterminado para volúmenes de Amazon Elastic Block Store (Amazon EBS), debe anular la selección de esa opción antes de importar la máquina virtual.

Importe la máquina virtual en como una imagen de máquina de Amazon (AMI). Utilice uno de los siguientes métodos:

- Utilice el comando import-image en la AWS CLI. Para obtener más información, consulte import-image en la Referencia de comandos de la AWS CLI .
- Use la operación ImportImage de la API. Para obtener más información, consulte ImportImagela referencia de la API de Amazon EC2.

Para obtener más información, consulte Importación de una VM como una imagen en la Guía del usuario de VM Import/Export.

Paso 6: Cree una imagen BYOL mediante la consola WorkSpaces

Realice estos pasos para crear una imagen WorkSpaces BYOL.

> **Note**
>
> Para realizar este procedimiento, compruebe que tiene permisos AWS Identity and Access Management (de IAM) para:

- Llame WorkSpaces **`ImportWorkspaceImage`**.
- Llamar a Amazon EC2 **`DescribeImages`** en relación con la imagen de Amazon EC2 que desea usar para crear la imagen de BYOL.
- Llamar a Amazon EC2 **`ModifyImageAttribute`** en relación con la imagen de Amazon EC2 que desea usar para crear la imagen de BYOL. Asegúrese de que los permisos de lanzamiento de la imagen de Amazon EC2 no estén restringidos. La imagen debe poder compartirse durante todo el proceso de creación de la imagen BYOL.

Para ver un ejemplo de política de IAM específica para BYOL WorkSpaces, consulte. Gestión de identidades y accesos para WorkSpaces Para obtener más información sobre el uso de permisos de IAM, consulte Cambio de los permisos de un usuario de IAM en la Guía del usuario de IAM.
Para crear un archivo Graphics.g4dn, GraphicsPro .g4dn, Graphics o un GraphicsPro paquete a partir de su imagen, póngase en contacto con el AWS Support Centro para añadir su cuenta a la lista de usuarios permitidos. Una vez que tu cuenta esté en la lista de usuarios permitidos, puedes usar el AWS CLI import-workspace-image comando para incorporar los archivos Graphics.g4dn, .g4dn, Graphics o imagen. GraphicsPro GraphicsPro Para obtener más información, consulte import-workspace-image en la Referencia de comandos de la AWS CLI .

Para crear una imagen de la máquina virtual Windows

1. Abre la consola en https://console.aws.amazon.com/workspaces/. WorkSpaces
2. En el panel de navegación, elija Images.
3. Elija Crear imagen de BYOL.
4. En la página Crear imagen de BYOL, proceda del siguiente modo:
   - Para el ID de AMI, elija el enlace Consola EC2 y la imagen de Amazon EC2 que importó como se describe en la sección anterior (Paso 5: importar la máquina virtual como imagen en Amazon EC2). El nombre de la imagen debe empezar por `ami-`, y debe ir seguido del identificador de la AMI (por ejemplo, `ami-1234567e`).
   - En Nombre de imagen, escriba un nombre único para la imagen.
   - En Descripción, escriba una descripción para ayudarle a identificar rápidamente la imagen.

- Para el tipo de instancia, elija el tipo de paquete adecuado (Regular, Graphics.G4DN, Graphics o GraphicsPro), según el protocolo que desee utilizar para la imagen, ya sea PCoIP o Streaming Protocol (WSP). WorkSpaces Si quieres crear un paquete .g4dn, elige Graphics.g4dn. GraphicsPro Para los paquetes no compatibles con la GPU (paquetes que no sean Graphics.g4dn, .g4dn, Graphics o), selecciona Normal. GraphicsPro GraphicsPro

  > **Note**
  >
  > - Por el momento, solo se pueden crear gráficos. G4dn, .g4dn, gráficos e imágenes para el protocolo PCoIP. GraphicsPro GraphicsPro
  > - Las imágenes de Windows 11 solo se pueden crear para el protocolo WSP.
  > - Los paquetes Graphics.g4dn y .g4dn no están disponibles actualmente para Windows 11. GraphicsPro
  > - Los gráficos y las imágenes no son compatibles con Windows 11. GraphicsPro

- (Opcional) En Seleccionar aplicaciones, elija la versión de Microsoft Office a la que desee suscribirse. Para obtener más información, consulte Añada Microsoft Office a su imagen BYOL.
- (Opcional) En Etiquetas, seleccione Añadir nueva etiqueta para asociar las etiquetas a esta imagen. Para obtener más información, consulte Etiquetado de recursos de WorkSpaces.

5. Elija Crear imagen de BYOL.

   Aunque la imagen se está creando, su estado en la página Imágenes de la consola aparece como Pendiente. El proceso de ingestión de BYOL tarda un mínimo de 90 minutos. Si también se ha suscrito a Office, el proceso tardará como mínimo 3 horas.

   Si la validación de imágenes no se realiza correctamente, la consola muestra un código de error. Cuando se complete la creación de imágenes, el estado cambiará a Available (Disponible).

Paso 7: crear un paquete personalizado a partir de la imagen de BYOL

Tras crearse su imagen de BYOL, puede usar la imagen para crear un paquete personalizado. Para obtener más información, consulte Crea una WorkSpaces imagen y un paquete personalizados.

Paso 8: Registre un directorio dedicado para WorkSpaces

Para utilizar imágenes BYOL WorkSpaces, debe registrar un directorio con este fin.

Para registrar un directorio para WorkSpaces

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Actions (Acciones), Register (Registrar).
4. En el cuadro de diálogo Registrar directorio, en Habilitar el directorio dedicado WorkSpaces, seleccione Sí.
5. Elija Registro.

Si ya ha registrado un AWS Managed Microsoft AD directorio o un directorio de AD Connector WorkSpaces que no se ejecute en hardware dedicado, puede configurar un nuevo AWS Managed Microsoft AD directorio o un directorio de AD Connector para este fin. También puedes anular el registro del directorio y volver a registrarlo como directorio dedicado. WorkSpaces Para ello, siga estos pasos.

> **Note**
>
> Solo puede realizar este procedimiento si no WorkSpaces hay ninguno asociado al directorio.

Para anular el registro de un directorio y volver a registrarlo como dedicado WorkSpaces

1. Abra la consola en https://console.aws.amazon.com/workspaces/ WorkSpaces .
2. Termine la existente WorkSpaces.
3. En el panel de navegación, elija Directories (Directorios).
4. Seleccione el directorio y elija Actions, Deregister.
5. Cuando se le pida que confirme, elija Deregister.
6. Seleccione de nuevo el directorio y elija Actions (Acciones), Register (Registrar).
7. En el cuadro de diálogo Registrar directorio, en Habilitar el directorio dedicado WorkSpaces, seleccione Sí.
8. Elija Registro.

Paso 9: Inicie su BYOL WorkSpaces

Después de registrar un directorio como dedicado WorkSpaces, puede lanzar su BYOL WorkSpaces en este directorio. Para obtener información sobre cómo iniciar WorkSpaces, consulteLanzar un escritorio virtual utilizando WorkSpaces.

Vincule cuentas BYOL

Puede utilizar la vinculación BYOL para vincular cuentas y compartir configuraciones BYOL. Las configuraciones BYOL incluyen el rango CIDR que utilizan sus cuentas y las imágenes que utiliza para crear WorkSpaces con su licencia de Windows. Todas las cuentas vinculadas comparten la misma infraestructura de hardware subyacente.

La cuenta habilitada para la vinculación BYOL es la propietaria principal de la infraestructura de hardware subyacente y se denomina cuenta de origen. La cuenta Source administra el acceso a la infraestructura de hardware subyacente. Las cuentas de destino son las cuentas que están vinculadas a la cuenta de origen.

> **Important**
>
> Las API para vincular cuentas BYOL no están disponibles actualmente en. AWS GovCloud (US) Region

> **Note**
>
> Las AWS cuentas con las que desee vincularse deben formar parte de su organización y estar bajo la misma cuenta de pagador. Solo puede vincular cuentas dentro de la misma región.

Para vincular las cuentas de origen y destino

1. Envíe un enlace de invitación desde su cuenta de origen a la cuenta de destino mediante la CreateAccountLinkInvitationAPI.
2. Acepte el enlace pendiente de su cuenta de Target mediante la AcceptAccountLinkInvitationAPI.
3. Compruebe que el enlace se haya establecido mediante la API GetAccountLinkor ListAccountLinks.

Supervisa tu WorkSpaces

Puede utilizar las siguientes funciones para monitorear su WorkSpaces.

CloudWatch métricas

Amazon WorkSpaces publica puntos de datos en Amazon CloudWatch sobre su WorkSpaces. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Puede utilizar estas métricas para comprobar que su rendimiento WorkSpaces es el esperado. Para obtener más información, consulte Supervise sus CloudWatch métricas WorkSpaces de uso.

CloudWatch Eventos

Amazon WorkSpaces puede enviar eventos a Amazon CloudWatch Events cuando los usuarios inicien sesión en tu WorkSpace. Esto le permite responder al producirse el evento. Para obtener más información, consulte Supervisa tu WorkSpaces uso de Amazon EventBridge.

CloudTrail registros

AWS CloudTrail proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio de AWS en WorkSpaces. Con la información recopilada CloudTrail, puede determinar el destinatario de la solicitud WorkSpaces, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Registrar las llamadas a la WorkSpaces API mediante el uso CloudTrail. AWS CloudTrailregistra los eventos de inicio de sesión correctos y fallidos de los usuarios de tarjetas inteligentes. Para obtener más información, consulte Información sobre los eventos de inicio de sesión de AWS para usuarios de tarjetas inteligentes.

CloudWatch Monitor de Internet

Amazon CloudWatch Internet Monitor proporciona visibilidad sobre cómo los problemas de Internet afectan al rendimiento y la disponibilidad entre las aplicaciones alojadas AWS y los usuarios finales. También puede usar CloudWatch Internet Monitor para:

- Cree monitores para uno o más WorkSpace directorios.
- Supervisar el rendimiento de Internet.
- Genere alarmas en caso de problemas entre la red urbana de sus usuarios finales, incluida su ubicación y la ASN, que suele ser el proveedor de servicios de Internet (ISP), y sus regiones. WorkSpace

Internet Monitor utiliza los datos de conectividad que AWS recopila de su huella en la red global para calcular una línea base de rendimiento y disponibilidad del tráfico de Internet. Actualmente, Internet Monitor no puede proporcionar el rendimiento de Internet a un usuario final individual, pero sí a nivel de ciudad e ISP.

Controle su WorkSpaces salud mediante el panel de control CloudWatch automático

Puede supervisar WorkSpaces mediante un panel de control CloudWatch automático, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Las métricas se guardan durante 15 meses para acceder a la información histórica y supervisar el rendimiento de su aplicación o servicio web. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

El CloudWatch panel de control se crea automáticamente cuando utilizas tu AWS cuenta para configurar tu WorkSpaces. El panel te permite supervisar tus WorkSpaces métricas, como su estado y rendimiento, en todas las regiones. También puede usar el panel para los siguientes fines:

- Identifique los WorkSpace casos en mal estado.
- Identifique los modos de ejecución, los protocolos y los sistemas operativos que tienen WorkSpace instancias en mal estado.
- Vea el uso de los recursos críticos a lo largo del tiempo.
- Identifique las anomalías para ayudar a solucionar problemas.

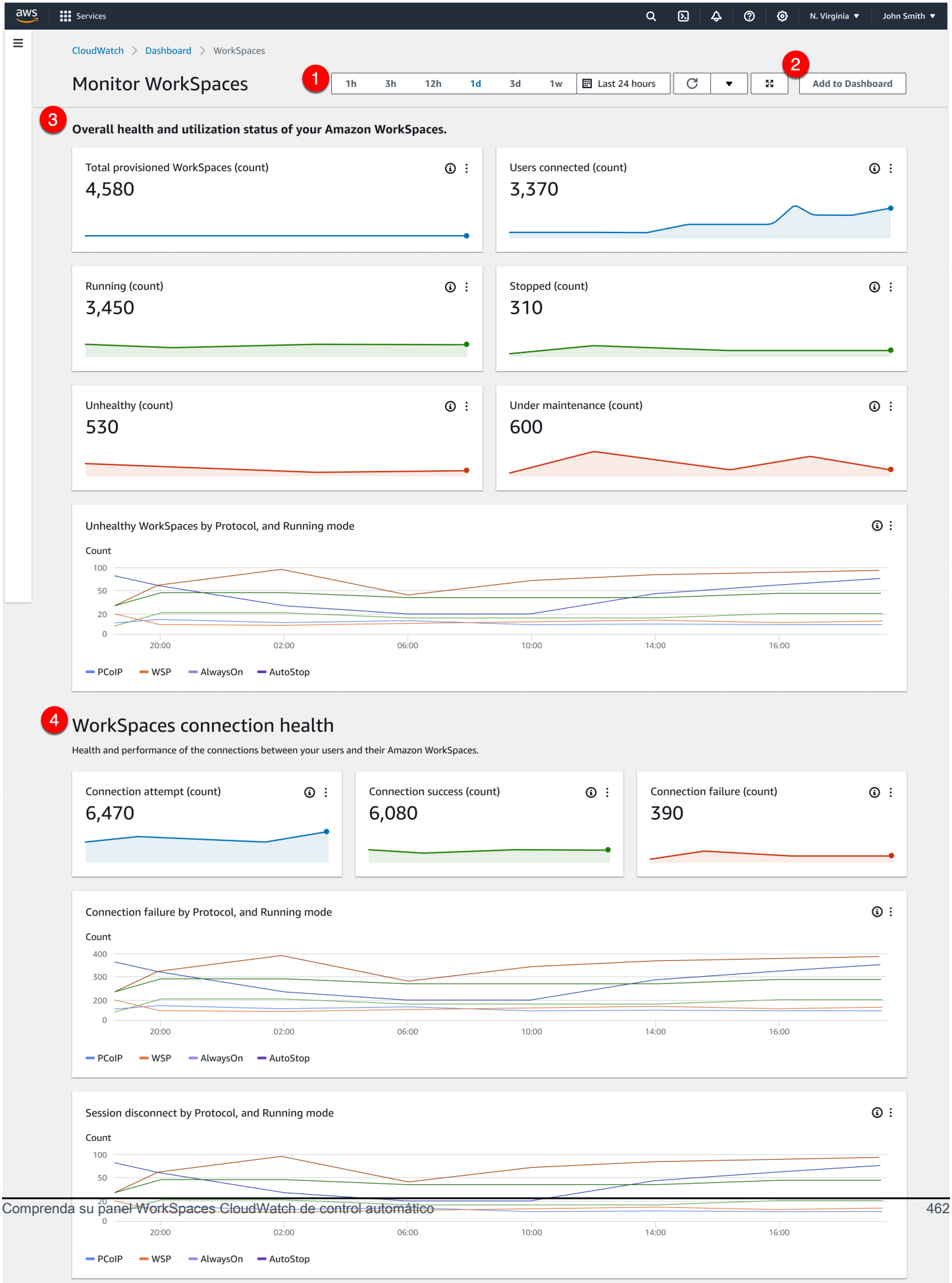
WorkSpaces CloudWatch Los paneles automáticos están disponibles en todas AWS las regiones comerciales.

Para usar el panel de control WorkSpaces CloudWatch automático

1. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Paneles.
3. Seleccione la pestaña Paneles automáticos.
4. Elija WorkSpaces.

Comprenda su panel WorkSpaces CloudWatch de control automático

El panel de control CloudWatch automático le permite obtener información sobre el rendimiento de sus WorkSpaces recursos y le ayuda a identificar los problemas de rendimiento.


aws
Services
N. Virginia
John Smith
CloudWatch
Dashboard
WorkSpaces
Monitor WorkSpaces
1
1h
3h
12h
1d
3d
1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

El panel de control consta de las siguientes funciones:

1. Vea los datos históricos mediante los controles de intervalo de fechas y hora.
2. Agregue una vista de panel personalizada a los paneles CloudWatch personalizados.
3. Supervise su estado general de uso y estado de uso WorkSpaces de la siguiente manera:
    a. Vea el número total de instancias aprovisionadas WorkSpaces, el número de usuarios conectados y el número de WorkSpace instancias en mal estado y en buen estado.
    b. Vea las variables en mal estado WorkSpaces y sus diferentes variables, como el protocolo y el modo de cómputo.
    c. Pase el ratón sobre el gráfico de líneas para ver el número de WorkSpace instancias en buen estado o en mal estado de un protocolo y modo de ejecución específicos durante un período de tiempo.
    d. Selecciona el menú de puntos suspensivos y, a continuación, selecciona Ver en métricas para ver las métricas en un gráfico de escala temporal.
4. Vea las métricas de conexión y sus diferentes variables, como el número de intentos de conexión, las conexiones correctas y las conexiones fallidas en su WorkSpaces entorno en un momento dado.
5. Vea InSession las latencias que afectan a la experiencia del usuario, como el tiempo de ida y vuelta (RTT), para determinar el estado de la conexión y la pérdida de paquetes para supervisar el estado de la red.
6. Vea el rendimiento del host y el uso de los recursos para identificar y solucionar posibles problemas de rendimiento.

Supervise sus CloudWatch métricas WorkSpaces de uso

WorkSpaces y Amazon CloudWatch están integrados, por lo que puedes recopilar y analizar las métricas de rendimiento. Puede monitorizar estas métricas mediante la CloudWatch consola, la interfaz de línea de CloudWatch comandos o mediante programación mediante la CloudWatch API. CloudWatch también permite configurar alarmas cuando se alcanza un umbral específico para una métrica.

Para obtener más información sobre el uso CloudWatch y las alarmas, consulta la Guía del CloudWatch usuario de Amazon.

Requisitos previos

Para obtener CloudWatch las métricas, habilite el acceso en el puerto 443 del `AMAZON` subconjunto de la `us-east-1`región. Para obtener más información, consulte Requisitos de dirección IP y puerto para WorkSpaces.

Contenido

WorkSpaces métricas

El espacio de nombres de `AWS/WorkSpaces` incluye las siguientes métricas.

Métrica	Descripción	Dimensiones	Statistics	Unidades

`Available` [1]	El número WorkSpaces que devolvió un estado saludable.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`Unhealthy` [1]	El número WorkSpaces que devolvió un estado insalubre.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades
		UserName		
ConnectionAttempt [2]	El número de intentos de conexión.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, mínimo, máximo, suma, muestras de datos	Recuento
ConnectionSuccess [2]	El número de conexiones realizadas correctamente.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

`ConnectionFailure` [2]	El número de conexiones que han producido un error.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`SessionLaunchTime` [2, 6]	La cantidad de tiempo que se tarda en iniciar una WorkSpace s sesión.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, mínimo, máximo, suma, muestras de datos	Segundo (tiempo)

`InSessionLatency` [2, 6]	El tiempo de ida y vuelta entre el WorkSpace s cliente y el WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, mínimo, máximo, suma, muestras de datos	Milisegundo (tiempo)

Métrica	Descripción	Dimensiones	Statistics	Unidades
SessionDisconnect [2, 6]	El número de conexiones que se cerraron, incluidas las iniciadas por el usuario y las que produjeron un error.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, mínimo, máximo, suma, muestras de datos	Recuento
UserConnected [3]	El número de los WorkSpaces que tiene un usuario conectado.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, mínimo, máximo, suma, muestras de datos	Recuento
Stopped	El número de los WorkSpaces que están detenidos.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

`Maintenance` [4]	El número de los WorkSpaces que están en mantenimiento.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`TrustedDeviceValidationAttempt` [5, 6]	El número de intentos de validación de la firma de autenticación del dispositivo.	`DirectoryId`	Promedio, mínimo, máximo, suma, muestras de datos	Recuento
`TrustedDeviceValidationSuccess` [5, 6]	Número de validaciones de firmas de autenticación de dispositivos realizadas correctamente.	`DirectoryId`	Promedio, mínimo, máximo, suma, muestras de datos	Recuento
`TrustedDeviceValidationFailure` [5, 6]	Número de validaciones fallidas de firmas de autenticación de dispositivos.	`DirectoryId`	Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades
`TrustedDeviceCertificateDaysBeforeExpiration` [6]	Días que faltan para que caduque el certificado raíz asociado al directorio.	`CertificateId`	Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`CPUUsage`	El porcentaje del recurso de CPU utilizado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, máximo y mínimo	Porcentaje

`MemoryUsage`	El porcentaje de memoria de la máquina utilizado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, máximo y mínimo	Porcentaje

Métrica	Descripción	Dimensiones	Statistics	Unidades
RootVolumeDiskUsage	El porcentaje del volumen del disco raíz utilizado.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, máximo y mínimo	Porcentaje
UserVolumeDiskUsage	El porcentaje del volumen de disco del usuario utilizado.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Promedio, máximo y mínimo	Porcentaje
UDPPacketLossRate [7]	El porcentaje de paquetes descartados entre el cliente y la puerta de enlace.	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Muestras de datos promedio, máximo y mínimo	Porcentaje

Métrica	Descripción	Dimensiones	Statistics	Unidades

`UpTime`	El tiempo transcurrido desde el último reinicio de un WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
			Promedio, máximo, mínimo, muestras de datos	Segundos

[1] envía WorkSpaces periódicamente solicitudes de estado a WorkSpace. A WorkSpace se marca `Available` cuando responde a estas solicitudes y `Unhealthy` cuando no responde a estas solicitudes. Estas métricas están disponibles en cada WorkSpace nivel de granularidad y también se agregan para todos los miembros WorkSpaces de una organización.

[2] WorkSpaces registra las métricas de las conexiones realizadas con cada una de ellas WorkSpace. Estas métricas se emiten después de que un usuario se haya autenticado correctamente a través del WorkSpaces cliente y, a continuación, el cliente inicie una sesión. Las métricas están disponibles en cada WorkSpace nivel de granularidad y también se agregan para todas las WorkSpaces de un directorio.

[3] envía WorkSpaces periódicamente solicitudes de estado de conexión a un WorkSpace. Los usuarios se registran como conectados cuando utilizan activamente sus sesiones. Esta métrica está disponible en cada WorkSpace nivel de granularidad y también se agrega para todos los miembros WorkSpaces de una organización.

[4] Esta métrica se aplica a los WorkSpaces que están configurados con un modo de AutoStop ejecución. Si tiene el mantenimiento activado WorkSpaces, esta métrica captura el número de los WorkSpaces que se encuentran actualmente en mantenimiento. Esta métrica está disponible en cada WorkSpace nivel de granularidad, que describe cuándo un objeto WorkSpace pasó a mantenimiento y cuándo se retiró.

[5] Si la función de dispositivos de confianza está habilitada para el directorio, Amazon WorkSpaces utiliza la autenticación basada en certificados para determinar si un dispositivo es de confianza.

Cuando los usuarios intentan acceder a sus dispositivos de confianza WorkSpaces, se emiten estas métricas para indicar que la autenticación del dispositivo de confianza se ha realizado correctamente o ha fallado. Estas métricas están disponibles a nivel de granularidad por directorio y solo para las aplicaciones cliente de Amazon WorkSpaces Windows y macOS.

[6] No está disponible en WorkSpaces Web Access.

[7] Esta métrica mide la pérdida media de paquetes.

- En PCoIP: mide la pérdida media de paquetes en la puerta de enlace del cliente.
- En el WSP: mide la pérdida media de paquetes desde el cliente hacia la puerta de enlace.

Dimensiones de las métricas WorkSpaces

Para filtrar los datos de las métricas, use las siguientes dimensiones.

Dimensión	Descripción
`DirectoryId`	Filtra los datos de las métricas para WorkSpaces incluirlos en el directorio especific ado. El formato del ID de directorio es `d-XXXXXXXXXX` .
`WorkspaceId`	Filtra los datos métricos según lo especificado WorkSpace. La forma del WorkSpace identific ador es `ws-XXXXXXXXXX` .
`CertificateId`	Filtra los datos de la métrica al certificado raíz especificado asociado al directorio. La forma del ID del certificado es `wsc-XXXXXXXXX` .
`RunningMode`	Filtra los datos métricos WorkSpaces según su modo de ejecución. La forma del modo de ejecución es AutoStop o AlwaysOn.
`BundleId`	Filtra los datos métricos WorkSpaces según el protocolo. La forma del paquete es `wsb-XXXXXXXXXX` .

Dimensión	Descripción
`ComputeType`	Filtra los datos métricos WorkSpaces por tipo de cálculo.
`Protocol`	Filtra los datos métricos WorkSpaces por tipo de protocolo.
`UserName`	Filtra los datos de las métricas WorkSpaces por el nombre del usuario.

Ejemplo de monitorización

En el siguiente ejemplo, se muestra cómo se puede utilizar AWS CLI para responder a una CloudWatch alarma y determinar cuáles de los WorkSpaces componentes de un directorio han sufrido errores de conexión.

Para responder a una CloudWatch alarma

1. Determine a qué directorio se aplica la alarma usando el comando describe-alarms.

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. Obtenga la lista del WorkSpaces directorio especificado mediante el comando describe-workspaces.

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. Obtenga las CloudWatch métricas de cada uno de los componentes del directorio mediante WorkSpace el comando get-metric-statistics.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
```

```
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Supervisa tu WorkSpaces uso de Amazon EventBridge

Puedes usar los eventos de Amazon WorkSpaces para ver, buscar, descargar, archivar, analizar y responder a los inicios de sesión correctos en tu WorkSpaces. Por ejemplo, puede utilizar eventos para lo siguiente:

- Guarde o archive los eventos de inicio de WorkSpaces sesión como registros para consultarlos en el futuro, analice los registros para buscar patrones y tome medidas en función de esos patrones.
- Utilice la dirección IP de la WAN para determinar desde dónde han iniciado sesión los usuarios y, a continuación, utilice políticas que permitan a los usuarios acceder únicamente a los archivos o datos desde los WorkSpaces que se cumplan los criterios de acceso establecidos en el tipo de evento de`WorkSpaces Access`.
- Analice los datos de inicio de sesión y realice acciones automatizadas mediante AWS Lambda.
- Utilizar los controles de las políticas para bloquear el acceso a los archivos y aplicaciones desde direcciones IP no autorizadas.
- Descubra la versión del WorkSpaces cliente a la que se ha conectado WorkSpaces.

Amazon WorkSpaces emite estos eventos haciendo todo lo posible. Los eventos se envían casi EventBridge en tiempo real. Con EventBridge él, puede crear reglas que activen acciones programáticas en respuesta a un evento. Por ejemplo, puede configurar una regla que invoque un tema de SNS para enviar una notificación por correo electrónico o que active una función de Lambda para realizar alguna acción. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

WorkSpaces Acceda a los eventos

WorkSpaces las aplicaciones cliente envían `WorkSpaces Access` eventos cuando un usuario inicia sesión correctamente en un WorkSpace. Todos los WorkSpaces clientes envían estos eventos.

Los eventos emitidos por el WorkSpaces uso del Protocolo de WorkSpaces Transmisión (WSP) requieren la versión 4.0.1 o posterior de la aplicación WorkSpaces cliente.

Los eventos se representan como objetos JSON. El siguiente es un ejemplo de los datos de un evento `WorkSpaces Access`.

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

Campos específicos del evento

`clientIpAddress`

La dirección IP de WAN de la aplicación cliente. Para los clientes cero PCoIP, esta es la dirección IP del cliente de autenticación de Teradici.

`actionType`

Este valor siempre es `successfulLogin`.

`workspacesClientProductName`

Los siguientes valores distinguen entre mayúsculas y minúsculas.

- `WorkSpaces Desktop client`: clientes de Windows, macOS y Linux
- `Amazon WorkSpaces Mobile client`: cliente de iOS

- `WorkSpaces Mobile Client`: clientes de Android
- `WorkSpaces Chrome Client`: cliente de Chromebook
- `WorkSpacesWebClient`: cliente de acceso web
- `AmazonWorkSpacesThinClient`— Dispositivo Amazon WorkSpaces Thin Client
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` : cliente cero

`loginTime`

Hora en la que el usuario inició sesión en WorkSpace.

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

El identificador del directorio de WorkSpace. Debe anteponer al identificador del directorio el dominio `domain/`. Por ejemplo, `"domain/d-123456789"`.

`clientVersion`

La versión del cliente utilizada para conectarse a WorkSpaces.

`workspaceId`

Es el identificador de la WorkSpace.

Cree una regla para gestionar WorkSpaces los eventos

Utilice el siguiente procedimiento para crear una regla que gestione los WorkSpaces eventos.

Requisito previo

Para recibir notificaciones por correo electrónico, cree un tema de Amazon Simple Notification Service.

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Temas.
3. Elija Crear nuevo tema.
4. En Tipo, seleccione Estándar.
5. En Nombre, ingrese un nombre para el tema.
6. Seleccione Crear nuevo tema.
7. Elija Crear una suscripción.
8. En Protocolo, elija Correo electrónico.
9. En Punto de conexión, ingrese una dirección de correo electrónico para recibir las notificaciones.
10. Seleccione Crear suscripción.
11. Recibirá un mensaje de correo electrónico con la siguiente línea de asunto: AWS Notification - Subscription Confirmation. Siga las instrucciones para confirmar la suscripción.

Para crear una regla para gestionar WorkSpaces los eventos

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Seleccione Crear regla.
3. En Nombre, ingrese un nombre para la regla.
4. En Tipo de regla, elija Regla con un patrón de evento.
5. Elija Siguiente.
6. En Event pattern (Patrón de eventos), realice una de las siguientes acciones:
    a. En Origen del evento, elija Servicios de AWS.
    b. En Servicio de AWS, elija WorkSpaces.
    c. En Tipo de evento, selecciona WorkSpacesAcceso.
    d. De forma predeterminada, se envían notificaciones para cada evento. Si lo prefiere, puede crear un patrón de eventos que filtre los eventos para clientes o workspaces específicos.
7. Elija Siguiente.

8. Especifique un destino de la siguiente manera:
    a. Para Target types (Tipos de destino), elija Servicio de AWS.
    b. Para Seleccione un destino, elija Tema de SNS.
    c. En Tema, elija el tema SNS que creó para las notificaciones.
9. Elija Siguiente.
10. (Opcional) Añada etiquetas a la regla.
11. Elija Siguiente.
12. Seleccione Crear regla.

Información sobre los eventos de inicio de sesión de AWS para usuarios de tarjetas inteligentes

AWS CloudTrail registra los eventos de inicio de sesión correctos y fallidos de los usuarios de tarjetas inteligentes. Esto incluye eventos de inicio de sesión que se capturan cada vez que se pide a un usuario que resuelva un desafío o factor de credenciales específico, así como el estado de esa solicitud de verificación de credenciales en particular. Un usuario inicia sesión tras completar todos los desafíos de credenciales necesarios, lo que registra un evento de `UserAuthentication`.

En la siguiente tabla se muestran los nombres de cada evento de inicio de sesión de CloudTrail y sus propósitos.

Nombre de evento	Propósito del evento
`CredentialChallenge`	Se utiliza para notificar que el inicio de sesión de AWS ha solicitado que el usuario resuelva un desafío de credenciales específico y especifica el `CredentialType` que se requiere (por ejemplo, SMARTCARD).
`CredentialVerification`	Se utiliza para notificar que el usuario ha intentado resolver una solicitud de `CredentialChallenge` específica y precisa si la credencial se ha realizado correctamente o no.
`UserAuthentication`	Se utiliza para notificar que todos los requisitos de autenticación con los que se desafió al usuario se han completado con éxito y que el usuario ha iniciado sesión correctamente. Si los usuarios no completan

Nombre de evento	Propósito del evento
	correctamente los desafíos de credenciales requeridos, no se registrará ningún evento de `UserAuthentication` .

La siguiente tabla captura campos de datos de eventos útiles y adicionales que se encuentran en eventos específicos de CloudTrail de inicio de sesión.

Nombre de evento	Propósito del evento	Aplicabilidad al evento de inicio de sesión	Valores de ejemplo
`AuthWorkflowID`	Se utiliza para correlacionar todos los eventos emitidos en una secuencia de inicio de sesión completa. Para cada inicio de sesión de usuario, se pueden emitir varios eventos al iniciar sesión en AWS.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Se utiliza para notificar que el usuario ha intentado resolver una solicitud de `CredentialChallenge` específica y precisa si la credencial se ha realizado correctamente o no.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType": "SMARTCARD" (los valores posibles son: SMARTCARD)
`LoginTo`	Se utiliza para notificar que todos los requisitos de autenticación con los que se desafió al usuario se han completado con éxito y que el usuario ha iniciado sesión correctam	`UserAuthentication`	"LoginTo": "https://skylight.local“

Nombre de evento	Propósito del evento	Aplicabilidad al evento de inicio de sesión	Valores de ejemplo
	ente. Si los usuarios no completan correctam ente los desafíos de credenciales requeridos, no se registrará ningún evento de `UserAuthe ntication` .		

Ejemplos de eventos para escenarios de inicio de sesión de AWS

En los siguientes ejemplos se muestra la secuencia esperada de eventos de CloudTrail para diferentes escenarios de inicio de sesión.

Contenido

El inicio de sesión se realizó correctamente al autenticarse con una tarjeta inteligente

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión exitoso con tarjeta inteligente.

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
```

```
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```


Successful CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```

Successful UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
```

```
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

Inicio de sesión fallido al autenticarse solo con una tarjeta inteligente

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión fallido con tarjeta inteligente.

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
```

```
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Failed CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
```

```
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Continuidad empresarial para Amazon WorkSpaces

Amazon WorkSpaces se basa en la infraestructura AWS global, que se organiza en AWS regiones y zonas de disponibilidad. Estas regiones y zonas de disponibilidad ofrecen resiliencia en términos de aislamiento físico y redundancia de datos. Para obtener más información, consulte Resiliencia en Amazon WorkSpaces.

Amazon WorkSpaces también ofrece la redirección entre regiones, una función que funciona con las políticas de enrutamiento del Sistema de Nombres de Dominio (DNS) para redirigir a WorkSpaces los usuarios a una alternativa WorkSpaces cuando la principal WorkSpaces no está disponible. Por ejemplo, al utilizar políticas de enrutamiento de conmutación por error de DNS, puede conectar a sus usuarios a WorkSpaces la región de conmutación por error especificada cuando no puedan acceder a la WorkSpaces región principal.

Puede utilizar el redireccionamiento entre regiones para lograr la resiliencia regional y una alta disponibilidad. También puede usarlo para otros fines, como distribuir el tráfico o proporcionar alternativas WorkSpaces durante los períodos de mantenimiento. Si utiliza Amazon Route 53 para la configuración de DNS, puede aprovechar las comprobaciones de estado que supervisan CloudWatch las alarmas de Amazon.

Amazon WorkSpaces Multi-Region Resilience proporciona una infraestructura de escritorios virtuales redundante y automatizada en una WorkSpace región secundaria y agiliza el proceso de redireccionamiento de los usuarios a la región secundaria cuando no se puede acceder a la región principal debido a interrupciones.

Puede utilizar WorkSpaces la resiliencia multirregional con la redirección entre regiones para implementar una infraestructura de escritorio virtual redundante en una WorkSpace región secundaria y diseñar una estrategia de conmutación por error entre regiones como preparación para posibles eventos disruptivos. También puede utilizar esta solución para otros fines, como distribuir el tráfico o proporcionar alternativas durante los períodos de mantenimiento. WorkSpaces Si usa Route 53 para la configuración de DNS, puede aprovechar las comprobaciones de estado que monitorean CloudWatch las alarmas.

Contenido

Redirección entre regiones para Amazon WorkSpaces

Con la función de redireccionamiento entre regiones de Amazon WorkSpaces, puedes usar un nombre de dominio completo (FQDN) como código de registro para tu. WorkSpaces La redirección entre regiones funciona con las políticas de enrutamiento del sistema de nombres de dominio (DNS) para redirigir a WorkSpaces los usuarios a una alternativa WorkSpaces cuando la principal no está disponible. WorkSpaces Por ejemplo, mediante políticas de enrutamiento de conmutación por error de DNS, puede conectar a sus usuarios a WorkSpaces la AWS región de conmutación por error especificada cuando no puedan acceder a la WorkSpaces región principal.

Puede utilizar el redireccionamiento entre regiones junto con sus políticas de enrutamiento de conmutación por error de DNS para lograr la resiliencia regional y una alta disponibilidad. También puede utilizar esta función para otros fines, como distribuir el tráfico o proporcionar alternativas WorkSpaces durante los períodos de mantenimiento. Si utiliza Amazon Route 53 para la configuración de DNS, puede aprovechar las comprobaciones de estado que supervisan CloudWatch las alarmas de Amazon.

Para utilizar esta función, debe configurarla WorkSpaces para sus usuarios en dos (o más) AWS regiones. También debe crear códigos de registro especiales basados en FQDN denominados alias de conexión. Estos alias de conexión sustituyen a los códigos de registro específicos de la región para sus usuarios. WorkSpaces (Los códigos de registro específicos de la región siguen siendo válidos; sin embargo, para que el redireccionamiento entre regiones funcione, los usuarios deben utilizar el FQDN como código de registro).

Para crear un alias de conexión, se especifica una cadena de conexión, que es su FQDN, como `www.example.com` o `desktop.example.com`. Para utilizar este dominio para el redireccionamiento entre regiones, debe registrarlo en un registrador de dominios y configurar el servicio DNS de su dominio.

Una vez creados los alias de conexión, debe asociarlos a los WorkSpaces directorios de distintas regiones para crear pares de asociaciones. Cada par de asociación tiene una región principal y una o más regiones de conmutación por error. Si se produce una interrupción en la región principal, las políticas de enrutamiento de conmutación por error del DNS redirigen a WorkSpaces los usuarios a la WorkSpaces que haya configurado para ellos en la región de conmutación por error.

Para designar las regiones principales y de conmutación por error, debe definir la prioridad de la región (principal o secundaria) al configurar las políticas de enrutamiento de conmutación por error de DNS.

Contenido

Requisitos previos

- Debe ser propietario del dominio que desee utilizar como FQDN en sus alias de conexión y registrarlo. Si aún no utiliza otro registrador de dominios, puede utilizar Amazon Route 53 para registrar su dominio. Para obtener más información, consulte Registrar nombres de dominio mediante Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

> **Important**
>
> Debes tener todos los derechos necesarios para usar cualquier nombre de dominio que utilices junto con Amazon WorkSpaces. Usted acepta que el nombre de dominio no infringe ni infringe los derechos legales de ningún tercero ni infringe de ningún otro modo la legislación aplicable.

El nombre de dominio no puede superar los 255 caracteres. Para obtener más información sobre los nombres de dominio, consulte Formato de nombres de dominio DNS en la Guía para desarrolladores de Amazon Route 53.

El redireccionamiento entre regiones funciona tanto con nombres de dominio públicos como con nombres de dominio en zonas DNS privadas. Si utilizas una zona de DNS privada, debes proporcionar una conexión de red privada virtual (VPN) a la nube privada virtual (VPC) que la contiene. WorkSpaces Si WorkSpaces los usuarios intentan utilizar un FQDN privado de la Internet pública, las aplicaciones WorkSpaces cliente muestran el siguiente mensaje de error:

```
"We're unable to register the WorkSpace because of a DNS server issue.
Contact your administrator for help."
```

- Debe configurar su servicio de DNS y configurar las políticas de enrutamiento de DNS necesarias. La redirección entre regiones funciona junto con las políticas de enrutamiento de DNS para redirigir a WorkSpaces los usuarios según sea necesario.
- En cada región principal y de conmutación por error en la que desee configurar la redirección entre regiones, cree para sus usuarios. WorkSpaces Asegúrese de utilizar los mismos nombres de usuario en cada directorio de cada WorkSpaces región. Para mantener sincronizados los datos de usuario de Active Directory, te recomendamos usar AD Connector para que apunte al mismo Active Directory en cada región en la que hayas configurado WorkSpaces para tus usuarios. Para obtener más información sobre la creación WorkSpaces, consulta Launch WorkSpaces.

> **Important**
>
> Si configura su directorio AWS gestionado de Microsoft AD para la replicación multirregional, solo podrá registrar el directorio de la región principal para su uso en Amazon WorkSpaces. Los intentos de registrar el directorio en una región replicada para su uso con Amazon WorkSpaces fallarán. La replicación multirregional con Microsoft AD AWS administrado no se admite para su uso con Amazon WorkSpaces dentro de las regiones replicadas.

Cuando haya terminado de configurar la redirección entre regiones, debe asegurarse de que sus WorkSpaces usuarios utilizan el código de registro basado en el FQDN en lugar del código de registro basado en la región (por ejemplo) para su región principal. `WSpdx+ABC12D` Para ello, debe

enviarles un correo electrónico con la cadena de conexión del FQDN mediante el procedimiento descrito en Paso 5: envíe la cadena de conexión a sus usuarios WorkSpaces .

> **Note**
>
> Si crea los usuarios en la WorkSpaces consola en lugar de crearlos en Active Directory, envía WorkSpaces automáticamente un correo electrónico de invitación a los usuarios con un código de registro basado en la región cada vez que lance uno nuevo. WorkSpace Esto significa que, al configurar los usuarios en la región de conmutación WorkSpaces por error, estos también recibirán automáticamente correos electrónicos relacionados con estas conmutaciones por error. WorkSpaces Deberá indicar a sus usuarios que ignoren los correos electrónicos con códigos de registro basados en la región.

Limitaciones

- La redirección entre regiones no comprueba automáticamente si las conexiones a la región principal han fallado y, a continuación, se produce la conmutación por error a WorkSpaces otra región. En otras palabras, la conmutación por error automática no se produce.

  Para implementar un escenario de conmutación por error automática, debe utilizar algún otro mecanismo junto con el redireccionamiento entre regiones. Por ejemplo, puede usar una política de enrutamiento de DNS de conmutación por error de Amazon Route 53 junto con una comprobación de estado de Route 53 que monitorea una CloudWatch alarma en la región principal. Si se activa la CloudWatch alarma en la región principal, su política de enrutamiento de conmutación por error de DNS redirige a WorkSpaces los usuarios a la WorkSpaces que ha configurado para ellos en la región de conmutación por error.
- Cuando utilizas la redirección entre regiones, los datos de los usuarios no se conservan entre distintas regiones. WorkSpaces Para garantizar que los usuarios puedan acceder a sus archivos desde distintas regiones, te recomendamos que configures Amazon WorkDocs para tus WorkSpaces usuarios, si Amazon WorkDocs es compatible con tus regiones principal y de conmutación por error. Para obtener más información sobre Amazon WorkDocs, consulta Amazon WorkDocs Drive en la Guía de WorkDocs administración de Amazon. Para obtener más información sobre cómo habilitar Amazon WorkDocs para tus WorkSpace usuarios, consulta Registrar un directorio en WorkSpaces yHabilitar Amazon WorkDocs para Microsoft AD administrado por AWS. Para obtener información sobre cómo WorkSpaces los usuarios pueden

configurar Amazon WorkDocs en sus WorkSpaces, consulte Integrar con WorkDocs en la Guía del WorkSpaces usuario de Amazon.

- La redirección entre regiones solo se admite en la versión 3.0.9 o posterior de las aplicaciones cliente de Linux, macOS y Windows WorkSpaces . También puede utilizar el redireccionamiento entre regiones con Acceso web.
- La redirección entre regiones está disponible en todas AWSlas regiones en las que Amazon WorkSpaces está disponible, excepto en la región AWS GovCloud (US) Region s y en la región de China (Ningxia).

Paso 1: crear alias de conexión

Con la misma cuenta de AWS, cree el alias de conexión en cada región principal y de conmutación por error en la que desee configurar el redireccionamiento entre regiones.

Para crear un alias de conexión

1. Abre la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región principal para tu. WorkSpaces
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Redireccionamiento entre regiones, elija Crear alias de conexión.
5. En Cadena de conexión, introduzca un FQDN, como `www.example.com` o `desktop.example.com`. Cada cadena puede tener un máximo de 255 caracteres. Solo puede incluir letras (A-Z y a-z), números (0-9) y los siguientes caracteres: .-

   > **Important**
   >
   > Después de crear una cadena de conexión, siempre estará asociada a su cuenta de AWS. No puede volver a crear una cadena de conexión con otra cuenta aunque haya eliminado todas las instancias de la cadena de conexión de la cuenta original. La cadena de conexión está reservada globalmente para tu cuenta.

6. (Opcional) En Etiquetas, especifique las etiquetas que desee asociar a su alias de conexión.
7. Elija Crear alias de conexión.
8. Repita estos pasos, pero enStep 2, asegúrese de seleccionar la región de conmutación por error correspondiente a su región. WorkSpaces Si tiene más de una región de conmutación por error,

repita estos pasos con cada región de conmutación por error. Asegúrese de utilizar la misma cuenta de AWS para crear el alias de conexión en cada región de conmutación por error.

(Opcional) Paso 2: compartir un alias de conexión con otra cuenta

Puede compartir un alias de conexión con otra cuenta de AWS en la misma región de AWS. Al compartir un alias de conexión con otra cuenta se concede permiso a esa cuenta para asociar o desasociar dicho alias con un directorio propiedad de esa cuenta solo en la misma región. Solo la cuenta que posee un alias de conexión puede eliminarlo.

> **Note**
>
> Un alias de conexión se puede asociar con un solo directorio por región de AWS. Si comparte un alias de conexión con otra cuenta de AWS, solo una cuenta (su cuenta o la cuenta compartida) puede asociar el alias con un directorio de esa región.

Para compartir un alias de conexión con otra cuenta de AWS

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola de, elija la región de AWS en la que desea compartir el alias de conexión con otra cuenta de AWS.
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Asociaciones de redireccionamiento entre regiones, seleccione la cadena de conexión y, a continuación, Acciones, Compartir/dejar de compartir el alias de conexión.

   También puedes compartir un alias desde la página de detalles de su alias de conexión. Para ello, en Cuenta compartida, seleccione Compartir alias de conexión.
5. En la página Compartir o dejar de compartir el alias de conexión, en Compartir con una cuenta, introduzca el ID de la cuenta de AWS con la que quiere compartir su alias de conexión en esta región de AWS.
6. Elija Compartir.

Paso 3: asociar los alias de conexión a los directorios de cada región

Al asociar el mismo alias de conexión a un WorkSpaces directorio de dos o más regiones, se crea un par de asociaciones entre los directorios. Cada par de asociación tiene una región principal y una o más regiones de conmutación por error.

Por ejemplo, si su región principal es la región EE.UU. Oeste (Oregón), puede emparejar el WorkSpaces directorio de la región EE.UU. Oeste (Oregón) con un WorkSpaces directorio de la región EE.UU. Este (Norte de Virginia). Si se produce una interrupción en la región principal, la redirección entre regiones funciona junto con sus políticas de enrutamiento de conmutación por error de DNS y cualquier comprobación de estado que haya realizado en la región EE.UU. Oeste (Oregón) para redirigir a sus usuarios a la región WorkSpaces que ha configurado para ellos en la región EE.UU. Este (Norte de Virginia). Para obtener más información sobre el redireccionamiento entre regiones, consulte Qué ocurre durante el redireccionamiento entre regiones.

> **Note**
>
> Si sus WorkSpaces usuarios se encuentran a una distancia considerable de la región de conmutación por error (por ejemplo, a miles de kilómetros de distancia), es posible que su WorkSpaces experiencia responda menos de lo habitual. Para comprobar el tiempo de ida y vuelta (RTT) a las distintas AWS regiones desde tu ubicación, utiliza el Amazon WorkSpaces Connection Health Check.

Para asociar un alias de conexión a un directorio

Puede asociar un alias de conexión con un solo directorio por región de AWS. Si ha compartido un alias de conexión con otra cuenta de AWS, solo una cuenta (su cuenta o la cuenta compartida) puede asociar el alias con un directorio de esa región.

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región principal para tu. WorkSpaces
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Asociaciones de redireccionamiento entre regiones, seleccione la cadena de conexión y, a continuación, elija Acciones, Asociar/desasociar.

También puede asociar un alias de conexión a un directorio desde la página de detalles del alias de conexión. Para ello, en Directorio asociado, seleccione Asociar directorio.

5. En la página Asociar/desasociar, en Asociar a un directorio, seleccione el directorio al que desee asociar su alias de conexión en esta región de AWS.

> **Note**
>
> Si configura su directorio AWS gestionado de Microsoft AD para la replicación multirregional, solo podrá usar el directorio de la región principal con Amazon WorkSpaces. Los intentos de utilizar el directorio en una región replicada con Amazon WorkSpaces fallarán. La replicación multirregional con Microsoft AD AWS administrado no se admite para su uso con Amazon WorkSpaces dentro de las regiones replicadas.

6. Seleccione Asociar.
7. Repita estos pasos, pero asegúrese de Step 2 seleccionar la región de conmutación por error para su región. WorkSpaces Si tiene más de una región de conmutación por error, repita estos pasos con cada región de conmutación por error. Asegúrese de asociar el mismo alias de conexión a un directorio en cada región de conmutación por error.

Paso 4: configurar el servicio de DNS y las políticas de enrutamiento de DNS

Una vez que haya creado los alias de conexión y los pares de asociación de alias de conexión, podrá configurar el servicio DNS para el dominio que utilizó en las cadenas de conexión. Para ello, puede utilizar cualquier proveedor de servicios DNS. Si aún no tiene un proveedor de servicios de DNS preferido, puede utilizar Amazon Route 53. Para obtener más información, consulte Configuración de Amazon Route 53 como servicio DNS en la Guía para desarrolladores de Amazon Route 53.

Una vez que haya configurado el servicio de DNS para su dominio, debe configurar las políticas de enrutamiento de DNS que desee utilizar para el redireccionamiento entre regiones. Por ejemplo, puede utilizar las comprobaciones de estado de Amazon Route 53 para determinar si sus usuarios pueden conectarse a la WorkSpaces suya en una región determinada. Si sus usuarios no pueden conectarse, puede utilizar una política de conmutación por error de DNS para enrutar el tráfico de DNS de una región a otra.

Para obtener información sobre cómo dirigir las políticas, consulte Elección de una política de enrutado en la Guía para desarrolladores de Amazon Route 53. Para obtener más información sobre las comprobaciones de estado de Amazon Route 53, consulte Cómo verifica Amazon Route 53 el estado de los recursos en la Guía para desarrolladores de Amazon Route 53.

Al configurar las políticas de enrutamiento de DNS, necesitará el identificador de conexión para la asociación entre el alias de conexión y el WorkSpaces directorio de la región principal. También necesitará el identificador de conexión para la asociación entre el alias de conexión y el WorkSpaces directorio de la región o regiones de conmutación por error.

> **Note**
>
> El identificador de conexión no es el mismo que el identificador del alias de conexión. El identificador del alias de la conexión comienza por `wsca-`.

Para encontrar el identificador de conexión de una asociación de alias de conexión

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región principal para tu. WorkSpaces
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Asociaciones de redireccionamiento entre regiones, seleccione el texto de la cadena de conexión (el FQDN) para ver la página de detalles del alias de la conexión.
5. En la página de detalles del alias de conexión, en Directorio asociado, anote el valor que se muestra como identificador de conexión.
6. Repita estos pasos, pero enStep 2, asegúrese de seleccionar la región de conmutación por error correspondiente a su región. WorkSpaces Si tiene más de una región de conmutación por error, repita estos pasos para encontrar el identificador de conexión con cada región de conmutación por error.

Ejemplo: Para configurar una política de enrutamiento de conmutación por error de DNS mediante Route 53

En el siguiente ejemplo se configura una zona alojada pública para el dominio. Sin embargo, puede configurar una zona alojada pública o una zona alojada privada. Para obtener más información sobre

cómo configurar una zona alojada, consulte Uso de zonas alojadas en la Guía para desarrolladores de Amazon Route 53.

En este ejemplo también se utiliza una política de enrutamiento de conmutación por error. Puede usar otros tipos de políticas de enrutamiento para su estrategia de redireccionamiento entre regiones. Para obtener información sobre cómo dirigir las políticas, consulte Elección de una política de enrutado en la Guía para desarrolladores de Amazon Route 53.

Al configurar una política de enrutamiento de conmutación por error en Route 53, es necesario comprobar el estado de la región principal. Para obtener más información sobre la creación de una comprobación de estado en Route 53, consulte Creación de comprobaciones de estado de Amazon Route 53 y configuración de la conmutación por error a nivel de DNS y Creación, actualización y eliminación de comprobaciones de estado en la Guía para desarrolladores de Amazon Route 53.

Si quieres usar una CloudWatch alarma de Amazon con tu chequeo de estado de Route 53, también tendrás que configurar una CloudWatch alarma para monitorear los recursos de tu región principal. Para obtener más información CloudWatch, consulta ¿Qué es Amazon CloudWatch? en la Guía del CloudWatch usuario de Amazon. Para obtener más información sobre cómo Route 53 utiliza CloudWatch las alarmas en sus comprobaciones de estado, consulte Cómo determina Route 53 el estado de las comprobaciones de estado que supervisan CloudWatch las alarmas y Monitorización de una CloudWatch alarma en la Guía para desarrolladores de Amazon Route 53.

Para configurar una política de enrutamiento de conmutación por error de DNS en Route 53, primero debe crear una zona alojada para su dominio.

1. Abra la consola de Route 53 en https://console.aws.amazon.com/route53/.
2. En el panel de navegación, elija Zonas alojadas y, luego, Crear zona alojada.
3. En la página Zona alojada creada, introduzca su nombre de dominio (por ejemplo `example.com`) en Nombre de dominio.
4. En Tipo, seleccione Zona alojada pública.
5. Elija Crear zona alojada.

A continuación, cree una comprobación de estado para su región principal.

1. Abra la consola de Route 53 en https://console.aws.amazon.com/route53/.
2. En el panel de navegación, seleccione Comprobaciones de estado y, a continuación, Crear comprobación de estado.

3. En la página Configurar la comprobación de estado, introduzca un nombre para la comprobación.
4. En Qué controlar, seleccione Punto final, Estado de otros controles de estado (comprobación de estado calculada) o Estado de CloudWatch alarma.
5. En función de lo que haya seleccionado en el paso anterior, configure la comprobación de estado y, a continuación, seleccione Siguiente.
6. En la página Recibir una notificación cuando se produzca un error en la comprobación de estado, en Crear alarma, seleccione Sí o No.
7. Elija Crear comprobación de estado.

Una vez creada la comprobación de estado, podrá crear los registros de conmutación por error del DNS.

1. Abra la consola de Route 53 en https://console.aws.amazon.com/route53/.
2. En el panel de navegación, elija Zonas alojadas.
3. En la página Zonas alojadas, seleccione su nombre de dominio.
4. En la página de detalles del nombre de dominio, seleccione Crear registro.
5. En la página Elegir política de enrutamiento, seleccione Conmutación por error y, a continuación Siguiente.
6. En la página Configurar registros, en Configuración básica, introduzca el nombre del subdominio en el campo Nombre del registro. Por ejemplo, si su FQDN es `desktop.example.com`, introduzca **`desktop`**.

   > **Note**
   >
   > Si desea utilizar el dominio raíz, deje en blanco el campo Nombre del registro. Sin embargo, te recomendamos usar un subdominio, como `desktop` o `workspaces`, a menos que hayas configurado el dominio únicamente para usarlo con tu WorkSpaces.

7. En Tipo de registro, seleccione TXT: se usa para verificar los remitentes de correo electrónico y para valores específicos de la aplicación.
8. Deje los valores predeterminados del campo Segundos de TTL.
9. En Registros de conmutación por error para añadirlos a ***`su_nombre_de_dominio`***, seleccione Definir registro de conmutación por error.

Ahora necesita configurar los registros de conmutación por error para sus regiones principal y de conmutación por error.

Ejemplo: Para configurar el registro de conmutación por error de su región principal

1. En el cuadro de diálogo Definir registro de conmutación por error, en Valor/enrutar el tráfico a, seleccione la dirección IP u otro valor en función del tipo de registro.
2. Se abre un cuadro en el que puede introducir las entradas de texto de muestra. Introduzca el identificador de conexión de la asociación de alias de conexión de su región principal.
3. En Tipo de registro de conmutación por error, seleccione Principal.
4. En Comprobación de estado, seleccione una comprobación de estado que haya creado para su región principal.
5. En el campo ID de registro, introduzca una descripción para identificar este registro.
6. Elija Definir registro de conmutación por error. El nuevo registro de conmutación por error aparece en Registros de conmutación por error para añadirlo a ***su_nombre_de_dominio***.

Ejemplo: Para configurar el registro de conmutación por error de su región de conmutación por error

1. En Registros de conmutación por error para añadirlos a ***su_nombre_de_dominio***, seleccione Definir registro de conmutación por error.
2. En el cuadro de diálogo Definir registro de conmutación por error, en Valor/enrutar el tráfico a, seleccione la dirección IP u otro valor en función del tipo de registro.
3. Se abre un cuadro en el que puede introducir las entradas de texto de muestra. Introduzca el identificador de conexión de la asociación de alias de conexión de su región de conmutación por error.
4. En Tipo de registro de conmutación por error, seleccione Secundario.
5. (Opcional) En Comprobación de estado, introduzca una comprobación de estado que haya creado para su región de conmutación por error.
6. En el campo ID de registro, introduzca una descripción para identificar este registro.
7. Elija Definir registro de conmutación por error. El nuevo registro de conmutación por error aparece en Registros de conmutación por error para añadirlo a ***su_nombre_de_dominio***.

Si la comprobación de estado que has configurado para tu región principal no es correcta, tu política de enrutamiento de conmutación por error de DNS redirige a WorkSpaces los usuarios a tu región

de conmutación por error. Route 53 sigue supervisando la comprobación de estado de su región principal y, cuando la comprobación de estado de su región principal deja de fallar, Route 53 redirige automáticamente a WorkSpaces los usuarios a la región principal. WorkSpaces

Para obtener información acerca de cómo crear registros de DNS, consulte Creación de registros mediante la consola de Amazon Route 53 en la Guía del desarrollador de Amazon Route 53. Para obtener más información sobre cómo configurar registros TXT de DNS, consulte TXT record type en la Guía para desarrolladores de Amazon Route 53.

Paso 5: envíe la cadena de conexión a sus usuarios WorkSpaces

Para asegurarse de que sus usuarios WorkSpaces serán redirigidos según sea necesario durante una interrupción, debe enviar la cadena de conexión (FQDN) a sus usuarios. Si ya ha emitido códigos de registro basados en la región (por ejemplo`WSpdx+ABC12D`) a sus WorkSpaces usuarios, dichos códigos seguirán siendo válidos. Sin embargo, para que la redirección entre regiones funcione, WorkSpaces los usuarios deben utilizar la cadena de conexión como código de registro al registrarlos WorkSpaces en la aplicación cliente. WorkSpaces

> **Important**
>
> Si crea los usuarios en la WorkSpaces consola en lugar de crearlos en Active Directory, envía WorkSpaces automáticamente un correo electrónico de invitación a los usuarios con un código de registro basado en la región (por ejemplo`WSpdx+ABC12D`) cada vez que lance uno nuevo. WorkSpace Aunque ya haya configurado el redireccionamiento entre regiones, el correo electrónico de invitación que se envía automáticamente cuando se trata de un nuevo correo WorkSpaces contiene este código de registro basado en la región en lugar de la cadena de conexión.
>
> Para asegurarse de que sus WorkSpaces usuarios utilizan la cadena de conexión en lugar del código de registro basado en la región, debe enviarles otro correo electrónico con la cadena de conexión mediante el procedimiento que se indica a continuación.

Para enviar la cadena de conexión a sus usuarios WorkSpaces

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región principal para tu. WorkSpaces
3. En el panel de navegación, elige. WorkSpaces

4. En la WorkSpacespágina, utilice el cuadro de búsqueda para buscar un usuario al que desee enviar una invitación y, a continuación, seleccione el usuario correspondiente en los resultados WorkSpace de la búsqueda. Solo puede seleccionar uno WorkSpace a la vez.
5. Seleccione Actions (Acciones), Invite User (Invitar usuario).
6. En la WorkSpaces página Invitar a los usuarios a sus páginas, verás una plantilla de correo electrónico para enviarla a tus usuarios.
7. (Opcional) Si hay más de un alias de conexión asociado a su WorkSpaces directorio, seleccione la cadena de conexión que desee que usen sus usuarios en la lista de cadenas de alias de conexión. La plantilla de correo electrónico se actualiza para mostrar la cadena que ha seleccionado.
8. Copie el texto de la plantilla de correo electrónico y péguelo en un mensaje para los usuarios utilizando su propia aplicación de correo electrónico. En su aplicación de correo electrónico, puede modificar el texto según necesite. Cuando el correo electrónico de invitación esté listo, envíelo a los usuarios.

Diagrama de arquitectura de redireccionamiento entre regiones

El siguiente diagrama describe el proceso de implementación de la redirección entre regiones.

> **Note**
>
> La redirección entre regiones solo facilita la conmutación por error y la recuperación entre regiones. No facilita la creación y el mantenimiento WorkSpaces en la región secundaria y no permite la replicación de datos entre regiones. WorkSpaces tanto en la región principal como en la secundaria, deben gestionarse por separado.

Inicie la redirección entre regiones

En caso de que se produzca una interrupción, puede actualizar los registros de DNS manualmente o utilizar políticas de enrutamiento automatizadas basadas en las comprobaciones de estado, que determinan la región de conmutación por error. Recomendamos seguir los mecanismos de recuperación ante desastres descritos en Creación de mecanismos de recuperación ante desastres con Amazon Route 53.

Qué ocurre durante el redireccionamiento entre regiones

Durante la conmutación por error regional, WorkSpaces los usuarios se desconectan de los WorkSpaces de la región principal. Cuando intentan volver a conectarse, aparece el siguiente mensaje de error:

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

A continuación, se pedirá a los usuarios que inicien sesión de nuevo. Si utilizan el FQDN como código de registro, cuando vuelvan a iniciar sesión, sus políticas de enrutamiento de conmutación por error de DNS los redirigirán a la WorkSpaces que usted haya configurado para ellos en la región de conmutación por error.

> **Note**
>
> En algunos casos, es posible que los usuarios no puedan volver a conectarse cuando se registren de nuevo. Si se produce este comportamiento, deben cerrar y reiniciar la aplicación WorkSpaces cliente y, a continuación, intentar volver a iniciar sesión.

Desasociar un alias de conexión de un directorio

Solo la cuenta propietaria de un directorio puede disociar un alias de conexión del directorio.

Si ha compartido un alias de conexión con otra cuenta y esa cuenta ha asociado el alias de conexión a un directorio propiedad de esa cuenta, debe utilizarse esa cuenta para disociar el alias de conexión del directorio.

Para disociar un alias de conexión de un directorio

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola de, elija la región de AWS que contiene el alias de conexión que desea desasociar.
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Asociaciones de redireccionamiento entre regiones, seleccione la cadena de conexión y, a continuación, elija Acciones, Asociar/desasociar.

También puede disociar un alias de conexión de la página de detalles del alias de conexión. Para ello, en Directorio asociado, seleccione Desasociar.

5. En la página Asociar/desasociar, seleccione Desasociar.
6. En el cuadro de diálogo que le pide que confirme la disociación, seleccione Desasociar.

Dejar de compartir un alias de conexión

Solo el propietario de un alias de conexión puede dejar de compartir el alias. Si deja de compartir un alias de conexión con una cuenta, esa cuenta ya no podrá asociar el alias de conexión a un directorio.

Para dejar de compartir un alias de conexión

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, elija la región de AWS que contiene el alias de conexión que desea dejar de compartir.
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Asociaciones de redireccionamiento entre regiones, seleccione la cadena de conexión y, a continuación, Acciones, Compartir/dejar de compartir el alias de conexión.

   También puede dejar de compartir un alias de conexión desde la página de detalles del alias de conexión. Para ello, en Cuenta compartida, selecciona Dejar de compartir.
5. En la página Compartir/dejar de compartir alias de conexión, seleccione Dejar de compartir.
6. En el cuadro de diálogo que te pide que confirmes que no se comparte el alias de conexión, seleccione Dejar de compartir.

Eliminar un alias de conexión

Puedes eliminar un alias de conexión solo si es propiedad de tu cuenta y si no está asociado a un directorio.

Si ha compartido un alias de conexión con otra cuenta y esa cuenta ha asociado el alias de conexión a un directorio propiedad de esa cuenta, debe utilizarse esa cuenta para disociar el alias de conexión del directorio y poder eliminar el alias de conexión.

> **Important**
>
> Después de crear una cadena de conexión, siempre estará asociada a su cuenta de AWS. No puede volver a crear una cadena de conexión con otra cuenta aunque haya eliminado todas las instancias de la cadena de conexión de la cuenta original. La cadena de conexión está reservada globalmente para tu cuenta.

> **Warning**
>
> Si ya no va a utilizar un FQDN como código de registro para sus WorkSpaces usuarios, debe tomar ciertas precauciones para evitar posibles problemas de seguridad. Para obtener más información, consulte Consideraciones de seguridad si deja de utilizar la redireccionamiento entre regiones.

Para eliminar un alias de conexión

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, elija la región de AWS que contiene el alias de conexión que desea eliminar.
3. En el panel de navegación, elija Account Settings (Configuración de cuenta).
4. En Asociaciones de redireccionamiento entre regiones, seleccione la cadena de conexión y, a continuación, elija Eliminar.

   También puede eliminar un alias de conexión de la página de detalles del alias de conexión. En la parte superior derecha de la página, elija Eliminar.

   > **Note**
   >
   > Si el botón Eliminar está desactivado, asegúrese de ser el propietario del alias y de que el alias no esté asociado a un directorio.

5. En el cuadro de diálogo que le pide que confirme la eliminación, seleccione Eliminar.

Permisos de IAM para asociar y desasociar los alias de conexión

Si utiliza un usuario de IAM para asociar o desasociar los alias de conexión, el usuario debe tener permisos para `workspaces:AssociateConnectionAlias` y `workspaces:DisassociateConnectionAlias`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Important

Si va a crear una política de IAM para asociar o desasociar los alias de conexión para las cuentas que no son propietarios de los alias de conexión, no puede especificar un ID de cuenta en el ARN. En su lugar, debe utilizar * para el ID de cuenta, como se muestra en la siguiente directiva de ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
```

```
    }
  ]
}
```

Puede especificar un ID de cuenta en el ARN solo cuando esa cuenta sea propietaria del alias de conexión que se va a asociar o disociar.

Para obtener más información acerca de cómo trabajar con IAM, consulte Gestión de identidades y accesos para WorkSpaces.

Consideraciones de seguridad si deja de utilizar la redireccionamiento entre regiones

Si ya no va a utilizar un FQDN como código de registro para sus WorkSpaces usuarios, debe tomar las siguientes precauciones para evitar posibles problemas de seguridad:

- Asegúrese de emitir a sus WorkSpaces usuarios el código de registro específico de la región (por ejemplo`WSpdx+ABC12D`) para su WorkSpaces directorio e indicarles que dejen de usar el FQDN como código de registro.
- Si aún es propietario de este dominio, asegúrese de actualizar su registro TXT de DNS para eliminarlo de forma que no pueda utilizarse en un ataque de suplantación de identidad. Si eliminas este dominio de tu registro TXT de DNS y tus WorkSpaces usuarios intentan usar el FQDN como código de registro, sus intentos de conexión fallarán sin problemas.
- Si ya no eres propietario de este dominio, tus WorkSpaces usuarios deberán usar el código de registro específico de su región. Si siguen intentando utilizar el FQDN como código de registro, sus intentos de conexión podrían redirigirse a un sitio malintencionado.

Resiliencia multirregional para Amazon WorkSpaces

Amazon WorkSpaces Multi-Region Resilience (MRR) le permite redirigir a los usuarios a una región secundaria cuando no se puede acceder a WorkSpaces la región principal debido a eventos perturbadores, sin necesidad de que los usuarios cambien los códigos de registro al iniciar sesión en su estado de espera. WorkSpaces El modo de espera WorkSpaces es una función de Amazon WorkSpaces Multi-Region Resilience que agiliza la creación y la administración del despliegue en espera. Tras configurar un directorio de usuarios en la región secundaria, seleccione el directorio de usuarios de WorkSpace la región principal para el que desee crear un directorio en espera

WorkSpace . El sistema refleja automáticamente las imágenes del WorkSpace paquete principal en la región secundaria. A continuación, aprovisiona automáticamente una nueva reserva WorkSpace en tu región secundaria

La resiliencia WorkSpaces multirregional de Amazon se basa en la redirección entre regiones que aprovecha las capacidades de conmutación por error y comprobación del estado del DNS. Le permite utilizar un nombre de dominio completo (FQDN) como código de registro. WorkSpaces Cuando los usuarios inicien sesión WorkSpaces, podrá redirigirlos a WorkSpaces las regiones compatibles en función de las políticas de su sistema de nombres de dominio (DNS) para el FQDN. Si utiliza Amazon Route 53, le recomendamos que utilice comprobaciones de estado que supervisen CloudWatch las alarmas de Amazon al diseñar una estrategia de redireccionamiento entre regiones para. WorkSpaces Para obtener más información, consulte Creación de comprobaciones de estado de Amazon Route 53 y configuración de la conmutación por error de DNS en la Guía para desarrolladores de Amazon Route 53.

La replicación de datos es una función adicional del modo de espera WorkSpaces que replica los datos en un solo sentido desde la región principal a la región secundaria. Una vez habilitada la replicación de los datos, se toman instantáneas de EBS del sistema y de los volúmenes de usuarios cada 12 horas. Multi-Region Resilience comprueba periódicamente si hay instantáneas nuevas. Cuando se encuentran las instantáneas, se inicia una copia en la región secundaria. A medida que las copias llegan a la región secundaria, se utilizan para actualizar la región secundaria. WorkSpace

Contenido

Requisitos previos

- Debe crearlas WorkSpaces para los usuarios de la región principal antes de crear la versión en espera WorkSpaces. Para obtener más información sobre la creación WorkSpaces, consulteLanzar un escritorio virtual utilizando WorkSpaces.
- Para habilitar la replicación de datos en espera WorkSpaces, debe tener un Active Directory autoadministrado o un Microsoft AD AWS administrado configurado para replicar en las regiones en espera. Para obtener más información, consulte Crear el directorio AWS administrado de Microsoft AD y Agregar una región replicada.
- Asegúrese de actualizar los controladores de dependencia de la red, como los controladores ENA, NVMe y PV, en su servidor principal. WorkSpaces Debe hacerlo al menos una vez cada 6 meses. Para obtener más información, consulte Instalar o actualizar el controlador Elastic Network Adapter (ENA)Controladores NVMe de AWS para instancias de Windows y Actualizar los controladores PV en instancias de Windows.
- Asegúrese de actualizar periódicamente los agentes de EC2Config, EC2Launch y EC2Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada 6 meses. Para obtener más información, consulte Actualizar EC2Config y EC2Launch.
- Para garantizar una replicación de datos adecuada, asegúrese de que los Active Directories de las regiones principal y secundaria estén sincronizados con el FQDN, la OU y el SID del usuario.
- La cuota (límite) predeterminada para el modo de espera WorkSpaces es 0. Debe solicitar un aumento de la cuota de servicio antes de crear un servicio en espera WorkSpace. Para obtener más información, consulte WorkSpaces Cuotas de Amazon.
- Asegúrese de utilizar claves administradas por el cliente para cifrar tanto la clave principal como la en espera WorkSpaces. Puedes usar claves de una sola región o claves de varias regiones para cifrar la clave principal y la de reserva. WorkSpaces

Limitaciones

- El modo de espera WorkSpaces solo copia la imagen agrupada de la unidad principal, WorkSpaces pero no copia el volumen del sistema (unidad C) ni el volumen de usuarios (unidad D) de la unidad principal. WorkSpaces Para copiar el volumen del sistema (unidad C) o el volumen de usuario (unidad D) del dispositivo principal WorkSpaces al de reserva WorkSpaces, debe habilitar la replicación de datos.
- No puede modificar, reconstruir, restaurar ni migrar directamente un dispositivo en espera WorkSpace.

- La conmutación por error para el redireccionamiento entre regiones se controla mediante la configuración de DNS. Para implementar un escenario de conmutación por error automática, debe utilizar un mecanismo diferente junto con el redireccionamiento entre regiones. Por ejemplo, puede usar una política de enrutamiento de DNS de conmutación por error de Amazon Route 53 junto con una comprobación de estado de Route 53 que monitorea una CloudWatch alarma en la región principal. Si se CloudWatch activa la alarma en la región principal, su política de enrutamiento de conmutación por error de DNS redirige a WorkSpaces los usuarios a la WorkSpaces que ha configurado para ellos en la región de conmutación por error.
- La replicación de datos solo funciona en un sentido: copia los datos de la región principal a la región secundaria. Durante la WorkSpaces conmutación por error en modo de espera, puede acceder a los datos y a la aplicación entre 12 y 24 horas. Tras una interrupción, haga una copia de seguridad manual de todos los datos que haya creado en la unidad secundaria WorkSpace y cierre la sesión. Te recomendamos guardar tu trabajo en unidades externas, como una unidad de red, para poder acceder a tus datos desde la unidad principal WorkSpace.
- La replicación de datos no admite AWS Simple AD.
- Cuando se habilita la replicación de datos en modo de espera WorkSpaces, se toman instantáneas de EBS del volumen principal WorkSpaces (tanto del volumen raíz como del sistema) cada 12 horas. La instantánea inicial de un volumen de datos concreto está completa y las instantáneas posteriores son incrementales. Como resultado, la primera replicación de un determinado archivo WorkSpace tardará más que las siguientes. Las instantáneas se inician según un cronograma interno WorkSpaces y no se puede controlar el tiempo.
- Si la unidad principal WorkSpace y la de reserva se WorkSpace unen mediante el mismo dominio, le recomendamos que solo se conecte al dominio principal WorkSpace o al de reserva en un WorkSpace momento dado para evitar perder la conexión con el controlador de dominio.
- Si configura la replicación multirregional, solo podrá registrar el directorio de la región principal para su uso. AWS Managed Microsoft AD WorkSpaces Si intenta registrar el directorio en una región replicada para usarlo en ella WorkSpaces, se producirá un error. AWS Managed Microsoft AD No se admite la replicación multirregional WorkSpaces dentro de las regiones replicadas.
- Si ya ha configurado la redirección entre regiones y la ha creado tanto WorkSpaces en la región principal como en la secundaria sin utilizar el modo de espera WorkSpaces, no podrá convertir directamente el redireccionamiento existente WorkSpace en la región secundaria en una región en espera. WorkSpace WorkSpace En su lugar, debes cerrar la de tu región secundaria, seleccionar la WorkSpace región principal para la que deseas crear una reserva y usar la opción de espera WorkSpace WorkSpaces para crear la región en espera. WorkSpace

- Tras una interrupción, haz una copia de seguridad manual de todos los datos que hayas creado en la secundaria WorkSpace y cierra sesión. Te recomendamos guardar tu trabajo en unidades externas, como una unidad de red, para poder acceder a tus datos desde la unidad principal WorkSpace.
- WorkSpaces La resiliencia multirregional está disponible actualmente en las siguientes regiones:
  - Región del este de EE. UU. (Norte de Virginia)
  - Región del oeste de EE. UU (Oregón)
  - Región de Europa (Fráncfort)
  - Región de Europa (Irlanda)
- WorkSpaces La resiliencia multirregional solo se admite en la versión 3.0.9 o posterior de las aplicaciones WorkSpaces cliente de Linux, macOS y Windows. También puede utilizar la resiliencia multirregional con Acceso web.
- WorkSpaces Multi-Region Resilience es compatible con Windows y Bring Your Own License (BYOL). WorkSpaces No es compatible con Amazon Linux, Ubuntu o con GPU WorkSpaces (p. ej. WorkSpaces, Graphics.g4dn o .g4dn). GraphicsPro GraphicsPro
- Una vez finalizada la conmutación por error o la recuperación, espere de 15 a 30 minutos antes de conectarse a su. WorkSpace

Configure su sistema de resiliencia multirregional en espera WorkSpace

Para configurar su modo de espera de resiliencia multirregional WorkSpace

1. Configure los directorios de usuarios en las regiones principal y secundaria. Asegúrese de utilizar los mismos nombres de usuario en cada WorkSpaces directorio de cada región.

   Para mantener sincronizados los datos de usuario de Active Directory, te recomendamos usar AD Connector para que apunte al mismo Active Directory en cada región en la que hayas configurado WorkSpaces para tus usuarios. Para obtener más información sobre la creación de un directorio, consulta Registrar un directorio en WorkSpaces.

   > **Important**
   >
   > Si configura el AWS Managed Microsoft AD directorio para la replicación en varias regiones, solo podrá registrar el directorio de la región principal para usarlo con WorkSpaces él. Los intentos de registrar el directorio en una región replicada para

su uso en ella WorkSpaces fallarán. AWS Managed Microsoft AD No se admite la replicación multirregional WorkSpaces dentro de las regiones replicadas.

2. Cree WorkSpaces para sus usuarios de la región principal. Para obtener más información sobre la creación WorkSpaces, consulte Launch WorkSpaces.
3. Cree una zona de espera WorkSpace en la región secundaria. Para obtener más información sobre la creación de una reserva WorkSpace, consulte Crear una reserva WorkSpace.
4. Cree y asocie cadenas de conexión (FQDN) a los directorios de usuarios de las regiones principales y secundarias.

   Debe habilitar el redireccionamiento entre regiones en su cuenta, ya que el modo de espera WorkSpaces se basa en el redireccionamiento entre regiones. Sigue los pasos 1 a 3 de las instrucciones para el redireccionamiento entre regiones para Amazon. WorkSpaces
5. Configure el servicio DNS y las políticas de enrutamiento de DNS.

   Debe configurar su servicio de DNS y configurar las políticas de enrutamiento de DNS necesarias. La redirección entre regiones funciona junto con las políticas de enrutamiento de DNS para redirigir a WorkSpaces los usuarios según sea necesario.
6. Cuando haya terminado de configurar el redireccionamiento entre regiones, debe enviar a sus usuarios un correo electrónico con una cadena de conexión de FQDN. Para obtener más información, consulte el paso 5: Enviar la cadena de conexión a los usuarios. WorkSpaces Asegúrese de que sus WorkSpaces usuarios utilizan el código de registro basado en el FQDN en lugar del código de registro basado en la región (por ejemplo, wspdx+ABC12d) para su región principal.

   Important

   - Si crea los usuarios en la WorkSpaces consola en lugar de crearlos en Active Directory, envía WorkSpaces automáticamente un correo electrónico de invitación a los usuarios con un código de registro basado en la región cada vez que lance uno nuevo. WorkSpace Esto significa que, al configurar los usuarios WorkSpaces de la región secundaria, los usuarios también recibirán automáticamente los correos electrónicos de estos usuarios secundarios. WorkSpaces Deberá indicar a sus usuarios que ignoren los correos electrónicos con códigos de registro basados en la región.

- Los códigos de registro específicos de la región siguen siendo válidos; sin embargo, para que la redirección entre regiones funcione, los usuarios deberán utilizar el FQDN como código de registro.

Cree un modo de espera WorkSpace

Antes de crear una en espera WorkSpace, asegúrese de haber cumplido los requisitos previos, como la creación de un directorio de usuarios en las regiones principal y secundaria, el aprovisionamiento WorkSpaces para los usuarios de la región principal, la configuración del redireccionamiento entre regiones en su cuenta y la solicitud de aumentar el WorkSpaces límite de espera a través de la cuota de servicio.

Para crear un modo de espera WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región principal para tu. WorkSpaces
3. En el panel de navegación, elige. WorkSpaces
4. Seleccione la opción para la que WorkSpace desee crear un modo de WorkSpace espera.
5. Selecciona Acciones y, a continuación, selecciona Crear modo de espera WorkSpace.
6. Selecciona la región secundaria en la que crearás tu modo de espera y WorkSpace, a continuación, selecciona Siguiente.
7. Seleccione el directorio de usuarios de la región secundaria y, a continuación, elija Siguiente.
8. (Opcional) Agregue la clave de cifrado, habilite el cifrado de datos y administre las etiquetas.

   - Para añadir una clave de cifrado, introdúzcala en Introducir clave de cifrado.
   - Para habilitar la replicación de datos, seleccione Habilitar la replicación de datos. Luego, marca la casilla de verificación para confirmar que autorizas un cargo mensual adicional.
   - Para añadir una etiqueta, elija Agregar nueva etiqueta.

   A continuación, elija Siguiente.

> **Note**
>
> - Si el original WorkSpace está cifrado, este campo se rellena automáticamente. Sin embargo, puede optar por usar su propia clave de cifrado.
> - Se tarda unos minutos en actualizar el estado de la replicación de los datos.
> - Una vez que la WorkSpace copia en espera se haya actualizado correctamente con las instantáneas de la cámara principal WorkSpace, podrá encontrar las marcas horarias de las instantáneas en Recovery Snapshot.

9. Revise la configuración de su modo de espera WorkSpaces y, a continuación, seleccione Crear.

> **Note**
>
> - Para ver información sobre tu modo de espera WorkSpaces, ve a la página de WorkSpace detalles principal.
> - El modo de espera WorkSpace solo copia la imagen de paquete de la unidad principal, WorkSpace pero no copia el volumen del sistema (unidad C) ni el volumen de usuario (unidad D) de la unidad principal WorkSpaces. De forma predeterminada, la replicación de datos está desactivada. Para copiar el volumen del sistema (unidad C) o el volumen de usuario (unidad D) del dispositivo principal WorkSpaces al de reserva WorkSpaces, debe habilitar la replicación de datos.

Administre un modo de espera WorkSpace

No puede modificar, reconstruir, restaurar ni migrar directamente un dispositivo en espera WorkSpace.

Para habilitar la replicación de datos para su dispositivo en espera WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. Ve a tu región principal y selecciona el WorkSpace ID principal.
3. Desplázate hacia abajo hasta la WorkSpace sección En espera y selecciona Editar en espera WorkSpace.

4. Selecciona Activar la replicación de datos. Luego, marca la casilla de verificación para confirmar que autorizas un cargo mensual adicional. A continuación, elija Guardar.

> **Note**
>
> - El modo de espera WorkSpaces no puede hibernar. Si detiene el modo de espera WorkSpace, no se conserva el trabajo no guardado. Recomendamos a los usuarios que guarden siempre su trabajo antes de salir del modo de espera. WorkSpaces
> - Para habilitar la replicación de datos en espera WorkSpaces, debe tener un Active Directory autoadministrado o un Microsoft AD AWS administrado configurado para replicar en las regiones en espera. Para configurar sus directorios, siga los pasos 1 a 3 de la sección Tutorial de Cómo crear continuidad empresarial con Amazon WorkSpaces y AWS Directory Services o consulte Uso de Active Directory AWS gestionado por varias regiones con Amazon. WorkSpaces La replicación multirregional solo se admite en la edición Enterprise de AWS Managed Microsoft AD.
> - Se tarda unos minutos en actualizar el estado de la replicación de los datos.
> - Una vez que la WorkSpace copia en espera se haya actualizado correctamente con las instantáneas de la cámara principal WorkSpace, podrá encontrar las marcas horarias de las instantáneas en Recovery Snapshot.

Elimine una copia en espera WorkSpace

Puede terminar un modo de espera WorkSpace de la misma manera que termina uno normal WorkSpace.

Para eliminar un modo de espera WorkSpace

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región principal para tu. WorkSpaces
3. En el panel de navegación, elige. WorkSpaces
4. Seleccione el modo de espera WorkSpace y elija Eliminar. Eliminar un modo de espera tarda aproximadamente 5 minutos WorkSpace. Durante la eliminación, el estado del dispositivo

en espera se WorkSpace establecerá en Terminado. Cuando se complete la eliminación, el dispositivo en espera WorkSpace desaparecerá de la consola.

> **Note**
>
> Eliminar un modo de espera WorkSpace es una acción permanente y no se puede deshacer. Los datos del WorkSpace usuario en espera no se conservan y se destruyen. Para obtener ayuda con la copia de seguridad de los datos de los usuarios, ponte en contacto con AWS Support.

Replicación unidireccional de datos para modo de espera WorkSpaces

Al habilitar la replicación de datos en Multi-Region Resilience, puede replicar datos de una región principal a una región secundaria. Durante el estado estable, Multi-Region Resilience captura instantáneas del sistema (unidad C) y de los datos (unidad D) de la unidad principal WorkSpaces cada 12 horas. Estas instantáneas se transfieren a la región secundaria y se utilizan para actualizar la región en espera. WorkSpaces De forma predeterminada, la replicación de datos está deshabilitada en espera WorkSpaces.

Una vez habilitada la replicación de datos para el estado en espera WorkSpaces, se completa la instantánea inicial de un volumen de datos concreto, mientras que las instantáneas posteriores son incrementales. Como consecuencia, la primera replicación de un determinado archivo WorkSpace tardará más que las siguientes. Las instantáneas se activan a intervalos predeterminados WorkSpaces y los usuarios no pueden controlar el tiempo.

Durante la conmutación por error, cuando los usuarios son redirigidos a la región secundaria, pueden acceder a la región en espera WorkSpaces con datos y aplicaciones que tengan entre 12 y 24 horas de antigüedad. Mientras los usuarios estén en modo de espera WorkSpaces, Multi-Region Resilience no los obligará a cerrar sesión en el modo de espera WorkSpaces ni a actualizar el modo de espera WorkSpaces con las instantáneas de la región principal.

Tras una interrupción, los usuarios deben hacer una copia de seguridad manual de todos los datos que hayan creado en su dispositivo secundario WorkSpaces antes de cerrar sesión en el modo de espera. WorkSpaces Cuando vuelvan a iniciar sesión, se les redirigirá a la región principal y a la principal WorkSpaces.

Planee reservar la capacidad de recuperación de Amazon EC2

Amazon Multi-Region Resilience (MRR) se basa en los pools bajo demanda de Amazon EC2 de forma predeterminada. Si un tipo de instancia Amazon EC2 específico no está disponible para respaldar la recuperación, MRR intentará automáticamente escalar la instancia varias veces hasta encontrar un tipo de instancia disponible, pero en circunstancias extremas, es posible que las instancias no estén siempre disponibles. Para mejorar la disponibilidad de los tipos de instancias necesarios para las instancias más críticas WorkSpaces, ponte en contacto con AWS Support y te ayudaremos a planificar la capacidad.

Seguridad en Amazon WorkSpaces

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para conocer los programas de conformidad que se aplican a WorkSpaces, consulte AWS Services in Scope by Compliance Program (Servicios de AWS en el ámbito del programa de conformidad) y (Servicios de en el ámbito del programa de conformidad).
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar WorkSpaces. Muestra cómo configurar WorkSpaces para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros servicios de AWS que le ayudarán a supervisar y proteger sus recursos de WorkSpaces.

Contenido

Protección de datos en Amazon WorkSpaces

El AWS modelo de se aplica a protección de datos en Amazon WorkSpaces. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja WorkSpaces o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Para obtener más información sobre el WorkSpaces cifrado de terminales FIPS, consulte. Configurar Amazon WorkSpaces para obtener la autorización FedRAMP o la conformidad DoD SRG.

Cifrado en reposo

Puede cifrar sus volúmenes de almacenamiento WorkSpaces mediante AWS KMS Key from. AWS Key Management Service Para obtener más información, consulte Cifrado WorkSpaces.

Cuando crea WorkSpaces con volúmenes cifrados, WorkSpaces utiliza Amazon Elastic Block Store (Amazon EBS) para crear y gestionar esos volúmenes. EBS cifra los volúmenes con una clave de datos que utiliza el algoritmo estándar AES-256. Para obtener más información, consulte Amazon EBS Encryption en la Guía del usuario de Amazon EC2.

Cifrado en tránsito

En el caso de los PCoIP, los datos en tránsito se cifran mediante encriptación TLS 1.2 y firma de solicitud SigV4. El protocolo PCoIP utiliza tráfico UDP cifrado, con cifrado AES, para la transmisión de píxeles. La conexión de transmisión, que utiliza el puerto 4172 (TCP y UDP), se cifra mediante cifrados AES-128 y AES-256, pero el cifrado por defecto es de 128 bits. Puede cambiar este valor predeterminado a 256 bits, ya sea mediante la configuración de política de grupo Configurar configuración de seguridad de PCoIP para Windows WorkSpaces o modificando la configuración de seguridad de PCoIP en el archivo de Amazon Linux. `pcoip-agent.conf` WorkSpaces

Para obtener más información sobre la administración de políticas de grupo para Amazon WorkSpaces, consulte Configurar opciones de seguridad de PCoIP enAdministre su Windows WorkSpaces. Para obtener más información sobre la modificación del archivo `pcoip-agent.conf` consulte, Controle el comportamiento del agente PCoIP en Amazon Linux WorkSpaces y Configuración de seguridad de PCoIP en la documentación de Teradici.

En el WorkSpaces caso del Protocolo de transmisión (WSP), la transmisión y el control de los datos en tránsito se cifran mediante el cifrado DTLS 1.2 para el tráfico UDP y el cifrado TLS 1.2 para el tráfico TCP, con cifrados AES-256.

Gestión de identidades y accesos para WorkSpaces

De forma predeterminada, los usuarios de IAM no tienen permisos para los recursos y operaciones de WorkSpaces. Para permitir a los usuarios de IAM administrar los recursos de WorkSpaces,

debe crear una política de IAM que les conceda explícitamente permisos, y asociar la política a los usuarios o grupos de IAM que requieran esos permisos.

Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Create a permission set (Creación de un conjunto de permisos) en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda asumir. Siga las instrucciones de Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para obtener más información sobre las políticas de IAM, consulte Políticas y permisos en la Guía del usuario de IAM.

WorkSpaces también crea un rol de IAM, `workspaces_DefaultRole`, que permite al servicio WorkSpaces acceder a los recursos necesarios.

Para obtener más información sobre IAM, consulte Administración de identidades y acceso (IAM) y la Guía del usuario de IAM. Encontrará los recursos, acciones y claves de contexto de condición específicos de WorkSpaces que se utilizan en las políticas de permisos de IAM en Acciones, recursos y claves de condición para Amazon WorkSpaces en la Guía del usuario de IAM.

Para obtener una herramienta que le ayude a crear políticas de IAM, consulte Generador de políticas deAWS. También puede utilizar el simulador de política de IAM para probar si una política permitiría o denegaría una solicitud específica a AWS.

> **Note**
>
> Amazon WorkSpaces no admite el aprovisionamiento de credenciales de IAM en un WorkSpace (por ejemplo, con un perfil de instancia).

Contenido

Ejemplos de políticas

Los siguientes ejemplos muestran instrucciones de política que puede utilizar para controlar los permisos que tienen los usuarios de IAM para Amazon WorkSpaces.

Example 1: Realizar todas las tareas de WorkSpaces

La siguiente instrucción de política concede a un usuario de IAM permiso para realizar todas las tareas de WorkSpaces, incluida la creación y gestión de directorios. También concede permiso para ejecutar el procedimiento de configuración rápida.

Aunque Amazon WorkSpaces es totalmente compatible con los elementos `Action` y `Resource` al utilizar la API y las herramientas de línea de comandos, para utilizar Amazon WorkSpaces desde la consola de administración de AWS Management Console, un usuario de IAM debe tener permisos para las siguientes acciones y recursos:

- Acciones: `workspaces:*"` y `"ds:*"`
- Recursos: `"Resource": "*"`

El siguiente ejemplo de política muestra cómo permitir que un usuario de IAM utilice Amazon WorkSpaces desde AWS Management Console.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 2: Realizar tareas específicas del espacio de trabajo

Las siguientes instrucción de políticas conceden a un usuario de IAM permiso para realizar tareas específicas de WorkSpace, como lanzar y eliminar WorkSpaces. En la instrucción de política, la acción `ds:*` concede permisos amplios: un control absoluto sobre todos los objetos de Directory Services de la cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Para conceder también al usuario la capacidad de habilitar Amazon WorkDocs para usuarios dentro de WorkSpaces, añada la operación `workdocs` que se muestra en el siguiente ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Para conceder también al usuario la capacidad de utilizar el Asistente de lanzamiento de WorkSpaces, añada las operaciones `kms` que se muestran en el siguiente ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3: Realice todas las tareas de WorkSpaces para BYOL WorkSpaces

La siguiente declaración de política concede a un usuario de IAM permiso para realizar todas las tareas de WorkSpaces, incluidas las tareas de Amazon EC2 necesarias para crear WorkSpaces de traiga su propia licencia (BYOL).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Especificar los recursos de WorkSpaces en una política de IAM

Para especificar un recurso de en el elemento `Resource` de la instrucción de la política, utilice el nombre de recurso de Amazon (ARN). Puede controlar el acceso a sus recursos WorkSpaces permitiendo o denegando permisos para utilizar las acciones API que se especifican en el elemento `Action` de su instrucción de política IAM. WorkSpaces define los ARN para WorkSpaces, paquetes, grupos de IP y directorios.

ARN de espacio de trabajo

Los ARN de WorkSpace tienen la sintaxis que se muestra en el ejemplo siguiente.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

La región en la que se encuentra el WorkSpace (por ejemplo, `us-east-1`).

id_cuenta

El ID de la cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

identificador_espacio_trabajo

El ID del WorkSpace (por ejemplo, `ws-a1bcd2efg`).

Este es el formato del elemento `Resource` de una instrucción de política que identifica un WorkSpace específico:

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

Puede utilizar el carácter comodín `*` para especificar todos los WorkSpaces que pertenecen a una cuenta específica en una región específica.

ARN de imagen

Un ARN de imagen WorkSpace tiene la sintaxis que se muestra en el siguiente ejemplo.

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

region

La región en la que se encuentra la imagen del WorkSpace (por ejemplo, `us-east-1`).

id_cuenta

El ID de la cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

identificador_paquete

El ID de la imagen WorkSpace (por ejemplo, `wsi-a1bcd2efg`).

Este es el formato del elemento `Resource` de una instrucción de política que identifica una imagen específica.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

Puede utilizar el carácter comodín * para especificar todas las imágenes que pertenecen a una cuenta específica en una región específica.

ARN de paquete

Los ARN de los paquetes tienen la sintaxis que se muestra en el siguiente ejemplo.

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

region

La región en la que se encuentra el WorkSpace (por ejemplo, `us-east-1`).

id_cuenta

El ID de la cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

identificador_paquete

El ID del paquete de WorkSpace (por ejemplo, `wsb-a1bcd2efg`).

Este es el formato del elemento `Resource` de una instrucción de política que identifica un paquete específico.

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

Puede utilizar el comodín * para especificar todos los paquetes que pertenecen a una cuenta específica en una región específica.

ARN de grupo de IP

Los ARN de los grupos de IP tienen la sintaxis que se muestra en el ejemplo siguiente.

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

region

La región en la que se encuentra el WorkSpace (por ejemplo, `us-east-1`).

id_cuenta

El ID de la cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

grupoip_identificador

ID del grupo de IP (por ejemplo, `wsipg-a1bcd2efg`).

Este es el formato del elemento `Resource` de una instrucción de política que identifica un grupo de IP específico.

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

Puede utilizar el carácter comodín * para especificar todos los grupos de IP que pertenecen a una cuenta específica en una región específica.

ARN de directorio

Los ARN de los directorios tienen la sintaxis que se muestra en el ejemplo siguiente.

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

region

La región en la que se encuentra el WorkSpace (por ejemplo, `us-east-1`).

id_cuenta

El ID de la cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

directorio_identificador

ID del directorio (por ejemplo, `d-12345a67b8`).

Este es el formato del elemento `Resource` de una instrucción de política que identifica un directorio específico.

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

Puede utilizar el carácter comodín para especificar todos los directorios que pertenecen a una cuenta específica en una región específica.

Alias de conexión ARN

Un alias de conexión ARN tiene la sintaxis que se muestra en el siguiente ejemplo.

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

region

La región en la que se encuentra el alias de conexión (por ejemplo,`us-east-1`).

id_cuenta

El ID de la cuenta de AWS, sin guiones (por ejemplo, `123456789012`).

connectionalias_identifier

El ID del alias de conexión (por ejemplo, `wsca-12345a67b8`).

Este es el formato del elemento `Resource` de una instrucción de política que identifica un alias de conexión específico.

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

Puede utilizar el carácter comodín * para especificar todos los alias de conexión que pertenecen a una cuenta específica en una región específica.

Acciones de API que no admiten los permisos a nivel de recursos

No puede especificar el ARN de un recurso con las siguientes acciones de API:

- `AssociateIpGroups`
- `CreateIpGroup`
- `CreateTags`
- `DeleteTags`
- `DeleteWorkspaceImage`
- `DescribeAccount`
- `DescribeAccountModifications`
- `DescribeIpGroups`
- `DescribeTags`
- `DescribeWorkspaceDirectories`
- `DescribeWorkspaceImages`
- `DescribeWorkspaces`
- `DescribeWorkspacesConnectionStatus`
- `DisassociateIpGroups`
- `ImportWorkspaceImage`
- `ListAvailableManagementCidrRanges`
- `ModifyAccount`

En el caso de las acciones de la API que no admiten los permisos a nivel de recursos, debe especificar la instrucción de recursos que se muestra en el ejemplo siguiente.

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

Acciones de la API que no admiten restricciones en el nivel de cuenta sobre recursos compartidos

Para las siguientes acciones de API, no puede especificar un ID de cuenta en el ARN del recurso cuando el recurso no es propiedad de la cuenta:

- `AssociateConnectionAlias`
- `CopyWorkspaceImage`
- `DisassociateConnectionAlias`

Para estas acciones de la API, puedes especificar un ID de cuenta en el ARN del recurso solo cuando esa cuenta sea propietaria de los recursos sobre los que se va a actuar. Cuando la cuenta no es propietaria de los recursos, debe especificar * para el ID de cuenta, tal y como se muestra en el siguiente ejemplo.

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

Crear el rol workspaces_DefaultRole

Antes de poder registrar un directorio mediante la API, debe comprobar que existe un rol denominado `workspaces_DefaultRole`. Este rol se crea mediante la configuración rápida o si lanza un WorkSpace utilizando la AWS Management Console, y concede a Amazon WorkSpaces permiso para acceder a recursos específicos de AWS en su nombre. Si este rol no existe, puede crearlo mediante el siguiente procedimiento.

Para crear el rol workspaces_DefaultRole

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la izquierda, seleccione Roles.
3. Elija Create role (Crear rol).
4. En Seleccione el tipo de entidad de confianza, elija Otra cuenta de AWS.
5. En Account ID (ID de cuenta), escriba el ID de la cuenta sin guiones ni espacios.
6. En Options (Opciones), no especifique multi-factor authentication (MFA).
7. Elija Siguiente: Permisos.

8. En la página Asociar políticas de permisos, seleccione las políticas administradas por AWS AmazonWorkSpacesServiceAccess y AmazonWorkSpacesSelfServiceAccess.
9. En Establecer límite de permisos, se recomienda que no utilice un límite de permisos debido a la posibilidad de conflictos con las políticas asociadas a este rol. Estos conflictos podrían bloquear ciertos permisos necesarios para el rol.
10. Elija Next: Tags (Siguiente: etiquetas).
11. En la página Add tags (optional) [Agregar etiquetas (opcional)], añada las etiquetas que correspondan.
12. Elija Next: Review (Siguiente: revisar).
13. En la página Revisión, en Nombre del rol, ingrese **`workspaces_DefaultRole`**.
14. (Opcional) En Role description (Descripción del rol), escriba una descripción.
15. Elija Create Role (Crear rol).
16. En la página Summary (Resumen) del rol workspaces_DefaultRole, seleccione la pestaña Trust relationships (Relaciones de confianza).
17. En la pestaña Trust relationships (Relaciones de confianza), elija Edit trust relationship (Editar relación de confianza).
18. En la página Edit Trust Relationship (Editar relación de confianza), sustituya la instrucción de política existente por la siguiente instrucción.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. Elija Update Trust Policy (Actualizar política de confianza).

Crear el rol de servicio AmazonWorkSpacesPCAAccess

Antes de que los usuarios puedan iniciar sesión mediante la autenticación basada en certificados, debe comprobar que existe un rol denominado `AmazonWorkSpacesPCAAccess`. Este rol se crea cuando habilita la autenticación basada en certificados en un directorio mediante la AWS Management Console, y concede a Amazon WorkSpaces permiso para acceder a los recursos de AWS Private CA en su nombre. Si este rol no existe porque no utiliza la consola para administrar la autenticación basada en certificados, puede crearlo mediante el siguiente procedimiento.

Para crear el rol de servicio AmazonWorkSpacesPCAAccess utilizando la AWS CLI

1. Cree un archivo JSON llamado `AmazonWorkSpacesPCAAccess.json` con el siguiente texto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Ajuste la ruta de `AmazonWorkSpacesPCAAccess.json` según sea necesario y ejecute los siguientes comandos de la AWS CLI para crear el rol de servicio y asociar la política administrada AmazonWorkspacesPCAAccess.

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

Políticas administradas por AWS para WorkSpaces

El uso de las políticas administradas por AWS facilita añadir permisos a usuarios, grupos y roles en lugar de tener que escribir las políticas usted mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para comenzar rápidamente, utilice las políticas administradas por AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas por AWS, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas por AWS. No puede cambiar los permisos en las políticas administradas por AWS. En ocasiones, en los servicios se podrían añadir permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan permisos de una política administrada por AWS, por lo que las actualizaciones de la política no desharán sus permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada por `ReadOnlyAccess` AWS proporciona acceso de solo lectura a todos los servicios y recursos AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Política administrada por AWS: AmazonworkspacesAdmin

Esta política proporciona acceso a las acciones administrativas de Amazon WorkSpaces. Proporciona los siguientes permisos:

- `workspaces`: Permite el acceso para realizar acciones administrativas en los recursos de WorkSpaces.
- `kms`: Permite acceder a la lista y descripción de claves KMS, así como a la lista de alias.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

Política administrada porAWS: AmazonWorkspace/PCAAccess

Esta política administrada proporciona acceso a los recursos de autoridad de certificación privada (CA privada) de AWS Certificate Manager Private en su cuenta de AWS para la autenticación basada en certificados. Se incluye en el rol AmazonWorkspaceSPCAAccess y proporciona los siguientes permisos:

- `acm-pca`: Permite el acceso a la CA privada de AWS para administrar la autenticación basada en certificados.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

Política administrada por AWS: AmazonWorkSpacesSelfServiceAccess

Esta política proporciona acceso al servicio Amazon WorkSpaces para realizar acciones de autoservicio de WorkSpaces iniciadas por un usuario. Se incluye en el rol `workspaces_DefaultRole` y proporciona los siguientes permisos:

- `workspaces`: Permite a los usuarios acceder a las funciones de administración de WorkSpaces de autoservicio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Política administrada por AWS: AmazonWorkspacesServiceAccess

Esta política proporciona acceso a las cuentas de los clientes al servicio Amazon WorkSpaces para lanzar un WorkSpace. Se incluye en el rol `workspaces_DefaultRole` y proporciona los siguientes permisos:

- `ec2`: Permite el acceso para administrar los recursos de Amazon EC2 asociados a un WorkSpace, como las interfaces de red.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Actualizaciones de WorkSpaces a las políticas administradas por AWS

Consulte los detalles sobre las actualizaciones de las políticas administradas por AWS para WorkSpaces desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
the section called “AmazonWorkSpacesAdmin”: Política actualizada	WorkSpaces ha añadido la acción `workspaces:RestoreWorkspace` a la política administrada por Amazon WorkSpacesAdmin, concediendo a los administr	25 de junio de 2023

Cambio	Descripción	Fecha
	adores acceso para restaurar WorkSpaces.	
the section called “AmazonWorkspacesPCAAccess”: Añadió una nueva política.	WorkSpaces añadió una nueva política administrada para conceder permiso a `acm-pca` para administrar la CA privada de AWS con el fin de administrar la autenticación basada en certificados.	18 de noviembre de 2022
WorkSpaces comenzó a realizar un seguimiento de los cambios	WorkSpaces comenzó a realizar un seguimiento de los cambios de sus políticas administradas por WorkSpaces.	1 de marzo de 2021

Validación de conformidad para Amazon WorkSpaces

Los auditores externos evalúan la seguridad y conformidad de Amazon WorkSpaces como parte de varios programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de los servicios de AWS en el ámbito de programas de conformidad específicos, consulte AWS Services in Scope by Compliance Program (Servicios en el ámbito de programas de conformidad). Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Para obtener más información sobre WorkSpaces y FedRAMP, consulte Configurar Amazon WorkSpaces para obtener la autorización FedRAMP o la conformidad DoD SRG..

Su responsabilidad de conformidad al utilizar WorkSpaces se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. AWS proporciona los siguientes recursos para ayudarle con la conformidad:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones que cumplan los requisitos de HIPAA.
- AWSRecursos de conformidad de: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.

Resiliencia en Amazon WorkSpaces

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Amazon WorkSpaces también ofrece redireccionamiento entre regiones, una característica que funciona con las políticas de enrutamiento de conmutación por error de su sistema de nombres de dominio (DNS) para redirigir a los usuarios de WorkSpaces a WorkSpaces alternativos en otra región de AWS cuando sus WorkSpaces principales no están disponibles. Para obtener más información, consulte Redirección entre regiones para Amazon WorkSpaces.

Seguridad de la infraestructura en Amazon WorkSpaces

Como se trata de un servicio administrado, Amazon WorkSpaces está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Para acceder a los WorkSpaces a través de la red se utilizan las llamadas a la API publicadas en AWS. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de red

Una Virtual Private Cloud (VPC) es una red virtual en su propia área, aislada lógicamente en la nube de AWS. Puede implementar sus escritorios de WorkSpaces en una subred privada de la VPC. Para obtener más información, consulte Configurar una VPC para WorkSpaces.

Para permitir únicamente el tráfico de intervalos de direcciones específicos (por ejemplo, de la red corporativa), actualice el grupo de seguridad de la VPC o utilice un grupo de control de acceso IP.

Puede restringir el acceso a escritorios de WorkSpaces a dispositivos de confianza con certificados válidos. Para obtener más información, consulte Restrinja el WorkSpaces acceso a dispositivos de confianza.

Aislamiento en hosts físicos

Los diferentes escritorios de WorkSpaces que se encuentran en el mismo host físico están aislados entre sí a través del hipervisor. Es como si estuvieran en hosts físicos distintos. Cuando se elimina

un escritorio de WorkSpaces, el hipervisor limpia la memoria asignada (la establece en cero) antes de asignarla a un nuevo escritorio de WorkSpaces.

Autorización de usuarios corporativos

Con WorkSpaces, los directorios se administran a través de AWS Directory Service. Puede crear un directorio administrado independiente para los usuarios. O bien, puede realizar la integración con el entorno de Active Directory existente para que los usuarios puedan usar sus credenciales actuales para obtener acceso fácilmente a los recursos corporativos. Para obtener más información, consulte Administrar directorios para WorkSpaces.

Para controlar aún más el acceso a sus escritorios de WorkSpaces, utilice la autenticación multifactor. Para obtener más información, consulte Cómo habilitar la autenticación multifactor para los servicios de AWS.

Realizar solicitudes a la API de Amazon WorkSpaces a través de un punto de conexión de interfaz de VPC.

Puede conectarse directamente a los puntos de conexión de la API de Amazon WorkSpaces a través de un punto de conexión de interfaz en su nube privada virtual (VPC) en lugar de conectarse a través de Internet. Cuando utiliza un punto de conexión de interfaz de VPC, la comunicación entre su VPC y el punto de conexión de la API de Amazon WorkSpaces se realiza de forma completa y segura dentro de la red de AWS.

> **Note**
>
> Esta función solo se puede utilizar para conectarse a los puntos de enlace de la API de WorkSpaces. Para conectarse a WorkSpaces mediante los clientes de WorkSpaces, se requiere conectividad a Internet, tal como se describe en Requisitos de dirección IP y puerto para WorkSpaces.

Los puntos de conexión de la API de Amazon WorkSpaces son compatibles con los puntos de conexión de la interfaz de Amazon Virtual Private Cloud (Amazon VPC) que funcionan con AWS PrivateLink. Cada punto de enlace de la VPC se representa mediante una o varias interfaces de red (que también se conocen como «interfaces de red elástica» o «ENI») con direcciones IP privadas de las subredes de la VPC.

El punto de conexión de la interfaz de la VPC conecta su VPC directamente con el punto de conexión de la API de Amazon WorkSpaces sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con el punto de conexión de la API de Amazon WorkSpaces.

Puede crear un punto de conexión de interfaz para conectarse a Amazon WorkSpaces con los comandos de la AWS Management Console o de la AWS Command Line Interface (AWS CLI). Para obtener instrucciones, consulte Creación de un punto de enlace de interfaz.

Una vez que haya creado un punto de conexión VPC, puede utilizar los siguientes comandos CLI de ejemplo que utilizan el parámetro `endpoint-url` para especificar puntos de conexión de interfaz al punto de conexión API de Amazon WorkSpaces:

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

Si habilita los nombres de host DNS privados para el punto de enlace de la VPC, no necesita especificar la URL del punto de enlace. El nombre de host DNS de la API de Amazon WorkSpaces que la CLI y el SDK de Amazon WorkSpaces utilizan de forma predeterminada (https://api.workspaces.*Region*.amazonaws.com) soluciona el punto de conexión de la VPC.

El punto de conexión de la API de Amazon WorkSpaces admite puntos de conexión de VPC en todas las regiones de AWS en las que estén disponibles Amazon VPC y Amazon WorkSpaces. Amazon WorkSpaces permite realizar llamadas a todas sus API públicas desde su VPC.

Para obtener más información sobre AWS PrivateLink, consulte la documentación de AWS PrivateLink. Para obtener información sobre el precio de los puntos de enlace de la VPC, consulte Precios de VPC. Para obtener más información sobre la VPC y los puntos de enlace, visite Amazon VPC.

Para ver una lista de los puntos de conexión de la API de Amazon WorkSpaces de cada región, consulte Puntos de conexión de la API de WorkSpaces.

> **Note**
>
> Los puntos de conexión de la API de Amazon WorkSpaces con AWS PrivateLink no son compatibles con los puntos de conexión de la API de Amazon WorkSpaces del Estándar Federal de Procesamiento de Información (FIPS).

Creación de una política de punto de conexión de VPC para Amazon WorkSpaces

Puede crear una política de puntos de conexión de VPC de Amazon para Amazon WorkSpaces para especificar lo siguiente:

- La entidad de seguridad que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Controlar el acceso a servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

> **Note**
>
> LaLas políticas de punto de conexión de VPC no son compatibles con los puntos de conexión de Amazon WorkSpaces del Estándar Federal de Procesamiento de Información (FIPS).s políticas de punto de enlace de la VPC no son compatibles con los puntos de enlace de de Federal Information Processing Standard (FIPS).

El siguiente ejemplo de política de punto de conexión de la VPC especifica que todos los usuarios que tienen acceso al punto de conexión de la interfaz de la VPC tienen permiso para invocar el punto de conexión alojado en Amazon WorkSpaces denominado `ws-f9abcdefg`.

```
{
     "Statement": [
```

```
        {
            "Action": "workspaces:*",
            "Effect": "Allow",
            "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
            "Principal": "*"
        }
    ]
}
```

En este ejemplo, se deniegan las siguientes acciones:

- Invocar puntos de conexión alojados en Amazon WorkSpaces que sean distintos de `ws-f9abcdefg`.
- Realizar acciones en un recurso que no sea el especificado (ID de WorkSpace: `ws-f9abcdefg`).

> **Note**
>
> En este ejemplo, los usuarios pueden realizar otras acciones de la API de Amazon WorkSpaces desde fuera de la VPC. Para restringir las llamadas a la API únicamente a las realizadas desde dentro de la VPC, consulte Gestión de identidades y accesos para WorkSpaces para obtener información sobre el uso de políticas basadas en identidades para controlar el acceso a los puntos de conexión de la API de Amazon WorkSpaces.

Conecte su red privada a su VPC

Para llamar a la API de Amazon WorkSpaces a través de su VPC, tiene que conectarse desde una instancia que esté dentro de la VPC o conectar su red privada a su VPC mediante AWS Virtual Private Network (AWS VPN) o AWS Direct Connect. Para más información, consulte Conexiones VPN en la Guía del usuario de Amazon Virtual Private Cloud (Amazon VPC). Para obtener información acerca de AWS Direct Connect, consulte Creación de una conexión en la Guía del usuario de AWS Direct Connect.

Gestión de actualizaciones en WorkSpaces

Le recomendamos que parchee, actualice y proteja periódicamente el sistema operativo y las aplicaciones de su dispositivo WorkSpaces. Puede configurarlos WorkSpaces para que se actualicen

WorkSpaces durante un período de mantenimiento regular o puede actualizarlos usted mismo. Para obtener más información, consulte Mantenimiento de escritorios de WorkSpaces.

En el caso de sus aplicaciones WorkSpaces, puede utilizar cualquier servicio de actualización automática proporcionado o seguir las recomendaciones del fabricante de la aplicación para instalar las actualizaciones.

Solucionar problemas WorkSpaces

La siguiente información puede ayudarle a solucionar problemas con su WorkSpaces.

Habilitar el registro avanzado

Para ayudar a solucionar los problemas que puedan experimentar tus usuarios, puedes habilitar el registro avanzado en cualquier WorkSpaces cliente de Amazon.

El registro avanzado genera archivos de registro que contienen información de diagnóstico y detalles de depuración, incluidos datos detallados de rendimiento. Para los clientes de versiones superiores a la versión 1.0 y 2.0, estos archivos de registro avanzados se cargan automáticamente en una base de datos en. AWS

> **Note**
>
> Para AWS revisar los archivos de registro avanzados y recibir asistencia técnica en caso de problemas con sus WorkSpaces clientes, póngase en contacto con. AWS Support Para obtener más información, consulte el Centro de AWS Support.

Para habilitar el registro avanzado para Acceso web

Para habilitar el registro avanzado para Acceso web

1. Abre tu cliente de Amazon WorkSpaces Web Access.
2. En la parte superior de la página de inicio de WorkSpaces sesión, selecciona Registro de diagnóstico.
3. En el cuadro de diálogo emergente, asegúrese de que la opción Registro de diagnóstico esté activada.
4. En Nivel de registro, seleccione Registro avanzado.

Para acceder a los archivos de registro en Google Chrome, Microsoft Edge y Firefox

1. Abra el menú contextual (haga clic con el botón derecho) en los navegadores o pulse Ctrl+Mayús+I (o, comando+opción+I en Mac) en el teclado para abrir el panel de herramientas para desarrolladores.

2. En el panel de herramientas para desarrolladores, seleccione la pestaña Consola para buscar los archivos de registro.

Para acceder a los archivos de registro en Safari

1. Seleccione Safari, Ajustes.
2. En la sección Avanzado, elija Windows VSS.
3. Seleccione Mostrar funciones para desarrolladores web en la barra de menú.
4. En la pestaña Desarrollo de la barra de menú, elija Desarrollo > Show Web Inspector.
5. En el panel de Safari Web Inspector, seleccione la pestaña Consola para buscar los archivos de registro.

Para habilitar el registro avanzado en los clientes con la versión 4.0 o posterior

Los registros de clientes de Windows se almacenan en la siguiente ubicación:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Para habilitar el registro avanzado en los clientes de Windows

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra la aplicación del símbolo del sistema.
3. Lanza el WorkSpaces cliente con la `-l3` bandera.

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> Si WorkSpaces está instalado para un usuario y no para todos, utilice los siguientes comandos:
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> ```

```
workspaces.exe -l3
```

Los registros de clientes de macOS se almacenan en la siguiente ubicación:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

Para habilitar el registro avanzado en los clientes de macOS

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra Terminal.
3. Ejecute el siguiente comando de la .

```
open -a workspaces --args -l3
```

Para habilitar el registro avanzado de clientes de Android

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra el menú del cliente Android.
3. Seleccione Support.
4. Seleccione Configuración de registros.
5. Seleccione Habilitar el registro avanzado.

Para recuperar los registros de los clientes Android después de habilitar el registro avanzado:

- Seleccione Extract log para guardar los registros comprimidos de forma local.

Los registros de clientes de Linux se almacenan en la siguiente ubicación:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Para habilitar el registro avanzado de clientes de Linux

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra Terminal.
3. Ejecute el siguiente comando de la .

```
/opt/workspacesclient/workspacesclient -l3
```

Para habilitar el registro avanzado en los clientes con la versión 3.0 o posterior

Los registros de clientes de Windows se almacenan en la siguiente ubicación:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Para habilitar el registro avanzado en los clientes de Windows

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra la aplicación del símbolo del sistema.
3. Lanza el WorkSpaces cliente con la `-l3` bandera.

   ```
   c:
   cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
   workspaces.exe -l3
   ```

   > **Note**
   >
   > Si WorkSpaces está instalado para un usuario y no para todos, utilice los siguientes comandos:
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

Los registros de clientes de macOS se almacenan en la siguiente ubicación:

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

Para habilitar el registro avanzado en los clientes de macOS

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra Terminal.

3. Ejecute el siguiente comando de la .

```
open -a workspaces --args -l3
```

Para habilitar el registro avanzado de clientes de Android

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra el menú del cliente Android.
3. Seleccione Support.
4. Seleccione Configuración de registros.
5. Seleccione Habilitar el registro avanzado.

Para recuperar los registros de los clientes Android después de habilitar el registro avanzado:

- Seleccione Extract log para guardar los registros comprimidos de forma local.

Los registros de clientes de Linux se almacenan en la siguiente ubicación:

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Para habilitar el registro avanzado de clientes de Linux

1. Cierra el WorkSpaces cliente de Amazon.
2. Abra Terminal.
3. Ejecute el siguiente comando de la .

```
/opt/workspacesclient/workspacesclient -l3
```

Para habilitar el registro avanzado de clientes 1.0+ y 2.0+

1. Abre el WorkSpaces cliente.
2. Seleccione el icono con forma de engranaje que se encuentra en la esquina superior derecha de la aplicación cliente.
3. Seleccione Advanced Settings (Configuración avanzada).
4. Seleccione la casilla de verificación Enable Advanced Logging (Habilitar el registro avanzado).

5. Seleccione Guardar.

Los registros de clientes de Windows se almacenan en la siguiente ubicación:

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

Los registros de clientes de macOS se almacenan en la siguiente ubicación:

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

Solución de problemas específicos

La siguiente información puede ayudarle a solucionar problemas específicos con su WorkSpaces.

Problemas

- No puedo crear Amazon Linux WorkSpace porque hay caracteres no válidos en el nombre de usuario
- He cambiado el shell de mi Amazon Linux WorkSpace y ahora no puedo aprovisionar una sesión de PCoIP
- Mi Amazon Linux WorkSpaces no arranca
- El inicio WorkSpaces en mi directorio conectado a menudo falla
- El inicio WorkSpaces falla debido a un error interno
- Cuando intento registrar un directorio, el registro falla y deja el directorio en estado de ERROR
- Mis usuarios no pueden conectarse a Windows WorkSpace con un banner de inicio de sesión interactivo
- Mis usuarios no se pueden conectar a un Windows WorkSpace
- Mis usuarios tienen problemas cuando intentan iniciar sesión WorkSpaces desde WorkSpaces Web Access
- El WorkSpaces cliente de Amazon muestra una pantalla gris que dice «Cargando...» durante un tiempo antes de volver a la pantalla de inicio de sesión. No aparece ningún otro mensaje de error.
- Mis usuarios reciben el mensaje "WorkSpace Estado: insalubre». No hemos podido conectarlo con su WorkSpace. Vuelva a intentarlo en unos minutos".
- Mis usuarios reciben el mensaje «Este dispositivo no está autorizado a acceder al WorkSpace. Póngase en contacto con su administrador para obtener ayuda".

- Los usuarios reciben el mensaje «No hay red. Se ha perdido la conexión de red. Compruebe la conexión de red o póngase en contacto con el administrador para obtener ayuda”. al intentar conectarse a un WSP WorkSpace
- El WorkSpaces cliente produce un error de red a mis usuarios, pero pueden usar otras aplicaciones habilitadas para la red en sus dispositivos
- Mis WorkSpace usuarios ven el siguiente mensaje de error: «El dispositivo no se puede conectar al servicio de registro. Compruebe la configuración de red".
- Mis usuarios de cliente cero PCoIP están recibiendo el error “El certificado suministrado no es válido debido a la marca temporal”
- Las impresoras USB y otros periféricos USB no funcionan para los clientes cero PCoIP
- Mis usuarios omitieron actualizar sus aplicaciones cliente de Windows o macOS y no se les solicita que instalen la versión más reciente
- Mis usuarios no pueden instalar la aplicación cliente de Android en sus Chromebooks
- Mis usuarios no reciben correos electrónicos de invitación ni de restablecimiento de contraseña
- Mis usuarios no ven la opción "¿Olvidó la contraseña?" en la pantalla de inicio de sesión del cliente
- Cuando intento instalar aplicaciones en un sistema Windows, recibo el mensaje «El administrador del sistema ha establecido políticas para impedir esta instalación» WorkSpace
- No, WorkSpaces en mi directorio puedo conectarme a Internet
- My WorkSpace ha perdido su acceso a Internet
- Aparece el error “DNS no disponible” cuando intento conectarme a mi directorio on-premise
- Aparece el error “Problemas de conectividad detectados” cuando intento conectarme a mi directorio en las instalaciones
- Aparece el error “Registro SRV” cuando intento conectarme a mi directorio en las instalaciones
- Mi Windows WorkSpace entra en modo de suspensión cuando está inactivo
- Uno de los míos WorkSpaces tiene un estado de UNHEALTHY
- My WorkSpace se bloquea o se reinicia inesperadamente
- El mismo nombre de usuario tiene más de uno WorkSpace, pero el usuario solo puede iniciar sesión en uno de los WorkSpaces
- Tengo problemas para usar Docker con Amazon WorkSpaces
- Recibo ThrottlingException errores en algunas de mis llamadas a la API
- Mi WorkSpace sistema se sigue desconectando cuando lo dejo correr en segundo plano

- La federación SAML 2.0 no funciona. Mis usuarios no están autorizados a transmitir su WorkSpaces escritorio.
- Mis usuarios se desconectan de sus WorkSpaces sesiones cada 60 minutos.
- Mis usuarios reciben un error de URI de redireccionamiento cuando se federan mediante el flujo iniciado por el proveedor de identidades (IdP) de SAML 2.0, o se inicia una instancia adicional de la aplicación WorkSpaces cliente cada vez que mis usuarios intentan iniciar sesión desde el cliente después de federarse en el IdP.
- Mis usuarios reciben el mensaje «Algo ha ido mal: se ha producido un error al iniciar tu WorkSpace» cuando intentan iniciar sesión en la aplicación WorkSpaces cliente después de federarse al IdP.
- Mis usuarios reciben el mensaje «No se pueden validar las etiquetas» cuando intentan iniciar sesión en la aplicación WorkSpaces cliente después de federarse con el IdP.
- Mis usuarios reciben el mensaje: «El cliente y el servidor no se pueden comunicar porque no poseen un algoritmo común».
- Mi micrófono o cámara web no funcionan en Windows. WorkSpaces
- Mis usuarios no pueden iniciar sesión mediante la autenticación basada en certificados y se les pide la contraseña en el WorkSpaces cliente o en la pantalla de inicio de sesión de Windows cuando se conectan a su sesión de escritorio.
- Estoy intentando hacer algo que requiere un medio de instalación de Windows, pero WorkSpaces no lo proporciona.
- Quiero lanzarlo WorkSpaces con un directorio AWS gestionado existente creado en una región no WorkSpaces compatible.
- Quiero actualizar Firefox en Amazon Linux 2.
- Mi usuario puede restablecer su contraseña mediante el WorkSpaces cliente, ignorando la configuración de la Política de contraseñas detallada (FFGP) que está configurada. AWS Managed Microsoft AD
- Mis usuarios reciben el mensaje de error «Este sistema operativo/plataforma no está autorizado a acceder a su WorkSpace» cuando intentan acceder a WorkSpace Windows/Linux mediante Web Access

No puedo crear Amazon Linux WorkSpace porque hay caracteres no válidos en el nombre de usuario

Para Amazon Linux WorkSpaces, nombres de usuario:

- Pueden contener un máximo de 20 caracteres
- Pueden contener letras, espacios y números representables en UTF-8
- Pueden incluir los siguientes caracteres especiales: _ .-#
- No pueden comenzar con un símbolo de guion (-) como primer carácter del nombre de usuario

> **Note**
>
> Estas limitaciones no se aplican a Windows WorkSpaces. Windows WorkSpaces admite los símbolos @ y - para todos los caracteres del nombre de usuario.

He cambiado el shell de mi Amazon Linux WorkSpace y ahora no puedo aprovisionar una sesión de PCoIP

Para anular el shell predeterminado para Linux WorkSpaces, consulte. Anular el shell predeterminado de Amazon Linux WorkSpaces

Mi Amazon Linux WorkSpaces no arranca

A partir del 20 de julio de 2020, Amazon Linux WorkSpaces utilizará nuevos certificados de licencia. Estos nuevos certificados solo son compatibles con las versiones 2.14.1.1, 2.14.7, 2.14.9 y 20.10.6 o posteriores del agente PCoIP.

Si utiliza una versión no compatible del agente PCoIP, debe actualizarla a la versión más reciente (20.10.6), que incluye las últimas correcciones y mejoras de rendimiento compatibles con los nuevos certificados. Si no realiza estas actualizaciones antes del 20 de julio, se WorkSpaces producirá un error en el aprovisionamiento de las sesiones de su Linux y los usuarios finales no podrán conectarse a las suyas WorkSpaces.

Para actualizar el agente a la versión más reciente

1. Abra la WorkSpaces consola en https://console.aws.amazon.com/workspaces/.
2. En el panel de navegación, elija WorkSpaces.
3. Selecciona tu Linux WorkSpace y reinícialo seleccionando Acciones, Reiniciar WorkSpaces. Si el WorkSpace estado es`STOPPED`, debe elegir Acciones, Iniciar WorkSpaces primero y esperar hasta que se encuentre en ese estado `AVAILABLE` antes de poder reiniciarlo.

4. Una vez que se WorkSpace haya reiniciado y su estado seaAVAILABLE, le recomendamos que cambie el estado del WorkSpace a ADMIN_MAINTENANCE mientras realiza la actualización. Cuando haya terminado, cambie el estado del WorkSpace a. AVAILABLE Para obtener más información sobre el modo ADMIN_MAINTENANCE, consulte Mantenimiento manual.

   Para cambiar el estado de un WorkSpace toADMIN_MAINTENANCE, haga lo siguiente:

   a. Seleccione WorkSpace y elija Acciones, Modificar WorkSpace.
   b. Elija Modify State (Modificar estado).
   c. En Intended State, seleccione ADMIN_MAINTENANCE.
   d. Elija Modificar.

5. Conéctese a su Linux WorkSpace a través de SSH. Para obtener más información, consulte Habilita las conexiones SSH para tu Linux WorkSpaces.
6. Para detener el agente PCoIP, ejecute el comando siguiente:

   ```
   sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
   ```

7. Para comprobar la versión del agente y confirmar que la actualización se ha realizado correctamente, ejecute el siguiente comando:

   ```
   rpm -q pcoip-agent-standard
   ```

   El comando de verificación debería producir el siguiente resultado:

   ```
   pcoip-agent-standard-20.10.6-1.el7.x86_64
   ```

8. Desconéctelo WorkSpace y reinícielo de nuevo.
9. Si configuró el estado del WorkSpace ADMIN_MAINTENANCE enStep 4, repita el proceso Step 4 y establezca el estado previsto enAVAILABLE.

Si su Linux WorkSpace sigue sin iniciarse después de actualizar el agente PCoIP, póngase en contacto con Support AWS .

El inicio WorkSpaces en mi directorio conectado a menudo falla

Compruebe que se puede obtener acceso a los dos servidores DNS o controladores de dominio del directorio on-premise desde cada una de las subredes que especificó cuando se conectó al

directorio. Para comprobar la conectividad, puede iniciar una instancia de Amazon EC2 en cada subred y vincular la instancia al directorio utilizando las direcciones IP de los dos servidores DNS.

El inicio WorkSpaces falla debido a un error interno

Compruebe si las subredes están configuradas para asignar direcciones IPv6 automáticamente a las instancias lanzadas en la subred. Para comprobar esta configuración, abra la consola de Amazon VPC, seleccione la subred y elija Subnet Actions, Modify auto-assign IP settings. Si esta configuración está habilitada, no podrá iniciar WorkSpaces con los paquetes de rendimiento o gráficos. En su lugar, desactive esta configuración y especifique las direcciones IPv6 manualmente cuando lance las instancias.

Cuando intento registrar un directorio, el registro falla y deja el directorio en estado de ERROR

Este problema puede producirse si intenta registrar un directorio AWS administrado de Microsoft AD que se ha configurado para la replicación en varias regiones. Aunque el directorio de la región principal se puede registrar correctamente para su uso con Amazon WorkSpaces, se produce un error al intentar registrar el directorio en una región replicada. La replicación multirregional con Microsoft AD AWS administrado no se admite para su uso con Amazon WorkSpaces dentro de las regiones replicadas.

Mis usuarios no pueden conectarse a Windows WorkSpace con un banner de inicio de sesión interactivo

Si se ha implementado un mensaje de inicio de sesión interactivo para mostrar un banner de inicio de sesión, los usuarios no podrán acceder a Windows. WorkSpaces El PCoIP no admite actualmente la configuración de la política de grupo de los mensajes de inicio de sesión interactivos. WorkSpaces WorkSpaces Muévala a una unidad organizativa (OU) en la que no se aplique la política de Interactive logon: Message text for users attempting to log on grupo. El mensaje de inicio de sesión es compatible con WSP WorkSpaces y los usuarios deben volver a iniciar sesión después de aceptar el banner de inicio de sesión.

Mis usuarios no se pueden conectar a un Windows WorkSpace

Mis usuarios reciben el siguiente error cuando intentan conectarse a Windows WorkSpaces:

```
"An error occurred while launching your WorkSpace. Please try again."
```

Este error suele producirse cuando no se WorkSpace puede cargar el escritorio de Windows mediante PCoIP. Compruebe lo siguiente:

- Este mensaje aparece si el servicio PCoIP Standard Agent para Windows no está en ejecución. Conéctese mediante RDP para comprobar que el servicio está en ejecución, que está configurado para iniciarse automáticamente y que puede comunicarse a través de la interfaz de administración (eth0).

- Si se ha desinstalado el agente PCoIP, reinícielo a través de WorkSpace la WorkSpaces consola de Amazon para volver a instalarlo automáticamente.

- También podría recibir este error en el WorkSpaces cliente de Amazon después de un largo retraso si el grupo de WorkSpaces seguridad se modificó para restringir el tráfico saliente. La restricción del tráfico saliente impide que Windows se comunique con los controladores de directorio para iniciar sesión. Compruebe que sus grupos de seguridad le permiten WorkSpaces comunicarse con los controladores de directorio en todos los puertos necesarios a través de la interfaz de red principal.

Otra causa de este error está relacionada con la directiva de grupo de asignación de derechos de usuario. Si la siguiente política de grupo está mal configurada, impide que los usuarios puedan acceder a su Windows WorkSpaces:

Configuración del equipo/Configuración de Windows/Configuración de seguridad/Políticas locales/Asignación de derechos de usuario

- Política incorrecta:

  Política: acceder a este equipo desde la red

  Configuración: *Nombre de dominio*\Equipos de dominio

  GPO ganador: permitir acceso a archivos
- Política correcta:

  Política: acceder a este equipo desde la red

  Configuración: *Nombre de dominio*Usuarios de dominio

GPO ganador: permitir acceso a archivos

> **Note**
>
> Esta configuración de política debe aplicarse a Usuarios de dominio en lugar de Equipos de dominio.

Para obtener más información, consulte Acceder a este equipo desde la configuración de política de seguridad de red y Configurar opciones de política de seguridad en la documentación de Microsoft Windows.

Mis usuarios tienen problemas cuando intentan iniciar sesión WorkSpaces desde WorkSpaces Web Access

Amazon WorkSpaces se basa en una configuración de pantalla de inicio de sesión específica para permitir a los usuarios iniciar sesión correctamente desde su cliente de acceso web.

Para permitir que los usuarios de Web Access inicien sesión en su cuenta WorkSpaces, debe configurar una política de grupo y tres ajustes de política de seguridad. Si estas opciones no están configuradas correctamente, es posible que los usuarios experimenten tiempos de inicio de sesión prolongados o pantallas negras al intentar iniciar sesión en su WorkSpaces cuenta. Para configurar estas opciones, consulte Habilitar y configurar Amazon WorkSpaces Web Access.

> **Important**
>
> A partir del 1 de octubre de 2020, los clientes ya no podrán usar el cliente Amazon WorkSpaces Web Access para conectarse a Windows 7 custom WorkSpaces o a Windows 7 Bring Your Own License (BYOL) WorkSpaces.

El WorkSpaces cliente de Amazon muestra una pantalla gris que dice «Cargando...» durante un tiempo antes de volver a la pantalla de inicio de sesión. No aparece ningún otro mensaje de error.

Este comportamiento suele indicar que el WorkSpaces cliente puede autenticarse a través del puerto 443, pero no puede establecer una conexión de streaming a través del puerto 4172 (PCoIP) o el puerto 4195 (WSP). Esta situación puede producirse cuando no se cumplen los requisitos previos de la red. Los problemas en el lado del cliente suelen provocar que se produzcan errores en la comprobación de red en el cliente. Para ver qué comprobaciones de estado están fallando, seleccione el icono de comprobación de red (que suele ser un triángulo rojo con un signo de exclamación en la esquina inferior derecha de la pantalla de inicio de sesión en el caso de los clientes que usen la versión 2.0 o posterior o el icono de red

en la esquina superior derecha para los clientes que usen la versión 3.0 o posterior).

> **Note**
>
> La causa más común de este problema es que hay un proxy o un firewall del lado del cliente que impide el acceso a través del puerto 4172 o 4195 (TCP y UDP). Si se produce un error en esta comprobación de estado, examine la configuración del firewall local.

Si se aprueba la comprobación de red, es posible que haya un problema con la configuración de red del. WorkSpace Por ejemplo, una regla de Firewall de Windows podría bloquear el puerto UDP 4172 o 4195 de la interfaz de administración. Conéctese al cliente WorkSpace mediante un protocolo de escritorio remoto (RDP) para comprobar que WorkSpace cumple con los requisitos de puerto necesarios.

Mis usuarios reciben el mensaje "WorkSpace Estado: insalubre». No hemos podido conectarlo con su WorkSpace. Vuelva a intentarlo en unos minutos".

Este error suele indicar que el SkyLightWorkSpacesConfigService servicio no responde a las comprobaciones de estado.

Si acabas de reiniciar o iniciar el WorkSpace, espera unos minutos y vuelve a intentarlo.

Si se WorkSpace ha estado ejecutando durante algún tiempo y sigue apareciendo este error, conéctese mediante RDP para comprobar que el servicio: SkyLightWorkSpacesConfigService

- está en ejecución.
- está configurado para iniciarse automáticamente.
- puede comunicarse a través de la interfaz de administración (eth0).
- no lo está bloqueando un software antivirus de terceros.

Mis usuarios reciben el mensaje «Este dispositivo no está autorizado a acceder al WorkSpace. Póngase en contacto con su administrador para obtener ayuda".

Este error indica que los grupos de control de acceso IP están configurados en el WorkSpace directorio, pero la dirección IP del cliente no está en la lista de direcciones permitidas.

Compruebe la configuración del directorio. Confirme que la dirección IP pública desde la que se conecta el usuario permite el WorkSpace acceso a.

Los usuarios reciben el mensaje «No hay red. Se ha perdido la conexión de red. Compruebe la conexión de red o póngase en contacto con el administrador para obtener ayuda”. al intentar conectarse a un WSP WorkSpace

Si se produce este error y los usuarios no tienen problemas de conectividad, asegúrese de que el puerto 4195 está abierto en los cortafuegos de su red. Para WorkSpaces usar el Protocolo de WorkSpaces Transmisión (WSP), el puerto utilizado para transmitir la sesión del cliente se cambió del 4172 al 4195.

El WorkSpaces cliente produce un error de red a mis usuarios, pero pueden usar otras aplicaciones habilitadas para la red en sus dispositivos

Las aplicaciones WorkSpaces cliente dependen del acceso a los recursos de la AWS nube y requieren una conexión que proporcione un ancho de banda de descarga de al menos 1 Mbps. Si un dispositivo tiene una conexión intermitente a la red, la aplicación WorkSpaces cliente podría informar de un problema con la red.

WorkSpaces impone el uso de certificados digitales emitidos por Amazon Trust Services a partir de mayo de 2018. Amazon Trust Services ya es una CA raíz de confianza en los sistemas operativos compatibles con WorkSpaces. Si la lista de entidades emisoras de certificados raíz del sistema operativo no está actualizada, el dispositivo no se puede conectar WorkSpaces y el cliente genera un error de red.

Para reconocer problemas de conexión debidos a errores de certificado

- Clientes cero de PCoIP: aparece el siguiente mensaje de error.

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- Otros clientes: las comprobaciones de estado fallan y aparece un triángulo de advertencia rojo para Internet.

Para resolver errores de certificado

- Aplicación cliente para Windows
- Clientes cero PCoIP
- Otras aplicaciones cliente

Aplicación cliente para Windows

Utilice una de las siguientes soluciones para errores de certificado.

Solución 1: actualizar la aplicación cliente

Durante la instalación, la aplicación cliente garantiza que el sistema operativo confía en los certificados emitidos por Amazon Trust Services.

Solución 2: agregue Amazon Trust Services a la lista de CA raíz local

1. Abra https://www.amazontrust.com/repository/.
2. Descargue el certificado de Starfield en formato DER (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92).
3. Abra Microsoft Management Console. (Desde el símbolo del sistema, ejecute mmc).

4. Seleccione File (Archivo), Add/Remove Snap-in (Añadir/quitar complemento), Certificates (Certificados), Add (Añadir).
5. En la página Certificates snap-in C(Complemento de certificados), seleccione Computer account (Cuenta del equipo) y haga clic en Next (Siguiente). Mantenga el valor predeterminado, Local computer (Equipo local). Seleccione Finalizar. Seleccione Aceptar.
6. En Certificates (Local Computer) [Certificados (Equipo local)], expanda Trusted Root Certification Authorities (Entidades de certificación raíz de confianza). Seleccione Action (Acción), All Tasks (Todas las tareas), Import (Importar).
7. Siga el asistente para importar el certificado que ha descargado.
8. Cierre la aplicación cliente y reiníciela. WorkSpaces

Solución 3: implementar Amazon Trust Services como CA de confianza mediante la directiva de grupo

Agregue el certificado Starfield a las entidades de certificación raíz de confianza para el dominio mediante la directiva de grupo. Para obtener más información, consulte Use Policy to Distribute Certificates.

Clientes cero PCoIP

Para conectarse directamente a un firmware que WorkSpace utilice la versión 6.0 o posterior, descargue e instale el certificado emitido por Amazon Trust Services.

Para agregar Amazon Trust Services como entidad de certificación raíz de confianza

1. Abra https://certs.secureserver.net/repository/.
2. Descargue el certificado en Starfield Certificate Chain (Cadena de certificado de Starfield) con la huella digital 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58.
3. Cargue el certificado al cliente cero. Para obtener más información, consulte Uploading Certificates en la documentación de Teradici.

Otras aplicaciones cliente

Agregue el certificado de Starfield (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) desde Amazon Trust

Services. Para obtener más información acerca de cómo agregar una entidad de certificación raíz, consulte la siguiente documentación:

- Android: Añadir y quitar certificados
- Chrome OS: Administrar certificados de cliente en dispositivos Chrome
- macOS e iOS: Installing a CA's Root Certificate on Your Test Device

Mis WorkSpace usuarios ven el siguiente mensaje de error: «El dispositivo no se puede conectar al servicio de registro. Compruebe la configuración de red".

Cuando se produce un error en el servicio de registro, es posible que WorkSpace los usuarios vean el siguiente mensaje de error en la página de comprobación del estado de la conexión: «El dispositivo no puede conectarse al servicio de WorkSpaces registro. No podrás registrar tu dispositivo en WorkSpaces. Compruebe la configuración de red".

Este error se produce cuando la aplicación WorkSpaces cliente no puede acceder al servicio de registro. Normalmente, esto ocurre cuando se ha eliminado el WorkSpaces directorio. Para resolver este error, asegúrese de que el código de registro sea válido y corresponda a un directorio en ejecución en la AWS nube.

Mis usuarios de cliente cero PCoIP están recibiendo el error “El certificado suministrado no es válido debido a la marca temporal”

Si el NTP no está habilitado en Teradici, los usuarios de cliente cero PCoIP podrían recibir errores de certificado. Para configurar el NTP, consulte Configuración del cliente de PCoIP Zero para WorkSpaces.

Las impresoras USB y otros periféricos USB no funcionan para los clientes cero PCoIP

A partir de la versión 20.10.4 del agente PCoIP, Amazon WorkSpaces deshabilita la redirección USB de forma predeterminada a través del registro de Windows. Esta configuración de registro afecta al comportamiento de los periféricos USB cuando los usuarios utilizan dispositivos PCoIP de cliente cero para conectarse a sus dispositivos. WorkSpaces

WorkSpaces Si utiliza la versión 20.10.4 o posterior del agente PCoIP, los dispositivos periféricos USB no funcionarán con los dispositivos PCoIP cero cliente hasta que haya activado la redirección USB.

> **Note**
>
> Si utiliza controladores de impresora virtual de 32 bits, también debe actualizar dichos controladores a sus versiones de 64 bits.

Para habilitar el redireccionamiento USB en los dispositivos cliente cero PCoIP

Le recomendamos que introduzca estos cambios de registro a través de la política de grupo. WorkSpaces Para obtener más información, consulte Configuración del agente y Ajustes configurables en la documentación de Teradici.

1. Establezca el siguiente valor de clave del Registro en 1 (habilitado):

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ PCoIP\ pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = ESPADA

   KeyValue = 1
2. Establezca el siguiente valor de clave del Registro en 1 (habilitado):

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Políticas\ Teradici\ PCoIP\ pcoip_admin_defaults

   KeyName = pcoip.enable_usb

   KeyType = ESPADA

   KeyValue = 1
3. Si aún no lo ha hecho, cierre la WorkSpace sesión y vuelva a iniciarla. Sus dispositivos USB deberían funcionar ahora.

Mis usuarios omitieron actualizar sus aplicaciones cliente de Windows o macOS y no se les solicita que instalen la versión más reciente

Cuando los usuarios omiten las actualizaciones de la aplicación cliente de Amazon WorkSpaces Windows, se establece la clave de registro de SkipThisversiones y ya no se les pide que actualicen sus clientes cuando se publique una nueva versión del cliente. Para actualizar a la última versión, puede editar el registro tal y como se describe en Actualización de la aplicación cliente de WorkSpaces Windows a una versión más reciente de la Guía del WorkSpaces usuario de Amazon. También puede ejecutar el siguiente PowerShell comando:

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

Cuando los usuarios omiten las actualizaciones de la aplicación cliente de Amazon WorkSpaces macOS, se establece la `SUSkippedVersion` preferencia y ya no se les pide que actualicen sus clientes cuando se publique una nueva versión del cliente. Para actualizar a la última versión, puedes restablecer esta preferencia tal y como se describe en Actualizar la aplicación cliente de WorkSpaces macOS a una versión más reciente de la Guía del WorkSpaces usuario de Amazon.

Mis usuarios no pueden instalar la aplicación cliente de Android en sus Chromebooks

La versión 2.4.13 es la versión final de la aplicación cliente Amazon WorkSpaces Chromebook. Como Google está eliminando gradualmente la compatibilidad con las aplicaciones de Chrome, no habrá más actualizaciones en la aplicación cliente de WorkSpaces Chromebook y no se admite su uso.

En el caso de los Chromebooks que admiten la instalación de aplicaciones de Android, te recomendamos que utilices en su lugar la aplicación cliente de Android. WorkSpaces

En algunos casos, es posible que tenga que habilitar los Chromebooks de los usuarios para instalar aplicaciones Android. Para obtener más información, consulte Configurar Android para Chromebooks.

Mis usuarios no reciben correos electrónicos de invitación ni de restablecimiento de contraseña

Los usuarios no reciben automáticamente correos electrónicos de bienvenida o de restablecimiento de WorkSpaces contraseña creados con AD Connector o un dominio de confianza. Los correos electrónicos de invitación tampoco se envían automáticamente si el usuario ya existe en Active Directory.

Para enviar de forma manual correos electrónicos de bienvenida a estos usuarios, consulte Enviar un correo electrónico de invitación.

Para restablecer las contraseñas de usuario, consulte Configurar las herramientas de administración de Active Directory para WorkSpaces.

Mis usuarios no ven la opción "¿Olvidó la contraseña?" en la pantalla de inicio de sesión del cliente

Si utiliza Conector AD o un dominio de confianza, los usuarios no podrán restablecer sus propias contraseñas. (El ¿Has olvidado tu contraseña? la opción de la pantalla de inicio de sesión de la aplicación WorkSpaces cliente no estará disponible). Para obtener información acerca de cómo restablecer las contraseñas de usuario, consulte Configurar las herramientas de administración de Active Directory para WorkSpaces.

Cuando intento instalar aplicaciones en un sistema Windows, recibo el mensaje «El administrador del sistema ha establecido políticas para impedir esta instalación» WorkSpace

Puede abordar este problema modificando la configuración de la política de grupo de Windows Installer. Para implementar esta política WorkSpaces en varios directorios, aplique esta configuración a un objeto de política de grupo que esté vinculado a la unidad WorkSpaces organizativa (OU) desde una instancia EC2 unida a un dominio. Si utiliza Conector AD, puede realizar estos cambios desde un controlador de dominio. Para obtener más información acerca del uso de las herramientas de administración de Active Directory para trabajar con objetos de políticas de grupo, consulte Instalación de las herramientas de administración de Active Directory en la Guía de administración de AWS Directory Service .

El siguiente procedimiento muestra cómo configurar la configuración de Windows Installer para el objeto de política de WorkSpaces grupo.

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente esté instalada en su dominio.
2. Abra la herramienta de administración de políticas de grupo en su WorkSpace cliente de Windows y busque y seleccione el objeto de política de WorkSpaces grupo para las cuentas de sus WorkSpaces máquinas. En el menú principal, elija Action (Acción), Edit (Editar).
3. En el editor de administración de políticas de grupo, elija Computer Configuration (Configuración del equipo), Policies (Políticas), Administrative Templates (Plantillas administrativas), Classic Administrative Templates (Plantillas administrativas clásicas), Windows Components (Componentes de Windows), Windows Installer.
4. Abra la configuración Turn Off Windows Installer (Desactivar Windows Installer).
5. En el cuadro de diálogo Turn Off Windows Installer (Desactivar Windows Installer), cambie Not Configured (No configurado) a Enabled (Habilitado) y, a continuación, establezca Disable Windows Installer (Deshabilitar Windows Installer) en Never (Nunca).
6. Seleccione Aceptar.
7. Para aplicar los cambios de política de grupo, realice una de las siguientes acciones:
   - Reinicie el WorkSpace (en la WorkSpaces consola, seleccione y WorkSpace, a continuación, elija Acciones, reinicie WorkSpaces).
   - En el símbolo del sistema administrativo, introduzca gpupdate /force.

No, WorkSpaces en mi directorio puedo conectarme a Internet

WorkSpaces no se puede comunicar con Internet de forma predeterminada. Para que tengan conexión a Internet, debe proporcionarles acceso de manera explícita. Para obtener más información, consulte Proporcione acceso a Internet desde su WorkSpace.

My WorkSpace ha perdido su acceso a Internet

Si WorkSpace ha perdido el acceso a Internet y no puede conectarse WorkSpace mediante RDP, este problema probablemente se deba a la pérdida de la dirección IP pública del WorkSpace. Si ha habilitado la asignación automática de direcciones IP elásticas a nivel de directorio, se le asignará una dirección IP elástica (del grupo proporcionado por Amazon) WorkSpace cuando se lance. Sin embargo, si asocias una dirección IP elástica de tu propiedad a una y WorkSpace, posteriormente, desasocias esa dirección IP elástica de la WorkSpace, WorkSpace pierde su dirección IP pública y no obtiene automáticamente una nueva del grupo proporcionado por Amazon.

Para asociar una nueva dirección IP pública del grupo proporcionado por Amazon al WorkSpace, debes volver a crear el. WorkSpace Si no quiere volver a crear el WorkSpace, debe asociar otra dirección IP elástica de su propiedad al. WorkSpace

Se recomienda no modificar la interfaz de red elástica de a WorkSpace después de WorkSpace su lanzamiento. Una vez asignada una dirección IP elástica a WorkSpace, WorkSpace conserva la misma dirección IP pública (a menos que WorkSpace se reconstruya, en cuyo caso obtiene una nueva dirección IP pública).

Aparece el error “DNS no disponible” cuando intento conectarme a mi directorio on-premise

Cuando se conecta al directorio en las instalaciones aparece un mensaje de error similar al siguiente.

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

Es necesario que Conector AD pueda comunicarse con los servidores DNS en las instalaciones a través de TCP y UDP en el puerto 53. Asegúrese de que los grupos de seguridad y los firewalls on-premise permiten la comunicación TCP y UDP a través de dicho puerto.

Aparece el error “Problemas de conectividad detectados” cuando intento conectarme a mi directorio en las instalaciones

Cuando se conecta al directorio en las instalaciones aparece un mensaje de error similar al siguiente.

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

Es necesario que Conector AD pueda comunicarse con los controladores de dominio en las instalaciones a través de TCP y UDP en los siguientes puertos. Asegúrese de que los grupos de seguridad y firewall locales permiten la comunicación TCP y UDP a través de dichos puertos:

- 88 (Kerberos)
- 389 (LDAP)

Aparece el error “Registro SRV” cuando intento conectarme a mi directorio en las instalaciones

Cuando se conecta al directorio en las instalaciones, aparece un mensaje de error similar a los siguientes:

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

Cuando Conector AD se conecta al directorio, necesita obtener los registros SRV `_ldap._tcp.`*`dns-domain-name`* y `_kerberos._tcp.`*`dns-domain-name`*. Este error aparece si el servicio no puede obtener estos registros de los servidores DNS que especificó al conectarse a su directorio. Asegúrese de que los servidores DNS contienen estos registros SRV. Para obtener más información, consulte SRV Resource Records en Microsoft TechNet.

Mi Windows WorkSpace entra en modo de suspensión cuando está inactivo

Para resolver este problema, conéctese al plan de energía WorkSpace y cámbielo a Alto rendimiento mediante el siguiente procedimiento:

1. En el WorkSpace Panel de control, selecciona Hardware o Hardware y sonido (el nombre puede variar según la versión de Windows).
2. En Power Options (Opciones de energía), seleccione Choose a power plan (Elegir un plan de energía).
3. En el panel Elegir o personalizar un plan de energía, elija el plan de energía Alto rendimiento y, después. Cambiar configuración del plan.
   - Si la opción para elegir el plan de energía Alto rendimiento está desactivada, elija Cambiar los ajustes que no están disponibles actualmente y, a continuación, elija el plan de energía Alto rendimiento.
   - Si no aparece el plan Alto rendimiento, seleccione la flecha situada a la derecha de Mostrar planes adicionales para mostrarlo o Crear un plan de energía en el menú de navegación de la izquierda, elija Alto rendimiento, escriba un nombre al plan de energía y, a continuación, seleccione Siguiente.
4. En la página Cambiar la configuración del plan: Alto rendimiento, asegúrese de que Apagar la pantalla y (si está disponible) Poner el ordenador en reposo están configuradas en Nunca.

5. Si ha realizado algún cambio en el plan Alto rendimiento, seleccione Guardar cambios (o elija Crear si quiere crear otro plan).

Si los pasos anteriores no resuelven el problema, haga lo siguiente:

1. En el WorkSpace Panel de control, selecciona Hardware o Hardware y sonido (el nombre puede variar según la versión de Windows).
2. En Power Options (Opciones de energía), seleccione Choose a power plan (Elegir un plan de energía).
3. En el panel Choose or customize a power plan (Elegir o personalizar un plan de energía), seleccione el enlace Change plan settings (Cambiar la configuración del plan) situado a la derecha del plan de energía High performance (Alto rendimiento) y, a continuación, elija el enlace Change advanced power settings (Cambiar la configuración avanzada de energía).
4. En la lista de opciones de configuración que aparece en el cuadro de diálogo Power Options (Opciones de energía), elija el signo más situado a la izquierda de Hard disk (Disco duro) para mostrar las opciones pertinentes.
5. Compruebe que el valor Turn off hard disk after (Apagar disco duro tras) para Plugged in (Con corriente alterna) es superior al valor de On battery (Con batería) (el valor predeterminado son 20 minutos).
6. Elija el signo más que aparece a la izquierda de PCI Express (PCI Express) y haga lo mismo para Link State Power Management (Administración de energía del estado de vínculos).
7. Compruebe que la configuración de Link State Power Management (Administración de energía del estado de vínculos) está establecida en Off (Desactivada).
8. Elija OK (Aceptar) (o Apply (Aplicar) si ha cambiado alguna configuración) para cerrar el cuadro de diálogo.
9. Si ha cambiado algún valor, elija Guardar cambios en el panel Change settings for the plan (Cambiar configuración del plan).

Uno de los míos WorkSpaces tiene un estado de **UNHEALTHY**

El WorkSpaces servicio envía periódicamente solicitudes de estado a un WorkSpace. WorkSpaceSe marca A `UNHEALTHY` cuando no responde a estas solicitudes. Las causas más comunes de este problema son:

- Una aplicación WorkSpace está bloqueando los puertos de red, lo que impide que responda a la solicitud de estado. WorkSpace
- El alto uso WorkSpace de la CPU impide responder a la solicitud de estado de manera oportuna.
- Se WorkSpace ha cambiado el nombre de la computadora. Esto impide que se establezca un canal seguro entre WorkSpaces y el WorkSpace.

Puede intentar solucionar esta situación a través de los siguientes métodos:

- Reinicie el WorkSpace desde la WorkSpaces consola.
- Conéctese al dispositivo en mal estado WorkSpace mediante el siguiente procedimiento, que solo debe utilizarse para solucionar problemas:

  1. Conéctese a un operativo WorkSpace en el mismo directorio que el que está en mal estado WorkSpace.
  2. Desde el punto de WorkSpace vista operativo, utilice el Protocolo de escritorio remoto (RDP) para conectarse al dispositivo en mal estado WorkSpace utilizando la dirección IP del dispositivo en mal WorkSpace estado. En función de la magnitud del problema, es posible que no puedas conectarte con el dispositivo en mal WorkSpace estado.
  3. En caso de avería WorkSpace, confirme que se cumplen los requisitos mínimos de puerto.
- Asegúrese de que el SkyLightWorkSpacesConfigService servicio pueda responder a los controles de estado. Para solucionar este problema, consulte Mis usuarios reciben el mensaje "WorkSpace Estado: insalubre». No hemos podido conectarlo con su WorkSpace. Vuelva a intentarlo en unos minutos"..
- Reconstruya el WorkSpace desde la WorkSpaces consola. Dado que la reconstrucción de un WorkSpace puede provocar una pérdida de datos, esta opción solo debe utilizarse si todos los demás intentos de corregir el problema no han tenido éxito.

My WorkSpace se bloquea o se reinicia inesperadamente

Si su WorkSpace configuración para PCoIP se bloquea o se reinicia repetidamente y sus registros de errores o volcados indican que hay problemas `spacedeskHookKmode.sys` o si recibe los siguientes mensajes de error`spacedeskHookUmode.dll`, puede que tenga que deshabilitar el acceso web a: WorkSpace

```
The kernel power manager has initiated a shutdown transition.
```

```
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - Estos pasos de solución de problemas no se aplican a los configurados para el WorkSpaces Protocolo de transmisión (WSP). WorkSpaces Solo se aplican a los WorkSpaces que están configurados para PCoIP.
> - Únicamente debe deshabilitar Acceso web si no va a permitir que los usuarios utilicen Acceso web.

Para deshabilitar el acceso web al WorkSpace, debe deshabilitar el acceso web en el WorkSpaces directorio y reiniciar el. WorkSpace

El mismo nombre de usuario tiene más de uno WorkSpace, pero el usuario solo puede iniciar sesión en uno de los WorkSpaces

Si elimina un usuario de Active Directory (AD) sin eliminarlo primero WorkSpace y, a continuación, lo vuelve a agregar a Active Directory y crea uno nuevo WorkSpace para ese usuario, el mismo nombre de usuario ahora tendrá dos WorkSpaces en el mismo directorio. Sin embargo, si el usuario intenta conectarse a su original WorkSpace, recibirá el siguiente error:

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

Además, las búsquedas del nombre de usuario en la WorkSpaces consola de Amazon solo muestran el nuevo WorkSpace, aunque ambos WorkSpaces sigan existiendo. (Para encontrar el original, busca WorkSpace el WorkSpace ID en lugar del nombre de usuario).

Este comportamiento también puede producirse si cambia el nombre de un usuario en Active Directory sin eliminarlo primero. WorkSpace Si, a continuación, cambia su nombre de usuario por el nombre de usuario original y crea uno nuevo WorkSpace para el usuario, el mismo nombre de usuario tendrá dos WorkSpaces en el directorio.

Este problema se produce porque Active Directory utiliza el identificador de seguridad (SID) del usuario, en lugar del nombre de usuario, para identificar de forma exclusiva al usuario. Cuando se

elimina y se vuelve a crear un usuario en Active Directory, se le asigna un nuevo SID, incluso aunque su nombre de usuario siga siendo el mismo. Durante las búsquedas de un nombre de usuario, la WorkSpaces consola de Amazon utiliza el SID para buscar coincidencias en Active Directory. Los WorkSpaces clientes de Amazon también utilizan el SID para identificar a los usuarios cuando se conectan a ellos WorkSpaces.

Para resolver este problema, siga uno de estos pasos:

- Si este problema se produjo porque el usuario se eliminó y se volvió a crear en Active Directory, es posible que pueda restaurar el objeto del usuario eliminado original si tiene habilitada la característica Papelera de reciclaje en Active Directory. Si puedes restaurar el objeto de usuario original, asegúrate de que el usuario pueda conectarse a su objeto original WorkSpace. Si es posible, puedes eliminar el nuevo WorkSpace después de hacer una copia de seguridad y transferir manualmente los datos de usuario del nuevo WorkSpace al original WorkSpace (si es necesario).
- Si no puede restaurar el objeto de usuario original, elimine el original del usuario WorkSpace. En su WorkSpace lugar, el usuario debería poder conectarse al nuevo y usarlo. Asegúrese de hacer una copia de seguridad y transferir manualmente los datos del usuario del original WorkSpace al nuevo WorkSpace.

> **Warning**
>
> Eliminar un WorkSpace es una acción permanente y no se puede deshacer. Los datos del WorkSpace usuario no persisten y se destruyen. Para obtener ayuda para realizar el backup de los datos de usuario, póngase en contacto con AWS Support.

Tengo problemas para usar Docker con Amazon WorkSpaces

Windows WorkSpaces

La virtualización anidada (incluido el uso de Docker) no es compatible con Windows. WorkSpaces Para obtener más información, consulte la documentación de Docker.

Linux WorkSpaces

Para usar Docker en Linux WorkSpaces, asegúrese de que los bloques CIDR utilizados por Docker no se superpongan con los bloques CIDR utilizados en las dos interfaces de red elásticas (ENI)

asociadas a. WorkSpace Si tiene problemas con el uso de Docker en Linux WorkSpaces, póngase en contacto con Docker para obtener ayuda.

Recibo ThrottlingException errores en algunas de mis llamadas a la API

La frecuencia predeterminada permitida para las llamadas a la WorkSpaces API es una velocidad constante de dos llamadas a la API por segundo, con una velocidad máxima de «ráfaga» permitida de cinco llamadas a la API por segundo. En la siguiente tabla se muestra cómo funciona el límite de la tasa de ráfaga en las solicitudes de API.

Segundo	Número de solicitudes enviadas	Número neto de solicitudes permitidas	Detalles
1	0	5	Durante el primer segundo (segundo 1), se permiten cinco solicitudes, hasta alcanzar la tasa de ráfaga máxima de cinco llamadas por segundo.
2	2	5	Como en el segundo 1 se emitieron dos o menos llamadas, la capacidad de ráfaga completa de cinco llamadas sigue estando disponible.
3	5	5	Como en el segundo 2 solo se emitieron dos llamadas, la capacidad de ráfaga completa de cinco llamadas sigue estando disponible.
4	2	2.	Como en el segundo 3 se utilizó toda la capacidad de ráfaga, solo está disponible la tasa constante de dos llamadas por segundo.
5	3	2	Como no hay más capacidad de ráfaga, solo se permiten dos llamadas en este momento. Esto significa que una de las tres llamadas a la API estará restringida. La única llamada restringida responderá tras un breve retraso.
6	0	1	Como una de las llamadas del segundo 5 está intentándose de nuevo en el segundo 6, solo hay

Segundo	Número de solicitudes enviadas	Número neto de solicitudes permitidas	Detalles
			capacidad para una llamada más en el segundo 6, ya que el límite de la tasa constante es de dos llamadas por segundo.
7	0	3	Ahora que ya no hay más llamadas a la API restringi das en la cola, el límite de la tasa continúa aumentand o hasta alcanzar el límite de la tasa de ráfaga, que es de cinco llamadas.
8	0	5	Como no se emitieron llamadas en el segundo 7, se permite el número máximo de solicitudes.
9	0	5	Aunque no se emitieron llamadas en el segundo 8, el límite de la tasa no aumenta por encima de cinco.

Mi WorkSpace sistema se sigue desconectando cuando lo dejo correr en segundo plano

Los usuarios de Mac deben comprobar si la característica Power Nap está activada. Si está desactivada, haga clic en ella para activarla. Para desactivar Power Nap, abra el terminal y ejecute el siguiente comando:

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

La federación SAML 2.0 no funciona. Mis usuarios no están autorizados a transmitir su WorkSpaces escritorio.

Esto podría ocurrir porque la política insertada que está integrada para el rol de IAM de federación SAML 2.0 no incluye permisos para transmitir desde el directorio Nombre de recurso de Amazon (ARN). La función de IAM la asume el usuario federado que accede a un WorkSpaces directorio. Edite los permisos del rol para incluir el ARN del directorio y asegúrese de que el usuario tenga un

WorkSpace en el directorio. Para obtener más información, consulte Autenticación con SAML 2.0 y solución de problemas de federación con SAML 2.0. AWS

Mis usuarios se desconectan de sus WorkSpaces sesiones cada 60 minutos.

Si ha configurado la autenticación SAML 2.0 para WorkSpaces, según su proveedor de identidad (IdP), es posible que deba configurar la información que el IdP pasa como atributos AWS de SAML como parte de la respuesta de autenticación. Esto incluye la configuración del elemento Atributo con el atributo `SessionDuration` establecido en `https://aws.amazon.com/SAML/Attributes/SessionDuration`.

`SessionDuration` especifica la cantidad máxima de tiempo que una sesión de streaming federada puede permanecer activa antes de que se requiera la segunda autenticación. Aunque `SessionDuration` es un atributo opcional, se recomienda incluirlo en la respuesta de autenticación SAML. Si no especifica este atributo, la duración de la sesión se establece por defecto en 60 minutos.

Para resolver este problema, configure el IdP para que incluya el valor `SessionDuration` en la respuesta de autenticación SAML y establezca el valor según sea necesario. Para obtener más información, consulte Paso 5: Cree declaraciones para la respuesta de autenticación SAML.

Mis usuarios reciben un error de URI de redireccionamiento cuando se federan mediante el flujo iniciado por el proveedor de identidades (IdP) de SAML 2.0, o se inicia una instancia adicional de la aplicación WorkSpaces cliente cada vez que mis usuarios intentan iniciar sesión desde el cliente después de federarse en el IdP.

Este error se produce debido a una URL de estado de retransmisión que no es válida. Asegúrese de que el estado de retransmisión en la configuración de la federación de IdP sea correcto y que la URL de acceso del usuario y el nombre del parámetro del estado de retransmisión estén configurados correctamente para la federación de IdP en las propiedades del directorio. WorkSpaces Si son válidos y el problema persiste, ponte en contacto con AWS Support. Para obtener más información, consulte Configuración de SAML.

Mis usuarios reciben el mensaje «Algo ha ido mal: se ha producido un error al iniciar tu WorkSpace» cuando intentan iniciar sesión en la aplicación WorkSpaces cliente después de federarse al IdP.

Revise las notificaciones SAML 2.0 de su federación. El valor del NameID del sujeto SAML debe coincidir con WorkSpaces el nombre de usuario y, por lo general, es el mismo que el atributo AccountNamesAM del usuario de Active Directory. Además, el elemento de atributo que tiene el `PrincipalTag:Email` atributo establecido `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` debe coincidir con la dirección de correo electrónico del WorkSpaces usuario tal como se define en el WorkSpaces directorio. Para obtener más información, consulte Configuración de SAML.

Mis usuarios reciben el mensaje «No se pueden validar las etiquetas» cuando intentan iniciar sesión en la aplicación WorkSpaces cliente después de federarse con el IdP.

Revise los valores de los atributos `PrincipalTag` de las aserciones de SAML 2.0 de su federación, como: `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` Los valores de las etiquetas pueden incluir combinaciones de caracteres `_ . : / = + - @`, letras, números y espacios. Para obtener más información, consulte Reglas de etiquetado en IAM y. AWS STS

Mis usuarios reciben el mensaje: «El cliente y el servidor no se pueden comunicar porque no poseen un algoritmo común».

Este problema puede producirse si no habilita TLS 1.2.

Mi micrófono o cámara web no funcionan en Windows. WorkSpaces

Abra el menú Inicio y compruebe su configuración de privacidad

- Inicio > Configuración > Privacidad > Cámara
- Inicio > Configuración > Privacidad > Micrófono

Si estas opciones están desactivadas, actívalas.

Como alternativa, WorkSpaces los administradores pueden crear un objeto de política de grupo (GPO) para habilitar el micrófono o la cámara web según sea necesario.

Mis usuarios no pueden iniciar sesión mediante la autenticación basada en certificados y se les pide la contraseña en el WorkSpaces cliente o en la pantalla de inicio de sesión de Windows cuando se conectan a su sesión de escritorio.

La autenticación basada en certificados no se realizó correctamente durante la sesión. Si el problema persiste, el error de autenticación basada en certificados puede deberse a uno de los siguientes problemas:

- El WorkSpaces o el cliente no son compatibles. La autenticación basada en certificados es compatible con los paquetes de Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) que utilizan la última WorkSpaces aplicación cliente de Windows.
- Debe WorkSpaces reiniciarse después de habilitar la autenticación basada en certificados en el Directorio. WorkSpaces
- WorkSpaces no pudo comunicarse con AWS Private CA el certificado o AWS Private CA no lo emitió. Consulte AWS CloudTrail para determinar si se emitió un certificado. Para obtener más información, consulte Administración de la autenticación basada en certificados.
- El controlador de dominio no tiene un certificado de controlador de dominio para el inicio de sesión con tarjeta inteligente o ha caducado. Para obtener más información, consulte el paso 7, «Configure los controladores de dominio con un certificado de controlador de dominio para autenticar a los usuarios de tarjetas inteligentes» en Requisitos previos.
- El certificado no es de confianza. Para obtener más información, consulte el paso 7, «Publique la CA privada en Active Directory» en Requisitos previos. Ejecute `certutil -viewstore -enterprise NTAuth` en los controladores de dominio para confirmar que la CA está publicada.
- Hay un certificado en la memoria caché, pero los atributos del usuario que invalidó el certificado han cambiado. Póngase en contacto con nosotros AWS Support para borrar la memoria caché antes de que caduque el certificado (24 horas). Para obtener más información, consulte el Centro de AWS Support.
- El userPrincipalName formato del atributo `UserPrincipalName` SAML no tiene el formato correcto o no se resuelve en el dominio real del usuario. Para obtener más información, consulte el paso 1 de Requisitos previos.
- El atributo `ObjectSid` (opcional) de la aserción SAML no coincide con el identificador de seguridad (SID) de Active Directory del usuario especificado en `NameID` de SAML_Subject.

Confirme que la asignación de atributos es correcta en su federación de SAML y que su proveedor de identidad de SAML está sincronizando el atributo SID para el usuario de Active Directory.

- Hay configuraciones de política de grupo que modifican la configuración predeterminada de Active Directory para el inicio de sesión con tarjeta inteligente o toman medidas si se retira una tarjeta inteligente de un lector de tarjetas inteligentes. Esta configuración puede provocar un comportamiento inesperado adicional además de los errores enumerados anteriormente. La autenticación basada en certificados presenta una tarjeta inteligente virtual en el sistema operativo de la instancia y la elimina una vez finalizado el inicio de sesión. Compruebe la Configuración de la política de grupo principal para las tarjetas y Configuración adicional de la política de grupo para tarjetas inteligentes y claves de registro, incluido el comportamiento de eliminación de las tarjetas inteligentes.
- El punto de distribución de la CRL de la CA privada no está en línea ni se puede acceder a él desde el controlador de WorkSpaces dominio. Para obtener más información, consulte el paso 5 de Requisitos previos.
- Para comprobar si hay alguna CA obsoleta en el dominio o el bosque, ejecute `PKIVIEW.msc` la CA para verificarla. Si hay CA obsoletas, utilice el `PKIVIEW.msc` mmc para eliminarlas manualmente.
- Para comprobar si la replicación de Active Directory funciona y si no hay controladores de dominio obsoletos en el dominio, ejecute. `repadmin /replsum`

Los pasos adicionales de solución de problemas incluyen revisar los registros de eventos de Windows de la WorkSpaces instancia. Uno de los eventos más comunes de fallo de inicio de sesión es el Evento 4625: No se pudo iniciar sesión con una cuenta en el registro de seguridad de Windows.

Si el problema persiste, póngase en contacto con AWS Support. Para obtener más información, consulte el Centro de AWS Support.

Estoy intentando hacer algo que requiere un medio de instalación de Windows, pero WorkSpaces no lo proporciona.

Si utiliza un paquete público AWS proporcionado, puede utilizar las instantáneas de EBS de los medios de instalación del sistema operativo Windows Server proporcionadas por Amazon EC2 cuando las necesite.

Cree un volumen de EBS a partir de estas instantáneas, adjúntelo a Amazon EC2 y transfiera los archivos a donde están los archivos WorkSpace según sea necesario. Si utiliza Windows 10 con

BYOL activado WorkSpaces y necesita un medio de instalación, tendrá que preparar su propio medio de instalación. Para obtener más información, consulte Añadir componentes de Windows mediante medios de instalación. Como no puede adjuntar directamente un volumen de EBS a un WorkSpace, tendrá que adjuntarlo a una instancia de Amazon EC2 y copiar los archivos.

Quiero lanzarlo WorkSpaces con un directorio AWS gestionado existente creado en una región no WorkSpaces compatible.

Para lanzar Amazon WorkSpaces con un directorio en una región que actualmente no es compatible con WorkSpaces, sigue los pasos que se indican a continuación.

> **Note**
>
> Si recibes errores al ejecutar AWS Command Line Interface comandos, asegúrate de usar la AWS CLI versión más reciente. Para obtener más información, consulte Confirme que está ejecutando una versión reciente de la AWS CLI.

Paso 1: crear conexiones de nube privada virtual (VPC) con otra VPC de su cuenta

1. Cree una conexión de emparejamiento de VPC con una VPC de una región diferente: Para obtener más información, consulte Crear con VPC en la misma cuenta y en diferentes regiones.
2. Acepte la conexión de emparejamiento de VPC. Para obtener más información, consulte Creación y aceptación de conexiones de emparejamiento de VPC.
3. Después de activar la conexión de emparejamiento de VPC, puede ver sus conexiones de emparejamiento de VPC mediante la consola de Amazon VPC, la o una API. AWS CLI

Paso 2: actualizar las tablas de enrutamiento para la conexión de emparejamiento de VPC en ambas regiones

Actualice las tablas de enrutamiento para activar la comunicación con la VPC homóloga a través de IPv4 o IPv6. Para obtener más información, consulte Actualización de las tablas de ruteo para conexiones de emparejamiento de VPC

Paso 3: Crea un AD Connector y registra Amazon WorkSpaces

1. Para consultar los requisitos previos del Conector AD, consulte Requisitos previos del Conector AD.

2. Conecte su directorio actual con Conector AD. Para obtener más información, consulte Creación de un Conector AD.
3. Cuando el estado del Connector AD cambie a Activo, abra la consola de AWS Directory Service y, a continuación, elija el hipervínculo para su ID de directorio.
4. Para AWS aplicaciones y servicios, elige Amazon WorkSpaces para activar el acceso WorkSpaces a este directorio.
5. Registra el directorio con WorkSpaces. Para obtener más información, consulte Registrar un directorio en WorkSpaces.

Quiero actualizar Firefox en Amazon Linux 2.

Paso 1: comprobar que la actualización automática esté habilitada

Para comprobar que la actualización automática está habilitada, ejecute el comando `systemctl status *os-update-mgmt.timer | grep enabled` en su. WorkSpace En el resultado, debe haber dos líneas con la palabra `enabled` en ellas.

Paso 2: iniciar una actualización

Firefox normalmente se actualiza automáticamente en Amazon Linux 2 WorkSpaces junto con todos los demás paquetes de software del sistema durante el período de mantenimiento. Sin embargo, esto depende del tipo WorkSpaces que utilices.

- Pues AlwaysOn WorkSpaces, el período de mantenimiento semanal es los domingos de 00h00 a 04h00, en la zona horaria del. WorkSpace
- Para AutoStop WorkSpaces. A partir del tercer lunes del mes y durante un máximo de dos semanas, el período de mantenimiento estará abierto todos los días entre las 00h00 y las 05h00, en la zona horaria de la región correspondiente al. AWS WorkSpace

Para obtener más información sobre los períodos de mantenimiento, consulte mantenimiento. WorkSpace

También puede iniciar un ciclo de actualización inmediato reiniciándolo WorkSpace y volviéndolo a conectar después de 15 minutos. También puede iniciar las actualizaciones ingresando `sudo yum update`. Para iniciar una actualización solo para Firefox, ingresa `sudo yum install firefox`.

Si no puede configurar el acceso a los repositorios de Amazon Linux 2 y prefiere instalar Firefox con archivos binarios creados por Mozilla, consulte Instalar Firefox desde versiones de Mozilla en el Centro de soporte de Mozilla. Te recomendamos que desinstales por completo la versión de Firefox empaquetada con RPM para asegurarte de no ejecutar una versión desactualizada por error. Para desinstalarla, ejecuta el comando `sudo yum remove firefox`.

También puede descargar los paquetes RPM necesarios de los repositorios de Amazon Linux 2 ejecutando el comando `yumdownloader firefox` en otra máquina. Luego, carga lateralmente los repositorios WorkSpaces, donde podrás instalarlos con un comando estándar como. YUM `sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`

> **Note**
>
> El nombre exacto del archivo cambiará en función de la versión del paquete.

Paso 3: comprobar que se esté utilizando el repositorio de Firefox

Amazon Linux Extras proporciona automáticamente actualizaciones de Firefox para Amazon Linux 2 WorkSpaces. Amazon Linux 2 WorkSpaces creado después del 31 de julio de 2023 ya tendrá activado el repositorio Firefox Extra. Para comprobar que WorkSpace está utilizando el repositorio Firefox Extra, ejecute el siguiente comando.

```
yum repolist | grep amzn2extra-firefox
```

El resultado del comando debería tener el mismo aspecto que `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10` si se utiliza el repositorio Firefox Extra. Estará vacío si no se utiliza el repositorio Extra de Firefox. Si no se utiliza el repositorio Firefox Extra, puedes intentar habilitarlo manualmente con el siguiente comando:

```
sudo amazon-linux-extras install firefox
```

Si la activación del repositorio de Firefox Extra sigue fallando, comprueba tu acceso a Internet y asegúrate de que los puntos finales de la VPC no estén configurados. Para seguir recibiendo actualizaciones de Firefox para Amazon Linux 2 WorkSpaces a través de los repositorios de YUM, asegúrese de poder acceder a WorkSpaces los repositorios de Amazon Linux 2. Para obtener más información sobre cómo acceder a los repositorios de Amazon Linux 2 sin acceso a Internet, consulte este artículo del centro de conocimiento.

Mi usuario puede restablecer su contraseña mediante el WorkSpaces cliente, ignorando la configuración de la Política de contraseñas detallada (FFGP) que está configurada. AWS Managed Microsoft AD

Si el WorkSpaces cliente de tu usuario está asociado a AWS Managed Microsoft AD, tendrá que restablecer su contraseña con la configuración de complejidad predeterminada.

La contraseña de complejidad predeterminada distingue mayúsculas de minúsculas y debe tener entre 8 y 64 caracteres, ambos inclusive. Debe contener al menos un carácter de cada una de las siguientes categorías:

- Caracteres en minúsculas (a-z)
- Caracteres en mayúsculas (a-z)
- Números (0-9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Asegúrese de que la contraseña no incluya caracteres Unicode que no se puedan imprimir, como espacios en blanco, tabulaciones con forma de carruaje, saltos de línea y caracteres nulos.

Si su organización requiere que utilice el FFGP WorkSpaces, póngase en contacto con el administrador de Active Directory para restablecer la contraseña de usuario directamente desde Active Directory y no desde el cliente. WorkSpaces

Mis usuarios reciben el mensaje de error «Este sistema operativo/plataforma no está autorizado a acceder a su WorkSpace» cuando intentan acceder a WorkSpace Windows/Linux mediante Web Access

La versión del sistema operativo que el usuario intenta utilizar no es compatible con WorkSpaces Web Access. Asegúrese de habilitar el acceso web en la configuración Otra plataforma del WorkSpace directorio. Para obtener más información sobre cómo habilitar su acceso a WorkSpace la web, consulteHabilitar y configurar Amazon WorkSpaces Web Access.

Política de fin de vida de las aplicaciones cliente de Amazon WorkSpaces

La política de fin de vida útil (EOL) de Amazon WorkSpaces se aplica a versiones principales específicas (y a todas sus versiones secundarias) de WorkSpaces que ya no reciben soporte y cuya compatibilidad con las versiones más recientes ya no se ha sometido a pruebas.

El ciclo de vida de una versión de cliente de WorkSpaces consta de tres fases: soporte general, orientación técnica y fin de vida útil (EOL). La fase de soporte general comienza en la fecha del lanzamiento público inicial de un cliente de WorkSpaces y dura un tiempo determinado. Durante la fase de soporte general, el equipo de soporte de WorkSpaces ofrece soporte completo para los problemas de configuración. Las resoluciones de defectos y las solicitudes de funciones se implementan para esa versión principal y las versiones secundarias asociadas del cliente de WorkSpaces.

La orientación técnica se proporciona desde el final de la fase de soporte general hasta la fecha de fin de vida. Durante la fase de orientación técnica, recibirá asistencia y orientación únicamente para las configuraciones compatibles. Las resoluciones de defectos y las solicitudes de características se implementan únicamente para las versiones más recientes únicamente del cliente de WorkSpaces. No se implementan para las versiones más antiguas. Durante la fase de orientación técnica, si es necesaria una corrección, AWS programará para la próxima versión disponible públicamente y tendrá la opción de actualizar a la versión más reciente de WorkSpaces para recibir asistencia relacionada con la corrección.

La EOL de una versión principal se produce cuando han finalizado el soporte general y la orientación técnica. Después de la fecha de fin de vida, no se proporciona ningún otro tipo de soporte o mantenimiento. AWS detiene las pruebas para detectar problemas de compatibilidad. Para obtener soporte continuo, debe actualizar a la última versión del cliente de WorkSpaces.

Consulte esta tabla para obtener más información acerca de la compatibilidad con versiones específicas.

Cliente de Windows	Soporte general	Orientación técnica	EOL
2.x	2018	31 de marzo de 2023	31 de agosto de 2023

Cliente de Linux	Soporte general	Orientación técnica	EOL
4.x para Ubuntu 18.04	12 de agosto de 2021	31 de marzo de 2023	31 de agosto de 2023
3.x para Ubuntu 18.04	25 de noviembre de 2019	31 de marzo de 2023	31 de agosto de 2023

Cliente para macOS	Soporte general	Orientación técnica	EOL
2.x	2019	31 de marzo de 2023	31 de agosto de 2023
1.x	2018	31 de marzo de 2023	31 de agosto de 2023

Cliente para iPad	Soporte general	Orientación técnica	EOL
1.x	2018	31 de marzo de 2023	31 de agosto de 2023

Cliente de Android	Soporte general	Orientación técnica	EOL
2.x	2019	31 de marzo de 2023	31 de agosto de 2023
1.x	2018	31 de marzo de 2023	31 de agosto de 2023

Acceso web	Soporte general		
Google Chrome	Versión actual, más las dos versiones principales más recientes		
Firefox	Versión actual, más las dos versiones		

Acceso web	Soporte general		
	principales más recientes		
Microsoft Edge	Versión actual, más las dos versiones principales más recientes		

Clientes no compatibles

Los siguientes clientes de WorkSpaces no son compatibles.

Sistema operativo	Versión del cliente	Soporte general	Orientación técnica	EOL	Notas
Windows	5.11	3 de julio de 2023	1 de octubre de 2023	1 de octubre de 2023	No se admite debido a problemas de calidad
Windows	5.10	19 de junio de 2023	1 de octubre de 2023	1 de octubre de 2023	No se admite debido a problemas de calidad
Windows	5.9	9 de mayo de 2023	1 de octubre de 2023	1 de octubre de 2023	No se admite debido a problemas de calidad

Preguntas frecuentes sobre la EOL

Estoy usando una versión de un cliente de WorkSpaces que ha alcanzado la EOL. ¿Qué debo hacer para actualizar a una versión compatible?

Vaya a la página de descargas del cliente de WorkSpaces para descargar e instalar una versión totalmente compatible de WorkSpaces.

¿Puedo usar una versión del cliente de WorkSpaces que haya alcanzado su fin de vida con un WorkSpace compatible?

Recomendamos encarecidamente que actualicen sus clientes a la última versión, ya que las resoluciones y funciones anteriores ya no se aplican a las versiones de los clientes que han alcanzado su EOL. Si utiliza una versión de cliente que ha alcanzado su fin de vida útil, póngase en contacto con el equipo de soporte AWS para obtener más información.

Estoy usando una versión de un cliente de WorkSpaces que ha alcanzado la EOL. ¿Puedo seguir denunciando problemas al respecto?

Primero debes actualizar a una versión compatible e intentar reproducir el problema. Si el problema persiste en la versión compatible, abra un caso de soporte con el equipo de soporte de AWS.

Utilizo una versión de cliente de WorkSpaces compatible en un sistema operativo que ha alcanzado su fin de vida. ¿Puedo seguir denunciando problemas al respecto?

La asistencia técnica y las actualizaciones de software ya no están disponibles para los sistemas operativos que han alcanzado su fin de vida y AWS no proporcionan soporte a los clientes de WorkSpaces que utilizan sistemas operativos que han alcanzado su fin de vida. Utilice un sistema operativo compatible para garantizar la compatibilidad con sus clientes de WorkSpaces.

WorkSpaces Cuotas de Amazon

Amazon WorkSpaces proporciona diferentes recursos que puedes usar en tu cuenta en una región determinada, como imágenes WorkSpaces, paquetes, directorios, alias de conexión y grupos de control de IP. Cuando cree su cuenta de Amazon Web Services, estableceremos unas cuotas predeterminadas (también denominadas «límites») para el número de recursos que puede crear.

Las siguientes son las cuotas predeterminadas de tu WorkSpaces cuenta. AWS Puede utilizar la consola de Service Quotas para consultar las cuotas predeterminadas y solicitar aumentos de cuota para las cuotas ajustables.

En algunas regiones, donde Service Quotas no está disponible, debe presentar un caso de asistencia para solicitar un aumento del límite. Para obtener más información, consulte Ver una cuota de servicio y Solicitud de aumento de cuota en la Guía del usuario de Service Quotas.

Resource	Predeterminado	Descripción	Ajustable
WorkSpaces	1	El número máximo de WorkSpaces personas en esta cuenta en la región actual.	Sí
Gráficos WorkSpaces	0	El número máximo de gráficos WorkSpaces de esta cuenta en la región actual. **Note** El paquete de Graphics dejará de ser compatible a partir del 30 de noviembre de 2023. Te	Sí

Resource	Predeterminado	Descripción	Ajustable
		recomendamos migrar tu paquete WorkSpaces a Graphics.G4DN. Para obtener más información, consulte Migrar un WorkSpace.	
Gráficos. G4DN WorkSpaces	0	El número máximo de WorkSpaces Graphics.g4dn en esta cuenta en la región actual.	Sí
GraphicsPro WorkSpaces	0	El número máximo de GraphicsPro WorkSpaces en esta cuenta en la región actual.	Sí
GraphicsPro.g4dn WorkSpaces	0	El número máximo de GraphicsPro .g4dn WorkSpaces en esta cuenta en la región actual.	Sí
En espera WorkSpaces	0	El número máximo de WorkSpaces en esta cuenta en la región actual.	Sí

Resource	Predeterminado	Descripción	Ajustable
Paquetes	50	Número máximo de paquetes de esta cuenta en la región actual. Esta cuota se aplica solo a las agrupaciones personalizadas, no a los paquetes públicos.	No
Alias de conexión	20	Número máximo de alias de conexión de esta cuenta en la región actual.	No
Directorios	50	El número máximo de directorios que se pueden registrar para su uso con Amazon WorkSpaces en esta cuenta en la región actual.	No
Imágenes	40	Número máximo de imágenes de esta cuenta en la región actual.	Sí
Grupos de control de acceso a direcciones IP	100	Número máximo de grupos de control de acceso a IP para esta cuenta en la región actual.	No

Resource	Predeterminado	Descripción	Ajustable
Grupos de control de acceso a direcciones IP por directorio	25	El número máximo de grupos de control de acceso a direcciones IP por directorio en esta cuenta en la región actual.	No
Reglas por grupo de control de acceso a direcciones IP	10	El número máximo de reglas por grupo de control de acceso de IP en esta cuenta en la región actual.	No

Limitación de la API

La tarifa permitida es de dos llamadas por segundo. Para obtener más información, consulte Excepciones de limitación.

WorkSpaces Versiones del agente anfitrión del Streaming Protocol (WSP)

El agente host del WorkSpaces Streaming Protocol (WSP) es un agente host que se ejecuta dentro de su. WorkSpace Transmite sus píxeles WorkSpace a una aplicación cliente e incluye funciones integradas en la sesión, como el audio y el vídeo bidireccionales y la impresión. Para obtener más información sobre el Protocolo de WorkSpaces transmisión (WSP), consulte Protocols for Amazon WorkSpaces.

Le recomendamos que mantenga el software de su agente de host actualizado con la última versión. Puede reiniciarlo manualmente WorkSpaces para actualizar el agente anfitrión del WSP. El agente anfitrión de WSP también se actualiza automáticamente durante el período de mantenimiento WorkSpaces predeterminado habitual. Para obtener más información sobre las ventanas de mantenimiento, consulte WorkSpace mantenimiento. Algunas de estas funciones requieren la última versión WorkSpaces del cliente. Para obtener más información sobre las versiones más recientes de los clientes, consulte WorkSpaces Clientes.

En la siguiente tabla se describen los cambios de cada versión del agente de host de WSP.

Release	Date	Cambios
• Windows WorkSpaces : 2.1.0.1554	15 de mayo de 2024	• Se agregó soporte para el tiempo de espera de desconexión por inactividad. • Se agregó una nueva configura ción de política de grupo para configurar el tiempo de espera de desconexión por inactividad. • Se ha corregido un error que WorkSpaces provocaba que se desconectara y se mostrara una pantalla blanca cuando los usuarios modificaban la configura ción de pantalla.

Release	Date	Cambios
		• Correcciones de errores y mejoras de rendimiento.
• Ubuntu WorkSpaces : 2.1.0.1342	29 de febrero de 2024	• Se cambió la resolución preferida de la cámara web a entre 480 x 360 y 640 x 480. • Correcciones de errores y mejoras de rendimiento.
• WorkSpaces Windows: 2.0.0.1425	22 de febrero de 2024	• Se ha añadido compatibilidad con las solicitudes de WebAuthn redireccionamiento durante la sesión desde aplicaciones web que se ejecutan en navegador es remotos de Google Chrome o Microsoft Edge. Esta función añade un mensaje de navegador único que solicita al usuario que habilite la extensión de redirecci onamiento DCV WebAuthn . Solo es compatible con Windows WorkSpaces y clientes WorkSpace s nativos. • Se ha corregido un error que provocaba que a veces apareciera una pantalla blanca o congelada al iniciar sesión. • Correcciones de errores y mejoras de rendimiento.

Release	Date	Cambios
• Windows WorkSpaces : 2.0.0.1304	11 de enero de 2024	• Se ha corregido un error relacionado con posibles bloqueos de la transmisión durante el inicio de sesión. • Se ha corregido un error relacionado con el registro.
• Windows: 2.0.0.1288 WorkSpaces	16 de noviembre de 2023	• Se agregó compatibilidad con el controlador de pantalla indirecta (IDD) en Windows 10+, lo que reduce el consumo de CPU y mejora el rendimiento de la transmisión. • Se agregó una nueva configuración de política de grupo para habilitar o deshabilitar el controlador IDD. • Se corrigieron errores relacionados con la transparencia de la imagen del portapapeles. • Se corrigieron errores que preservaban los factores de escala de Windows. • Correcciones de errores y mejoras de rendimiento.

Release	Date	Cambios
• Windows WorkSpaces : 2.0.0.1164	13 de octubre de 2023	• Se agregó compatibilidad para VSync en el controlador de pantalla virtual. • Se agregó una nueva configuración de política de grupo para habilitar o deshabilitar VSync. • Se han mejorado los problemas de reconexión y fiabilidad. • Correcciones de errores y mejoras de rendimiento.
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces : 2.1.0.1086	18 de agosto de 2023	• Se agregó una nueva configuración para habilitar o deshabilitar el redireccionamiento de zona horaria. • Se extendió el tiempo de espera de inicio de sesión y se agregó una opción de configuración. • Puerta de enlace mejorada para permitir reconexiones más rápidas después de una interrupción. • Correcciones de errores y mejoras de rendimiento.

Release	Date	Cambios
• Amazon Linux WorkSpaces - 2.0.0.907	30 de junio de 2023	• Se agregó compatibilidad con el SDK de extensiones de DCV para permitir integraciones específicas de los ISV. • Se ha modificado el comportamiento de desconexión para que al cerrar sesión se termine la sesión del usuario. • Se ha agregado compatibilidad con el redireccionamiento de zonas horarias. • Se extendió el tiempo de espera de inicio de sesión y se agregó una opción de configuración. • Se han corregido problemas de actualización. • Correcciones de errores y mejoras de rendimiento.
• Windows: 2.0.0.829 WorkSpaces	8 de junio de 2023	• Se modificó el comportamiento de desconexión para que al cerrar sesión se termine la sesión del usuario. • Se corrigieron errores relacionados con la sincronización A/V y los teclados japoneses. • Se ha mejorado la fiabilidad del instalador de WSP.

Release	Date	Cambios
• Ubuntu: 2.1.0.829 WorkSpaces	16 de mayo de 2023	• Se modificó el comportamiento de desconexión para que al cerrar sesión se termine la sesión del usuario. • Se agregó compatibilidad con el SDK de extensiones de DCV para permitir integraciones específicas de los ISV. • Se ha agregado compatibilidad con el redireccionamiento de zonas horarias. • Se han corregido problemas de actualización.

Release	Date	Cambios
• Windows: 2.0.0.799 WorkSpaces	8 de mayo de 2023	• Transporte QUIC mejorado basado en UDP con varias optimizaciones de calidad y rendimiento de imagen. • Se agregó compatibilidad con el SDK de extensiones de DCV para permitir integraciones específicas de los ISV. • Se agregaron nuevas configuraciones de políticas de grupo para habilitar o deshabilitar el SDK de extensiones. • Diseños de teclado mejorados en coreano, japonés y alemán. • Se corrigieron errores relacionados con la congelación de sesiones, la aceleración del hardware, el redireccionamiento de la impresora, el detalle de los registros y la configuración de la política de grupo en target-fps.

Note

- Para obtener información sobre cómo comprobar la versión de su agente de host, consulte ¿Qué sistemas operativos de cliente y host son compatibles con la última versión de WSP?.
- Para obtener información sobre cómo actualizar la versión del agente anfitrión, consulte Si ya tengo un WSP WorkSpace, ¿cómo lo actualizo? .
- Para ver las notas de publicación de la versión del cliente macOS de WSP, consulte las notas de la versión en la sección de aplicaciones cliente WorkSpaces macOS de la Guía del WorkSpaces usuario.

- Para ver las notas de lanzamiento de la versión de cliente de Windows de WSP, consulte las notas de la versión en la sección de aplicaciones cliente de WorkSpaces Windows de la Guía del WorkSpaces usuario.

Extensión SDK compatible con WSP

Amazon WorkSpaces Streaming Protocol (WSP) se basa en la tecnología NICE DCV, que permite el acceso remoto de alto rendimiento a las instancias de WorkSpaces para una amplia gama de cargas de trabajo y casos de uso. Con la extensión NICE DCV del SDK, los desarrolladores pueden personalizar la experiencia de WSP WorkSpaces para los usuarios finales, incluyendo:

- Facilitar el soporte de hardware personalizado.
- Mejorar la usabilidad de aplicaciones de terceros en sesiones remotas. Por ejemplo, añadiendo una terminación de audio local para aplicaciones VoIP o una reproducción de vídeo local para aplicaciones de conferencias.
- Proporcionar al software de accesibilidad, como los lectores de pantalla, información sobre la sesión remota y las aplicaciones que se ejecutan de forma remota.
- Permitir que el software de seguridad analice el nivel de seguridad del punto de conexión local para permitir políticas de acceso condicional.
- Realizar transferencias de datos arbitrarias a través de una sesión remota establecida.

Para empezar a utilizar la extensión NICE DCV del SDK, consulte la documentación de la extensión NICE DCV del SDK. Puede encontrar el propio SDK en el repositorio GitHub de la extensión NICE DCV del SDK. Además, también puede encontrar ejemplos de integración del SDK en el repositorio GitHub de muestras de la extensión NICE del SDK de DCV.

Los siguientes son compatibles con WorkSpaces.

- Protocolo de transmisión: WorkSpaces Streaming Protocol (WSP)
- Cliente de WorkSpaces para Windows: 5.9.0.4110 y versiones superiores.

> **Note**
>
> Los clientes de WorkSpaces para Android, iOS y el acceso web no son compatibles con la extensión NICE DCV del SDK.

- WorkSpaces es compatible con: servidores Windows, Linux y Ubuntu.

Historial de documentos para WorkSpaces

La siguiente tabla describe los cambios importantes en el servicio WorkSpaces y en la Guía de administración de Amazon WorkSpaces a partir del 1 de enero de 2018. Actualizamos la documentación con frecuencia para dar cuenta de los comentarios que nos envía.

Para recibir notificaciones sobre estas actualizaciones, puede suscribirse al canal RSS de WorkSpaces.

Cambio	Descripción	Fecha
Actualización de la política administrada de AmazonWorkSpacesAdmin	WorkSpaces ha añadido la acción workspaces:RestoreWorkspace a la política administrada AmazonWorkSpacesAdmin, concediendo a los administradores acceso para restaurar WorkSpaces.	17 de julio de 2023
Extensión SDK compatible con WSP	Con la extensión NICE DCV del SDK, los desarrolladores pueden personalizar la experiencia de WSP WorkSpaces para los usuarios finales.	25 de mayo de 2023
Versiones del agente de host de WorkSpaces Streaming Protocol (WSP)	Información sobre la versión del WorkSpaces Streaming Protocol (WSP).	8 de mayo de 2023
Lanzamiento de Amazon WorkSpaces en AWS GovCloud (Este de EE. UU.)	Amazon WorkSpaces está disponible en AWS (Este de EE. UU.)	3 de mayo de 2023
Compatibilidad con la cámara web de Amazon WorkSpaces	Amazon WorkSpaces ahora admite audio y vídeo (AV) en tiempo real al redirigir sin	5 de abril de 2021

	problemas la entrada de vídeo de la cámara web local a los escritorios de Windows WorkSpaces mediante el protocolo WorkSpaces Streaming Protocol (WSP).	
Compatibilidad de las tarjetas inteligentes de Amazon WorkSpaces con la aplicación cliente WorkSpaces para macOS	Ahora puede utilizar la aplicación cliente Amazon WorkSpaces para macOS con tarjetas inteligentes Common Access Card (CAC) y personal Identity Verification (PIV). El soporte de tarjetas inteligentes está disponible en WorkSpaces utilizando el WorkSpaces Streaming Protocol (WSP).	5 de abril de 2021
API de administración de paquetes de Amazon WorkSpaces	Ya están disponibles las API de administración de paquetes de Amazon WorkSpaces. Estas acciones de la API admiten operaciones de creación, eliminación y asociación de imágenes para paquetes de WorkSpaces.	15 de marzo de 2021
Lanzamiento de Amazon WorkSpaces en Asia-Pacífico (Bombay)	Amazon WorkSpaces está disponible en la región de Asia-Pacífico (Bombay)	8 de marzo de 2021

WorkSpaces Streaming Protocol (WSP)	El WorkSpaces Streaming Protocol (WSP) ya está disponible tanto para los WorkSpaces con licencia incluida (Windows Server 2016) como para los WorkSpaces basados en Windows 10 basados en BYOL en todos los tipos de paquetes, excepto en Graphics y GraphicsPro. WSP también está disponibl e para Linux WorkSpaces en la región de AWS GovCloud (EE.UU.-Oeste).	1 de diciembre de 2020
Tarjetas inteligentes	Amazon WorkSpaces ahora admite la autenticación con tarjeta inteligente previa a la sesión (inicio de sesión) y durante la sesión en WorkSpaces para Windows y Linux en la región de AWS GovCloud (EE.UU.-Oeste).	1 de diciembre de 2020
Compartir imágenes personali zadas	Puede compartir imágenes de WorkSpaces personalizadas entre cuentas de AWS. La cuenta del destinatario puede copiarla y utilizarla para crear paquetes para lanzar nuevos WorkSpaces.	1 de octubre de 2020

Redireccionamiento entre regiones	Ahora puede usar el redirecci onamiento entre regiones, una característica que funciona con las políticas de enrutamie nto del sistema de nombres de dominio (DNS) para redirigir a los usuarios a escritorios de WorkSpaces alternativos cuando sus WorkSpaces principales no estén disponibl es.	10 de septiembre de 2020
Suscríbase a Microsoft Office 2016 o 2019 para WorkSpace s BYOL	Ya puede suscribirse a Microsoft Office Professional 2016 o 2019 proporcionado por AWS en los WorkSpaces de Traiga su propia licencia de Windows (BYOL).	3 de septiembre de 2020
Automatización BYOL en China (Ningxia)	Puede utilizar la automatiz ación de traiga su propia licencia (BYOL) para simplific ar el proceso de uso de sus licencias de escritorio de Windows 10 para sus WorkSpaces en China (Ningxia).	2 de abril de 2020

Comprobador de imágenes	La herramienta Comprobador de imágenes le ayuda a determinar si su Windows WorkSpace cumple los requisitos para la creación de imágenes. El comprobador de imágenes realiza una serie de pruebas en el escritorio de WorkSpaces que desea utilizar para crear la imagen y proporciona orientación sobre cómo resolver cualquier problema que encuentre.	30 de marzo de 2020
Migrar WorkSpaces	La característica de migración de Amazon WorkSpaces le permite migrar un WorkSpace de un paquete a otro, conservando al mismo tiempo los datos del volumen de usuario. Puede utilizar esta característica para migrar WorkSpaces desde la experiencia de escritorio de Windows 7 a la de Windows 10. También puede utilizar esta característica para migrar WorkSpaces de un paquete público o personalizado a otro.	9 de enero de 2020

Integración de PrivateLink para las API de Amazon WorkSpaces	Puede conectarse directamente a los puntos de conexión de la API de Amazon WorkSpaces a través de un punto de conexión de interfaz en su nube privada virtual (VPC) en lugar de conectarse a través de Internet. Cuando utiliza un punto de conexión de interfaz de VPC, la comunicación entre su VPC y el punto de conexión de la API de Amazon WorkSpaces se realiza de forma completa y segura dentro de la red de AWS.	25 de noviembre de 2019
Cliente Linux para Amazon WorkSpaces	Los usuarios pueden usar ahora el cliente Linux para obtener acceso a sus escritorios de WorkSpaces.	25 de noviembre de 2019
Lanzamiento de Amazon WorkSpaces en China (Ningxia)	Amazon WorkSpaces está disponible en la región de China (Ningxia).	13 de noviembre de 2019
Restaurar WorkSpaces al último estado correcto conocido	Puede utilizar la característica de restauración para revertir un WorkSpace a su último estado correcto conocido.	18 de septiembre de 2019

Cifrado de puntos de conexión de FIPS	Para cumplir con el Programa federal de administración de riesgos y autorizaciones (FedRAMP) o la Guía de requisitos de seguridad de computación en la nube (SRG) del departamento de defensa (DoD), puede configurar Amazon WorkSpaces para que utilice el cifrado de punto de conexión de las Normas federales de procesamiento de la información (FIPS) en el nivel de directorio.	12 de septiembre de 2019
Copiar imágenes de WorkSpaces	Puede copiar las imágenes dentro de la misma región o en otras regiones.	27 de junio de 2019
Capacidades de gestión de WorkSpace de autoservicio para usuarios	Puede habilitar capacidad es de gestión de WorkSpace de autoservicio para sus usuarios, a fin de que les proporcionen un mayor control sobre su experiencia.	19 de noviembre de 2018
Automation de BYOL	Puede usar la automatización de Bring-Your-Own-License (BYOL) para simplificar el proceso de utilización de las licencias de escritorio de Windows 7 y Windows 10 para sus WorkSpaces.	16 de noviembre de 2018
Grupos de PowerPro y GraphicsPro	Los paquetes PowerPro y GraphicsPro ya están disponibles para WorkSpaces.	18 de octubre de 2018

Monitorizar los inicios de sesión correctos de WorkSpace	Puede usar eventos de Amazon CloudWatch Events para monitorizar los inicios de sesión correctos de WorkSpace y responder a ellos.	17 de septiembre de 2018
Acceso web para WorkSpaces para Windows 10	Ahora los usuarios pueden utilizar el cliente Acceso web para acceder a un WorkSpace con las versiones para escritorio de Windows 10.	24 de agosto de 2018
Inicio de sesión con URI	Puede utilizar identificadores uniformes de recursos (URI) para proporcionar a los usuarios acceso a sus WorkSpaces.	31 de julio de 2018
WorkSpaces de Amazon Linux	Puede aprovisionar WorkSpaces de Amazon Linux para sus usuarios.	26 de junio de 2018
Grupos de control de acceso a direcciones IP	Puede controlar las direcciones IP desde las que los usuarios tienen acceso a sus escritorios de WorkSpaces.	30 de abril de 2018
Actualizaciones locales	Puede actualizar sus escritorios de WorkSpaces BYOL de Windows 10 a una versión más reciente de Windows 10.	9 de marzo de 2018

Actualizaciones anteriores

En la tabla siguiente se describen los cambios importantes realizados en el servicio Amazon WorkSpaces y en su documentación antes del 1 de enero de 2018.

Cambio	Descripción	Fecha
Opciones de computación flexibles	Puede cambiar sus escritorios de WorkSpaces entre los paquetes Value, Standard, Performance y Power	22 de diciembre de 2017
Almacenamiento configurable	Puede configurar el tamaño de los volúmenes raíz y de usuario de sus escritorios de WorkSpaces cuando los lance y aumentar el tamaño de estos volúmenes más adelante.	22 de diciembre de 2017
Controlar el acceso de los dispositivos	Puede especificar los tipos de dispositivos que tienen acceso a WorkSpaces. Además puede limitar el acceso a WorkSpaces a los dispositivos de confianza (también conocidos como dispositivos administrados).	19 de junio de 2017
Confianzas entre bosques	Puede establecer una relación de confianza entre su AWS Managed Microsoft AD y el dominio local de Microsoft Active Directory y aprovisionar después WorkSpaces para los usuarios en el dominio local.	9 de febrero de 2017
Paquetes de Windows Server 2016	WorkSpaces ofrece paquetes con tecnología Windows Server 2016 que incluyen una experiencia de escritorio de Windows 10.	29 de noviembre de 2016
Acceso web	Puede acceder a los WorkSpaces para Windows desde un navegador web utilizando el acceso web a WorkSpaces.	18 de noviembre de 2016
WorkSpaces por horas	Puede configurar los espacios de trabajo para que la facturación se realice por horas.	18 de agosto de 2016
BYOL de Windows 10	Puede traer su licencia de escritorio de Windows 10 a WorkSpaces (BYOL).	21 de julio de 2016

Cambio	Descripción	Fecha
Compatibilidad del etiquetado	Puede usar etiquetas para administrar y controlar los WorkSpaces.	17 de mayo de 2016
Registros guardados	Cada vez que introduce un nuevo código de registro, el cliente de WorkSpaces lo guarda. De este modo, resulta más sencillo cambiar entre espacios de trabajo de diferentes directorios o regiones.	28 de enero de 2016
BYOL de Windows 7, cliente de Chromebook y cifrado de WorkSpaces	Puede traer su licencia de escritorio de Windows 7 a WorkSpaces (BYOL), ,utilizar el cliente Chromebook y utilizar el cifrado de WorkSpace.	1 de octubre de 2015
Monitoreo de CloudWatch	Se ha añadido información sobre el monitoreo de CloudWatch.	28 de abril de 2015
Reconexión automática de sesiones	Se ha añadido información sobre la característica de reconexión automática de sesiones en las aplicaciones cliente de escritorio de WorkSpaces.	31 de marzo de 2015
Direcciones IP públicas	Puede asignar automáticamente una dirección IP pública a sus WorkSpaces.	23 de enero de 2015
Lanzamiento de WorkSpaces en Asia-Pacífico (Singapur)	WorkSpaces está disponible en la región Asia-Pacífico (Singapur).	15 de enero de 2015
Se ha añadido el paquete Value, se ha actualizado el paquete Standard y se ha agregado Office 2013	El paquete Value está disponible, el hardware del paquete Standard se ha actualizado y Microsoft Office 2013 está disponible en los paquetes Plus.	6 de noviembre de 2014
Compatibilidad con imágenes y paquetes	Puede crear una imagen de un WorkSpace que haya personalizado y, a continuación, crear un paquete personalizado del WorkSpace a partir de la imagen.	28 de octubre de 2014

Cambio	Descripción	Fecha
Compatibilidad con el cliente cero PCoIP	Puede obtener acceso a los dispositivos de cliente cero PCoIP de WorkSpaces.	15 de octubre de 2014
Lanzamiento de WorkSpaces en Asia-Pacífico (Tokio)	WorkSpaces está disponible en la región de Asia-Pacífico (Tokio).	26 de agosto de 2014
Compatibilidad con impresoras locales	Puede habilitar la compatibilidad con las impresoras locales en los WorkSpaces.	26 de agosto de 2014
Autenticación multifactor	Puede utilizar la autenticación multifactor en los directorios conectados.	11 de agosto de 2014
Compatibilidad con OU predeterminadas y con el dominio de destino	Puede seleccionar una unidad organizativa (OU) predeterminada en la que se ubiquen las cuentas de equipo de los WorkSpace y un dominio independiente en el que se creen dichas cuentas.	7 de julio de 2014
Añadir grupos de seguridad	Puede añadir un grupo de seguridad a sus instancias de WorkSpaces.	7 de julio de 2014
Lanzamiento de WorkSpaces en Asia-Pacífico (Sídney)	WorkSpaces está disponible en la región de Asia-Pacífico (Sídney).	15 de mayo de 2014
Lanzamiento de WorkSpaces en Europa (Irlanda)	WorkSpaces está disponible en la región de Europa (Irlanda).	5 de mayo de 2014
Versión beta pública	WorkSpaces está disponible en versión beta pública.	25 de marzo de 2014

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.