Guía de administración

Amazon WorkSpaces

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

Amazon WorkSpaces: Guía de administración

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es WorkSpaces? ... 1
Conexión mediante una aplicación cliente ... 3
Utilizar sus propias licencias de escritorio de Windows ... 4
Uso de las licencias de escritorio Bring Your Own Windows en WorkSpaces ... 4
Vídeos sobre cómo cargar y crear imágenes de BYOL ... 17
Vincula cuentas BYOL en WorkSpaces ... 17
Mensajes de error comunes y sus soluciones ... 18
Lista de mensajes de SysPrep error y correcciones de errores ... 24
Use y administre el WorkSpaces personal ... 26
WorkSpaces Opciones personales ... 27
Comience a usar WorkSpaces Personal ... 27
Crea un WorkSpace ... 37
Conéctese al WorkSpace ... 40
Pasos a seguir a continuación ... 41
Acceso y protocolos de red ... 42
Protocolos para Amazon WorkSpaces ... 42
Requisitos de la VPC ... 44
AWS Global Accelerator (AGA) ... 50
Zonas de disponibilidad para WorkSpaces ... 52
Requisitos de puertos y direcciones IP ... 54
Requisitos de red ... 159
Dispositivos de confianza ... 162
Integración con SAML 2.0 ... 165
Acceso a Microsoft Entra ID ... 190
Autenticación con tarjeta inteligente ... 194
Acceso a Internet ... 206
Grupos de seguridad ... 207
Grupos de control de acceso a direcciones IP ... 209
PCoCliente IP cero ... 212
Configuración de Android para Chromebook ... 213
Configuración del acceso web ... 214
Configuración de Amazon WorkSpaces Thin Client ... 219
Configuración del cifrado de puntos de conexión de FIPS ... 223
Habilite las conexiones SSH para Linux WorkSpaces ... 225

Configuración y componentes del servicio necesarios ... 232
Administre los directorios de WorkSpaces ... 239
Registre un AWS Directory Service directorio existente ... 241
Seleccionar una unidad organizativa ... 243
Configurar direcciones IP públicas automáticas ... 244
Controlar el acceso de los dispositivos ... 245
Administrar los permisos de administrador local ... 245
Actualizar la cuenta del Conector AD (Conector AD) ... 246
Autenticación multifactor (Conector AD) ... 246
Cree un directorio ... 247
Actualice los servidores DNS para WorkSpaces ... 274
Eliminar directorio ... 282
Configurar la administración del directorio ... 285
Administración de usuarios ... 288
Administración de usuarios ... 288
Cree varios WorkSpaces para un usuario ... 290
Personalice la forma en que los usuarios inician sesión en sus WorkSpaces ... 292
Habilite las capacidades de administración de autoservicio WorkSpaces ... 294
Habilitar la optimización de audio de Amazon Connect ... 298
Habilitar las cargas de registros de diagnóstico ... 301
Administrar WorkSpaces personal ... 302
Administre Windows WorkSpaces ... 304
Administre su Amazon Linux 2 WorkSpaces ... 352
Administra tu Ubuntu WorkSpaces ... 362
Administre su Rocky Linux WorkSpaces ... 370
Administre su Red Hat Enterprise Linux WorkSpaces ... 377
Optimice la comunicación en tiempo real ... 384
Administración del modo de ejecución ... 397
Administración de aplicaciones ... 400
Modificar un WorkSpace ... 407
Personalización de la marca ... 414
Etiquetar recursos ... 422
Mantenimiento ... 424
Encriptado WorkSpaces ... 427
Reiniciar un WorkSpace ... 437
Reconstruye un WorkSpace ... 438

Restaurar un WorkSpace ... 441
BYOL de Microsoft 365 ... 442
Actualice el BYOL de Windows WorkSpaces ... 446
Migre un WorkSpace ... 456
Eliminar un WorkSpace ... 464
Paquetes e imágenes ... 466
Opciones de paquete ... 469
Creación de una imagen y un paquete personalizados ... 475
Actualizar un paquete personalizado ... 497
Copiar una imagen personalizada ... 498
Compartir o dejar de compartir una imagen personalizada ... 501
Eliminar un paquete o imagen personalizado ... 504
Monitor WorkSpaces personal ... 505
Supervise con panel CloudWatch de control automático ... 507
Supervise mediante CloudWatch métricas ... 510
Supervise con Amazon EventBridge ... 525
Descripción de los eventos AWS de inicio de sesión para usuarios de tarjetas inteligentes .. 529
Cree cuadros de mando personalizados CloudWatch ... 536
Continuidad empresarial ... 543
Redireccionamiento entre regiones ... 544
Resiliencia multirregional ... 562
Solución de problemas ... 572
Habilitar el registro avanzado ... 572
Solución de problemas específicos ... 577
Notas de la versión ... 611
Utilice y gestione los WorkSpaces grupos ... 620
Regiones y zonas de disponibilidad admitidas ... 620
Administración de directorios ... 623
Configuración de SAML 2.0 y creación de un directorio de grupos ... 624
Actualizar los detalles de directorio ... 644
Anular el registro de un directorio de grupos WorkSpaces ... 648
Redes y acceso ... 648
Acceso a Internet ... 649
Requisitos de la VPC ... 650
Configuración del cifrado de puntos de conexión de FIPS ... 664
Puntos de conexión de VPC de Amazon S3 ... 665

Conexiones a su VPC ... 667
Conexiones de usuarios ... 669
Crea una WorkSpaces piscina ... 673
Administrar WorkSpaces grupos ... 676
Modo de ejecución ... 676
Paquetes ... 677
Modificación de un grupo ... 678
Eliminar un grupo ... 678
Auto Scaling para WorkSpaces piscinas ... 679
Uso de Active Directory ... 691
Dominios de Active Directory ... 692
Antes de empezar ... 693
Autenticación basada en certificados ... 695
Administración ... 702
Más información ... 710
Paquetes e imágenes ... 710
Opciones de paquete ... 712
Creación de una imagen y un paquete personalizados ... 715
Administración de imágenes y paquetes personalizados ... 732
Uso de scripts de sesión para administrar la experiencia ... 733
Monitoreo de WorkSpaces grupos ... 744
WorkSpaces Métricas y dimensiones de los pools ... 744
Administración del almacenamiento persistente ... 747
Administración de las carpetas principales ... 747
Habilitación de la persistencia de configuración de aplicaciones para los usuarios ... 754
Cómo funciona la persistencia de configuración de aplicaciones ... 755
Habilitación de la persistencia de configuración de la aplicación ... 757
Administre VHDs la configuración de las aplicaciones de sus usuarios ... 759
Códigos de notificación de solución de problemas ... 766
Seguridad ... 771
Protección de los datos ... 772
Cifrado en reposo ... 773
Cifrado en tránsito ... 773
Identity and Access Management ... 774
Ejemplos de políticas ... 775
Especifique WorkSpaces los recursos en una política de IAM ... 783

Cree el rol workspaces_ DefaultRole ... 788
Cree el rol de servicio AmazonWorkSpaces PCAAccess ... 790
AWS políticas gestionadas para WorkSpaces ... 791
Acceso a las instancias de streaming WorkSpaces y a los scripts de las mismas ... 800
Validación de conformidad ... 805
Resiliencia ... 806
Seguridad de la infraestructura ... 806
Aislamiento de red ... 807
Aislamiento en hosts físicos ... 807
Autorización de usuarios corporativos ... 807
Cree y transmita desde puntos finales de VPC de interfaz ... 808
Realice solicitudes a la WorkSpaces API de Amazon a través de un punto final de interfaz de VPC ... 813
Cree una política de puntos de conexión de VPC para Amazon WorkSpaces ... 814
Conecte su red privada a su VPC ... 816
Administración de actualizaciones ... 816
Cuotas ... 817
WorkSpaces fin de la vida útil del cliente ... 824
Versiones de cliente no compatibles ... 830
EOL FAQs ... 831
Estoy usando una versión de un WorkSpaces cliente que ha alcanzado su EOL. ¿Qué debo hacer para actualizar a una versión compatible? ... 831
¿Puedo usar una versión del WorkSpaces cliente que haya alcanzado su fin de vida con una versión compatible? WorkSpace ... 831
Estoy usando una versión de un WorkSpaces cliente que ha alcanzado su fin de vida. ¿Puedo seguir denunciando problemas al respecto? ... 831
Estoy usando una versión de WorkSpaces cliente compatible en un sistema operativo que ha alcanzado su EOL. ¿Puedo seguir denunciando problemas al respecto? ... 832
Guía para desarrolladores de SDK de extensiones ... 833
Historial de documentos ... 834
Actualizaciones anteriores ... 842
... dcccxlvi

¿Qué es Amazon WorkSpaces?

Amazon WorkSpaces le permite aprovisionar escritorios virtuales basados en la nube, conocidos como WorkSpacespara sus usuarios. Estos escritorios pueden ejecutar Microsoft Windows, Amazon Linux 2, Ubuntu Linux, Rocky Linux o Red Hat Enterprise Linux. 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.

Amazon te WorkSpaces permite elegir entre WorkSpaces Personal y WorkSpaces Pools en función de tu organización y de las necesidades de los usuarios.

- WorkSpaces Personal: elija WorkSpaces Personal si necesita escritorios virtuales persistentes diseñados para los usuarios que necesitan un escritorio altamente personalizado y aprovisionado para su uso exclusivo. Esto es similar a un equipo de sobremesa físico que se asigna a una persona. Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal.
- WorkSpaces Pool: elija WorkSpaces Pool para escritorios virtuales no persistentes diseñados para los usuarios que necesitan acceder a entornos de escritorio altamente seleccionados alojados en una infraestructura efímera. Para obtener más información, consulte Administrar WorkSpaces grupos.

Puede configurar los WorkSpaces escritorios de varias formas:

- Elija entre una variedad de configuraciones de hardware, configuraciones de software y AWS regiones. Para obtener más información, consulta Amazon WorkSpaces Bundles ythe section called “Creación de una imagen y un paquete personalizados”.
- Si WorkSpaces utiliza Windows, puede traer sus propias licencias y aplicaciones o adquirirlas en el AWS Marketplace for Desktop Apps.
- Si WorkSpaces ejecuta Windows 10 u 11, puede unir su ID de Entra WorkSpaces a Microsoft para que los usuarios puedan usar sus credenciales de ID de Entra existentes para obtener un acceso sin problemas a las aplicaciones de Microsoft 365 para empresas. También puedes inscribirte WorkSpaces en Intune para administrar tus escritorios virtuales con Intune. Para obtener más información, consulte Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal. Para obtener más información sobre Microsoft Entra ID, consulte ¿Qué es Microsoft Entra ID? Para obtener más información sobre Microsoft Intune, consulte Microsoft Intune administra identidades, aplicaciones y dispositivos de forma segura.

- Elija un protocolo PCo IP o DCV. Para obtener más información, consulte Protocolos para WorkSpaces uso personal.
- Cree un Microsoft Active Directory gestionado e independiente para sus usuarios o conéctelo WorkSpaces a su Active Directory local para que los usuarios puedan usar sus credenciales existentes y obtener un acceso sin problemas a los recursos corporativos. Para obtener más información, consulte the section called “Administre los directorios de WorkSpaces”.
- 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, las E/S del disco y las instantáneas de volumen.
- Elija qué direcciones IP pueden usar sus usuarios para acceder a sus. WorkSpaces
- Elija la facturación mensual o por hora para WorkSpaces. Para más información, consulte Precios de WorkSpaces.

Para obtener más información sobre cómo trabajar con WorkSpaces, consulte:

- WorkSpacesRecursos de Amazon: incluye documentos técnicos, publicaciones de blog, seminarios web y sesiones de re:Invent
- Aprovisionar escritorios en la nube
- Mejores prácticas para la implementación de Amazon WorkSpaces
- Amazon WorkSpaces FAQs
- Para ver detalles y ejemplos de WorkSpaces precios, consulte WorkSpaces Precios.

Conectarse WorkSpaces mediante una aplicación cliente

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

> **Note**
>
> No puedes usar un navegador web para conectarte 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 sin cliente (los dispositivos con cero cliente de Teradici solo son compatibles con PCo IP).

En Windows, macOS y Linux PCs, puede usar 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.

Traiga sus propias licencias de escritorio de Windows WorkSpaces

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, consulte WorkSpaces Precios.

> **Important**
>
> La creación de imágenes no es compatible con los sistemas Windows 11 que se hayan actualizado de una versión de Windows 11 a una versión más reciente de Windows 11 (una actualización de una característica o versión de Windows). Por ejemplo, un sistema Windows 11 23H2 que se actualizó a la 24H2 no se puede usar para crear una imagen. Sin embargo, el proceso de creación de imágenes admite las actualizaciones acumulativas o de seguridad de Windows. WorkSpaces

Temas

- Uso de las licencias de escritorio Bring Your Own Windows en WorkSpaces
- Vídeos sobre cómo cargar y crear imágenes de BYOL
- Vincula cuentas BYOL en WorkSpaces
- Mensajes de error comunes y sus soluciones
- Lista de mensajes de SysPrep error y correcciones de errores

Uso de las licencias de escritorio Bring Your Own Windows en WorkSpaces

Sigue los siguientes pasos para importar y usar tu propia licencia de escritorio de Windows en Amazon WorkSpaces

Paso 1: Requisitos previos para usar Windows BYOL con Amazon WorkSpaces

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 non-GPU-enabled paquetes (paquetes distintos de Graphics.G4dn, GraphicsPro .g4dn, Graphics y GraphicsPro), compruebe que va a utilizar un mínimo de 50 por región. WorkSpaces Estos 50 pueden ser AutoStop WorkSpaces cualquier combinación de y. WorkSpaces AlwaysOn El uso de un mínimo de 50 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**
  >
  > - Como parte del proceso de importación de imágenes, recupera AWS automáticamente los registros del sistema para resolver los errores de importación de imágenes, proporcionar ayuda para solucionar problemas y enviar mensajes de error precisos a los usuarios.
  > - Graphics.g4dn, GraphicsPro .g4dn, Graphics y los GraphicsPro paquetes no están disponibles en la región de África (Ciudad del Cabo) ni en la región de Israel (Tel Aviv).
  > - 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 económicos no están disponibles para Windows 11 y WorkSpaces Pools. Para obtener más información sobre la migración de su paquete WorkSpaces de valor existente, consulte. Migrar un WorkSpace archivo en WorkSpaces Personal
  > - Para disfrutar de la mejor experiencia de videoconferencia, recomendamos utilizar paquetes de alimentación (4 vCPU, 16 GB de memoria o más).

- WorkSpaces puede utilizar 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

- Antes de importar una imagen de máquina virtual personalizada por BYOL, valide la imagen.

  WorkSpaces solo admite imágenes con el modo de arranque UEFI activado. Para obtener más información sobre cómo EC2 Image Builder detecta el modo de arranque, consulte Tipos de volúmenes y sistemas de archivos compatibles con VM Import/Export en la Guía del Import/Export usuario de VM.

Versiones de Windows compatibles con BYOL

Su máquina virtual debe ejecutar una de las siguientes versiones de Windows:

- 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 utiliza. 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.

Paso 2: Habilite su cuenta para BYOL

Una vez que hayas confirmado que cumples los requisitos previos para usar el BYOL de Windows con WorkSpaces, tendrás que habilitar tu cuenta para usar imágenes BYOL.

1. En la WorkSpaces consola, vaya a la página de configuración de la cuenta.
2. En la sección Traiga su propia licencia (BYOL), se muestra el estado de habilitación de BYOL de su cuenta. Si el estado indica que su cuenta no está habilitada, pulse el botón Comenzar con BYOL.
3. En la página BYOL, selecciona Habilitar cuenta para BYOL.

   > **Note**
   >
   > La activación de su cuenta para BYOL solo se aplica a una sola región. Toma nota de la región en la que te encuentras actualmente y, si deseas usar una región diferente, cámbiate a esa región antes de habilitar tu cuenta.

4. Aparece una ventana emergente que confirma que entiendes los requisitos mínimos para usar WorkSpaces BYOL. Confirma que entiendes los requisitos y selecciona Activar cuenta.

   > **Note**
   >
   > Si planea usar Graphics WorkSpaces con BYOL, cree un ticket de AWS Support. La consola aún no admite la activación de gráficos mediante BYOL. WorkSpaces

5. En la mayoría de los casos, las cuentas se activan automáticamente. Sin embargo, algunas cuentas requieren una revisión adicional. El estado de activación se muestra en la página BYOL una vez actualizada.

6. Cuando su cuenta esté habilitada para BYOL, continúe con el siguiente paso.

(Opcional) Valide la imagen antes de importarla

> **Note**
>
> Este paso solo se aplica a las imágenes de máquinas virtuales personalizadas que se van a importar. Si va a importar una ISO de Windows, puede omitir este paso.

Si va a importar una imagen de máquina virtual personalizada, le recomendamos que ejecute la herramienta WorkSpaces Image Checker para asegurarse de que su máquina virtual sea compatible con WorkSpaces ella. La herramienta Image Checker ejecuta una serie de pruebas y puede ayudar a solucionar problemas de compatibilidad.

Para descargar el script del comprobador de compatibilidad de imágenes

Antes de descargar y ejecutar el script del comprobador de compatibilidad de imágenes, compruebe que las últimas actualizaciones de seguridad de Windows estén instaladas en la máquina virtual. Mientras se ejecuta este script, deshabilita el servicio Windows Update.

1. Descargue el archivo.zip del script Image Compatibility Checker desde ImageCompatibilityChecker.zip a su carpeta. `Downloads`
2. En la carpeta `Downloads`, cree una carpeta `BYOL`.
3. Extraiga los archivos de `ImageCompatibilityChecker.zip` y cópielos en la carpeta `Downloads\BYOL`.
4. Elimine la carpeta `Downloads\ImageCompatibilityChecker.zip` para que solo queden los archivos extraídos.

Realice estos pasos para ejecutar el script del comprobador de compatibilidad de imágenes.

Para ejecutar el script del comprobador de compatibilidad de imágenes

1. Abre Powershell como administrador.
    1. Selecciona el botón de inicio de Windows.
    2. Haga clic con el botón PowerShell derecho en

   3. Elija Ejecutar como administrador.
   4. Si el Control de cuentas de usuario lo solicita, seleccione Sí.
2. En la PowerShell línea de comandos, vaya al directorio en el que se encuentra el script del Comprobador de compatibilidad de imágenes. 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 del equipo. Si lo hace, se ejecutará el script del comprobador de compatibilidad de imágenes:

   ```
   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. Introduzca el siguiente comando para ejecutar el script del comprobador de compatibilidad de imágenes:

   ```
   .\ImageCompatibilityChecker.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 Ejecutar 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, `WorkSpacesImageCompatabilityCheckLogYYYY-MM-DD_HHmmss.txt` y `ImageInfo.text`. Estos archivos se encuentran en el directorio que contiene los archivos de script del Comprobador de compatibilidad de imágenes.

> **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).

    También aparecerá una petición para ejecutar Sysprep. Ciérrela y no ejecute aún Sysprep.

12. Apague la máquina virtual y expórtela. Para obtener más información, consulte Exportación de la máquina virtual desde su entorno de virtualización en la Guía del Import/Export usuario de la máquina virtual.

13. (Opcional) Inicie la máquina virtual y ejecute el script del comprobador de compatibilidad de imágenes una vez más. Deberían aprobarse todas las validaciones. Volverá a aparecer una pantalla con un botón para ejecutar Sysprep. Elija Run Sysprep (Ejecutar Sysprep). Si Sysprep funciona correctamente, la máquina virtual exportada que exportó desde el paso 12 se puede importar a Amazon Elastic Compute Cloud (Amazon EC2).

    Si Sysprep no se ejecuta correctamente, revise los registros de Sysprep de la ruta `%WINDIR%\System32\Sysprep\Panther`, vuelva a la máquina virtual que ha exportado en el paso 12, resuelva los problemas notificados y vuelva a completar el paso 12 exportando la máquina virtual corregida. A continuación, volverá a ejecutar el script del comprobador de compatibilidad de imágenes para asegurarse de que se hayan resuelto los problemas.

    El motivo más común por el que se produce un error en Sysprep es que no se han desinstalado los Modern AppX Packages para todos los usuarios. Utilice el `Remove-AppxPackage` PowerShell cmdlet para eliminar los paquetes de AppX.

14. Importa la máquina virtual que exportaste en el paso 12 a Amazon EC2.

Paso 3: Cree una imagen BYOL mediante la consola WorkSpaces

Realice estos pasos para importar la imagen y crear una imagen WorkSpaces BYOL:

1. Ve al panel de navegación y selecciona Imágenes y, a continuación, Importar imagen.
2. Siga los pasos de la página Importar imagen según la opción de imagen base y el tipo de imagen que desee importar:

    - Importación de máquinas virtuales: importa una imagen de máquina virtual que ya se ha personalizado. Puede importar un `OVF` archivo `VHDXVMDK`, o.
    - Importación ISO: importa una imagen ISO de Windows que descargó de Microsoft y que no se ha personalizado.

- Importación de AMI: importa una EC2 AMI de Amazon existente para utilizarla como imagen WorkSpaces BYOL.

3. Realice una de las siguientes acciones:

   - Para la opción de importación de máquinas virtuales, cargue el archivo en Amazon S3 y, a continuación, especifique la ubicación del archivo que se va a importar. Tenga en cuenta que el bucket de S3 que utilice debe estar en la misma región en la que pretende implementar BYOL WorkSpaces.
   - Para la importación ISO, importe una imagen ISO de Windows que haya descargado de Microsoft y que no se haya personalizado. Tenga en cuenta que el bucket de S3 que utilice debe estar en la misma región en la que pretende implementar BYOL WorkSpaces.
   - Para la importación de la AMI, especifique el ID de la AMI.

4. Vaya a Configuración de infraestructura.

   WorkSpaces crea automáticamente una canalización de Amazon EC2 Image Builder para crear su imagen BYOL. La configuración de la infraestructura define cómo se configura EC2 Image Builder para crear la imagen. Puede personalizarlo mediante los siguientes ajustes:

   - Valores predeterminados del servicio: crea y utiliza un rol y una política de IAM predeterminados para crear su imagen.
   - Utilice una configuración de infraestructura existente: ofrece una selección de configuraciones de infraestructura personalizadas que se configuran en Amazon EC2 Image Builder. Para obtener más información, consulte Crear una configuración de infraestructura en la Guía del usuario de EC2 Image Builder.

5. Vaya a Configuración avanzada y seleccione si desea finalizar la instancia de EC2 compilación si la imagen presenta errores de importación.

   - Si decide finalizar la instancia en caso de error, no podrá acceder a la instancia para depurar los errores durante el flujo de trabajo de importación de imágenes.
   - Si decides no terminar la instancia, la instancia se puede usar para depurar errores, pero es posible que incurras en costes adicionales por su ejecución. EC2

6. Ve a Detalles de la imagen para especificar las propiedades de la imagen, incluido el nombre de la imagen.

   - Nombre de la imagen: identificador único de la imagen.

- Tipo de cálculo: especifique si esta imagen debe utilizar hardware no gráfico o básico o hardware gráfico
- Versión del sistema operativo: elija la versión de la imagen para el sistema operativo Windows
- Versión semántica: defina una versión semántica de la imagen, que se almacenará en EC2 Image Builder. Para obtener más información, consulte Control de versiones semántico en Image Builder en la Guía del usuario de EC2 Image Builder

> **Note**
>
> Durante el proceso de importación BYOL, los recursos de EC2 Image Builder se crearán en su AWS cuenta. Para crear la imagen, `AWSServiceRoleForImageBuilder` se crea automáticamente un rol vinculado al servicio denominado si aún no existe. Este rol contendrá la política AWS gestionada `AWSServiceRoleForImageBuilder`. También debe tener los permisos necesarios para que VM Import/Export importe una imagen de máquina virtual personalizada.

Mientras se crea la imagen, el estado de la página Imágenes de la consola aparece como Pendiente. El proceso de ingestión de BYOL tarda un mínimo de 90 minutos.

Los errores que se produzcan al importar la imagen se mostrarán en la página de imágenes junto con las soluciones sugeridas. Los registros detallados se encuentran en Amazon CloudWatch en el grupo de registros Image Builder que se creó al importar la imagen. Los posibles tipos de error son:

- Errores de imagen: Image Builder no ha podido crear EC2 la imagen. Solucione los problemas en su entorno de virtualización e importe una imagen nueva.
- Errores de Image Builder: se produjo un error al intentar crear la imagen. Consulta los registros de Image Builder en Amazon CloudWatch para obtener más información
- EC2 errores: hay problemas con la imagen que no se pudieron solucionar automáticamente. Para resolver estos errores, puedes conectarte a la EC2 instancia de Amazon si estaba configurada para que no finalizara en caso de error de compilación y realizar correcciones directamente. A continuación, puedes volver a intentar la importación desde la página de imágenes.
- Errores corregidos automáticamente: estos problemas los ha solucionado automáticamente. WorkSpaces No hay que hacer nada más.

Para obtener información detallada sobre los errores más comunes, consulte Mensajes de error comunes y sus soluciones.

Paso 4: Elija el rango de direcciones IP para su interfaz de administración BYOL

BYOL WorkSpaces se ejecuta en hardware dedicado para cumplir con los términos de licencia de Microsoft. Para ello, se ha creado una interfaz de administración BYOL para establecer una conexión segura entre su red de WorkSpaces administración AWS gestionada WorkSpaces y la suya. Para obtener más información, consulte Interfaces de red.

Si tiene otra AWS cuenta habilitada para BYOL en la misma región, puede usar la misma interfaz de administración en todas las cuentas para reservar menos direcciones IP. Para ello, omita este paso y continúe con el siguiente.

Selección de un rango de direcciones IP de la interfaz de administración

1. Vuelva a la página BYOL en la configuración de la cuenta.
2. En la sección Elegir rango de IP, selecciona el botón Elegir rango de IP.
3. Introduzca un rango de búsqueda proporcionando un rango de direcciones IP que esté disponible en su red. WorkSpaces devuelve /16 rangos de direcciones IP de máscara de red disponibles que coinciden con su búsqueda.
4. Elija un rango de direcciones IP disponible (que se muestra como bloques CIDR).

> **Note**
>
> Tenga en cuenta que, una vez que elija el rango de IP para la interfaz de administración, no podrá cambiarlo.

(Opcional) Vincule cuentas BYOL

Si tiene otra AWS cuenta habilitada para BYOL en la misma región, puede usar la misma interfaz de administración en todas las cuentas para reservar menos direcciones IP.

Para vincularse a una cuenta BYOL existente, no seleccione un rango de direcciones IP.

Vincular cuentas BYOL

1. Inicie sesión en la AWS cuenta que ya está habilitada para WorkSpaces BYOL.

2. Ve a la página BYOL en la configuración de la cuenta.
3. En la sección Elegir rango de IP, selecciona el botón Enviar invitación en la sección de vinculación de cuentas.
4. Indique el AWS ID de la cuenta que no está habilitada para BYOL y a la que desea vincular.

> **Note**
>
> Las dos cuentas deben usar BYOL en la misma región.

5. Una vez enviada la invitación de vinculación, vuelve a la AWS cuenta que aún no está habilitada para BYOL. En la página de configuración de la cuenta, verás un banner de notificación en el que se indica que tienes una invitación pendiente para vincular una cuenta BYOL. Selecciona Ver invitación en el banner.
6. Confirma la invitación a vincular la cuenta.

Paso 5: Crea un paquete personalizado a partir de la imagen BYOL en WorkSpaces

Después de crear tu imagen BYOL siguiendo las instrucciones de, puedes usar la imagen para crear un paquete personalizado. Para obtener más información, consulte Crear una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal.

Paso 6: Crea un directorio dedicado para Amazon WorkSpaces

Para utilizar imágenes BYOL WorkSpaces, debe crear un directorio con este fin.

Para crear un directorio para WorkSpaces, consulte Crear un directorio para WorkSpaces Personal. Asegúrese de seleccionar Activar el directorio dedicado WorkSpaces al crear el directorio.

> **Important**
>
> Si no aparece la WorkSpaces opción dedicada habilitada al registrar el directorio, asegúrese de haber completado los pasos para habilitar BYOL en su cuenta y región.
> Si ya ha registrado un directorio AD AWS administrado de Microsoft o un directorio AD Connector WorkSpaces que no se ejecuta en hardware dedicado, puede configurar un nuevo directorio AD AWS administrado de Microsoft o un directorio AD Connector para este fin. También puedes anular el registro del directorio y volver a registrarlo como directorio dedicado. WorkSpaces Para obtener más información sobre cómo registrar y anular el

registro de un directorio de AWS Directory Service existente, consulte Registrar un directorio de AWS Directory Service existente con WorkSpaces Personal.

Paso 7: Inicie su BYOL WorkSpaces

Inicie su BYOL Personal WorkSpaces

Para lanzar un personal WorkSpaces, consulte Crear un WorkSpaces personal WorkSpace en Personal.

Lanza tu piscina BYOL WorkSpaces

Para lanzar una WorkSpaces piscina, debes lanzar una personal WorkSpace, crear una imagen de esa persona y luego usar esa imagen para lanzar una piscina. WorkSpace

Para crear una imagen para las piscinas BYOL WorkSpaces

1. Crea una imagen personal WorkSpace con la imagen BYOL que quieras usar para tus WorkSpaces piscinas. Para obtener información sobre cómo iniciar WorkSpaces Personal, consulte Crear un archivo WorkSpace en WorkSpaces Personal.
2. Inicie sesión en la cuenta personal WorkSpace y asegúrese de que todas las actualizaciones de Windows estén instaladas.
3. Actualiza tus EC2 configuraciones de Amazon. Para actualizar EC2 las configuraciones con Windows 10, consulta Instalar la última versión de EC2 Config. Para actualizar EC2 las configuraciones con Windows 11, consulta Instalar la última versión de EC2 Launch.
4. Añada una lista de exclusiones de Windows Defender. Para obtener más información, consulte Agregar una exclusión a Seguridad de Windows.

   Añada las siguientes carpetas a la lista de exclusiones de Windows Defender:

   - `C:\Program Files\Amazon\`
   - `C:\ProgramData\Amazon\*`
   - `C:\Program Files\NICE\`
   - `C:\ProgramData\NICE\`
   - `C:\Program Files (x86)\AWS Tools\*`
   - `C:\Program Files (x86)\AWS SDK for .NET\*`

- `C:\AWSEUC\`(Esto es para el script de la sesión)

5. Introduzca el siguiente comando para deshabilitar la actualización de Windows durante el inicio.
6. Abre Powershell como administrador.

   1. Selecciona el botón de inicio de Windows.
   2. Haga clic con el botón PowerShell derecho en
   3. Elija Ejecutar como administrador.
   4. Si el Control de cuentas de usuario lo solicita, seleccione Sí.

7. Ejecute los siguientes comandos:

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Force
```

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Force
```

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU"
 -Name "NoAutoUpdate" -Value 1 -Force
```

8. Reinicie el WorkSpace. Para obtener más información, consulte Reiniciar un WorkSpace en WorkSpaces Personal.

   > **Note**
   >
   > Se recomienda hacer lo siguiente antes de empezar a crear una imagen para los WorkSpaces grupos BYOL.
   >
   > - Elimine las aplicaciones de inicio innecesarias.
   > - Elimine o deshabilite las tareas programadas innecesarias. Abra el menú de inicio, seleccione Tareas programadas, seleccione las tareas que desea deshabilitar y, a continuación, elija Deshabilitar.

9. Ejecute el comprobador de imágenes después del reinicio mediante el siguiente comando.

```
C:\Program Files\Amazon\ImageChecker.exe
```

10. Resuelva los errores que haya detectado el comprobador de imágenes. Para obtener más información, consulte Consejos para resolver los problemas detectados por el comprobador de imágenes.

11. Una vez que todas las pruebas hayan superado el comprobador de imágenes, vuelva a la WorkSpaces consola.
12. En el panel de navegación, en WorkSpaces, selecciona Personal. Elija el BYOL personal y WorkSpaces, a continuación, elija Acciones, Crear imagen.
13. En el panel de navegación, elija Images. En Imágenes, compruebe si se ha creado la imagen.

Ahora puedes lanzar WorkSpaces Pools con la imagen que has creado. Para obtener más información sobre el lanzamiento de WorkSpaces grupos, consulte Crear un WorkSpaces grupo.

Vídeos sobre cómo cargar y crear imágenes de BYOL

En los siguientes vídeos podrá ver una demostración de cómo se cargan imágenes de BYOL.

En el siguiente vídeo podrá ver una demostración de cómo se crean imágenes de BYOL con Microsoft Hyper-V.

Para ver una demostración sobre la creación de imágenes BYOL con VMware Workstation, vea el siguiente vídeo.

Vincula cuentas BYOL en WorkSpaces

Puede usar la vinculación de BYOL para vincular cuentas y compartir las configuraciones de 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 de BYOL es la propietaria principal de la infraestructura de hardware subyacente, y se denomina cuenta de origen. La cuenta de origen 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**
>
> APIs para BYOL, la vinculación de cuentas no están disponibles 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 en la misma región.

Cómo 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 ListAccountLinksAPI GetAccountLinko.

Mensajes de error comunes y sus soluciones

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 BYOL requiere un sistema sin un agente de PCo propiedad intelectual.

Desinstale el agente PCo IP. Para obtener información sobre la desinstalación del agente PCo IP, consulte Desinstalar el cliente de software PCo IP 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 mediante BYOL requiere que la cuenta _BYOL esté habilitada WorkSpaces

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, consulta Cambiar TCP/IP la configuración.

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 la unidad C puede estar presente en una imagen de máquina de Amazon que se esté utilizando para importar una WorkSpace imagen BYOL. 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 mediante BYOL requiere un sistema sin VMware herramientas.

VMWare las herramientas deben estar desinstaladas. Para obtener más información, consulte Desinstalar e instalar manualmente VMware las herramientas 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 mediante BYOL requiere que esté deshabilitada. AutoLogon

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 el Comprobador de compatibilidad de imágenes para obtener detalles sobre el software antivirus que desea desinstalar.

La importación mediante BYOL requiere que los sistemas Windows 10 tengan un modo de arranque antiguo.

La BIOS anterior BootMode debe usarse en Windows 10. Para obtener más información, consulte Modos de arranque.

La importación mediante BYOL requiere que el estado de almacenamiento reservado de Windows esté desactivado

Para deshabilitar el estado de almacenamiento reservado

1. Instale todas las actualizaciones de Windows y reinicie el sistema operativo.
2. Asegúrese de que no haya actualizaciones nuevas.
3. Ejecute cualquiera de los siguientes comandos en Powershell como administrador.
   - ```
     Set-WindowsReservedStorageState -State Disabled
     ```
   - ```
     DISM.exe /Online /Set-ReservedStorageState /State:Disabled
     ```
4. Reinicie el sistema.

> **Note**
>
> Si el almacenamiento reservado está en uso, es posible que no esté deshabilitado y aparezca el siguiente mensaje de error: `This operation is not supported when reserved storage is in use. Please wait for any servicing operations to complete and then try again later.`

La importación BYOL tiene una letra de unidad restringida en uso.

The `D:` Drive es una letra de disco restringida para WorkSpaces. Asegúrese de que no `D:` se utilice o no se asigne a ella durante el lanzamiento de una instancia desde la imagen.

La importación por BYOL tiene una imagen del sistema operativo que no es compatible con el protocolo de streaming seleccionado.

La imagen que se está importando no es compatible con el protocolo de streaming elegido; consulte Creación de una imagen BYOL mediante la WorkSpaces consola.

La importación mediante BYOL no es compatible con la integridad de la memoria.

La integridad de la memoria no se admite cuando Credential Guard está habilitado en el sistema operativo Windows de un. WorkSpace Se detectó la integridad de la memoria y no UEFILock se puede deshabilitar durante la importación de imágenes. Importe una imagen con la opción UEFILock deshabilitada; consulte Desactivar Credential Guard.

Lista de mensajes de SysPrep error y correcciones de errores

La AMI que está importando tiene paquetes de AppX instalados. Elimínelos y vuelva a importar la imagen.

Es posible que los Modern AppX Packages aún estén instalados para los usuarios. Para eliminar el paquete de AppX, ejecute el `cmdlet` de Powershell, `Remove-AppxPackage`.

> **Note**
>
> Durante el proceso de importación de BYOL, se limpiarán los paquetes de AppX infractores y se volverá a intentar con Sysprep. Si el proceso de importación de imágenes sigue fallando, significa que los paquetes de AppX deberán limpiarse manualmente.

La AMI que está importando tiene habilitado el almacenamiento reservado. Deshabilítelo después de que Windows actualice y vuelva a importar la imagen.

Cómo deshabilitar el almacenamiento reservado

1. Introduzca `regedit.exe` para abrir el editor del registro.

2. Vaya a la clave del registro: `HKLM\Software\Microsoft\Windows\CurrentVersion\ReserveManager`.
3. Cambie el valor del parámetro `ShippedWithReserves` de `1` a `0`.
4. Cambie el valor de `ActiveScenario` a `0`.
5. Deshabilite el almacenamiento reservado en Windows con el siguiente comando:

```
DISM.exe /Online /Set-ReservedStorageState /State:Disabled
```

La AMI que está importando tiene instalado un software antivirus o antispyware. Elimínelo y vuelva a importar la imagen.

Debe desinstalar el software antivirus. Ejecute el comprobador de compatibilidad de imágenes para obtener detalles sobre el software antivirus que desea desinstalar. Para obtener más información, consulte (Opcional) Valide la imagen antes de importarla.

Se ha producido un error desconocido en la AMI que está importando durante la AMI SysPrep.

SysPrep no se pudo determinar el motivo del error. Póngase en contacto con AWS el servicio de asistencia en https://aws.amazon.com/support.

Uso y administración de WorkSpaces datos personales

WorkSpaces Personal ofrece escritorios virtuales persistentes diseñados para los usuarios que necesitan un escritorio altamente personalizado y aprovisionado para su uso exclusivo, similar a un ordenador de escritorio físico asignado a una persona.

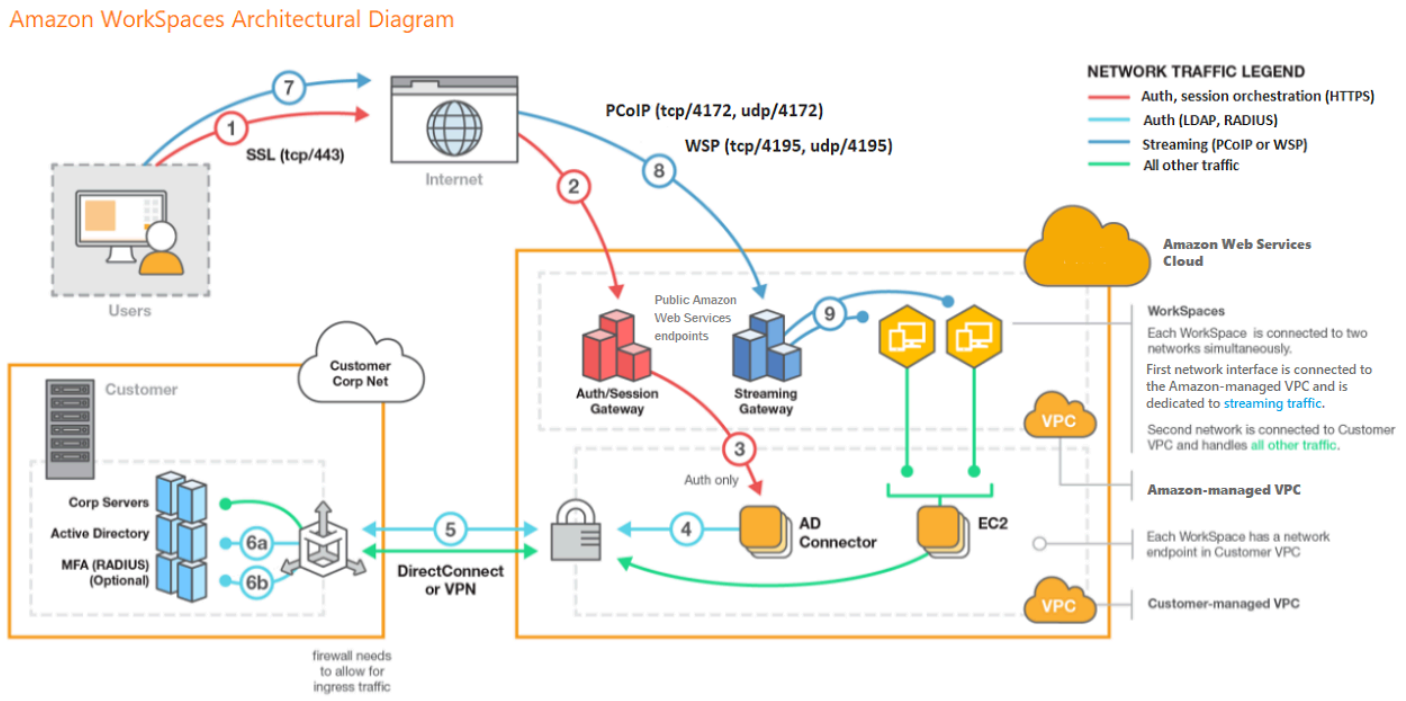
Cada uno WorkSpace está asociado a una nube privada virtual (VPC) y a un directorio para almacenar y administrar la información para usted WorkSpaces y sus usuarios. Para obtener más información, consulte the section called “Requisitos de la VPC”. Los directorios los administra el WorkSpaces servicio o a través del AWS Directory Service, que ofrece las siguientes opciones: Simple AD, AD Connector o AWS Directory Service for Microsoft Active Directory, también conocido como Microsoft AD AWS administrado. Para obtener más información, consulte la Guía de administración de AWS Directory Service.

WorkSpaces utiliza el directorio IAM Identity Center (para los directorios gestionados por Amazon WorkSpaces), 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 (DCV) 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 ese AD Connector de uso.



Opciones para crear una WorkSpace con WorkSpaces Personal

Existen varios métodos para crear un WorkSpace. Puede utilizar las instrucciones de configuración rápida, las instrucciones de configuración avanzada o elegir una de las siguientes opciones:

- Crear un directorio AWS administrado de Microsoft AD para WorkSpaces Personal
- Cree un directorio de Simple AD para WorkSpaces Personal
- Cree un AD Connector para WorkSpaces uso personal
- Cree una relación de confianza entre su directorio AWS administrado de Microsoft AD y su dominio local para Personal WorkSpaces
- Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal
- Cree un directorio personalizado dedicado con WorkSpaces Personal

Comience a usar WorkSpaces Personal

Si es la primera vez WorkSpaces que lo utiliza, puede elegir entre configurar su cuenta WorkSpaces Personal con una configuración rápida o avanzada. En los siguientes tutoriales se describe cómo aprovisionar un escritorio basado en la nube, lo que se conoce como WorkSpaceuso WorkSpaces y AWS Directory Service.

> **Note**
>
> Para empezar a usar WorkSpaces Pools, consulteConfigurar SAML 2.0 y crear un directorio de WorkSpaces grupos.

WorkSpaces Configuración rápida personal

En este tutorial, aprenderá a aprovisionar un escritorio virtual de Microsoft Windows, Amazon Linux 2, Ubuntu Linux, Rocky Linux o Red Hat Enterprise Linux basado en la nube, conocido como WorkSpace, mediante WorkSpaces y AWS Directory Service.

En este tutorial se utiliza la opción de configuración rápida para lanzar su WorkSpace. Esta opción solo está disponible si nunca ha lanzado un WorkSpace. Para otras opciones, consulte Crear un directorio para WorkSpaces Personal.

> **Note**
>
> Esta opción de configuración rápida y este tutorial no se aplican a los WorkSpaces grupos.

> **Note**
>
> La configuración rápida se admite en las siguientes AWS regiones:
>
> - 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
- Qué hace la configuración rápida
- Paso 1: inicia el WorkSpace
- Paso 2: Conexión a la WorkSpace
- Paso 3: limpieza (opcional)
- Pasos a seguir a continuación

Antes de empezar

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

- Debe tener una AWS cuenta para crear o administrar una WorkSpace. Los usuarios no necesitan una AWS cuenta para conectarse y usar su WorkSpaces.
- WorkSpaces no está disponible en todas las regiones. Verifica las regiones compatibles y selecciona una región para tu WorkSpaces. Para obtener más información sobre las regiones compatibles, consulta WorkSpaces los precios por AWS región.

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

- Al lanzar un paquete WorkSpace, debes seleccionar un WorkSpace paquete. Para obtener más información, consulta Amazon WorkSpaces Bundles y Amazon WorkSpaces Pricing.
- Al lanzar un paquete WorkSpace, debes seleccionar qué protocolo (PCoIP o DCV) quieres usar con tu paquete. Para obtener más información, consulte Protocolos para WorkSpaces uso personal.
- Al lanzar un WorkSpace, debe especificar la información del perfil del usuario, incluidos el nombre de usuario y la dirección de correo electrónico. Los usuarios completan sus perfiles especificando una contraseña. La información sobre WorkSpaces los usuarios se almacena en un directorio. Para obtener más información, consulte the section called “Administre los directorios de WorkSpaces”.

Qué hace la configuración rápida

La instalación rápida realiza las siguientes tareas:

- Crea una función de IAM para permitir que el WorkSpaces servicio cree interfaces de red elásticas y enumere sus WorkSpaces directorios. 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 personal WorkSpaces , a continuación, siga los pasos de uno de los tutoriales que se enumeran en Crear un directorio para WorkSpaces Personal. Elija el tutorial correspondiente al tipo de Active Directory que desea utilizar.
- Configura un directorio AD simple en la VPC y lo habilita para. WorkDocs Este directorio Simple AD se utiliza para almacenar el usuario y WorkSpace la información. El primero que Cuenta de AWS 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 los especificados Cuentas de AWS y los añade al directorio.
- Crea WorkSpaces. Cada uno WorkSpace recibe una dirección IP pública para proporcionar acceso a Internet. El modo de ejecución es AlwaysOn. Para obtener más información, consulte Administra el modo de ejecución en WorkSpaces Personal.
- 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.

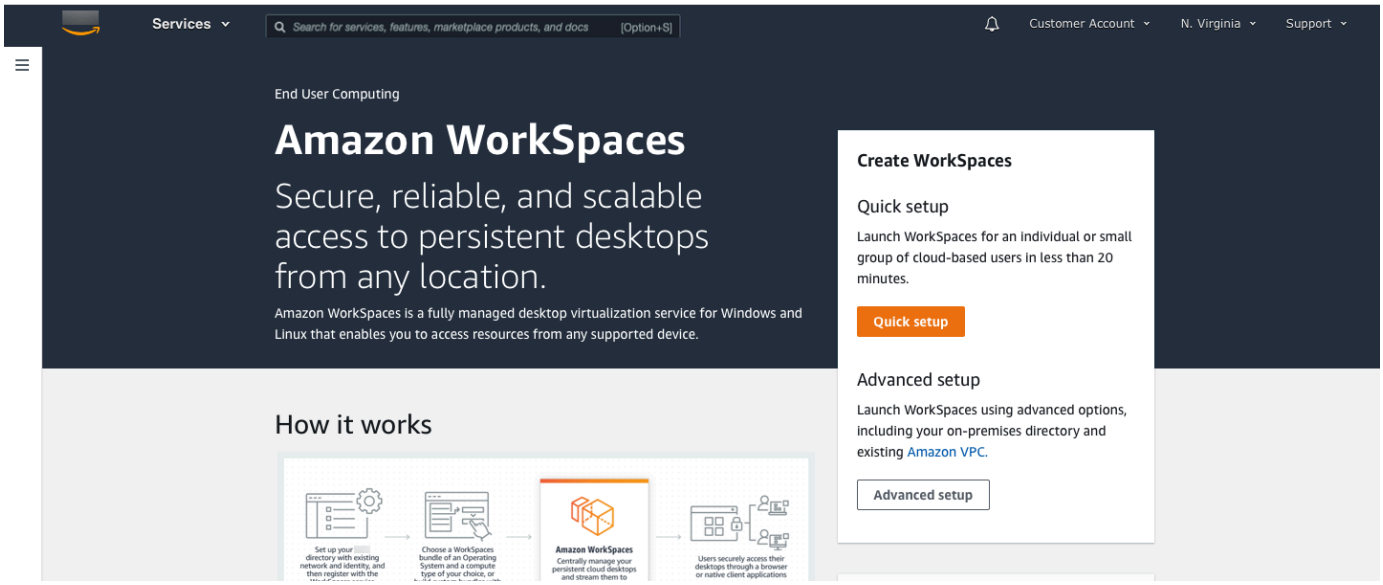
† El primero que Cuenta de AWS crea Quick Setup es tu administrador Cuenta de AWS. No puedes actualizarlo Cuenta de AWS desde la WorkSpaces consola. No comparta con nadie más la información de esta cuenta. Para invitar a otros usuarios a usarlo WorkSpaces, crea uno nuevo Cuentas de AWS para ellos.

Paso 1: inicia el WorkSpace

Con una configuración rápida, puede iniciar el primero WorkSpace en minutos.

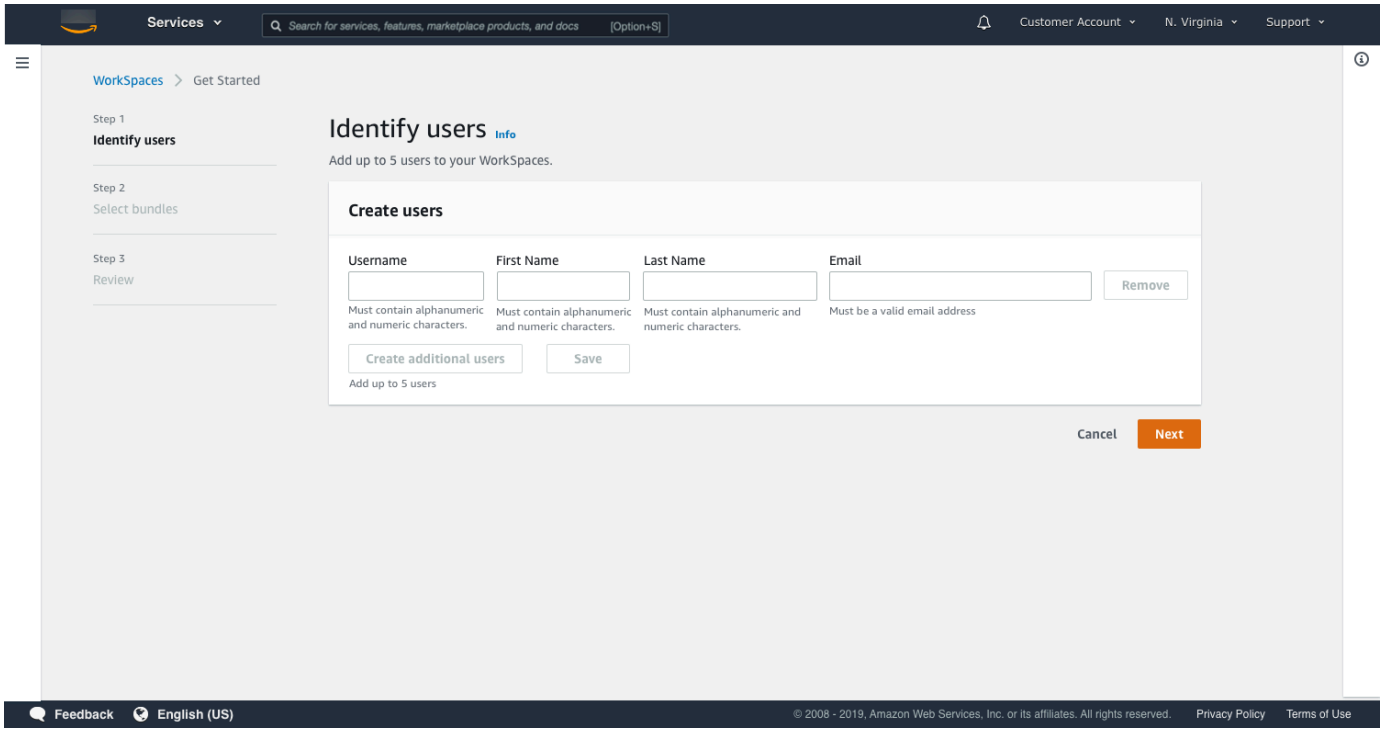
Para lanzar un WorkSpace

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Elija Quick setup (Configuración rápida). Si no ves este botón, significa que ya has lanzado una WorkSpace en esta región o no estás utilizando una de las regiones que admiten la configuración rápida. En este caso, consulte Crear un directorio para WorkSpaces Personal.

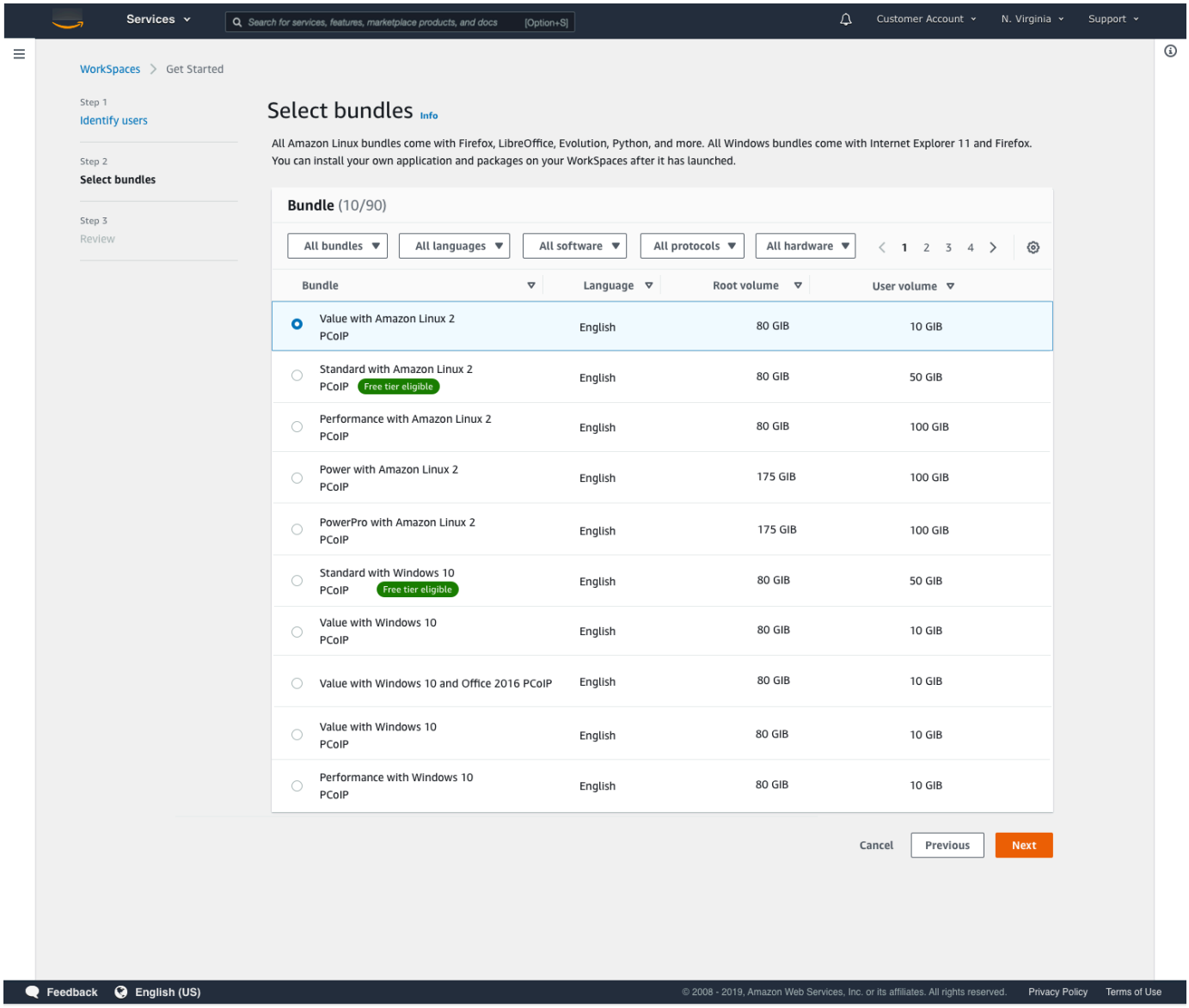


3. En Identificar usuarios, introduzca el nombre de usuario y el nombre. Apellido y correo electrónico. A continuación, elija Siguiente.

> **Note**
>
> Si es la primera vez que lo utilizas WorkSpaces, te recomendamos que crees un usuario para probarlo.



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



5. Revise su información. A continuación, seleccione Crear WorkSpace.
6. El lanzamiento tarda unos 20 minutos. WorkSpace 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 creado el directorio y su estado es`ACTIVE`, puede seleccionar WorkSpacesen el panel de navegación izquierdo el progreso del proceso de WorkSpace inicio. El estado inicial de 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: Conexión a la WorkSpace

Después de recibir el correo electrónico de invitación, puede conectarse WorkSpace con el cliente que prefiera. Después de iniciar sesión, el cliente muestra el WorkSpace escritorio.

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 a su 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. Consulta WorkSpaces la Guía del WorkSpaces usuario de Amazon en la Guía del usuario de Amazon para obtener más información sobre los requisitos de cada cliente y, a continuación, sigue 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 Web Access.

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

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 WorkSpaces Clients and Peripheral Device Support en la Guía del WorkSpaces usuario de Amazon.

Paso 3: limpieza (opcional)

Si ha terminado con lo WorkSpace que creó para este tutorial, puede eliminarlo. Para obtener más información, consulte the section called “Eliminar un WorkSpace”.

> **Note**
>
> Simple AD está disponible de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.
> Para eliminar directorios vacíos, consulte Eliminar un directorio de WorkSpaces Personal.
> Si eliminas tu directorio Simple AD, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

Pasos a seguir a continuación

Puedes seguir personalizando el WorkSpace que acabas de crear. Por ejemplo, puede instalar software y, a continuación, crear un paquete personalizado a partir de su WorkSpace. También puede realizar diversas tareas administrativas para su WorkSpaces directorio WorkSpaces y el suyo. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal
- Administrar WorkSpaces personal
- Administrar directorios para WorkSpaces Personal

Para crear más WorkSpaces, lleve a cabo una de las siguientes acciones:

- Si desea seguir utilizando la VPC y el directorio AD simple que se crearon mediante una configuración rápida, puede añadir WorkSpaces usuarios adicionales siguiendo los pasos de la Crear un WorkSpace en WorkSpaces personal sección del tutorial Cómo lanzar un WorkSpace AD simple.

- Si necesita usar otro tipo de directorio o si necesita usar un Active Directory existente, consulte el tutorial correspondiente en Crear un directorio para WorkSpaces Personal.

Para obtener más información sobre el uso de las aplicaciones WorkSpaces cliente, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte WorkSpaces Clients and Peripheral Device Support en la Guía del WorkSpaces usuario de Amazon.

Comience con la configuración avanzada WorkSpaces personal

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

En este tutorial se utiliza la opción de configuración avanzada para lanzar su WorkSpace.

> **Note**
>
> La configuración avanzada es compatible en todas las regiones para WorkSpaces.

Tareas

- Antes de empezar
- Mediante la configuración avanzada para iniciar su WorkSpace

Antes de empezar

Antes de empezar, asegúrese de tener una AWS cuenta que pueda usar para crear o administrar una WorkSpace. Los usuarios no necesitan una AWS cuenta para conectarse y usar su WorkSpaces.

Revise y comprenda los siguientes conceptos antes de continuar:

- Al lanzar un paquete WorkSpace, debes seleccionar un WorkSpace paquete. Para obtener más información, consulta Amazon WorkSpaces Bundles.
- Al lanzar un paquete WorkSpace, debe seleccionar qué protocolo (PCoIP o DCV) quiere usar con su paquete. Para obtener más información, consulte Protocolos para WorkSpaces uso personal.
- Al lanzar un WorkSpace, debe especificar la información del perfil del usuario, incluidos el nombre de usuario y la dirección de correo electrónico. Los usuarios completan sus perfiles

especificando una contraseña. La información sobre WorkSpaces los usuarios se almacena en un directorio. Para obtener más información, consulte the section called “Administre los directorios de WorkSpaces”.

Mediante la configuración avanzada para iniciar su WorkSpace

Para usar la configuración avanzada para iniciar su WorkSpace:

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Elija uno de los siguientes tipos de directorio y, a continuación, seleccione Siguiente:
   - AWS Microsoft AD gestionado
   - 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.

Crear un WorkSpace en WorkSpaces personal

WorkSpaces le permite aprovisionar escritorios Windows y Linux virtuales basados en la nube para sus usuarios, lo que se conoce como WorkSpaces.

Antes de crear un directorio personal WorkSpace, realice una de las siguientes acciones para crear un directorio:

- Crear un directorio de Simple AD.
- Cree un AWS Directory Service para Microsoft Active Directory, también conocido como 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.

- Cree un directorio dedicado que utilice Microsoft Entra ID como fuente de identidad (a través del Centro de identidades de IAM). WorkSpaces en el directorio están unidos a un ID de Entra nativo y están inscritos en Microsoft Intune a través del modo controlado por el usuario de Microsoft Windows Autopilot.

> **Note**
>
> Actualmente, estos directorios solo son compatibles con Windows 10 y 11 Bring Your Own Licenses personal. WorkSpaces

- Cree un directorio dedicado que utilice un proveedor de identidad de su elección como fuente de identidad (a través del Centro de identidades de IAM). WorkSpaces en el directorio están unidos a un ID de Entra nativo y están inscritos en Microsoft Intune a través del modo controlado por el usuario de Microsoft Windows Autopilot.

> **Note**
>
> Actualmente, estos directorios solo son compatibles con Windows 10 y 11 Bring Your Own Licenses personal. WorkSpaces

Ahora que ha creado un directorio, está listo para crear uno personal WorkSpace.

Para crear un personal WorkSpace

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Selecciona Launch WorkSpaces, Personal.
4. Elija Create (Creación de) WorkSpaces.
5. En Incorporación (opcional), puedes elegir Recomendarme opciones en función de mi caso de uso para recibir recomendaciones sobre el tipo de opciones WorkSpace que quieres usar. Puedes saltarte este paso si sabes que quieres usar el modo personal WorkSpaces.
6. Selecciona Siguiente. WorkSpaces registra su AD Connector.
7. En Configurar WorkSpaces, introduce los siguientes detalles:
   - En Bundle, elige entre las siguientes opciones el tipo de paquete que quieres usar para tu WorkSpaces.

- Usa un WorkSpaces paquete base: elige uno de los paquetes del menú desplegable. Para obtener más información sobre el tipo de paquete que ha seleccionado, elija Detalles del paquete. Para comparar los paquetes que se ofrecen para los grupos, elija Comparar todos los paquetes.
- Utilizar su propio paquete personalizado o de BYOL: elija un paquete que haya creado anteriormente. Para crear un paquete personalizado, consulte Crea una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal.

> **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, consulta Amazon WorkSpaces Bundles. Para obtener más información sobre las especificaciones de los paquetes, los usos recomendados y los precios, consulta WorkSpaces los precios de Amazon.

- Para el modo Running, elige una de las siguientes opciones para configurar tu disponibilidad personal WorkSpace inmediata y la forma de pagarla (mensual o por hora):
  - AlwaysOn— Factura una tarifa mensual por el uso ilimitado de su WorkSpaces. Este modo es el mejor para los usuarios que utilizan su escritorio principal a tiempo WorkSpace completo.
  - AutoStop— Facturas por hora. Con este modo, se WorkSpaces detiene después de un período específico de desconexión y se guarda el estado de las aplicaciones y los datos.
- En Etiquetas, especifique el valor del par de claves que desee usar. Una clave puede ser una categoría general, como "proyecto", "propietario" o "entorno", con valores específicos asociados.

8. En Seleccionar directorio, introduzca los siguientes detalles:
   - Elija el directorio que ha creado. Para crear un directorio, elija Crear directorio. Para obtener más información sobre cómo crear directorios personales, consulte Registrar un AWS Directory Service directorio existente con WorkSpaces Personal.
   - Elija los usuarios de ese directorio WorkSpaces para los que desee aprovisionar personal de la siguiente manera.
     1. Elija Creación de usuarios.

2. Introduzca las opciones Nombre de usuario, Nombre, Apellido y Correo electrónico del usuario. Para añadir usuarios adicionales, seleccione Crear usuario adicional e introduzca su información.

9. En Personalización (opcional), puede personalizar los paquetes, el cifrado del volumen raíz y de usuarios y el volumen de usuarios de todos los usuarios o de usuarios específicos.
10. Elija Crear WorkSpaces. El estado inicial de WorkSpace es PENDIENTE. Cuando haya terminado la creación, el estado es AVAILABLE y se envía una invitación a la dirección de correo electrónico que ha especificado para los usuarios.
11. Envíe invitaciones a la dirección de correo electrónico de cada usuario. Para obtener más información, consulte Enviar un correo electrónico de invitación.

> **Note**
>
> - Estas invitaciones no se envían automáticamente si se utiliza AD Connector o una relación de confianza.
> - 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.
> - En todas las regiones, el texto del correo electrónico de invitación está en inglés (EE. UU.). En las siguientes regiones, el texto en inglés va precedido de un segundo idioma:
> - Asia-Pacífico (Seúl): coreano
> - Asia-Pacífico (Tokio): japonés
> - Canadá (central): francés (canadiense)
> - China (Ningxia): chino simplificado

Conéctese al WorkSpace

Puede conectarse a su cuenta WorkSpace mediante el cliente que prefiera. Después de iniciar sesión, el cliente mostrará el WorkSpace escritorio.

Para conectarse al WorkSpace

1. Abra el enlace del correo electrónico de invitación.

2. Consulta WorkSpaces la Guía del WorkSpaces usuario de Amazon en la Guía del usuario de Amazon para obtener más información sobre los requisitos de cada cliente y, a continuación, sigue 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 Web Access.

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

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. (El ¿Ha olvidado su 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 personal.

Pasos a seguir a continuación

Puedes seguir personalizando la WorkSpace que acabas de crear. Por ejemplo, puede instalar software y, a continuación, crear un paquete personalizado a partir de su WorkSpace. También puede realizar diversas tareas administrativas para su WorkSpaces directorio WorkSpaces y el suyo. Si ha terminado con el suyo WorkSpace, puede eliminarlo. Para obtener más información, consulte la documentación siguiente.

- Crea una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal
- Administrar WorkSpaces personal
- Administrar directorios para WorkSpaces Personal
- Eliminar un archivo WorkSpace en WorkSpaces Personal

Para obtener más información sobre el uso de las aplicaciones WorkSpaces cliente, como la configuración de varios monitores o el uso de dispositivos periféricos, consulte WorkSpaces Clients and Peripheral Device Support en la Guía del WorkSpaces usuario de Amazon.

Protocolos de red y acceso para WorkSpaces personal

Como WorkSpace administrador, debe saber cómo administrar las WorkSpaces redes y el acceso, empezando por los protocolos.

Protocolos para WorkSpaces uso personal

Amazon WorkSpaces admite dos protocolos: PCo IP y DCV. El protocolo que elijas depende de varios factores, como el tipo de dispositivos WorkSpaces desde los que accederán los usuarios, el sistema operativo utilizado, las condiciones de red a las que se enfrentarán los usuarios y si los usuarios necesitan soporte de vídeo bidireccional. WorkSpaces

Requisitos

Los DCV 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)
- Agente de host Rocky Linux, versión 2.1.0.1628 o superior
- Agente de host de Red Hat Enterprise Linux, versión 2.1.0.1628 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)
- Cliente Ubuntu 22.04, versión 2024.x o superior
- Amazon WorkSpaces Thin Client (para obtener más información, consulte la documentación de Amazon WorkSpaces Thin Client)
- 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 DCV

- Si necesita una mayor loss/latency tolerancia para adaptarse a las condiciones de la red de sus usuarios finales. Por ejemplo, hay usuarios que acceden a sus redes 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 2022. WorkSpaces
- Si necesitas usar Ubuntu WorkSpaces.
- Si necesita usar Windows 11 BYOL WorkSpaces.
- Si necesitas usar paquetes basados en la GPU de Windows o Ubuntu (Graphics.G4DN y.g4dn). GraphicsPro
- Si necesita que sus usuarios se autentiquen durante la sesión con autenticadores como Windows Hello. WebAuthn YubiKey

Cuándo usar la IP PCo

- 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.
- Si necesita usarlo WorkSpaces en la región de China (Ningxia)

> **Note**
>
> - Un directorio puede contener una combinación de PCo IP y DCV WorkSpaces .
> - Un usuario puede tener una PCo IP y una DCV WorkSpace siempre que ambas WorkSpaces estén ubicadas en directorios separados. El mismo usuario no puede tener una PCo IP y un DCV WorkSpace en el mismo directorio. Para obtener más información sobre la creación de varios WorkSpaces para un usuario, consulteCrear varios WorkSpaces para un usuario en WorkSpaces Personal.
> - 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 archivo en WorkSpaces Personal.
> - Si lo WorkSpace creó con paquetes de PCo IP, puede modificar el protocolo de transmisión para migrar entre los dos protocolos sin necesidad de volver a construirlo 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 únicamente los paquetes Power PowerPro, GeneralPurpose .4xlarge o GeneralPurpose .8xlarge.

En los siguientes temas se ofrece información adicional sobre cómo administrar las redes y el acceso de Personal: WorkSpaces

Configurar una VPC para personal 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 Best Practices for VPCs and Networking in Amazon WorkSpaces Deployments y Best Practices for Deployment: WorkSpaces VPC Design.

Contenido

- Requisitos
- Configurar una VPC con subredes privadas y una gateway NAT
- Configurar una VPC con subredes públicas

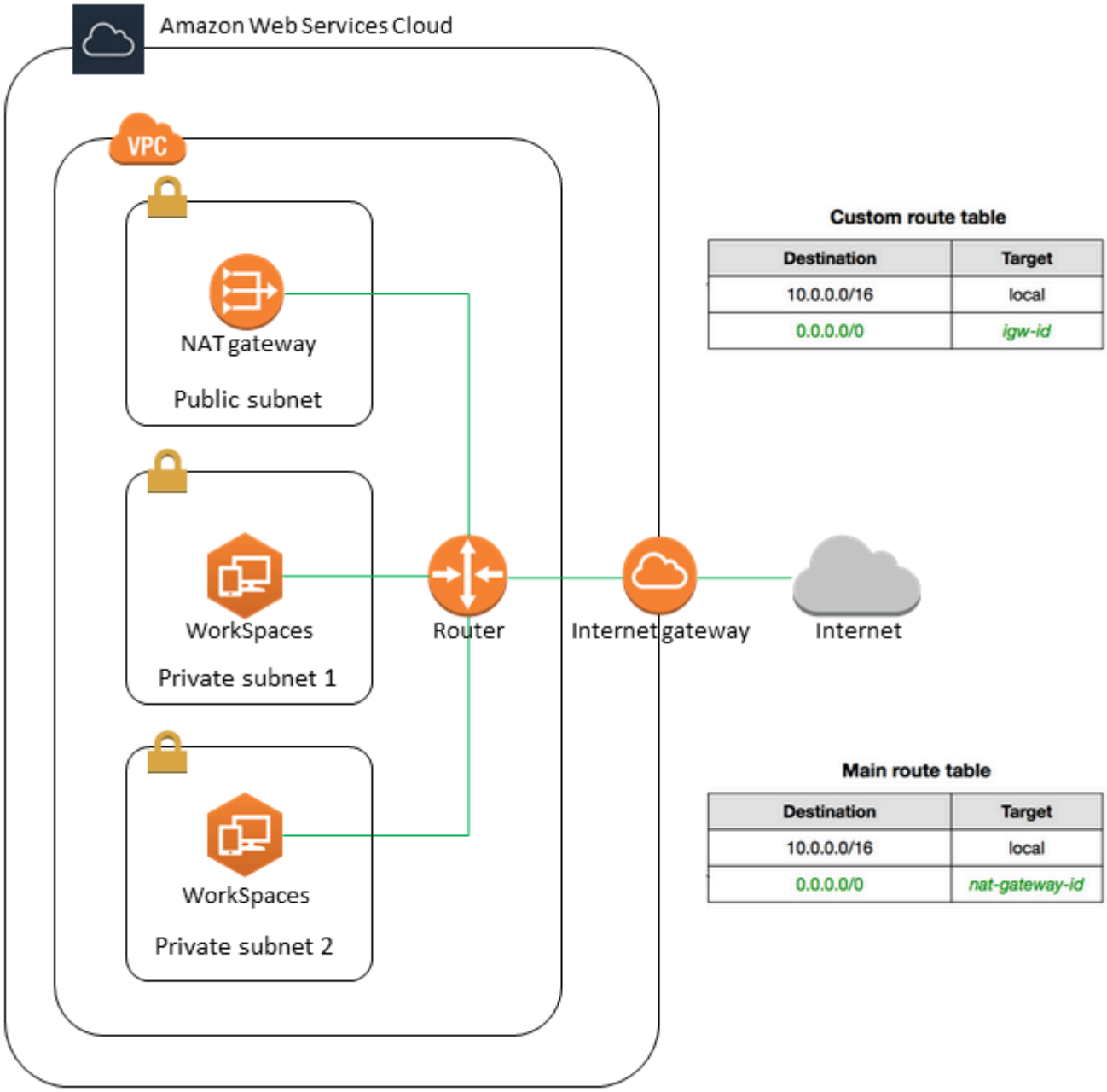
Requisitos

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 para WorkSpaces personal

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 Creación de 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 Personalice AZs y elija sus zonas de disponibilidad. De lo contrario AWS , selecciónelas por usted. Para hacer una selección apropiada, consulte Zonas de disponibilidad para WorkSpaces personal.
    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 Creación de VPC.

IPv6 Bloques CIDR

Puede asociar bloques IPv6 CIDR a su VPC y sus subredes. Sin embargo, si configura las subredes para que asignen IPv6 direcciones automáticamente a las instancias lanzadas en la subred, no podrá utilizar los paquetes de gráficos. (Sin embargo, puedes usar Graphics.G4dn, GraphicsPro .g4dn y paquetes). GraphicsPro Esta restricción se debe a una limitación de hardware de los tipos de instancias de la generación anterior que no son compatibles. IPv6

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

De forma predeterminada, la configuración de asignación automática de IPv6 direcciones está deshabilitada. 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 asignar direcciones IP elásticas de forma automática 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 Creación de 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 Personalice AZs y elija sus zonas de disponibilidad. De lo contrario AWS , selecciónelas por usted. Para hacer una selección apropiada, consulte Zonas de disponibilidad para WorkSpaces personal.
   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 Creación de VPC.

IPv6 Bloques CIDR

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

subred, no podrá usar paquetes de gráficos. (Sin embargo, puede usar GraphicsPro paquetes). Esta restricción se debe a una limitación de hardware de los tipos de instancias de la generación anterior que no son compatibles. IPv6

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

De forma predeterminada, la configuración de asignación automática de IPv6 direcciones está deshabilitada. 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Amplíe la fila (elija el icono de flecha) correspondiente a WorkSpace y anote el valor de WorkSpace IP. Esta es la dirección IP privada principal del WorkSpace.
4. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
5. En el panel de navegación, elige Elastic IPs. Si no tiene una dirección IP elástica disponible, elija Asignar dirección IP elástica y elija el grupo de direcciones de Amazon o el grupo de IPv4 direcciones propiedad del IPv4 cliente y, a continuación, elija Asignar. Anote la nueva dirección IP.
6. En el panel de navegación, elija Network Interfaces.
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 IPv4 dirección 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).

Configurar AWS Global Accelerator (AGA) para personal WorkSpaces

Puede activar AWS Global Accelerator (AGA) a nivel de WorkSpaces directorio o para WorkSpaces ejecutar individualmente el protocolo DCV. Cuando está activado, el servicio enruta automáticamente el tráfico de streaming a través de la ubicación AWS perimetral más cercana y a través de la red AWS global, de forma redundante y sin atascos. Esto ayuda a ofrecer una experiencia de streaming más estable y con mayor capacidad de respuesta. El WorkSpaces servicio gestiona completamente el uso de AGA y está sujeto a los límites de volumen de datos salientes.

Contenido

- Requisitos
- Limitaciones
- Límites de datos salientes
- Habilite AGA para un WorkSpaces directorio
- Habilite AGA para uso individual WorkSpaces

Requisitos

- WorkSpaces utilice una variedad de IPv4 direcciones públicas para los puntos finales dedicados de AWS Global Accelerator (AGA). Asegúrese de configurar las políticas de firewall para los dispositivos que acceden a WorkSpaces través de AGA. Si los puntos finales de AGA están bloqueados por el firewall, el tráfico de WorkSpaces streaming no se enrutará a través de AGA. Para obtener más información sobre los rangos de IP de los puntos finales de AGA en cada AWS región, consulte. Servidores de puerta de enlace de DCV
- Para acceder a WorkSpaces través de AGA, los usuarios deben utilizar las versiones de WorkSpaces cliente 5.23 o posteriores.

Limitaciones

- Solo puede habilitar AGA para DCV WorkSpaces . Si habilita AGA a nivel de WorkSpaces directorio, solo se aplicará al DCV WorkSpaces del directorio.
- No puede habilitar AGA en un directorio (o WorkSpaces en el directorio) que tenga habilitados los grupos de control de acceso IP y FIPS. Debe deshabilitar los grupos de control de acceso IP o FIPS antes de habilitar AGA en el directorio.

Límites de datos salientes

Los siguientes son los límites de volumen de datos aplicables a los WorkSpaces paquetes.

- Paquetes económicos, estándar y de rendimiento: incluyen 20 GB de datos salientes de AGA por usuario y mes.
- Paquetes de PowerPro energía y gráficos: incluyen 50 GB de datos salientes AGA por usuario y mes.

Estos límites de datos salientes están destinados a cubrir el uso de datos de los usuarios que transmiten desde sus. WorkSpaces Más allá de estos límites, el WorkSpaces servicio podría restringir el uso de AGA y dirigir WorkSpaces el tráfico fuera de AGA de case-by-case forma ocasional.

Habilite AGA para un WorkSpaces directorio

Puede configurar los ajustes de AGA a nivel de directorio. La configuración se aplicará a todos los DCV WorkSpaces del directorio, a menos que la persona la anule. WorkSpaces

Para habilitar AGA en un directorio

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. En la columna ID de directorio, elija el ID de directorio del directorio para el que desee configurar los ajustes de AGA.
4. En la página de detalles del directorio, desplácese hacia abajo hasta la sección de configuración de AWS Global Accelerator (AGA) y seleccione Editar.
5. Seleccione Activar AGA (automático).

6. Usar siempre TCP con AGA está seleccionada de forma predeterminada. Si deselecciona esta opción, el WorkSpaces cliente determinará si se utiliza TCP o UDP con AGA en función de la configuración del protocolo de streaming DCV de sus clientes.
7. Seleccione Save.

Después de habilitar AGA para un WorkSpaces directorio, el DCV WorkSpaces del directorio utilizará AGA para la transmisión a partir de la siguiente sesión. No es necesario reiniciar.

Habilite AGA para uso individual WorkSpaces

Puede configurar los ajustes de AGA de forma individual WorkSpaces, lo que anula los ajustes heredados del directorio al que WorkSpaces están asociados.

Para habilitar AGA para usuarios individuales WorkSpaces

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación WorkSpaces, selecciona Personal.
3. En la columna WorkSpace ID, selecciona el WorkSpace ID de la WorkSpace que deseas configurar los ajustes de AGA.
4. En la página de WorkSpaces detalles, desplácese hacia abajo hasta la sección de configuración de AWS Global Accelerator (AGA) y seleccione Editar.
5. Para ello, seleccione Anular manualmente las configuraciones de AGA. WorkSpace
6. Seleccione Activar AGA (automático).
7. Usar siempre TCP con AGA está seleccionada de forma predeterminada. Si deselecciona esta opción, el WorkSpaces cliente determinará si se utiliza TCP o UDP con AGA en función de la configuración del protocolo de streaming DCV de sus clientes.
8. Seleccione Save.

Zonas de disponibilidad para WorkSpaces personal

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.

Ver la zona de disponibilidad IDs 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 muestran las zonas de disponibilidad IDs que puede utilizar para cada región. Para ver la asignación de las zonas de disponibilidad IDs a las zonas de disponibilidad de tu cuenta, consulta la IDs sección AZ para tus recursos en la Guía del AWS RAM usuario.

Nombre de región	Código de región	AZ compatible IDs
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`

Nombre de región	Código de región	AZ compatible IDs
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`
Europa (París)	`eu-west-3`	`euw3-az1`, `euw3-az2`, `euw3-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`
AWS GovCloud (EE. UU.-Oeste)	`us-gov-west-1`	`usgw1-az1` , `usgw1-az2` , `usgw1-az3`
AWS GovCloud (EE. UU.-Este)	`us-gov-east-1`	`usge1-az1` , `usge1-az2` , `usge1-az3`

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

Requisitos de dirección IP y puerto para WorkSpaces Personal

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 según la AWS región. Estos

puertos también deben estar abiertos en los firewalls que se ejecuten en el cliente. Para obtener más información sobre los rangos de direcciones AWS IP de las distintas regiones, consulte AWS Intervalos de direcciones IP en Referencia general de Amazon Web Services.

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 (UDP y 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 de la PCo IP WorkSpaces. Este puerto debe estar abierto a la puerta de enlace PCo IP 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 PCoServidores de puerta de enlace IP.

En el PCo caso de IP WorkSpaces, las aplicaciones cliente de escritorio no admiten el uso de un servidor proxy ni el descifrado mediante TLS ni la inspección 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 DCV. WorkSpaces Este puerto debe estar abierto a los rangos de direcciones IP de la puerta de enlace DCV 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 de DCV.

Para DCV 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 función 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.
> - La aplicación WorkSpaces cliente primero intenta transmitir mediante UDP (QUIC) para obtener un rendimiento óptimo. Si la red del cliente solo permite el TCP, se utilizará el TCP. El cliente WorkSpaces web se conectará a través del puerto TCP 4195 o 443. Si el puerto 4195 está bloqueado, el cliente solo intentará conectarse a través del puerto 443.

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 DCV, este puerto se utiliza 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 DCV. Para obtener más información, consulte Servidores de puerta de enlace de DCV.

El acceso web a DCV 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 o 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 aplicación WorkSpaces cliente primero intenta transmitir mediante UDP (QUIC) para obtener un rendimiento óptimo. Si la red del cliente solo permite el TCP, se utilizará el TCP. El cliente WorkSpaces web se conectará a través del puerto TCP 4195 o 443. Si el puerto 4195 está bloqueado, el cliente solo intentará conectarse a través del puerto 443.

Por lo general, el navegador web selecciona aleatoriamente un puerto de origen en el rango alto para usarlo en la transmisión de tráfico. 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/ https://opfcaptcha-prod.s3.cn-north-1.amazonaws.com
Actualización automática del cliente	• https://d2td7dqidlhjx7.cloudfront.net/ • En la región AWS GovCloud (EEUU-Oeste): https://d2td7dqidlhjx7.cloudfront. net/prod/pdt/windows/WorkSpacesAppCastx64.xml
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominios (IPv4): • https://skylight-client-ds.us-east-1.amazonaws.com

Categoría	Dominio o dirección IP
	• https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-south-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com • https://skylight-client-ds.ca-central-1.amazonaws.com • https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.eu-west-3.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • En la región AWS GovCloud (EE. UU.-Oeste):

Categoría	Dominio o dirección IP
	https://skylight-client-ds.us-gov-west-1.amazonaws.com • En la región AWS GovCloud (EEUU-Este): https://skylight-client-ds.us-gov-east-1.amazonaws.com • En la región AWS GovCloud (EEUU-Oeste): https://skylight-client-ds.us-gov-west-1.amazonaws.com • En la región AWS GovCloud (EEUU-Este): https://skylight-client-ds.us-gov-east-1.amazonaws.com Dominios (IPv6): • skylight-client-dshttps://.eu-west-2.api.aws • skylight-client-dshttps://.eu-west-1.api.aws • skylight-client-dshttps://.us-east-1.api.aws • skylight-client-dshttps://.ap-southeast-1.api.aws • skylight-client-dshttps://.sa-east-1.api.aws • skylight-client-dshttps://.ap-northeast-1.api.aws • skylight-client-dshttps://.us-west-2.api.aws • skylight-client-dshttps://.ap-southeast-2.api.aws • skylight-client-dshttps://.ap-south-1.api.aws • skylight-client-dshttps://.af-south-1.api.aws • skylight-client-dshttps://.eu-central-1.api.aws

Categoría	Dominio o dirección IP
	• skylight-client-dshttps://.ap-northeast-2.api .aws • skylight-client-dshttps://.il-central-1.api.aws • skylight-client-dshttps://.ca-central-1.api.aws • httpsskylight-client-ds://. us-gov-east-1.api. aws • https://. skylight-client-ds us-gov-west-1.api. aws

Categoría	Dominio o dirección IP
Servicio de mensajería dinámica (para aplicaciones cliente de 3.0 WorkSpaces o más)	Dominios (IPv4): • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • https://ws-client-service.ap-south-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • https://ws-client-service.eu-west-1.amazonaws.com • https://ws-client-service.eu-west-2.amazonaws.com • https://ws-client-service.eu-west-3.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com

Categoría	Dominio o dirección IP
	• En la región AWS GovCloud (EE. UU.-Oeste): https://ws-client-service.us-gov-west-1.amazonaws.com • En la región AWS GovCloud (EEUU-Este): https://ws-client-service.us-gov-east-1.amazonaws.com Dominios (): IPv6 • ws-client-servicehttps://.eu-west-2.api.aws • ws-client-servicehttps://.eu-west-1.api.aws • https://ws-client-service.us-east-1.amazonaws.com • ws-client-servicehttps://.ap-southeast-1.api.aws • ws-client-servicehttps://.sa-east-1.api.aws • ws-client-servicehttps://.ap-northeast-1.api.aws • ws-client-servicehttps://.us-west-2.api.aws • ws-client-servicehttps://.ap-southeast-2.api.aws • ws-client-servicehttps://.ap-south-1.api.aws • ws-client-servicehttps://.af-south-1.api.aws • ws-client-servicehttps://.eu-central-1.api.aws • ws-client-servicehttps://.ap-northeast-2.api.aws • ws-client-servicehttps://.il-central-1.api.aws • ws-client-servicehttps://.ca-central-1.api.aws

Categoría	Dominio o dirección IP
	• httpsws-client-service://. us-gov-east-1.api.aws • https://. ws-client-service us-gov-west-1.api.aws

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/*<region>*/*<directory ID>* 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/ • Europa (París) — https://d2kmf63k5sit88.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/

Categoría	Dominio o dirección IP
	• Asia-Pacífico (Bombay): https://d78hovzzqqtsb.cloudfront.net/ • 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/ • Europa (París) — https://d1a3pnge9on3sx.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 la región (EEUU-Oeste): AWS GovCloud • Configuración de directorios de clientes: https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/ <directory ID>

Categoría	Dominio o dirección IP
	• Gráficos de la página de inicio de sesión de la marca compartida en el nivel del directorio del cliente: https://workspace-client-assets-pdt.s3-us-gov-west-1.amazonaws.com • Archivo CSS para el estilo de las páginas de inicio de sesión: https://s3.amazonaws.com/workspaces-clients-css/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/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://workspace-client-assets-pdt.s3-us-gov-east-1.amazonaws.com • Archivo CSS para el estilo de las páginas de inicio de sesión: https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript archivo para las páginas de inicio de sesión:

Categoría	Dominio o dirección IP
	No aplicable
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado

Categoría	Dominio o dirección IP
Puntos de conexión de autenticación con tarjeta inteligente anteriores a la sesión	• https://smartcard.af-south-1.signin.aws • https://smartcard.af-south-1.apps.signin.aws • https://smartcard.ap-south-1.signin.aws • https://smartcard.ap-south-1.apps.signin.aws • https://smartcard.ap-southeast-1.signin.aws • https://smartcard.ap-southeast-1.apps.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-southeast-2.apps.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.ap-northeast-1.apps.signin.aws • https://smartcard.ap-northeast-2.signin.aws • https://smartcard.ap-northeast-2.apps.signin.aws • https://smartcard.ca-central-1.signin.aws • https://smartcard.ca-central-1.apps.signin.aws • https://smartcard.eu-central-1.signin.aws • https://smartcard.eu-central-1.apps.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.eu-west-1.apps.signin.aws • https://smartcard.eu-west-2.signin.aws • https://smartcard.eu-west-2.apps.signin.aws • https://smartcard.eu-west-3.signin.aws • https://smartcard.eu-west-3.apps.signin.aws • https://smartcard.il-central-1.signin.aws • https://smartcard.il-central-1.apps.signin.aws

Categoría	Dominio o dirección IP
	• https://smartcard.sa-east-1.signin.aws • https://smartcard.sa-east-1.apps.signin.aws • https://smartcard.us-east-1.signin.aws • https://smartcard.us-east-1.apps.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.us-west-2.apps.signin.aws • https://smartcard.us-gov-east-1.signin-fips.amazonaws-us-gov.com • https://smartcard.us-gov-east-1.apps.signin-fips.amazonaws-us-gov.com • https://smartcard.us-gov-west-1.signin.amazonaws-us-gov.com • https://smartcard.us-gov-west-1.apps.signin.amazonaws-us-gov.com • https://smartcard.signin.amazonaws-us-gov.com

Categoría	Dominio o dirección IP
Páginas de inicio de sesión del usuario	• https://af-south-1.signin.aws • https://af-south-1.signin.aws.amazon.com • https://af-south-1.sso.signin.aws • https://af-south-1.apps.signin.aws • https://ap-south-1.signin.aws • https://ap-south-1.signin.aws.amazon.com • https://ap-south-1.sso.signin.aws • https://ap-south-1.apps.signin.aws • https://ap-southeast-1.signin.aws • https://ap-southeast-1.signin.aws.amazon.com • https://ap-southeast-1.sso.signin.aws • https://ap-southeast-1.apps.signin.aws • https://ap-southeast-2.signin.aws • https://ap-southeast-2.signin.aws.amazon.com • https://ap-southeast-2.sso.signin.aws • https://ap-southeast-2.apps.signin.aws • https://ap-northeast-1.signin.aws • https://ap-northeast-1.signin.aws.amazon.com • https://ap-northeast-1.sso.signin.aws • https://ap-northeast-1.apps.signin.aws • https://ap-northeast-2.signin.aws • https://ap-northeast-2.signin.aws.amazon.com • https://ap-northeast-2.sso.signin.aws • https://ap-northeast-2.apps.signin.aws • https://ca-central-1.signin.aws

Categoría	Dominio o dirección IP
	• https://ca-central-1.signin.aws.amazon.com • https://ca-central-1.sso.signin.aws • https://ca-central-1.apps.signin.aws • https://eu-central-1.signin.aws • https://eu-central-1.signin.aws.amazon.com • https://eu-central-1.sso.signin.aws • https://eu-central-1.apps.signin.aws • https://eu-west-1.signin.aws • https://eu-west-1.signin.aws.amazon.com • https://eu-west-1.sso.signin.aws • https://eu-west-1.apps.signin.aws • https://eu-west-2.signin.aws • https://eu-west-2.signin.aws.amazon.com • https://eu-west-2.sso.signin.aws • https://eu-west-2.apps.signin.aws • https://eu-west-3.signin.aws • https://eu-west-3.signin.aws.amazon.com • https://eu-west-3.sso.signin.aws • https://eu-west-3.apps.signin.aws • https://il-central-1.signin.aws • https://il-central-1.signin.aws.amazon.com • https://il-central-1.sso.signin.aws • https://il-central-1.apps.signin.aws • https://sa-east-1.signin.aws • https://sa-east-1.signin.aws.amazon.com • https://sa-east-1.sso.signin.aws • https://sa-east-1.apps.signin.aws • https://us-east-1.signin.aws • https://us-east-1.signin.aws.amazon.com

Categoría	Dominio o dirección IP
	• https://us-east-1.sso.signin.aws • https://us-east-1.apps.signin.aws • https://us-west-2.signin.aws • https://us-west-2.signin.aws.amazon.com • https://us-west-2.sso.signin.aws • https://us-west-2.apps.signin.aws • https://us-gov-east-1.signin-fips.amazonaws-us-gov.com • https://us-gov-east-1.sso.signin-fips.aws-us-gov.com • https://us-gov-east-1.apps.signin-fips.aws-us-gov.com • https://us-gov-west-1.signin.amazonaws-us-gov.com • https://us-gov-west-1.sso.signin.aws-us-gov.com • https://us-gov-west-1.apps.signin.aws-us-gov.com *directory_id* https://.awsapps.com/ Note el identificador 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.awsapps.com/directory/*directory id*/

Categoría	Dominio o dirección IP
	Note el identificador del directorio es el dominio del cliente.

Categoría	Dominio o dirección IP
Agente de WS	Dominios (IPv4): • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com • https://ws-broker-service.ap-south-1.amazonaws.com • https://ws-broker-service.ap-northeast-2.amazonaws.com • https://ws-broker-service.ap-southeast-1.amazonaws.com • https://ws-broker-service.ap-southeast-2.amazonaws.com • https://ws-broker-service.ap-northeast-1.amazonaws.com • https://ws-broker-service.ca-central-1.amazonaws.com • https://ws-broker-service.eu-central-1.amazonaws.com • https://ws-broker-service.eu-west-1.amazonaws.com • https://ws-broker-service.eu-west-2.amazonaws.com • https://ws-broker-service.eu-west-3.amazonaws.com • https://ws-broker-service.sa-east-1.amazonaws.com

Categoría	Dominio o dirección IP
	• https://ws-broker-service.af-south-1.amazonaws.com • https://ws-broker-service.il-central-1.amazonaws.com • https://ws-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 Dominios (): IPv6 • ws-broker-servicehttps://.eu-west-3.api.aws • ws-broker-servicehttps://.eu-west-2.api.aws • ws-broker-servicehttps://.eu-west-1.api.aws • ws-broker-servicehttps://.us-east-1.api.aws • ws-broker-servicehttps://.us-west-2.api.aws • ws-broker-servicehttps://.eu-central-1.api.aws • ws-broker-servicehttps://.ap-northeast-1.api.aws • ws-broker-servicehttps://.ap-northeast-2.api.aws • ws-broker-servicehttps://.ap-southeast-1.api.aws • ws-broker-servicehttps://.ap-southeast-2.api.aws • ws-broker-servicehttps://.sa-east-1.api.aws • ws-broker-servicehttps://.ap-south-1.api.aws

Categoría	Dominio o dirección IP
	• ws-broker-servicehttps://.af-south-1.api.aws • ws-broker-servicehttps://.ca-central-1.api.aws • ws-broker-servicehttps://.il-central-1.api.aws • httpsws-broker-service://. us-gov-west-1.api.aws • https://. ws-broker-service us-gov-east-1.api.aws • ws-broker-service-fipshttps://.us-west-2.api.aws • ws-broker-service-fipshttps://.us-east-1.api.aws • httpsws-broker-service-fips://. us-gov-west-1.api.aws • https://. ws-broker-service-fips us-gov-east-1.api.aws

Categoría	Dominio o dirección IP
WorkSpaces Puntos finales de la API	Dominios (IPv4): • 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.eu-west-3.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com

Categoría	Dominio o dirección IP
	• https://workspaces.af-south-1.amazonaws.com • 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 Dominios (): IPv6 • https://workspaces.eu-west-3.api.aws • https://workspaces.eu-west-2.api.aws • https://workspaces.eu-west-1.api.aws • https://workspaces.us-east-1.api.aws • https://workspaces.us-west-2.api.aws • https://workspaces.eu-central-1.api.aws • https://workspaces.ap-northeast-1.api.aws • https://workspaces.ap-northeast-2.api.aws • https://workspaces.ap-southeast-1.api.aws • https://workspaces.ap-southeast-2.api.aws • https://workspaces.sa-east-1.api.aws • https://workspaces.ap-south-1.api.aws • https://workspaces.af-south-1.api.aws • https://workspaces.ca-central-1.api.aws • https://workspaces.il-central-1.api.aws • https://workspaces. us-gov-west-1.api.aws

Categoría	Dominio o dirección IP
	• https://workspaces. us-gov-east-1.api.aws • https://workspaces-fips.us-west-2.api.aws • https://workspaces-fips.us-east-1.api.aws • https://workspaces-fips. us-gov-west-1.api.aws • https://workspaces-fips. us-gov-east-1.api.aws

Categoría	Dominio o dirección IP
WorkSpaces Puntos de conexión para el inicio de sesión único (SSO) de SAML	Dominios: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-latido • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-latido • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-latido • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-latido • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-latido • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-latido • https://euc-sso-sm.eu-west-3.amazonaws.com/v1/report-latido • https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-latido • https://euc-sso-sm.us-gov-west-1.amazonaws.com/v1/report-latido

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

Dominios y direcciones IP para añadir a tu lista de direcciones IP permitidas PCo

Categoría	Dominio o dirección IP
PCoPuerta de enlace de sesión IP (PSG)	PCoServidores de puerta de enlace IP
Agente de sesiones (PCM)	Dominios (IPv4): • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.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

Categoría	Dominio o dirección IP
	• https://skylight-cm.ca-central-1.amazonaws.com • 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.eu-west-3.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 Dominios ()IPv6: • https://skylight-cm.us-east-1.api.aws • https://skylight-cm.us-west-2.api.aws • https://skylight-cm.eu-west-3.api.aws • https://skylight-cm.eu-west-2.api.aws • https://skylight-cm.eu-west-1.api.aws

Categoría	Dominio o dirección IP
	• https://skylight-cm.eu-central-1.api.aws • https://skylight-cm.ap-northeast-1.api.aws • https://skylight-cm.ap-northeast-2.api.aws • https://skylight-cm.ap-southeast-1.api.aws • https://skylight-cm.ap-southeast-2.api.aws • https://skylight-cm.ap-south-1.api.aws • https://skylight-cm.sa-east-1.api.aws • https://skylight-cm.af-south-1.api.aws • https://skylight-cm.ca-central-1.api.aws • https://skylight-cm.il-central-1.api.aws • https://skylight-cm. us-gov-west-1.api.aws • https://skylight-cm. us-gov-east-1.api.aws • skylight-cm-fipshttps://.us-west-2.api.aws • skylight-cm-fipshttps://.us-east-1.api.aws • httpsskylight-cm-fips://. us-gov-west-1.api.aws • https://. skylight-cm-fips us-gov-east-1.api.aws

Categoría	Dominio o dirección IP
Servidores TURN de acceso web para IP PCo	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 • Web Access no está disponible actualmente en la región de África (Ciudad del Cabo). • Web Access no está disponible actualmente en la región de Israel (Tel Aviv).

Dominios y direcciones IP para añadir a la lista de permitidos de DCV

Categoría	Dominio o dirección IP
Puerta de enlace de sesión DCV (WSG)	Servidores de puerta de enlace de DCV
Servidores TURN de Web Access para DCV	Servidores de puerta de enlace de DCV

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 (Mumbai)	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 52.78.44.253 52.79.54.102

Región	El nombre del host de comprobación de estado	Direcciones IP
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
Europa (Irlanda)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224

Región	El nombre del host de comprobación de estado	Direcciones IP
Europa (Londres)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
Europa (París)	drp-cdg.amazonworkspaces.com	51.17.52.90 51,17109231 51,16190,43
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/	51,17,5,90 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 (Estados Unidos-Este)	drp-osu.amazonworkspaces.com	18.253,251,70 18,254,0118

PCoServidores de puerta de enlace IP

WorkSpaces utiliza PCo IP para transmitir la sesión de escritorio a los clientes a través del puerto 4172. Para sus servidores de puerta de enlace PCo IP, WorkSpaces utiliza un pequeño rango de IPv6 direcciones EC2 IPv4 AND públicas de Amazon. Esto permite establecer políticas de firewall más detalladas para los dispositivos que obtienen acceso a WorkSpaces. Tenga en cuenta que el WorkSpaces cliente prioriza las IPv6 conexiones cuando es compatible y se IPv6 puede acceder a las puertas de enlace. Si no IPv6 está disponible, vuelve a. IPv4

Región	Código de región	Intervalo de direcciones IP públicas
Este de EE. UU. (Norte de Virginia)	us-east-1	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255 2600:1 o 32:8000: :/39
Oeste de EE. UU. (Oregón)	us-west-2	35.80.88.0 - 35.80.95.255

Región	Código de región	Intervalo de direcciones IP públicas
		44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255 2600:1 o 32:4000: :/39
Asia-Pacífico (Bombay)	ap-south-1	13.126.243.0 - 13.126.243.255 2406: da32:a000: :/40
Asia-Pacífico (Seúl)	ap-northeast-2	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255 2406: da 32:2000: :/40
Asia-Pacífico (Singapur)	ap-southeast-1	18.141.152,0 - 18.141.152.255 18.141.154,0 - 18.141.155.255 52.76.127.0 - 52.76.127.255 2406:da 32:8000: :/40
Asia-Pacífico (Sídney)	ap-southeast-2	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255 2406:da32:c000: :/40

Región	Código de región	Intervalo de direcciones IP públicas
Asia-Pacífico (Tokio)	ap-northeast-1	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255 2406:da 32:4000: :/40
Canadá (centro)	ca-central-1	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255 2600:1 o 32:1000: :/40
Europa (Fráncfort)	eu-central-1	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255 2a05:d 032:4000: :/40
Europa (Irlanda)	eu-west-1	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255 2a05:d 032:8000: :/40
Europa (Londres)	eu-west-2	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255 2a05:d032:c000: :/40
Europa (París)	eu-west-3	5144,204,0-51,44.207255

Región	Código de región	Intervalo de direcciones IP públicas
América del Sur (São Paulo)	sa-east-1	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255 2600:1 f32:e000:/40
África (Ciudad del Cabo)	af-south-1	13.246.120.0 - 13.246.123.255 2406:da 32:1000: :/40
Israel (Tel Aviv)	il-central-1	51.17.28.0-51.17.31.255 2a05:d 032:5000: :/40
AWS GovCloud (US-Oeste)	us-gov-west-1	52.61.193.0 - 52.61.193.255 2600:1 o 32:2000: :/40
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	18.254.140.0 - 18.254.143.255 2600:1 o 32:5000: :/40

Servidores de puerta de enlace de DCV

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

> **Note**
>
> En el caso de los WorkSpaces grupos que no son de BYOL, no se garantizan los rangos de direcciones IP. En su lugar, debe permitir incluir en la lista los nombres de dominio de la

puerta de enlace DCV. Para obtener más información, consulte Nombres de dominio de la puerta de enlace DCV.

WorkSpaces utiliza un pequeño rango de IPv6 direcciones IPv4 y EC2 públicas de Amazon para sus servidores de puerta de enlace DCV. Esto le permite establecer políticas de firewall más precisas para los dispositivos a los que acceden. WorkSpaces WorkSpaces utilice un rango diferente de IPv4 direcciones públicas para los puntos finales dedicados de AWS Global Accelerator (AGA). Asegúrese de configurar sus políticas de firewall para incluir en una lista los rangos de IP permitidos si planea habilitar AGA para su servidor. WorkSpaces Tenga en cuenta que el WorkSpaces cliente prioriza las IPv6 conexiones cuando es compatible y se puede IPv6 acceder a las puertas de enlace. Si no IPv6 está disponible, vuelve a. IPv4

Si usa AGA + IPv6, debe incluir en la lista de permitidos los rangos IPv6 CIDR de los `GLOBALACCELERATOR` rangos. Consulte la ubicación y los rangos de direcciones IP de los servidores Global Accelerator Edge en la Guía para desarrolladores de AWS Global Accelerator para obtener más información.

Región	Código de región	Intervalo de direcciones IP públicas
Este de EE. UU. (Norte de Virginia)	us-east-1	• 3.227.4.0/22 • 44.209.84.0/22 • 93.77.138.0/24 (puntos finales AGA) • 93.77.139.0/24 (puntos de valoración AGA) • 2600:1 de 28:34 c: :/48
Este de EE. UU. (Ohio)	us-east-2	• 3.146.84.0/22 • 93.77.130.0/24 (puntos finales de AGA) • 93.77.131.0/24 (puntos de valoración AGA) • 2600:1 de 26:28::/48

Región	Código de región	Intervalo de direcciones IP públicas
Oeste de EE. UU. (Oregón)	us-west-2	• 34.223.96.0/22 • 93.77.148.0/24 (puntos finales de AGA) • 93.77.149.0/24 (puntos de valoración AGA) • 2600:1 de 24:34::/48
Asia-Pacífico (Bombay)	ap-south-1	• 65.1.156.0/22 • 93.77.142.0/24 (puntos finales de AGA) • 93.77.143.0/24 (puntos finales AGA) • 2406:da2a:14: :/48
Asia-Pacífico (Seúl)	ap-northeast-2	• 3.35.160.0/22 • 93.77.156.0/24 (puntos finales de AGA) • 93.77.157.0/24 (puntos de valoración AGA) • 2406:da 22:4: :/48
Asia-Pacífico (Singapur)	ap-southeast-1	• 13.212.132.0/22 • 93.77.158.0/24 (puntos finales de AGA) • 93.77.159.0/24 (puntos de valoración AGA) • 2406:da 28:28:/48

Región	Código de región	Intervalo de direcciones IP públicas
Asia-Pacífico (Sídney)	ap-southeast-2	• 3.25.248.0/22 • 93.77.150.0/24 (puntos finales de AGA) • 93.77.151.0/24 (puntos de valoración AGA) • 2406:da2c:24: :/48
Asia-Pacífico (Tokio)	ap-northeast-1	• 3.114.164.0/22 • 93.77.134.0/24 (puntos finales de AGA) • 93.77.135.0/24 (puntos de valoración AGA) • 2406:da 24:28: :/48
Canadá (centro)	ca-central-1	• 3.97.20.0/22 • 93.77.128.0/24 (puntos finales de AGA) • 93.77.129.0/24 (puntos de valoración AGA) • 2600:1 de 21:8::/48
Europa (Fráncfort)	eu-central-1	• 18.192.216.0/22 • 93.77.154.0/24 (puntos finales de AGA) • 93.77.155.0/24 (puntos de valoración AGA) • 2a05:d 024:18::/48

Región	Código de región	Intervalo de direcciones IP públicas
Europa (Irlanda)	eu-west-1	• 3.248.176.0/22 • 93.77.132.0/24 (puntos finales de AGA) • 93.77.133.0/24 (puntos de valoración AGA) • 2a 05:d 028:40: :/48
Europa (Londres)	eu-west-2	• 18.134.68.0/22 • 93.77.140.0/24 (puntos finales de AGA) • 93.77.141.0/24 (puntos de valoración AGA) • 2a 05: d02c: 8: /48
Europa (París)	eu-west-3	• 51.44.72.0/22 • 93.77.144.0/24 (puntos finales de AGA) • 93.77.145.0/24 (puntos de valoración AGA) • 2a05:d 02:1 c: :/48
América del Sur (São Paulo)	sa-east-1	• 15.228.64.0/22 • 93.77.146.0/24 (puntos finales de AGA) • 93.77.147.0/24 (puntos de valoración AGA) • 2600:1 f2e:14::/48

Región	Código de región	Intervalo de direcciones IP públicas
África (Ciudad del Cabo)	af-south-1	• 13.246.108.0/22 • 93.77.136.0/24 (puntos finales de AGA) • 93.77.137.0/24 (puntos de valoración AGA) • 2406:da21:c: :/48
Israel (Tel Aviv)	il-central-1	• 51.17.72.0/22 • 93.77.152.0/24 (puntos finales de AGA) • 93.77.153.0/24 (puntos de valoración AGA) • 2a 05:d 025:1000: :/48
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23 • 2600:1 de 22:28:/48
AWS GovCloud (EEUU-Este)	us-gov-east-1	• 18.254.148.0/22 • 2600:1 de 25:14: :/48

Nombres de dominio de la puerta de enlace de DCV

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

Región	Dominio
Este de EE. UU. (Norte de Virginia)	• *.prod.us-east-1.highlander.aws.a2z.com

Región	Dominio
	• (FIPS) *.wsp-fips.prod.us-east-1.highlander.aws.a2z.com
Oeste de EE. UU. (Oregón)	• *.prod.us-west-2.highlander.aws.a2z.com • (FIPS) *.wsp-fips.prod.us-west-2.highlander.aws.a2z.com
Asia-Pacífico (Mumbai)	*.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
Europa (París)	*.prod.eu-west-3.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 (EEUU-Oeste)	• *.prod. us-gov-west-1.highlander.aws.a2z.com • (FIPS) *.wsp-fips.prod. us-gov-west-1.highlander.aws.a2z.com

Región	Dominio
AWS GovCloud (Este de EE. UU.)	• *.prod. us-gov-east-1.highlander.aws.a2z.com • (FIPS) *.wsp-fips.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, la PCo IP BYOL 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 DCV BYOL, los rangos de direcciones IP WorkSpaces 54.239.224.0/20 y 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 el DCV 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 que se muestran en la siguiente tabla. PCoIP/DCV

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 (Mumbai)	PCoIP/WSP: 192.168.0.0/16

Región	Rango de direcciones IP
	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
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
Europa (París)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

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

Puertos de la interfaz de administración

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

- TCP de entrada en el puerto 4172. Se utiliza para establecer la conexión de streaming en el protocolo PCo IP.
- UDP de entrada en el puerto 4172. Se utiliza para transmitir las entradas del usuario en el protocolo PCo IP.
- 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 transmisión y para transmitir las entradas del usuario en el protocolo DCV.
- UDP de entrada en el puerto 8220. Este puerto se utiliza para establecer la conexión de transmisión y para transmitir las entradas del usuario en el protocolo DCV.

- 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. 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 DCV 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. En el caso de un directorio Simple AD, el grupo de seguridad creado por AWS Directory Service tendrá estos puertos configurados correctamente. 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 over TLS/SSL)
  - TCP 1024-65535: puertos dinámicos para RPC
  - TTCP 3268-3269: catálogo global

  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/

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

Categoría	Detalles
Configuración de directorios	Autenticación del cliente al 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 de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.us-east-1.signin.aws
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com
WorkSpaces Puntos finales de API	Dominios: https://workspaces.us-east-1.amazonaws.com
Agente de sesiones (PCM)	Dominios: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com
Servidores TURN de acceso web para IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	• 3.227.4.0/22 • 44.209.84.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.us-west-2.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.us-west-2.amazonaws.com

Categoría	Detalles
Configuración de directorios	Autenticación del cliente al 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 de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.us-west-2.signin.aws
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com
WorkSpaces Puntos finales de 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://skylight-cm-fips.us-west-2.amazonaws.com
Servidores TURN de acceso web para IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	34.223.96.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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 (Mumbai)

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

Categoría	Detalles
Configuración de directorios	Autenticación del cliente al 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.ap-south-1.amazonaws.com
WorkSpaces Puntos finales de API	Dominio: • https://workspaces.ap-south-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.ap-south-1.amazonaws.com
Servidores TURN de acceso web para IP PCo	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	• 13.127.57.82 • 13,234250,73
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	13.126.243.0 - 13.126.243.255
Intervalo de direcciones IP de los servidores de puerta de enlace de DCV	65.1.156.0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace de DCV	*.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 1.0+ y 2.0+) WorkSpaces	https://device-metrics-us-2.amazon.com/
Métricas de clientes (para aplicaciones cliente de 3.0 o más) WorkSpaces	Dominio: https://skylight-client-ds.ap-northeast-2.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.ap-northeast-2.amazonaws.com
Configuración de directorios	Autenticación del cliente al directorio de clientes antes de iniciar sesión en WorkSpace: • https://d32i4gd7pg4909.cloudfront.net/prod/<región>/<ID del directorio> Conexiones de los clientes de macOS:

Categoría	Detalles
	• 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.ap-northeast-2.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	3.35.160.0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.ap-southeast-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.ap-southeast-1.amazonaws.com
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 (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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.ap-southeast-1.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	13.212.132.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.ap-southeast-2.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.ap-southeast-2.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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 de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.ap-southeast-2.signin.aws
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.ap-southeast-2.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	3.25.248.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.ap-northeast-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.ap-northeast-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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 de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.ap-northeast-1.signin.aws
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.ap-northeast-1.amazonaws.com

Categoría	Detalles
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	3.114.164.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.ca-central-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.ca-central-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.ca-central-1.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	3.97.20.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.eu-central-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.eu-central-1.amazonaws.com

Categoría	Detalles
Configuración de directorios	Autenticación del cliente al 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.eu-central-1.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	18.192.216.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.eu-west-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.eu-west-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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 de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.eu-west-1.signin.aws
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	3.248.176.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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://skylight-client-ds.eu-west-2.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.eu-west-2.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.eu-west-2.amazonaws.com
WorkSpaces Puntos finales de 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 IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	18.134.68.0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace de DCV	*.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

Europa (París)

Dominios y direcciones IP para agregar a la lista de permitidos

Categoría	Detalles
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/Cliente
Actualización automática del cliente	https://d2td7dqidlhjx7.cloudfront.net/
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://skylight-client-ds.eu-west-3.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.eu-west-3.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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://d2kmf63k5sit88.cloudfront.net/prod/<region>/<directory ID> 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 (París) — https://d1a3pnge9on3sx.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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.eu-west-3.amazonaws.com
WorkSpaces Puntos finales de API	Dominio: • https://workspaces.eu-west-3.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.eu-west-3.amazonaws.com
Servidores TURN de acceso web para IP PCo	Servidor: • turno: *.eu-west-3.rdn.amazonaws.com
El nombre del host de comprobación de estado	drp-cdg.amazonworkspaces.com
Direcciones IP de la comprobación de estado	• 51.17.52.90 • 51,17109231 • 51,16190,43
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 51.44.204.0-51.44.207.255 2a 05: d 032:2000: /40
Intervalo de direcciones IP de los servidores de puerta de enlace de DCV	51.17.72.0/22
Nombre de dominio de la puerta de enlace de DCV	*.prod.eu-west-3.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://skylight-client-ds.sa-east-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.sa-east-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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: • 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.sa-east-1.amazonaws.com
WorkSpaces Puntos finales de API	Dominio: • https://workspaces.sa-east-1.amazonaws.com

Categoría	Detalles
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.sa-east-1.amazon aws.com
Servidores TURN de acceso web para IP PCo	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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 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 DCV	15.228.64.0/22
Nombre de dominio de la puerta de enlace de DCV	*.prod.sa-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

África (Ciudad del Cabo)

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/
Métricas de clientes (para aplicaciones WorkSpaces cliente de más de 3.0)	Dominio: https://skylight-client-ds.af-south-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.af-south-1.amazonaws.com

Categoría	Detalles
Configuración de directorios	Autenticación del cliente al 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: • África (Ciudad del Cabo): https://di5ygl2cs0mrh.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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces Puntos finales de API	Dominio: • https://workspaces.af-south-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.af-south-1.amazonaws.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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 13.246.120.0 - 13.246.123.255
Intervalo de direcciones IP de los servidores de puerta de enlace de DCV	15.228.64.0/22

Categoría	Detalles
Nombre de dominio de la puerta de enlace de DCV	*.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/
Métricas de clientes (para aplicaciones WorkSpaces cliente de más de 3.0)	Dominio: https://skylight-client-ds.il-central-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.il-central-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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: • 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 clientes de Web Access y Teradici PCo IP Zero)	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: • https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces Puntos finales de API	Dominio: • https://workspaces.il-central-1.amazonaws.com
Agente de sesiones (PCM)	Dominio: • https://skylight-cm.il-central-1.amazonaws.com
Servidores TURN de acceso web para IP PCo	Servidor: • turn:*.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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 51.17.28.0-51.17.31.255
Intervalo de direcciones IP de los servidores de puerta de enlace de DCV	51.17.72.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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/
Actualización automática del cliente	https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/WorkSpacesAppCast.xml
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: h https://skylight-client-ds.us-gov-west-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.us-gov-west-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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>

Categoría	Detalles
	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: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript archivo para las páginas de inicio de sesión: • No aplicable
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado
Puntos de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.signin.amazonaws-us-gov.com
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://login.us-gov-home.awsapps.com/directory//(dónde está el dominio del cliente) <directory id><directory id>

Categoría	Detalles
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
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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 52.61.193.0 - 52.61.193.255

Categoría	Detalles
Intervalo de direcciones IP de los servidores de puerta de enlace de DCV	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
Nombre de dominio de la puerta de enlace de DCV	*.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/WorkSpacesAppCast.xml
Comprobación de la conectividad	https://connectivity.amazonworkspaces.com/
Client Metrics (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: h https://skylight-client-ds.us-gov-east-1.amazonaws.com
Servicio de mensajería dinámica (para aplicaciones WorkSpaces cliente de 3.0 o más)	Dominio: https://ws-client-service.us-gov-east-1.amazonaws.com
Configuración de directorios	Autenticación del cliente al 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://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: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript archivo para las páginas de inicio de sesión: • No aplicable
Servicio de registro de Forrester	https://fls-na.amazon.com/
Servidores de comprobación de estado (DRP)	Servidores de comprobación de estado

Categoría	Detalles
Puntos de conexión de autenticación con tarjeta inteligente anteriores a la sesión	https://smartcard.signin.amazonaws-us-gov.com
Dependencia de registro (para clientes de Web Access y Teradici PCo IP Zero)	https://s3.amazonaws.com
Páginas de inicio de sesión del usuario	https://login.us-gov-home.awsapps.com/directory//(dónde está el dominio del cliente) <directory id><directory id>
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
PCoIntervalos de direcciones IP públicas de servidores de puerta de enlace IP	• 18.254.140.0 - 18.254.143.255
Intervalo de direcciones IP de los servidores de puerta de enlace de DCV	18.254.148.0/22
Nombre de dominio de la puerta de enlace de DCV	*.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 para WorkSpaces Personal

WorkSpaces Los usuarios pueden conectarse a ellos WorkSpaces mediante la aplicación cliente de un dispositivo compatible. Como alternativa, pueden usar un navegador web para conectarse WorkSpaces que admita esta forma de acceso. Para ver una lista de las WorkSpaces que admiten el acceso a navegadores web, consulta «¿Qué WorkSpaces paquetes de Amazon admiten el acceso a la web?» en Acceso de clientes, Acceso web y Experiencia de usuario.

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

> **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.

Para ofrecer a sus usuarios una buena experiencia con sus dispositivos cliente WorkSpaces, compruebe que los 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 Personal.
- Para obtener el mejor rendimiento de PCo IP, el tiempo de ida y vuelta (RTT) desde la red del cliente hasta la región en la que WorkSpaces se encuentra debe ser inferior a 100 ms. Si el RTT está entre 100 ms y 200 ms, el usuario puede acceder a él, pero el rendimiento se ve WorkSpace afectado. 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 WorkSpaces cliente.

  Para obtener el mejor rendimiento del DCV, el RTT desde la red del cliente hasta la región en la que WorkSpaces se encuentra debe ser inferior a 250 ms. Si el RTT está entre 250 ms y 400 ms, el usuario puede acceder a él, pero el WorkSpace rendimiento se reduce.

  Para comprobar el RTT de las distintas AWS regiones desde su ubicación, utilice el Amazon WorkSpaces Connection Health Check.
- Para utilizar cámaras web con DCV, recomendamos un ancho de banda de carga mínimo de 1,7 megabits por segundo.
- Si los usuarios van a acceder a WorkSpaces ellas a través de una red privada virtual (VPN), la conexión debe admitir una unidad de transmisión (MTU) máxima de al menos 1200 bytes.

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

- Los clientes requieren acceso HTTPS a WorkSpaces los recursos 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 el acceso HTTPS para que los usuarios puedan completar correctamente el registro y acceder a sus WorkSpaces.

- Para permitir el acceso desde dispositivos cliente con PCo IP cero, debe utilizar un paquete de protocolos PCo IP para WorkSpaces. También debe habilitar el protocolo de tiempo de red (NTP) en Teradici. Para obtener más información, consulte Configurar clientes PCo IP cero para WorkSpaces Personal.

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

Para verificar los requisitos de red para clientes 3.0+

1. Abre tu WorkSpaces cliente. 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, seleccion e 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. Abre tu WorkSpaces cliente. 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 acceso a dispositivos de confianza para WorkSpaces uso personal

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.

> **Note**
>
> Actualmente, esta función solo está disponible cuando sus directorios WorkSpaces personales se administran mediante el AWS Directory Service directorio Simple AD, AD Connector y AWS Managed Microsoft AD.

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 PCo IP, clientes RDP y aplicaciones de escritorio remoto.

> **Note**
>
> Al habilitar el acceso para clientes específicos, asegúrese de bloquear el acceso a otros tipos de dispositivos que no necesite. Para obtener más información sobre cómo llevar a cabo este procedimiento, consulte el paso 3.7 que se indica 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 los 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 los clientes.
- Utilice un algoritmo de cifrado sólido. Recomendamos usar SHA256 RSA, SHA256 ECDSA o ECDSA. SHA384 SHA512
- 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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 a qué dispositivos pueden 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, Android, Web Access, Chromebooks y dispositivos cliente PCo IP zero.

   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.

Integre SAML 2.0 con Personal WorkSpaces

> **Note**
>
> SAML 2.0 solo está disponible cuando sus directorios WorkSpaces personales se administran mediante el directorio AWS Directory Service Simple AD, AD Connector y AWS Managed Microsoft AD. La función no se aplica a los directorios gestionados por Amazon WorkSpaces, que normalmente utilizan el Centro de identidad de IAM para la autenticación de usuarios en lugar de la federación SAML 2.0.

La integración de SAML 2.0 con la autenticación WorkSpaces de sesión de escritorio permite a los usuarios usar sus credenciales de proveedor de identidad (IdP) de SAML 2.0 y sus métodos de autenticación existentes a través de su navegador web predeterminado. Al utilizar su IdP para autenticar a los usuarios WorkSpaces, puede protegerlos mediante el uso de funciones del WorkSpaces IdP, como la autenticación multifactorial 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 WorkSpaces cliente, WorkSpaces Web Access y un proveedor de identidad (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 inicia el WorkSpaces flujo. Por ejemplo, cuando los usuarios abren la aplicación cliente e inician sesión.
- Cuando WorkSpaces Web Access 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 WorkSpaces directorio y los usuarios están autorizados para la aplicación WorkSpaces SAML 2.0. Los usuarios crean un WorkSpace para sus nombres de usuario,`user`, en un directorio que está habilitado para la autenticación SAML 2.0. Además, los usuarios instalan la aplicación WorkSpaces cliente en su dispositivo o utilizan Web Access 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 WorkSpaces cliente en sus dispositivos sin tener que introducir un código de WorkSpaces registro. Los usuarios no inician sesión en ellos WorkSpaces mediante el flujo iniciado por el IdP. WorkSpaces la autenticación 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 WorkSpaces aplicación en el portal de usuarios del IdP.
3. Los usuarios son redirigidos a esta página en el navegador y la aplicación WorkSpaces cliente se abre automáticamente.

4. La aplicación WorkSpaces cliente ya está registrada y los usuarios pueden seguir iniciando sesión haciendo clic en Continuar para iniciar sesión. 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 registrarlos automáticamente a WorkSpaces través de un navegador web sin tener que introducir un código de WorkSpaces registro. Los usuarios no inician sesión en ellos WorkSpaces mediante el flujo iniciado por el IdP. WorkSpaces la autenticación debe originarse en Web Access.

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 WorkSpaces aplicación desde el portal de usuarios del IdP.
3. Los usuarios son redirigidos a esta página en el navegador. Para abrirla WorkSpaces, selecciona Amazon WorkSpaces en el navegador.

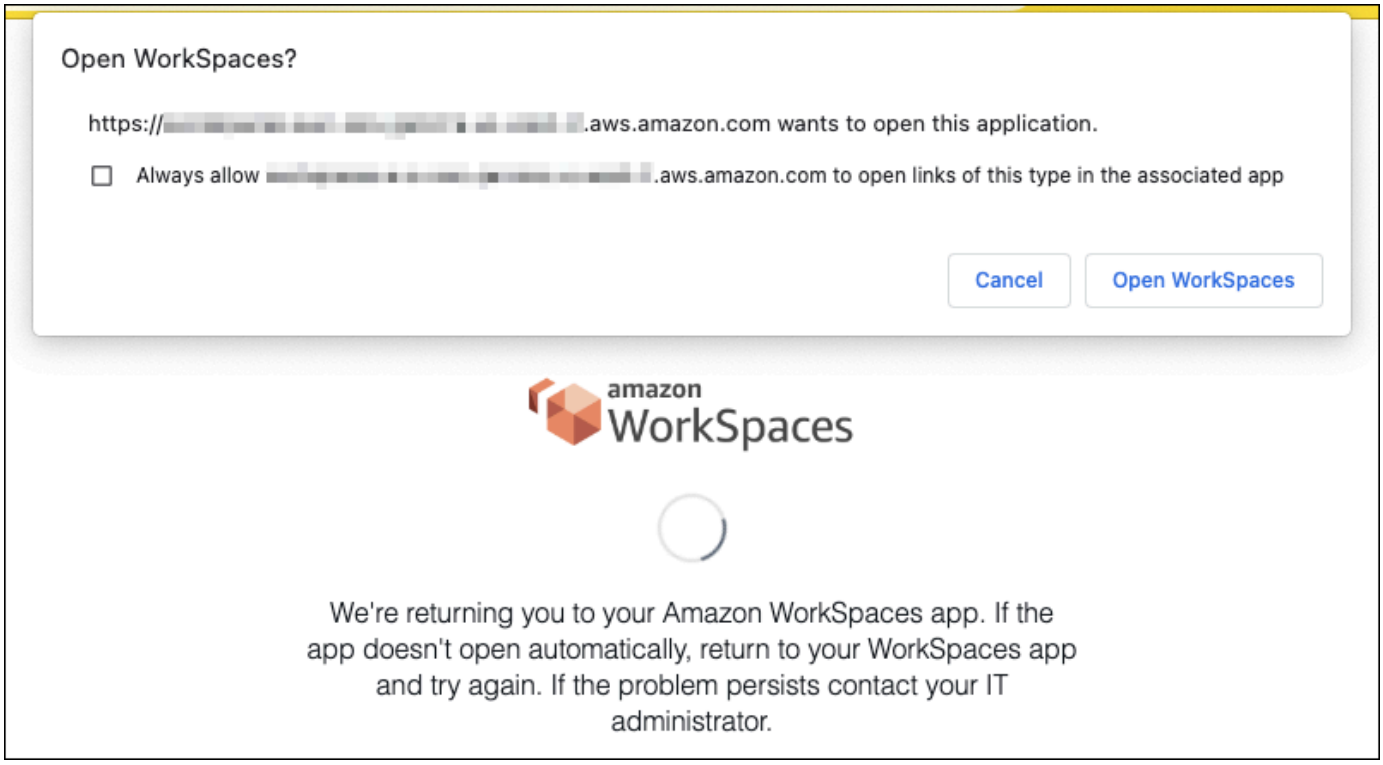
4. La aplicación WorkSpaces cliente ya está registrada y los usuarios pueden seguir iniciando sesión a través de WorkSpaces Web Access.

WorkSpaces flujo iniciado por el cliente

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

1. Los usuarios inician la aplicación WorkSpaces cliente (si aún no se está ejecutando) y hacen clic en Continuar para iniciar sesión. 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. Se redirige a los usuarios a la aplicación WorkSpaces cliente para que completen el inicio de sesión en la suya WorkSpace. WorkSpaces los nombres de usuario se rellenan automáticamente a partir de la afirmación SAML 2.0 del IdP. Al utilizar la autenticación basada en certificados (CBA), los usuarios inician sesión automáticamente.
5. Los usuarios inician sesión en su. WorkSpace

WorkSpaces Flujo iniciado por el acceso web

El flujo iniciado por el acceso web permite a los usuarios iniciar sesión en su cuenta WorkSpaces después de iniciar sesión en un IdP.

1. Los usuarios inician el acceso WorkSpaces 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 iniciados sesión en el IdP, los usuarios se redirigen a esta página en el navegador y hacen clic en Iniciar sesión en. WorkSpaces
4. Los usuarios fueron redirigidos a la aplicación del WorkSpaces cliente para completar el inicio de sesión en su WorkSpace. WorkSpaces los nombres de usuario se rellenan automáticamente a partir de la afirmación SAML 2.0 del IdP. Al utilizar la autenticación basada en certificados (CBA), los usuarios inician sesión automáticamente.
5. Los usuarios inician sesión en su. WorkSpace

Configurar SAML 2.0 para personal WorkSpaces

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
- Requisitos previos
- Paso 1: Crear un proveedor de identidades SAML en IAM AWS
- Paso 2: crear un rol de IAM de federación de SAML 2.0
- Paso 3: incrustar una política en línea para el rol de IAM
- Paso 4: configurar el proveedor de identidades de SAML 2.0
- Paso 5: crear declaraciones para la respuesta de autenticación SAML
- Paso 6: configurar el estado de retransmisión de la federación
- Paso 7: Habilita la integración con SAML 2.0 en tu directorio WorkSpaces

Requisitos

- La autenticación SAML 2.0 está disponible en las siguientes regiones:
  - Región 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 del cliente no podrán conectarse a la autenticación WorkSpaces habilitada para SAML 2.0 a menos que esté habilitada 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. Para un usuario con a WorkSpace, los atributos s AMAccount Nombre y correo electrónico 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 transmisión de usuario de SAML que incluyan una aserción de tipo de sujeto de SAML con un valor de persistent. Si SAML:sub_type es persistente, el 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:

    JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333: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 de SAML 2.0, puede usar políticas de control de acceso IP si están disponibles en el 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.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
```

```
            "Resource": "arn:aws:workspaces:us-east-1:123456789012: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 saml-metadata.xml a https://signin.aws.amazon.com/static/ tu IdP. En este paso se actualizan los metadatos de su proveedor de identidades. Para 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:

- NameID del sujeto de SAML: 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 atributo s AMAccount Name del usuario de Active Directory.
- Tipo de sujeto de SAML (con un valor establecido en `persistent`): al establecer el valor en `persistent` se garantiza que el IdP 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 incluye uno o varios elementos `AttributeValue` que enumera el rol de IAM y el IdP de SAML a los que el IdP ha asignado al usuario. El rol y el IdP se especifican como un par delimitado por comas de. ARNs 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 incluye un elemento `AttributeValue` que proporciona la dirección de correo electrónico del usuario. El valor debe coincidir con la dirección WorkSpaces de correo electrónico del usuario definida en el WorkSpaces directorio. Los valores de las etiquetas pueden incluir combinaciones de 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\usernamecorp.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 una 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 Este de EE. UU. (Norte de Virginia)	• workspaces.euc-sso.us-east-1.aws.amazon.com • espacios de trabajo (FIPS). 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 • espacios de trabajo (FIPS). euc-sso-fips.us-west-2.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	Punto de conexión del estado de retransmisión
Región de Asia-Pacífico (Sídney)	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
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 • espacios de trabajo (FIPS). 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 • espacios de trabajo (FIPS). 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.).

Con un flujo iniciado por un proveedor de identidades (IdP), puede optar por especificar el cliente que desea usar para la federación de SAML 2.0. Para ello, especifique `native` o `web` al final de la URL del estado de retransmisión, después de `&client=`. Si el parámetro se especifica en una URL de estado de retransmisión, las sesiones correspondientes se iniciarán automáticamente en el cliente especificado.

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. Abre la WorkSpaces consola en la versión 2/homehttps://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>`

Proveedor de identidades	Parámetro	URL de acceso del usuario
Auth0	`RelayState`	`https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>`
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**
>
> PCoWeb Access no admite IP con SAML.

10. Seleccione Save. 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 y personal WorkSpaces

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 de raíz y subordinada. CAs 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 paquetes de Windows WorkSpaces on DCV 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 `ObjectSid` en su declaración de SAML. Esto es necesario para realizar un mapeo sólido con el 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.

   > **Note**
   >
   > Según Microsoft KB5 014754, el `ObjectSid` atributo será obligatorio para la autenticación basada en certificados después del 10 de septiembre de 2025.

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 EC2 instancia 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 que ejecuta los Servicios de certificados, lo que permite que EC2 los puertos TCP 135 y 49152-65535 habiliten la inscripción automática de certificados. Además, la EC2 instancia en ejecución debe permitir el acceso entrante a los 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. Como alternativa, puede utilizar la política de grupo y la herramienta Microsoft PKI Health Tool (PKIView) 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 automáticamente la CA a las autoridades emisoras de certificados raíz de confianza y a los NTAuth almacenes Enterprise para los WorkSpaces escritorios cuando se unan al dominio.

Habilitación de la autenticación basada en certificados

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

1. Abra la WorkSpaces consola en la versión https://console.aws.amazon.com/workspaces/v2/home.
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 WorkSpaces de Windows en DCV 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.

Habilitación del uso compartido entre cuentas de una CA privada

Al utilizar el uso compartido entre cuentas de una 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 y personal WorkSpaces .
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 es necesario 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 APIs. Al configurar el recurso compartido, confirme que el recurso compartido de RAM de la CA privada de la cuenta de recursos utilice la plantilla de permisos administrada por `AWS RAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority`. Esta plantilla se alinea con la plantilla de PCA utilizada por el rol de WorkSpaces servicio al emitir los certificados CBA.
3. Una vez que el recurso se haya compartido correctamente, podrá ver la CA privada compartida mediante la consola de Private CA en 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 una CA privada compartida. ARNs Ejemplo de comandos de la CLI:

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

Accede a Microsoft Entra ID y personal unido WorkSpaces

Puede crear un personal BYOL de Windows 10 u 11 WorkSpaces que esté unido a Microsoft Entra ID e inscrito en Intune. Para obtener más información, consulta Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal.

Flujo de trabajo de autenticación

En las siguientes secciones se describe el flujo de trabajo de autenticación iniciado por la aplicación WorkSpaces cliente, WorkSpaces Web Access, y un proveedor de identidad (IdP) de SAML 2.0, Microsoft Entra ID:

- Cuando el IdP inicia el flujo. Por ejemplo, cuando los usuarios eligen una aplicación en el portal de usuarios de Entra ID en un navegador web.
- Cuando el cliente inicia el WorkSpaces flujo. Por ejemplo, cuando los usuarios abren la aplicación cliente e inician sesión.
- Cuando WorkSpaces Web Access 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.onmicrosoft.com` para iniciar sesión en el IdP. En Entra ID, una aplicación empresarial está configurada para integrarse con IAM Identity Center. Los usuarios crean una WorkSpace para sus nombres de usuario en un directorio que utiliza el Centro de Identidad de IAM como fuente de identidad para conectarse a un inquilino de Entra ID. Además, los usuarios instalan la aplicación WorkSpaces cliente en su dispositivo o utilizan Web Access 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 WorkSpaces cliente en sus dispositivos sin tener que introducir un código de WorkSpaces registro. Los usuarios no inician sesión en ellos WorkSpaces mediante el flujo iniciado por el IdP. WorkSpaces la autenticación debe originarse en la aplicación cliente.

1. Con el navegador web, los usuarios inician sesión en el IdP (Microsoft Entra ID).
2. Tras iniciar sesión en el IdP, los usuarios eligen la aplicación AWS IAM Identity Center en el portal de usuarios del IdP.
3. Los usuarios son redirigidos al portal de AWS acceso en el navegador. A continuación, los usuarios eligen el WorkSpaces icono.
4. Los usuarios son redirigidos a la página siguiente y la aplicación WorkSpaces cliente se abre automáticamente. Selecciona Abrir WorkSpaces aplicación Amazon si la aplicación cliente no se abre automáticamente.

5. La aplicación WorkSpaces cliente ya está registrada y los usuarios pueden seguir iniciando sesión haciendo clic en Continuar para iniciar sesión. 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 registrarlos automáticamente a WorkSpaces través de un navegador web sin tener que introducir un código de WorkSpaces registro. Los usuarios no inician sesión en ellos WorkSpaces mediante el flujo iniciado por el IdP. WorkSpaces la autenticación debe originarse en Web Access.

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 AWS IAM Identity Center desde el portal de usuarios del IdP.
3. Se redirige a los usuarios al portal de AWS acceso en el navegador. A continuación, los usuarios eligen el WorkSpaces icono.
4. Los usuarios son redirigidos a esta página en el navegador. Para abrirla WorkSpaces, selecciona Amazon WorkSpaces en el navegador.

5. La aplicación WorkSpaces cliente ya está registrada y los usuarios pueden seguir iniciando sesión a través de WorkSpaces Web Access.

WorkSpaces flujo iniciado por el cliente

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

1. Los usuarios inician la aplicación WorkSpaces cliente (si aún no se está ejecutando) y hacen clic en Continuar para iniciar sesión. 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 WorkSpaces cliente, en la pantalla de inicio de sesión de Windows.
5. Los usuarios completan el inicio de sesión en Windows con el nombre de usuario y credenciales de Entra ID.

WorkSpaces Flujo iniciado por el acceso web

El flujo iniciado por el acceso web permite a los usuarios iniciar sesión en su cuenta WorkSpaces después de iniciar sesión en un IdP.

1. Los usuarios inician el acceso WorkSpaces 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 iniciados sesión en el IdP, los usuarios se redirigen a esta página en el navegador y hacen clic en Iniciar sesión en. WorkSpaces
4. Los usuarios son redirigidos a la aplicación WorkSpaces cliente, en la pantalla de inicio de sesión de Windows.
5. Los usuarios completan el inicio de sesión en Windows con el nombre de usuario y credenciales de Entra ID.

Experiencia de usuario principiante

Si inicias sesión por primera vez en un Microsoft Entra ID unido a Windows WorkSpaces, debes pasar por la out-of-box experiencia (OOBE). Durante el OOBE, se WorkSpaces unen a Entra ID. Puede personalizar la experiencia OOBE configurando el perfil de piloto automático asignado al grupo de dispositivos de Microsoft Intune que cree para su. WorkSpaces Para obtener más información, consulte Paso 3: configurar el modo controlado por el usuario de Windows Autopilot.

Utilizar tarjetas inteligentes para la autenticación en WorkSpaces Personal

Los paquetes de Windows y Linux WorkSpaces en DCV permiten el uso de tarjetas inteligentes de tarjeta de acceso común (CAC) y de verificación de identidad personal (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
- Limitaciones
- Configuración del directorio:
- Habilite las tarjetas inteligentes para Windows WorkSpaces
- Habilitar tarjetas inteligentes para Linux WorkSpaces

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 protocolo DCV sea compatible. La autenticación previa a la sesión está disponible en las siguientes regiones:
  - Región de Asia-Pacífico (Sídney)
  - Asia Pacífico (Tokio)
  - Región de Europa (Irlanda)
  - AWS GovCloud Región (EE. UU.-Este)
  - AWS GovCloud Región (EE. UU.-Oeste)
  - Región 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 DCV.

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 AMAccount nombre s del mismo usuario. Un AMAccount nombre s no 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 Habilitación o deshabilitación de la sesión de desconexión en el bloqueo de pantalla para DCV.

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 Habilitación o deshabilitación del redireccionamiento de tarjetas inteligencias para DCV.

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.

Habilitar tarjetas inteligentes para Linux WorkSpaces

> **Note**
>
> Actualmente, Linux WorkSpaces en DCV 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 DCV.

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, `rootca` donde 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 los paquetes de Amazon Linux DCV. 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 DCV activado. Al iniciar el WorkSpace en la WorkSpaces consola de Amazon, en la página Select Bundles, asegúrese de seleccionar DCV 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 individualmente 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 estás 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 para WorkSpaces personal

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 personal 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 WorkSpaces Personal

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 desconectar 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 EC2 seguridad de Amazon para instancias de Linux o Grupos de EC2 seguridad de Amazon para instancias de Windows.

Puede añadir un grupo WorkSpaces de seguridad predeterminado a un directorio. 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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 la https://console.aws.amazon.com/workspaces/versión 2/home.
   b. Amplíe cada una WorkSpace y registre su WorkSpace dirección IP.
2. Busque el ENI de cada uno WorkSpace y actualice su asignación de grupo de seguridad.
   a. Abre la EC2 consola de Amazon 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. Repite este proceso según sea necesario para cualquier otro WorkSpaces.

Grupos de control de acceso IP para WorkSpaces Personal

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

Un grupo de control de acceso IP actúa como un firewall virtual que controla las direcciones IP desde las que los usuarios pueden acceder a sus WorkSpaces direcciones. 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 IP por región y AWS cuenta. 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 ellos 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 sus usuarios acceden a ellos WorkSpaces a través de una puerta de enlace NAT o una VPN, debe crear reglas que permitan el tráfico desde las direcciones IP públicas de la puerta de enlace NAT o la VPN.

> **Note**
>
> - Los grupos de control de acceso IP no permiten el uso de direcciones IP dinámicas para NATs. Si utiliza una NAT, configúrela para que use una dirección IP estática en lugar de

una dinámica. Asegúrese de que la NAT enrute todo el tráfico UDP a través de la misma dirección IP estática durante toda la WorkSpaces sesión.

- Los grupos de control de acceso IP controlan las direcciones IP desde las que los usuarios pueden conectar sus sesiones de streaming WorkSpaces. Los usuarios aún pueden ejecutar funcionalidades, como reiniciar, reconstruir o apagar, desde cualquier dirección IP mediante Amazon WorkSpaces public APIs.
- Los grupos de control de acceso IP no se aplican cuando el punto final de la VPC para la transmisión está configurado para un directorio.

Puede utilizar esta función con Web Access, los clientes PCo IP cero y las aplicaciones cliente para macOS, 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. Abre la WorkSpaces consola en la versión 2/home. 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 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 IP a un directorio para asegurarse de que solo WorkSpaces se accede a ellos desde redes de confianza.

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

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

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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. Abre la WorkSpaces consola en la v2/home. 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 la conexión a un WorkSpace, el usuario se desconecta del. WorkSpace

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 WorkSpaces consola en la https://console.aws.amazon.com/workspaces/v2/home.
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).

Configurar clientes PCo IP cero para WorkSpaces Personal

PCoLos clientes IP cero solo son compatibles con WorkSpaces los paquetes que utilizan el protocolo PCo IP.

Si su dispositivo de cliente cero tiene la versión de firmware 6.0.0 o posterior, los usuarios pueden conectarse directamente a la suya WorkSpaces . Cuando sus usuarios se conecten directamente a ellos WorkSpaces mediante un dispositivo de cliente cero, le recomendamos que utilice la autenticación multifactor (MFA) con WorkSpaces su directorio. 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 multifactorial (AD Connector) para personal WorkSpaces
- 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 PCo IP 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 la versión 6.0.0 o posterior, puede obtener el firmware más reciente mediante una suscripción a Desktop Access en /desktop-access. https://www.teradici.com

> **Important**
>
> - En la Interfaz Web Administrativa PCo IP (AWI) de Teradici o en la Consola de Administración PCo IP (MC) de Teradici, asegúrese de activar el Protocolo de tiempo de red (NTP). Para el nombre DNS del host NTP, utilice **`pool.ntp.org`** y establezca el puerto host NTP como 123. Si el NTP no está activado, los usuarios del cliente PCo IP cero podrían recibir errores en los certificados, como «El certificado suministrado no es válido debido a una marca de tiempo».
> - A partir de la versión 20.10.4 del agente PCo IP, 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 cliente de PCo IP cero para conectarse a sus dispositivos. WorkSpaces Para obtener más información, consulte Las impresoras USB y otros periféricos USB no funcionan para los clientes con IP cero PCo.

Para obtener información sobre la configuración y la conexión con un dispositivo cliente PCo IP cero, consulte PCoIP Zero Client en la Guía del WorkSpaces usuario de Amazon. Para obtener una lista de los dispositivos de cliente PCo IP cero aprobados, consulte los clientes PCo IP cero en el sitio web de Teradici.

Configurar Android para Chromebook for Personal WorkSpaces

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 el acceso WorkSpaces web para WorkSpaces personal

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 a la web con DCV para Windows y Ubuntu WorkSpaces es compatible en todas las regiones en las que esté disponible el DCV WorkSpaces . DCV para Amazon Linux solo WorkSpaces está disponible en AWS GovCloud (EE. UU. al oeste).
> - Recomendamos encarecidamente utilizar Web Access con DCV WorkSpaces para obtener la mejor calidad de streaming y la mejor experiencia de usuario. Las siguientes son limitaciones al utilizar el acceso web con PCo IP WorkSpaces:
> - El AWS GovCloud (US) Regions acceso web con PCo IP no es compatible en Asia Pacífico (Bombay), África (Ciudad del Cabo), Europa (Fráncfort) e Israel (Tel Aviv)
> - El acceso web con PCo IP solo es compatible con Windows WorkSpaces, no con Amazon Linux o Ubuntu WorkSpaces.
> - El acceso web no está disponible para algunos Windows 10 WorkSpaces que utilizan el protocolo PCo IP. Si su PCo IP WorkSpaces funciona con Windows Server 2019 o 2022, el acceso web no está disponible.
> - Las funciones del acceso a la web con PCo IP son limitadas. Admite la salida de vídeo, la salida de audio, el teclado y el ratón. No admite muchas características, como la entrada de vídeo, la entrada de audio, el redireccionamiento del portapapeles y las cámaras web.
> - Si utilizas macOS en una VPN y utilizas el navegador web Firefox, el navegador web no admitirá la transmisión de PCo IP 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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 Save.

> **Note**
>
> Después de habilitar 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 (GPOs) para aplicar la configuración y administrar Windows WorkSpaces o los usuarios que forman parte de su WorkSpaces directorio de Windows. Se recomienda crear una unidad organizativa para los objetos de WorkSpaces ordenador y una unidad organizativa para los objetos WorkSpaces de usuario.

Para obtener información sobre cómo utilizar las herramientas de administración de Active Directory para trabajar con ellas GPOs, consulte Instalación de las herramientas de administración de Active Directory en la Guía de AWS Directory Service administración.

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 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 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 WorkSpaces Thin Client

La mayoría de WorkSpaces los paquetes son compatibles con Amazon WorkSpaces Thin Client 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 Thin Client Access?» en Acceso de clientes, Acceso web y Experiencia de usuario.

Paso 1: Habilite el control de acceso a su Amazon WorkSpaces Thin Client

Usted controla el acceso de Thin Client WorkSpaces a su directorio mediante un control de acceso basado en agentes de usuario. Siga los siguientes pasos para cada directorio al WorkSpaces que desee permitir el acceso de los usuarios a través del cliente Thin Client Access.

Para habilitar el acceso de Thin Client a su WorkSpaces

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

6. Seleccione Save.

Paso 2: Configure el acceso entrante y saliente a los puertos para Thin Client Access

Amazon WorkSpaces Thin Client 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 Thin Client Access.

Para permitir que los usuarios de Thin Client 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 (GPOs) para aplicar la configuración y administrar Windows WorkSpaces o los usuarios que forman parte de su WorkSpaces directorio de Windows. Se recomienda crear una unidad organizativa para los objetos de WorkSpaces ordenador y una unidad organizativa para los objetos WorkSpaces de usuario.

Para obtener información sobre cómo utilizar las herramientas de administración de Active Directory para trabajar con ellas GPOs, consulte Instalación de las herramientas de administración de Active Directory en la Guía de AWS Directory Service administración.

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 WorkSpaces Thin Client Access, 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 busque y seleccione un GPO en el nivel de dominio o controlador de dominio del directorio que utiliza para el suyo. 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.

Configure la autorización de FedRAMP o el cumplimiento de las normas SRG del DoD para personal WorkSpaces

Para cumplir con el Programa federal de gestión de riesgos y autorizaciones (FedRAMP) o la Guía de requisitos de seguridad de la computación en nube (SRG) del Departamento de Defensa (DoD), debe configurar WorkSpaces Amazon para que utilice el cifrado de puntos finales de los estándares federales de procesamiento de información (FIPS) a nivel de directorio. También debe utilizar una AWS región de EE. UU. que cuente con la autorización de FedRAMP o que cumpla con las normas SRG del DoD.

El nivel de autorización de FedRAMP (moderado o alto) o el nivel de impacto SRG del DoD (2, 4 o 5) depende de la AWS región 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 de punto final FIPS, también puede cifrar su. WorkSpaces Para obtener más información, consulte WorkSpaces Cifrado en WorkSpaces modo personal.

Requisitos

- Debe crearlo WorkSpaces en una AWS región de EE. UU. que cuente con la autorización de FedRAMP o que cumpla con las normas SRG del DoD.
- El WorkSpaces directorio debe configurarse para usar el modo validado por FIPS 140-2 para el cifrado de puntos finales.

> **Note**
>
> Para usar la configuración del modo validado por FIPS 140-2, el WorkSpaces directorio debe ser nuevo o todos los existentes WorkSpaces en el directorio deben usar el modo validado por FIPS 140-2 para el cifrado de los puntos finales. De lo contrario, no podrá usar esta configuración y, por lo tanto, la WorkSpaces que cree no cumplirá con los requisitos de seguridad de FedRAMP o DoD.
> Consulte el paso 3 que aparece a continuación para obtener más información sobre cómo verificar el directorio.

- Los usuarios deben acceder a ellas WorkSpaces desde una de las siguientes aplicaciones cliente: WorkSpaces
  - Windows 2.4.3 o posterior
  - macOS: 2.4.3 o posterior para PCo IP WorkSpaces y 5.21.0 o posterior para DCV WorkSpaces
  - 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. Abre la consola en la versión WorkSpaces v2/home. 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, autorizado por FedRAMP y compatible con SRG del DoD, WorkSpaces no tenga ningún directorio asociado. WorkSpaces Si están WorkSpaces asociados al directorio y el directorio aún no está habilitado para usar el modo validado por FIPS 140-2, finalice el directorio o cree uno nuevo. WorkSpaces
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 WorkSpaces desde este directorio que estén autorizados por FedRAMP y cumplan con las normas SRG del DoD. Para acceder a ellas WorkSpaces, los usuarios deben usar una de las aplicaciones WorkSpaces cliente enumeradas anteriormente en la sección de requisitos.

Habilite las conexiones SSH para su Linux WorkSpaces en Personal WorkSpaces

Si usted o sus usuarios desean conectarse a su 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. Después de crear o actualizar el grupo de seguridad, los usuarios y otras personas pueden usar PuTTY u otros terminales para conectarse desde sus dispositivos a su 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. Este tutorial es WorkSpaces solo para Amazon Linux 2.

Contenido

- Requisitos previos para las conexiones SSH a Linux WorkSpaces
- Habilite las conexiones SSH a todos los Linux WorkSpaces de un directorio
- Autenticación basada en contraseña en WorkSpaces
- Habilite las conexiones SSH a un Linux específico WorkSpace
- Conéctate a un Linux WorkSpace mediante Linux o PuTTY

Requisitos previos para las conexiones SSH a Linux WorkSpaces

- Habilitar el tráfico SSH entrante en un WorkSpace : para agregar una regla que permita el tráfico SSH entrante a uno o más Linux WorkSpaces, asegúrese de tener las direcciones IP públicas o privadas de los dispositivos que requieren conexiones SSH en su dispositivo. 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 EC2 instancia en la misma VPC que la suya. WorkSpace

  Si piensa 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 un dispositivo 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 del Linux al WorkSpace que desea conectarse y su nombre de usuario

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/v2/home.
2. En el panel de navegación, elija WorkSpaces.
3. En la lista de WorkSpaces, elige aquella a la WorkSpace 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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
7. En el panel de navegación, elija Network Interfaces.
8. En el cuadro de búsqueda, escribe la WorkSpace IP que anotaste 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 IPv4 pública. 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 del 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 Linux WorkSpaces de un directorio

Para habilitar las conexiones SSH a todos los 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 Linux WorkSpaces de un directorio

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Elija Creación de 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.
8. Adjunte este grupo de seguridad a su. WorkSpaces Para obtener más información sobre cómo agregar este grupo de seguridad al suyo WorkSpaces, consulteGrupos de seguridad para WorkSpaces Personal. Si desea adjuntar automáticamente grupos de seguridad adicionales al suyo WorkSpaces, consulte esta entrada de blog.

Autenticación basada en contraseña en WorkSpaces

Para habilitar la autenticación por contraseña en el Linux recién creado WorkSpaces

1. Inicie el WorkSpaces cliente e inicie sesión en su WorkSpace.
2. Abra la ventana Terminal.
3. En la ventana Terminal, ejecute el siguiente comando para habilitar la autenticación mediante contraseña SSH en cloud-init.

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 true" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single --name set-passwords'
```

Este script hará lo siguiente:

- Crear un archivo de configuración en el directorio de cloud-init `/etc/cloud/cloud.cfg.d/`.
- Modificar el archivo de configuración para indicar a cloud-init que habilite la autenticación mediante contraseña SSH.
- Restablecer el módulo de cloud-init `set-passwords` para que pueda volver a ejecutarse.
- Ejecutar automáticamente el módulo de cloud-init `set-passwords`. Esto escribirá un archivo que permite la autenticación mediante contraseña SSH en el directorio de configuración de SSH, `/etc/ssh/sshd_config.d/`, y reiniciará SSHD para que la configuración tenga efecto inmediatamente.

Esto permite la autenticación mediante contraseña SSH WorkSpace y se conservará en las imágenes personalizadas. Si habilitas la autenticación con contraseña SSH solo en el archivo de configuración de SSHD, sin configurar cloud-init, la configuración no se conservará durante la generación de imágenes en algunos Linux. WorkSpaces Para obtener más información, consulte Set Passwords en la documentación del módulo de cloud-init.

Para deshabilitar la autenticación por contraseña en los Linux existentes WorkSpaces

1. Inicie el WorkSpaces cliente e inicie sesión en su WorkSpace.
2. Abra la ventana Terminal.
3. En la ventana Terminal, ejecute el siguiente comando para deshabilitar la autenticación mediante contraseña SSH en cloud-init.

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 false" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single –name set-passwords'
```

Este script hará lo siguiente:

- Crear un archivo de configuración en el directorio de cloud-init `/etc/cloud/cloud.cfg.d/`.

- Modificar el archivo de configuración para indicar a cloud-init que deshabilite la autenticación mediante contraseña SSH.
- Restablecer el módulo de cloud-init `set-passwords` para que pueda volver a ejecutarse.
- Ejecutar automáticamente el módulo de cloud-init `set-passwords`. Esto escribirá un archivo que permite la autenticación mediante contraseña SSH en el directorio de configuración de SSH, `/etc/ssh/sshd_config.d/`, y reiniciará SSHD para que la configuración tenga efecto inmediatamente.

Esto deshabilita inmediatamente el SSH en las imágenes personalizadas WorkSpace y persistirá en ellas.

Habilite las conexiones SSH a un Linux específico WorkSpace

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

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

1. Abre la EC2 consola de Amazon 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, escribe la dirección IP privada a la WorkSpace que deseas 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 (Edición de).
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 IPv4 dirección es`203.0.113.25`, especifique `203.0.113.25/32` que se muestre esta IPv4 dirección 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. Seleccione Save.

Conéctate a un 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 la sección «Requisitos previos para las conexiones SSH a Linux WorkSpaces», que aparece anteriormente en este tema.

Para conectarse a un Linux mediante Linux WorkSpace

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

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

   A continuación, mostramos un ejemplo del comando SSH donde:

   - *NetBIOS_NAME*Es cualquier empresa
   - Ella *Username* es Jane Doe
   - El *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 un 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 Personal

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”
- the section called “Componentes para Rocky Linux ”
- the section called “Componentes para Red Hat Enterprise Linux ”

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`

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

- C:\Archivos de programa\Amazon
- C:\ProgramData\ Amazon

Agente PCo IP de 32 bits

El 29 de marzo de 2021, actualizamos el agente PCo IP de 32 bits a 64 bits. En el caso de Windows WorkSpaces que utilizan el protocolo PCo IP, 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 PCo IP 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 va a filtrar las rutas a algún componente PCo IP de 32 bits, asegúrese de añadir las rutas a las versiones de 64 bits de los componentes. Como es WorkSpaces posible que no se actualicen todos al mismo tiempo, no sustituya la ruta de 32 bits por la ruta de 64 bits o es WorkSpaces posible que algunas de las suyas no funcionen. 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`.

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

PCoClientes IP cero y dispositivos USB: a partir de la versión 20.10.4 del agente PCo IP, 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 cliente de PCo IP cero para conectarse a sus dispositivos. WorkSpaces Para obtener más información, consulte Las impresoras USB y otros periféricos USB no funcionan para los clientes con IP cero PCo.

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 2 WorkSpaces en modo WorkSpaces personal.

- `/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/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/share/X11`
- `/usr/bin/euc-analytics-agent`
- `/var/lib/skylight`
- `/var/log/skylight`
- `/var/log/eucanalytics`

Componentes de servicio necesarios para Rocky Linux

En Red Hat Enterprise Linux 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.

- `/etc/dcv`
- `/etc/os-release`
- `/etc/pam.d/dcv-graphical-sso`
- `/etc/pam.d/dcv`
- `/etc/systemd/system/euc-analytic-agent.service`
- `/etc/wsp`

- `/usr/bin/euc-analytics-agent`
- `/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.path`
- `/usr/lib/systemd/system/xdcv-console.service`
- `/usr/lib/systemd/system/xdcv-console-update.service`
- `/usr/share/X11`
- `/var/lib/skylight`
- `/var/log/eucanalytics`
- `/var/log/skylight`

Componentes de servicio necesarios para Red Hat Enterprise Linux

En Red Hat Enterprise 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.

- `/etc/dcv`
- `/etc/os-release`
- `/etc/pam.d/dcv-graphical-sso`
- `/etc/pam.d/dcv`
- `/etc/systemd/system/euc-analytic-agent.service`
- `/etc/wsp`
- `/usr/bin/euc-analytics-agent`
- `/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.path`
- `/usr/lib/systemd/system/xdcv-console.service`
- `/usr/lib/systemd/system/xdcv-console-update.service`
- `/usr/share/X11`
- `/var/log/eucanalytics`
- `/var/log/skylight`

Administrar directorios para WorkSpaces Personal

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

- Conector AD: Use el Microsoft Active Directory local existente. Los usuarios pueden iniciar sesión WorkSpaces con sus credenciales locales y acceder a los recursos locales desde sus. WorkSpaces
- AWS Managed Microsoft AD — Cree un Microsoft Active Directory alojado en AWS.
- Simple AD: cree un directorio que sea compatible con Microsoft Active Directory, con tecnología Samba 4 y alojado en AWS.
- Confianza cruzada: cree una relación de confianza entre su AWS Managed Microsoft AD directorio y su dominio local.
- Microsoft Entra ID: cree un directorio que utilice Microsoft Entra ID como origen de identidad (a través de IAM Identity Center). Los miembros WorkSpaces del directorio se unen mediante la autenticación nativa de Microsoft Entra y se inscriben en Microsoft Intune mediante el modo controlado por el usuario de Microsoft Windows Autopilot. Los directorios que utilizan Microsoft Entra ID solo admiten licencias Bring Your Own de Windows 10 y 11 WorkSpaces.
- Personalizado: cree un directorio que utilice el proveedor de identidad que prefiera (a través del Centro de identidades de IAM). WorkSpaces en el directorio se administran mediante la solución de administración de dispositivos que elija, por ejemplo. JumpCloud Los directorios que utilizan proveedores de identidad personalizados solo admiten licencias Bring Your Own de Windows 10 y 11 WorkSpaces.

Para ver tutoriales que muestran cómo configurar estos directorios y cómo iniciarlos WorkSpaces, consulteCrear un directorio para WorkSpaces Personal.

> **Tip**
>
> Para obtener información detallada sobre las consideraciones de diseño de directorios y nubes privadas virtuales (VPC) para varios escenarios de implementación, consulte Best Practices for Deplying 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 mediante la WorkSpaces consola y otras tareas mediante la política de grupo. Para obtener más información acerca de la administración de usuarios y grupos, consulte Administrar usuarios en WorkSpaces Personal y Configurar las herramientas de administración de Active Directory para WorkSpaces personal.

> **Note**
>
> - Actualmente, los directorios compartidos no se admiten para su uso con Amazon WorkSpaces.
> - 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.
> - Los conectores Simple AD y AD Connector están disponibles de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD o AD Connector durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.
>
> Para eliminar directorios vacíos, consulte Eliminar un directorio de WorkSpaces Personal. Si eliminas el directorio Simple AD o AD Connector, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

Contenido

- Registrar un AWS Directory Service directorio existente con WorkSpaces Personal
- Selecciona una unidad organizativa para WorkSpaces Personal
- Configurar direcciones IP públicas automáticas para WorkSpaces Personal
- Acceso al dispositivo de control para WorkSpaces personal
- Administrar los permisos de administrador local para WorkSpaces Personal
- Actualizar la cuenta de AD Connector (AD Connector) para WorkSpaces Personal
- Autenticación multifactorial (AD Connector) para personal WorkSpaces
- Crear un directorio para WorkSpaces Personal
- Actualizar los servidores DNS para WorkSpaces Personal
- Eliminar un directorio de WorkSpaces Personal
- Configurar las herramientas de administración de Active Directory para WorkSpaces personal

Registrar un AWS Directory Service directorio existente con WorkSpaces Personal

WorkSpaces Para permitir el uso de un AWS Directory Service directorio existente, debe registrarlo en WorkSpaces. Después de registrar un directorio, puede iniciarlo WorkSpaces en el directorio.

Requisitos

Para registrar un directorio para su uso en él WorkSpaces, debe cumplir los siguientes requisitos:

- Si utilizas AWS Managed Microsoft AD Simple AD, tu directorio puede estar en una subred privada dedicada, siempre que el directorio tenga acceso a la VPC en la que se encuentra WorkSpaces .

Para obtener más información sobre el diseño de directorios y VPC, consulte el documento técnico Best Practices for Deplying Amazon WorkSpaces.

> **Note**
>
> Los conectores Simple AD y AD Connector están disponibles de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD o AD Connector durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.

Para eliminar directorios vacíos, consulte Eliminar un directorio de WorkSpaces Personal. Si eliminas el directorio Simple AD o AD Connector, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

Para registrar un directorio de AWS Directory Service existente

1. Abra la WorkSpaces consola en la versión https://console.aws.amazon.com/workspaces/v2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Create directory.
4. En la página Crear directorio, en WorkSpaces Tipo, elija Personal. Para la administración de WorkSpace dispositivos, elija AWS Directory Service.
5. Seleccione el directorio que desee registrar en la tabla Directorios de AWS Directory Service.
6. Seleccione dos subredes de su VPC que no sean de la misma zona de disponibilidad. Estas subredes se utilizarán para lanzar su. WorkSpaces Para obtener más información, consulte Zonas de disponibilidad para WorkSpaces personal.

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

7. En Habilitar los permisos de autoservicio, seleccione Sí para que los usuarios puedan WorkSpaces reconstruirlos y cambiar el tamaño del volumen, el tipo de procesamiento y el modo de ejecución. La activación puede afectar a la cantidad que pagas por Amazon WorkSpaces. En caso contrario, elija No.
8. Elija Registro. Inicialmente el valor de Registered es `REGISTERING`. Una vez completado el registro, el valor es `Yes`.

Una vez que hayas registrado el AWS Directory Service directorio, puedes crear un directorio personal WorkSpace. Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal.

Cuando haya terminado de usar el directorio con WorkSpaces, puede anular su registro. 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 WorkSpaces consola en la v2/home. 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 deba confirmar la selección, haga clic en Confirm (Confirmar). Cuando se complete la eliminación del registro, el directorio se eliminará del registro y de la lista.

Selecciona una unidad organizativa para WorkSpaces Personal

> **Note**
>
> Esta función solo está disponible para los directorios administrados a través de AWS Directory Service, incluidos AD Connector, AWS Managed Microsoft AD y Simple AD.

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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio.
4. En Dominio y unidad organizativa de destino, seleccione Editar.

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

Configurar direcciones IP públicas automáticas para WorkSpaces Personal

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 personal 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 crear el WorkSpace, debe asociar otra dirección IP elástica de su propiedad al. WorkSpace

Para configurar direcciones IP elásticas

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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. Elija Actualizar.

Acceso al dispositivo de control para WorkSpaces personal

Puede especificar los tipos de dispositivos a los que tiene acceso en WorkSpaces función de la plataforma del dispositivo. Puede utilizar los certificados para restringir el acceso WorkSpaces a dispositivos de confianza (también conocidos como dispositivos gestionados).

Para controlar el acceso de los dispositivos a WorkSpaces

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio.
4. En Opciones de control de acceso, elija Editar.
5. En Dispositivos de confianza, especifique 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 acceso a dispositivos de confianza para WorkSpaces uso personal.
6. Seleccione Save.

Administrar los permisos de administrador local para WorkSpaces Personal

> **Note**
>
> Esta función solo está disponible para los directorios administrados a través de AWS Directory Service, incluidos AD Connector, AWS Managed Microsoft AD y Simple AD.

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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio.
4. En Configuración de administrador local, seleccione Editar.
5. Para garantizar que los usuarios sean administradores locales, elija Habilitar configuración de administrador local.
6. Seleccione Save.

Actualizar la cuenta de AD Connector (AD Connector) para WorkSpaces Personal

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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio y elija Ver detalles.
4. En Cuenta AD Connector, seleccione Editar.
5. Introduzca las credenciales de inicio de sesión de la nueva cuenta.
6. Seleccione Save.

Autenticación multifactorial (AD Connector) para personal WorkSpaces

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

> **Note**
>
> - El servidor RADIUS puede estar alojado en las instalaciones AWS o puede estar alojado de forma local.

- Los nombres de usuario deben coincidir entre Active Directory y su servidor RADIUS.

Para habilitar la autenticación multifactor

1. Abra la WorkSpaces consola en la versión 2/homehttps://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

Crear un directorio para WorkSpaces Personal

WorkSpaces Personal le permite usar directorios gestionados a través de AWS Directory Service ellos para almacenar y administrar información para usted WorkSpaces y sus usuarios. Utilice las siguientes opciones para crear un directorio WorkSpaces personal:

- Crear un directorio de Simple AD.

- Cree un AWS Directory Service para Microsoft Active Directory, también conocido como 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.
- Cree un WorkSpaces directorio de Microsoft Entra ID dedicado.
- Cree un WorkSpaces directorio personalizado dedicado.

> **Note**
>
> - Actualmente, no se admite el uso de directorios compartidos con Amazon WorkSpaces.
> - 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.
> - Los conectores Simple AD y AD Connector están disponibles de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD o AD Connector durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.

Antes de crear un directorio

- WorkSpaces no está disponible en todas las regiones. Verifica las regiones compatibles y selecciona una región para tu WorkSpaces. Para obtener más información sobre las regiones compatibles, consulta WorkSpaces los precios por AWS región.
- Cree una cloud virtual privada al menos con dos subredes privadas. Para obtener más información, consulte Configurar una VPC para personal 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 WorkSpace. Para obtener más información, consulte Proporcione acceso a Internet para WorkSpaces personal.

Para obtener más información sobre cómo eliminar un directorio vacío, consulte Eliminar un directorio de WorkSpaces Personal. Si eliminas el directorio Simple AD o AD Connector, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

Contenido

- Identifique el nombre de la computadora para su directorio WorkSpaces personal
- Crear un directorio AWS administrado de Microsoft AD para WorkSpaces Personal
- Cree un directorio de Simple AD para WorkSpaces Personal
- Cree un AD Connector para WorkSpaces uso personal
- Cree una relación de confianza entre su directorio AWS administrado de Microsoft AD y su dominio local para Personal WorkSpaces
- Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal
- Cree un directorio personalizado dedicado con WorkSpaces Personal

Identifique el nombre de la computadora para su directorio WorkSpaces personal

El valor de nombre de equipo que se muestra para a WorkSpace en la WorkSpaces consola de Amazon varía en función del tipo de ordenador que WorkSpace hayas lanzado (Amazon Linux, Ubuntu o Windows). El nombre de la computadora de a WorkSpace puede estar en uno de estos formatos:

- Amazon Linux: A- *xxxxxxxxxxxxx*
- Red Hat Enterprise Linux: R- *xxxxxxxxxxxxx*
- Rocky Linux: R- *xxxxxxxxxxxxx*
- Ubuntu: U- *xxxxxxxxxxxxx*
- Windows: IP-C *xxxxxx* o WSAMZN- o AMAZ- *xxxxxxx* EC2 *xxxxxxx*

En Windows WorkSpaces, el formato del nombre del equipo viene determinado por el tipo de paquete y, en el caso de que se haya WorkSpaces creado a partir de paquetes públicos o a partir 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 nombres de equipo de Windows WorkSpaces lanzados a partir de paquetes públicos utilizan el formato WSAMZN- en lugar del *xxxxxxx* formato IP-C. *xxxxxx*

En el caso de 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 ordenadores están en formato AMAZ-. EC2 *xxxxxxx* Si la imagen pública se creó el 22 de junio de 2020 o después de esa fecha, los nombres de los ordenadores están en formato WSAMZN-. *xxxxxxx*

En el caso de los paquetes Bring Your Own License (BYOL), de forma predeterminada, se utiliza el *xxxxxxx* formato DESKTOP *xxxxxxx* o EC2 AMAZ para los nombres de equipo.

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 para WorkSpaces Personal.

> **Important**
>
> Una vez creado un WorkSpace , puede cambiar el nombre de su equipo de forma segura. Por ejemplo, puede ejecutar un PowerShell script con el comando `Rename-Computer` en su ordenador WorkSpace o de forma remota. A continuación, se mostrará el valor del nombre de ordenador actualizado para a WorkSpace en la WorkSpaces consola de Amazon.

Crear un directorio AWS administrado de Microsoft AD para WorkSpaces Personal

En este tutorial, crearemos un directorio AWS administrado de Microsoft AD. Para encontrar tutoriales que utilicen las otras opciones, consulte Crear un directorio para WorkSpaces Personal.

En primer lugar, cree un directorio AWS administrado de 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. Añadirá un usuario en el siguiente paso cuando lance. WorkSpace

> **Note**
>
> - Actualmente, los directorios compartidos no se admiten para su uso con Amazon WorkSpaces.

- Si su directorio AWS gestionado de Microsoft AD se ha configurado para la replicación en varias regiones, solo se puede 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.

Para crear un directorio de Microsoft AD AWS administrado

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Create directory.
4. En la página Crear directorio, en WorkSpaces Tipo, elija Personal. A continuación, para la administración de WorkSpace dispositivos, elija AWS Directory Service.
5. Seleccione Crear directorio, que abre la página Configurar un directorio en AWS Directory Service
6. Elija AWS Managed Microsoft AD y luego Siguiente.
7. Configure el directorio del modo siguiente:

   a. En Nombre de la organización, introduzca un nombre de organización único para su directorio (por ejemplo, my-demo-directory). 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 iniciar el suyo WorkSpaces, siga el procedimiento indicado Actualizar los servidores DNS para WorkSpaces Personal para asegurarse de que se actualiza correctamente. WorkSpaces

   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 contraseña, consulte Crear su directorio AWS administrado de Microsoft AD en la Guía de AWS Directory Service administración.

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 Paso siguiente.

8. Elija Create directory.

9. Volverá a la página de creación de un directorio en la WorkSpaces consola. 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`.

Una vez que hayas creado un directorio AWS gestionado de Microsoft AD, puedes registrarlo en Amazon WorkSpaces. Para obtener más información, consulte Registrar un AWS Directory Service directorio existente con WorkSpaces Personal

Cree un directorio de Simple AD para WorkSpaces Personal

En este tutorial, lanzamos uno WorkSpace que usa Simple AD. Para encontrar tutoriales que utilicen las otras opciones, consulte Crear un directorio para WorkSpaces Personal.

> **Note**
>
> - 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 Simple AD, consulte Disponibilidad regional para AWS Directory Service.
> - Simple AD está disponible de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.

Al crear un directorio de Simple AD. AWS Directory Service crea dos servidores de directorios, uno en cada una de las subredes privadas de la VPC. En el directorio hay usuarios inicialmente. Añada un usuario después de crear. WorkSpace Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal

Creación de un directorio de AD sencillo

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Create directory.
4. En la página Crear directorio, en WorkSpaces Tipo, elija Personal. A continuación, para la administración de WorkSpace dispositivos, elija AWS Directory Service.
5. Seleccione Crear directorio, que abre la página Configurar un directorio en AWS Directory Service
6. Seleccione Simple AD y, a continuación, Siguiente.
7. Configure el directorio del modo siguiente:

   a. En Nombre de la organización, introduzca un nombre de organización único para su directorio (por ejemplo, my-example-directory). 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 iniciar el suyo WorkSpaces, siga el procedimiento indicado Actualizar los servidores DNS para WorkSpaces Personal para asegurarse de que se actualiza correctamente. WorkSpaces

   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 Siguiente.
8. Elija Create directory.
9. Volverá a la página de creación de directorio en la WorkSpaces consola. 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 completa las siguientes tareas en su nombre:

- Crea una función de IAM para permitir que el WorkSpaces servicio cree interfaces de red elásticas y enumere sus WorkSpaces directorios. El nombre de este rol es `workspaces_DefaultRole`.
- Configura un directorio AD simple en la VPC que se utiliza para almacenar el usuario y WorkSpace la información. 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 de directorio y otro para WorkSpaces el directorio.

Una vez que hayas creado un directorio Simple AD, puedes registrarlo en Amazon WorkSpaces. Para obtener más información, consulte Registrar un AWS Directory Service directorio existente con WorkSpaces Personal

Cree un AD Connector para WorkSpaces uso personal

En este tutorial vamos a crear un AD Connector. Para encontrar tutoriales que utilicen las otras opciones, consulte Crear un directorio para WorkSpaces Personal.

Creación de un Conector AD

> **Note**
>
> AD Connector está disponible de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio AD Connector durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.
> Para eliminar directorios vacíos, consulte Eliminar un directorio de WorkSpaces Personal.
> Si eliminas tu directorio de AD Connector, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

Para crear una instancia de Conector AD

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/v2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Create directory.
4. En la página Crear directorio, en WorkSpaces Tipo, elija Personal. A continuación, para la administración de WorkSpace dispositivos, elija AWS Directory Service.
5. Seleccione Crear directorio, que abre la página Configurar un directorio en AWS Directory Service
6. Elija AWS Managed Microsoft AD y luego Siguiente.
7. En Nombre de la organización, introduzca un nombre de organización único para su directorio (por ejemplo, my-example-directory). Este nombre debe tener al menos cuatro caracteres, incluir caracteres alfanuméricos y guiones (-), y comenzar o terminar por un carácter distinto de un guion.
8. En Connected directory DNS (DNS de directorio conectado), escriba el nombre completo del directorio local (por ejemplo, «ejemplo.com»).
9. En Connected directory NetBIOS name (Nombre de NetBIOS de directorio conectado), escriba el nombre abreviado del directorio local (por ejemplo, «ejemplo»).
10. 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.

11. En Contraseña de la cuenta del conector y en Confirmar contraseña, introduzca la contraseña del usuario local.
12. 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 del servidor DNS después de iniciar el suyo WorkSpaces, siga el procedimiento indicado Actualizar los servidores DNS para WorkSpaces Personal para asegurarse de que se actualiza correctamente. WorkSpaces

13. (Opcional) En Description (Descripción), escriba una descripción del directorio.
14. Mantenga Size en Small.
15. En VPC, seleccione la VPC.
16. En Subnets, seleccione las subredes. Los servidores DNS que especifique deben ser accesibles desde cada subred.
17. Elija Create directory.
18. Volverá a la página de creación de directorio en la WorkSpaces consola. 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`.

Cree una relación de confianza entre su directorio AWS administrado de Microsoft AD y su dominio local para Personal WorkSpaces

En este tutorial vamos a crear una relación de confianza entre el directorio de AWS Managed Microsoft AD y el dominio en las instalaciones. Para encontrar tutoriales que utilicen las otras opciones, consulte Crear un directorio para WorkSpaces Personal.

> **Note**
>
> El inicio WorkSpaces Cuentas de AWS en un dominio de confianza independiente funciona con Microsoft AD AWS administrado cuando se configura con una relación de confianza con el directorio local. Sin embargo, WorkSpaces el uso de Simple AD o AD Connector no se puede iniciar WorkSpaces para los usuarios de un dominio de confianza.

Para establecer la relación de confianza

1. Configure Microsoft AD AWS administrado en su nube privada virtual (VPC). Para obtener más información, consulte Crear un directorio de Microsoft AD AWS administrado en la Guía de AWS Directory Service administración.

   > **Note**
   >
   > - Actualmente, los directorios compartidos no se admiten para su uso con Amazon WorkSpaces.
   > - Si su directorio AWS gestionado de Microsoft AD se ha configurado para la replicación en varias regiones, solo se puede 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.

2. Cree una relación de confianza entre su Microsoft AD AWS administrado y su dominio local. Asegúrese de que la confianza se configura de manera bidireccional. Para obtener más información, consulte el tutorial: Creación de una relación de confianza entre su Microsoft AD AWS administrado y su dominio local en la Guía de AWS Directory Service administración.

Se puede usar una confianza unidireccional o bidireccional para administrar y autenticar a los usuarios y grupos locales y, por lo tanto WorkSpaces, se WorkSpaces puede aprovisionar a los usuarios y grupos locales. Para obtener más información, consulte Implementación de Amazon WorkSpaces mediante un dominio de recursos de confianza unidireccional con AWS Directory Service.

> **Note**
>
> - Red Hat Enterprise Linux, Rocky Linux y Ubuntu WorkSpaces utilizan System Security Services Daemon (SSSD) para la integración con Active Directory, y SSSD no admite la confianza en los bosques. En su lugar, configure la confianza externa. Se recomienda la confianza bidireccional para Amazon Linux, Ubuntu, Rocky Linux y Red Hat Enterprise Linux. WorkSpaces

- No puede utilizar un navegador web (Web Access) para conectarse a Linux. WorkSpaces

Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal

En este tutorial, creamos Bring Your Own License (BYOL) para Windows 10 y 11 personal WorkSpaces que son Microsoft Entra ID unidos e inscritos en Microsoft Intune. Antes de WorkSpaces crearla, primero tiene que crear un directorio WorkSpaces personal dedicado a Entra ID. WorkSpaces

> **Note**
>
> Microsoft Entra joined personal WorkSpaces está disponible en todas AWS las regiones en las que Amazon WorkSpaces está disponible, excepto en África (Ciudad del Cabo), Israel (Tel Aviv) y China (Ningxia).

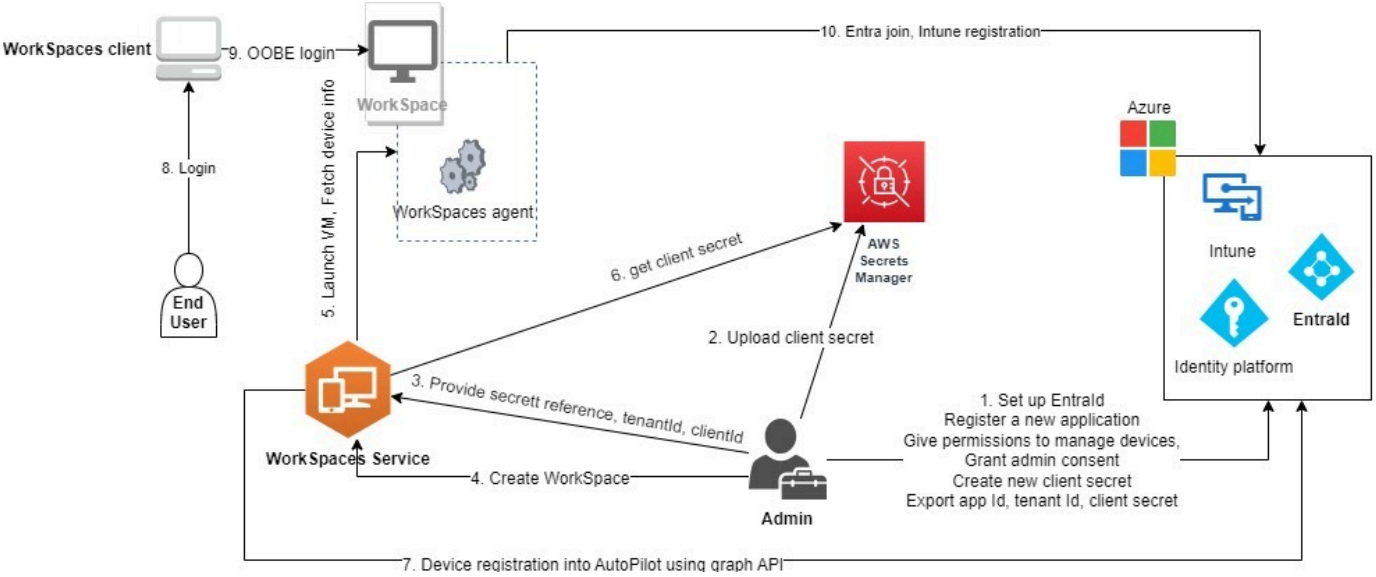
Contenido

- Descripción general
- Requisitos y limitaciones
- Paso 1: habilitar IAM Identity Center y sincronizarlo con Microsoft Entra ID
- Paso 2: registrar una aplicación de Microsoft Entra ID para conceder permisos para Windows Autopilot
- Paso 3: configurar el modo controlado por el usuario de Windows Autopilot
- Paso 4: Crea un secreto AWS Secrets Manager
- Paso 5: Crear un WorkSpaces directorio de Microsoft Entra ID dedicado
- Configure la aplicación IAM Identity Center para un WorkSpaces directorio (opcional)
- Cree una integración entre regiones del IAM Identity Center (opcional)

Descripción general

Un WorkSpaces directorio personal de Microsoft Entra ID contiene toda la información necesaria para iniciar Microsoft Entra ID unida WorkSpaces que se asigna a los usuarios administrados con Microsoft Entra ID. La información del usuario está disponible a WorkSpaces través del Centro de Identidad de AWS IAM, que actúa como intermediario de identidades para transferir la identidad de sus empleados desde Entra ID a. AWS El modo controlado por el usuario del Autopilot de

Microsoft Windows se utiliza para realizar la inscripción WorkSpaces en Intune y unirse a Entra. En el diagrama siguiente se ilustra el proceso de Autopilot.



Requisitos y limitaciones

- Plan P1 de Microsoft Entra ID o posterior.
- Microsoft Entra ID e Intune están habilitados y tienen asignaciones de roles.
- Administrador de Intune: necesario para administrar los perfiles de implementación de Autopilot.
- Administrador global: necesario para conceder el consentimiento del administrador a los permisos de la API asignados a la aplicación creada en el paso 3. La aplicación se puede crear sin este permiso. Sin embargo, un administrador global tendría que dar su consentimiento de administrador a los permisos de la aplicación.
- Asigne licencias de suscripción de usuario de Windows 10/11 VDA, E3 o E5 a sus usuarios. WorkSpaces
- Los directorios Entra ID solo son compatibles con Windows 10 u 11 Bring Your Own License Personal. WorkSpaces A continuación se indican las versiones compatibles.
  - Windows 10 versión 21H2 (actualización de diciembre 2021)
  - Windows 10 versión 22H2 (actualización de noviembre de 2022)
  - Windows 11 Enterprise 23H2 (versión de octubre de 2023)
  - Windows 11 Enterprise 22H2 (versión de octubre de 2022)
- La licencia Bring Your Own License (BYOL) está habilitada para tu AWS cuenta y tienes una imagen BYOL de Windows 10 u 11 válida importada a tu cuenta. Para obtener más información, consulte Traiga sus propias licencias de escritorio de Windows WorkSpaces.

- Los directorios Microsoft Entra ID solo admiten Windows 10 u 11 BYOL personal WorkSpaces.
- Los directorios de Microsoft Entra ID solo admiten el protocolo DCV.

Paso 1: habilitar IAM Identity Center y sincronizarlo con Microsoft Entra ID

Para crear datos personales unidos a Microsoft Entra ID WorkSpaces y asignarlos a sus usuarios de Entra ID, debe hacer que la información del usuario esté disponible a AWS través del Centro de identidades de IAM. El IAM Identity Center es el AWS servicio recomendado para gestionar el acceso de los usuarios a los recursos. AWS Para obtener más información, consulte ¿Qué es Centro de identidades de IAM? Solo tendrá que configurarlo una vez.

Si no dispone de una instancia del IAM Identity Center que pueda integrar con la suya WorkSpaces, le recomendamos que cree una en la misma región que la suya. WorkSpaces Si ya tiene una instancia de AWS Identity Center en una región diferente, puede configurar la integración entre regiones. Para obtener más información sobre la configuración entre regiones, consulte. the section called “ Cree una integración entre regiones del IAM Identity Center (opcional)”

> **Note**
>
> No se admite la integración entre regiones entre el Centro de Identidad de IAM WorkSpaces y el Centro de Identidad de IAM. AWS GovCloud (US) Region

1. Habilite IAM Identity Center con sus AWS Organizaciones, especialmente si utiliza un entorno de varias cuentas. También puede crear una instancia de cuenta de IAM Identity Center. Para obtener más información, consulte Habilitar el centro de identidad de AWS IAM. Cada WorkSpaces directorio se puede asociar a una instancia, organización o cuenta del IAM Identity Center.

   Si utiliza una instancia de organización e intenta crear un WorkSpaces directorio en una de las cuentas de los miembros, asegúrese de tener los siguientes permisos del IAM Identity Center.

   - `"sso:DescribeInstance"`
   - `"sso:CreateApplication"`
   - `"sso:PutApplicationGrant"`
   - `"sso:PutApplicationAuthenticationMethod"`
   - `"sso:DeleteApplication"`

- `"sso:DescribeApplication"`
- `"sso:getApplicationGrant"`

Para obtener más información, consulte Información general sobre la administración de permisos de acceso para los recursos de Centro de identidades de IAM. Además, asegúrese de que ninguna política de control de servicios (SCPs) bloquee estos permisos. Para obtener más información SCPs, consulte Políticas de control de servicios (SCPs).

2. Configure IAM Identity Center y Microsoft Entra ID para sincronizar automáticamente algunos o todos los usuarios del inquilino de Entra ID con la instancia de IAM Identity Center. Para obtener más información, consulte Configurar SAML y SCIM con el ID de Microsoft Entra y el centro de identidad de IAM y el tutorial: Configurar el centro de identidad de AWS IAM para el aprovisionamiento automático de usuarios.
3. Compruebe que los usuarios que configuró en Microsoft Entra ID estén sincronizados correctamente con la instancia del AWS IAM Identity Center. Si aparece un mensaje de error en Microsoft Entra ID, esto indica que el usuario de Entra ID se ha configurado de un modo que IAM Identity Center no lo admite. El mensaje de error identificará este problema. Por ejemplo, si el objeto de usuario de Entra ID carece de nombre, apellido o nombre para mostrar, recibirá un mensaje de error similar a. and/or `"2 validation errors detected: Value at 'name.givenName' failed to satisfy constraint: Member must satisfy regular expression pattern: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\ \r ]+; Value at 'name.givenName' failed to satisfy constraint: Member must have length greater than or equal to 1"` Para obtener más información, consulte Algunos usuarios no logran sincronizarse con Centro de identidades de IAM desde un proveedor de SCIM externo.

> **Note**
>
> WorkSpaces utiliza el atributo Entra ID UserPrincipalName (UPN) para identificar a los usuarios individuales y tiene las siguientes limitaciones:
>
> - UPNs no puede superar los 63 caracteres.
> - Si cambias el UPN después de asignar un WorkSpace a un usuario, el usuario no podrá conectarse a él a WorkSpace menos que cambies el UPN al que tenía antes.

Paso 2: registrar una aplicación de Microsoft Entra ID para conceder permisos para Windows Autopilot

WorkSpaces Personal usa el modo controlado por el usuario del Autopilot de Microsoft Windows para inscribirse en WorkSpaces Microsoft Intune y unirlos a Microsoft Entra ID.

Para permitir que Amazon WorkSpaces registre WorkSpaces Personal en Autopilot, debes registrar una aplicación Microsoft Entra ID que conceda los permisos necesarios de la API de Microsoft Graph. Para obtener más información sobre el registro de una aplicación de Entra ID, consulte Inicio rápido: Registro de una aplicación en la plataforma de identidad de Microsoft.

Le recomendamos proporcionar los siguientes permisos de la API en la aplicación de Entra ID.

- Para crear una nueva cuenta personal WorkSpace que deba unirse a Entra ID, se requiere el siguiente permiso de la API.
  - `DeviceManagementServiceConfig.ReadWrite.All`
- Cuando cancelas una cuenta personal WorkSpace o la reconstruyes, se utilizan los siguientes permisos.

> **Note**
>
> Si no proporciona estos permisos, se WorkSpace cancelarán, pero no se eliminarán de sus usuarios de Intune y Entra ID y tendrá que eliminarlos por separado.

  - `DeviceManagementServiceConfig.ReadWrite.All`
  - `Device.ReadWrite.All`
  - `DeviceManagementManagedDevices.ReadWrite.All`
- Estos permisos requieren el consentimiento del administrador. Para obtener más información, consulte Grant tenant-wide admin consent to an application.

A continuación, debe añadir un secreto de cliente para la aplicación de Entra ID. Para obtener más información, consulte Adición de credenciales. Asegúrese de recordar la cadena de secreto del cliente, ya que la necesitará al crear el secreto de AWS Secrets Manager en el paso 4.

Paso 3: configurar el modo controlado por el usuario de Windows Autopilot

Asegúrese de conocer el Step by step tutorial for Windows Autopilot user-driven Microsoft Entra join in Intune.

Cómo configurar Microsoft Intune para Autopilot

1. Inicio de sesión en el Centro de administración de Microsoft Intune
2. Crea un nuevo grupo de dispositivos de piloto automático para uso personal. WorkSpaces Para obtener más información, consulte Create device groups for Windows Autopilot.
   a. Seleccione Grupos, Nuevo grupo
   b. En Tipo de grupo, seleccione Seguridad.
   c. En Tipo de pertenencia, elija Dispositivo dinámico.
   d. Seleccione Editar consulta dinámica para crear una regla de pertenencia dinámica. La regla debe tener el siguiente formato:

```
(device.devicePhysicalIds -any (_ -eq "[OrderID]:WorkSpacesDirectoryName"))
```

> **Important**
>
> `WorkSpacesDirectoryName`debe coincidir con el nombre del directorio WorkSpaces personal de Entra ID que creaste en el paso 5. Esto se debe a que la cadena del nombre del directorio se utiliza como etiqueta de grupo cuando se WorkSpaces registran escritorios virtuales en Autopilot. Además, la etiqueta de grupo se asigna al atributo `OrderID` en los dispositivos con Microsoft Entra.

3. Seleccione Dispositivos, Windows, Inscripción. En Opciones de inscripción, seleccione Inscripción automática. En Ámbito de usuario de MDM, seleccione Todos.
4. Cree un perfil de implementación de Autopilot. Para obtener más información, consulte Create an Autopilot deployment profile.
   a. En Windows Autopilot, seleccione Perfiles de implementación, Crear perfil.
   b. En la pantalla Perfiles de implementación de Windows Autopilot, seleccione el menú desplegable Crear perfil y elija PC de Windows.
   c. En la pantalla Crear perfil, en la página Sobre la Out-of-box experiencia (OOBE). En Modo de implementación, seleccione Controlado por el usuario. En Vincular a Microsoft Entra ID,

seleccione Vinculado a Microsoft Entra. Puede personalizar los nombres de los ordenadores de los datos personales que tenga registrados en Entra ID WorkSpaces seleccionando Sí en la plantilla de nombre de dispositivo para crear una plantilla que pueda utilizarse al asignar un nombre a un dispositivo durante la inscripción.

d. En la página Asignaciones, en Asignar a, elija Grupos seleccionados. Elija Seleccionar grupos que desea incluir y seleccione el grupo de dispositivos de Autopilot que acaba de crear en el paso 2.

Paso 4: Crea un secreto AWS Secrets Manager

Debe crear un código secreto AWS Secrets Manager para almacenar de forma segura la información, incluidos el ID de la aplicación y el secreto del cliente, de la aplicación Entra ID en la que creóPaso 2: registrar una aplicación de Microsoft Entra ID para conceder permisos para Windows Autopilot. Solo tendrá que configurarlo una vez.

Para crear un AWS Secrets Manager secreto

1. Cree una clave administrada por el cliente en AWS Key Management Service. La clave se utilizará más adelante para cifrar el AWS Secrets Manager secreto. No utilices la clave predeterminada para cifrar el secreto, ya que el servicio no puede acceder a ella. WorkSpaces Siga los pasos que se indican a continuación para crear la clave.

   a. Abre la AWS KMS consola en https://console.aws.amazon.com/kms.
   b. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
   c. Elija Crear clave.
   d. En la página Configurar clave, en Tipo de clave, seleccione Simétrico. En Uso de claves, elija Cifrar y descifrar.
   e. En la página de revisión, en el editor de políticas clave, asegúrate de permitir el `workspaces.amazonaws.com` acceso principal del WorkSpaces servicio a la clave incluyendo los siguientes permisos en la política clave.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "workspaces.amazonaws.com"
        ]
```

```
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

2. Cree el secreto en AWS Secrets Manager, utilizando la AWS KMS clave creada en el paso anterior.

   a. Abra la consola de Secrets Manager en https://console.aws.amazon.com/secretsmanager/.

   b. Elija Almacenar un secreto nuevo.

   c. En la página Seleccionar tipo de secreto, en Tipo de secreto, seleccione Otro tipo de secreto.

   d. En Pares clave/valor, en el cuadro claves, introduzca “application_id” en el cuadro de claves y, a continuación, copie el identificador de la aplicación de Entra ID del paso 2 y péguelo en el cuadro de valores.

   e. Seleccione Añadir fila y, en el cuadro de claves, introduzca “application_password” y, a continuación, copie el secreto de cliente de la aplicación de Entra ID del paso 2 y péguelo en el cuadro de valores.

   f. Elija la AWS KMS clave que creó en el paso anterior en la lista desplegable de claves de cifrado.

   g. Elija Siguiente.

   h. En la página Configurar secreto, introduzca las opciones Nombre del secreto y Descripción.

   i. En la sección Permisos de recursos, seleccione Editar permisos.

   j. Asegúrese de permitir el `workspaces.amazonaws.com` acceso principal del WorkSpaces servicio al secreto incluyendo la siguiente política de recursos en los permisos de recursos.

      JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : [ "workspaces.amazonaws.com"]
```

```
    },
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "*"
  } ]
}
```

Paso 5: Crear un WorkSpaces directorio de Microsoft Entra ID dedicado

Cree un WorkSpaces directorio dedicado que almacene información para los usuarios de Microsoft Entra ID WorkSpaces y Entra ID.

Para crear un directorio de ID de WorkSpaces Entra

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. En la página Crear directorio, en WorkSpaces Tipo, elija Personal. Para la administración de WorkSpace dispositivos, selecciona Microsoft Entra ID.
4. Para el ID de inquilino de Microsoft Entra, introduce el ID de inquilino de Microsoft Entra ID WorkSpaces al que quieres que se una tu directorio. No podrá cambiar el ID de inquilino una vez creado el directorio.
5. Para el identificador y la contraseña de la aplicación Entra ID, selecciona el AWS Secrets Manager secreto que creaste en el paso 4 de la lista desplegable. No podrá cambiar el secreto asociado al directorio una vez creado el directorio. Sin embargo, siempre puedes actualizar el contenido del secreto, incluido el ID de la aplicación Entra ID y su contraseña, a través de la AWS Secrets Manager consola de la dirección https://console.aws.amazon.com/secretsmanager/.
6. Si su instancia del IAM Identity Center se encuentra en la misma AWS región que su WorkSpaces directorio, en User Identity Source, seleccione la instancia del IAM Identity Center que configuró en el paso 1 de la lista desplegable. No podrá cambiar la instancia de IAM Identity Center asociada al directorio una vez creado el directorio.

   Si la instancia del IAM Identity Center se encuentra en una AWS región diferente a la de su WorkSpaces directorio, seleccione Habilitar la interregión y, a continuación, seleccione la región en la lista desplegable.

> **Note**
>
> Si ya tiene una instancia del IAM Identity Center en una región diferente, debe optar por configurar una integración entre regiones. Para obtener más información sobre la configuración entre regiones, consulte. the section called “ Cree una integración entre regiones del IAM Identity Center (opcional)”

7. En Nombre del directorio, introduzca un nombre único para el directorio (por ejemplo, `WorkSpacesDirectoryName`).

> **Important**
>
> El nombre del directorio debe coincidir con el `OrderID` utilizado para crear la consulta dinámica para el grupo de dispositivos de Autopilot que ha creado con Microsoft Intune en el paso 3. La cadena con el nombre del directorio se utiliza como etiqueta de grupo al registrar datos personales WorkSpaces en Windows Autopilot. La etiqueta de grupo se asigna al atributo `OrderID` de los dispositivos con Microsoft Entra.

8. (Opcional) En Description (Descripción), escriba una descripción del directorio.
9. Para la VPC, seleccione la VPC que utilizó para lanzar su. WorkSpaces Para obtener más información, consulte Configurar una VPC para personal WorkSpaces .
10. En Subredes, seleccione dos subredes de la VPC que no sean de la misma zona de disponibilidad. Estas subredes se utilizarán para lanzar su red personal. WorkSpaces Para obtener más información, consulte Zonas de disponibilidad para WorkSpaces personal.

> **Important**
>
> Asegúrese de que las subredes WorkSpaces lanzadas tengan acceso a Internet, lo cual es necesario cuando los usuarios inician sesión en los escritorios de Windows. Para obtener más información, consulte Proporcione acceso a Internet para WorkSpaces personal.

11. Para la configuración, seleccione Activar la opción dedicada. WorkSpace Debe habilitarlo para crear un directorio WorkSpaces personal dedicado al lanzamiento de Bring Your Own License (BYOL) para Windows 10 u 11 personal WorkSpaces.

> **Note**
>
> Si no ves la opción Activar la WorkSpace opción dedicada en Configuración, significa que tu cuenta no está habilitada para BYOL. Para habilitar BYOL en la cuenta, consulte Traiga sus propias licencias de escritorio de Windows WorkSpaces.

12. (Opcional) En el caso de las etiquetas, especifique el valor del par de claves que desee utilizar como personal WorkSpaces en el directorio.
13. Revise el resumen del directorio y elija Crear directorio. Se tarda unos minutos en conectar a su directorio. El estado inicial del directorio es `Creating`. Cuando la creación del directorio se completa, el estado cambia a `Active`.

Una vez creado el directorio, también se crea automáticamente una aplicación de IAM Identity Center. Para buscar el ARN de la aplicación, vaya a la página de resumen del directorio.

Ahora puede usar el directorio para iniciar Windows 10 u 11 personal WorkSpaces que esté inscrito en Microsoft Intune y unido a Microsoft Entra ID. Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal.

Después de crear un directorio WorkSpaces personal, puede crear uno personal WorkSpace. Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal

Configure la aplicación IAM Identity Center para un WorkSpaces directorio (opcional)

Una vez creado el directorio, se crea automáticamente la aplicación correspondiente de IAM Identity Center. Puede encontrar el ARN de la aplicación en la sección Resumen de la página de detalles del directorio. De forma predeterminada, todos los usuarios de la instancia de Identity Center pueden acceder a sus instancias asignadas WorkSpaces sin necesidad de configurar la aplicación de Identity Center correspondiente. Sin embargo, puede gestionar el acceso de los usuarios a WorkSpaces un directorio configurando la asignación de usuarios para la aplicación IAM Identity Center.

Cómo configurar la asignación de usuarios para la aplicación de IAM Identity Center

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En la pestaña de aplicaciones AWS gestionadas, elija la aplicación para el WorkSpaces directorio. Los nombres de las aplicaciones tienen el siguiente formato:`WorkSpaces.wsd-xxxxx`, donde `wsd-xxxxx` está el ID del WorkSpaces directorio.
3. Elija Acciones, Editar detalles.

4. Cambie la opción Método de asignación de usuarios y grupos de No requerir asignaciones a Requerir asignaciones.
5. Seleccione Save changes (Guardar cambios).

Tras realizar este cambio, los usuarios de la instancia de Identity Center perderán el acceso a su asignación a WorkSpaces menos que se les asigne a la aplicación. Para asignar los usuarios a la aplicación, utilice el AWS CLI comando `create-application-assignment` para asignar usuarios o grupos a una aplicación. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

Cree una integración entre regiones del IAM Identity Center (opcional)

Recomendamos que su instancia del IAM Identity Center WorkSpaces y la instancia asociada estén en la misma región. AWS Sin embargo, si ya tiene una instancia del IAM Identity Center configurada en una región diferente de la suya, puede crear una integración entre WorkSpaces regiones. Al crear una integración entre regiones WorkSpaces y el Centro de Identidad de IAM, permite realizar llamadas entre regiones para acceder WorkSpaces a la información de su instancia del Centro de Identidad de IAM y almacenarla, como los atributos de usuario y grupo.

> **Important**
>
> Amazon WorkSpaces admite el centro de identidad de IAM entre regiones y WorkSpaces las integraciones solo para instancias a nivel de organización. WorkSpaces no admite las integraciones del centro de identidad de IAM entre regiones para las instancias a nivel de cuenta. Para obtener más información sobre los tipos de instancias del Centro de Identidad de IAM y sus casos de uso, consulte Descripción de los tipos de instancias del Centro de Identidad de IAM.

Si crea una integración entre regiones entre un WorkSpaces directorio y una instancia del IAM Identity Center, es posible que experimente una mayor latencia durante la implementación WorkSpaces y durante el inicio de sesión debido a las llamadas entre regiones. El aumento de la latencia es proporcional a la distancia entre su WorkSpaces región y la región del centro de identidad de IAM. Le recomendamos que realice pruebas de latencia para su caso de uso específico.

Puede habilitar las conexiones entre regiones del centro de identidad de IAM durante el paso 5: Crear un directorio de ID WorkSpaces de Microsoft Entra dedicado. En cuanto a la fuente de identidad del usuario, elija la instancia del IAM Identity Center en la que haya configurado en el the

section called “Paso 1: habilitar IAM Identity Center y sincronizarlo con Microsoft Entra ID” menú desplegable.

> **Important**
>
> No puede cambiar la instancia del Centro de Identidad de IAM asociada al directorio después de crearla.

Cree un directorio personalizado dedicado con WorkSpaces Personal

Antes de crear un BYOL personal de Windows 10 y 11 WorkSpaces y asignarlo a sus usuarios, gestionado con los proveedores de identidad de AWS IAM Identity Center (IdPs), debe crear un directorio personalizado WorkSpaces dedicado. El personal no WorkSpaces está unido a ningún Active Directory de Microsoft, pero se puede administrar con la solución de administración de dispositivos móviles (MDM) que elija, como JumpCloud. Para obtener más información al respecto JumpCloud, consulte este artículo. Para encontrar tutoriales que utilicen las otras opciones, consulte Crear un directorio para WorkSpaces Personal.

> **Note**
>
> - Amazon no WorkSpaces puede crear ni gestionar cuentas de usuario en cuentas personales WorkSpaces lanzadas en un directorio personalizado. Como administrador, tendrá que administrarlos.
> - El WorkSpaces directorio personalizado está disponible en todas AWS las regiones en las que Amazon WorkSpaces está disponible, excepto en África (Ciudad del Cabo), Israel (Tel Aviv) y China (Ningxia).
> - Amazon no WorkSpaces puede crear ni gestionar cuentas de usuario WorkSpaces mediante directorios personalizados. Para asegurarse de que el software de agente de MDM que utilice pueda crear el perfil de usuario en Windows WorkSpaces, póngase en contacto con los proveedores de soluciones de MDM. La creación del perfil de usuario permite a los usuarios iniciar sesión en el escritorio de Windows desde la pantalla de inicio de sesión de Windows.

Contenido

- Requisitos y limitaciones

- Paso 1: habilitar IAM Identity Center y conectarse con el proveedor de identidades
- Paso 2: Cree un directorio personalizado dedicado WorkSpaces

Requisitos y limitaciones

- Los WorkSpaces directorios personalizados solo son compatibles con Windows 10 u 11 Bring Your Own License Personal. WorkSpaces
- Los WorkSpaces directorios personalizados solo admiten el protocolo DCV.
- Asegúrese de habilitar BYOL en su AWS cuenta y de tener su propio AWS KMS servidor al que WorkSpaces pueda acceder su personal para activar Windows 10 y 11. Para obtener más información, consulte Traiga sus propias licencias de escritorio de Windows WorkSpaces.
- Asegúrese de instalar previamente el software del agente MDM en la imagen BYOL que importó a su cuenta. AWS

Paso 1: habilitar IAM Identity Center y conectarse con el proveedor de identidades

Para asignarla WorkSpaces a los usuarios gestionados con sus proveedores de identidad, la información del usuario debe estar disponible a AWS través del Centro de Identidad de AWS IAM. Recomendamos utilizar el Centro de identidad de IAM para gestionar el acceso de sus usuarios a los AWS recursos. Para obtener más información, consulte ¿Qué es Centro de identidades de IAM? Solo tendrá que configurarlo una vez.

Para poner la información del usuario a disposición de AWS

1. Active el Centro de identidad de IAM. AWS Puede habilitar el Centro de Identidad de IAM en sus AWS organizaciones, especialmente si utiliza un entorno con varias cuentas. También puede crear una instancia de cuenta de IAM Identity Center. Para obtener más información, consulte Habilitar el centro de identidad de AWS IAM. Cada WorkSpaces directorio se puede asociar a una organización o instancia de cuenta del IAM Identity Center. Cada instancia del IAM Identity Center se puede asociar a uno o más directorios WorkSpaces personales.

   Si utiliza una instancia de organización e intenta crear un WorkSpaces directorio en una de las cuentas de los miembros, asegúrese de tener los siguientes permisos del IAM Identity Center.

   - `"sso:DescribeInstance"`
   - `"sso:CreateApplication"`
   - `"sso:PutApplicationGrant"`

- `"sso:PutApplicationAuthenticationMethod"`
- `"sso:DeleteApplication"`
- `"sso:DescribeApplication"`
- `"sso:getApplicationGrant"`

Para obtener más información, consulte Información general sobre la administración de permisos de acceso para los recursos de Centro de identidades de IAM. Asegúrese de que ninguna política de control de servicios (SCPs) bloquee estos permisos. Para obtener más información SCPs, consulte Políticas de control de servicios (SCPs).

2. Configure IAM Identity Center y el proveedor de identidades (IdP) para sincronizar automáticamente los usuarios del IdP con la instancia de IAM Identity Center. Para obtener más información, consulte Tutoriales sobre orígenes de identidad y elija el tutorial específico del IdP que desea utilizar. Por ejemplo, usar el centro de identidad de IAM para conectarse a su plataforma de JumpCloud directorios.
3. Compruebe que los usuarios que configuró en su IDP estén sincronizados correctamente con la instancia del AWS IAM Identity Center. La primera sincronización puede tardar hasta una hora, según la configuración del IdP.

Paso 2: Cree un directorio personalizado dedicado WorkSpaces

Cree un directorio WorkSpaces personal dedicado que almacene información sobre su personal WorkSpaces y sus usuarios.

Para crear un WorkSpaces directorio personalizado dedicado

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Directories (Directorios).
3. Elija Create directory.
4. En la página Crear directorio, como WorkSpacestipo, elija Personal. Para la administración de WorkSpace dispositivos, selecciona Personalizado.
5. En Origen de identidad del usuario, seleccione la instancia de IAM Identity Center que ha configurado en el paso 1 de la lista desplegable. No podrá cambiar la instancia de IAM Identity Center asociada al directorio una vez creado el directorio.

> **Note**
>
> Debe especificar una instancia del IAM Identity Center para el directorio o no podrá iniciar personal WorkSpaces con el directorio mediante la WorkSpaces consola. WorkSpaces Los directorios sin un centro de identidad asociado solo son compatibles con las soluciones de los socios WorkSpaces principales.

6. En Nombre del directorio, introduzca un nombre único para el directorio.
7. En el caso de la VPC, seleccione la VPC que utilizó para lanzar su. WorkSpaces Para obtener más información, consulte Configurar una VPC para personal WorkSpaces .
8. En Subredes, seleccione dos subredes de la VPC que no sean de la misma zona de disponibilidad. Estas subredes se utilizarán para lanzar su red personal. WorkSpaces Para obtener más información, consulte Zonas de disponibilidad para WorkSpaces personal.

> **Important**
>
> Asegúrese de que las subredes WorkSpaces lanzadas tengan acceso a Internet, lo cual es necesario cuando los usuarios inician sesión en los escritorios de Windows. Para obtener más información, consulte Proporcione acceso a Internet para WorkSpaces personal.

9. Para la configuración, seleccione Activar la opción dedicada. WorkSpace Debe habilitarlo para crear un directorio WorkSpaces personal dedicado al lanzamiento de Bring Your Own License (BYOL) para Windows 10 u 11 personal WorkSpaces.
10. (Opcional) En el caso de las etiquetas, especifique el valor del par de claves que desee utilizar como personal WorkSpaces en el directorio.
11. Revise el resumen del directorio y elija Crear directorio. Se tarda unos minutos en conectar a su directorio. El estado inicial del directorio es `Creating`. Cuando la creación del directorio se completa, el estado cambia a `Active`.

Una vez creado el directorio, también se crea automáticamente una aplicación de IAM Identity Center. Para buscar el ARN de la aplicación, vaya a la página de resumen del directorio.

Ahora puede usar el directorio para iniciar Windows 10 u 11 personal WorkSpaces que esté inscrito en Microsoft Intune y unido a Microsoft Entra ID. Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal.

Una vez que haya creado un directorio WorkSpaces personal, podrá crear uno personal WorkSpace. Para obtener más información, consulte Crear un WorkSpace en WorkSpaces personal

Actualizar los servidores DNS para WorkSpaces Personal

Si necesita actualizar las direcciones IP del servidor DNS de su Active Directory después de iniciar el suyo WorkSpaces, también debe actualizarlas WorkSpaces con la nueva configuración del servidor DNS.

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

- Actualice la configuración de DNS WorkSpaces antes de actualizar la configuración de DNS de Active Directory.
- Vuelva a WorkSpaces crearlo después de actualizar la configuración de DNS de Active Directory.

Se recomienda actualizar la configuración de DNS WorkSpaces antes de actualizar la configuración de DNS de Active Directory (tal y como se explica en el paso 1 del procedimiento siguiente).

Si desea volver a crearla, WorkSpaces actualice una de las direcciones IP del servidor DNS de su Active Directory (paso 2) y, a continuación, siga el procedimiento indicado Reconstruir un WorkSpace in WorkSpaces Personal para volver a crear la suya WorkSpaces. Una vez que haya reconstruido la suya WorkSpaces, siga el procedimiento del paso 3 para probar las actualizaciones del servidor DNS. Tras completar ese paso, actualiza la dirección IP del segundo servidor DNS en Active Directory y, a continuación, WorkSpaces vuelve a crearla. 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 ninguna nueva WorkSpaces durante los 15 minutos anteriores y los 15 minutos posteriores a cambiar la 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: Actualiza la configuración del servidor DNS en tu 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*.

Actualice la configuración del servidor DNS para Windows WorkSpaces

Si tiene varios WorkSpaces, puede implementar la siguiente actualización del registro en el WorkSpaces aplicando un objeto de política de grupo (GPO) en la unidad organizativa de Active Directory correspondiente a su WorkSpaces unidad organizativa. Para obtener más información sobre cómo trabajar con GPOs, consulteAdministre su Windows WorkSpaces en WorkSpaces Personal.

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 Windows WorkSpace, abre el cuadro de búsqueda de Windows e ingresa **`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 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 PowerShell comandos para actualizar el registro y reiniciar el servicio SkyLightWorkspaceConfigService.

1. En Windows WorkSpace, abra el cuadro de búsqueda de Windows e introduzca**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, ejecuta 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 la PowerShell ventana, ejecuta 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 para Amazon Linux 2 WorkSpaces

Si tiene más de un Amazon Linux 2 WorkSpace, le recomendamos que utilice una solución de administración de la configuración para distribuir y aplicar la política. Por ejemplo, puede utilizar Ansible.

Para actualizar la configuración del servidor DNS en Amazon Linux 2 WorkSpace

1. En su sistema Linux WorkSpace, abra una ventana de terminal.
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*.

Actualice la configuración del servidor DNS para Ubuntu WorkSpaces

Si tiene más de un Ubuntu WorkSpace, le recomendamos que utilice una solución de administración de la configuración para distribuir y aplicar la política. Por ejemplo, puede usar Landscape.

Para actualizar la configuración del servidor DNS en un Ubuntu WorkSpace

1. En tu Ubuntu WorkSpace, abre una ventana de Terminal y ejecuta el siguiente comando. 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/netplan/zz-workspaces-domain.yaml
```

2. En el archivo yaml, aparecerá el siguiente comando `nameserver`.

```
nameservers:
    search:[Your domain FQDN]
    addresses:[OldIP1, OldIP2]
```

   Sustituya *OldIP1* y *OldIP2* por *NewIP1* y *NewIP2*.

   Si tiene varias direcciones IP de servidores de DNS, añádalas como valores separados por comas. Por ejemplo, `[NewDNSIP1, NewDNSIP2, NewDNSIP3]`.

3. Guarde el archivo yaml.
4. Ejecute el comando `sudo netplan apply` para aplicar los cambios.
5. Ejecute el comando `resolvectl status` para comprobar que se está utilizando la nueva dirección IP de DNS.
6. Continúe con el Paso 2 y actualice la configuración del servidor de DNS en Active Directory.

Actualice la configuración del servidor DNS para Red Hat Enterprise Linux WorkSpaces

Si tiene más de un Red Hat Enterprise Linux WorkSpace, le recomendamos que utilice una solución de administración de la configuración para distribuir y aplicar la política. Por ejemplo, puede utilizar Ansible.

Para actualizar la configuración del servidor DNS en un Red Hat Enterprise Linux WorkSpace

1. En su Red Hat Enterprise Linux WorkSpace, abra una ventana de terminal y ejecute el siguiente comando. 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 nmcli conn modify CustomerNIC ipv4.dns 'NewIP1 NewIP2'
   ```

2. Ejecute el siguiente comando.

   ```
   sudo systemctl restart NetworkManager
   ```

3. Para comprobar la configuración actualizada de la red y el servidor de DNS, ejecute el siguiente comando.

   ```
   nmcli device show eth1
   ```

4. Continúe con el Paso 2 y actualice la configuración del servidor de DNS en Active Directory.

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 Microsoft AD administrado: configure los reenviadores condicionales de 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*.

Pruebe la configuración actualizada del servidor DNS para Windows WorkSpaces

1. Apague el servidor DNS de *OldIP1*.
2. Inicie sesión en Windows WorkSpace.
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.

Pruebe la configuración actualizada del servidor DNS para Linux WorkSpaces

1. Apague el servidor DNS de *OldIP1*.
2. Inicie sesión en un Linux WorkSpace.
3. En tu Linux WorkSpace, abre una ventana de Terminal.
4. Las direcciones IP del servidor DNS devueltas en la respuesta del DHCP se escriben en el `/etc/resolv.conf` archivo local del WorkSpace. Ejecute el siguiente comando para mostrar el contenido del archivo `/etc/resolv.conf` .

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

   Debería ver la siguiente 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 `/etc/resolv.conf` archivo, esos cambios se perderán al WorkSpace reiniciarlo.

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 la siguiente 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 un directorio de WorkSpaces Personal

> **Note**
>
> Los conectores Simple AD y AD Connector están disponibles de forma gratuita para su uso WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD o AD Connector durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.
> Si eliminas el directorio Simple AD o AD Connector, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

¿Qué sucede cuando se elimina un directorio?

Cuando se elimina un AWS Directory Service for Microsoft Active Directory directorio o un AD simple, se eliminan todos los datos y las instantáneas del directorio y no se pueden recuperar. Una vez eliminado el directorio, todas EC2 las instancias de Amazon que estén unidas al directorio

permanecerán intactas. No se puede, sin embargo, utilizar las credenciales del directorio para iniciar sesión en estas instancias. Debes iniciar sesión en estas instancias con una instancia Cuenta de AWS que sea local.

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

Elimine un ID de Entra o un directorio personalizado WorkSpaces

El WorkSpaces directorio Entra ID le permite crear un BYOL para Windows 10 u 11 unido a Entra ID. WorkSpaces Para obtener más información, consulte Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal.

Puede crear WorkSpaces directorios personalizados WorkSpaces que no estén unidos a un dominio de Active Directory, sino que utilicen su propio software de administración de dispositivos y el IAM Identity Center. Para obtener más información, consulte Cree un directorio personalizado dedicado con WorkSpaces Personal.

Para eliminar un ID de Entra o un directorio personalizado WorkSpaces

1. Elimine todo lo que WorkSpaces esté en el directorio. Para obtener más información, consulte Eliminar un archivo WorkSpace en WorkSpaces Personal.
2. En el panel de navegación, elija Directories (Directorios).
3. Seleccione el directorio.
4. Elija Acciones, Eliminar.
5. Cuando se le pida confirmación, introduzca eliminar.

Eliminar un AWS directorio de Directory Service

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

Para anular el registro de un directorio

1. Abra la WorkSpaces consola en la versión 2/homehttps://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.

Eliminación de un directorio

1. Elimine todo WorkSpaces en el directorio. Para obtener más información, consulte Eliminar un archivo WorkSpace en WorkSpaces Personal.
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 WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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, seleccione 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 paquete o una imagen personalizados en WorkSpaces Personal.

Configurar las herramientas de administración de Active Directory para WorkSpaces personal

Realizará la mayoría de las tareas administrativas de su WorkSpaces directorio mediante herramientas de administración de directorios, como las herramientas de administración de Active Directory. Sin embargo, utilizará la WorkSpaces consola para realizar algunas tareas relacionadas con el directorio. Para obtener más información, consulte Administrar directorios para WorkSpaces Personal.

Si crea un directorio con Microsoft AD AWS administrado o Simple AD que incluya cinco o más WorkSpaces, le recomendamos que centralice la administración en una EC2 instancia de Amazon. Aunque puede instalar las herramientas de administración de directorios en un WorkSpace, usar una EC2 instancia de Amazon es una solución más sólida.

Configurar las herramientas de administración de Active Directory

1. Lance una instancia de Amazon EC2 Windows y únala a su WorkSpaces directorio mediante una de las siguientes opciones:
   - Si aún no tienes una instancia de Amazon EC2 Windows, puedes unirla al dominio de tu directorio cuando la lances. Para obtener más información, consulte Cómo unirse sin problemas a una EC2 instancia de Windows en la Guía de AWS Directory Service administración.
   - Si ya tienes una instancia de Amazon EC2 Windows, puedes unirla a tu 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 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 Managed 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 AD Simple, no con AD AWS administrado. Para los directorios creados con AD AWS administrado, consulte Administrar usuarios y grupos en Microsoft AD AWS administrado en la Guía de AWS Directory Service administración.

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 ***username***Propiedades, 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

Puedes crear nuevos usuarios desde la WorkSpaces consola de Amazon solo durante el proceso de lanzamiento de un WorkSpace, y no puedes eliminar usuarios a través de la WorkSpaces consola de Amazon. La mayoría de las tareas de administración de usuarios, incluida la administración de grupos de usuarios, deben realizarse a través del directorio.

> **Important**
>
> Antes de poder eliminar un usuario, debes eliminar el que esté WorkSpace asignado a ese usuario. Para obtener más información, consulte Eliminar un archivo WorkSpace en WorkSpaces Personal.

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

- Si usa Microsoft AD AWS administrado, consulte Administrar usuarios y grupos en Microsoft AD AWS administrado en la Guía de AWS Directory Service administración.
- 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.

Restablecimiento de una contraseña de usuario

Cuando restablezca la contraseña de un usuario, no configure User must change password at next logon. De lo contrario, los usuarios no podrán conectarse a su WorkSpaces. En su lugar, asigne una contraseña temporal segura a cada usuario y pida a los usuarios que cambien manualmente sus contraseñas WorkSpace la próxima vez que inicien sesión.

> **Note**
>
> Si utilizas AD Connector o si tus usuarios se encuentran en la región AWS GovCloud (EE. UU. Oeste), 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.)

Administrar usuarios en WorkSpaces Personal

Cada uno WorkSpace está asignado a un solo usuario y no puede ser compartido por varios usuarios. De forma predeterminada, solo se permite uno WorkSpace por usuario por directorio.

Contenido

- Administrar usuarios en WorkSpaces Personal
- Crear varios WorkSpaces para un usuario en WorkSpaces Personal
- Personalice la forma en que los usuarios inician sesión WorkSpaces en su cuenta WorkSpaces personal
- Habilite las capacidades de WorkSpaces administración de autoservicio para sus usuarios en Personal WorkSpaces
- Habilite la optimización de audio de Amazon Connect para sus usuarios en WorkSpaces Personal
- Habilitar la carga de registros de diagnóstico en Personal WorkSpaces

Administrar usuarios en WorkSpaces Personal

Como administrador de WorkSpaces, puede realizar las siguientes tareas para administrar WorkSpaces los usuarios.

Edición de la información de usuario

Puede utilizar la WorkSpaces consola para editar la información de usuario de un WorkSpace.

> **Note**
>
> Esta función solo está disponible si utiliza Microsoft AD AWS administrado o AD Simple. 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. Si usa Microsoft Entra ID o un WorkSpaces directorio personalizado, puede administrar usuarios y grupos con Microsoft Entra ID o sus proveedores de identidad.

Para editar la información de usuario

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija 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 WorkSpaces consola de Amazon solo durante el proceso de lanzamiento de una WorkSpace, y no puede eliminar usuarios a través de la WorkSpaces consola de Amazon. 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. Realizarás la mayoría de las tareas administrativas de tu WorkSpaces directorio mediante 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 personal.

> **Important**
>
> Antes de poder eliminar un usuario, debe eliminar el WorkSpace asignado a ese usuario. Para obtener más información, consulte Eliminar un archivo WorkSpace en WorkSpaces Personal.

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

- Si usa Microsoft AD AWS administrado, consulte Administrar usuarios y grupos en Microsoft AD AWS administrado en la Guía de AWS Directory Service administración.
- 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. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. En la WorkSpacespágina, utiliza el cuadro de búsqueda para buscar el usuario al que quieres enviar una invitación y, a continuación, selecciona el usuario correspondiente en los resultados WorkSpace de la búsqueda. Solo puedes seleccionar uno WorkSpace a la vez.
4. Seleccione Acciones, Invitar usuario.
5. En la página Invitar a los usuarios a la WorkSpace página, selecciona Enviar invitación.

Crear varios WorkSpaces para un usuario en WorkSpaces Personal

De forma predeterminada, solo puede crear uno WorkSpace por usuario por directorio. Sin embargo, si es necesario, puede crear más de uno WorkSpace para un usuario, en función de la configuración del directorio.

- Si solo tiene un directorio 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 directorio diferente WorkSpace , pero WorkSpaces tienen el mismo código de registro, siempre y cuando todos WorkSpaces estén creados en el mismo directorio de la misma región. AWS
- Si tiene varios directorios para el usuario WorkSpaces, cree el directorio WorkSpaces para el usuario en directorios separados. Puede utilizar el mismo nombre de usuario en los directorios, o puede utilizar diferentes nombres de usuario en los directorios. WorkSpaces Tendrán códigos de registro diferentes.

> **Tip**
>
> Para que puedas localizar fácilmente todos los WorkSpaces que has creado para un usuario, utiliza el mismo nombre de usuario base para cada uno WorkSpace.
> Por ejemplo, si tiene un usuario llamado Mary Major con el nombre de usuario de Active Directory mmajor, WorkSpaces créelo con nombres de usuario como mmajor, mmajor1, mmajor2, mmajor3 u otras variantes, como mmajor_windows o mmajor_linux. Siempre que todos WorkSpaces tengan el mismo nombre de usuario base inicial (mmajor), puedes ordenar por el nombre de usuario de tu WorkSpaces consola WorkSpaces para agrupar todos los de ese usuario.

> **Important**
>
> - Un usuario puede tener una PCo IP y un DCV WorkSpace siempre que ambos WorkSpaces estén ubicados en directorios separados. El mismo usuario no puede tener una PCo IP y un DCV WorkSpace en el mismo directorio.
> - Si va a configurar varios WorkSpaces para utilizarlos con la redirección entre regiones, debe configurarlos WorkSpaces en distintos directorios de distintas AWS regiones y utilizar los mismos nombres de usuario en cada directorio. Para obtener más información sobre el redireccionamiento entre regiones, consulte Redirección entre regiones para Personal WorkSpaces .

Para cambiar de uno a otro WorkSpaces, el usuario inicia sesión con el nombre de usuario y el código de registro asociados a un espacio de trabajo concreto. Si el usuario utiliza una versión 3.0 o

superior de las aplicaciones WorkSpaces cliente para Windows, macOS o Linux, puede asignarles diferentes nombres desde Configuración, administrar la WorkSpaces información de inicio de sesión en la aplicación cliente.

Personalice la forma en que los usuarios inician sesión WorkSpaces en su cuenta WorkSpaces personal

Personalice el acceso de sus usuarios WorkSpaces mediante identificadores de recursos uniformes (URIs) para proporcionar una experiencia de inicio de sesión simplificada que se integre con los flujos de trabajo existentes en su organización. Por ejemplo, puede generar automáticamente un inicio de sesión URIs que registre a sus usuarios mediante su código WorkSpaces 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 WorkSpaces del 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 Personal WorkSpaces .

Puede configurar el acceso mediante URI a WorkSpaces las aplicaciones cliente en los siguientes dispositivos compatibles:

- Equipos Windows
- Equipos macOS
- Equipos con Ubuntu Linux, versiones 18.04, 20.04 y 22.04
- iPads
- Dispositivos Android

Para poder acceder URIs a ellos WorkSpaces, los usuarios deben instalar primero la aplicación cliente para su dispositivo. Para ello, deben abrir https://clients.amazonworkspaces.com/y seguir las instrucciones.

El acceso a los URI puede hacerse con los navegadores Firefox y Chrome en equipos Windows y macOS, con el navegador Firefox en equipos Ubuntu Linux 18.04, 20.04 y 22.04 y con los navegadores Internet Explorer y Microsoft Edge en equipos 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 aplicació n cliente de Linux no permite utilizar el propio directorio workspaces://).

Sintaxis admitida	Descripción
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 de WorkSpaces registro. También rellena automáticamente el nombre de usuario en el campo username (nombre de usuario) y el código de multi-factor authentication (MFA) en el campo MFA code (Código MFA) de la página de inicio de sesión del cliente.
espacios de trabajo://@registrationcode? MFACode=mfa	Registra un usuario mediante su código de WorkSpaces 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 WorkSpaces administración de autoservicio para sus usuarios en Personal WorkSpaces

En WorkSpaces, puede habilitar las capacidades de WorkSpace administración de autoservicio para que sus usuarios tengan más control sobre su experiencia. También puede reducir su carga

de trabajo del equipo 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. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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. Desplácese hacia abajo hasta Permisos de autoservicio y seleccione 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 en grupos establecidos 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 WorkSpaces personal.

  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 cálculo. 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 de funcionamiento. Para obtener más información, consulte Administra el modo de ejecución en WorkSpaces Personal.

> **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 realizando una WorkSpace reconstrucción, los usuarios se desconectan de los suyos y no pueden usarlos ni realizar cambios en ellos WorkSpace. 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. Seleccione Save.

Habilite la optimización de audio de Amazon Connect para sus usuarios en WorkSpaces Personal

En la consola WorkSpaces de administración, puede habilitar la optimización de audio del Panel de control de contactos (CCP) de Amazon Connect para sus WorkSpaces flotas a fin de mejorar la seguridad y habilitar un audio de calidad nativa. Tras habilitar la optimización del audio por CCP, los terminales del cliente procesarán el audio CCP, mientras que los WorkSpaces usuarios podrán interactuar con el CCP desde dentro de sus terminales. WorkSpaces

La optimización de audio del panel de control de contactos (CCP) de Amazon Connect funciona con:

- El cliente de Windows. WorkSpaces
- Amazon Linux y Windows WorkSpaces.
- WorkSpaces mediante PCo IP o DCV.

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 transmisiones de Amazon Connect, consulte el GitHub repositorio enhttps://github.com/aws/amazon-connect-streams. El CCP personalizado que cree es el CCP que utilizarán sus agentes de Amazon Connect en sus servidores. WorkSpaces
- Debe tener un navegador web instalado en los puntos finales del WorkSpaces cliente que sea compatible 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 WorkSpaces consola en la versión 2/homehttps://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. Abre la WorkSpaces consola en la v2/home. 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 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. Abre la WorkSpaces consola en la v2/home. 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 la carga de registros de diagnóstico en Personal WorkSpaces

Para solucionar problemas con los WorkSpaces clientes, habilite la carga automática de registros de diagnóstico. Esta opción es compatible actualmente con 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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. Elija Ver detalles.
6. Seleccione Editar.
7. Seleccione Cargas de registros de diagnóstico
8. Seleccione Save.

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 cargar 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, consulte la referencia de la API WorkSpaces .

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:
> - Cliente de Windows (versión 5.4.0 o posterior)
> - Cliente de macOS (versión 5.8.0 o posterior)
> - Cliente de Ubuntu 22.04 (versión 2023.1)
> - Cliente de Ubuntu 20.04 (versión 2023.1)
> - También puede obtener acceso a la característica de carga de registros de diagnóstico con el cliente de Web Access.

Administrar WorkSpaces personal

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 NVMe, como los controladores ENA y PV, en su ordenador WorkSpaces. Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulte Install or upgrade Elastic Network Adapter (ENA) driver , Controladores NVMe de AWS for Windows instances y Upgrade PV drivers on Windows instances.
> - Asegúrese de actualizar periódicamente los agentes EC2 Config, EC2 EC2 Launch y Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulta Update EC2 Config and EC2 Launch.

Contenido

- Administre su Windows WorkSpaces en WorkSpaces Personal
- Administre su Amazon Linux 2 WorkSpaces en modo WorkSpaces personal
- Administra tu Ubuntu WorkSpaces en modo WorkSpaces personal
- Administre su Rocky Linux WorkSpaces
- Administre su Red Hat Enterprise Linux WorkSpaces
- Optimice WorkSpaces para la comunicación en tiempo real en WorkSpaces Personal
- Administra el modo de ejecución en WorkSpaces Personal
- Administrar aplicaciones en WorkSpaces Personal
- Modificar un WorkSpace en WorkSpaces personal
- Personaliza la marca en WorkSpaces Personal
- Etiquete los recursos en WorkSpaces Personal
- Mantenimiento WorkSpaces personal
- WorkSpaces Cifrado en WorkSpaces modo personal
- Reiniciar un WorkSpace en WorkSpaces Personal
- Reconstruir un WorkSpace in WorkSpaces Personal
- Restaurar un archivo WorkSpace en WorkSpaces Personal
- Microsoft 365 Bring Your Own License (BYOL) en forma personal WorkSpaces
- Actualizar Windows BYOL WorkSpaces en Personal WorkSpaces
- Migrar un WorkSpace archivo en WorkSpaces Personal

- Eliminar un archivo WorkSpace en WorkSpaces Personal

Administre su Windows WorkSpaces en WorkSpaces Personal

Puede usar los objetos de política de grupo (GPOs) para aplicar la configuración y administrar Windows WorkSpaces o los usuarios que forman parte de su WorkSpaces directorio de Windows.

> **Note**
>
> - Si usa Microsoft Entra ID o un WorkSpaces directorio personalizado, puede administrar usuarios y grupos con Microsoft Entra ID o sus proveedores de identidad. Para obtener más información, consulte Cree un directorio de Microsoft Entra ID dedicado con WorkSpaces Personal.
> - Las instancias de Linux no cumplen la política de grupo. Para obtener información sobre la administración de Amazon Linux WorkSpaces, consulteAdministre su Amazon Linux 2 WorkSpaces en modo WorkSpaces personal.

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 PCo IP o DCV.

> **Warning**
>
> La configuración de la política de grupo puede afectar a la experiencia de WorkSpace los 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 IP no admite actualmente la configuración de la política de grupo de los mensajes de inicio de sesión interactivos. PCo WorkSpaces El mensaje de inicio de sesión es compatible con DCV WorkSpaces y los usuarios deben volver a iniciar sesión después de aceptar el banner de inicio de sesión. Los mensajes de inicio de sesión no se admiten cuando el inicio de sesión basado en certificados está activado.

- 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.
- La eliminación de 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 eliminas el grupo de usuarios integrado de la política de seguridad Permitir el inicio de sesión local, WorkSpaces los usuarios de tu PCo IP no podrán conectarse a él a WorkSpaces través de las aplicaciones WorkSpaces cliente. Su PCo IP WorkSpaces tampoco recibirá actualizaciones del software del agente PCo IP. PCoLas actualizaciones del agente IP 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 Activa o desactiva la redirección de entrada de audio para IP PCo o Habilitación o deshabilitación del redireccionamiento de entrada de audio para DCV.
- 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, DCV WorkSpaces no admite la opción «Establecer un límite de tiempo para las sesiones de Servicios de Escritorio Remoto activas pero inactivas». Evite usarla durante las sesiones de DCV, 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 con las que trabajar GPOs, consulteConfigurar las herramientas de administración de Active Directory para WorkSpaces personal.

Contenido

- Instalación de los archivos de plantillas administrativas de política de grupo para DCV
- Administración de la configuración de política de grupo para DCV
- Instale la plantilla administrativa de política de grupo para PCo IP
- Administre la configuración de la política de grupo para la PCo IP
- Establecer la duración máxima de un ticket de Kerberos
- Configurar los ajustes del servidor proxy del dispositivo para acceder a Internet
  - Cómo utilizar el proxy del tráfico de escritorio
  - Recomendación sobre el uso de servidores proxy
- Habilite la compatibilidad con el complemento multimedia Amazon WorkSpaces for Zoom Meeting
  - Habilitación del complemento multimedia de Zoom Meeting
    - Requisitos previos
    - Antes de empezar
    - Instalación de los componentes de Zoom
  - Habilite el complemento multimedia Zoom Meeting para PCo IP
    - Requisitos previos

- Cree la clave de registro en un host de Windows WorkSpaces
- Solución de problemas

Instalación de los archivos de plantillas administrativas de política de grupo para DCV

Para usar la configuración de política de grupo específica de la DCV, debe agregar la plantilla administrativa de la política de grupo `wsp.admx` y `wsp.adml` los archivos de la DCV al almacén central del controlador de dominio de su WorkSpaces directorio. 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 EC2 instancia de administración de directorios WorkSpace o de Amazon que esté unida a su WorkSpaces directorio.

Cómo instalar la plantilla administrativa de política de grupo para DCV

1. Desde un sistema Windows en ejecución WorkSpace, haz 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 EC2 instancia de Amazon 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 EC2 instancia de Amazon 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 *`yourdomainname`* organizativa (OU) 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 *`yourdomainname`* OU (o cualquier OU incluida en ella), 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 acerca de la *`yourdomainname`* OU, consulte Qué se crea en la Guía de AWS Directory Service administración.

7. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
8. Ahora puede usar este objeto de política de grupo del DCV para modificar la configuración de la política de grupo específica WorkSpaces al usar el DCV.

Administración de la configuración de política de grupo para DCV

Para usar la configuración de políticas de grupo para administrar las ventanas WorkSpaces que usan DCV

1. Asegúrese de que la plantilla administrativa de política de WorkSpaces grupo más reciente para DCV esté instalada en el almacén central del controlador de dominio de su WorkSpaces directorio.
2. Compruebe que los archivos de plantilla administrativa estén instalados correctamente. Para obtener más información, consulte Para comprobar que los archivos de plantilla administrativa están instalados correctamente.

Configuración de la compatibilidad con impresoras para DCV

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 DCV) le permite utilizar características específicas de la impresora, como la impresión a doble cara, pero necesita que se instale el controlador de impresora compatible con el 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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la configuración de Configure remote printing.
3. 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.

4. Seleccione Aceptar.
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`**.

Configuración del redireccionamiento del portapapeles (copiar/pegar) para DCV

De forma predeterminada, WorkSpaces admite la redirección bidireccional (copiar/pegar) del portapapeles. 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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la configuración Configure clipboard redirection.
3. 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.

4. Seleccione Aceptar.
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.

Establecimiento del tiempo de espera de reanudación de la sesión para DCV

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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Activar/desactivar la reconexión automática.
3. 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).
4. Seleccione Aceptar.
5. El cambio en la configuración de la política de grupo se aplica 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`**.

Habilitación o deshabilitación del redireccionamiento de entrada de vídeo para DCV

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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Activar/desactivar el redireccionamiento de entrada de vídeo.
3. En el cuadro de diálogo Activar/desactivar el redireccionamiento de entrada de vídeo, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
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`**.

Habilitación o deshabilitación del redireccionamiento de entrada de audio para DCV

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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.

2. Abra la opción Activar/desactivar el redireccionamiento de entrada de audio.
3. En el cuadro de diálogo Activar/desactivar el redireccionamiento de entrada de vídeo, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
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`**.

Habilitación o deshabilitación del redireccionamiento de salida de audio para DCV

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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Activar/desactivar el redireccionamiento de salida de audio.
3. En el cuadro de diálogo Activar/desactivar el redireccionamiento de salida de audio, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
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, selecciona y WorkSpace, a continuación, selecciona Acciones > Reiniciar WorkSpaces.
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Deshabilitación del redireccionamiento de zona horaria para DCV

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.
- Los usuarios que viajan mucho quieren 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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Activar/desactivar el redireccionamiento de zona horaria.
3. En el cuadro de diálogo Activar/desactivar el redireccionamiento de zona horaria, seleccione Desactivado.
4. Seleccione Aceptar.
5. El cambio en la configuración de la política de grupo se aplica 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`**.
6. 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.

Establecimiento de la configuración de seguridad de DCV

En el caso de DCV, los datos en tránsito se cifran mediante el cifrado 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- -GCM- AES128 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 utilizar la configuración de la política de grupo para modificar el modo de seguridad TLS y añadir 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.

Cómo configurar la seguridad de DCV

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra Configurar los ajustes de seguridad.
3. 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.
4. Seleccione Aceptar.
5. 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`**.

Configuración de las extensiones para DCV

De forma predeterminada, la compatibilidad WorkSpaces con las extensiones está deshabilitada. Si es necesario, puede configurar el uso WorkSpace de las 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.

Cómo configurar las extensiones para DCV

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Configurar extensiones.
3. 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.
4. Seleccione Aceptar.
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, selecciona y WorkSpace, a continuación, selecciona Acciones, Reiniciar WorkSpaces.
   - En el símbolo del sistema administrativo, introduzca **`gpupdate /force`**.

Habilitación o deshabilitación del redireccionamiento de tarjetas inteligencias para DCV

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 en WorkSpaces Personal.

Para habilitar o deshabilitar la redirección de tarjetas inteligentes para Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Activar/desactivar el redireccionamiento de tarjetas inteligentes.
3. En el cuadro de diálogo Activar/desactivar el redireccionamiento de tarjetas inteligentes, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
5. El cambio en la configuración de la política de grupo se aplica después de reiniciar la WorkSpace 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 WebAuthn (FIDO2) la redirección para DCV

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 (FIDO2) la redirección para el DCV requiere lo siguiente:

- Agente de host de DCV, versión 2.0.0.1425 o posterior
- WorkSpaces clientes:
  - Linux Ubuntu 22.04 2023.3 o posterior
  - Windows 5.19.0 o posterior
  - Cliente de Mac 5.19.0 o posterior
- 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 FIDO2 compatibles, para completar el proceso de autenticación.

Para habilitar o deshabilitar la redirección WebAuthn (FIDO2) para Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la configuración de activar/desactivar WebAuthn la redirección.
3. En el cuadro de diálogo Activar/desactivar el WebAuthn redireccionamiento, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
5. 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. Luego, 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 los usuarios que habiliten la extensión de navegador en el navegador.

> **Note**
>
> Se trata de una petición de navegador que se realice una vez. Los usuarios recibirán la notificación cuando actualice el agente de DCV a la versión 2.0.0.1425 o posterior. Si los usuarios finales no necesitan la WebAuthn redirección, pueden simplemente 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 los 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.

Descripción de la mensajería nativa WebAuthn de la extensión de redireccionamiento

WebAuthn La redirección en los navegadores Chrome y Edge utiliza una extensión de navegador y un servidor de mensajería nativo. El host de mensajería nativo es un componente que permite la comunicación entre la extensión y la aplicación host. En una configuración típica, el navegador permite todos los hosts de mensajería nativos de forma predeterminada. Sin embargo, puede optar por utilizar una lista de mensajes bloqueados nativa, donde el valor de * significa que se deniegan todos los hosts de mensajería nativos a menos que se permita explícitamente. En este caso, debe habilitar el host de mensajería nativo de Amazon DCV WebAuthn Redirection especificando explícitamente el valor `com.dcv.webauthnredirection.nativemessagehost` en la lista de permitidos.

Para obtener más información, siga las instrucciones de su navegador:

- Para Google Chrome, consulta Hosts permitidos para la mensajería nativa.
- Para Microsoft Edge, consulte Mensajería nativa.

Administración e instalación de 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.

En el caso de Microsoft Edge

1. Descargue e instale la plantilla administrativa de Microsoft Edge.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon 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 Configuración del equipo, Plantillas administrativas, Microsoft Edge y Extensiones.
9. Abra el ajuste Configurar ajustes de administración de extensiones y establézcalo en Habilitado.
10. En Configurar 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 surtirá efecto después de que se reinicie la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. Luego, selecciona Acciones, Reiniciar WorkSpaces).

> **Note**
>
> Para bloquear la instalación de la extensión, aplique el siguiente ajuste de administración de configuración:
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

En el caso de Google Chrome

1. Descargue e instale la plantilla administrativa de Google Chrome. Para obtener más información, consulta Cómo configurar las políticas del navegador Chrome como gestionado PCs.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon 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 Configuración del equipo, Plantillas administrativas, Google Chrome y Extensiones.
9. Abra el ajuste Configurar ajustes de administración de extensiones y establézcalo en Habilitado.
10. En Configurar 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 surtirá efecto después de que se reinicie la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. Luego, selecciona Acciones, Reiniciar WorkSpaces).

> **Note**
>
> Para bloquear la instalación de la extensión, aplique el siguiente ajuste de administración de configuración:
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Habilitación o deshabilitación del redireccionamiento de WebRTC para DCV

La redirección WebRTC mejora la comunicación en tiempo real al transferir el procesamiento WorkSpaces de audio y vídeo al cliente local, lo que mejora el rendimiento y reduce la latencia. Sin embargo, la redirección de WebRTC no es universal y requiere que los proveedores de aplicaciones de terceros desarrollen integraciones específicas con ella. WorkSpaces De forma predeterminada, la redirección WebRTC no está habilitada. WorkSpaces Para utilizar el redireccionamiento de WebRTC, asegúrese de lo siguiente:

- La integración de proveedores de aplicaciones de terceros
- WorkSpaces las extensiones se habilitan mediante la configuración de la política de grupo
- El redireccionamiento de WebRTC esté habilitado
- La extensión del navegador de redireccionamiento de WebRTC esté instalada y habilitada

> **Note**
>
> Esta redirección se implementa como una extensión y requiere que habilite la compatibilidad con las WorkSpaces extensiones mediante la configuración de la política de grupo. Si las extensiones están deshabilitadas, el redireccionamiento de WebRTC no funcionará.

Requisitos

El redireccionamiento de WebRTC para DCV requiere lo siguiente:

- Agente de host de DCV, versión 2.0.0.1622 o posterior
- WorkSpaces clientes:

  - Windows 5.21.0 o posterior
  - Cliente web
- Navegadores web instalados en los WorkSpaces que ejecuta la extensión de redireccionamiento WebRTC de Amazon DCV:
  - Google Chrome 116+
  - Microsoft Edge 116+

Habilitar o deshabilitar la redirección WebRTC para Windows WorkSpaces

Si es necesario, puede habilitar o deshabilitar la compatibilidad con la redirección WebRTC para WorkSpaces Windows mediante la configuración de la política de grupo. Si deshabilita o no establece esta configuración, el redireccionamiento de WebRTC se deshabilitará.

Cuando la función esté habilitada, las aplicaciones web que estén integradas con Amazon WorkSpaces podrán redirigir las llamadas a la API de WebRTC al cliente local.

Para habilitar o deshabilitar la redirección WebRTC para Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Configurar el redireccionamiento de WebRTC.
3. En el cuadro de diálogo Configurar el redireccionamiento de WebRTC, seleccione Habilitado o Deshabilitado.
4. Seleccione Aceptar.
5. El cambio en la configuración de la política de grupo surte efecto 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. Luego, selecciona Acciones, Reiniciar WorkSpaces).

Instalación de la extensión de redireccionamiento de WebRTC de Amazon DCV

Los usuarios instalan la extensión de redireccionamiento de WebRTC de Amazon DCV para usar el redireccionamiento de WebRTC después de habilitar la característica. Para ello, deberán llevar a cabo una de las siguientes acciones:

- Se les pedirá a los usuarios que habiliten la extensión de navegador en el navegador.

> **Note**
>
> Como petición de navegador que se realiza una vez, los usuarios recibirán la notificación cuando habilite el redireccionamiento de WebRTC.

- Puede forzar la instalación de la extensión de redireccionamiento para los 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.

Administración e instalación de la extensión del navegador mediante la política de grupo

Puede instalar la extensión de redireccionamiento de WebRTC de Amazon DCV mediante una política de grupo, ya sea de forma centralizada desde el dominio para los hosts de sesión que estén vinculados a un dominio de Active Directory (AD) o mediante el editor de políticas de grupo local para cada host de sesión. Este proceso será diferente según el navegador que utilice.

En el caso de Microsoft Edge

1. Descargue e instale la plantilla administrativa de Microsoft Edge.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon 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 Configuración del equipo, Plantillas administrativas, Microsoft Edge y Extensiones.
9. Abra el ajuste Configurar ajustes de administración de extensiones y establézcalo en Habilitado.
10. En Configurar ajustes de administración de extensiones, introduzca lo siguiente:

```
{"kjbbkjjiecchbcdoollhgffghfjnbhef":
{"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 surtirá efecto después de que se reinicie la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. Luego, selecciona Acciones, Reiniciar WorkSpaces).

> **Note**
>
> Para bloquear la instalación de la extensión, aplique el siguiente ajuste de administración de configuración:
>
> ```
> {"kjbbkjjiecchbcdoollhgffghfjnbhef":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

En el caso de Google Chrome

1. Descargue e instale la plantilla administrativa de Google Chrome. Para obtener más información, consulta Cómo configurar las políticas del navegador Chrome como gestionado PCs.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon 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 Configuración del equipo, Plantillas administrativas, Google Chrome y Extensiones.

9. Abra el ajuste Configurar ajustes de administración de extensiones y establézcalo en Habilitado.
10. En Configurar ajustes de administración de extensiones, introduzca lo siguiente:

```
{"diilpfplcnhehakckkpmcmibmhbingnd":
{ "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 surtirá efecto después de que se reinicie la WorkSpace sesión. Para aplicar los cambios en la política de grupo, reiníciela WorkSpace yendo a la WorkSpaces consola de Amazon y seleccionando WorkSpace. Luego, selecciona Acciones, Reiniciar WorkSpaces).

> **Note**
>
> Para bloquear la instalación de la extensión, aplique el siguiente ajuste de administración de configuración:
>
> ```
> {"diilpfplcnhehakckkpmcmibmhbingnd":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

Habilitación o deshabilitación de la sesión de desconexión en el bloqueo de pantalla para DCV

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, según el 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 en WorkSpaces Personal.

Para habilitar o deshabilitar la sesión de desconexión mediante el bloqueo de pantalla para Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Activar/desactivar la sesión de desconexión en el bloqueo de pantalla.
3. En el cuadro de diálogo Activar/desactivar la sesión de desconexión en el bloqueo de pantalla, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
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`**.

Habilitación o deshabilitación del controlador de pantalla indirecta (IDD) para DCV

De forma predeterminada, WorkSpaces admite el uso del controlador de pantalla indirecto (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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la configuración Habilitar el controlador de pantalla AWS indirecta.
3. En el cuadro de diálogo Habilitar el controlador de pantalla AWS indirecta, seleccione Activado o Desactivado.
4. Seleccione Aceptar.

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:

   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`.

Configuración de los ajustes de pantalla para DCV

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 YUV42 0. Al seleccionar Activar YUV444 codificación, se activa la YUV444 codificación 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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Configurar los ajustes de visualización.
3. 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.
4. Seleccione Aceptar.
5. El cambio en la configuración de la política de grupo se efectuará 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:
   - 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`**.

Activa o desactiva VSync el controlador de solo pantalla AWS virtual para DCV

De forma predeterminada, WorkSpaces admite el uso de la VSync función para el controlador de solo pantalla AWS virtual. Si es necesario para Windows WorkSpaces, puede usar la configuración de la política de grupo para deshabilitar esta función.

Para habilitarla o deshabilitarla VSync en Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la VSync función Activar de la configuración del controlador de pantalla AWS virtual únicamente.
3. En la VSync función Activar del cuadro de diálogo del controlador de solo pantalla AWS virtual, seleccione Activado o Desactivado.
4. Seleccione Aceptar.
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 política de grupo, realice una de las siguientes acciones:

a. Reinicie la WorkSpace realizando 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 el símbolo del sistema administrativo, introduzca `gpupdate /force`.

b. Vuelva a conectarse a WorkSpace la para aplicar la configuración.

c. Vuelva a reiniciar el escritorio de WorkSpaces.

Configuración de la verbosidad del registro para DCV

De forma predeterminada, el nivel de detalle del registro de DCV 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. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra la opción Configurar la verbosidad del registro.
3. 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.
4. Seleccione Aceptar.
5. El cambio en la configuración de la política de grupo se aplica después de la siguiente actualización de la política de grupo para la WorkSpace sesión y después de reiniciarla. WorkSpace 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`**.

Configuración del tiempo de espera de desconexión por inactividad para DCV

WorkSpaces permite configurar el tiempo que un usuario puede permanecer inactivo mientras está conectado a una WorkSpace antes de que se desconecte. A continuación se muestran ejemplos de entrada de actividad del usuario:

- Eventos de teclado
- Eventos del ratón (movimiento del cursor, desplazamiento, hacer clic)
- Eventos de lápiz óptico
- Eventos táctiles (tocar pantallas táctiles, tabletas)
- Eventos de gamepad
- Operaciones de almacenamiento de archivos (cargas, descargas, creación de directorios, elementos de listas)
- Streaming por cámara web

La entrada y salida de audio y los cambios de píxeles no se consideran actividad del usuario.

Al habilitar el tiempo de espera de desconexión por inactividad, también puede notificar al usuario que la sesión se desconectará dentro del tiempo configurado, a menos que interactúe.

De forma predeterminada, el tiempo de espera de desconexión por inactividad está deshabilitado, el valor del tiempo de espera está establecido en 0 minutos y la notificación está deshabilitada. Si habilita esta configuración de política, el valor del tiempo de espera de desconexión por inactividad se establece de forma predeterminada en 60 minutos y el valor de la advertencia de desconexión por inactividad se establece de forma predeterminada en 60 segundos. WorkSpacesEn Windows, puede usar la configuración de la política de grupo para configurar esta función.

Para configurar el tiempo de espera de desconexión por inactividad para Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra el ajuste Configurar tiempo de espera de desconexión por inactividad.

3. En el cuadro de diálogo Configurar tiempo de espera de desconexión por inactividad, elija Habilitado y, a continuación, establezca el valor de tiempo de espera de desconexión que desee (en minutos) y, de forma opcional, el valor del temporizador de advertencia (en segundos).
4. Elija Apply (Aplicar), OK (Aceptar).
5. El cambio realizado en la configuración de la política de grupo se aplicará inmediatamente después de aplicar el cambio.

Configuración de la transferencia de archivos para DCV

De forma predeterminada, Amazon WorkSpaces desactiva la función de transferencia de archivos. Puede habilitarla para permitir a los usuarios cargar y descargar archivos entre su ordenador local y la WorkSpaces sesión. Los archivos se guardarán en la carpeta Mi almacenamiento de la WorkSpaces sesión.

Para habilitar la transferencia de archivos para Windows WorkSpaces

1. En el editor de administración de políticas de grupo, elija Configuración de equipo, Políticas, Plantillas administrativas, Amazon y DCV.
2. Abra el ajuste Configurar el almacenamiento de la sesión.
3. En el cuadro de diálogo Configurar el almacenamiento de la sesión, seleccione Habilitado.
4. (Opcional) Especifique una carpeta para el almacenamiento de la sesión (por ejemplo, `c:/session-storage`). Si no se especifica, la carpeta predeterminada para el almacenamiento de la sesión será la carpeta de inicio.
5. Puede configurarla WorkSpaces con una de las siguientes opciones de transferencia de archivos:
   - Elija `Download and Upload` para permitir la transferencia de archivos bidireccional.
   - Elija `Upload Only` permitir que solo se carguen archivos desde un ordenador local a su WorkSpaces sesión.
   - Elija `Download Only` permitir únicamente la descarga de archivos de la WorkSpaces sesión a un equipo local.
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 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`**.

Instale la plantilla administrativa de política de grupo para PCo IP

Para utilizar la configuración de política de grupo específica de Amazon WorkSpaces cuando utilice el protocolo PCo IP, debe añadir la plantilla administrativa de política de grupo adecuada a la versión del agente PCo IP (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 utilizar 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`pcoip_agent.exe`, busque y compruebe su valor en la columna Plataforma para determinar si el agente PCo IP es de 32 o 64 bits. (Es posible que vea una combinación de WorkSpaces componentes de 32 y 64 bits; esto es normal).

Instale la plantilla administrativa de política de grupo para PCo IP (32 bits)

Para usar la configuración de política de grupo específica para WorkSpaces el uso del protocolo PCo IP con el agente PCo IP de 32 bits, debe instalar la plantilla administrativa de política de grupo para

PCo IP. Realice el siguiente procedimiento en una EC2 instancia de administración de directorios WorkSpace o de Amazon 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 política de grupo para PCo IP

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 administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a tu WorkSpaces directorio, abre la herramienta de administración de políticas de grupo (gpmc.msc) y navega hasta la unidad organizativa de tu dominio que contiene las cuentas de tu 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, introduce un nombre descriptivo para el GPO, como Políticas de WorkSpaces máquina, y deja 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. A partir de ahora, puede utilizar este objeto de directiva de grupo para modificar las opciones de configuración de la directiva de grupo específicas de WorkSpaces.

Para comprobar que el archivo de plantilla administrativa está instalado correctamente

1. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon 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 sus cuentas de WorkSpaces máquina y selecciónelo. Elija Action, Edit en el menú principal.

2. En el editor de administración de políticas de grupo, seleccione Configuración del equipo, Políticas, Plantillas administrativas, Plantillas administrativas clásicas y Variables de sesión PCo IP.
3. Ahora puede usar este objeto de política de grupo de variables de sesión PCo IP para modificar la configuración de política de grupo que es específica de Amazon WorkSpaces cuando usa PCo IP.

> **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.

Instale la plantilla administrativa de política de grupo para PCo IP (64 bits)

Para usar la configuración de política de grupo específica del protocolo PCo IP, debe agregar la plantilla administrativa de la política de grupo `PCoIP.admx` y `PCoIP.adml` los archivos de PCo IP al almacén central del controlador de dominio de su WorkSpaces directorio. 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 EC2 instancia de administración de directorios WorkSpace o de Amazon que esté unida a su WorkSpaces directorio.

Para instalar los archivos de plantilla administrativa de la política de grupo para PCo IP

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 EC2 instancia de Amazon 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 EC2 instancia de Amazon 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 *`yourdomainname`* organizativa (OU) 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 *yourdomainname* OU (o cualquier OU incluida en ella), 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 acerca de la *yourdomainname* OU, consulte Qué se crea en la Guía de AWS Directory Service administración.

7. En el editor de administración de políticas de grupo, elija Configuración del equipo, políticas, plantillas administrativas y variables de sesión PCo IP.
8. Ahora puede usar este objeto de política de grupo de variables de sesión PCo IP para modificar la configuración de la política de grupo específica WorkSpaces cuando se usa PCo IP.

> **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 la política de grupo para la PCo IP

Use la configuración de la política de grupo para administrar las ventanas WorkSpaces que usan PCo IP.

Configure el soporte de la impresora para PCo IP

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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
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 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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
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 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 IP PCo

De forma predeterminada, admite la redirección del WorkSpaces portapapeles. 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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
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 IP PCo

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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
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 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 de entrada de audio para IP PCo

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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
3. Abre la opción Activar/desactivar el audio en la configuración de la sesión PCo IP.
4. En el cuadro de diálogo Activar/desactivar el audio en la sesión PCo IP, 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 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`**.

Inhabilite la redirección de zona horaria para IP PCo

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.

- Los usuarios que viajan mucho quieren 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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
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 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.

Configure los ajustes de seguridad PCo IP

En el PCo caso de la IP, los datos en tránsito se cifran mediante el cifrado TLS 1.2 y la firma de solicitudes SigV4. El protocolo PCo IP 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 PCo IP.

También puede usar esta configuración de política de grupo para modificar el modo de seguridad TLS y bloquear determinados conjuntos de cifrado. En el cuadro de diálogo Configurar la política de grupo de ajustes de seguridad PCo IP se ofrece una explicación detallada de estas opciones y de los conjuntos de cifrado compatibles.

Para configurar los ajustes PCo de seguridad IP

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpaces grupo más reciente para PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
3. Abre la opción Configurar los ajustes de seguridad PCo IP.
4. En el cuadro de diálogo Configurar los ajustes de seguridad PCo IP, seleccione Activado. Para establecer el cifrado predeterminado para el tráfico de streaming en 256 bits, vaya a la opción Cifrados de datos PCo IP y seleccione únicamente AES-256-GCM.
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 se proporcionan en el cuadro de diálogo Configurar los ajustes de seguridad IP. PCo
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 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 PCo IP (32 bits) o la plantilla administrativa de política de WorkSpaces grupo para PCo IP (64 bits) más reciente.
2. En una administración de directorios WorkSpace o en una EC2 instancia de Amazon que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión PCo IP.
3. Abra la opción Activar/desactivar USB en la sesión de PCoIP.
4. Seleccione Habilitada y, a continuación, elija OK.
5. Abre la opción Configurar las reglas de dispositivos PCo IP USB permitidos y no permitidos.
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 VID/PID combinación es 1xxxxaaaa, donde xxxx es el VID en formato hexadecimal y aaaa es el PID en formato hexadecimal. Para este ejemplo, 1050 es el VID, y 0407 es el PID. Para obtener más valores de USB, consulte Valores de ID de YubiKey USB. YubiKey
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 authorization/unauthorization reglas, consulte Teradici PCo IP Standard Agent 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 WorkSpaces administración de autoservicio para sus usuarios en Personal WorkSpaces .

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

Para DCV 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.

DCV 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 a la web 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

Con el complemento Zoom VDI, Zoom admite una comunicación optimizada en tiempo real para DCV e PCo IP basados en Windows WorkSpaces. 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 celebra en casa del usuario. WorkSpace

Habilitación del complemento multimedia de Zoom Meeting

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 utilizar el complemento, asegúrese de que se cumplen los siguientes requisitos.

- WorkSpaces Cliente 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 el ajuste de política de grupo Extensiones. Para obtener más información, consulte Configuración de las extensiones para DCV.

2. Deshabilite el ajuste de política de grupo Reconexión automática. Para obtener más información, consulte Establecimiento del tiempo de espera de reanudación de la sesión para DCV.

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 Using Zoom for 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 optimiza el tráfico de Zoom confirmando que el estado del complemento de VDI aparece como Conectado en el cliente Zoom VDI. Para obtener más información, consulta Cómo confirmar la WorkSpaces optimización de Amazon.

Habilite el complemento multimedia Zoom Meeting para PCo IP

Los usuarios con permiso administrativo para Active Directory pueden generar una clave de registro con el objeto de política de grupo (GPO). Esto permite a los usuarios enviar la clave de registro a todos los WorkSpaces Windows 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 utilizar 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. Seleccione el nuevo DWORD y cambie la opción 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.

Solución de problemas

Realice las siguientes acciones para solucionar los problemas de Zoom en Windows. WorkSpaces

- Confirme que la clave de registro se ha activado y aplicado de forma correcta.
- 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 Soporte través del Soporte 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 2 WorkSpaces en modo WorkSpaces personal

Para las cargas de trabajo que requieren RPM Package Manager (RPM), recomendamos usar Red Hat Enterprise Linux o Rocky Linux. Es posible que Amazon Linux 2 no proporcione las versiones más recientes de algunas aplicaciones y bibliotecas, como Firefox y glibc, que pueda necesitar.

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 Ansible.

> **Note**
>
> La redirección de impresoras locales no está disponible para Amazon Linux. WorkSpaces

Controle el comportamiento del DCV en Amazon Linux WorkSpaces

El comportamiento de DCV 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 DCV tienen actualmente las siguientes limitaciones:
> - Actualmente, solo está disponible 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 DCV Amazon Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección del portapapeles. Utilice el archivo de configuración de DCV 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 DCV 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 son: *X*
   ```

`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 DCV Amazon Linux WorkSpaces

De forma predeterminada, admite la redirección de entrada de audio WorkSpaces . Utilice el archivo de configuración de DCV para deshabilitar 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 DCV 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 para son: *X*

   `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 DCV 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 de DCV 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 DCV 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 son: *X*

   habilitado: el redireccionamiento de zona horaria está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento de zona horaria está deshabilitado

Controle el comportamiento del agente PCo IP en Amazon Linux WorkSpaces

El comportamiento del agente PCo IP se controla mediante los ajustes de configuración del `pcoip-agent.conf` archivo, que se encuentra en el `/etc/pcoip-agent/` directorio. 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 IP | PCo Amazon Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección del portapapeles. Utilice la configuración del agente PCo IP para deshabilitar esta función, si es necesario. Esta configuración se aplica al reiniciar el WorkSpace.

Para configurar la redirección del portapapeles para IP: PCo 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 son: *X*

   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 los canales virtuales PCo IP en la documentación de Teradici.

Habilitar o deshabilitar la redirección de entrada de audio para IP Amazon Linux PCo WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de audio. Utilice la configuración del agente PCo IP para deshabilitar esta función, si es necesario. Esta configuración se aplica al reiniciar el WorkSpace.

Para habilitar o deshabilitar la redirección de entrada de audio para IP | Amazon Linux PCo 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 para son: *X*

   0: el redireccionamiento de entrada de audio está desactivado

   1: el redireccionamiento de entrada de audio está habilitado

Habilitar o deshabilitar la redirección de zona horaria para PCo IP | 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 PCo IP para deshabilitar esta función. Esta configuración se aplica al reiniciar el WorkSpace.

Para habilitar o deshabilitar la redirección de zona horaria para PCo IP | 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 *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 Habilite las conexiones SSH para su Linux WorkSpaces en Personal 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 listas de control de acceso a la red (ACLs) y 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 información sobre el uso de la biblioteca Extras, consulte la biblioteca Extras (Amazon Linux) en la Guía del EC2 usuario de Amazon 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 para WorkSpaces personal.

Utilice tarjetas inteligentes para la autenticación en Linux WorkSpaces

Los paquetes Linux WorkSpaces on DCV 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 en WorkSpaces Personal.

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

En el caso de DCV 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.

DCV 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 a la web 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 en modo WorkSpaces personal

Tu WorkSpaces paquete de Ubuntu incluye una suscripción a Ubuntu Pro de Canonical. 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:

- Administre su Ubuntu WorkSpaces
- Proporcione acceso a ellos a WorkSpaces los usuarios

Puede administrar Ubuntu WorkSpaces con una política de grupo utilizando 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 DCV en Ubuntu WorkSpaces

El comportamiento de DCV 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 de DCV para deshabilitar 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 son: *X*

   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 para Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de audio. Utilice el archivo de configuración de DCV para deshabilitar 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 son: *X*

   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 para Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de vídeo. Utilice el archivo de configuración de DCV para deshabilitar 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 son: *X*

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 para 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 están destinadas a 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 de DCV 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 *X* son:

habilitado: el redireccionamiento de zona horaria está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de zona horaria está deshabilitado

Habilite o deshabilite la redirección de impresoras para Ubuntu WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de impresoras. Utilice el archivo de configuración de DCV para deshabilitar 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 *X* son:

   habilitado: el redireccionamiento a la impresora está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento a la impresora está deshabilitado

Habilitación o deshabilitación de la sesión de desconexión en el bloqueo de pantalla para DCV

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 de DCV para habilitar 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 *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, tienes que 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 tu 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 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 PCo caso de IP WorkSpaces, las aplicaciones cliente de escritorio no admiten el uso de un servidor proxy ni el descifrado mediante TLS ni la inspección del tráfico del puerto 4172 en UDP (para el tráfico de escritorio). Necesitan una conexión directa a los puertos 4172.

En el caso de DCV 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.

DCV 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 a la web 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.

Administre su Rocky Linux WorkSpaces

Puede administrar Rocky Linux WorkSpaces con soluciones de configuración y administración, como Ansible.

> **Note**
>
> No puede eliminar, modificar ni ocultar ningún aviso de derechos de autor, marca comercial u otros avisos de propiedad o confidencialidad que estén contenidos en o sobre el software Rocky Linux.

Controle el comportamiento del DCV en Rocky Linux WorkSpaces

El comportamiento de DCV se controla mediante la configuración del archivo `wsp.conf`, que se encuentra en el directorio `/etc/wsp/`. Para implementar y hacer cumplir los cambios en la política, utilice una solución de administración de la configuración que sea compatible con Rocky Linux. 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 usted WorkSpace.

En las secciones siguientes, se describe cómo activar o desactivar determinadas funciones.

Habilite o deshabilite la redirección del portapapeles para Rocky Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección del portapapeles. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para activar o desactivar la redirección del portapapeles en Rocky 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 grupo `[policies]`.

   ```
   clipboard = X
   ```

   Donde los valores posibles son: *X*

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 para Rocky Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de audio. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para activar o desactivar la redirección de entrada de audio en Rocky 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 grupo `[policies]`.

   ```
   audio-in = X
   ```

   Donde los valores posibles son: *X*

   habilitado: el redireccionamiento de entrada de audio está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento de entrada de audio está desactivado

Habilite o deshabilite la redirección de entrada de vídeo para Rocky Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de vídeo. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para activar o desactivar la redirección de entrada de vídeo en Rocky 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 grupo `[policies]`.

```
video-in = X
```

Donde los valores posibles son: *X*

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 para Rocky 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 viajan mucho y quieren mantener su WorkSpaces zona horaria única para mantener la coherencia y mantener sus preferencias personales.

Utilice el archivo de configuración de DCV para configurar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de zona horaria en Rocky 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 grupo `[policies]`.

```
timezone-redirection = X
```

Donde los valores posibles *X* son:

habilitado: el redireccionamiento de zona horaria está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de zona horaria está deshabilitado

Habilite o deshabilite el redireccionamiento de impresoras para Rocky Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de impresoras. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para activar o desactivar la redirección de impresoras en Rocky 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 grupo `[policies]`.

```
remote-printing = X
```

Donde los valores posibles *X* son:

habilitado: el redireccionamiento a la impresora está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento a la impresora está deshabilitado

Habilitación o deshabilitación de la sesión de desconexión en el bloqueo de pantalla para DCV

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 de DCV para habilitar esta característica, si es necesario.

Para activar o desactivar la sesión de desconexión mediante el bloqueo de pantalla en Rocky 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 grupo `[policies]`.

   ```
   disconnect-on-lock = X
   ```

   Donde los valores posibles *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 Rocky Linux WorkSpaces

De forma predeterminada, solo los usuarios y cuentas asignados en el grupo de administradores de dominio pueden conectarse a Rocky Linux WorkSpaces mediante SSH. Para permitir que otros usuarios y cuentas se conecten a Rocky Linux WorkSpaces mediante SSH, le recomendamos que cree un grupo de administradores dedicado para sus administradores de Rocky Linux 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 Rocky Linux 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 Rocky Linux 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 tu Linux. WorkSpaces

Anule el shell predeterminado para Rocky Linux WorkSpaces

Para anular el shell predeterminado de Rocky 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 iniciar sesión para que el cambio surta efecto.

Administre su Red Hat Enterprise Linux WorkSpaces

Al igual que Windows y Amazon Linux WorkSpaces, Red Hat Enterprise Linux WorkSpaces está unido a un dominio, por lo que puede usar los usuarios y grupos de Active Directory para:

- Administre su Red Hat Enterprise Linux WorkSpaces
- Proporcione acceso a ellos a WorkSpaces los usuarios

Puede administrar Red Hat Enterprise Linux WorkSpaces con una política de grupo mediante ADsys. Consulte Red Hat Enterprise Linux Active Directory integration FAQ para obtener más información. También puede utilizar otras soluciones de configuración y administración, como Landscape y Ansible.

Controle el comportamiento del DCV en Red Hat Enterprise Linux WorkSpaces

El comportamiento de DCV 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 Red Hat Enterprise Linux. 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.

Habilite o deshabilite la redirección del portapapeles para Red Hat Enterprise Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección del portapapeles. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para activar o desactivar la redirección del portapapeles para Red Hat Enterprise 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 grupo `[policies]`.

   ```
   clipboard = X
   ```

   Donde los valores posibles son: *X*

   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

Habilite o deshabilite la redirección de entrada de audio para Red Hat Enterprise Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de audio. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de entrada de audio para Red Hat Enterprise 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 grupo `[policies]`.

   ```
   audio-in = X
   ```

   Donde los valores posibles para son: *X*

   habilitado: el redireccionamiento de entrada de audio está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento de entrada de audio está desactivado

Habilite o deshabilite la redirección de entrada de vídeo para Red Hat Enterprise Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de entrada de vídeo. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de entrada de vídeo para Red Hat Enterprise 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 grupo `[policies]`.

   ```
   video-in = X
   ```

Donde los valores posibles para son: *X*

habilitado: el redireccionamiento de entrada de vídeo está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de entrada de vídeo está desactivado

Habilite o deshabilite la redirección de zona horaria para Red Hat Enterprise 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 viajan mucho y quieren mantener su WorkSpaces zona horaria única para mantener la coherencia y mantener sus preferencias personales.

Utilice el archivo de configuración de DCV para configurar esta característica, si es necesario.

Para habilitar o deshabilitar la redirección de zonas horarias para Red Hat Enterprise 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 grupo `[policies]`.

```
timezone-redirection = X
```

Donde los valores posibles *X* son:

habilitado: el redireccionamiento de zona horaria está habilitado (de forma predeterminada)

deshabilitado: el redireccionamiento de zona horaria está deshabilitado

Habilite o deshabilite el redireccionamiento de impresoras para Red Hat Enterprise Linux WorkSpaces

De forma predeterminada, WorkSpaces admite la redirección de impresoras. Utilice el archivo de configuración de DCV para deshabilitar esta característica, si es necesario.

Para habilitar o deshabilitar el redireccionamiento de impresoras para Red Hat Enterprise 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 grupo `[policies]`.

   ```
   remote-printing = X
   ```

   Donde los valores posibles *X* son:

   habilitado: el redireccionamiento a la impresora está habilitado (de forma predeterminada)

   deshabilitado: el redireccionamiento a la impresora está deshabilitado

Habilitación o deshabilitación de la sesión de desconexión en el bloqueo de pantalla para DCV

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 de DCV para habilitar esta característica, si es necesario.

Para activar o desactivar la sesión de desconexión mediante el bloqueo de pantalla para Red Hat Enterprise 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 grupo `[policies]`.

   ```
   disconnect-on-lock = X
   ```

   Donde los valores posibles *X* son:

   habilitado: la desconexión al bloquear la pantalla está activada

   deshabilitado: la desconexión al bloquear la pantalla está desactivada (de forma predeterminada)

Otorgue acceso SSH a los administradores de Red Hat Enterprise Linux WorkSpaces

De forma predeterminada, solo los usuarios y las cuentas asignados en el grupo de administradores de dominio pueden conectarse a Red Hat Enterprise Linux WorkSpaces mediante SSH. Para permitir que otros usuarios y cuentas se conecten a Red Hat Enterprise Linux WorkSpaces mediante SSH, le recomendamos que cree un grupo de administradores dedicado para sus administradores de Red Hat Enterprise Linux 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 Red Hat Enterprise Linux, no WorkSpaces necesita 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 conectarse mediante SSH, debe añadir su clave pública SSH a `$HOME/.ssh/authorized_keys` su Red Hat Enterprise Linux WorkSpace o editarla `/etc/ssh/sshd_config` para configurarla. PasswordAuthentication `yes` Para obtener más información sobre cómo habilitar las conexiones SSH, consulte Habilitar las conexiones SSH para Linux. WorkSpaces

Anule el shell predeterminado para Red Hat Enterprise Linux WorkSpaces

Para anular el shell predeterminado de Red Hat Enterprise 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**
>
> Después de realizar este cambio, debe reiniciar WorkSpace o cerrar la sesión WorkSpace (no solo desconectarse) y, a continuación, volver a iniciar sesión para que el cambio surta efecto.

Optimice WorkSpaces para la comunicación en tiempo real en WorkSpaces Personal

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, que 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 mensajería sin conexión. audio/video La mayoría de estas funciones están disponibles sin problemas WorkSpaces como funciones 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 la optimización de 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

- ¿Qué modo de optimización RTC utilizar?
- Guía de optimización de RTC

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 DCV. 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		

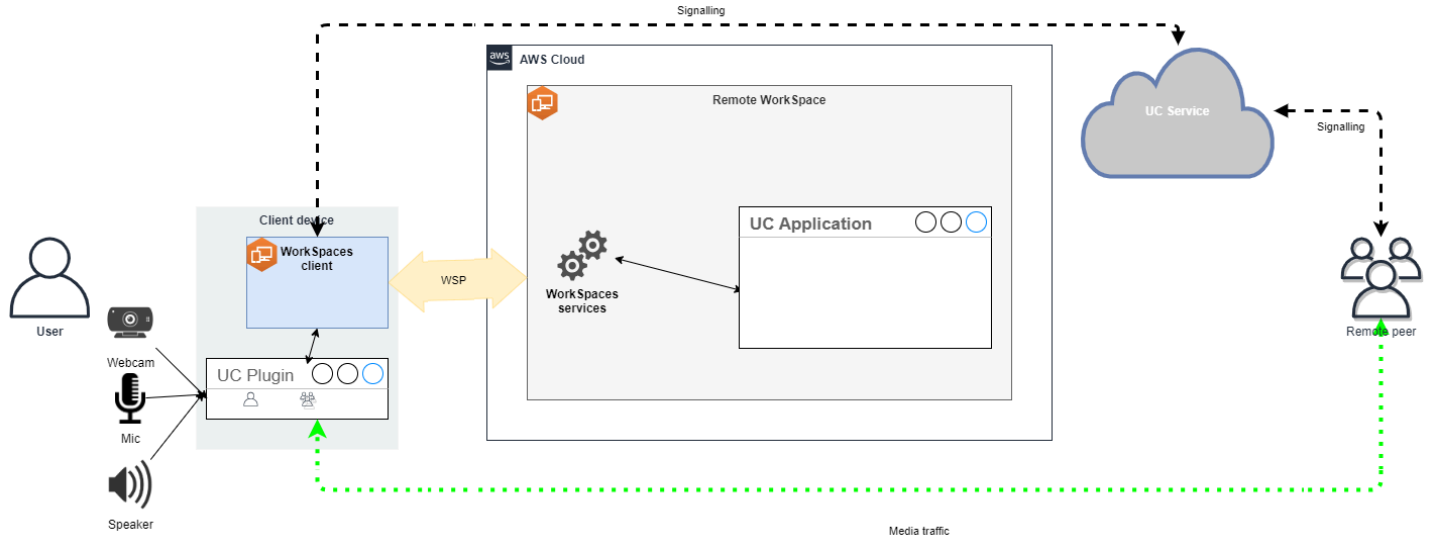
Característica	RTC directo	RTC multimedia optimizado	RTC optimizado durante la sesión
Salas de chat grupales	No requiere configuración RTC		
Audioconferencias grupales	Óptima	Óptima	Buena
Videoconferencias grupales	Buena	Óptima	Buena
Llamadas de audio individuales	Óptima	Óptima	Buena
Videollamadas individuales	Buena	Óptima	Buena
Pizarra	No requiere configuración RTC		
Audio/video clips/messaging	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 que el proveedor de aplicaciones de UC SDKs proporciona Amazon. 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 UC que funciona desde dentro WorkSpace 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 PCo IP y DCV WorkSpaces)
- Reuniones de Cisco Webex (solo para DCV 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:

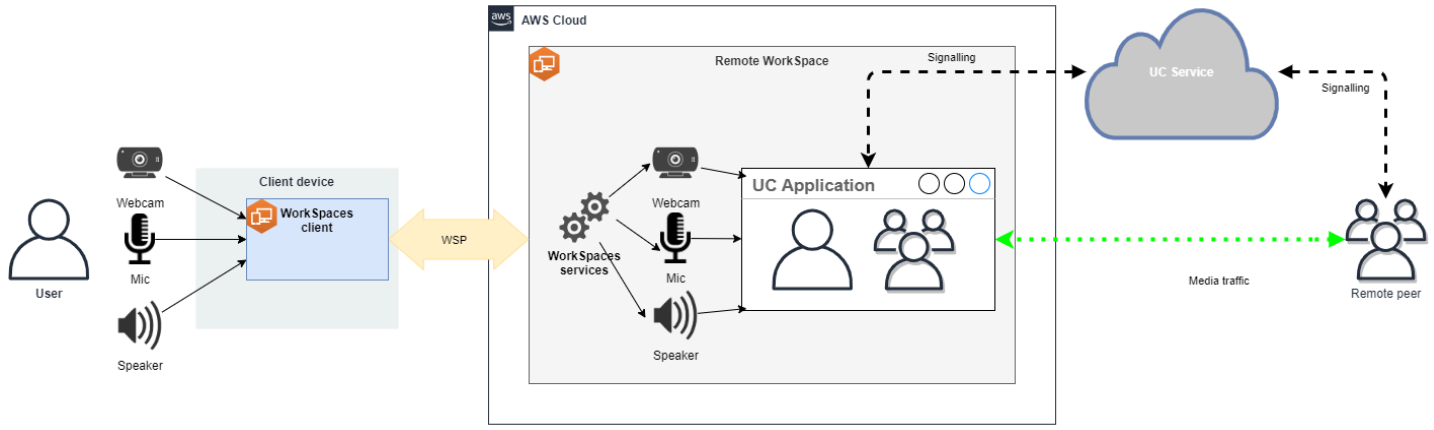
- La extensión de cliente UC debe estar instalada en el dispositivo cliente.
- La extensión de cliente UC requiere una administración y actualizaciones independientes.
- Es posible que las extensiones de cliente UC no estén disponibles en determinadas plataformas de cliente, como las plataformas móviles 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 de una persona local. Los flujos de audio y vídeo generados por la aplicación se capturan mediante DCV y se transmiten al cliente. En el cliente, las señales del micrófono (tanto en DCV como PCo IP WorkSpaces) y de la cámara web (solo en DCV 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.



El protocolo DCV 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 recomiendan 4 núcleos	4.0 GB DE RAM	Power (4 vCPU, 16 GB de memoria)	• PowerPro (8 vCPU, 32 GB de memoria) • GeneralPurpose4x grande (16 vCPU, 64 GB de memoria) • GeneralPurpose.8x grande (32 vCPU, 128 GB de memoria)	Performance (2 vCPU, 8 GB de memoria)	• PowerPro (8 vCPU, 32 GB de memoria) • GeneralPurpose4x grande (16 vCPU, 64 GB de memoria) • GeneralPurpose.8x grande (32 vCPU, 128 GB de memoria)	Requisitos de hardware para Microsoft Teams
Zoom	Se requieren 2 núcleos,	4.0 GB DE RAM	Power (4 vCPU,	• PowerPro (8 vCPU,	Performance (2 vCPU,	• PowerPro (8 vCPU,	Requisitos del sistema

			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
	se recomiendan 4 núcleos		16 GB de memoria)	32 GB de memoria) • GeneralPurpose4x grande (16 vCPU, 64 GB de memoria) • GeneralPurpose.8x grande (32 vCPU, 128 GB de memoria)	8 GB de memoria)	32 GB de memoria) • GeneralPurpose4x grande (16 vCPU, 64 GB de memoria) • GeneralPurpose.8x grande (32 vCPU, 128 GB de memoria)	Zoom: Windows, macOS, Linux

			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
Webex	Se requieren 2 núcleos	4.0 GB DE RAM	Power (4 vCPU, 16 GB de memoria)	• PowerPro (8 vCPU, 32 GB de memoria) • GeneralPurpose4x grande (16 vCPU, 64 GB de memoria) • GeneralPurpose.8x grande (32 vCPU, 128 GB de memoria)	Performance (2 vCPU, 8 GB de memoria)	• PowerPro (8 vCPU, 32 GB de memoria) • GeneralPurpose4x grande (16 vCPU, 64 GB de memoria) • GeneralPurpose.8x grande (32 vCPU, 128 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, para los usuarios que realizan videollamadas o retransmisiones de vídeo de forma habitual, se recomienda encarecidamente optar por la configuración PowerPro o por una superior.

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.

Cómo sacar partido del transporte QUIC basado en UDP con DCV

El transporte UDP es especialmente adecuado para transmitir aplicaciones RTC. Para aumentar al máximo la eficiencia, asegúrese de que la red esté configurada para utilizar el transporte QUIC para DCV. 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 el redireccionamiento de entrada de vídeo para DCV 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

Se recomienda encarecidamente a los usuarios que utilicen Power PowerPro, GeneralPurpose .4xlarge o GeneralPurpose .8xlarge WorkSpaces para realizar videoconferencias que restrinjan la resolución máxima de las cámaras web redirigidas. En el caso de PowerPro GeneralPurpose .4xlarge o GeneralPurpose .8xlarge, 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 al cliente, lo WorkSpaces 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
```

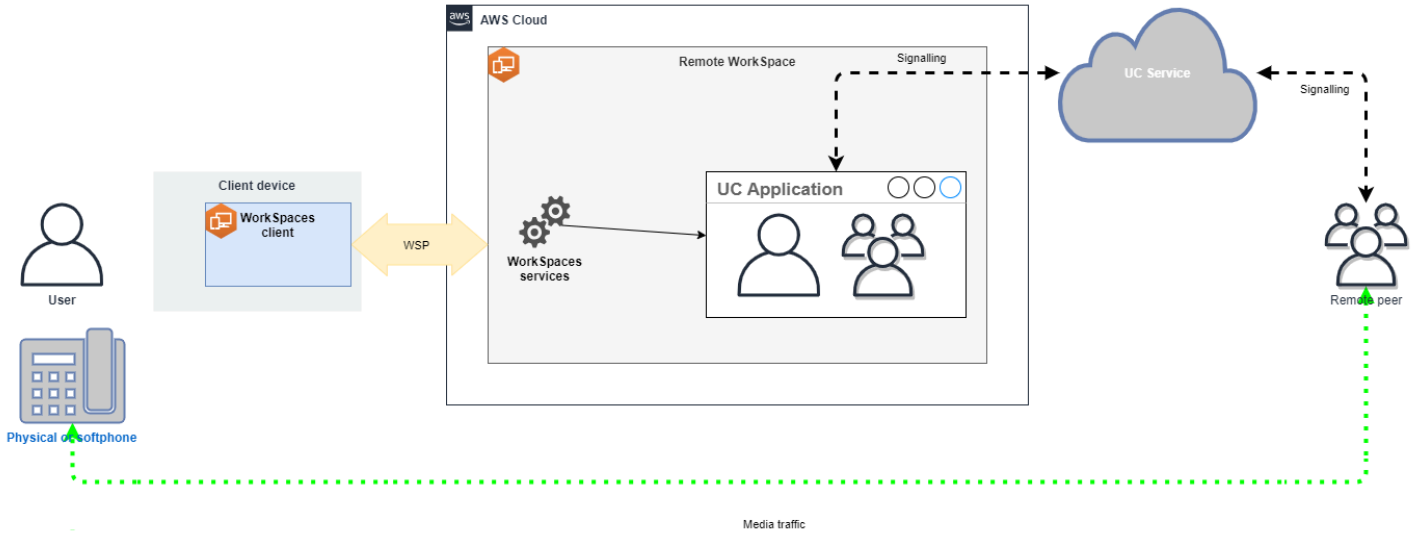
3. Cree un nombre de valor de cadena `default-profile` y configúrelo en `voice`.

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

Administra el modo de ejecución en WorkSpaces Personal

El modo de funcionamiento de a WorkSpace determina su disponibilidad inmediata y la forma de pagarla (mensual o por hora). Puede elegir entre los siguientes modos de ejecución al crear el WorkSpace:

- AlwaysOn— Úselo cuando pague una tarifa mensual fija para un uso ilimitado de su WorkSpaces. Este modo es el mejor para los usuarios que utilizan su escritorio principal a tiempo WorkSpace completo.
- AutoStop— Úsalo cuando pagues WorkSpaces por horas. Con este modo, te WorkSpaces detienes después de un período específico de desconexión y se guarda el estado de las aplicaciones y los datos.

Para más información, consulte Precios de WorkSpaces.

AutoStop WorkSpaces

Para configurar la hora de parada automática, selecciónela WorkSpace en la WorkSpaces consola de Amazon, elija Acciones, Modifique las propiedades del modo de ejecución y, a continuación, configure la AutoStop hora (horas). De forma predeterminada, la AutoStop hora (horas) está configurada en 1 hora, lo que significa que WorkSpace se detiene automáticamente una hora después de la WorkSpace desconexión.

Cuando a WorkSpace se desconecte y el período de AutoStop tiempo haya expirado, es posible que pasen varios minutos adicionales WorkSpace hasta que se detenga automáticamente. Sin embargo, la facturación se detiene tan pronto como vence el período de AutoStop tiempo y no se le cobrará por ese tiempo adicional.

Cuando se WorkSpaces admite la hibernación, el estado del escritorio se guarda en el volumen raíz del WorkSpace. Se WorkSpace reanuda cuando un usuario inicia sesión. Todos los documentos abiertos y los programas en ejecución vuelven a su estado guardado y todos los sistemas WorkSpaces operativos admiten la hibernación.

AutoStop Gráficos. G4dn, .g4dn, Graphics y GraphicsPro GeneralPurpose .4xlarge o GeneralPurpose .8xlarge no admiten la GraphicsPro hibernación, por lo que no pueden conservar el estado de los datos y los programas cuando se detienen. En el caso de estos sistemas de parada automática WorkSpaces, te recomendamos guardar el trabajo cada vez que termines de usarlos.

En el caso de la licencia Bring Your Own License (BYOL) AutoStop WorkSpaces, un gran número de inicios de sesión simultáneos podría aumentar considerablemente el tiempo de WorkSpaces disponibilidad. Si espera que varios usuarios inicien sesión en su BYOL AutoStop WorkSpaces al mismo tiempo, consulte a su administrador de cuentas para que le asesore.

> **Important**
>
> AutoStop WorkSpaces se detienen automáticamente solo si WorkSpaces están desconectados.

A WorkSpace se desconecta únicamente en las siguientes circunstancias:

- Si el usuario se desconecta manualmente de la aplicación WorkSpaces cliente de Amazon WorkSpace o la cierra.
- 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, AutoStop WorkSpace los usuarios deberían desconectarse manualmente de sus WorkSpaces dispositivos cada día cuando terminen de usarlos. Para desconectarse manualmente, selecciona Desconectar WorkSpace o salir WorkSpaces de Amazon en el WorkSpaces menú Amazon de las aplicaciones WorkSpaces cliente para Linux, macOS o Windows. Para Android o iPad, seleccione Desconectar en el menú de la barra lateral.

AutoStop WorkSpaces es posible que no se detenga automáticamente en las siguientes situaciones:

- Si el dispositivo cliente solo está bloqueado, en modo inactivo o inactivo (por ejemplo, la tapa del portátil está cerrada) en lugar de apagarse, es posible que la WorkSpaces aplicación siga ejecutándose en segundo plano. Mientras la WorkSpaces aplicación siga ejecutándose, es WorkSpace posible que no se desconecte y, por lo tanto, no se detenga automáticamente. WorkSpace
- WorkSpaces solo puede detectar la desconexión cuando los usuarios utilizan WorkSpaces clientes. Si los usuarios utilizan clientes de terceros, es WorkSpaces posible que no puedan detectar la desconexión y, por lo tanto, es WorkSpaces posible que no se detenga automáticamente y que la facturación no se suspenda.

Modificar el modo de ejecución

Puede cambiar el modo de ejecución en cualquier momento.

Para modificar el modo de ejecución de un WorkSpace

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione el modo WorkSpace de ejecución que desee modificar y elija Acciones, Modificar.
4. Seleccione el nuevo modo de ejecución AlwaysOno y AutoStop, a continuación, elija Guardar.

Para modificar el modo de ejecución de un WorkSpace mediante el AWS CLI

Utilice el comando modify-workspace-properties.

Detenga e inicie un AutoStop WorkSpace

Cuando AutoStop WorkSpaces se desconecta, se detienen automáticamente después de un período de desconexión específico y se suspende la facturación por hora. Para optimizar aún más los costes, puedes suspender manualmente los cargos por hora asociados AutoStop WorkSpaces a ellos. Las WorkSpace paradas y todas las aplicaciones y datos se guardan para la próxima vez que un usuario inicie sesión en WorkSpace.

Cuando un usuario vuelve a conectarse a una parada WorkSpace, se reanuda desde donde la dejó, normalmente en menos de 90 segundos.

Puede reiniciar (reiniciar) las AutoStop WorkSpaces que estén disponibles o se encuentren en estado de error.

Para detener un AutoStop WorkSpace

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Selecciona lo que WorkSpace quieres detener y elige Acciones, Detener. WorkSpaces
4. Cuando se le pida que confirme, seleccione Detener WorkSpace.

Para iniciar una AutoStop WorkSpace

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione el WorkSpaces para empezar y elija Acciones, Iniciar. WorkSpaces
4. Cuando se le pida que confirme, elija Start WorkSpace.

Para eliminar los costos fijos de infraestructura asociados AutoStop WorkSpaces, elimínelos WorkSpace de su cuenta. Para obtener más información, consulte Eliminar un archivo WorkSpace en WorkSpaces Personal.

Para detener e iniciar un AutoStop WorkSpace uso del AWS CLI

Utilice los WorkSpacescomandos stop WorkSpaces y start.

Administrar aplicaciones en WorkSpaces Personal

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 la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. En el panel de navegación izquierdo, selecciona. 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 sus WorkSpace paquetes de aplicaciones de 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
- Microsoft Visual Studio Professional 2022
- Microsoft Visual Studio Enterprise 2022

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)	Microsoft Visual Studio Professional/Enterprise 2022
Windows Server 2016	Desinstalar	No admitido	No admitido	No admitido	No admitido	No admitido
Windows Server 2019	No compatible	Desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar	No compatible
Windows Server 202	No compatible	Desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar
Windows 10	Desinstalar	Desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar
Windows 11	Desinstalar	Desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar	Instalar/desinstalar

Important

- Microsoft Office/Visio/Project debe seguir las mismas ediciones. Por ejemplo, no se pueden mezclar aplicaciones de las versiones Standard con aplicaciones de las versiones Professional.
- Microsoft Office/Visio/Project debe seguir las mismas versiones. Por ejemplo, no se pueden mezclar aplicaciones de 2019 con aplicaciones de 2021.

- Microsoft Office/Visio/Project 2021 Standard/Professional no es compatible con Value, Graphics ni GraphicsPro WorkSpaces paquetes.
- Microsoft Visual Studio 2022 Enterprise/Professional no admite Value, Standard, Graphics ni GraphicsPro WorkSpaces paquetes. Los paquetes de rendimiento se pueden usar para cargas de trabajo de Visual Studio que requieren menos recursos. Sin embargo, para obtener los mejores resultados, se recomienda usar Visual Studio con tipos de paquetes de cuatro núcleos o posteriores. Los tipos de paquetes Power, General Purpose.4XLarge PowerPro, General Purpose.8XLarge, Graphics.G4DN y .g4dn cumplen este requisito. GraphicsPro Para obtener más información, consulte Visual Studio 2022 Product Family System Requirements.
- 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 las aplicaciones de install/uninstall Microsoft 365, debe traer sus propias herramientas e instaladores, Administrar el flujo de trabajo de las aplicaciones no puede las aplicaciones de install/uninstall Microsoft 365.
- Puedes crear una imagen personalizada de las aplicaciones WorkSpaces installed/uninstalled a través de Administrar aplicaciones.
- En el caso de las regiones que permiten la suscripción, como África (Ciudad del Cabo), la conexión a WorkSpaces Internet debe estar habilitada a nivel de directorio.

Actualice los paquetes de aplicaciones en un WorkSpace

1. Abra la WorkSpaces consola en la versión 2/homehttps://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 la versión 2/homehttps://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.

Actualice las cargas de trabajo de Microsoft Visual Studio 2022 en un WorkSpace

De forma predeterminada, Microsoft Visual Studio 2022 se instala con las siguientes cargas de trabajo y requiere 18 GB de espacio en el disco duro:

- Editor principal de Visual Studio
- Desarrollo de Azure
- Procesamiento y almacenamiento de datos
- Desarrollo de escritorio .NET
- Desarrollo de interfaz de usuario de aplicaciones multiplataforma NET
- Desarrollo de ASP.NET y web
- Desarrollo de Node.js

Los usuarios tienen la flexibilidad de añadir o eliminar cargas de trabajo y componentes individuales, lo que les permite adaptar la aplicación a sus requisitos específicos. Es importante tener en cuenta que la instalación de cargas de trabajo adicionales requiere más espacio en el disco. Para obtener más información sobre las configuraciones de las cargas de trabajo, consulte Modify Visual Studio workloads, components, and language packs.

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 administración 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 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 crea WorkSpace uno nuevo con un WorkSpace ID nuevo.

Para obtener más información, consulte Cómo WorkSpace migrar WorkSpaces una aplicación modificada mediante Administrar aplicaciones 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 en WorkSpaces personal

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 PCo IP.

Para ver el estado de modificación actual de un WorkSpace, selecciona 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 WorkSpaces administración de autoservicio para sus usuarios en Personal WorkSpaces .

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 en grupos establecidos 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 GeneralPurpose .4xlarge o GeneralPurpose .8xlarge WorkSpace con un mínimo de 175 GB para el volumen raíz y 100 GB para el volumen de usuario.
- Puedes lanzar 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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. Seleccione Save changes (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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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. Seleccione Save changes (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 de procesamiento Standard, Power, Performance, PowerPro GeneralPurpose .4xlarge y GeneralPurpose .8xlarge. Para obtener más información sobre estos tipos de procesamiento, consulte Amazon WorkSpaces Bundles.

Note

- Si el sistema operativo de origen no es Windows Server 2022 o Windows 11, no puede cambiar el tipo de cómputo de PowerPro a GeneralPurpose.
- Si va a modificar el tipo de procesamiento de un non-GPU-enabled paquete a GeneralPurpose .xlarge o GeneralPurpose .8xlarge, WorkSpaces debe cumplir con un tamaño mínimo de volumen raíz de 175 GB y un tamaño de volumen de usuario de 100 GB. Para aumentar el tamaño de su volumen, consulte. WorkSpaces Modificar los tamaños de los volúmenes
- Puede cambiar el tipo de procesamiento 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 archivo en WorkSpaces Personal.
- GraphicsPro El paquete estará disponible el 31 de octubre de 2025 end-of-life. Te recomendamos migrar tus paquetes GraphicsPro WorkSpaces a los compatibles antes del 31 de octubre de 2025. Para obtener más información, consulte Migrar un WorkSpace archivo en WorkSpaces Personal.
- No puede cambiar el tipo de procesamiento de los gráficos ni GraphicsPro a ningún otro valor.

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. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione WorkSpace y elija Acciones, Modificar el tipo de procesamiento.
4. En Tipo de computación, elija un tipo de computación.
5. Seleccione Save changes (Guardar cambios).

Para cambiar el tipo de procesamiento de un WorkSpace

Utilice el modify-workspace-propertiescomando con la `ComputeTypeName` propiedad.

Modificar protocolos

Si WorkSpace se ha creado con paquetes de PCo IP, puede modificar su protocolo de streaming mediante la AWS CLI o la WorkSpaces API de Amazon. Esto le permite migrar el protocolo utilizando el existente WorkSpace sin utilizar la función de WorkSpace migración. Esto también le permite usar DCV y mantener su volumen raíz sin volver a crear la PCo IP existente WorkSpaces durante el proceso de migración.

- Solo puede modificar su protocolo si WorkSpace se creó con paquetes de PCo IP y no está habilitado para la GPU. WorkSpace
- Antes de modificar el protocolo a DCV, asegúrese de que WorkSpace cumple los siguientes requisitos para un DCV. WorkSpace
  - Su WorkSpaces cliente admite el DCV
  - La región en la que WorkSpace está desplegado es compatible con DCV
  - Los requisitos de dirección IP y puerto para DCV están abiertos. Para obtener más información, consulte los requisitos de dirección IP y puerto para WorkSpaces.

- Asegúrese de que el paquete actual esté disponible con DCV.
- Para disfrutar de la mejor experiencia con las videoconferencias, recomendamos utilizar únicamente Power PowerPro, GeneralPurpose .4xlarge o GeneralPurpose .8xlarge.

> **Note**
>
> - Recomendamos encarecidamente realizar pruebas con un dispositivo que no sea de producción WorkSpaces antes de empezar a cambiar el protocolo.
> - Si modifica el protocolo de PCo IP a DCV y, a continuación, lo modifica de nuevo a PCo IP, no podrá conectarse a WorkSpaces través del acceso web.

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 `DCV`, 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. `DCV`

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 marca en WorkSpaces Personal

Amazon te WorkSpaces permite crear una WorkSpaces experiencia familiar para tus usuarios APIs al personalizar la apariencia de tu página de inicio de sesión con el logotipo WorkSpace 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 en lugar de mostrarse en la WorkSpaces marca predeterminada.

Se admiten los siguientes caracteres:

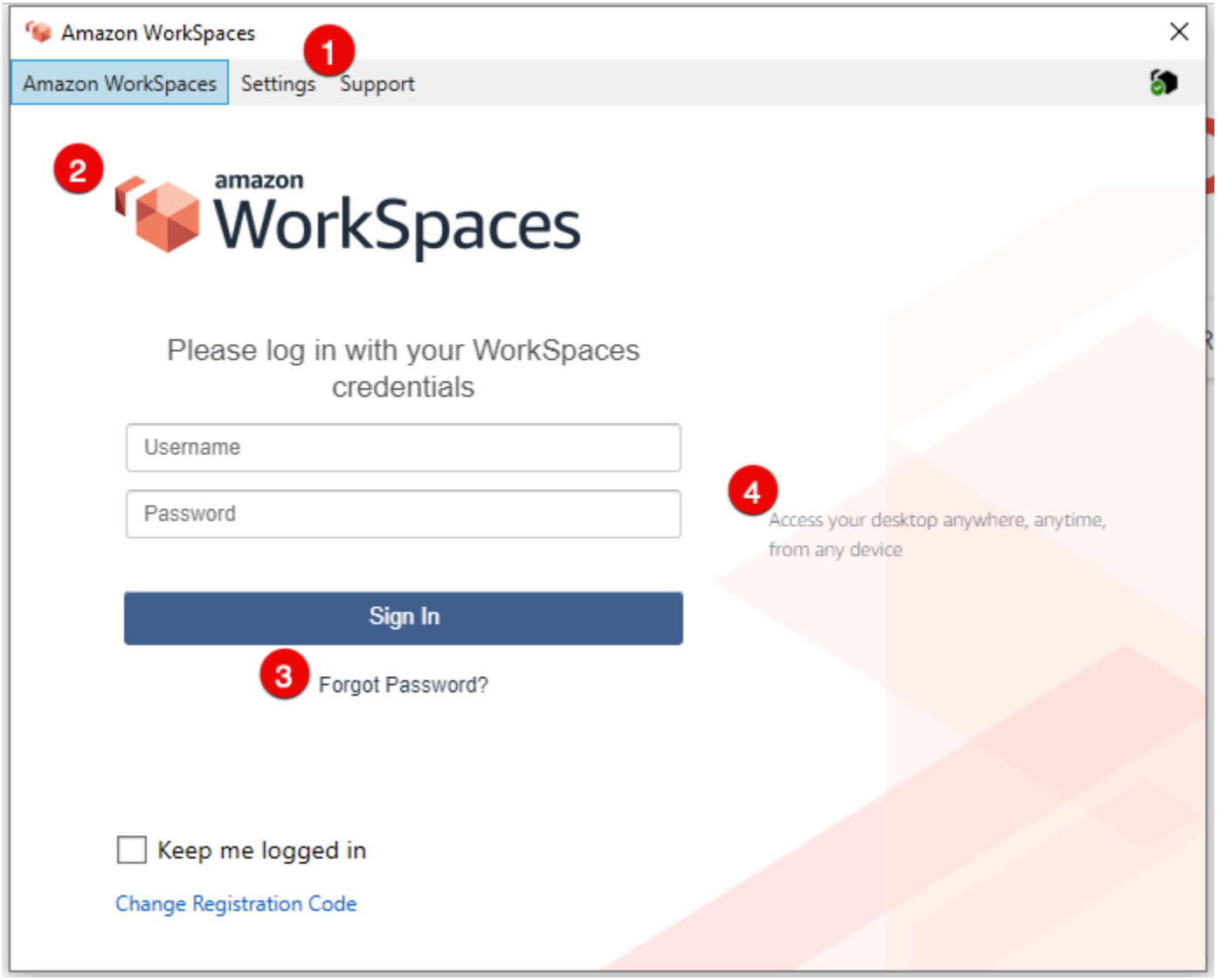
- Windows
- Linux
- Android
- MacOS
- iOS
- Acceso web

> **Note**
>
> Para modificar los elementos de marca mediante la AWS GovCloud (US) Region versión de WorkSpaces cliente incluida ClientBranding APIs en la versión 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 la contraseña de su cuenta 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 integraci ón 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 caractere s. • Etiquetas HTML compatibl es: `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`

A continuación, se muestran ejemplos de fragmentos de código para su uso. ImportClientBranding

AWS CLI 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 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.

Etiquete los recursos en WorkSpaces Personal

Puede organizar y administrar sus propios recursos 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 etiquetas es una forma sencilla pero eficaz de gestionar AWS los recursos 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 agregas etiquetas a una existente WorkSpace el 15 de julio, las etiquetas no aparecerán en tu informe de asignación de costes 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 WorkSpaces recursos en el Cost Explorer, debe activar las etiquetas que ha aplicado a WorkSpaces los recursos siguiendo las instrucciones de Activación de etiquetas de asignación de costes definidas por el usuario en la Guía del AWS Billing usuario.
> 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 Cost Explorer, WorkSpaces los recursos 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

- Al crearlos, puede añadir etiquetas a los siguientes recursos: imágenes WorkSpaces importadas y grupos de control de acceso IP.
- Puede añadir etiquetas a los recursos existentes de los siguientes tipos: directorios registradosWorkSpaces, paquetes personalizados, imágenes y grupos de control de acceso 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 `aws:workspaces:` prefijos `aws:` o en los nombres o valores de las etiquetas porque están reservados para AWS su uso. Los nombres y valores de etiquetas que tienen estos prefijos no se pueden editar.

Para actualizar las etiquetas de un recurso existente mediante la consola (directorios o grupos de control de acceso IP) WorkSpaces

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija uno de los siguientes tipos de recursos: directorios o WorkSpacescontroles de acceso 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 WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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 Etiquetas, elija 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 mediante el AWS CLI

Utilice los comandos create-tags y delete-tags.

Mantenimiento WorkSpaces personal

Le recomendamos que realice WorkSpaces el mantenimiento de forma regular. WorkSpaces programa los períodos de mantenimiento predeterminados para su WorkSpaces. Durante el período de mantenimiento, 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 actualizaciones del sistema operativo que WorkSpace está configurado para usar. Durante el mantenimiento, WorkSpaces es posible que no esté disponible.

De forma predeterminada, Windows WorkSpaces está configurado 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

WorkSpaces Debe tener acceso a Internet para poder instalar actualizaciones del sistema operativo e implementar aplicaciones. Para obtener más información, consulte the section called “Acceso a Internet”.

Periodos de mantenimiento para AlwaysOn WorkSpaces

AlwaysOn WorkSpacesEn efecto, el período de mantenimiento viene determinado por la configuración del sistema operativo. El valor predeterminado es un período de cuatro horas comprendido entre las 00h00 y las 04h00, en la zona horaria del, todos los domingos por la WorkSpace mañana. De forma predeterminada, la zona horaria de an AlwaysOn WorkSpace es la zona horaria de la región para. AWS WorkSpace Sin embargo, si se conecta desde otra región y la redirección de zona horaria está habilitada y, a continuación, WorkSpace se desconecta, la zona horaria de la región desde la que se conectó.

Puede deshabilitar la redirección de zona horaria para Windows WorkSpaces mediante la política de grupo. Puede deshabilitar la redirección de zonas horarias para Linux WorkSpaces mediante la configuración del agente PCo IP.

Para Windows WorkSpaces, puede configurar el período de mantenimiento mediante la política de grupo; consulte Configurar los ajustes de la política de grupo para las actualizaciones automáticas. No puede configurar el período de mantenimiento para Linux WorkSpaces.

Ventanas de mantenimiento para AutoStop WorkSpaces

AutoStop WorkSpaces se inician automáticamente una vez al mes para instalar actualizaciones importantes. 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 00:00 y las 05:00 horas, en la zona horaria de la región correspondiente al AWS . WorkSpace Se WorkSpace puede mantener cualquier día del período de mantenimiento. Durante este período, solo se WorkSpaces mantienen los productos de más de 7 días.

Durante el período de mantenimiento, el estado de WorkSpace se establece en`MAINTENANCE`. WorkSpace

Aunque no puede modificar la zona horaria que se utiliza para el mantenimiento AutoStop WorkSpaces, puede desactivar el período de mantenimiento de la AutoStop WorkSpaces siguiente manera. Si desactiva el modo de mantenimiento, no WorkSpaces se reiniciará ni entrará en ese estado. `MAINTENANCE`

Para deshabilitar el modo de mantenimiento

1. Abra la WorkSpaces consola en la versión 2/home. 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 prefieres, puedes mantener tu WorkSpaces propio horario. Cuando realice tareas de mantenimiento, le recomendamos que cambie el estado WorkSpace a Mantenimiento. Cuando haya terminado, cambie el estado del WorkSpace a Disponible.

Cuando a WorkSpace está en estado de mantenimiento, se producen los siguientes comportamientos:

- No WorkSpace responde a las solicitudes de reinicio, detención, inicio o reconstrucción.
- Los usuarios no pueden iniciar sesión en WorkSpace.
- An no AutoStop WorkSpace está hibernado.

Para cambiar el estado del WorkSpace uso de la consola

> **Note**
>
> Para cambiar el estado de a WorkSpace, WorkSpace debe estar en el estado Disponible. La configuración Modificar estado no está disponible cuando a no WorkSpace está en el estado Disponible.

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.

3. Seleccione su estado WorkSpace y elija Acciones, Modificar estado.
4. En Modificar estado, elija Disponible o Mantenimiento.
5. Seleccione Save.

Para cambiar el estado del WorkSpace uso del AWS CLI

Utilice el comando modify-workspace-state.

WorkSpaces Cifrado en WorkSpaces modo personal

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 asegura de que todos los datos almacenados en reposo, del disco I/O al volumen y de las instantáneas creadas a partir de los volúmenes estén cifrados.

> **Note**
>
> - Además de cifrar los suyos WorkSpaces, también puede utilizar el cifrado FIPS para terminales en determinadas AWS regiones de EE. UU. Para obtener más información, consulte Configure la autorización de FedRAMP o el cumplimiento de las normas SRG del DoD para personal WorkSpaces .
> - BitLocker Amazon no admite el cifrado WorkSpaces.

Contenido

- Requisitos previos
- Límites
- Descripción general del WorkSpaces cifrado mediante AWS KMS
- WorkSpaces contexto de cifrado
- Conceda WorkSpaces permiso para usar una clave KMS en su nombre
- Cifra un WorkSpace
- Ver cifradas 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 los volúmenes de usuario y raíz de su. WorkSpace Para obtener más información, 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 de KMS gestionadas, incluida la que WorkSpaces admite Amazon, se rotan todos los 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 EC2 del usuario de Amazon.

Cuando se inicia 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 a 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 Administración de identidad y acceso 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 GetKeyPolicyoperación para obtener la política de claves 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 PutKeyPolicyoperación 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 Administración de identidad y acceso 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.

JSON

```
{
  "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:ReEncryptFrom",
        "kms:ReEncryptTo",
        "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 gestionada 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.

JSON

```
{
    "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.

JSON

```
{
    "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.

JSON

```
{
  "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 la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. Selecciona Iniciar WorkSpaces y completa 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. Elija Iniciar WorkSpaces.

Ver cifradas 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 en WorkSpaces Personal

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 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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 el AWS CLI

Utilice el comando reboot-workspaces.

Para reiniciar de forma masiva WorkSpaces

Utilice la amazon-workspaces-admin-module.

Reconstruir un WorkSpace in WorkSpaces Personal

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 archivo WorkSpace en WorkSpaces Personal.

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 archivo en WorkSpaces Personal.

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. Abre la WorkSpaces consola en la versión 2/homehttps://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.

Solución de problemas

Si regenera un WorkSpace después de cambiar el atributo de AMAccountnombre de usuario 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.

Reconstruir Microsoft Entra ID unido WorkSpaces

Cuando un usuario inicia sesión en su cuenta WorkSpace por primera vez después de la reconstrucción, tiene que volver a pasar por la out-of-box experiencia (OOBE), de forma similar a cuando se le asignó una nueva. WorkSpace Como resultado, se crea una nueva carpeta de perfiles de usuario en la que se WorkSpace reemplaza la carpeta de perfiles de usuario original. Por lo tanto, durante la reconstrucción de una entrada a la que se ha unido WorkSpace, el contenido de la carpeta de perfil de usuario original se guarda `D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated>` en la carpeta reconstruida WorkSpace. El usuario debe copiar el contenido del perfil original de la carpeta de `D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated>` al perfil del usuario en D:\Users\<USERNAME> para restaurar todos los datos del perfil de usuario, incluidos los iconos del escritorio, los atajos y los archivos de datos.

> **Note**
>
> Para Microsoft Entra ID WorkSpaces, recomendamos utilizar siempre Restore, siempre que sea posible WorkSpaces, en lugar de Rebuild WorkSpaces.

Restaurar un archivo WorkSpace en WorkSpaces Personal

Al restaurar a, WorkSpace se recrean tanto el volumen raíz como el volumen de usuario mediante una instantánea de cada volumen que se tomó cuando estaba en buen WorkSpace estado. Al restaurar WorkSpace , se revierten los datos de los volúmenes raíz y de usuario hasta el momento en que se crearon las instantáneas. La reconstrucción de a WorkSpace solo revierte los datos del volumen de usuarios. Esto significa que la restauración requiere disponer de instantáneas tanto del volumen raíz como del volumen de usuario, mientras que la reconstrucción de un WorkSpace solo requiere una instantánea del volumen de usuario. Para reconstruir un WorkSpace, consulteReconstruir un WorkSpace in WorkSpaces Personal.

Al restaurar un, se WorkSpace produce lo siguiente:

- El volumen raíz (para Microsoft Windows, unidad C; para Linux, /) se restaura a la fecha y hora especificadas mediante una instantánea. Se perderán todas las aplicaciones que se han instalado o la configuración del sistema que se ha modificado después de crear la instantánea.
- El volumen de usuario (para Microsoft Windows, la unidad D; para Linux, /home) se vuelve a crear a la fecha y hora especificadas mediante una instantánea. El contenido actual del volumen de usuario se sobrescribe.

El punto de restauración

Al seleccionar Acciones y Reconstruir o Restaurar WorkSpace, se muestran la fecha y la hora de las instantáneas utilizadas para la operación. Para comprobar la fecha y la hora de las instantáneas utilizadas para la operación mediante el AWS CLI, utilice el describe-workspace-snapshotscomando.

Cuando hay que hacer instantáneas

Las instantáneas del volumen raíz y de usuario se toman de la siguiente manera.

- Después de crear a WorkSpace por primera vez: normalmente, las instantáneas iniciales de los volúmenes raíz y de usuario se toman poco después de crear a (normalmente, en 30 minutos). WorkSpace En algunas AWS regiones, es posible que se tarden varias horas en tomar las instantáneas iniciales después de crear WorkSpace un.

  Si a WorkSpace deja de estar en buen estado antes de que se tomen las instantáneas iniciales, no se WorkSpace podrá restaurar. En ese caso, puede intentar reconstruirlo WorkSpace o ponerse en contacto con AWS Support para obtener ayuda.

- Durante el uso normal: las instantáneas automáticas para su uso al restaurar un WorkSpace están programadas cada 12 horas. Si WorkSpace está en buen estado, las instantáneas del volumen raíz y del volumen de usuarios se crean aproximadamente al mismo tiempo. Si no WorkSpace está en buen estado, las instantáneas se crean solo para el volumen de usuarios.
- Tras la restauración de un: cuando WorkSpace se restaura un WorkSpace, se toman nuevas instantáneas poco después de que finalice la restauración (normalmente en un plazo de 30 minutos). En algunas AWS regiones, es posible que se tarden varias horas en tomar estas instantáneas tras la restauración de WorkSpace una.

  Una WorkSpace vez restaurada una, si WorkSpace pierde su estado antes de poder tomar nuevas instantáneas, no WorkSpace podrá volver a restaurarla. En ese caso, puede intentar reconstruirlo WorkSpace o ponerse en contacto con AWS Support para obtener ayuda.

Puede restaurar un WorkSpace solo si se cumplen las siguientes condiciones:

- WorkSpace Debe tener un estado de`AVAILABLE`, `ERRORUNHEALTHY`, o`STOPPED`.
- Deben existir instantáneas de los volúmenes raíz y de usuario.

Para restaurar un WorkSpace

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Seleccione la WorkSpace que desea restaurar y elija Acciones, Reconstruir o Restaurar. WorkSpace
4. En Instantánea, seleccione la marca de tiempo de la instantánea.
5. Elija Restore (Restaurar).

Para restaurar un WorkSpace mediante el AWS CLI

Utilice el comando restore-workspace.

Microsoft 365 Bring Your Own License (BYOL) en forma personal WorkSpaces

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, Microsoft 365 G3/G5 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
- Migre sus aplicaciones actuales WorkSpaces para usar Microsoft 365 Apps para empresas
- Actualice sus aplicaciones de Microsoft 365 para empresas en WorkSpaces

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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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 del 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 Office AWS, puede instalar y configurar Microsoft 365 Apps for Enterprise en su WorkSpaces.

Si ya WorkSpaces tiene una licencia de Microsoft Office AWS, 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.

Actualizar Windows BYOL WorkSpaces en Personal 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
- Consideraciones
- Limitaciones conocidas
- Resumen de la configuración de la clave del Registro
- Realizar una actualización local
- Solución de problemas
- Actualice el WorkSpace registro mediante un script PowerShell

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. En su lugar, recomendamos realizar cualquier personalización del perfil de usuario mediante Group Policy Objects (GPOs). Las personalizaciones realizadas se GPOs pueden modificar o revertir fácilmente 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 in situ utiliza dos scripts de registro (`enable-inplace-upgrade.ps1`y`update-pvdrivers.ps1`) para realizar los cambios necesarios WorkSpaces que permiten ejecutar el 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

Clave del Registro	Tipo	Valores
		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. 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 .

Cómo 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 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 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. El estado de la WorkSpace instancia puede aparecer igual que durante la actualización. `UNHEALTHY`

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 restaurará automáticamente la versión de Windows 10 y 11 que existía 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%` tras 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 archivo en WorkSpaces Personal

> **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 PCo IP al DCV.
- 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). GraphicsPro.g4dn, Graphics y GraphicsPro) paquetes a paquetes, o en la otra dirección. non-GPU-enabled
- 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.
- Puede migrar el BYOP BYOL WorkSpaces de Windows 10 a Windows 11 y el BYOP con licencia incluida de Windows Server 2019 a Windows Server WorkSpaces 2022.

Para obtener más información sobre los WorkSpaces paquetes de Amazon, consultaPaquetes e imágenes para Personal WorkSpaces .

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
- Escenarios de migración
- Qué ocurre durante la migración
- Prácticas recomendadas
- Solución de problemas
- Cómo se ve afectada la facturación
- Migración de un WorkSpace

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 PCo IP a DCV, primero debe crear un paquete BYOL con el protocolo DCV. A continuación, puede migrar su BYOL PCo IP a ese paquete BYOL de WorkSpaces DCV.
- No puede migrar un paquete WorkSpace creado a partir de paquetes públicos o personalizados a un paquete BYOL.
- Los archivos Graphics.g4dn, GraphicsPro .g4dn, Graphics y GraphicsPro bundles están disponibles para el protocolo IP en Windows y Ubuntu. PCo Los archivos.g4dn y .g4dn están disponibles para el protocolo DCV en Windows y Ubuntu. GraphicsPro Gráficos y aún no se pueden migrar a DCV. GraphicsPro WorkSpaces
- Actualmente, no WorkSpaces 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.
- No puede migrar BYOP WorkSpaces a PCo IP o DCV. WorkSpaces
- No puede migrar un dominio de Active Directory unido a uno de WorkSpaces Microsoft Entra. WorkSpaces

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
BYOL BYOP de Windows 10	BYOL BYOP de Windows 11	Sí
BYOL BYOP de Windows 11	BYOL BYOP de Windows 10	No
BYOP público con Windows Server 2019	BYOP público con Windows Server 2022	Sí
BYOP público con Windows Server 2022	BYOP público con Windows Server 2019	No

> **Note**
>
> El acceso a la web no está disponible para la rama IP del paquete público de Windows 10 con Windows Server 2019. PCo

> **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 de la nueva 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 `AVAILABLESTOPPED`, 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
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 PCo IP a DCV, primero debe crear un paquete BYOL con el protocolo DCV. A continuación, puede migrar su BYOL PCo IP a ese paquete BYOL de WorkSpaces DCV.

5. Seleccione Migrar WorkSpaces.

   `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 paquete o una imagen personalizados en WorkSpaces Personal.

Para migrar WorkSpaces a través de AWS 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 un archivo WorkSpace en WorkSpaces Personal

Cuando haya terminado con un 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 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.

> **Note**
>
> Los conectores Simple AD y AD Connector están disponibles de forma gratuita WorkSpaces. Si no WorkSpaces se utiliza con tu directorio Simple AD o AD Connector durante 30 días consecutivos, se cancelará automáticamente el registro de este directorio para su uso en Amazon WorkSpaces y se te cobrará por él según las condiciones de AWS Directory Service precios.
> Para eliminar directorios vacíos, consulte Eliminar un directorio de WorkSpaces Personal. Si eliminas el directorio Simple AD o AD Connector, siempre podrás crear uno nuevo cuando quieras WorkSpaces volver a usarlo.

Para eliminar un WorkSpace

Puede eliminar una WorkSpace que se encuentre en cualquier estado excepto Suspendido.

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Selecciona tu WorkSpace y elige Eliminar.
4. Cuando se le pida confirmación, seleccione Eliminar WorkSpace. Se tarda aproximadamente 5 minutos en eliminar un WorkSpace. Durante la eliminación, el estado de WorkSpace se establece en Terminando. Cuando se complete la eliminación, WorkSpace desaparecerá de la consola.
5. (Opcional) Para eliminar paquetes e imágenes personalizados que no vaya a volver a usar, consulte Eliminar un paquete o una imagen personalizados en WorkSpaces Personal.
6. (Opcional) Tras eliminar todo WorkSpaces el contenido de un directorio, puede eliminarlo. Para obtener más información, consulte Eliminar un directorio de WorkSpaces Personal.
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 mediante el AWS CLI

Utilice el comando terminate-workspaces.

Paquetes e imágenes para Personal WorkSpaces

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. En la siguiente tabla se 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 del ciclo de vida o fecha de retirada
Windows Server 2016	Incluido	DCV, IP PCo	Valor, estándar, rendimiento, potencia, gráficos (retirados) PowerPro, gráficos. G4dn GraphicsPro, .g4dn GraphicsPro	12 de enero de 2027
Windows Server 2019	Incluido	DCV, IP PCo	Valor, estándar, rendimiento, potencia, gráficos (retirados) PowerPro, gráficos. G4dn GraphicsPro, .g4dn GraphicsPro	9 de enero de 2029
Windows Server 2022	Incluido	DCV, IP PCo	Estándar, rendimiento, potencia, GeneralPurpose .4xlarge PowerPro, GeneralPurpose .8xlarge, gráficos (retirados), graphics.G4dn, .g4dn GraphicsPro GraphicsPro	14 de octubre de 2031
Windows 10	Traiga su propia licencia (BYOL)	PCoDCV, IP	Valor, estándar, rendimiento, potencia, gráficos (retirados) PowerPro, gráficos. G4dn GraphicsPro, .g4dn GraphicsPro	Dentro del período soporte
Windows 11	Traiga su propia licencia (BYOL)	DCV	Estándar, rendimiento, potencia, .4xlarge, .8xlarge PowerPro GeneralPurpose GeneralPurpose	Dentro del período soporte
Amazon Linux 2	Incluido	PCoDCV, IP	Valor, estándar, rendimiento, potencia PowerPro	Dentro del período soporte

Sistema operativo	Licencias	Protocolos de transmisión	Paquetes compatibles	Política del ciclo de vida o fecha de retirada
Ubuntu 22.04 LTS	Incluido	DCV	Valor, estándar, rendimiento, potencia, gráficos. PowerPro G4dn, .g4dn GraphicsPro	Junio de 2032
Rocky Linux 8	Incluido	DCV	Valor, estándar, rendimiento, potencia, PowerPro	31 de mayo de 2029
Red Hat Enterprise Linux 8	Incluido	DCV	Valor, estándar, rendimiento, potencia, PowerPro	31 de mayo de 2029

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 PCo IP.

Contenido

- Opciones de paquetes para WorkSpaces Personal
- Crea una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal
- Actualizar un paquete personalizado para WorkSpaces Personal
- Copiar una imagen personalizada en WorkSpaces Personal
- Compartir o dejar de compartir una imagen personalizada en Personal WorkSpaces
- Eliminar un paquete o una imagen personalizados en WorkSpaces Personal

Opciones de paquetes para WorkSpaces Personal

Antes de seleccionar un paquete, asegúrese de que el paquete que desea seleccionar sea compatible con su protocolo WorkSpaces, sistema operativo, red y tipo de cómputo. Para obtener más información sobre los protocolos, consulte Protocols for Amazon WorkSpaces. Para obtener más información sobre las redes, consulta los requisitos de red de los WorkSpaces clientes de Amazon.

> **Note**
>
> - Recomendamos no superar la latencia de red máxima de 250 ms para PCo IP WorkSpaces. Para obtener la mejor experiencia de WorkSpaces usuario de PCo IP, recomendamos mantener la latencia de la red por debajo de los 100 ms. Cuando el tiempo de ida y vuelta (RTT) supere los 375 ms, la conexión del WorkSpaces cliente se apagará. Para obtener la mejor experiencia de usuario del DCV, recomendamos mantener el RTT por debajo de 250 ms. Si el RTT está entre 250 ms y 400 ms, el usuario puede acceder a él 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.
> - Los paquetes BYOP (Bring Your Own Protocol) son para Core. WorkSpaces Los paquetes BYOP proporcionados por Amazon WorkSpaces no tienen instalado un protocolo de streaming WorkSpaces proporcionado. No podrás conectarte mediante WorkSpaces clientes o pasarelas. Para entender el modelo de responsabilidad compartida de Amazon WorkSpaces Core, consulte la Guía de integración de socios tecnológicos de Amazon WorkSpaces Core. Para obtener más información, consulte Amazon WorkSpaces Core.

> **Important**
>
> - GraphicsPro El paquete estará end-of-life disponible el 31 de octubre de 2025. Te recomendamos migrar tus paquetes GraphicsPro WorkSpaces a los compatibles antes del 31 de octubre de 2025. Para obtener más información, consulte Migrar un WorkSpace archivo en WorkSpaces Personal.

- El paquete de Graphics dejará de ser compatible a partir del 30 de noviembre de 2023. Recomendamos cambiar al paquete Graphics.G4DN para usar el paquete Graphics. WorkSpaces
- Los gráficos y GraphicsPro los paquetes no están disponibles actualmente en la región de Asia Pacífico (Bombay).

Los siguientes son los paquetes que WorkSpaces se ofrecen. Para obtener información sobre los paquetes disponibles WorkSpaces, consulta Amazon WorkSpaces Bundles.

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
- Correo electrónico

Este paquete no se recomienda para conferencias de audio y vídeo, uso compartido de pantalla, procesamiento de textos, herramientas de desarrollo de software, aplicaciones de inteligencia empresarial y aplicaciones gráficas.

Paquete de rendimiento

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Mensajería instantánea
- Correo electrónico
- Hojas de cálculo
- Procesamiento de audio
- Material didáctico

Este paquete no se recomienda para videoconferencias, uso compartido de pantalla, herramientas de desarrollo de software, aplicaciones de inteligencia empresarial y aplicaciones gráficas.

Paquete de energía

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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.

PowerPro paquete

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos

- Correo electrónico
- 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 aprendizaje automático, la formación de modelos y las aplicaciones gráficas.

Paquetes de uso general

Estos paquetes, incluidos los paquetes GeneralPurpose .4xlarge y GeneralPurpose .8xlarge, son adecuados para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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
- Procesamiento por lotes
- Capacitación con modelos de aprendizaje automático (ML) basados en CPU

Este paquete no se recomienda para el renderizado 3D, el diseño fotorrealista, la transmisión de juegos o el entrenamiento con modelos de aprendizaje automático para modelos complejos.

GraphicsPro paquete

Este paquete ofrece un nivel básico de rendimiento gráfico y un alto nivel de rendimiento de CPU y memoria para su WorkSpaces. Está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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 conferencias de audio y vídeo, renderización 3D y diseño fotorrealista.

Paquete Graphics.G4DN

Este paquete ofrece un alto nivel de rendimiento gráfico y un nivel moderado de rendimiento de CPU y memoria, WorkSpaces y es ideal para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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 (computer-aided design/computer-fabricación asistida)

Este paquete no se recomienda para conferencias de audio y vídeo, renderización 3D, diseño fotorrealista y entrenamiento con modelos de aprendizaje automático.

GraphicsPro.paquete g4dn

Este paquete ofrece un alto nivel de rendimiento gráfico, rendimiento de CPU y memoria para usted, WorkSpaces y es ideal para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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 (computer-aided design/computer-fabricación asistida)
- 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 para WorkSpaces Personal

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 dos 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 uniforme (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 feature/version actualización de Windows). Sin embargo, el proceso de WorkSpaces creación de 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 archivo en WorkSpaces Personal.

- 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 archivo en WorkSpaces Personal.
- GraphicsPro El paquete estará disponible el 31 de octubre de 2025 end-of-life. Te recomendamos migrar tus paquetes GraphicsPro WorkSpaces a los compatibles antes del 31 de octubre de 2025. Para obtener más información, consulte the section called “Migre un WorkSpace”.
- Los gráficos y GraphicsPro los paquetes no están disponibles actualmente en la región de Asia Pacífico (Bombay).
- Los volúmenes de almacenamiento de 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

- Requisitos para crear imágenes personalizadas de Windows
- Requisitos para crear imágenes personalizadas de Linux
- 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 y componentes del servicio necesarios”.
  - Windows PowerShell versión 3.0 o posterior
  - Servicios de Escritorio remoto
  - AWS Controladores PV
  - Administración remota de Windows (WinRM)
  - Agentes y controladores PCo IP de Teradici
  - Agentes y controladores de STXHD
  - AWS y certificados WorkSpaces
  - 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 PCo IP o DCV de Teradici
  - 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 la cuota, utilice el formulario de límites de WorkSpaces .
- Asegúrate de no intentar crear una imagen a partir de una imagen cifrada 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 Personal.
- En el caso de Windows WorkSpaces, no configure ningún objeto de política de grupo (GPOs) 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 cualquier personalización en el perfil de usuario y aplicarla después de la creación de la imagen. GPOs GPOs se pueden modificar o revertir fácilmente y, por lo tanto, son menos propensas 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 DCV activado, consulte Utilizar tarjetas inteligentes para la autenticación en WorkSpaces Personal 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 y PV NVMe, en su ordenador. WorkSpaces Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulte Install or upgrade Elastic Network Adapter (ENA) driver , Controladores NVMe de AWS for Windows instances y Upgrade PV drivers on Windows instances.
- Asegúrese de actualizar periódicamente los agentes EC2 Config, EC2 EC2 Launch y Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulta Update EC2 Config and EC2 Launch.

(Opcional) Paso 1: especificar un formato de nombre de equipo personalizado para la imagen

En el caso de las imágenes WorkSpaces lanzadas a partir de una versión personalizada o de Bring Your Own License (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>`. En el caso de las imágenes basadas en Windows 10, los nombres de los equipos que WorkSpaces utilizarán los paquetes personalizados comenzarán por EC2 AMAZ-. *`xxxxxxx`* En el caso de las imágenes basadas en Windows 11, los nombres de equipo para los que se WorkSpaces utilizan paquetes personalizados comenzarán por WORKSPA-. *`xxxxxxx`*

> **Note**
>
> - Sysprep ignora los valores `<RegisteredOrganization>` y `<RegisteredOwner>` de la sección `<settings pass="oobeSystem">`.
> - Tanto **<** RegisteredOrganization **>** como **<** RegisteredOwner **>** son valores obligatorios.

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">`, si utiliza Windows 10, se quitará la marca de comentario de `<ComputerName>*</ComputerName>`. Si utiliza Windows 11, no necesitará eliminar la marca de comentario de esta sección. Asegúrese de que `<ComputerName>` esté configurado 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">`, se mostrará el campo `<RegisteredOrganization>` en Windows 10 y Windows 11. La etiqueta `<RegisteredOwner>` solo se mostrará en Windows 10 de forma predeterminada. Si utiliza Windows 11, tendrá que añadir esta etiqueta. Establezca `<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 de los equipos WorkSpaces creados a partir del paquete personalizado comenzarán por EC2 AMAZ-*`xxxxxxx`*.

> **Note**
>
> - Sysprep ignora los valores `<RegisteredOrganization>` y `<RegisteredOwner>` de la sección `<settings pass="oobeSystem">`.
> - Tanto < RegisteredOrganization > como < RegisteredOwner > son valores obligatorios.

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 actualizaciones acumulativas y de seguridad de Windows más recientes 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 que WorkSpace haya superado 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 Windows 10 que se han actualizado de una versión de Windows 10 a una versión más reciente de Windows 10 (una feature/version actualización 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 AWS Support Centro para reparar su EC2 Config o EC2 Launch.

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 el 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 la versión 1.2 de TLS debe estar habilitada

Para configurar SSL/TLS para Windows, consulte Cómo habilitar TLS 1.2 en la documentación de Microsoft Windows.

Solo puede existir un perfil de usuario en 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 es compatible con los sistemas Windows que se han actualizado de una versión de Windows 10 a una versión más reciente de Windows 10 (una feature/version actualización de Windows).

Para crear imágenes, utilice una WorkSpace que no se haya actualizado a feature/version 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 (GPOs) restringen el acceso a la huella digital del certificado RDP cuando lo solicitan el servicio EC2 Config o los scripts de EC2 lanzamiento durante

la configuración de la instancia de Windows. Antes de intentar crear una imagen, muévela WorkSpace a una nueva unidad organizativa (OU) cuya herencia esté bloqueada y no GPOs se haya 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. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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 en WorkSpaces Personal 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, asegúrese 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 el paquete 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 GeneralPurpose .4xlarge o GeneralPurpose .8xlarge WorkSpace con un mínimo de 175 GB para el volumen raíz y 100 GB para el volumen de usuario.
> - Puedes lanzar 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
- /.d/70-persistent-net.rules etc/udev/rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- var/log/pcoip/-agente
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /-estado var/lib/skylight/domain de unión
- /var/lib/skylight/configuration-datos
- /-data.json var/lib/skylight/config
- /inicio
- etc/default/grub.d/zz/-hibernation.cfg
- /etc/netplan/zz-workspaces-dominio.yaml

- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/AccountsService/users

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/.clave
- /.clave var/lib/skylight/public

Actualizar un paquete personalizado para WorkSpaces Personal

Para actualizar un WorkSpaces paquete personalizado existente, modifique uno basado en el paquete, cree una imagen a partir del WorkSpace paquete y actualice el paquete con la nueva imagen. WorkSpace A continuación, puede lanzar un nuevo paquete WorkSpaces con el paquete actualizado.

> **Important**
>
> WorkSpaces Los existentes no se actualizan automáticamente al actualizar el paquete en el que se basan. Para actualizar los paquetes existentes WorkSpaces que se basan en un paquete que has actualizado, debes volver a crearlos WorkSpaces o eliminarlos y volver a crearlos.

Para actualizar un paquete mediante la consola

1. Conéctese a uno WorkSpace que esté 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.

   Como alternativa, puede crear uno nuevo WorkSpace con el mismo paquete de software básico (Plus o Standard) que la imagen utilizada para crear el paquete y realizar los cambios.
2. Si todavía está conectado a WorkSpace, desconéctese seleccionando Amazon WorkSpaces y Disconnect en la aplicación WorkSpaces cliente.

3. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
4. En el panel de navegación, elija WorkSpaces.
5. Seleccione WorkSpace y elija Acciones, Crear imagen. Si el estado de WorkSpace es`STOPPED`, debe iniciarlo primero (elija Acciones, Iniciar WorkSpaces) antes de poder elegir Acciones, Crear imagen.
6. Escriba un nombre y una descripción para la imagen y, a continuación, elija Create Image (Crear imagen). No WorkSpace 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 para WorkSpaces Personal.
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. Si es necesario, actualice cualquier elemento existente WorkSpaces que esté basado en el lote reconstruyéndolo WorkSpaces o eliminándolo y volviéndolo a crear. Para obtener más información, consulte Reconstruir un WorkSpace in WorkSpaces Personal.

Para actualizar un paquete mediante programación

Para eliminar un paquete mediante programación, utilice la acción de la API UpdateWorkspaceBundle. Para obtener más información, consulta UpdateWorkspaceBundlela referencia de la WorkSpaces API de Amazon.

Copiar una imagen personalizada en WorkSpaces Personal

Puede copiar una WorkSpaces imagen personalizada dentro de una región o de una AWS región a otra. 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 la AWS GovCloud (US) Region década de 1980, para copiar imágenes desde y hacia otras AWS regiones, ponte en contacto con AWS Support.
En las regiones de suscripción voluntaria, para copiar imágenes a otras regiones, ponte en contacto con AWS Support. Para obtener más información sobre las regiones registradas, consulte Regiones disponibles.

También puedes copiar una imagen que otra AWS cuenta haya compartido contigo. Para obtener más información sobre las imágenes compartidas, consulte Compartir o dejar de compartir una imagen personalizada en Personal 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 WorkSpaces las cuotas de Amazon, consulta 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.

JSON

```
{
  "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.
>
> JSON
>
> ```
> {
>  "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 Administración de identidad y acceso para WorkSpaces.

Copia en bloque de imágenes

Puede copiar imágenes una por una mediante la consola. Para copiar imágenes de forma masiva, usa la operación de CopyWorkspaceImage API o el copy-workspace-image comando

en AWS Command Line Interface (AWS CLI). Para obtener más información, consulta CopyWorkspaceImagela referencia de la WorkSpaces API de Amazon o copy-workspace-imagela referencia de AWS CLI comandos.

> **Important**
>
> Antes de copiar una imagen compartida, asegúrate de que se ha compartido desde la AWS cuenta correcta. Para determinar si una imagen se ha compartido y ver el ID de AWS cuenta propietario de la imagen, utilice las operaciones de DescribeWorkspaceImagePermissionsAPI DescribeWorkSpaceImagesy o los describe-workspace-image-permissionscomandos describe-workspace-imagesy de AWS CLI.

Para copiar una imagen mediante la consola

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Images.
3. Seleccione la imagen y elija Acciones, Copiar imagen.
4. En Seleccione el destino, seleccione la AWS región 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 Etiquete los recursos en WorkSpaces Personal.
7. Elija Copiar imagen.

Compartir o dejar de compartir una imagen personalizada en Personal WorkSpaces

Puedes compartir WorkSpaces imágenes personalizadas entre AWS cuentas de la misma AWS región. Una vez que se ha compartido una imagen, la cuenta del destinatario puede copiarla en otras AWS regiones según sea necesario. Para obtener más información sobre cómo copiar imágenes, consulte Copiar una imagen personalizada en WorkSpaces Personal.

> **Note**
>
> En la región de China (Ningxia), solo puede copiar imágenes dentro de la misma región.

En la AWS GovCloud (US) Region década de 1980, para copiar imágenes desde y hacia otras AWS regiones, ponte en contacto con AWS Support.

No se aplican cargos adicionales por compartir una imagen. Sin embargo, se aplica la cuota de número de imágenes en la AWS región. 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 WorkSpaces las cuotas de Amazon, consulta 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

Solo puedes compartir imágenes de Bring Your Own License (BYOL) con AWS cuentas que estén habilitadas para BYOL. La AWS cuenta con la que desee compartir las imágenes de BYOL también debe formar parte de su organización (con la misma cuenta de pago).

> **Note**
>
> Por el momento, no se permite compartir imágenes BYOL entre AWS cuentas en las regiones (EE. UU. Oeste) y AWS GovCloud AWS GovCloud (EE. UU. Este). Para compartir imágenes BYOL entre cuentas de las regiones (EE. UU. Oeste) y AWS GovCloud AWS GovCloud (EE. UU. Este), póngase en contacto con Support. AWS

Imágenes compartidas con usted

Si las imágenes se comparten con usted, puede copiarlas. A continuación, puedes usar tus copias de las imágenes compartidas para crear paquetes para lanzar nuevos. WorkSpaces

> **Important**
>
> Antes de copiar una imagen compartida, asegúrate de que se ha compartido desde la AWS cuenta correcta. Para determinar mediante programación si se ha compartido una imagen, utilice las operaciones DescribeWorkSpaceImagesy de la DescribeWorkspaceImagePermissionsAPI o los describe-workspace-image-permissionscomandos describe-workspace-imagesy de la interfaz de línea de comandos (CLI). 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 WorkSpaces consola en la versión 2/home. 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. A continuación, la cuenta del destinatario podrá utilizar su copia de la imagen compartida para crear paquetes para lanzar nuevos. WorkSpaces

Para dejar de compartir una imagen

1. Abre la WorkSpaces consola en la versión 2/homehttps://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, selecciona la AWS cuenta con la que quieres dejar de compartir y, a continuación, selecciona 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, todas las copias de las imágenes compartidas que ya estén en la cuenta del destinatario permanecerán en esa cuenta y se WorkSpaces podrán abrir nuevas a partir de esas copias.

Para compartir o dejar de compartir imágenes mediante programación

Para compartir o dejar de compartir imágenes mediante programación, usa la operación UpdateWorkspaceImagePermissionAPI o el comando update-workspace-image-permission AWS Command Line Interface ()AWS CLI. Para determinar si se ha compartido una imagen, utilice la operación DescribeWorkspaceImagePermissionsAPI o el comando describe-workspace-image-permissionsCLI.

Eliminar un paquete o una imagen personalizados en WorkSpaces Personal

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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Bundles.
3. Seleccione el paquete y elija Eliminar.
4. Cuando se le pida confirmación, seleccione 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 dos horas después de eliminar un paquete antes de crear uno nuevo con el mismo nombre.

Eliminación de 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Images.
3. Seleccione la imagen y elija Eliminar.
4. Cuando se le pida confirmación, seleccione 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.

Monitor WorkSpaces personal

Puede utilizar las siguientes funciones para monitorear su WorkSpaces.

CloudWatch métricas

Amazon WorkSpaces publica puntos de datos en Amazon CloudWatch sobre su WorkSpaces. CloudWatchle 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 Supervisa tus 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 acciones realizadas por un usuario, un rol o un AWS servicio 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 CloudTrail registra los eventos de inicio de sesión correctos y fallidos de los usuarios de tarjetas inteligentes. Para obtener más información, consulte Descripción de los eventos AWS de inicio de sesión 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 red global para calcular una base de rendimiento y disponibilidad para el tráfico conectado a Internet. Actualmente, Internet Monitor no puede proporcionar el rendimiento de Internet a un usuario final individual, pero sí a nivel de ciudad e ISP.

Registros de acceso de Amazon S3

Si los usuarios tienen datos de configuración de la aplicación o datos de carpetas de inicio almacenados en buckets de Amazon S3 considere la posibilidad de ver los registros de acceso al servidor de Amazon S3 para monitorear el acceso. Estos registros de acceso proporcionan registros detallados sobre las solicitudes que se realizan a un bucket. Los registros de acceso al servidor resultan útiles para muchas aplicaciones. Por ejemplo, la información del registro de acceso puede ser útil en auditorías de acceso y seguridad. Para obtener más información, consulte el tema Registro de acceso al servidor de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

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 mantienen durante 15 meses para obtener acceso a la información histórica y para supervisar el rendimiento de su servicio o aplicación 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 utilizar el panel para lo siguiente:

- 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.
- Ver el uso de los recursos críticos a lo largo del tiempo.
- Identificar las anomalías con el fin de ayudar a solucionar problemas.

WorkSpaces CloudWatch Los paneles automáticos están disponibles en todas las regiones AWS comerciales.

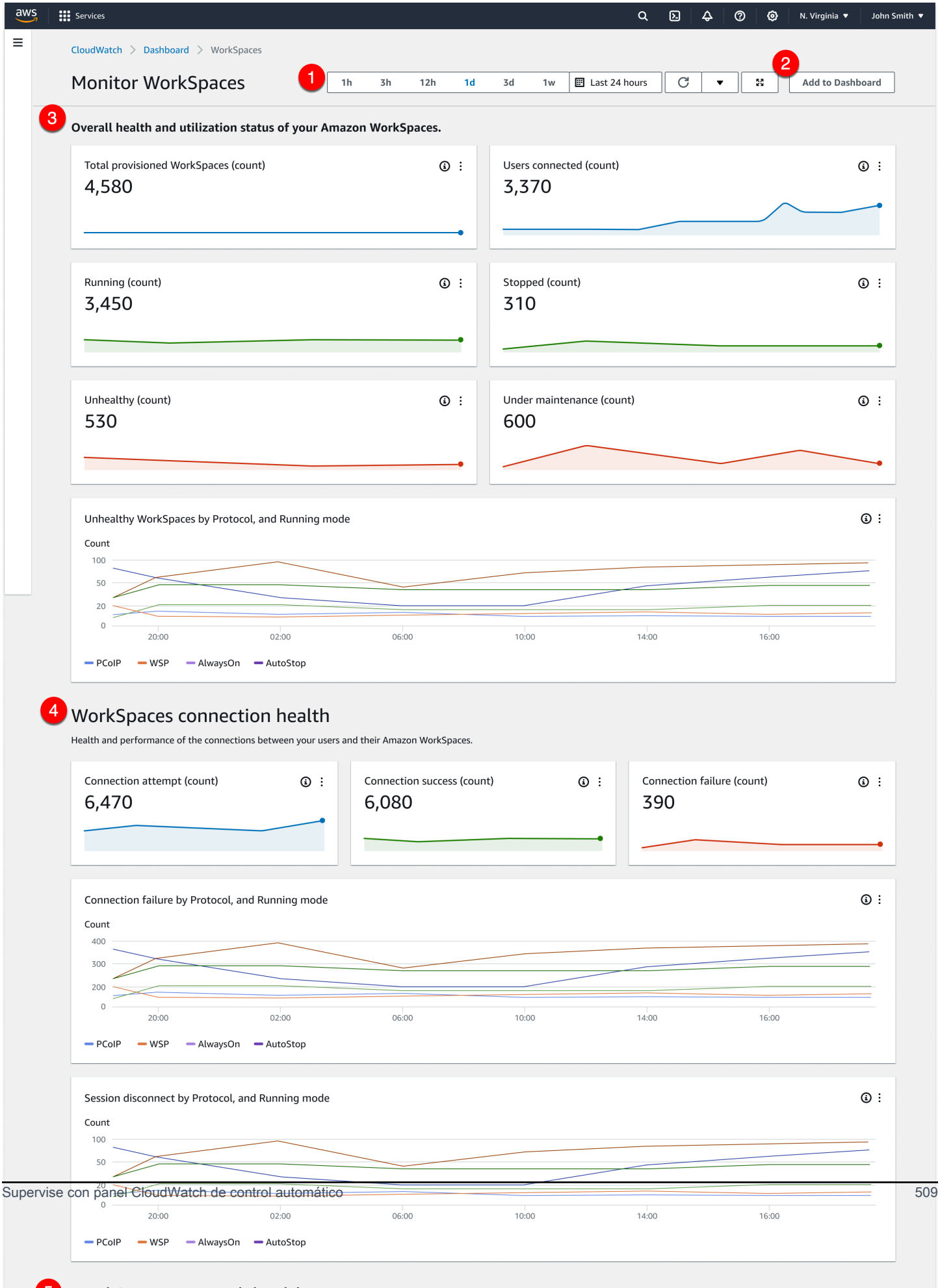
Para usar el panel de control WorkSpaces CloudWatch automático

1. Abra 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 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 consta de las siguientes características:

1. Visualización de 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. Seleccione el menú de puntos suspensivos y, a continuación, elija Ver en métricas para ver las métricas en un gráfico de escala de tiempo.
4. Consulte 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. Visualización del rendimiento del host y el uso de los recursos para identificar y solucionar posibles problemas de rendimiento.

Supervisa tus CloudWatch métricas WorkSpaces de uso

WorkSpaces y Amazon CloudWatch están integrados, por lo que puedes recopilar y analizar las métricas de rendimiento. Puede supervisar 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 Personal.

Contenido

- WorkSpaces métricas
- Dimensiones de las WorkSpaces métricas
- Ejemplo de monitorización

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`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`Unhealthy` [1]	El número WorkSpaces que devolvió un estado insalubre.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`		

`ConnectionAttempt` [2]	El número de intentos de conexión.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

`ConnectionSuccess` [2]	El número de conexiones realizadas correctamente.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`ConnectionFailure` [2]	El número de conexiones que han producido un error.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

`SessionLaunchTime` [2, 6]	La cantidad de tiempo que se tarda en iniciar una WorkSpaces sesión.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Segundo (tiempo)

`InSessionLatency` [2, 6]	El tiempo de ida y vuelta entre el WorkSpaces cliente y el WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			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`
		`ComputerName`
			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`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

`Stopped`	El número de los WorkSpaces que están detenidos.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

`Maintenance` [4]	El número de los WorkSpaces que están en mantenimiento.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades
`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
`TrustedDeviceCertificateDaysBeforeExpiration` [6]	Días que faltan para que caduque el certificado raíz asociado al directorio.	`CertificateId`	Promedio, mínimo, máximo, suma, muestras de datos	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades

`CPUUsage`	El porcentaje de los recursos utilizados de la CPU.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, Máximo, Mínimo	Porcentaje

`MemoryUsage`	El porcentaje de la memoria de la máquina utilizada.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, Máximo, Mínimo	Porcentaje

Métrica	Descripción	Dimensiones	Statistics	Unidades

`RootVolumeDiskUsage`	El porcentaje del volumen del disco raíz utilizado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, Máximo, Mínimo	Porcentaje

`UserVolumeDiskUsage`	El porcentaje del volumen del disco del usuario utilizado.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, Máximo, Mínimo	Porcentaje

Métrica	Descripción	Dimensiones	Statistics	Unidades

`UDPPacketLossRate` [7]	El porcentaje de paquetes eliminados entre el cliente y la puerta de enlace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			Promedio, Máximo, Mínimo, Muestras de datos	Porcentaje

`UpTime`	El tiempo transcurrido desde el último reinicio de un WorkSpace.	`DirectoryId`
		`WorkspaceId`
		`RunningMode`
		`Protocol`
		`ComputeType`
		`BundleId`
		`UserName`
		`ComputerName`
			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 por 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 el promedio de pérdida de paquetes.

- En PCo IP: mide la pérdida media de paquetes UDP del cliente a la puerta de enlace.

> **Note**
>
> Esto se mide en la puerta de enlace.

- En DCV: mide el promedio de pérdida de paquetes UDP del cliente a la puerta de enlace.

> **Note**
>
> Esto se mide en la puerta de enlace.

Dimensiones de las WorkSpaces métricas

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 especificado. El formato del ID de directorio es `d-XXXXXXXXXX` .
`WorkspaceId`	Filtra los datos métricos según lo especificado WorkSpace. La forma del WorkSpace identificador 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` .
`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.

Dimensión	Descripción
	Note El `UserName` no puede incluir caracteres que no sean ASCII, como, por ejemplo: • Letras acentuadas: é, à, ö, ñ, etc. • Alfabetos no latinos • Símbolos: ©#, ®#, €, £, µ, ¥, etc.
`ComputerName`	Filtra los datos de las métricas según lo especificado WorkSpace. Consulte varios formatos para el nombre del WorkSpaces equipo.

Ejemplo de monitorización

El siguiente ejemplo muestra cómo se puede utilizar AWS CLI para responder a una CloudWatch alarma y determinar cuáles de WorkSpaces los directorios 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 WorkSpace mediante 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 para WorkSpaces usar DCV 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 con PCo IP cero, esta es la dirección IP del cliente de autenticación 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 Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/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. Elija 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 subscripción.
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 que gestione los eventos WorkSpaces

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. Elija 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.

Descripción de los eventos AWS de inicio de sesión 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 CloudTrail evento de inicio de sesión y sus finalidades.

Nombre de evento	Propósito del evento
`CredentialChallenge`	Notifica que al AWS iniciar sesión se ha solicitado al usuario que resuelva un problema de credenciales específico y especifica lo `CredentialType` que se requiere (por ejemplo, una TARJETA INTELIGENTE).
`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.

Nombre de evento	Propósito del evento
`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 correctamente los desafíos de credenciales requeridos, no se registrará ningún evento de `UserAuthentication` .

En la siguiente tabla, se muestran otros campos de datos de eventos útiles incluidos en eventos de inicio de sesión específicos. CloudTrail

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» (valores posibles en la actualidad: SMARTCARD)
`LoginTo`	Se utiliza para notificar que todos los requisitos de autenticación con los	`UserAuthentication`	"LoginTo«:" https://skylight.local»

Nombre de evento	Propósito del evento	Aplicabilidad al evento de inicio de sesión	Valores de ejemplo
	que se desafió al usuario se han completado con éxito y que el usuario ha iniciado sesión correctamente. Si los usuarios no completan correctamente los desafíos de credenciales requeridos, no se registrará ningún evento de `UserAuthentication` .		

Ejemplos de eventos para escenarios de AWS inicio de sesión

Los siguientes ejemplos muestran la secuencia de CloudTrail eventos esperada para diferentes escenarios de inicio de sesión.

Contenido

- El inicio de sesión se realizó correctamente al autenticarse con una tarjeta inteligente
- Inicio de sesión fallido al autenticarse solo con una tarjeta inteligente

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"
    }
}
```

Con error 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"
    }
}
```

Cree CloudWatch cuadros de mando personalizados mediante plantillas AWS CloudFormation

AWS proporciona AWS CloudFormation plantillas que puede utilizar para crear CloudWatch paneles personalizados. WorkSpaces Elija una de las siguientes opciones de AWS CloudFormation plantilla para crear paneles personalizados para su WorkSpaces consola. AWS CloudFormation

Aspectos que hay que tener en cuenta antes de comenzar

Tenga en cuenta lo siguiente antes de empezar con los CloudWatch paneles personalizados:

- Cree sus paneles de control de la Región de AWS misma forma que los desplegados WorkSpaces que desee supervisar.
- También puede crear paneles personalizados mediante la CloudWatch consola.
- Los CloudWatch paneles personalizados pueden tener un coste asociado. Para obtener información sobre los precios, consulta Amazon CloudWatch Pricing

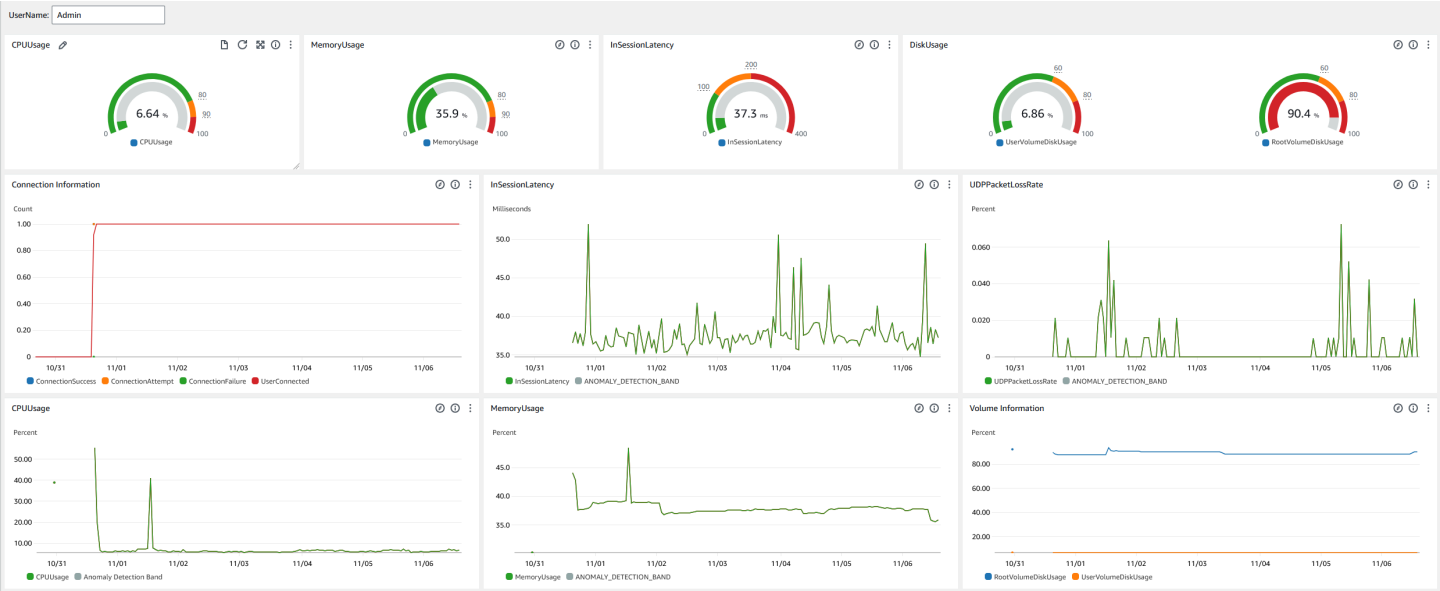
Panel de servicio de asistencia

El panel de Help Desk muestra las siguientes métricas para una información específica WorkSpace:

- Uso de la CPU
- Uso de memoria

- Latencia durante la sesión
- Volumen raíz
- Volumen de usuarios
- Pérdida de paquetes
- Consumo de disco

A continuación se muestra un ejemplo del panel de servicio de asistencia.



Complete el siguiente procedimiento para crear un panel personalizado en CloudWatch uso AWS CloudFormation.

1. Abre la página Crear pila en la AWS CloudFormation consola. Este enlace abre la página con la ubicación del depósito de Amazon S3 de la plantilla de CloudWatch panel personalizado de Help Desk rellenada previamente.
2. Revise las selecciones predeterminadas en la página Crear pila. Tenga en cuenta que el campo URL de Amazon S3 viene rellenado previamente con la ubicación del bucket de Amazon S3 de la AWS CloudFormation plantilla.
3. Elija Siguiente.
4. En el cuadro de texto Nombre de pila, escriba el nombre de la pila.

   El nombre de pila es un identificador que le ayuda a encontrar una en particular en una lista de pilas. El nombre de una pila puede contener únicamente caracteres alfanuméricos (con

distinción entre mayúsculas y minúsculas) y guiones. Debe comenzar con un carácter alfabético y no puede tener más de 128 caracteres.

5. En el cuadro de DashboardNametexto, introduce el nombre que quieres asignar a tu panel de control.

   El nombre del panel solo puede incluir caracteres alfanuméricos, el signo del guion (−) y el signo del guion bajo (_).

6. Elija Siguiente.
7. Revise las selecciones predeterminadas en la página Configurar opciones de pila y elija Siguiente.
8. Desplácese hasta Las transformaciones pueden requerir capacidades de acceso y marque las casillas para confirmar. A continuación, selecciona Enviar para crear la pila y el CloudWatch panel personalizado.

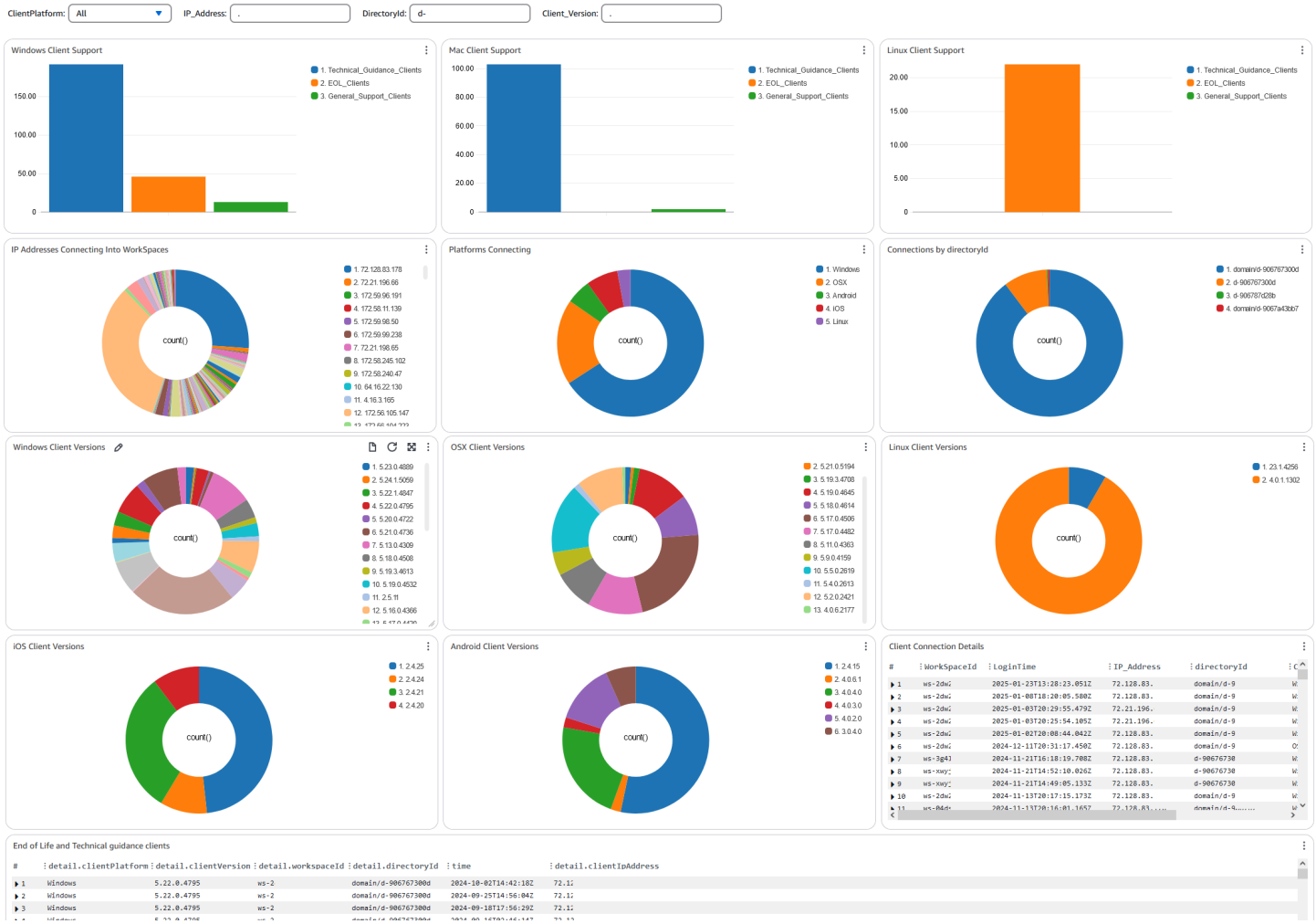
   > **Important**
   >
   > Es posible que haya un costo asociado a los CloudWatch paneles personalizados. Para obtener información sobre los precios, consulta Amazon CloudWatch Pricing

9. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
10. En el panel de navegación de la izquierda, elija Paneles.
11. En Paneles personalizados, seleccione el panel con el nombre que ha introducido anteriormente en este procedimiento.
12. Con la plantilla de ejemplo del Help Desk, introduzca UserName la WorkSpace que desea supervisar sus datos.

Panel de información de conexión

El panel de control de Connection Insights muestra las versiones de los clientes, las plataformas y las direcciones IP que están conectadas al suyo WorkSpaces. Este panel le permite comprender mejor cómo se conectan los usuarios para que pueda enviarles notificaciones de forma proactiva con un cliente obsoleto. Las variables dinámicas le permiten supervisar los detalles de las direcciones IP o directorios específicos.

A continuación se muestra un ejemplo del panel de información sobre la conexión.



Complete el siguiente procedimiento para crear un panel personalizado en CloudWatch uso AWS CloudFormation.

1. Abre la página Crear pila en la AWS CloudFormation consola. Este enlace abre la página con la ubicación del depósito de Amazon S3 de la plantilla de CloudWatch panel personalizado de Connection Insights rellenada previamente.
2. Revise las selecciones predeterminadas en la página Crear pila. Tenga en cuenta que el campo URL de Amazon S3 viene rellenado previamente con la ubicación del bucket de Amazon S3 de la AWS CloudFormation plantilla.
3. Elija Siguiente.
4. En el cuadro de texto Nombre de pila, escriba el nombre de la pila.

   El nombre de pila es un identificador que le ayuda a encontrar una en particular en una lista de pilas. El nombre de una pila puede contener únicamente caracteres alfanuméricos (con

distinción entre mayúsculas y minúsculas) y guiones. Debe comenzar con un carácter alfabético y no puede tener más de 128 caracteres.

5. En el cuadro de DashboardNametexto, introduce el nombre que quieres asignar a tu panel de control. Introduzca otra información relevante sobre la configuración del grupo de CloudWatch acceso.

   El nombre del panel solo puede incluir caracteres alfanuméricos, el signo del guion (–) y el signo del guion bajo (_).

6. En la sección LogRetention, introduzca el número de días durante los que desea conservar LogGroup el suyo.
7. En SetupEventBridge, elija si desea implementar la EventBridge regla para obtener los registros de WorkSpaces acceso.
8. En la sección WorkSpaceAccessLogsName, introduzca el nombre de la CloudWatch LogGroup entidad que tiene los registros de WorkSpaces acceso.
9. Elija Siguiente.
10. Revise las selecciones predeterminadas en la página Configurar opciones de pila y elija Siguiente.
11. Desplácese hasta Las transformaciones pueden requerir capacidades de acceso y marque las casillas para confirmar. A continuación, seleccione Enviar para crear la pila y el CloudWatch panel personalizado.

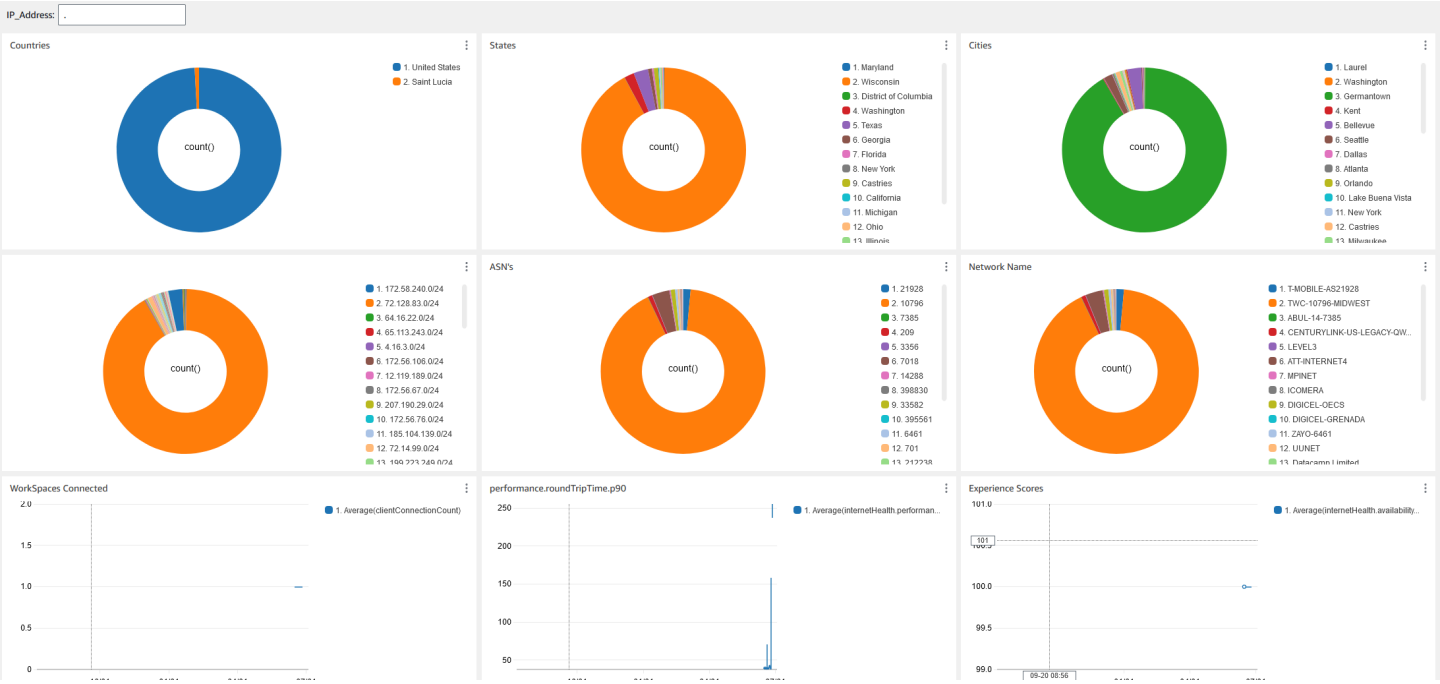
    > **Important**
    >
    > Es posible que haya un costo asociado a los CloudWatch paneles personalizados. Para obtener información sobre los precios, consulta Amazon CloudWatch Pricing

12. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
13. En el panel de navegación de la izquierda, elija Paneles.
14. En Paneles personalizados, seleccione el panel con el nombre que ha introducido anteriormente en este procedimiento.
15. Ahora puede supervisar sus datos mediante el panel WorkSpace de control de Connection Insights.

Panel de supervisión de Internet

El panel de supervisión de Internet muestra detalles sobre el proveedor de servicios de Internet (ISP) que utilizan los usuarios para unirse a sus WorkSpaces instancias. Proporciona detalles sobre la ciudad, el estado, la ASN, el nombre de la red, el número de personas conectadas WorkSpaces, el rendimiento y las puntuaciones de experiencia. También puede usar direcciones IP específicas para obtener los detalles de los usuarios que se conectan desde una determinada ubicación. Implemente un monitor de CloudWatch Internet para obtener información sobre los datos del ISP. Para obtener más información, consulte Uso de Amazon CloudWatch Internet Monitor.

A continuación se muestra un ejemplo del panel de supervisión de Internet.



Para crear un panel de control personalizado CloudWatch utilizando AWS CloudFormation

> **Note**
>
> Antes de crear un panel personalizado, asegúrese de crear un monitor de Internet con CloudWatch Internet Monitor. Para obtener más información, consulte Creación de un monitor en Amazon CloudWatch Internet Monitor mediante la consola

1. Abra la página Crear pila en la AWS CloudFormation consola. Este enlace abre la página con la ubicación del depósito de Amazon S3 de la plantilla de CloudWatch panel personalizado de monitoreo de Internet rellenada previamente.

2. Revise las selecciones predeterminadas en la página Crear pila. Tenga en cuenta que el campo URL de Amazon S3 viene rellenado previamente con la ubicación del bucket de Amazon S3 de la AWS CloudFormation plantilla.
3. Elija Siguiente.
4. En el cuadro de texto Nombre de pila, escriba el nombre de la pila.

   El nombre de pila es un identificador que le ayuda a encontrar una en particular en una lista de pilas. El nombre de una pila puede contener únicamente caracteres alfanuméricos (con distinción entre mayúsculas y minúsculas) y guiones. Debe comenzar con un carácter alfabético y no puede tener más de 128 caracteres.
5. En el cuadro de DashboardNametexto, introduce el nombre que quieres asignar a tu panel de control. Introduzca otra información relevante sobre la configuración del grupo de CloudWatch acceso.

   El nombre del panel solo puede incluir caracteres alfanuméricos, el signo del guion (–) y el signo del guion bajo (_).
6. En la sección ResourcesToMonitor, introduzca el ID de directorio del directorio para el que ha activado la supervisión de Internet.
7. En la sección MonitorName, ingresa el nombre del monitor de Internet que deseas usar.
8. Elija Siguiente.
9. Revise las selecciones predeterminadas en la página Configurar opciones de pila y elija Siguiente.
10. Desplácese hasta Las transformaciones pueden requerir capacidades de acceso y marque las casillas para confirmar. A continuación, selecciona Enviar para crear la pila y el CloudWatch panel personalizado.

    > **Important**
    >
    > Es posible que haya un costo asociado a los CloudWatch paneles personalizados. Para obtener información sobre los precios, consulta Amazon CloudWatch Pricing

11. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
12. En el panel de navegación de la izquierda, elija Paneles.
13. En Paneles personalizados, seleccione el panel con el nombre que ha introducido anteriormente en este procedimiento.

14. Ahora puede WorkSpace supervisar sus datos mediante el panel de control de Internet.

Continuidad empresarial para WorkSpaces personal

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 Personal WorkSpaces
- Resiliencia multirregional para el personal WorkSpaces

Redirección entre regiones para Personal 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
- Limitaciones
- Paso 1: crear alias de conexión
- (Opcional) Paso 2: compartir un alias de conexión con otra cuenta
- Paso 3: asociar los alias de conexión a los directorios de cada región
- Paso 4: configurar el servicio de DNS y las políticas de enrutamiento de DNS
- Paso 5: envíe la cadena de conexión a sus usuarios WorkSpaces
- Diagrama de arquitectura de redireccionamiento entre regiones
- Inicio del redireccionamiento entre regiones
- Qué ocurre durante el redireccionamiento entre regiones
- Desasociar un alias de conexión de un directorio
- Dejar de compartir un alias de conexión
- Eliminar un alias de conexión
- Permisos de IAM para asociar y desasociar los alias de conexión
- Consideraciones de seguridad si deja de utilizar la redireccionamiento entre regiones

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 disponer de todos los derechos necesarios para utilizar 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 el 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.
- 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 AWS las regiones en las que Amazon WorkSpaces está disponible, excepto en la región AWS GovCloud (US) Region s y en la región China (Ningxia).

Paso 1: crear alias de conexión

Con la misma AWS cuenta, cree alias de conexión en cada región principal y de conmutación por error en la que desee configurar la redirección entre regiones.

Para crear un alias de conexión

1. Abra la consola en la versión WorkSpaces 2/home. https://console.aws.amazon.com/workspaces/
2. En la esquina superior derecha de la consola, selecciona la región principal AWS 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 tu AWS cuenta. 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 WorkSpaces región. 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 AWS cuenta 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 AWS cuenta de la misma AWS región. 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 solo se puede asociar a un directorio por AWS región. Si comparte un alias de conexión con otra AWS cuenta, solo una cuenta (su cuenta o la cuenta compartida) podrá asociar el alias a un directorio de esa región.

Para compartir un alias de conexión con otra AWS cuenta

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En la esquina superior derecha de la consola, selecciona la AWS región en la que quieres compartir el alias de conexión con otra cuenta. 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, introduce el ID de AWS cuenta con el que quieres compartir el alias de conexión en esta región. 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 asociación 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 a un solo directorio por AWS región. Si ha compartido un alias de conexión con otra AWS cuenta, solo una cuenta (su cuenta o la cuenta compartida) puede asociar el alias a un directorio de esa región.

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En la esquina superior derecha de la consola, selecciona la región principal AWS 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. 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. Elija Asociar.

7. Repita estos pasos, pero asegúrese de Step 2 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 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 la versión 2/homehttps://console.aws.amazon.com/workspaces/.

2. En la esquina superior derecha de la consola, selecciona la región principal AWS 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 otras comprobaciones 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, le recomendamos usar un subdominio, como `desktop` o`workspaces`, a menos que haya configurado el dominio únicamente para usarlo con su 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 a los que añadir ***`your_domain_name`***, selecciona 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 a los que desea añadirlo. *`your_domain_name`*

Ejemplo: Para configurar el registro de conmutación por error de su región de conmutación por error

1. En Registros de conmutación por error a los que añadir ***your_domain_name***, elija 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 a los que desea añadirlo. *your_domain_name*

Si la comprobación de estado que configuró para su región principal no es correcta, su política de enrutamiento de conmutación por error de DNS redirige a WorkSpaces los usuarios a su 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En la esquina superior derecha de la consola, selecciona la región principal AWS para tu. WorkSpaces
3. En el panel de navegación, elija WorkSpaces.
4. En la WorkSpacespágina, utiliza el cuadro de búsqueda para buscar un usuario al que quieras enviar una invitación y, a continuación, selecciona 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

En el siguiente diagrama se describe el proceso de implementación del redireccionamiento entre regiones.

> **Note**
>
> El redireccionamiento 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.

Inicio del redireccionamiento 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. Se recomienda seguir los mecanismos de recuperación ante desastres que se describen en Creating Disaster Recovery Mechanisms Using Amazon Route 53.

Qué ocurre durante el redireccionamiento entre regiones

Durante la conmutación por error de una región, WorkSpaces los usuarios se desconectan 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En la esquina superior derecha de la consola, selecciona la AWS región que contiene el alias de conexión que deseas 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. Abre la WorkSpaces consola en la versión 2/home. https://console.aws.amazon.com/workspaces/
2. En la esquina superior derecha de la consola, selecciona la AWS región que contiene el alias de conexión que quieres 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 tu cuenta. 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 la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. En la esquina superior derecha de la consola, selecciona la AWS región que contiene el alias de conexión que deseas 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`.

JSON

```
{
  "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.

JSON

```
{
  "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 Administración de identidad y acceso 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 el personal 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 de despliegues 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 recuperación ante errores 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. La resiliencia multirregional comprueba periódicamente si hay instantáneas nuevas. Si se detectan instantáneas nuevas, se inicia una copia en la región secundaria. A medida que las copias llegan a la región secundaria, se utilizan para actualizar la secundaria. WorkSpace

Contenido

- Requisitos previos
- Limitaciones
- Configure su sistema de resiliencia multirregional en espera WorkSpace
- Crea un modo de espera WorkSpace
- Administre un modo de espera WorkSpace
- Elimine una copia en espera WorkSpace
- Replicación unidireccional de datos para modo de espera WorkSpaces
- Plan para reservar la EC2 capacidad de recuperación de Amazon

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, consulteCrear un directorio para WorkSpaces Personal.
- 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 ENA NVMe, y los controladores PV de su dispositivo principal WorkSpaces. Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulte Install or upgrade Elastic Network Adapter (ENA) driver , Controladores NVMe de AWS for Windows instances y Upgrade PV drivers on Windows instances.
- Asegúrese de actualizar periódicamente los agentes EC2 Config, EC2 EC2 Launch y Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulta Update EC2 Config and EC2 Launch.
- Para garantizar una replicación de datos adecuada, asegúrese de que los directorios de Active Directory 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 de reserva 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 se realiza de forma unidireccional, copiando 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 determinado volumen de datos está llena y las instantáneas posteriores son graduales. Como resultado, la primera replicación de un determinado proceso 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 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 2, Ubuntu, Red Hat Enterprise Linux WorkSpaces, GeneralPurpose .4xlarge, GeneralPurpose .8xlarge ni con GPU WorkSpaces (p. ej., Graphics.G4dn o .g4dn). GraphicsPro GraphicsPro
- Una vez completada 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 tanto en las regiones principal como en la 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.

   Debes habilitar el redireccionamiento entre regiones en tu 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 de DNS y las políticas de enrutamiento de DNS.

   Debe configurar el servicio de DNS y configurar las políticas de enrutamiento de DNS necesarias. La redirección entre regiones funciona en conjunto con sus políticas de enrutamiento de DNS para redirigir a los usuarios según sea WorkSpaces 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 + ABC12 D) 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 el redireccionamiento entre regiones funcione, los usuarios deben utilizar el FQDN como código de registro.

Crea 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. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En la esquina superior derecha de la consola, selecciona la región principal AWS para tu. WorkSpaces
3. En el panel de navegación, elija WorkSpaces.
4. Selecciona una para la WorkSpace que quieras crear una versión en espera WorkSpace .
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) Añada la clave de cifrado, habilite el cifrado de datos y administre las etiquetas.

   - Para añadir una clave de cifrado, escríbala en Introducir clave de cifrado.
   - Para habilitar la replicación de datos, seleccione Habilitar la replicación de datos. A continuación, marque la casilla de verificación para confirmar que autoriza el 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.
   > - La actualización del estado de la replicación de datos puede tardar unos minutos.

- Una vez que el modo de espera WorkSpace se haya actualizado correctamente con las instantáneas del dispositivo principal WorkSpace, podrá encontrar las marcas horarias de las instantáneas en Instantánea de recuperación.

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. La replicación de datos está desactivada de forma predeterminada. 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 la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Ve a tu región principal y selecciona el ID principal WorkSpace .
3. Desplázate hacia abajo hasta la WorkSpace sección En espera y selecciona Editar en espera WorkSpace.
4. Seleccione Habilitar la replicación de datos. A continuación, marque la casilla de verificación para confirmar que autoriza el 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 Edition de AWS Managed Microsoft AD.
- La actualización del estado de la replicación de datos puede tardar unos minutos.
- Una vez que la WorkSpace copia en espera se haya actualizado correctamente con las instantáneas de la versión principal WorkSpace, encontrará 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. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En la esquina superior derecha de la consola, selecciona la región principal AWS para tu. WorkSpaces
3. En el panel de navegación, elija WorkSpaces.
4. Selecciona la opción en espera WorkSpace y selecciona 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 la característica de resiliencia multirregional, puede replicar datos de una región principal a una secundaria. Durante el estado estable, Multi-Region Resilience captura instantáneas del sistema (unidad C) y de los datos (unidad D) del sistema 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.

Plan para reservar la EC2 capacidad de recuperación de Amazon

Amazon Multi-Region Resilience (MRR) se basa en los pools de Amazon EC2 On-Demand de forma predeterminada. Si un tipo de EC2 instancia de Amazon específico no está disponible para respaldar

la recuperación, MRR intentará escalar automáticamente 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.

Solución de problemas de Personal 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.

   ```
   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.

   ```
   /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.

   ```
   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.

   ```
   /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 Save.

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
- Cambié el shell de mi Amazon Linux WorkSpace y ahora no puedo aprovisionar una sesión PCo IP
- Mi Amazon Linux WorkSpaces no arranca
- El inicio WorkSpaces en mi directorio conectado a menudo falla
- El lanzamiento WorkSpaces falla y se produce 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 un Windows WorkSpace con un banner de inicio de sesión interactivo
- Mis usuarios no se pueden conectar a un Windows WorkSpace
- Mis usuarios tienen problemas al intentar 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 DCV WorkSpace
- El WorkSpaces cliente muestra un error de red a mis usuarios, pero estos 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".
- Los usuarios de mi cliente PCo IP zero reciben el mensaje de error «El certificado suministrado no es válido debido a la marca de tiempo»
- Las impresoras USB y otros periféricos USB no funcionan para los clientes con IP cero PCo
- 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 en las instalaciones
- 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 compatible WorkSpaces .
- 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 «Esto no OS/platform está autorizado a acceder a su WorkSpace» cuando intentan acceder a él Windows/Linux WorkSpace mediante Web Access
- El de mi usuario WorkSpace se muestra como en mal estado después de conectarse a una AutoStop WorkSpace que está detenida
- Gnome se bloquea en los paquetes de WorkSpaces Ubuntu después de iniciar sesión

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.

Cambié el shell de mi Amazon Linux WorkSpace y ahora no puedo aprovisionar una sesión PCo IP

Para anular el shell predeterminado para Linux WorkSpaces, consulteAnular 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 IP. PCo

Si utiliza una versión no compatible del agente PCo IP, 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 producirá un error en

el aprovisionamiento de las sesiones de su Linux WorkSpaces y los usuarios finales no podrán conectarse a las suyas. WorkSpaces

Para actualizar su agente PCo IP a la versión más reciente

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija WorkSpaces.
3. Selecciona tu Linux y WorkSpace 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 sea`AVAILABLE`, 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 to`ADMIN_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 Habilite las conexiones SSH para su Linux WorkSpaces en Personal WorkSpaces .
6. Para actualizar el agente PCo IP, ejecute el siguiente comando:

   ```
   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. Desconéctese del 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 en`AVAILABLE`.

Si su Linux WorkSpace sigue sin iniciarse después de actualizar el agente PCo IP, póngase en contacto con AWS Support.

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. Puede verificar esta conectividad lanzando una EC2 instancia de Amazon en cada subred y uniendo la instancia a su directorio mediante las direcciones IP de los dos servidores DNS.

El lanzamiento WorkSpaces falla y se produce un error interno

Compruebe si las subredes están configuradas para asignar IPv6 direcciones 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, deshabilite esta configuración y especifique IPv6 las direcciones manualmente al lanzar 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 un 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 su Windows. WorkSpaces IP no admite actualmente la configuración de la política de grupo de los mensajes de inicio de sesión interactivos. PCo

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 el DCV WorkSpaces y los usuarios tienen que 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 PCo IP. Comprueba lo siguiente:

- Este mensaje aparece si el servicio PCo IP Standard Agent para Windows no se está ejecutando. 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 PCo IP, reinícielo WorkSpace a través de 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:*Domain name*\ Ordenadores de dominio

GPO ganador: permitir acceso a archivos

- Política correcta:

  Política: acceder a este equipo desde la red

  Configuración:*Domain name*\ Usuarios del 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 al intentar 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 cuando intenten iniciar sesión en su WorkSpaces Para configurar estas opciones, consulte Habilitar y configurar el acceso WorkSpaces web para WorkSpaces personal.

> **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 (DCV). 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 tu WorkSpace, espera unos minutos e inténtalo de nuevo.

Si WorkSpace ha estado ejecutándose 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 puede estar ocurriendo una de las siguientes situaciones:

- 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.
- En el control de acceso, el sistema operativo del dispositivo no está permitido como dispositivo de confianza o el dispositivo no tiene instalados los certificados adecuados cuando se utiliza la opción Dispositivos de confianza. Añada el tipo de dispositivo como dispositivo de confianza de la siguiente manera:

  1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/v2/home.
  2. En el panel de navegación, elija Directories (Directorios).
  3. Seleccione el directorio que esté utilizando.

4. Desplácese hasta Opciones de control de acceso y seleccione Editar.
5. En Dispositivos de confianza, seleccione Permitir todo en el menú desplegable para los tipos de dispositivos a los que desee permitir el acceso. Si desea restringir los dispositivos a los que tengan certificados de cliente instalados, seleccione Dispositivos de confianza.
6. Si ha elegido Dispositivos de confianza en el paso anterior, asegúrese de haber importado al menos un certificado raíz y de que el certificado de cliente emitido por la autoridad raíz de certificados (CA) se haya instalado en el cliente. Para obtener más información sobre la creación, la implementación y la importación de certificados raíz, consulte Restrinja el acceso a dispositivos de confianza para WorkSpaces uso personal.
7. Seleccione Save.

- No se permite el acceso a tus tipos de dispositivos. WorkSpaces Conceda acceso al tipo de dispositivo de la siguiente manera:

  1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
  2. En el panel de navegación, elija Directories (Directorios).
  3. Seleccione el directorio que esté utilizando.
  4. Desplácese hasta Otras plataformas y seleccione Editar.
  5. Selecciona uno de los siguientes tipos de dispositivos a los que deseas conceder WorkSpaces acceso.
     - ChromeOS
     - iOS
     - Linux
     - Acceso web
     - Clientes cero
  6. Seleccione Save.

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 DCV 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 DCV, el puerto utilizado para transmitir la sesión del cliente se cambió del 4172 al 4195.

El WorkSpaces cliente muestra un error de red a mis usuarios, pero estos 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 se considera una CA raíz de confianza en los sistemas operativos admitidos por 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

- PCoClientes con IP cero: 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
- PCoClientes con IP cero
- Otras aplicaciones cliente

Aplicación cliente para Windows

Utilice una de las siguientes soluciones para errores de certificado.

Solución 1: actualizar la aplicación cliente

Descargue e instale la última aplicación cliente de Windows desde https://clients.amazonworkspaces.com/. 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 WorkSpaces cliente y reiníciela.

Solución 3: implementar Amazon Trust Services como CA de confianza mediante la directiva de grupo

Agregue el certificado Starfield a la raíz CAs de confianza del dominio mediante la política de grupo. Para obtener más información, consulte Use Policy to Distribute Certificates.

PCoClientes con IP cero

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 se puede conectar 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. Por lo general, 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.

Los usuarios de mi cliente PCo IP zero reciben el mensaje de error «El certificado suministrado no es válido debido a la marca de tiempo»

Si el Protocolo de tiempo de red (NTP) no está habilitado en Teradici, es posible que los usuarios de su cliente PCo IP cero reciban errores en los certificados. Para configurar el NTP, consulte Configurar clientes PCo IP cero para WorkSpaces Personal.

Las impresoras USB y otros periféricos USB no funcionan para los clientes con IP cero PCo

A partir de la versión 20.10.4 del agente PCo IP, 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 cliente de PCo IP cero para conectarse a sus dispositivos. WorkSpaces

WorkSpaces Si utiliza la versión 20.10.4 o posterior del agente PCo IP, los dispositivos periféricos USB no funcionarán con los dispositivos cliente de PCo IP cero 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 la redirección USB en los dispositivos cliente con IP PCo cero

Le recomendamos que introduzca estos cambios en el registro a WorkSpaces través de la política de grupo. 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\ IP\ pcoip_admin PCo

   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\ IP\ pcoip_admin_defaults PCo

   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 SkipThisVersionregistro 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. Dado que 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 Chromebook for Personal WorkSpaces .

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 personal.

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 personal.

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, aplica esta configuración a un objeto de política de grupo que esté vinculado a la unidad WorkSpaces organizativa (OU) desde una instancia unida a un dominio EC2 . 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. Compruebe que la plantilla administrativa de políticas de grupo de WorkSpaces más reciente está 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 para WorkSpaces personal.

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

Le recomendamos que no modifique 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 en las instalaciones

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 en las instalaciones 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 Registros de recursos de SRV 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. Desde el WorkSpace Panel de control y, a continuación, 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 PCo IP WorkSpace configurada 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 dispositivos configurados para WorkSpaces DCV. Solo se aplican a los WorkSpaces que están configurados para PCo IP.
> - 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, vuelve a cambiar 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 (ENIs) 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 capacidad para una llamada más en el segundo 6, ya

Segundo	Número de solicitudes enviadas	Número neto de solicitudes permitidas	Detalles
			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 restringidas en la cola, el límite de la tasa continúa aumentando 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 de NameID del sujeto SAML debe coincidir con WorkSpaces el nombre de usuario y, por lo general, es el mismo que el atributo AMAccount s Name 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 Windows WorkSpaces en paquetes DCV 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 se haya publicado.
- Hay un certificado en la memoria caché, pero los atributos del usuario que invalidó el certificado han cambiado. Póngase en contacto con nosotros Soporte para borrar la memoria caché antes de que caduque el certificado (24 horas). Para obtener más información, consulte el Centro de Soporte.
- 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 algún elemento obsoleto CAs en el dominio o el bosque, ejecute `PKIVIEW.msc` la CA para verificarlo. Si están obsoletos CAs, utilice el `PKIVIEW.msc` mmc para eliminarlos manualmente.
- Para comprobar que la replicación de Active Directory funcione y que no haya 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 Soporte. Para obtener más información, consulte el Centro de Soporte.

Estoy intentando hacer algo que requiere un medio de instalación de Windows, pero WorkSpaces no lo proporciona.

Si utilizas un paquete público AWS proporcionado, puedes usar las instantáneas de EBS de los medios de instalación del sistema operativo Windows Server que Amazon EC2 te proporciona cuando las necesites.

Cree un volumen de EBS a partir de estas instantáneas, adjúntelo a Amazon EC2 y transfiera los archivos a WorkSpace donde estén los archivos 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 EC2 instancia de Amazon y copiar los archivos.

Quiero lanzarlo WorkSpaces con un directorio AWS gestionado existente creado en una región no compatible WorkSpaces .

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, consulta Crear con la misma cuenta y VPCs en distintas 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 sus tablas de enrutamiento para activar la comunicación con la VPC homóloga a través IPv4 de 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. En el AWS caso de las aplicaciones y los servicios, elige Amazon WorkSpaces para activar WorkSpaces el acceso 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 de dispositivo 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 los repositorios de forma lateral 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 estás utilizando WorkSpace el repositorio Extra de Firefox, ejecuta 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 entre mayúsculas y minúsculas y debe tener un mínimo de 8 caracteres y un máximo de 64. Deben incluir, como mínimo, 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 no imprimibles, como espacios en blanco, tabulaciones de retorno de carro, saltos de línea y caracteres nulos.

Si su organización requiere que aplique el FFGP WorkSpaces, póngase en contacto con el administrador de Active Directory para restablecer la contraseña de su usuario directamente desde Active Directory en lugar de hacerlo desde el WorkSpaces cliente.

Mis usuarios reciben el mensaje de error «Esto no OS/platform está autorizado a acceder a su WorkSpace» cuando intentan acceder a él Windows/Linux WorkSpace 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, consulte[Habilitar y configurar el acceso WorkSpaces web para WorkSpaces personal](#).

El de mi usuario WorkSpace se muestra como en mal estado después de conectarse a una AutoStop WorkSpace que está detenida

Es posible que su usuario esté utilizando un software que se sabe que causa problemas en las interfaces de red al reanudar la hibernación. Por ejemplo, si WorkSpace tiene instalada la aplicación NPCAP 1.1, actualícela a la versión 1.2 o superior para resolver este problema.

Gnome se bloquea en los paquetes de WorkSpaces Ubuntu después de iniciar sesión

Si WorkSpace se lanza a con el `ubuntu` nombre de usuario, habrá conflictos con el `ubuntu` usuario que existe por defecto. Esto provocará bloqueos en Gnome y, posiblemente, otros efectos negativos en el rendimiento. Para evitar este problema, no especifiques el `ubuntu` nombre de usuario al aprovisionar Ubuntu. WorkSpaces

Versiones del agente anfitrión de DCV en Personal WorkSpaces

El agente anfitrión de DCV es un agente de alojamiento que se ejecuta dentro de su. WorkSpace Transmite sus píxeles WorkSpace a una aplicación cliente e incluye funciones integradas en la sesión, como audio y vídeo bidireccionales, e impresión. Para obtener más información sobre DCV, 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 DCV. El agente anfitrión del DCV 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 en cada versión del agente anfitrión de DCV para WorkSpaces Personal.

Release	Date	Cambios
• Windows WorkSpaces : 2.1.0.2000	7 de julio de 2025	• Soporte de WebAuth redirecci onamiento mejorado para aplicacio nes nativas. • Correcciones de errores y mejoras de rendimiento.
• Ubuntu WorkSpaces : 2.1.0.1923	1 de mayo de 2025	• Correcciones de errores y mejoras de rendimiento.
• Rocky Linux WorkSpaces : 2.1.0.1843 • Red Hat Enterprise Linux - 2.1.0.1843 WorkSpaces	10 de abril de 2025	• Correcciones de errores y mejoras de rendimiento.
• Windows: 2.1.0.1840 WorkSpaces	19 de marzo de 2025	• Se solucionó un problema por el que se mostraba la lista de impresoras aunque el GPO

Release	Date	Cambios
		de redirección de impresoras estuviera deshabilitado. • Correcciones de errores y mejoras de rendimiento.
• Windows WorkSpaces : 2.1.0.1792	19 de noviembre de 2024	Correcciones de errores y mejoras de rendimiento.
• Windows: 2.1.0.1786 WorkSpaces	31 de octubre de 2024	• Se cambió el nombre del WorkSpaces Streaming Protocol (WSP) a Amazon DCV. • Se ha corregido un problema de atenuación del audio en el agente DCV para los clientes que utilizaban la aplicación Avaya. • Se corrigieron los problemas de inicio de SmartCard sesión que se producían cuando el usuario estaba inactivo en la página de solicitud del PIN. • Se ha corregido un problema de WebAuthn redireccionamiento durante el primer intento de inicio de sesión en el navegador Chrome. • Correcciones de errores y mejoras de rendimiento.
• Windows WorkSpaces : 2.1.0.1757	19 de agosto de 2024	• Se añadido compatibilidad con la integración de IAM Identity Center (IdC). • Correcciones de errores y mejoras de rendimiento.

Release	Date	Cambios
• Windows: 2.1.0.1696 WorkSpaces	29 de julio de 2024	• Se ha añadido compatibilidad con los hosts de Windows Graphics. • Se ha añadido compatibilidad con el redireccionamiento de WebRTC para Amazon Connect. • Se ha solucionado un problema que podía impedir que el servicio se ejecutara al iniciar el sistema. • Correcciones de errores y mejoras de rendimiento.
• Windows: 2.1.0.1554 WorkSpaces	15 de mayo de 2024	• Se ha añadido compatibilidad con el tiempo de espera de desconexión por inactividad. • Se ha añadido una nueva configuración de política de grupo para configurar el tiempo de espera de desconexión por inactividad. • Se ha corregido un error que provocaba WorkSpaces que se desconectara y se mostrara una pantalla blanca cuando los usuarios modificaban la configuración de pantalla. • Correcciones de errores y mejoras de rendimiento.
• Ubuntu WorkSpaces : 2.1.0.1342	29 de febrero de 2024	• Se ha cambiado la resolución preferida de la cámara web entre 480 x 360 y 640 x 480. • Correcciones de errores y mejoras de rendimiento.

Release	Date	Cambios
• Windows: 2.0.0.1425 WorkSpaces	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 solucionado un problema que provocaba que a veces apareciera la pantalla en blanco o se bloqueara al iniciar sesión. • Correcciones de errores y mejoras de rendimiento.
• Windows WorkSpaces : 2.0.0.1304	11 de enero de 2024	• Se ha solucionado un error relacionado con posibles bloqueos de transmisión durante el inicio de sesión. • Se ha solucionado un error relacionado con el registro.

Release	Date	Cambios
• Windows WorkSpaces : 2.0.0.1288	16 de noviembre de 2023	• Se ha añadido 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 ha añadido una nueva configuración de política de grupo para habilitar o deshabilitar el controlador de IDD. • Se han solucionado errores relacionados con la transparencia de las imágenes del portapapeles. • Se han solucionado errores que preservaban los factores de escala de Windows. • Correcciones de errores y mejoras de rendimiento.
• Windows WorkSpaces : 2.0.0.1164	13 de octubre de 2023	• Se agregó soporte para el controlador VSync de pantalla virtual. • Se agregó una nueva configura ción 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.

Release	Date	Cambios
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces : 2.1.0.1086	18 de agosto de 2023	• Se agregó una nueva configura ción 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.
• 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 comportam iento 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.

Release	Date	Cambios
• 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 relaciona dos con la A/V sincronización y los teclados japoneses. • Se ha mejorado la fiabilidad del instalador de DCV.
• Ubuntu WorkSpaces - 2.1.0.829	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 optimizac iones 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 configura ciones 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 más información sobre cómo comprobar la versión del agente de host, consulte What client and host operating systems are supported by the latest version of DCV?
- Para obtener información sobre cómo actualizar la versión del agente anfitrión, consulte Si ya tengo un DCV WorkSpace, ¿cómo lo actualizo? .
- Para ver las notas de la versión de cliente DCV para macOS, consulte las notas de la versión en la sección de aplicaciones cliente de WorkSpaces macOS de la Guía del WorkSpaces usuario.

- Para ver las notas de lanzamiento de la versión cliente DCV para Windows, consulte las notas de la versión en la sección de aplicaciones cliente para WorkSpaces Windows de la Guía del WorkSpaces usuario.

Use y administre WorkSpaces grupos

WorkSpaces Pools ofrece escritorios virtuales no persistentes, diseñados para los usuarios que necesitan acceder a entornos de escritorio altamente seleccionados alojados en una infraestructura efímera.

Temas

- Regiones de AWS y zonas de disponibilidad para WorkSpaces piscinas
- Administrar directorios para WorkSpaces grupos
- Redes y acceso para WorkSpaces piscinas
- Crear una WorkSpaces piscina
- Administrar WorkSpaces grupos
- Uso de Active Directory con WorkSpaces grupos
- Paquetes e imágenes para piscinas WorkSpaces
- Monitorización de WorkSpaces grupos
- Habilitar y administrar el almacenamiento persistente para WorkSpaces grupos
- Habilite la persistencia de la configuración de la aplicación para los usuarios de sus WorkSpaces grupos
- WorkSpaces Códigos de notificación de solución de problemas de piscinas

Regiones de AWS y zonas de disponibilidad para WorkSpaces piscinas

WorkSpaces Las piscinas están disponibles en las siguientes Regiones de AWS ubicaciones.

> **Note**
>
> Para conocer los datos Regiones de AWS que se aplican a WorkSpaces Personal, consulta los WorkSpaces puntos de conexión y las cuotas de Amazon en la guía de Referencia general de AWS referencia.

Nombre de la región	Región	Punto de conexión	Protocolo	Zonas de disponibilidad
Este de EE. UU. (Norte de Virginia)	us-east-1	workspaces.us-east-1.amazonaws.com workspaces-fips.us-east-1.amazonaws.com	HTTPS HTTPS	use1-az2, use1-az4, use1-az6
Oeste de EE. UU. (Oregón)	us-west-2	workspaces.us-west-2.amazonaws.com workspaces-fips.us-west-2.amazonaws.com	HTTPS HTTPS	usw2-az1, usw2-az2, usw2-az3
Asia-Pacífico (Bombay)	ap-south-1	workspaces.ap-south-1.amazonaws.com	HTTPS	aps1-az1, aps1-az3
Asia-Pacífico (Seúl)	ap-northeast-2	workspaces.ap-northeast-2.amazonaws.com	HTTPS	apne2-az1, apne2-az3
Asia-Pacífico (Singapur)	ap-southeast-1	workspaces.ap-southeast-1.amazonaws.com	HTTPS	apse1-az1, apse1-az2
Asia-Pacífico (Sídney)	ap-southeast-2	workspaces.ap-southeast-2.amazonaws.com	HTTPS	apse2-az1,

Nombre de la región	Región	Punto de conexión	Protocolo	Zonas de disponibilidad
				apse2-az3
Asia-Pacífico (Tokio)	ap-northeast-1	workspaces.ap-northeast-1.amazonaws.com	HTTPS	apne1-az1, apne1-az4
Canadá (centro)	ca-central-1	workspaces.ca-central-1.amazonaws.com	HTTPS	cac1-az1, cac1-az2
Europa (Fráncfort)	eu-central-1	workspaces.eu-central-1.amazonaws.com	HTTPS	euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	workspaces.eu-west-1.amazonaws.com	HTTPS	euw1-az1, euw1-az2, euw1-az3
Europa (Londres)	eu-west-2	workspaces.eu-west-2.amazonaws.com	HTTPS	euw2-az2, euw2-az3

Nombre de la región	Región	Punto de conexión	Protocolo	Zonas de disponibilidad
Europa (París)	eu-west-3	workspaces.eu-west-3.amazonaws.com	HTTPS	euw3-az1, euw3-az2, euw3-az3
América del Sur (São Paulo)	sa-east-1	workspaces.sa-east-1.amazonaws.com	HTTPS	sae1-az1, sae1-az3
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	workspaces.us-gov-east-1.amazonaws.com workspaces-fips.us-gov-east-1.amazonaws.com	HTTPS HTTPS	usgw1-az1, usgw1-az2, usgw1-az3
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	workspaces.us-gov-west-1.amazonaws.com workspaces-fips.us-gov-west-1.amazonaws.com	HTTPS HTTPS	usge1-az1, usge1-az2, usge1-az3

Administrar directorios para WorkSpaces grupos

WorkSpaces Pools utiliza un directorio para almacenar y administrar su información WorkSpaces y la de sus usuarios. En esta sección, le mostramos cómo crear y administrar directorios para WorkSpaces grupos.

Contenido

- Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos
- Actualice los detalles del directorio de sus WorkSpaces piscinas
- Anular el registro de un directorio de grupos WorkSpaces

Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos

Puede habilitar el registro de las aplicaciones WorkSpaces cliente y el inicio de sesión WorkSpaces en un WorkSpaces grupo configurando la federación de identidades mediante SAML 2.0. Para ello, utilice un rol de AWS Identity and Access Management (IAM) y una URL de estado de retransmisión para configurar el proveedor de identidades (IdP) de SAML 2.0 y habilitarlo para AWS. De este modo, los usuarios federados tienen acceso a un directorio de grupos WorkSpace . El estado de retransmisión es el punto final del WorkSpaces directorio al que se redirige a los usuarios después de iniciar AWS sesión correctamente.

> **Important**
>
> WorkSpaces Pools no admite configuraciones de SAML 2.0 basadas en IP.

Temas

- Paso 1: tener en cuenta los requisitos
- Paso 2: Completar los requisitos previos
- Paso 3: crear un proveedor de identidades de SAML en IAM
- Paso 4: Crear un directorio de WorkSpace grupos
- Paso 5: crear un rol de IAM de federación de SAML 2.0
- Paso 6: configurar el proveedor de identidades de SAML 2.0
- Paso 7: crear aserciones para la respuesta de autenticación de SAML
- Paso 8: configurar el estado de retransmisión de la federación
- Paso 9: Habilita la integración con SAML 2.0 en el directorio de tu grupo WorkSpace
- Solución de problemas
- Especifique los detalles de Active Directory para el directorio de WorkSpaces grupos

Paso 1: tener en cuenta los requisitos

Al configurar SAML para un directorio de grupos, se aplican los siguientes requisitos. WorkSpaces

- El rol workspaces_ DefaultRole IAM debe existir en su cuenta. AWS Este rol se crea automáticamente cuando se utiliza la configuración WorkSpaces rápida o si anteriormente se ha iniciado uno con la. WorkSpace AWS Management Console Concede WorkSpaces permiso a Amazon para acceder a AWS recursos específicos en tu nombre. Si el rol ya existe, es posible que tengas que adjuntarle la política AmazonWorkSpacesPoolServiceAccess gestionada, que Amazon WorkSpaces utiliza para acceder a los recursos necesarios en la AWS cuenta de WorkSpaces Pools. Para obtener más información, consulte Cree el rol workspaces_ DefaultRole y AWS política gestionada: AmazonWorkSpacesPoolServiceAccess.
- Puedes configurar la autenticación SAML 2.0 para los WorkSpaces grupos Regiones de AWS que admiten la función. Para obtener más información, consulte Regiones de AWS y zonas de disponibilidad para WorkSpaces piscinas.
- 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 que lo admiten 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 solo se admite en los siguientes clientes. WorkSpaces Para ver los WorkSpaces clientes más recientes, consulta la página de descargas de Amazon WorkSpaces Client.
  - Aplicación cliente de Windows (versión 5.20.0 o posterior)
  - Cliente de macOS (versión 5.20.0 o posterior)
  - Acceso web

Paso 2: Completar los requisitos previos

Complete los siguientes requisitos previos antes de configurar su conexión de IdP de SAML 2.0 a un directorio de grupos. WorkSpaces

- Configure el IdP para establecer una relación de confianza con AWS.
- Consulte Integración de proveedores de soluciones SAML de terceros AWS para obtener más información sobre la configuración de la federación. AWS Como ejemplo pertinente se incluye la integración de IdP con IAM para obtener acceso a la AWS Management Console.

- 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.
- Cree un WorkSpaces directorio de grupos mediante la WorkSpaces consola. Para obtener más información, consulte Uso de Active Directory con WorkSpaces grupos.
- Cree un WorkSpaces grupo para los usuarios que puedan iniciar sesión en el IdP mediante un tipo de directorio compatible. Para obtener más información, consulte Crear una WorkSpaces piscina.

Paso 3: crear un proveedor de identidades de SAML en IAM

Para comenzar, debe crear un proveedor de identidades (IdP) de SAML en IAM. 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 en la Guía del usuario de AWS Identity and Access Management . Para obtener información sobre cómo trabajar con SAML IdPs en AWS GovCloud (US) Regions, consulte AWS Identity and Access Managementla Guía del usuario.AWS GovCloud (US)

Paso 4: Crear un directorio de WorkSpace grupos

Complete el siguiente procedimiento para crear un directorio WorkSpaces de grupos.

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Elija Directorios en el panel de navegación.
3. Elija Create directory.
4. Como WorkSpace tipo, selecciona Pool.
5. En la sección Origen de identidad de usuario de la página:
   a. Introduzca un valor de marcador de posición en el cuadro de texto URL de acceso de usuario. Por ejemplo, introduzca `placeholder` en el cuadro de texto. Lo editará más adelante, después de configurar los derechos de la aplicación en el IdP.
   b. Deje en blanco el cuadro de texto Nombre del parámetro del estado de retransmisión. Lo editará más adelante, después de configurar los derechos de la aplicación en el IdP.
6. En la sección Información del directorio de la página, introduzca un nombre y una descripción para el directorio. El nombre y la descripción del directorio deben tener menos de 128 caracteres

y pueden incluir caracteres alfanuméricos y los siguientes caracteres especiales: `_ @ # % * + = : ? . / ! \ -`. El nombre y la descripción del directorio no pueden empezar por un carácter especial.

7. En la sección Redes y seguridad de la página:

   a. Elija una VPC y dos subredes con acceso a los recursos de red que necesite la aplicación. Para lograr una mayor tolerancia a errores, debe elegir dos subredes en diferentes zonas de disponibilidad.

   b. Elija un grupo de seguridad que permita WorkSpaces crear enlaces de red en su VPC. Los grupos de seguridad controlan el tráfico de red desde el que se permite que fluya hacia WorkSpaces la VPC. Por ejemplo, si tu grupo de seguridad restringe todas las conexiones HTTPS entrantes, los usuarios que accedan a tu portal web no podrán cargar sitios web HTTPS desde el. WorkSpaces

8. La sección Configuración de Active Directory es opcional. Sin embargo, si planea usar un AD con sus WorkSpaces grupos, debe especificar los detalles de Active Directory (AD) durante la creación del directorio WorkSpaces de grupos. No puede editar la configuración de Active Directory para el directorio de WorkSpaces grupos después de crearla. Para obtener más información sobre cómo especificar los detalles de AD para el WorkSpaces directorio de grupos, consulteEspecifique los detalles de Active Directory para el directorio de WorkSpaces grupos. Tras completar el proceso descrito en ese tema, debería volver a él para terminar de crear el directorio de WorkSpaces grupos.

   Puede omitir la sección Config de Active Directory si no planea usar un AD con sus WorkSpaces grupos.

9. En la sección Propiedades de transmisión de la página:

   - Elija el comportamiento de los permisos del portapapeles e introduzca una copia en el límite de caracteres local (opcional) y péguela en el límite de caracteres de la sesión remota (opcional).
   - Elija si desea permitir o no la impresión en el dispositivo local.
   - Elija si desea permitir o no el registro de diagnósticos.
   - Elija si desea permitir o no el inicio de sesión con tarjeta inteligente. Esta característica solo se aplica si ha habilitado la configuración de AD anteriormente en este procedimiento.

10. En la sección Almacenamiento de la página, puede optar por habilitar las carpetas de inicio.

11. En la sección Rol de IAM de la página, seleccione un rol de IAM para que esté disponible para todas las instancias de transmisión de escritorio. Para crear uno nuevo, elija Crear un nuevo rol de IAM.

    Cuando aplicas una función de IAM desde tu cuenta a un directorio de WorkSpace grupos, puedes realizar solicitudes de AWS API desde un WorkSpace directorio del WorkSpace grupo sin tener que administrar AWS las credenciales manualmente. Para obtener más información, consulte Crear un rol para delegar permisos a un usuario de IAM en la Guía del usuario de AWS Identity and Access Management .
12. Elija Create directory.

Paso 5: crear un rol de IAM de federación de SAML 2.0

Complete el procedimiento que se indica a continuación para crear un rol de IAM de federación de SAML 2.0 en la consola de IAM.

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Seleccione Crear rol.
4. Seleccione Federación SAML 2.0 para el tipo de entidad de confianza.
5. En el proveedor basado en SAML 2.0, elija el proveedor de identidades que ha creado en IAM. Para obtener más información, consulte Crear un proveedor de identidades de SAML en IAM.
6. Seleccione Permitir solo acceso mediante programación para permitir el acceso.
7. Elija SAML:sub_type para el atributo.
8. En Valor, introduzca `https://signin.aws.amazon.com/saml`. Este valor restringe el acceso del rol a solicitudes de transmisión de usuario de SAML que incluyan una aserción de tipo de sujeto de SAML con un valor de `persistent`. Si SAML:sub_type es persistente, el IdP envía el mismo valor único para el elemento `NameID` en todas las solicitudes de SAML desde un usuario particular. Para obtener más información, consulte Identificación única de los usuarios en la federación basada en SAML en la Guía del usuario de AWS Identity and Access Management .
9. Elija Siguiente para continuar.
10. No realice cambios ni selecciones en la página Añadir permisos. Elija Siguiente para continuar.
11. Introduzca un nombre y la descripción para el rol.
12. Seleccione Crear rol.

13. En la página Roles, seleccione el rol que acaba de crear.
14. Seleccione la pestaña Relaciones de confianza.
15. Elija Editar la política de confianza.
16. En el cuadro de texto JSON Editar política de confianza, añade la TagSession acción sts: a la política de confianza. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de AWS Identity and Access Management .

    El resultado debe ser similar al siguiente ejemplo:

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": {
7                  "Federated": "arn:aws:iam::[redacted]:saml-provider/[redacted]"
8              },
9              "Action": [
10                 "sts:AssumeRoleWithSAML",
11                 "sts:TagSession"
12             ],
13             "Condition": {
14                 "StringEquals": {
15                     "SAML:sub_type": "persistent"
16                 }
17             }
18         }
19     ]
20 }
```

17. Elija Actualizar política.
18. Elija la pestaña Permisos.
19. En la sección Políticas de permisos de la página, elija Añadir permisos y luego Crear política insertada.
20. En la sección Editor de políticas de la página, seleccione JSON.
21. En el cuadro de texto JSON Editor de políticas, escriba la política siguiente. Asegúrese de reemplazar:

    - *<region-code>*con el código de la AWS región en la que creó el directorio de su WorkSpace grupo.
    - *<account-id>*con el ID AWS de la cuenta.
    - *<directory-id>*con el ID del directorio que creó anteriormente. Puede obtenerlo en la WorkSpaces consola.

Para los recursos en AWS GovCloud (US) Regions, utilice el siguiente formato para el ARN:. `arn:aws-us-gov:workspaces:<region-code>:<account-id>:directory/<directory-id>`

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:<US East (N. Virginia)>:<account-
id>:directory/<directory-id>",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

22. Elija Siguiente.
23. Escriba un nombre para la política y elija Create policy (Crear política).

Paso 6: configurar el proveedor de identidades de SAML 2.0

En función del IdP de SAML 2.0, es posible que tenga que actualizarlo manualmente para que confíe en AWS como proveedor de servicios. Para ello, descargue el `saml-metadata.xml` archivo que se encuentra en https://signin.aws.amazon.com/static/saml-metadata.xml y, a continuación, cárguelo en su IdP. Esto actualiza los metadatos del IdP.

Para algunos IdPs, es posible que la actualización ya esté configurada. Puede omitir este paso si ya se ha configurado. Si la actualización aún no está configurada en el IdP, revise la documentación facilitada por este para obtener más información sobre cómo actualizar los metadatos. Algunos proveedores ofrecen la opción de escribir la URL del archivo XML en su panel, y el IdP obtiene

e instala el archivo automáticamente. Otros requieren que descargue el archivo de la URL y, a continuación, lo cargue en su panel.

> **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 7: crear aserciones para la respuesta de autenticación de SAML

Configure la información que su IdP envía AWS como atributos de SAML en su respuesta de autenticación. En función del IdP, es posible que ya se haya configurado. Puede omitir este paso si ya se ha configurado. Si no se ha configurado, indique lo siguiente:

- NameID del sujeto de SAML: el identificador único del usuario que está iniciando sesión. No cambies la format/value parte de este campo. De lo contrario, la característica de carpeta de inicio no funcionará según lo previsto porque se tratará al usuario como un usuario diferente.

  > **Note**
  >
  > En el caso de los WorkSpaces grupos unidos a un dominio, el `NameID` valor para el usuario debe proporcionarse en el `domain\username` formato que utilice el`sAMAccountName`, o en el `username@domain.com` formato que utilice`userPrincipalName`, o simplemente. `userName` Si utiliza el formato `sAMAccountName`, puede especificar el dominio con el nombre de NetBIOS o con el nombre completo del dominio (FQDN). El formato `sAMAccountName` es obligatorio para situaciones de confianza unidireccional de Active Directory. Para obtener más información, consulte Uso de Active Directory con WorkSpaces grupos. Si solo se ha proporcionado `userName`, el usuario iniciará sesión en el dominio principal.

- Tipo de sujeto de SAML (con un valor establecido en **`persistent`**): al establecer el valor en `persistent`, se garantiza que el IdP envíe el mismo valor único para el elemento `NameID` en

todas las solicitudes de SAML de un usuario particular. Asegúrese de que la política de IAM incluya una condición para permitir solo las solicitudes de SAML con un `sub_type` de SAML configurado como `persistent`, tal y como se describe en la sección Paso 5: crear un rol de IAM de federación de SAML 2.0.

- **`Attribute`**elemento con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/Attributes/Role: este elemento contiene uno o más **`AttributeValue`** elementos que enumeran el rol de IAM y el IdP de SAML a los que su IdP asigna al usuario. El rol y el IdP se especifican como un par delimitado por comas de. ARNs Un ejemplo del valor esperado es `arn:aws:iam::<account-id>:role/<role-name>,arn:aws:iam::<account-id>:saml-provider/<provider-name>`.
- **`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 incluir caracteres alfanuméricos y los siguientes caracteres especiales: `_ . : / = + - @`. 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.
- **`Attribute`**elemento con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/Attributes/:EmailPrincipalTag: 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 directorio. WorkSpaces Los valores de las etiquetas pueden incluir combinaciones de letras, números, espacios y caracteres `_ . : / = + - @`. Para obtener más información, consulte Reglas para etiquetar en IAM y AWS STS en la Guía del usuario de AWS Identity and Access Management .
- **`Attribute`**Elemento (opcional) con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/ Attributes/PrincipalTag: UserPrincipalName — Este elemento contiene un `AttributeValue` elemento que proporciona Active Directory al `userPrincipalName` usuario que inicia sesión. El valor debe proporcionarse en el formato `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 y personal WorkSpaces .
- **`Attribute`**Elemento (opcional) con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/ Attributes/PrincipalTag: ObjectSid (opcional): este elemento contiene un `AttributeValue` elemento que proporciona el identificador de seguridad (SID) de Active Directory para el 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 y personal WorkSpaces .

- **`Attribute`**Elemento (opcional) con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/ Attributes/:DomainPrincipalTag: 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 el formato `domain.com` y debe incluir los subdominios.
- **`Attribute`**Elemento (opcional) con el **`Name`** atributo establecido en https://aws.amazon.com/SAML/ Attributes/ SessionDuration: 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 el SAML en la Guía del usuario. SessionDurationAttributeAWS Identity and Access Management

> **Note**
>
> Aunque `SessionDuration` es un atributo opcional, se recomienda incluirlo en la respuesta de SAML. Si no especifica 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 sobre cómo configurar estos elementos, consulte Configure aserciones SAML para la respuesta de autenticación en la Guía del usuario de AWS Identity and Access Management . Para obtener información sobre los requisitos de configuración específicos de su IdP, consulte la documentación de su IdP.

Paso 8: configurar el estado de retransmisión de la federación

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

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

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

En la siguiente tabla, se enumeran los puntos finales del estado de retransmisión de AWS las regiones en las que está disponible la autenticación WorkSpaces SAML 2.0. AWS Se han eliminado las regiones en las que la función de WorkSpaces grupos no está disponible.

Región	Punto de conexión del estado de retransmisión
Región Este de EE. UU. (Norte de Virginia)	• workspaces.euc-sso.us-east-1.aws.amazon.com • espacios de trabajo (FIPS). 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 • espacios de trabajo (FIPS). euc-sso-fips.us-west-2.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
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	Punto de conexión del estado de retransmisión
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
AWS GovCloud (EE. UU.-Oeste)	• workspaces.euc-sso. us-gov-west-1. amazonaws-us-gov.com • espacios de trabajo (FIPS). euc-sso-fips. us-gov-west-1. amazonaws-us-gov.com **Note** Para obtener información sobre cómo trabajar con SAML IdPs en AWS GovCloud (US) Regions, consulta la Guía del usuario de Amazon WorkSpacesAWS 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 • espacios de trabajo (FIPS). euc-sso-fips. us-gov-east-1. amazonaws-us-gov.com **Note** Para obtener información sobre cómo trabajar con SAML IdPs en AWS GovCloud (US) Regions, consulta la Guía del usuario de Amazon WorkspacesAWS GovCloud (EE. UU.).

Paso 9: Habilita la integración con SAML 2.0 en el directorio de tu grupo WorkSpace

Complete el siguiente procedimiento para habilitar la autenticación SAML 2.0 en el directorio del WorkSpaces pool.

1. Abra la WorkSpaces consola en la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. Elija Directorios en el panel de navegación.
3. Seleccione la pestaña Directorios de grupos.
4. Elija el ID del directorio que desea editar.
5. Elija Editar en la sección Autenticación de la página.
6. Seleccione Editar proveedor de identidad de SAML 2.0.
7. En la opción URL de acceso del usuario, que a veces se denomina URL de SSO, sustituya el valor del marcador de posición por la URL de SSO que le proporcionó el IdP.
8. En la opción Nombre del parámetro de enlace profundo del IdP, introduzca el parámetro aplicable al IdP y a la aplicación que ha configurado. El valor predeterminado es `RelayState` si omite el nombre del parámetro.

En la siguiente tabla se enumeran los nombres de los parámetros de acceso de usuario URLs y de enlace directo que son exclusivos de los distintos proveedores de identidad para las aplicaciones.

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>`

Proveedor de identidades	Parámetro	URL de acceso del usuario
Auth0	`RelayState`	`https://<default-tenant-name> .us.auth0.com/samlp/ <client-id>`
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId= <sp-id>`
PingOne para empresas	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid= <app-id>&idpid=<idp-id>`

9. Seleccione Save.

> **Important**
>
> La revocación de SAML 2.0 de un usuario no desconectará directamente su sesión. Solo se eliminarán cuando se agote el tiempo de espera. También pueden finalizarlo mediante la TerminateWorkspacesPoolSessionAPI.

Solución de problemas

La siguiente información puede ayudarle a solucionar problemas específicos con sus WorkSpaces grupos.

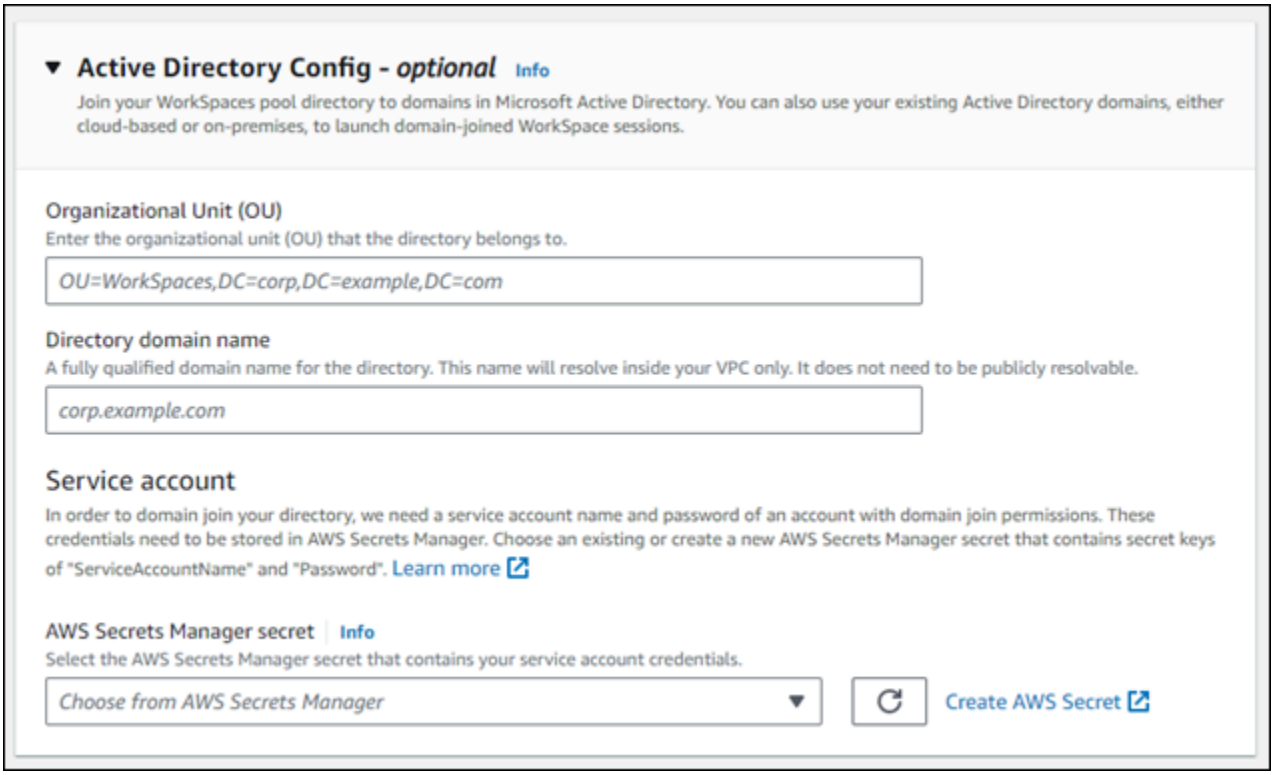
Recibo un mensaje que indica que no es posible iniciar sesión en el cliente de WorkSpaces Pools tras completar la autenticación SAML

Las notificaciones `nameID` y `PrincipalTag:Email` las de SAML deben coincidir con el nombre de usuario y el correo electrónico configurados en Active Directory. Es posible que algunos IdP necesiten actualizarse, refrescarse o volver a implementarse después de ajustar determinados atributos. Si realizas un ajuste y no se refleja en la captura de SAML, consulta la documentación o

el programa de soporte de tu IdP para conocer los pasos específicos necesarios para que el cambio surta efecto.

Especifique los detalles de Active Directory para el directorio de WorkSpaces grupos

En este tema, le mostramos cómo especificar los detalles de Active Directory (AD) en la página Crear un WorkSpaces grupo de directorios de la WorkSpaces consola. Al crear el directorio WorkSpaces de grupos, debe especificar los detalles de su AD si planea usar un AD con sus WorkSpaces grupos. No puede editar la configuración de Active Directory para el directorio de WorkSpaces grupos después de crearla. A continuación se muestra un ejemplo de la sección Config de Active Directory de la página de directorio Create WorkSpaces Pool.



> **Note**
>
> El proceso completo para crear un WorkSpaces directorio de grupos se describe en el Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos tema. Los procedimientos descritos en esta página representan solo un subconjunto de pasos del proceso completo para crear un directorio de WorkSpaces grupos.

Temas

- Especificación de la unidad organizativa y el nombre de dominio del directorio de AD
- Especificación de la cuenta de servicio para el directorio de AD

Especificación de la unidad organizativa y el nombre de dominio del directorio de AD

Complete el siguiente procedimiento para especificar una unidad organizativa (OU) y un nombre de dominio de directorio para su AD en la página Crear un directorio WorkSpaces de grupos.

1. En Unidad organizativa, introduzca la OU a la que pertenece el grupo. WorkSpace las cuentas de máquina se colocan en la unidad organizativa (OU) que especifique para el directorio del WorkSpaces grupo.

   > **Note**
   >
   > El nombre de la unidad organizativa no puede contener espacios. Si especifica un nombre de unidad organizativa que contiene espacios, al intentar volver a unirse al dominio de Active Directory, WorkSpaces no podrá reproducir los objetos del equipo correctamente y la unión del dominio no funcionará.

2. En Nombre de dominio del directorio, proporcione el nombre de dominio completo (FQDN) del dominio de Active Directory (por ejemplo, `corp.example.com`). Cada AWS región solo puede tener un valor de configuración de directorio con un nombre de directorio específico.

   - Puede unir los directorios de su WorkSpaces grupo a los dominios de Microsoft Active Directory. También puede usar sus dominios de Active Directory existentes, ya sean basados en la nube o locales, para lanzar dominios WorkSpaces unidos.
   - También puede utilizarlos AWS Directory Service for Microsoft Active Directory, también conocidos como AWS Managed Microsoft AD, para crear un dominio de Active Directory. A continuación, puede usar ese dominio para respaldar sus WorkSpaces recursos.
   - Al unirse WorkSpaces a su dominio de Active Directory, puede:
     - Ofrecer acceso a los usuarios y a las aplicaciones a los recursos de Active Directory, como las impresoras y el uso compartido de archivos de las sesiones de transmisión.
     - Utilizar las configuraciones de políticas de grupo que están disponibles en la consola de administración de políticas de grupo (GPMC) para definir la experiencia del usuario final.
     - Transmita aplicaciones en streaming que requieren que los usuarios se autentiquen mediante sus credenciales de inicio de sesión de Active Directory.

- Aplicar sus políticas de conformidad y seguridad de la compañía a sus instancias de streaming de WorkSpaces .

3. En Cuenta de servicio, continúe con la siguiente sección Especificación de la cuenta de servicio para el directorio de AD de esta página.

Especificación de la cuenta de servicio para el directorio de AD

Al configurar Active Directory (AD) para sus WorkSpaces grupos como parte del proceso de creación de directorios, debe especificar la cuenta de servicio de AD que se utilizará para administrar el AD. Para ello, debe proporcionar las credenciales de la cuenta de servicio, que deben almacenarse AWS Secrets Manager y cifrarse mediante una clave AWS Key Management Service (AWS KMS) gestionada por el cliente. En esta sección, le mostramos cómo crear la clave administrada por el AWS KMS cliente y el secreto de Secrets Manager para almacenar las credenciales de su cuenta de servicio de AD.

Paso 1: Crear una clave administrada por el cliente de AWS KMS

Complete el siguiente procedimiento para crear una clave administrada por el AWS KMS cliente

1. Abra la AWS KMS consola 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. Elija Crear una clave y luego Siguiente.
4. Seleccione Simétrica en el tipo de clave, elija Cifrar y descifrar en el uso de clave y luego seleccione Siguiente.
5. Introduzca un alias para la clave, como, por ejemplo, `WorkSpacesPoolDomainSecretKey`, y luego seleccione Siguiente.
6. No elija un administrador de claves. Elija Siguiente para continuar.
7. No defina permisos de uso de claves. Elija Siguiente para continuar.
8. En la sección Política de claves de la página, añada lo siguiente:

```
        {
            "Sid": "Allow access for Workspaces SP",
            "Effect": "Allow",
            "Principal": {
                "Service": "workspaces.amazonaws.com"
            },
```

```
            "Action": "kms:Decrypt",
            "Resource": "*"
        }
```

El resultado debe ser similar al del siguiente ejemplo.

```
4    "Statement": [
5        {
6            "Sid": "Enable IAM User Permissions",
7            "Effect": "Allow",
8            "Principal": {
9                "AWS": "arn:aws:iam::[redacted]:root"
10           },
11           "Action": "kms:*",
12           "Resource": "*"
13       },
14       {
15           "Sid": "Allow access for Workspaces SP",
16           "Effect": "Allow",
17           "Principal": {
18               "Service": [
19                   "workspaces.amazonaws.com"
20               ]
21           },
22           "Action": "kms:Decrypt",
23           "Resource": "*"
24       }
```

9. Seleccione Finalizar.

   Su clave gestionada por el AWS KMS cliente ya está lista para usarse con Secrets Manager. Continúe con la sección Paso 2: crear el secreto de Secrets Manager para almacenar las credenciales de la cuenta de servicio de AD de esta página.

Paso 2: crear el secreto de Secrets Manager para almacenar las credenciales de la cuenta de servicio de AD

Complete el siguiente procedimiento para crear un secreto de Secrets Manager con el fin de almacenar las credenciales de la cuenta de servicio de AD.

1. Abra la AWS Secrets Manager consola en https://console.aws.amazon.com/secretsmanager/.
2. Elija Create a new secret (Elegir un nuevo secerto).
3. Elija Otro tipo de secreto.
4. Para el primer key/value par, introduzca `Service Account Name` la clave y el nombre de la cuenta de servicio para el valor, por ejemplo`domain\username`.

5. Para el segundo key/value par, introduzca una `Service Account Password` como clave y la contraseña de la cuenta de servicio para el valor.
6. Para la clave de cifrado, elija la clave gestionada por el AWS KMS cliente que creó anteriormente y, a continuación, elija Siguiente.
7. Escriba un nombre para el secreto, como, por ejemplo, `WorkSpacesPoolDomainSecretAD`.
8. Seleccione Editar permisos en la sección Permisos de recursos de la página.
9. Introduzca la siguiente política de permiso:

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "workspaces.amazonaws.com"
                ]
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

10. Elija Guardar para guardar la política de permiso.
11. Elija Siguiente para continuar.
12. No configure la rotación automática. Elija Siguiente para continuar.
13. Seleccione Almacenar para terminar de almacenar el secreto.

Ya se han guardado en Secrets Manager las credenciales de la cuenta de servicio de AD. Continúe con la sección Paso 3: seleccionar el secreto de Secrets Manager que incluye las credenciales de la cuenta de servicio de AD de esta página.

Paso 3: seleccionar el secreto de Secrets Manager que incluye las credenciales de la cuenta de servicio de AD

Complete el siguiente procedimiento para seleccionar el secreto de Secrets Manager que creó en la configuración de Active Directory para el directorio de su WorkSpaces grupo.

- En Cuenta de servicio, elija el AWS Secrets Manager secreto que contiene las credenciales de su cuenta de servicio. Complete los siguientes pasos para crear el secreto, si aún no lo ha hecho. El secreto debe cifrarse mediante una clave gestionada por el AWS Key Management Service cliente.

Ahora que ha completado todos los campos de la sección Config de Active Directory de la página Crear WorkSpaces directorio de grupos, puede continuar con la creación del directorio WorkSpaces de grupos. Vaya a Paso 4: Crear un directorio de WorkSpace grupos y comience con el paso 9 del procedimiento.

Actualice los detalles del directorio de sus WorkSpaces piscinas

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

Autenticación

Puede configurar opciones de autenticación adicionales para sus WorkSpaces grupos. Pools requiere la autenticación de SAML 2.0.

Cómo habilitar y configurar la autenticación de proveedor de identidades de SAML 2.0

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Elija Directorios en el panel de navegación.
3. Elija el directorio que desea configurar.
4. Vaya a Autenticación y seleccione Editar.
5. Seleccione Editar proveedor de identidad de SAML 2.0.
6. Marque la casilla de verificación Habilitar la autenticación de SAML 2.0.
7. Introduzca la URL de acceso de usuario para dirigir al cliente de WorkSpaces Pools durante el inicio de sesión federado.
8. Introduzca el nombre del parámetro de enlace profundo del IdP (opcional).

9. Seleccione Save.

Cómo habilitar y configurar la autenticación basada en certificados

1. Abra la WorkSpaces consola en la versión 2/home. https://console.aws.amazon.com/workspaces/
2. Elija Directorios en el panel de navegación.
3. Elija el directorio que desea configurar.
4. Vaya a Autenticación y seleccione Editar.
5. Elija Editar la autenticación basada en certificados.
6. Marque la casilla de verificación Habilitar la autenticación basada en certificados.
7. Elija en el menú desplegable Autoridad de certificación privada (CA) de AWS Certificate Manager (ACM).
8. Seleccione Save.

Grupo de seguridad

Aplique un grupo de seguridad a los WorkSpaces grupos de su directorio.

Para configurar un grupo de seguridad para sus WorkSpaces grupos

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Elija Directorios en el panel de navegación.
3. Elija el directorio que desea configurar.
4. Vaya a Grupo de seguridad y seleccione Editar.
5. En el menú desplegable, elija un grupo de seguridad.

Configuración de Active Directory

Configure su directorio Active Directory Config con una unidad organizativa (OU), un nombre de dominio del directorio y un secreto de AWS Secrets Manager.

Cómo configurar Active Directory

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/v2/home.

2. Elija Directorios en el panel de navegación.
3. Elija el directorio que desea configurar.
4. Vaya a Configuración de Active Directory y seleccione Editar.
5. Para buscar una unidad organizativa (OU), puede empezar a escribir todo o parte de su nombre y elegir la que desee usar.

> **Note**
>
> (Opcional) Tras elegir la OU, reconstruya la existente WorkSpaces para actualizarla. Para obtener más información, consulte Reconstruir un WorkSpace in WorkSpaces Personal

6. Seleccione Save.

> **Note**
>
> El nombre de dominio del directorio y el secreto de AWS Secrets Manager no se pueden editar una vez que hayas creado tu pool.

Propiedades de transmisión

Configura la forma en que tus usuarios pueden transferir datos entre su dispositivo agrupado WorkSpace y su dispositivo local.

Cómo configurar propiedades de transmisión

1. Abre la WorkSpaces consola en la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. Elija Directorios en el panel de navegación.
3. Elija el directorio que desea configurar.
4. Vaya a Propiedades de transmisión y seleccione Editar.
5. Configure las siguientes propiedades de transmisión:
   - Permisos del portapapeles
     - En la lista desplegable, elija una de las siguientes opciones:

    - Permitir copiar y pegar: permite copiar en un dispositivo local y pegar en una sesión remota.
    - Permitir pegar en una sesión remota: permite pegar en una sesión remota.
    - Permitir copiar en un dispositivo local: permite copiar en un dispositivo local.
    - Deshabilitado
  - Elija si desea permitir o no la impresión en el dispositivo local.
  - Elija si desea permitir o no el registro de diagnósticos.
  - Elija si desea permitir o no el inicio de sesión con tarjeta inteligente.
  - Para habilitar el almacenamiento de las carpetas de inicio, seleccione Habilitar las carpetas de inicio.
6. Seleccione Save.

rol de IAM

Seleccione un rol de IAM para sus grupos. WorkSpaces

Cómo seleccionar un rol de IAM

1. Abre la WorkSpaces consola en la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. Elija Directorios en el panel de navegación.
3. Elija el directorio que desea configurar.
4. Vaya a rol de IAM y elija Editar.
5. Elija un rol de IAM en la lista desplegable. Para crear un nuevo rol de IAM, elija Crear un nuevo rol de IAM.
6. Seleccione Save.

Etiquetas

Añada nuevas etiquetas a sus piscinas WorkSpaces

Cómo añadir una etiqueta nueva

1. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. Elija Directorios en el panel de navegación.

3. Elija el directorio que desea configurar.
4. Vaya a Etiquetas y seleccione Administrar etiquetas.
5. Elija Añadir etiquetas y escriba el valor del par de claves que desee usar. Una clave puede ser una categoría general, como "proyecto", "propietario" o "entorno", con valores específicos asociados.
6. Seleccione Save changes (Guardar cambios).

Anular el registro de un directorio de grupos WorkSpaces

Complete los siguientes procedimientos para anular el registro de un WorkSpaces directorio de grupos.

1. Abra la WorkSpaces consola en la versión 2/home. https://console.aws.amazon.com/workspaces/
2. Elija Directorios en el panel de navegación.
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.

Redes y acceso para WorkSpaces piscinas

En los temas siguientes se proporciona información sobre cómo permitir que los usuarios se conecten a los WorkSpaces grupos y cómo permitir que sus WorkSpaces grupos accedan a los recursos de la red e Internet.

Contenido

- Acceso a Internet para WorkSpaces piscinas
- Configurar una VPC para grupos WorkSpaces
- Configure la autorización de FedRAMP o el cumplimiento de las normas SRG del DoD para los grupos WorkSpaces
- Uso de puntos de enlace de VPC de Amazon S3 para funciones de grupos WorkSpaces
- Conexiones a su VPC para grupos WorkSpaces
- Conexiones de usuario a WorkSpaces grupos

Acceso a Internet para WorkSpaces piscinas

Si tus WorkSpaces WorkSpaces piscinas requieren acceso a Internet, puedes habilitarlo de varias maneras. Al elegir un método para habilitar el acceso a Internet, tenga en cuenta la cantidad de usuarios que debe admitir su implementación y sus objetivos de implementación. Por ejemplo:

- Si su implementación debe admitir más de 100 usuarios simultáneos, configure una VPC con subredes privadas y una puerta de enlace NAT.
- Si su implementación admite menos de 100 usuarios simultáneos, puede configurar una VPC nueva o existente con una subred pública.
- Si su implementación admite menos de 100 usuarios simultáneos y es la primera vez que usa WorkSpaces Pools y quiere empezar a usar el servicio, puede usar la VPC, la subred pública y el grupo de seguridad predeterminados.

En las secciones siguientes se proporciona más información acerca de estas opciones de implementación.

- Configurar una VPC con subredes privadas y una puerta de enlace NAT(recomendado): con esta configuración, puede lanzar los generadores de WorkSpaces grupos en una subred privada y configurar una puerta de enlace NAT en una subred pública de su VPC. A las instancias de streaming se les asigna una dirección IP privada a la que no se puede acceder directamente desde Internet.

  Además, a diferencia de las configuraciones que utilizan la opción de acceso a Internet predeterminado para habilitar el acceso a Internet, la configuración de NAT no se limita a 100 WorkSpaces en grupos. WorkSpaces Si la implementación debe admitir más de 100 usuarios simultáneos, utilice esta configuración.

  Puede crear y configurar una VPC nueva para utilizarla con una puerta de enlace NAT o agregar una puerta de enlace NAT a una VPC existente.
- Configurar una VPC nueva o existente con una subred pública— Con esta configuración, puede lanzar sus WorkSpaces grupos en una subred pública. Al activar esta opción, WorkSpaces Pools utiliza la puerta de enlace de Internet de la subred pública de Amazon VPC para proporcionar la conexión a Internet. A las instancias de streaming se les asigna una dirección IP pública a la que se puede acceder directamente desde Internet. Puede crear una VPC nueva o configurar una existente para este fin.

> **Note**
>
> Al configurar una VPC nueva o existente con una subred pública, se admiten un máximo de 100 en WorkSpaces los grupos. WorkSpaces Si la implementación debe admitir más de 100 usuarios simultáneos, utilice la configuración de puerta de enlace NAT en su lugar.

- Utilizar la VPC, la subred pública y el grupo de seguridad predeterminados— Si es la primera vez que WorkSpaces utilizas los grupos y quieres empezar a utilizar el servicio, puedes lanzar tus WorkSpaces grupos en una subred pública predeterminada. Al activar esta opción, WorkSpaces Pools utiliza la puerta de enlace de Internet de la subred pública de Amazon VPC para proporcionar la conexión a Internet. A las instancias de streaming se les asigna una dirección IP pública a la que se puede acceder directamente desde Internet.

  VPCs Los valores predeterminados están disponibles en las cuentas de Amazon Web Services creadas después del 4 de diciembre de 2013.

  La VPC predeterminada incluye una subred pública predeterminada en cada zona de disponibilidad y una puerta de enlace de Internet asociada a la VPC. La VPC también incluye un grupo de seguridad predeterminado.

  > **Note**
  >
  > Cuando utilizas la VPC, la subred pública y el grupo de seguridad predeterminados, se admiten un máximo de 100 en WorkSpaces los grupos. WorkSpaces Si la implementación debe admitir más de 100 usuarios simultáneos, utilice la configuración de puerta de enlace NAT en su lugar.

Configurar una VPC para grupos WorkSpaces

Al configurar WorkSpaces grupos, debe especificar la nube privada virtual (VPC) y al menos una subred en la que lanzar su. WorkSpaces Una VPC es una red virtual en su propia área, aislada lógicamente en la nube de Amazon Web Services. Una subred es un rango de direcciones IP en su VPC.

Al configurar la VPC para WorkSpaces grupos, puede especificar subredes públicas o privadas, o una combinación de ambos tipos de subredes. Las subredes públicas tienen acceso a Internet a través de una puerta de enlace de Internet. Las subredes privadas, que no tiene una ruta a una

puerta de enlace de Internet, requieren una puerta de enlace de traducción de direcciones de red (NAT) o una instancia NAT para proporcionar acceso a Internet.

Contenido

- Recomendaciones de configuración de VPC para grupos WorkSpaces
- Configurar una VPC con subredes privadas y una puerta de enlace NAT
- Configurar una VPC nueva o existente con una subred pública
- Utilizar la VPC, la subred pública y el grupo de seguridad predeterminados

Recomendaciones de configuración de VPC para grupos WorkSpaces

Al crear un grupo, WorkSpaces se especifica la VPC y una o más subredes que se van a utilizar. Puede proporcionar control de acceso adicional a la VPC especificando grupos de seguridad.

Las siguientes recomendaciones pueden ayudarle a configurar la VPC de forma más eficaz y segura. Además, pueden ayudarlo a configurar un entorno que permita un escalado efectivo de los WorkSpaces grupos. Con un escalado efectivo de los WorkSpaces grupos, puede satisfacer la demanda actual y prevista de los WorkSpaces usuarios y, al mismo tiempo, evitar el uso innecesario de recursos y los costos asociados.

Configuración general de la VPC

- Asegúrese de que la configuración de su VPC pueda satisfacer las necesidades de escalado de sus WorkSpaces grupos.

  A medida que desarrolle su plan de escalado de WorkSpaces grupos, tenga en cuenta que un usuario necesita uno WorkSpaces. Por lo tanto, el tamaño de sus WorkSpaces grupos determina la cantidad de usuarios que pueden transmitir simultáneamente. Por este motivo, para cada tipo de instancia que vaya a utilizar, asegúrese de que la cantidad WorkSpaces que la VPC puede admitir sea superior a la cantidad de usuarios simultáneos previstos para el mismo tipo de instancia.
- Asegúrese de que las cuotas de sus cuentas de WorkSpaces Pools (también denominadas límites) sean suficientes para satisfacer la demanda prevista. Para solicitar un aumento de cuota, puede utilizar la consola Service Quotas en https://console.aws.amazon.com/servicequotas/. Para obtener información sobre las cuotas de WorkSpaces grupos predeterminadas, consulte WorkSpaces Cuotas de Amazon.

- Si planea proporcionar acceso a Internet a sus WorkSpaces WorkSpaces grupos internos, le recomendamos que configure una VPC con dos subredes privadas para sus instancias de streaming y una puerta de enlace NAT en una subred pública.

  La puerta de enlace NAT permite que las subredes privadas se WorkSpaces conecten a Internet o a otros servicios. AWS Sin embargo, impide que Internet inicie una conexión con ellas. WorkSpaces Además, a diferencia de las configuraciones que utilizan la opción de acceso a Internet predeterminado para habilitar el acceso a Internet, la configuración de NAT admite más de 100 WorkSpaces. Para obtener más información, consulte Configurar una VPC con subredes privadas y una puerta de enlace NAT.

Interfaces de redes elásticas

- WorkSpaces Los grupos crean tantas interfaces de red elásticas (interfaces de red) como la capacidad máxima deseada de sus WorkSpaces grupos. De forma predeterminada, el límite de interfaces de red por región es 5000.

  Al planificar la capacidad para despliegues muy grandes, por ejemplo, miles de WorkSpaces, ten en cuenta el número de EC2 instancias de Amazon que también se utilizan en la misma región.

Subredes

- Si va a configurar más de una subred privada para la VPC, configure cada una en una zona de disponibilidad diferente. De este modo, aumenta la tolerancia a errores y puede ayudar a evitar problemas de falta de capacidad. Si utiliza dos subredes en la misma zona de disponibilidad, es posible que se quede sin direcciones IP, ya que los WorkSpaces grupos no utilizarán la segunda subred.
- Asegúrese de que los recursos de red necesarios para las aplicaciones sean accesibles a través ambas subredes privadas.
- Configure cada una de las subredes privadas con una máscara de subred que permita suficientes direcciones IP de cliente para tener capacidad para el número máximo de usuarios simultáneos previstos. Además, permita direcciones IP adicionales para tener en cuenta el crecimiento previsto. Para obtener más información, consulte Dimensionamiento de subredes y VPC para. IPv4
- Si utiliza una VPC con NAT, configure al menos una subred pública con una puerta de enlace NAT para acceder a Internet, preferiblemente dos. Configure las subredes públicas en las mismas zonas de disponibilidad donde residen las subredes privadas.

Para mejorar la tolerancia a los errores y reducir la posibilidad de que se produzcan errores de capacidad insuficiente en las implementaciones de WorkSpaces grupos grandes, considere la posibilidad de ampliar la configuración de VPC a una tercera zona de disponibilidad. Incluya una subred privada, una subred pública y una puerta de enlace NAT en esta zona de disponibilidad adicional.

Grupos de seguridad

- Utilice grupos de seguridad para proporcionar control de acceso adicional a la VPC.

  Los grupos de seguridad que pertenecen a su VPC le permiten controlar el tráfico de red entre los WorkSpaces grupos, las instancias de streaming y los recursos de red que requieren las aplicaciones. Estos recursos pueden incluir otros AWS servicios, como Amazon RDS o Amazon FSx, servidores de licencias, servidores de bases de datos, servidores de archivos y servidores de aplicaciones.
- Asegúrese de que los grupos de seguridad proporcionen acceso a los recursos de red que requieren las aplicaciones.

  Para obtener información general sobre los grupos de seguridad, consulte Controlar el tráfico de sus AWS recursos mediante grupos de seguridad en la Guía del usuario de Amazon VPC.

Configurar una VPC con subredes privadas y una puerta de enlace NAT

Si planea proporcionar acceso a Internet a sus WorkSpaces WorkSpaces grupos internos, le recomendamos que configure una VPC con dos subredes privadas para usted WorkSpaces y una puerta de enlace NAT en una subred pública. Puede crear y configurar una VPC nueva para utilizarla con una puerta de enlace NAT o agregar una puerta de enlace NAT a una VPC existente. Para obtener más recomendaciones de configuración de la VPC, consulte Recomendaciones de configuración de VPC para grupos WorkSpaces .

La puerta de enlace NAT permite que las subredes privadas se WorkSpaces conecten a Internet o a otros AWS servicios, pero impide que Internet inicie una conexión con ellos. WorkSpaces Además, a diferencia de las configuraciones que utilizan la opción de acceso a Internet predeterminado para habilitar el acceso a Internet WorkSpaces, esta configuración no está limitada a 100. WorkSpaces

Para obtener más información acerca del uso de puertas de enlace NAT y esta configuración, consulte Puertas de enlace NAT y VPC con subredes privadas y públicas (NAT) en la Guía del usuario de Amazon VPC.

Contenido

- Creación y configuración de una VPC nueva
- Agregar una puerta de enlace NAT a una VPC existente
- Habilitar el acceso a Internet para WorkSpaces las piscinas

Creación y configuración de una VPC nueva

En este tema se describe cómo utilizar el asistente de VPC para crear una VPC con una subred pública y una subred privada. Como parte de este proceso, el asistente crea una puerta de enlace de Internet y una puerta de enlace NAT. También crea una tabla de enrutamiento personalizada asociada con la subred pública y actualiza la tabla de enrutamiento principal asociada con la subred privada. La puerta de enlace NAT se creará automáticamente en la subred pública de su VPC.

Después de utilizar el asistente para crear la configuración inicial de la VPC, agregará una segunda subred privada. Para obtener más información acerca de esta configuración, consulte VPC con subredes privadas y públicas (NAT) en la Guía del usuario de Amazon VPC.

> **Note**
>
> Si ya tiene una VPC, complete los pasos descritos en Agregar una puerta de enlace NAT a una VPC existente en su lugar.

Contenido

- Paso 1: asignación de una dirección IP elástica
- Paso 2: creación de una VPC nueva
- Paso 3: adición de una segunda subred privada
- Paso 4: verificación y asignación de un nombre a las tablas de enrutamiento de la subred

Paso 1: asignación de una dirección IP elástica

Antes de crear la VPC, debe asignar una dirección IP elástica en su WorkSpaces región. Primero debe asignar una dirección IP elástica para usarla en la VPC y luego asociarla a la puerta de enlace

NAT. Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon VPC.

> **Note**
>
> Es posible que se apliquen cargos a las direcciones IP elásticas que utilice. Para obtener más información, consulta Elastic IP Addresses en la página de EC2 precios de Amazon.

Complete los siguientes pasos si aún no tiene una dirección IP elástica. Si desea utilizar una dirección IP elástica existente, compruebe que no esté actualmente asociada a otra instancia o interfaz de red.

Para asignar una dirección IP elástica

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Red y seguridad, selecciona Elastic IPs.
3. Elija Asignar nueva dirección y, a continuación, elija Asignar.
4. Tome nota de la dirección IP elástica.
5. En la parte superior derecha del IPs panel elástico, haz clic en el icono X para cerrar el panel.

Paso 2: creación de una VPC nueva

Complete los siguientes pasos para crear una VPC nueva con una subred pública y una subred privada.

Para crear una VPC nueva

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Panel de VPC.
3. Elija Lanzar el asistente de VPC.
4. En Paso 1: selección de una configuración de VPC, elija VPC con subredes pública y privada y, a continuación, elija Seleccionar.
5. En Paso 2: VPC con subredes pública y privada, configure la VPC como sigue:
   - Para el bloque IPv4 CIDR, especifique un bloque IPv4 CIDR para la VPC.
   - Para el bloque IPv6 CIDR, mantenga el valor predeterminado, Sin bloque CIDR. IPv6

- En Nombre de la VPC, escriba un nombre único para la VPC.

6. Configure la subred pública de la siguiente manera:
   - Para el CIDR de la subred pública, especifique el bloque IPv4 CIDR de la subred.
   - En Zona de disponibilidad, deje el valor predeterminado Sin preferencia.
   - En Nombre de la subred pública, escriba un nombre para la subred, como `WorkSpaces Public Subnet`.
7. Configure la primera subred privada de la siguiente manera:
   - Para el CIDR de la subred privada, especifique el IPv4 bloque CIDR de la subred. Tome nota del valor que especifique.
   - En Zona de disponibilidad, seleccione una zona específica y tome nota de la zona seleccionada.
   - En Nombre de la subred privada, escriba un nombre para la subred, como `WorkSpaces Private Subnet1`.
   - En los campos restantes, cuando corresponda, deje los valores predeterminados.
8. En ID de asignación de IP elástica, haga clic en el cuadro de texto y seleccione el valor que corresponda a la dirección IP elástica creada. Esta dirección se asigna a la puerta de enlace NAT. Si no tiene una dirección IP elástica, cree una mediante la consola de Amazon VPC en. https://console.aws.amazon.com/vpc/
9. En Puntos de conexión de servicio, si se requiere un punto de conexión de Amazon S3 para el entorno, especifique uno. Se precisa un punto de conexión de S3 para proporcionar a los usuarios acceso a las carpetas iniciales o para habilitar la persistencia de configuración de la aplicación para los usuarios de una red privada.

   Para especificar un punto de conexión de Amazon S3, haga lo siguiente:

   a. Elija Agregar punto de conexión.
   b. En Servicio, seleccione la entrada de la lista que termina en «s3" (la `com.amazonaws.`*`region`*`.s3` entrada que corresponde a la región en la que se está creando la VPC).
   c. En Subred, elija subnet-2.
   d. En Política, deje el valor predeterminado, Acceso completo.
10. En Habilitar nombres de host de DNS, deje el valor predeterminado, Sí.
11. En Tenencia de hardware, deje el valor Predeterminado.
12. Seleccione Crear VPC.

13. Tenga en cuenta que se necesitan varios minutos para configurar la VPC. Una vez creada la VPC, elija Aceptar.

Paso 3: adición de una segunda subred privada

En el paso anterior (Paso 2: creación de una VPC nueva), ha creado una VPC con una subred pública y una subred privada. Realice los siguientes pasos para agregar una segunda subred privada. Se recomienda agregar una segunda subred privada en una zona de disponibilidad diferente a la primera subred privada.

1. En el panel de navegación, elija Subredes.
2. Seleccione la primera subred privada que creó en el paso anterior. En la pestaña Descripción debajo de la lista de subredes, tome nota de la zona de disponibilidad de esta subred.
3. En la parte superior izquierda del panel de subredes, elija Crear subred.
4. En Etiqueta de nombre, escriba un nombre para la subred privada, como `WorkSpaces Private Subnet2`.
5. En VPC, seleccione la VPC que creó en el paso anterior.
6. En Zona de disponibilidad, seleccione una zona de disponibilidad distinta de la que está utilizando para la primera subred privada. La selección de una zona de disponibilidad diferente aumenta la tolerancia a errores y ayuda a evitar problemas de falta de capacidad.
7. Para el bloque IPv4 CIDR, especifique un rango de bloques CIDR único para la nueva subred. Por ejemplo, si su primera subred privada tiene un rango de bloques IPv4 CIDR de`10.0.1.0/24`, puede especificar un rango de bloques CIDR de `10.0.2.0/24` para la nueva subred privada.
8. Seleccione Crear.
9. Una vez creada la subred, elija Cerrar.

Paso 4: verificación y asignación de un nombre a las tablas de enrutamiento de la subred

Después de crear y configurar la VPC, siga los pasos siguientes para especificar un nombre para las tablas de enrutamiento y comprobar que:

- La tabla de enrutamiento asociada a la subred en la que reside su puerta de enlace NAT incluye una ruta que apunte el tráfico de Internet a una puerta de enlace de Internet. Esto garantiza que la puerta de enlace NAT pueda acceder a Internet.

- Las tablas de enrutamiento asociadas a las subredes privadas se configuran para apuntar el tráfico de Internet a la puerta de enlace NAT. Esto permite a las instancias streaming de sus subredes privadas comunicarse con Internet.

1. En el panel de navegación, elija Subredes y seleccione la subred pública que ha creado; por ejemplo, `WorkSpaces Public Subnet`.

   a. En la pestaña Tabla de enrutamiento, elija el ID de la tabla de enrutamiento; por ejemplo, `rtb-12345678`.

   b. Seleccione la tabla de enrutamiento. En Nombre, elija el icono de edición (lápiz) e introduzca un nombre (por ejemplo, `workspaces-public-routetable`) y, a continuación, seleccione la marca de verificación para guardar el nombre.

   c. Con la tabla de enrutamiento pública aún seleccionada, en la pestaña Rutas, compruebe que haya una ruta para el tráfico local y otra que envía el resto del tráfico hacia la puerta de enlace de Internet de la VPC. En la tabla siguiente se describen estas dos rutas:

Destino	Objetivo	Descripción
Bloque IPv4 CIDR de subred pública (por ejemplo, 10.0.0/20)	Local	Todo el tráfico de los recursos destinado a IPv4 las direcciones del bloque IPv4 CIDR de la subred pública se enruta localmente dentro de la VPC.
El tráfico destinado a todas las demás IPv4 direcciones (por ejemplo, 0.0.0.0/0	Saliente () `igw-` *`ID`*	El tráfico destinado a todas IPv4 las demás direcciones se enruta a la puerta de enlace de Internet (identificada por `igw-`*`ID`*) que creó el asistente de VPC.

2. En el panel de navegación, elija Subredes y seleccione la primera subred privada que ha creado (por ejemplo, `WorkSpaces Private Subnet1`).

   a. En la pestaña Tabla de enrutamiento, elija el ID de la tabla de enrutamiento.

   b. Seleccione la tabla de enrutamiento. En Nombre, elija el icono de edición (lápiz) e introduzca un nombre (por ejemplo, `workspaces-private-routetable`) y, a continuación, elija la marca de verificación para guardar el nombre.

c. En la pestaña Rutas, compruebe que la tabla de enrutamiento incluye las siguientes rutas:

Destino	Objetivo	Descripción
Bloque IPv4 CIDR de subred pública (por ejemplo, 10.0.0/20)	Local	Todo el tráfico de los recursos destinado a IPv4 las direcciones del bloque IPv4 CIDR de la subred pública se enruta localmente dentro de la VPC.
El tráfico destinado a todas las demás IPv4 direcciones (por ejemplo, 0.0.0.0/0	Saliente () `nat-` *`ID`*	El tráfico destinado a todas las demás IPv4 direcciones se enruta a la puerta de enlace NAT (identifi cada por `nat-`*`ID`*).
Tráfico destinado a buckets de S3 (aplicabl e si especificó un punto de conexión de S3) [`pl-`*`ID`* (`com.amazo naws.` *`region`*`.s3`)]	Almacenamiento () `vpce-` *`ID`*	El tráfico destinado a los buckets de S3 se enruta al punto final de S3 (identificado por `vpce-`*`ID`*).

3. En el panel de navegación, elija Subredes y seleccione la segunda subred privada que ha creado (por ejemplo, `WorkSpaces Private Subnet2`).
4. En la pestaña Tabla de enrutamiento, compruebe que la tabla de enrutamiento es la tabla de enrutamiento privada (por ejemplo, `workspaces-private-routetable`). Si la tabla de enrutamiento es diferente, elija Editar y seleccione esta tabla de enrutamiento.

Pasos siguientes

Para permitir que sus WorkSpaces grupos WorkSpaces internos accedan a Internet, complete los pasos que se indican a continuación. Habilitar el acceso a Internet para WorkSpaces las piscinas

Agregar una puerta de enlace NAT a una VPC existente

Si ya ha configurado una VPC, siga los pasos siguientes para agregar una puerta de enlace NAT a la VPC. Si necesita crear una VPC nueva, consulte Creación y configuración de una VPC nueva.

Para agregar una puerta de enlace NAT a un VPC existente

1. Para crear la puerta de enlace NAT, complete los pasos de Crear una puerta de enlace NAT en la Guía del usuario de Amazon VPC.
2. Compruebe que la VPC tiene al menos una subred privada. Recomendamos que especifique dos subredes privadas situadas en zonas de disponibilidad distintas para ofrecer alta disponibilidad y tolerancia a errores. Para obtener información sobre cómo crear una segunda subred privada, consulte Paso 3: adición de una segunda subred privada.
3. Actualice la tabla de enrutamiento asociada a una o varias de sus subredes privadas para que apunte el tráfico vinculado a Internet a la puerta de enlace NAT. Esto permite a las instancias streaming de sus subredes privadas comunicarse con Internet. Para ello, complete los pasos que se indican en Actualización de la tabla de enrutamiento de la Guía del usuario de Amazon VPC.

Pasos siguientes

Para permitir que tus usuarios de WorkSpaces In WorkSpaces Pools accedan a Internet, sigue los pasos que se indican a continuación. Habilitar el acceso a Internet para WorkSpaces las piscinas

Habilitar el acceso a Internet para WorkSpaces las piscinas

Una vez que la puerta de enlace NAT esté disponible en una VPC, puede habilitar el acceso a Internet para sus WorkSpaces grupos. Puede habilitar el acceso a Internet al crear el directorio de WorkSpaces grupos. Elija la VPC con una puerta de enlace NAT al crear el directorio. A continuación, seleccione una subred privada para Subred 1 y, si lo desea, otra subred privada para Subred 2. Si aún no tiene una subred privada en su VPC, puede que necesite crear una segunda subred privada.

Para probar su conectividad a Internet, inicie su WorkSpaces grupo y, a continuación, conéctese WorkSpace a uno del grupo y navegue por Internet.

Configurar una VPC nueva o existente con una subred pública

Si creó su cuenta de Amazon Web Services después del 4 de diciembre de 2013, tiene una VPC predeterminada en cada AWS región que incluye subredes públicas predeterminadas. Sin embargo,

es posible que desee crear su propia VPC no predeterminada o configurar una VPC existente para usarla con el directorio de su grupo. WorkSpaces En este tema se describe cómo configurar una VPC y una subred pública no predeterminadas para usarlas con grupos. WorkSpaces

Después de configurar la VPC y la subred pública, puede proporcionar acceso a Internet a sus WorkSpaces WorkSpaces grupos internos habilitando la opción Acceso a Internet predeterminado. Al habilitar esta opción, WorkSpaces Pools habilita la conectividad a Internet al asociar una dirección IP elástica a la interfaz de red que se conecta desde la instancia de streaming a la subred pública. Una dirección IP elástica es una IPv4 dirección pública a la que se puede acceder desde Internet. Por este motivo, le recomendamos que, en su lugar, utilice una puerta de enlace NAT para proporcionar acceso a Internet a sus WorkSpaces grupos WorkSpaces internos. Además, cuando el acceso a Internet predeterminado está activado, WorkSpaces se admiten un máximo de 100. Si la implementación debe admitir más de 100 usuarios simultáneos, utilice la configuración de puerta de enlace NAT en su lugar.

Para obtener más información, consulte los pasos en Configurar una VPC con subredes privadas y una puerta de enlace NAT. Para obtener más recomendaciones de configuración de la VPC, consulte Recomendaciones de configuración de VPC para grupos WorkSpaces .

Contenido

- Paso 1: configuración de una VPC con una subred pública
- Paso 2: habilite el acceso a Internet predeterminado para sus WorkSpaces piscinas

Paso 1: configuración de una VPC con una subred pública

Puede configurar su propia VPC no predeterminada con una subred pública mediante uno de los métodos siguientes:

- Crear una nueva VPC con una única subred pública
- Configurar una VPC existente

Crear una nueva VPC con una única subred pública

Cuando utiliza el asistente para VPC para crear una VPC nueva, el asistente crea una puerta de enlace de Internet y una tabla de enrutamiento personalizada que está asociada a la subred pública. La tabla de enrutamiento dirige todo el tráfico destinado a una dirección fuera de la VPC a la puerta de enlace de Internet. Para obtener más información acerca de esta configuración, consulte VPC con una única subred pública en la Guía del usuario de Amazon VPC.

1. Complete los pasos del Paso 1: creación de la VPC en la Guía del usuario de Amazon VPC para crear la VPC.
2. Para permitir el acceso WorkSpaces a Internet, complete los pasos que se indican a continuaciónPaso 2: habilite el acceso a Internet predeterminado para sus WorkSpaces piscinas.

Configurar una VPC existente

Si desea utilizar una VPC existente que no tiene una subred pública, puede agregarle una nueva subred pública. Además de una subred pública, también debe tener una puerta de enlace de Internet asociada a la VPC y una tabla de enrutamiento que dirija todo el tráfico destinado a una dirección fuera de la VPC a la puerta de enlace de Internet. Para configurar estos componentes, siga los pasos siguientes.

1. Para agregar una subred pública, siga los pasos descritos en Creación de una subred en la VPC. Use la VPC existente que planea usar con WorkSpaces Pools.

   Si la VPC está configurada para admitir el IPv6 direccionamiento, aparece la lista de bloqueos de IPv6 CIDR. Seleccione No asignar Ipv6.
2. Para crear y asociar una puerta de enlace de Internet a la VPC, complete los pasos descritos en Creación y asociación de una puerta de enlace de Internet.
3. Para configurar la subred de modo que dirija el tráfico de Internet a través de la puerta de enlace de Internet, siga los pasos que se describen en Crear una tabla de enrutamiento personalizada. En el paso 5, para Destination, utilice IPv4 format ()`0.0.0.0/0`.
4. Para permitir que tus creadores de imágenes WorkSpaces y tú accedan a Internet, sigue los pasos que se indican a continuaciónPaso 2: habilite el acceso a Internet predeterminado para sus WorkSpaces piscinas.

Paso 2: habilite el acceso a Internet predeterminado para sus WorkSpaces piscinas

Puede habilitar el acceso a Internet al crear el directorio WorkSpaces de grupos. Elija la VPC con una subred pública al crear el directorio. A continuación, seleccione una subred pública para Subred 1 y, si lo desea, otra subred pública para Subred 2.

Para probar su conectividad a Internet, inicie su WorkSpaces grupo y, a continuación, conéctese WorkSpace a uno del grupo y navegue por Internet.

Utilizar la VPC, la subred pública y el grupo de seguridad predeterminados

Su cuenta de Amazon Web Services, si se creó después del 4 de diciembre de 2013, tiene una VPC predeterminada en cada región. AWS La VPC predeterminada incluye una subred pública predeterminada en cada zona de disponibilidad y una puerta de enlace de Internet asociada a la VPC. La VPC también incluye un grupo de seguridad predeterminado. Si eres nuevo en los WorkSpaces grupos y quieres empezar a usar el servicio, puedes mantener la VPC y el grupo de seguridad predeterminados seleccionados al crear un WorkSpaces grupo. A continuación, seleccione al menos una subred predeterminada.

> **Note**
>
> Si su cuenta de Amazon Web Services se creó antes del 4 de diciembre de 2013, debe crear una nueva VPC o configurar una existente para usarla con Pools. WorkSpaces Le recomendamos que configure manualmente una VPC con dos subredes privadas para sus WorkSpaces grupos y una puerta de enlace NAT en una subred pública. Para obtener más información, consulte Configurar una VPC con subredes privadas y una puerta de enlace NAT. También puede configurar una VPC no predeterminada con una subred pública. Para obtener más información, consulte Configurar una VPC nueva o existente con una subred pública.

Puede habilitar el acceso a Internet al crear el directorio del WorkSpaces grupo.

Debe elegir la VPC predeterminada al crear el directorio. El nombre de VPC predeterminado usa el siguiente formato:. `vpc-` *`vpc-id`* `(No_default_value_Name)`

A continuación, seleccione una subred pública predeterminada para la subred 1 y, si lo desea, otra subred pública predeterminada para la subred 2. Los nombres de subred predeterminados utilizan el siguiente formato:. `subnet-` *`subnet-id`* `|` `(` *`IPv4 CIDR block`* `)` `| Default in` *`availability-zone`*

Puede probar su conectividad a Internet iniciando su WorkSpaces grupo, y luego conectándose a un WorkSpace grupo y navegando por Internet.

Configure la autorización de FedRAMP o el cumplimiento de las normas SRG del DoD para los grupos WorkSpaces

Para cumplir con el Programa federal de gestión de riesgos y autorizaciones (FedRAMP) o la Guía de requisitos de seguridad de la informática en la nube (SRG) del Departamento de Defensa (DoD), debe configurar WorkSpaces Amazon Pools para que utilicen el cifrado de puntos finales de los estándares federales de procesamiento de información (FIPS) a nivel de directorio. También debe utilizar una AWS región de EE. UU. que cuente con la autorización de FedRAMP o que cumpla con las normas SRG del DoD.

El nivel de autorización de FedRAMP (moderado o alto) o el nivel de impacto SRG del DoD (2, 4 o 5) depende de la AWS región 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.

Requisitos

- El directorio WorkSpaces Pools debe configurarse para usar el modo validado por FIPS 140-2 para el cifrado de puntos finales.

> **Note**
>
> Para usar la configuración del modo validado por FIPS 140-2, asegúrese de lo siguiente:
>
> - El directorio de WorkSpaces grupos es uno de los siguientes:
> - Nuevo y no asociado a un grupo
> - Asociado a un grupo existente que está en estado DETENIDO
> - El directorio del grupo se ha `StreamingExperiencePreferredProtocol`establecido en TCP.

- Debe crear sus WorkSpaces grupos en una AWS región de EE. UU. que cuente con la autorización de FedRAMP o que cumpla con las normas SRG del DoD.
- Los usuarios deben acceder a los mismos WorkSpaces desde una de las siguientes aplicaciones cliente: WorkSpaces
  - macOS: 5.20.0 o posterior
  - Windows: 5.20.0 o posterior
  - Acceso web

Para utilizar el cifrado de punto de enlace de FIPS

1. Abra la WorkSpaces consola en la versión 2/home. https://console.aws.amazon.com/workspaces/
2. En el panel de navegación, elija Directorios y, a continuación, elija el directorio que desee usar para la autorización de FedRAMP y el cumplimiento de las normas SRG del DoD.
3. En la página de detalles del directorio, elija el directorio que desee configurar para el modo de cifrado FIPS.
4. En la sección de cifrado de terminales, elija Editar y, a continuación, seleccione el modo validado por FIPS 140-2.
5. Seleccione Save.

Uso de puntos de enlace de VPC de Amazon S3 para funciones de grupos WorkSpaces

Al habilitar la persistencia de la configuración de la aplicación para un WorkSpaces grupo o las carpetas principales para un WorkSpaces directorio de grupos, WorkSpaces utiliza la VPC que especifique para su directorio para proporcionar acceso a los buckets de Amazon Simple Storage Service (Amazon S3). Para habilitar el acceso de WorkSpaces Pools a su punto de enlace S3 privado, adjunte la siguiente política personalizada a su punto de enlace de VPC para Amazon S3. Para obtener más información sobre los puntos de conexión de Amazon S3, consulte Puntos de conexión de VPC y Puntos de conexión para Amazon S3 en la Guía del usuario de Amazon VPC.

Commercial Regiones de AWS

Utilice la siguiente política para los recursos de las Regiones de AWS comerciales.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow-WorkSpaces-to-access-S3-buckets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:sts::<123456789012>:assumed-role/
workspaces_DefaultRole/WorkSpacesPoolSession"
```

```
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
            ]
        }
    ]
}
```

AWS GovCloud (US) Regions

Utilice la siguiente política para los recursos de las AWS GovCloud (US) Regions comerciales.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow-WorkSpaces-to-access-S3-buckets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:sts::<123456789012>:assumed-role/
workspaces_DefaultRole/WorkSpacesPoolSession"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion"
            ],
```

```
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ]
        }
    ]
}
```

Conexiones a su VPC para grupos WorkSpaces

Para habilitar la conectividad de los WorkSpaces grupos con los recursos de la red e Internet, configúrelos de la WorkSpaces siguiente manera.

Interfaces de red

Cada uno WorkSpaces de los WorkSpaces grupos tiene las siguientes interfaces de red:

- La interfaz de red del cliente proporciona conectividad a los recursos de la VPC, así como a Internet, y se utiliza para unirlos WorkSpaces a su directorio.
- La interfaz de red de administración está conectada a una red de administración de WorkSpaces grupos segura. Se utiliza para la transmisión interactiva del contenido WorkSpace al dispositivo del usuario y para permitir que WorkSpaces Pools lo gestione WorkSpace.

WorkSpaces Pools selecciona la dirección IP para la interfaz de red de administración del siguiente rango de direcciones IP privadas: 198.19.0.0/16. No utilice este rango para el CIDR de su VPC ni empareje su VPC con otra VPC con este rango, ya que esto podría crear un conflicto y provocar que no se pueda acceder a ella. WorkSpaces Además, no modifique ni elimine ninguna de las interfaces de red conectadas a una WorkSpace, ya que esto también podría provocar que quedara inalcanzable. WorkSpace

Rango de direcciones IP de interfaz de red de administración y puertos

El rango de direcciones IP de interfaz de red de administración es 198.19.0.0/16. Todos los puertos siguientes deben estar abiertos en la interfaz de red de administración: WorkSpaces

- TCP de entrada en el puerto 8300. Se utiliza para establecer la conexión de streaming.
- TCP saliente en el puerto 3128. Se utiliza para la administración de. WorkSpaces

- TCP de entrada en los puertos 8000 y 8443. Se utilizan para la gestión del WorkSpaces.
- UDP de entrada en el puerto 8300. Se utiliza para establecer la conexión de streaming por UDP.

Limite el rango de entrada de la interfaz de red de administración a 198.19.0.0/16.

> **Note**
>
> Para los WorkSpaces grupos de Windows BYOL de Amazon DCV, los rangos de direcciones IP 10.0.0.0/8 se utilizan en todas las regiones. AWS Estos rangos de IP se suman al bloque CIDR /16 que elija para administrar el tráfico en sus grupos BYOL. WorkSpaces

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

No lo desactive. IPv6 Si la desactiva IPv6, WorkSpaces las agrupaciones no funcionarán correctamente. Para obtener información sobre la configuración IPv6 para Windows, consulte la Guía de configuración IPv6 en Windows para usuarios avanzados.

> **Note**
>
> WorkSpaces Los grupos dependen de los servidores DNS de la VPC para devolver una respuesta de dominio inexistente (NXDOMAIN) para los nombres de dominio locales que no existen. Esto permite que la interfaz de red WorkSpaces administrada por Pools se comunique con los servidores de administración.
> Cuando crea un directorio con Simple AD, AWS Directory Service crea dos controladores de dominio que también funcionan como servidores DNS en su nombre. Como los controladores de dominio no proporcionan la respuesta de NXDOMAIN, no se pueden usar con WorkSpaces grupos.

Puertos de interfaz de red del cliente

- Para conectividad a Internet, los siguientes puertos deben estar abiertos a todos los destinos. Si utiliza un grupo de seguridad personalizado o modificado, es necesario añadir las reglas

manualmente. Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon VPC.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 4195

- Si lo une WorkSpaces a un directorio, los siguientes puertos deben estar abiertos entre la VPC de WorkSpaces Pools y los controladores de directorio.
  - 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 1024-65535: puertos dinámicos para RPC

  Para obtener una lista completa de puertos, consulte Requisitos de puertos de Active Directory y Active Directory Domain Services en la documentación de Microsoft.
- Todos WorkSpaces requieren que el puerto 80 (HTTP) esté abierto a la dirección IP `169.254.169.254` para permitir el acceso al servicio de EC2 metadatos. El rango de direcciones IP `169.254.0.0/16` está reservado para el uso del servicio WorkSpaces Pools para el tráfico de administración. Si no se excluye este rango, podrían producirse problemas de transmisión.

Conexiones de usuario a WorkSpaces grupos

Los usuarios pueden conectarse a WorkSpaces In WorkSpaces Pools a través del terminal de Internet público predeterminado.

De forma predeterminada, WorkSpaces Pools está configurado para enrutar las conexiones de streaming a través de la Internet pública. La conectividad a Internet es necesaria para autenticar a los usuarios y ofrecer los activos web que WorkSpaces Pools necesita para funcionar. Para que este tráfico sea posible, debe permitir los dominios enumerados en Dominios permitidos.

> **Note**
>
> Para la autenticación de los usuarios, WorkSpaces Pools es compatible con el lenguaje de marcado de aserciones de seguridad 2.0 (SAML 2.0). Para obtener más información, consulte Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos.

En los temas siguientes se proporciona información sobre cómo habilitar las conexiones de los usuarios a los grupos. WorkSpaces

Contenido

- Recomendaciones de ancho de banda
- Requisitos de dirección IP y puerto para dispositivos de usuario de WorkSpaces grupos
- Dominios permitidos

Recomendaciones de ancho de banda

Para optimizar el rendimiento de los WorkSpaces grupos, asegúrese de que el ancho de banda y la latencia de su red puedan satisfacer las necesidades de sus usuarios.

WorkSpaces Pools utiliza la visualización en la nube de escritorio (DCV) de NICE para permitir a los usuarios acceder a sus aplicaciones y transmitirlas de forma segura en diferentes condiciones de red. Para ayudar a reducir el consumo de ancho de banda, NICE DCV utiliza codificación y compresión de vídeo basada en H.264. Durante las sesiones de streaming, la salida visual de las aplicaciones se comprime y se transmite en streaming a los usuarios en una secuencia de píxeles cifrada mediante AES-256 a través de HTTPS. Una vez que se recibe la secuencia, se descifra y se emite en la pantalla local del usuario. Cuando los usuarios interactúan con sus aplicaciones de streaming, el protocolo NICE DCV captura su entrada y la devuelve a las aplicaciones de streaming a través de HTTPS.

Las condiciones de la red se miden constantemente durante este proceso y la información se envía a los WorkSpaces grupos. WorkSpaces Pools responde de forma dinámica a las condiciones cambiantes de la red cambiando la codificación de vídeo y audio en tiempo real para producir una transmisión de alta calidad para una amplia variedad de aplicaciones y condiciones de red.

El ancho de banda y la latencia recomendados para WorkSpaces las sesiones de streaming de Pools dependen de la carga de trabajo. Por ejemplo, un usuario que utiliza aplicaciones que realizan un

uso intensivo de gráficos llevar a cabo tareas de diseño asistido por computadora requerirá más ancho de banda y menor latencia que otro que utilice aplicaciones de productividad empresarial para escribir documentos.

La siguiente tabla proporciona orientación sobre el ancho de banda de red y la latencia recomendados para las sesiones de streaming de WorkSpaces Pools en función de las cargas de trabajo habituales.

Para cada carga de trabajo, la recomendación del ancho de banda se basa en lo que un usuario individual podría necesitar en un momento dado. La recomendación no refleja el ancho de banda necesario para un rendimiento sostenido. Cuando tan solo cambian algunos píxeles en la pantalla durante una sesión de streaming, el rendimiento sostenido es mucho menor. Aunque los usuarios que tienen menos ancho de banda disponible pueden utilizar aplicaciones de streaming, la velocidad de fotogramas o la calidad de imagen podrían no ser óptimas.

Carga de trabajo	Descripción	Ancho de banda recomendado por usuario	Latencia máxima recomendada de ida y vuelta
Aplicaciones de línea de negocio	Aplicaciones de redacción de documento s, utilidades de análisis de base de datos	2 Mbps	< 150 ms
Aplicaciones de gráficos	Aplicaciones de modelado y diseño asistido por computadora, edición fotográfica y de vídeo	5 Mbps	< 100 ms
Alta fidelidad	Conjuntos de datos de alta fidelidad o asignaciones en varios monitores	10 Mbps	< 50 ms

Requisitos de dirección IP y puerto para dispositivos de usuario de WorkSpaces grupos

WorkSpaces Los dispositivos de los usuarios de Pools requieren acceso saliente a los puertos 443 (TCP) y 4195 (UDP) cuando utilizan los puntos finales de Internet y, si utilizan servidores DNS para la resolución de nombres de dominio, el puerto 53 (UDP).

- El puerto 443 se utiliza para la comunicación HTTPS entre los dispositivos de los usuarios de WorkSpaces Pools y WorkSpaces cuando se utilizan los puntos finales de Internet. Normalmente, cuando los usuarios finales navegan por la web durante las sesiones de streaming, el navegador web selecciona de forma aleatoria un puerto de origen en el intervalo alto para tráfico de streaming. Debe asegurarse de que el tráfico de retorno a este puerto esté permitido.
- El puerto 4195 se utiliza para la comunicación UDP HTTPS entre los dispositivos de los usuarios de WorkSpaces Pools y WorkSpaces cuando se utilizan los puntos finales de Internet. Esto solo se admite actualmente en el cliente nativo de Windows. UDP no es compatible si se utilizan puntos de conexión de VPC.
- El puerto 53 se utiliza para la comunicación entre los dispositivos de los usuarios de WorkSpaces Pools y sus servidores DNS. El puerto debe estar abierto a las direcciones IP para sus servidores DNS de modo que los nombres de dominio público se puedan resolver. Si no se utilizan servidores DNS para resolver nombres de dominio, este puerto es opcional.

Dominios permitidos

Para que los usuarios de WorkSpaces Pools puedan acceder WorkSpaces, debe permitir varios dominios de la red desde los que los usuarios inicien el WorkSpaces acceso a. Para obtener más información, consulte Requisitos de dirección IP y puerto para WorkSpaces Personal. Tenga en cuenta que la página especifica que se aplica a WorkSpaces Personal, pero también se aplica a los WorkSpaces grupos.

> **Note**
>
> Si su bucket de S3 tiene un carácter "." en el nombre, el dominio utilizado es `https://s3.<aws-region>.amazonaws.com`. Si su bucket de S3 no tiene un carácter "." en el nombre, el dominio utilizado es `https://<bucket-name>.s3.<aws-region>.amazonaws.com`.

Crear una WorkSpaces piscina

Configure y cree un grupo desde el que se inicien y transmitan las aplicaciones de los usuarios.

> **Note**
>
> Debe crear un directorio antes de crear un WorkSpaces grupo. Para obtener más información, consulte Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos.

Cómo configurar y crear un grupo

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, selecciona Pool WorkSpaces.
3. Elija Crear WorkSpaces grupos.
4. En Incorporación (opcional), puedes elegir Recomendarme opciones en función de mi caso de uso para obtener recomendaciones sobre el tipo de opciones WorkSpace que quieres usar. Puedes saltarte este paso si sabes que quieres usar WorkSpaces Pools.
5. En Configurar WorkSpaces, introduzca los siguientes detalles:
   - En Nombre, introduzca un nombre identificador único para el grupo. No se admiten caracteres especiales.
   - En Descripción, escriba una descripción para el grupo (como máximo 256 caracteres).
   - En Bundle, elige entre las siguientes opciones el tipo de paquete que quieres usar para tu WorkSpaces.
     - Usa un WorkSpaces paquete base: elige uno de los paquetes del menú desplegable. Para obtener más información sobre el tipo de paquete que ha seleccionado, elija Detalles del paquete. Para comparar los paquetes que se ofrecen para los grupos, elija Comparar todos los paquetes.
     - Utilizar su propio paquete personalizado: elija un paquete que haya creado anteriormente. Para crear un paquete personalizado, consulte Crea una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal.
   - Para el modo en funcionamiento, elija una de las siguientes opciones para configurar la disponibilidad inmediata del grupo y la forma de pago:
     - AutoStop— A las instancias de Pools se les factura una tarifa de uso por hora, en función del paquete elegido, solo para las instancias que están conectadas a los usuarios. A las

instancias del grupo que no están conectadas a los usuarios se les factura una tarifa por hora baja por instancia detenida. Cuando los usuarios inician su sesión, comienzan a transmitir después de una espera de 1 a 2 minutos.

- AlwaysOn— A todas las instancias de grupos que se estén ejecutando se les factura la tarifa de uso por hora aplicable, incluso cuando los usuarios no estén conectados. Este modo es el mejor para los usuarios que no quieren esperar a que comience la transmisión.

- En Duración máxima de la sesión en minutos, seleccione el tiempo máximo que puede permanecer activa una sesión de streaming. Si hay usuarios que siguen estando conectados a una instancia de streaming cinco minutos antes de que se alcance este límite, se les pedirá que guarden cualquier documento que tengan abierto antes de desconectarlos. Una vez transcurrido este tiempo, la instancia se termina y se sustituye por una nueva instancia. La duración máxima de la sesión que puedes configurar en la consola de WorkSpaces Pools es de 5760 minutos (96 horas). La duración máxima de sesión que puede establecer mediante la API y la CLI de WorkSpaces Pools es de 432 000 segundos (120 horas).
- En Tiempo de espera de desconexión en minutos, elija la cantidad de tiempo que una sesión de streaming permanece activa después de que los usuarios se hayan desconectado. Si los usuarios intentan volver a conectarse a la sesión de streaming después de una desconexión o interrupción de la red dentro de este intervalo de tiempo, se conectarán a la sesión anterior. De lo contrario, se conectan a una sesión nueva con una nueva instancia de streaming.
- Si un usuario finaliza la sesión eligiendo Finalizar sesión o Cerrar sesión en la barra de herramientas de WorkSpaces Pools, no se aplica el tiempo de espera de desconexión. sino que se pide al usuario que guarde cualquier documento que tenga abierto y, a continuación, se le desconecta inmediatamente de la instancia de streaming. La instancia que estaba utilizando el usuario termina.
- En Tiempo de espera de desconexión de inactividad en minutos, elija la cantidad de tiempo que los usuarios pueden estar inactivos antes de desconectarlos de su sesión de streaming y de que comience el intervalo de tiempo Tiempo de espera de desconexión en minutos. Se notificará a los usuarios antes de que se desconecten por inactividad. Si intentan volver a conectarse a la sesión de streaming antes de que haya transcurrido el intervalo de tiempo especificado en Tiempo de espera de desconexión en minutos, se conectan a su sesión anterior. De lo contrario, se conectan a una sesión nueva con una nueva instancia de streaming. Si este valor se establece en 0, se deshabilita. Cuando este valor está deshabilitado, los usuarios no desconectan por inactividad.

> **Note**
>
> Los usuarios se consideran inactivos cuando dejan de introducir datos a través del teclado o del ratón durante su sesión de streaming. En el caso de los grupos vinculados a un dominio, la cuenta regresiva para el tiempo de espera de desconexión por inactividad no comienza hasta que los usuarios inicien sesión con su contraseña de dominio de Active Directory o con una tarjeta inteligente. Las cargas y descargas de archivos, la entrada y salida de audio y los cambios de píxeles no se consideran actividad del usuario. Si los usuarios siguen estando inactivos después de que haya transcurrido el intervalo de tiempo de Tiempo de espera de desconexión de inactividad en minutos, se desconectan.

- En Políticas de capacidad programada (opcional), elija Añadir nueva capacidad de programación. Indique la fecha y hora de inicio y finalización del aprovisionamiento del número mínimo y máximo de instancias para el grupo en función del número mínimo previsto de usuarios simultáneos.
- En Políticas de escalado manual (opcional), especifique las políticas de escalado de los grupos que se usarán para aumentar y reducir la capacidad del grupo. Amplíe Políticas de escalado manual para añadir nuevas políticas de escalado.

> **Note**
>
> El tamaño del grupo está limitado en función de la capacidad mínima y máxima que haya especificado.

  - Seleccione Añadir nuevas políticas de escalado horizontal e introduzca los valores para añadir instancias específicas si la utilización de la capacidad especificada es inferior o superior al valor del umbral indicado.
  - Seleccione Añadir nuevas políticas de reducción horizontal e introduzca los valores para eliminar instancias específicas si la utilización de la capacidad especificada es inferior o superior al valor del umbral indicado.
- En Etiquetas, especifique el valor del par de claves que desee usar. Una clave puede ser una categoría general, como "proyecto", "propietario" o "entorno", con valores específicos asociados.

6. En la página Seleccionar directorio, elija el directorio que ha creado. Para crear un directorio, elija Crear directorio. Para obtener más información, consulte Administrar directorios para WorkSpaces grupos.
7. Elija Crear WorkSpace grupo.

Administrar WorkSpaces grupos

Un WorkSpaces grupo consiste WorkSpaces en ejecutar la imagen que usted especifique.

Contenido

- Modo de ejecución para WorkSpaces piscinas
- WorkSpaces Paquetes de piscinas
- Modificación de un grupo
- Eliminar un grupo
- Escalado automático para WorkSpaces piscinas

Modo de ejecución para WorkSpaces piscinas

El modo de funcionamiento de una WorkSpaces piscina determina su disponibilidad inmediata y la forma de pagarla. Puede elegir entre los siguientes modos de ejecución al crear un WorkSpaces grupo:

- AutoStop— A las instancias de un WorkSpaces grupo se les factura una tarifa de uso por hora en función del paquete elegido, solo para las instancias que están conectadas a los usuarios. A las instancias de un WorkSpaces grupo que no están conectadas a los usuarios se les factura una tarifa por hora baja por instancia detenida. Cuando los usuarios inician su sesión, comienzan a transmitir después de 1 o 2 minutos.
- AlwaysOn— A las instancias en ejecución de un WorkSpaces pool se les factura la tarifa de uso por hora aplicable, incluso cuando los usuarios no están conectados. Este modo es el mejor para los usuarios que no quieren esperar a que comience la transmisión.

Para obtener más información, consulte WorkSpaces Precios.

Contenido

- Modificar el modo de ejecución

Modificar el modo de ejecución

Puede cambiar entre los modos de ejecución cuando un WorkSpaces grupo está detenido.

Para modificar el modo de ejecución de un WorkSpaces grupo

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, selecciona WorkSpacesAgrupaciones.
3. Seleccione el WorkSpaces grupo que desee modificar y confirme que está detenido. Luego, elija Acciones y Modificar el modo de ejecución.
4. Seleccione el nuevo modo de ejecución AlwaysOno y AutoStop, a continuación, elija Guardar.

Para modificar el modo de ejecución de un WorkSpaces grupo mediante el AWS CLI

- Utilice el comando update-workspaces-pool.

WorkSpaces Paquetes de piscinas

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 disponibles WorkSpaces se denominan paquetes públicos. Para obtener más información sobre los distintos paquetes públicos disponibles WorkSpaces, consulta Amazon WorkSpaces Bundles.

En la siguiente tabla se 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
Windows Server 2019	Incluido	DCV	Valor, estándar, rendimiento, potencia, PowerPro
Windows Server 2022	Incluido	DCV	Estándar, rendimiento, potencia, gráficos. PowerPro G4dn, .G4dn GraphicsPro

> **Note**
>
> - No se garantiza que las versiones del sistema operativo que el vendedor ya no admite funcionen ni cuentan con soporte técnico. AWS

Modificación de un grupo

Tras crear un WorkSpaces grupo, puede modificar lo siguiente:

- ID de directorio (si el WorkSpaces grupo está detenido)
- Detalles básicos
- Paquete y hardware
- Configuración de desconexión de sesiones
- Capacidad y escalado
- Actividades de escalado
- Etiquetas

Para modificar un WorkSpaces grupo

1. En el panel de navegación WorkSpaces, elija Pools.
2. Seleccione el grupo que desea modificar.
3. Vaya a la sección que desee modificar y elija Editar.
4. Realice las modificaciones pertinentes y seleccione Guardar.

Eliminar un grupo

Puede eliminar grupos para liberar recursos y evitar cargos no deseados en la cuenta. Se recomienda detener los grupos en ejecución que no se utilicen.

Para eliminar un grupo

1. En el panel de navegación WorkSpaces, elija Pools.
2. Seleccione el grupo que desee detener y, a continuación, elija Detener. Un grupo tarda unos cinco minutos en detenerse.

3. Cuando el estado del grupo sea Detenido, seleccione Eliminar.

Escalado automático para WorkSpaces piscinas

Auto Scaling le permite cambiar automáticamente el tamaño de los grupos para que la oferta de instancias disponibles se equipare con la demanda de los usuarios. El tamaño del grupo determina el número de usuarios que pueden transmitir de forma simultánea. Se requiere una instancia para cada sesión de usuario. Puede especificar la capacidad del grupo en cuanto a las instancias. Según las configuraciones del grupo y las políticas de escalado automático, estará disponible la cantidad requerida de instancias. Puede definir políticas de escalado para que el tamaño del grupo se ajuste automáticamente en función de una serie de métricas de uso, así como optimizar la cantidad de instancias disponibles de forma que se equipare con la demanda de los usuarios. Además, puede desactivar el escalado automático de forma que el tamaño del grupo en ejecución se mantenga fijo.

> **Note**
>
> - A medida que desarrolle su plan de escalado de WorkSpaces grupos, asegúrese de que la configuración de la red cumpla con sus requisitos.
> - Cuando usa el escalado, trabaja con la API del Auto Scaling de aplicaciones. Para que Auto Scaling funcione correctamente con WorkSpaces Pools, Application Auto Scaling requiere permiso para describir y actualizar sus pools y describir sus CloudWatch alarmas de Amazon, además de permisos para modificar la capacidad de su pool en su nombre.

Los siguientes temas proporcionan información que le ayudará a entender y utilizar Auto Scaling for WorkSpaces Pools.

Contenido

- Conceptos de escalado
- Administración del escalado de grupos mediante la consola
- Administración del escalado de grupos mediante la AWS CLI
- Recursos adicionales

Conceptos de escalado

WorkSpaces El escalado de piscinas lo proporciona Application Auto Scaling. Para obtener más información, consulte la Referencia de la API de Application Auto Scaling.

Para utilizar Auto Scaling with WorkSpaces Pools de forma eficaz, debe comprender los siguientes términos y conceptos.

Número mínimo capacity/minimum de sesiones de usuario para el grupo

El número mínimo de instancias. El número de instancias no puede ser inferior a este valor y las políticas de escalado no escalarán el grupo por debajo de este valor. Por ejemplo, si establece la capacidad mínima para un grupo en 2, el grupo nunca tendrá menos de dos instancias.

Número máximo capacity/maximum de sesiones de usuario para el grupo

El número máximo de instancias. El número de instancias no puede ser superior a este valor y las políticas de escalado no escalarán el grupo por encima de este valor. Por ejemplo, si establece la capacidad máxima para un grupo en 10, el grupo nunca tendrá más de 10 instancias.

Capacidad de sesión de usuario deseada

El número total de sesiones que se están ejecutando o están pendientes. Esto representa el número total de sesiones de transmisión simultáneas que puede admitir el grupo en un estado estable.

Acción de la política de escalado

La acción que las políticas de escalado llevan a cabo en el grupo cuando se cumple la opción Condición de la política de escalado. Puede elegir una acción basándose en % capacity o number of instance(s). Por ejemplo, si la opción Capacidad de sesión de usuario deseada está establecida en 4 y la opción Acción de la política de escalado está establecida en “Añadir un 25 % de capacidad”, la opción Capacidad de sesión de usuario deseada aumentará un 25 % a 5 cuando se cumpla la opción Condición de la política de escalado.

Condición de la política de escalado

La condición que desencadena la acción establecida en Scaling Policy Action. Esta condición incluye una métrica de la política de escalado, un operador de comparación y un umbral. Por ejemplo, para escalar un grupo cuando su utilización sea superior al 50 %, la condición de la política de escalado debe ser “Si utilización de la capacidad > 50 %”.

Métrica de la política de escalado

La política de escalado se basa en esta métrica. Las siguientes métricas están disponibles para políticas de escalado:

Capacity Utilization

El porcentaje de instancias de un grupo que se están utilizando. Puede utilizar esta métrica para escalar el grupo en función de su uso. Por ejemplo, Scaling Policy Condition: "si la condición es Capacity Utilization < 25%", llevar a cabo la acción Scaling Policy Action: "Remove 25 % capacity".

Capacidad disponible

El número de instancias del grupo que están disponibles para los usuarios. Puede utilizar esta métrica para mantener un búfer de capacidad disponible que permita a los usuarios iniciar sesiones de streaming. Por ejemplo, Scaling Policy Condition: "si la condición es Available Capacity < 5", llevar a cabo la acción Scaling Policy Action: "Add 5 instance(s)".

Errores de capacidad insuficiente

Número de solicitudes de sesión que se han rechazado por falta de capacidad. Esta métrica se puede utilizar para aprovisionar nuevas instancias para los usuarios que no pueden iniciar sesiones de streaming debido a la falta de capacidad. Por ejemplo, Scaling Policy Condition: "si la condición es Insufficient Capacity Error > 0", llevar a cabo la acción Scaling Policy Action: "Add 1 instance(s)".

Administración del escalado de grupos mediante la consola

Puede configurar y administrar el escalado mediante la WorkSpaces consola de una de las dos maneras siguientes: durante la creación del grupo o en cualquier momento, mediante la pestaña Grupos. Después de crear los grupos, vaya a la pestaña Políticas de escalado para añadir nuevas políticas de escalado para el grupo. Para obtener más información, consulte Crear una WorkSpaces piscina.

Para entornos de usuario que varían en número, defina políticas de escalado que permitan controlar cómo responderá el escalado a la demanda. Si prevé un número fijo de usuarios o existen otros motivos para deshabilitar el escalado, puede configurar el grupo con un número fijo de instancias para las sesiones de usuario.

Para ello, defina la capacidad mínima en el número de instancias que desee. Ajuste la capacidad máxima para que sea al menos el valor de la capacidad mínima. Esto evita errores de validación,

pero, en última instancia, se ignorará la capacidad máxima, ya que el grupo no se escalará. A continuación, elimine todas las políticas de escalado de ese grupo.

Cómo definir una política de escalado de grupos con la consola

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación, elija Pools (Grupos).
3. Seleccione el grupo.
4. En la página de ese grupo, desplácese hacia abajo hasta la capacidad y el escalado.
5. Seleccione Editar.
6. Edite las políticas existentes, establezca los valores deseados en su campo y seleccione Guardar. Los cambios de la política entrarán en vigor transcurridos unos minutos.
7. También puede añadir nuevas políticas de capacidad y escalado. Para ello, seleccione Añadir nueva capacidad de programación, Añadir nueva política de escalado horizontal o Añadir nueva política de reducción horizontal.

A continuación se muestra un ejemplo gráfico de la actividad de escalado cuando cinco usuarios se conectan al grupo y, a continuación, se desconectan. Este ejemplo es de un grupo en el que se utilizan los siguientes valores de la política de escalado:

- Capacidad mínima = 10
- Capacidad máxima = 50
- Escalar horizontalmente = si la utilización de la capacidad del grupo es superior al 75 %, añada cinco instancias
- Reducir horizontalmente = si la utilización de la capacidad del grupo es inferior al 25 %, elimine seis instancias

> **Note**
>
> Durante la sesión, se iniciarán cinco instancias nuevas durante un evento de escalado horizontal. Durante un evento de reducción horizontal, se recuperarán seis instancias si hay suficientes instancias sin sesiones de usuario activas y si el número total de instancias no cae por debajo de la capacidad mínima de 10 instancias. Las instancias con sesiones de usuario en ejecución no se recuperarán. Solo se recuperarán las instancias en las que no se esté ejecutando ninguna sesión de usuario.

Administración del escalado de grupos mediante la AWS CLI

Puede configurar y administrar el escalado de grupos mediante la AWS Command Line Interface (AWS CLI). Para funciones más avanzadas, como configurar los tiempos de enfriamiento de escalado vertical y horizontal, utilice la CLI. AWS Antes de ejecutar los comandos de las políticas de escalado, debe registrar el grupo como objetivo escalable. Para ello, utilice el siguiente comando: register-scalable-target

```
aws application-autoscaling register-scalable-target
  --service-namespace workspaces \
  --resource-id workspacespool/PoolId \
  --scalable-dimension workspaces:workspacespool:DesiredUserSessions \
  --min-capacity 1 --max-capacity 5
```

Ejemplos

- Ejemplo 1: Aplicación de una política de escalado basada en la utilización de la capacidad
- Ejemplo 2: Aplicación de una política de escalado basada en los errores de capacidad insuficiente
- Ejemplo 3: Aplicación de una política de escalado basada en la utilización de baja capacidad
- Ejemplo 4: Cambio de la capacidad del grupo en función de una programación
- Ejemplo 5: Aplicación de una política de escalado de seguimiento de destino

Ejemplo 1: Aplicación de una política de escalado basada en la utilización de la capacidad

Este ejemplo de AWS CLI establece una política de escalado que amplía un grupo en un 25% si la utilización es superior o igual al 75%.

El siguiente put-scaling-policycomando define una política de escalado basada en la utilización:

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
utilization.json
```

El contenido del archivo `scale-out-utilization.json` es el siguiente:

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
```

```
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 25
            }
        ],
        "Cooldown": 120
    }
}
```

Si el comando es correcto, el resultado es similar al siguiente, aunque algunos datos son exclusivos de cada cuenta y región. En este ejemplo, el identificador de la política es `e3425d21-16f0-d701-89fb-12f98dac64af`.

```
{"PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:e3425d21-16f0-d701-89fb-12f98dac64af:resource/workspaces/workspacespool/PoolId:policyName/scale-out-utilization-policy"}
```

Ahora, configure una CloudWatch alarma para esta política. Utilice los nombres, la región, el número de cuenta y el identificador de la política que se le apliquen a usted. Puede utilizar el ARN de la política devuelto por el comando anterior para el parámetro `-- alarm-actions`.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Available User Session Capacity exceeds 75 percent" \
--metric-name AvailableUserSessionCapacity \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 300 \
--threshold 75 \
--comparison-operator GreaterThanOrEqualToThreshold \
--dimensions "Name=WorkSpaces pool ID,Value=PoolId" \
--evaluation-periods 1 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

Ejemplo 2: Aplicación de una política de escalado basada en los errores de capacidad insuficiente

Este ejemplo de AWS CLI configura una política de escalado que escala el grupo en 1 si el grupo devuelve un `InsufficientCapacityError` error.

El comando siguiente define una política de escalado basada en la capacidad insuficiente:

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
capacity.json
```

El contenido del archivo `scale-out-capacity.json` es el siguiente:

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "ChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 1
            }
        ],
        "Cooldown": 120
    }
}
```

Si el comando es correcto, el resultado es similar al siguiente, aunque algunos datos son exclusivos de cada cuenta y región. En este ejemplo, el identificador de la política es `f4495f21-0650-470c-88e6-0f393adb64fc`.

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:f4495f21-0650-470c-88e6-0f393adb64fc:resource/
workspaces/workspacespool/PoolId:policyName/scale-out-insufficient-capacity-policy"}
```

Ahora, configure una CloudWatch alarma para esta política. Utilice los nombres, la región, el número de cuenta y el identificador de la política que se le apliquen a usted. Puede utilizar el ARN de la política devuelto por el comando anterior para el parámetro `--alarm-actions`.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when out of capacity is > 0" \
--metric-name InsufficientCapacityError \
--namespace AWS/WorkSpaces \
--statistic Maximum \
--period 300 \
--threshold 0 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 1 --unit Count \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

Ejemplo 3: Aplicación de una política de escalado basada en la utilización de baja capacidad

En este AWS CLI ejemplo, se establece una política de escalado que se amplía en el grupo para reducir la capacidad real cuando ésta `UserSessionsCapacityUtilization` es baja.

El comando siguiente define una política de escalado basada en la capacidad excesiva:

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-in-
capacity.json
```

El contenido del archivo `scale-in-capacity.json` es el siguiente:

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalUpperBound": 0,
                "ScalingAdjustment": -25
            }
        ],
        "Cooldown": 360
```

```
    }
}
```

Si el comando es correcto, el resultado es similar al siguiente, aunque algunos datos son exclusivos de cada cuenta y región. En este ejemplo, el identificador de la política es `12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90`.

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90:resource/
workspaces/workspacespool/PoolId:policyName/scale-in-utilization-policy"}
```

Ahora, configure una CloudWatch alarma para esta política. Utilice los nombres, la región, el número de cuenta y el identificador de la política que se le apliquen a usted. Puede utilizar el ARN de la política devuelto por el comando anterior para el parámetro `--alarm-actions`.

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Capacity Utilization is less than or equal to 25
 percent" \
--metric-name UserSessionsCapacityUtilization \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 120 \
--threshold 25 \
--comparison-operator LessThanOrEqualToThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 10 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

Ejemplo 4: Cambio de la capacidad del grupo en función de una programación

El cambio de la capacidad del grupo en función de una programación le permite escalar la capacidad del grupo como respuesta a los cambios previstos en la demanda. Por ejemplo, al inicio de un día laborable, es posible que espere que un determinado número de usuarios solicite conexiones de streaming al mismo tiempo. Para cambiar la capacidad de su grupo según un cronograma, puede usar la acción de la PutScheduledActionAPI Application Auto Scaling o el comando put-scheduled-action AWS CLI.

Antes de cambiar la capacidad de la piscina, puede enumerar la capacidad de la piscina actual mediante el comando WorkSpaces describe-workspaces-pools AWS CLI.

```
aws workspaces describe-workspaces-pools --name PoolId
```

La capacidad actual del grupo tendrá un aspecto similar al del siguiente resultado (tal y como se muestra en formato JSON):

```
{
    "CapacityStatus": {
        "AvailableUserSessions": 1,
        "DesiredUserSessions": 1,
        "ActualUserSessions": 1,
        "ActiveUserSessions": 0
    },
}
```

A continuación, utilice el comando `put-scheduled-action` para crear una acción programada para cambiar la capacidad del grupo. Por ejemplo, el siguiente comando cambia la capacidad mínima a 3 y la capacidad máxima a 5 cada día a las 9:00 h.

> **Note**
>
> Para expresiones cron, especifique cuándo realizar la acción en UTC. Para obtener más información, consulte Expresiones Cron.

```
aws application-autoscaling put-scheduled-action --service-namespace workspaces \
--resource-id workspacespool/PoolId \
--schedule="cron(0 9 * * ? *)" \
--scalable-target-action MinCapacity=3,MaxCapacity=5 \
--scheduled-action-name ExampleScheduledAction \
--scalable-dimension workspaces:workspacespool:DesiredUserSessions
```

Para confirmar que la acción programada para cambiar la capacidad de la piscina se creó correctamente, ejecute el describe-scheduled-actionscomando.

```
aws application-autoscaling describe-scheduled-actions --service-namespace workspaces
 --resource-id workspacespool/PoolId
```

Si la acción programada se ha creado correctamente, el resultado tiene un aspecto similar al siguiente.

```
{
    "ScheduledActions": [
        {
            "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
            "Schedule": "cron(0 9 * * ? *)",
            "ResourceId": "workspacespool/ExamplePool",
            "CreationTime": 1518651232.886,
            "ScheduledActionARN": "<arn>",
            "ScalableTargetAction": {
                "MinCapacity": 3,
                "MaxCapacity": 5
            },
            "ScheduledActionName": "ExampleScheduledAction",
            "ServiceNamespace": "workspaces"
        }
    ]
}
```

Para obtener más información, consulte Escalado programado en la Guía del usuario de Auto Scaling de aplicaciones.

Ejemplo 5: Aplicación de una política de escalado de seguimiento de destino

Con el escalado de seguimiento de destino puede especificar un nivel de utilización de capacidad para el grupo.

Al crear una política de escalado de seguimiento de objetivos, Application Auto Scaling crea y gestiona automáticamente CloudWatch las alarmas que activan la política de escalado. La política de escalado amplía o reduce la capacidad en función de las necesidades para mantener el uso de la capacidad en el valor objetivo especificado o en un valor próximo. Para garantizar la disponibilidad de la aplicación, el grupo se escala horizontalmente de un modo proporcional a la métrica tan rápido como puede, pero se reduce horizontalmente de un modo más gradual.

El siguiente put-scaling-policycomando define una política de escalado y seguimiento de objetivos que intenta mantener el 75% de utilización de la capacidad de un WorkSpaces grupo.

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://config.json
```

El contenido del archivo `config.json` es el siguiente:

```
{
  "PolicyName":"target-tracking-scaling-policy",
  "ServiceNamespace":"workspaces",
  "ResourceId":"workspacespool/PoolId",
  "ScalableDimension":"workspaces:workspacespool:DesiredUserSessions",
  "PolicyType":"TargetTrackingScaling",
  "TargetTrackingScalingPolicyConfiguration":{
    "TargetValue":75.0,
    "PredefinedMetricSpecification":{
      "PredefinedMetricType":"WorkSpacesAverageUserSessionsCapacityUtilization"
    },
    "ScaleOutCooldown":300,
    "ScaleInCooldown":300
  }
}
```

Si el comando es correcto, el resultado es similar al siguiente, aunque algunos datos son exclusivos de cada cuenta y región. En este ejemplo, el identificador de la política es 6d8972f3-efc8-437c-92d1-6270f29a66e7.

```
{
    "PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:6d8972f3-
efc8-437c-92d1-6270f29a66e7:resource/workspaces/workspacespool/PoolId:policyName/
target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca"
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d"
        }
    ]
```

```
}
```

Para obtener más información, consulte Políticas de escalado de seguimiento de destino en la Guía del usuario de Auto Scaling de aplicaciones.

Recursos adicionales

Para obtener más información sobre el uso de los comandos de la AWS CLI o las acciones de la API de Application Auto Scaling, consulte los siguientes recursos:

- Sección application-autoscaling de la Referencia de comandos de la AWS CLI
- Referencia de la API de Application Auto Scaling
- Guía del usuario de la aplicación Auto Scaling

Uso de Active Directory con WorkSpaces grupos

Puede unir sus WorkSpaces grupos de Windows WorkSpaces a dominios de Microsoft Active Directory y usar sus dominios de Active Directory existentes, ya sean basados en la nube o locales, para lanzar instancias de streaming unidas a un dominio. También puede usarlo AWS Directory Service for Microsoft Active Directory, también conocido como AWS Managed Microsoft AD, para crear un dominio de Active Directory y usarlo como soporte para los recursos de sus WorkSpaces grupos. Para obtener más información sobre el uso AWS Managed Microsoft AD, consulte Microsoft Active Directory en la Guía de AWS Directory Service administración.

Al unir WorkSpaces grupos a su dominio de Active Directory, puede:

- Ofrecer acceso a los usuarios y a las aplicaciones a los recursos de Active Directory, como las impresoras y el uso compartido de archivos de las sesiones de transmisión.
- Utilizar las configuraciones de políticas de grupo que están disponibles en la consola de administración de políticas de grupo (GPMC) para definir la experiencia del usuario final.
- Transmita aplicaciones en streaming que requieren que los usuarios se autentiquen mediante sus credenciales de inicio de sesión de Active Directory.
- Aplique sus políticas empresariales de cumplimiento y seguridad a sus WorkSpaces WorkSpaces grupos internos.

Contenido

- Información general de los dominios de Active Directory

- Antes de empezar a usar Active Directory con WorkSpaces grupos
- Autenticación basada en certificados
- WorkSpaces Administración de grupos de Active Directory
- Más información

Información general de los dominios de Active Directory

El uso de dominios de Active Directory con WorkSpaces grupos requiere comprender cómo funcionan juntos y las tareas de configuración que deberá realizar. Deberá completar las tareas siguientes:

1. Configurar las opciones de la política de grupo según sea necesario para definir la experiencia de usuario final y los requisitos de seguridad de las aplicaciones.
2. Cree el directorio unido a un dominio en WorkSpaces Pools.
3. Cree la aplicación WorkSpaces Pools en el proveedor de identidades SAML 2.0 y asígnela a los usuarios finales directamente o mediante grupos de Active Directory.

Flujo de autenticación del usuario

1. El usuario navega a `https://applications.exampleco.com`. La página de inicio de sesión solicita autenticación al usuario.
2. El servicio de federación solicita autenticación al almacén de identidades de la organización.
3. El almacén de identidades autentica al usuario y devuelve la respuesta de autenticación al servicio de federación.
4. Una vez realizada la autenticación, el servicio de federación publica la declaración de SAML en el navegador del usuario.
5. El navegador del usuario publica la afirmación SAML en el punto de conexión SAML de inicio de AWS sesión (). `https://signin.aws.amazon.com/saml` AWS Sign-In recibe la solicitud de SAML, la procesa, autentica al usuario y reenvía el token de autenticación al servicio Pools. WorkSpaces
6. Con el token de autenticación de AWS, WorkSpaces Pools autoriza al usuario y presenta las aplicaciones al navegador.
7. El usuario elige una aplicación y, según el método de autenticación de inicio de sesión de Windows que esté habilitado en el directorio WorkSpaces Pools, se le pide que introduzca su

contraseña de dominio de Active Directory o que elija una tarjeta inteligente. Si ambos métodos de autenticación están habilitados, el usuario puede elegir si desea introducir la contraseña de su dominio o utilizar la tarjeta inteligente. También puede utilizarse la autenticación basada en certificados para autenticar a los usuarios, lo que elimina la pregunta.

8. El sistema se pone en contacto con el controlador de dominio para la autenticación del usuario.
9. Una vez acabada la autenticación en el dominio, la sesión del usuario comienza con la conectividad de dominio.

Desde el punto de vista del usuario, este proceso es transparente. El usuario comienza navegando hasta el portal interno de la organización y es redirigido a un portal de WorkSpaces Pools, sin tener que introducir AWS las credenciales. Solo se necesita una contraseña de dominio de Active Directory o credenciales de tarjeta inteligente.

Antes de que un usuario pueda iniciar este proceso, debe configurar Active Directory con los derechos y la configuración de política de grupo necesarios y crear un directorio de grupos unido a un dominio WorkSpaces .

Antes de empezar a usar Active Directory con WorkSpaces grupos

Antes de usar dominios de Microsoft Active Directory con WorkSpaces grupos, tenga en cuenta los siguientes requisitos y consideraciones.

Contenido

- Entorno de dominio de Active Directory
- Unidos a un dominio en grupos WorkSpaces WorkSpaces
- Configuración de la política de grupo
- Autenticación con tarjeta inteligente

Entorno de dominio de Active Directory

- Debe tener un dominio de Microsoft Active Directory al que unir su WorkSpaces. Si no tiene un dominio de Active Directory o quiere usar su entorno local de Active Directory, consulte Servicios de dominio de Active Directory en la AWS nube: implementación de referencia de inicio rápido.
- Debe tener una cuenta de servicio de dominio con permisos para crear y administrar objetos informáticos en el dominio que desee utilizar con los WorkSpaces grupos. Para obtener

información, consulte How to Create a Domain Account in Active Directory en la documentación de Microsoft.

Al asociar este dominio de Active Directory a los WorkSpaces grupos, proporcione el nombre y la contraseña de la cuenta de servicio. WorkSpaces Pools usa esta cuenta para crear y administrar los objetos de computadora del directorio. Para obtener más información, consulte Concesión de permisos para crear y administrar objetos de equipo de Active Directory.

- Al registrar su dominio de Active Directory en WorkSpaces Pools, debe proporcionar un nombre distintivo de la unidad organizativa (OU). Cree una OU con este fin. El contenedor de ordenadores predeterminado no es una unidad organizativa y los WorkSpaces grupos no pueden usarlo. Para obtener más información, consulte Obtención del nombre distinguido de la unidad organizativa.
- Los directorios que planea usar con los WorkSpaces grupos deben estar accesibles a través de sus nombres de dominio completos (FQDNs) a través de la nube privada virtual (VPC) en la que WorkSpaces se lanza. Para obtener más información, consulte Active Directory and Active Directory Domain Services Port Requirements en la documentación de Microsoft.

Unidos a un dominio en grupos WorkSpaces WorkSpaces

Se requiere una federación de usuarios basada en SAML 2.0 para la transmisión de aplicaciones desde dominios unidos a un dominio. WorkSpaces Además, debe utilizar una imagen de Windows que permita vincular a un dominio de Active Directory. Todas las imágenes públicas publicadas a partir del 24 de julio de 2017 incluido admiten la incorporación a un dominio de Active Directory.

Configuración de la política de grupo

Compruebe la configuración de las siguientes opciones de política de grupo. Si es necesario, actualice la configuración tal como se describe en esta sección para que no impida que los WorkSpaces grupos autentiquen e inicien sesión a los usuarios de su dominio. De lo contrario, cuando los usuarios intenten iniciar sesión, es posible que WorkSpaces el inicio de sesión no se realice correctamente. En su lugar, aparece un mensaje en el que se notifica a los usuarios que «se ha producido un error desconocido».

- Configuración del equipo > Plantillas administrativas > Componentes de Windows > Opciones de inicio de sesión de Windows > Deshabilitar o habilitar la secuencia de atención segura: establezca en Habilitado para la opción Servicios.

- Computer Configuration > Administrative Templates > System > Logon > Exclude credential providers: compruebe que el CLSID siguiente no figure en la lista: `e7c1bab5-4b49-4e64-a966-8d99686f8c7c`
- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Logon > Interactive Logon: Message text for users attempting to log on: establezca esta opción en No definido.
- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Logon > Interactive Logon: Message title for users attempting to log on: establezca esta opción en No definido.

Autenticación con tarjeta inteligente

WorkSpaces Pools admite el uso de contraseñas de dominio de Active Directory o tarjetas inteligentes, como las tarjetas inteligentes Common Access Card (CAC) y Personal Identity Verification (PIV), para iniciar sesión con Windows en Pools. WorkSpaces WorkSpaces Para obtener información sobre cómo configurar el entorno de Active Directory para permitir el inicio de sesión con tarjetas inteligentes mediante entidades de certificación de terceros (CAs), consulte las Directrices para habilitar el inicio de sesión con tarjetas inteligentes con entidades de certificación de terceros en la documentación de Microsoft.

Autenticación basada en certificados

Puede usar la autenticación basada en certificados con WorkSpaces grupos unidos a Microsoft Active Directory. Esto elimina la solicitud al usuario de la contraseña del dominio de Active Directory cuando el usuario inicia sesión. 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 AWS Private Certificate Authority (AWS Private CA) recursos de su. Cuenta de AWS Con AWS Private CA, puede crear jerarquías de entidades de certificación (CA) privadas, incluidas las de raíz y subordinada. CAs También puede crear su propia

jerarquía de CA y emitir certificados desde ella que autentiquen a los usuarios internos. Para obtener más información, consulte Qué es. AWS Private CA

Cuando utiliza una CA AWS privada para la autenticación basada en certificados, WorkSpaces Pools solicita automáticamente los certificados de sus usuarios al reservar la sesión para cada uno de los miembros de un WorkSpace WorkSpaces grupo. Autentica a los usuarios en Active Directory con una tarjeta inteligente virtual proporcionada con los certificados.

La autenticación basada en certificados se admite en los grupos unidos a un dominio que ejecutan instancias de Windows WorkSpaces .

Contenido

- Requisitos previos
- Habilitación de la autenticación basada en certificados
- Administración de la autenticación basada en certificados
- Habilitación del uso compartido entre cuentas de una CA privada

Requisitos previos

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

1. Configure su directorio de WorkSpaces grupos con la integración de SAML 2.0 para utilizar la autenticación basada en certificados. Para obtener más información, consulte Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos.

   > **Note**
   >
   > No habilite la opción Inicio de sesión con tarjeta inteligente en el grupo si desea utilizar la autenticación basada en certificados.

2. Configurar el atributo `userPrincipalName` en su declaración de SAML. Para obtener más información, consulte Paso 7: crear aserciones para la respuesta de autenticación de SAML.
3. Configurar el atributo `ObjectSid` en su declaración de SAML. Puede usar este atributo para realizar una asignación sólida con el usuario de Active Directory. La autenticación basada en certificados produce un error si el atributo `ObjectSid` no coincide con el identificador de seguridad (SID) de Active Directory del usuario especificado en el `NameID`de SAML_Subject. Para

obtener más información, consulte Paso 7: crear aserciones para la respuesta de autenticación de SAML.

> **Note**
>
> Según Microsoft KB5 014754, el `ObjectSid` atributo será obligatorio para la autenticación basada en certificados después del 10 de septiembre de 2025.

4. Agregue el permiso `sts:TagSession` a la política de confianza de roles de IAM que utiliza con su configuración de SAML 2.0. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de AWS Identity and Access Management . Este permiso es necesario para usar la autenticación basada en certificados. Para obtener más información, consulte Paso 5: crear un rol de IAM de federación de SAML 2.0.
5. Cree una autoridad de certificación (CA) AWS privada mediante una CA privada, si no tiene ninguna configurada con su Active Directory. AWS Se requiere una CA privada para usar la autenticación basada en certificados. Para obtener más información, consulte Planning your AWS Private CA deployment en la Guía del usuario de AWS Private Certificate Authority . La siguiente configuración de CA AWS privada es común en muchos casos de uso de la autenticación basada en certificados:
   - Opciones de tipo de CA
     - 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.
     - Jerarquía de un solo nivel con una CA raíz: elija una CA subordinada para integrarla con una jerarquía de CA existente.
   - Opciones de algoritmos de clave: RSA 2048
   - Opciones de nombre distintivo por asunto: utilice las opciones más adecuadas para identificar esta CA en el almacén de entidades emisoras de certificados raíz de confianza de Active Directory.
   - 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 WorkSpaces grupos internos como desde el controlador WorkSpaces de dominio. Esto requiere acceso no autenticado al bucket de Amazon S3 configurado para entradas de CRL de CA AWS privadas

o a una CloudFront distribución con acceso al bucket de Amazon S3 si bloquea el acceso público. Para obtener más información sobre estas opciones, consulte Planning a certificate revocation list (CRL) en la Guía del usuario de AWS Private Certificate Authority .

6. Etiquete su CA privada con una clave que permita designar la CA `euc-private-ca` para su uso con la autenticación basada en certificados de WorkSpaces Pools. Esta clave no requiere ningún valor. Para obtener más información, consulte Managing tags for your private CA en la Guía del usuario de AWS Private Certificate Authority .
7. La autenticación basada en certificados utiliza tarjetas inteligentes virtuales para iniciar sesión. Para obtener más información, consulte Guidelines for enabling smart card logon with third-party certification authorities. Siga estos pasos:
   a. 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 Servicios de certificados de Active Directory configurada en su Active Directory, inscribirá automáticamente los controladores de dominio con certificados que permiten 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 utilizas Microsoft AD AWS administrado, puedes configurar los servicios de certificación en una EC2 instancia de Amazon que cumpla con los requisitos de certificados de controlador de dominio. Consulte Implementación de Active Directory en una nueva Amazon Virtual Private Cloud para ver, por ejemplo, las implementaciones de Microsoft AD AWS gestionado configuradas con Active Directory Certificate Services.
> Con los servicios de certificados AWS gestionados de Microsoft AD y Active Directory, también debe crear reglas de salida desde el grupo de seguridad de VPC del controlador hasta la instancia de EC2 Amazon que ejecuta Certificate Services. El grupo de seguridad debe tener acceso al puerto 135 de TCP y a los puertos 49152 a 65535 para habilitar la inscripción automática de certificados. La EC2 instancia de Amazon 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 de Microsoft AD AWS administrado, consulte Configurar las subredes y grupos de seguridad de la VPC.

b. En la consola de CA AWS privada, o con el SDK o la CLI, exporte el certificado de CA privada. Para obtener más información, consulte Exportación de un certificado privado.

c. Publique la CA privada 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 cualquiera *<path>**<file>* y ejecute los siguientes comandos como administrador de dominio. También puede usar la política de grupo y la herramienta Microsoft PKI Health Tool (PKIView) 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 de CA privada. Según la configuración de replicación de Active Directory, la CA puede tardar varios minutos en publicar en los controladores de dominio y WorkSpaces en los WorkSpaces grupos.

> **Note**
>
> Active Directory debe distribuir automáticamente la CA a las autoridades emisoras de certificados raíz de confianza y NTAuth las almacena WorkSpaces en WorkSpaces grupos cuando se unen al dominio.

> **Note**
>
> 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.

Para habilitar la autenticación basada en certificados

1. Abre la WorkSpaces consola en la versión 2/homehttps://console.aws.amazon.com/workspaces/.
2. Elija Directorios en el panel de navegación.
3. Seleccione la pestaña Directorios de grupos.
4. Elija el directorio que desea configurar.
5. Elija Editar en la sección Autenticación de la página.
6. Seleccione Editar la autenticación basada en certificados en la sección Autenticación basada en certificados de la página.
7. Elija Habilitar la autenticación basada en certificados.
8. Elija el certificado en la lista desplegable Autoridad de certificación (CA) privada de AWS Certificate Manager (ACM).

   Para que aparezca en la lista desplegable, debe almacenar la CA privada en la misma Cuenta de AWS y Región de AWS. También debe etiquetar la CA privada con una clave denominada `euc-private-ca`.
9. Configure el registro del directorio como alternativa. La opción de alternativa permite a los usuarios iniciar sesión con la contraseña de dominio de AD si la autenticación basada en certificados no se realiza correctamente. Esto solo se recomienda en los casos en que los usuarios conozcan las contraseñas de sus dominios. Cuando la opción de alternativa está desactivada, una sesión puede desconectar al usuario si se produce una pantalla de bloqueo o si se cierra sesión en Windows. Si la opción de alternativa está activada, la sesión solicita al usuario su contraseña de dominio de AD.
10. Seleccione Save.

Ya está habilitada la autenticación basada en certificados. Cuando los usuarios se autentiquen con SAML 2.0 en un directorio de WorkSpaces grupos utilizando el dominio unido WorkSpaces, ya no recibirán la solicitud de la contraseña del dominio. Los usuarios verán el mensaje Conexión con autenticación basada en certificados al conectarse a una sesión habilitada para la autenticación basada en certificados.

Administración de la autenticación basada en certificados

Tras habilitar la autenticación basada en certificados, revise las siguientes tareas.

Certificado de CA privada

En una configuración típica, el certificado de CA privada tiene un período de validez de 10 años. 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, consulte Managing the private CA lifecycle.

Certificados de usuario final

Los certificados de usuario final emitidos por la autenticación basada en certificados de AWS Private Certificate Authority for WorkSpaces Pools no requieren renovación ni revocación. Estos certificados son de corta duración. WorkSpaces Pools emite automáticamente un nuevo certificado para cada nueva sesión o cada 24 horas para las sesiones de larga duración. La sesión de WorkSpaces Pools regula el uso de estos certificados de usuario final. Si finaliza una sesión, WorkSpaces Pools deja de usar ese certificado. Estos certificados de usuario final tienen un período de validez más corto que una distribución AWS Private Certificate Authority 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

Puede utilizarlos CloudTrail para grabar las llamadas a la API realizadas por WorkSpaces grupos a una CA privada. Para obtener más información, consulte ¿Qué es AWS CloudTrail? en la Guía del AWS CloudTrail usuario y Uso CloudTrail en la Guía del AWS Private Certificate Authority usuario. En el historial de CloudTrail eventos, puedes ver los nombres de GetCertificatelos IssueCertificateeventos de la fuente de eventos acm-pca.amazonaws.com creados con el nombre de usuario de Pools. WorkSpaces EcmAssumeRoleSession Estos eventos se registrarán para cada solicitud de autenticación basada en un certificado de Pools. WorkSpaces Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Habilitación del uso compartido entre cuentas de una CA privada

El uso compartido entre cuentas de una CA privada (PCA) ofrece la posibilidad de conceder permisos para que otras cuentas usen una CA centralizada. La CA puede generar y emitir certificados mediante AWS Resource Access Manager (RAM) para administrar los permisos. Esto elimina la necesidad de una CA privada en cada cuenta. El uso compartido entre cuentas privadas de CA se puede utilizar con la autenticación basada en certificados (CBA) AppStream 2.0 dentro de la misma. Región de AWS

Para usar un recurso de CA privada compartido con WorkSpaces Pools CBA, complete los siguientes pasos:

1. Configure la CA privada para la CBA de forma centralizada. Cuenta de AWS Para obtener más información, consulte the section called “Autenticación basada en certificados”.
2. Comparta la CA privada con el recurso Cuentas de AWS donde los recursos de WorkSpaces Pools utilizan la CBA. Para ello, siga los pasos de Cómo usar la AWS RAM para compartir su cuenta cruzada de ACM Private CA. No necesita completar el paso 3 para crear un certificado. Puede compartir la CA privada con Cuentas de AWS individuales o compartirla a través de AWS Organizations. Si comparte con cuentas individuales, debe aceptar la CA privada compartida en su cuenta de recursos mediante la AWS Resource Access Manager consola o. APIs

   Al configurar el recurso compartido, confirme que el AWS Resource Access Manager recurso compartido 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 servicio de WorkSpaces Pools al emitir los certificados CBA.
3. Una vez que el recurso se haya compartido correctamente, podrá ver la CA privada compartida mediante la consola de Private CA en la cuenta de recursos.
4. Utilice la API o la CLI para asociar el ARN de CA privado con el CBA en el directorio WorkSpaces de grupos. En este momento, la consola de WorkSpaces Pools no admite la selección de una CA privada compartida. ARNs Para obtener más información, consulta la referencia de la API WorkSpaces de Amazon Service.

WorkSpaces Administración de grupos de Active Directory

La configuración y el uso de Active Directory con WorkSpaces grupos implican las siguientes tareas administrativas.

Tareas

- Concesión de permisos para crear y administrar objetos de equipo de Active Directory
- Obtención del nombre distinguido de la unidad organizativa
- Concesión de derechos de administrador local para imágenes personalizadas
- Bloqueo de la sesión en streaming cuando el usuario está inactivo
- Configuración de WorkSpaces grupos para usar confianzas de dominio

Concesión de permisos para crear y administrar objetos de equipo de Active Directory

Para permitir que los WorkSpaces grupos realicen operaciones con objetos informáticos de Active Directory, necesita una cuenta con permisos suficientes. Como práctica recomendada, use una cuenta que tenga solo los privilegios mínimos necesarios. Los permisos mínimos de la unidad organizativa (OU) de Active Directory son los siguientes:

- Crear objeto equipo
- Cambio de contraseña
- Restablecer contraseña
- Escribir descripción

Antes de configurar los permisos, primero tendrá que hacer lo siguiente:

- Obtenga acceso a un equipo o una EC2 instancia que esté unida a su dominio.
- Instalar el complemento MMC Usuarios y equipos de Active Directory. Para obtener más información, consulte Installing or Removing Remote Server Administration Tools for Windows 7 en la documentación de Microsoft.
- Inicie sesión como usuario de dominio con los permisos adecuados para modificar la configuración de seguridad de la OU.
- Cree o identifique al usuario, la cuenta de servicio o el grupo al que se delegarán permisos.

Para configurar permisos mínimos

1. Abra Active Directory Users and Computers (Usuarios y equipos de Active Directory) en el dominio o en el controlador de dominio.

2. En el panel de navegación de la izquierda, seleccione la primera OU para la que se proporcionarán privilegios de unión al dominio, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Delegate Control (Delegar control).
3. En la página Delegation of Control Wizard, elija Next, Add.
4. En Seleccionar usuarios, equipos o grupos, seleccione el usuario, la cuenta de servicio o el grupo previamente creados y, a continuación, elija Aceptar.
5. En la página Tareas que se delegarán, elija Crear una tarea personalizada para delegar y luego elija Siguiente.
6. Elija Only the following objects in the folder, Computer objects.
7. Elija Create selected objects in this folder, Next.
8. En Permissions, elija Read, Write, Change Password, Reset Password, Next.
9. En la página Completing the Delegation of Control Wizard, verifique la información y elija Finish.
10. Repite los pasos 2 a 9 para cualquier otra OUs persona que requiera estos permisos.

Si ha delegado permisos en un grupo, cree una cuenta de usuario o de servicio con una contraseña segura y añada dicha cuenta al grupo. Esta cuenta tendrá entonces los privilegios suficientes para conectarla WorkSpaces al directorio. Utilice esta cuenta al crear la configuración del directorio de WorkSpaces grupos.

Obtención del nombre distinguido de la unidad organizativa

Al registrar su dominio de Active Directory en WorkSpaces Pools, debe proporcionar un nombre distintivo de la unidad organizativa (OU). Cree una OU con este fin. El contenedor de ordenadores predeterminado no es una unidad organizativa y los WorkSpaces grupos no pueden usarlo. En el siguiente procedimiento se muestra cómo obtener este nombre.

> **Note**
>
> El nombre distinguido debe comenzar con **OU=** o no podrá usarse para objetos de equipo.

Antes de realizar este procedimiento, deberá hacer lo siguiente:

- Obtenga acceso a un equipo o una EC2 instancia que esté unida a su dominio.

- Instalar el complemento MMC Usuarios y equipos de Active Directory. Para obtener más información, consulte Installing or Removing Remote Server Administration Tools for Windows 7 en la documentación de Microsoft.
- Inicie sesión como usuario de dominio con los permisos adecuados para leer las propiedades de seguridad de la OU.

Para buscar el nombre distinguido de una OU

1. Abra Active Directory Users and Computers (Usuarios y equipos de Active Directory) en el dominio o en el controlador de dominio.
2. En View, asegúrese de que la opción Advanced Features esté habilitada.
3. En el panel de navegación izquierdo, seleccione la primera unidad organizativa que desee utilizar para los objetos del WorkSpaces ordenador, abra el menú contextual (haga clic con el botón derecho) y, a continuación, elija Propiedades.
4. Elija Attribute Editor.
5. En Attributes, para distinguishedName, elija View.
6. En Value (Valor), seleccione el nombre distinguido, abra el menú contextual y elija Copy (Copiar).

Concesión de derechos de administrador local para imágenes personalizadas

De forma predeterminada, los usuarios de dominio de Active Directory no tienen derechos de administrador local para las imágenes. Para conceder estos derechos, utilice las preferencias de la política de grupo del directorio, o manualmente mediante la cuenta de administrador local de una imagen. La concesión de derechos de administrador local a un usuario del dominio le permite instalar aplicaciones y crear imágenes personalizadas en los WorkSpaces grupos.

Contenido

- Uso de las preferencias de la política de grupo
- Utilice el grupo de administradores local del WorkSpace para crear imágenes

Uso de las preferencias de la política de grupo

Puede utilizar las preferencias de la política de grupo para conceder derechos de administrador local a usuarios o grupos de Active Directory y a todos los objetos de equipo de la OU especificada. Los

usuarios o grupos de Active Directory a los que desea conceder permisos de administrador local deben existir previamente. Para utilizar las preferencias de la política de grupo, primero tendrá que hacer lo siguiente:

- Obtenga acceso a un ordenador o a una EC2 instancia que esté unida a su dominio.
- Instale el complemento MMC de la consola de administración de políticas de grupo (GPMC). Para obtener más información, consulte Installing or Removing Remote Server Administration Tools for Windows 7 en la documentación de Microsoft.
- Inicie sesión como usuario del dominio con permisos para crear objetos de política de grupo (GPOs). Enlace GPOs al correspondiente OUs.

Para utilizar las preferencias de la política de grupo para conceder permisos de administrador local

1. En el directorio o en un controlador de dominio, abra el símbolo del sistema como administrador, escriba `gpmc.msc` y, a continuación, pulse INTRO.
2. En el árbol de la consola de la izquierda, seleccione la OU donde creará el nuevo GPO o usará uno ya existente y, a continuación, realice una de las operaciones siguientes:
   - Cree un nuevo GPO; para ello, abra el menú contextual (haga clic con el botón derecho) y elija Create a GPO in this domain and link it here (Crear un GPO en este dominio y vincularlo aquí). En Name, proporcione un nombre descriptivo para este GPO.
   - Seleccione un GPO existente.
3. Abra el menú contextual del GPO y elija Edit (Editar).
4. En el árbol de la consola, elija Computer Configuration (Configuración del equipo), Preferences (Preferencias), Windows Settings (Configuración de Windows), Control Panel Settings (Configuración del panel de control) y Local Users and Groups (Usuarios y grupos locales).
5. Seleccione Local Users and Groups (Usuarios y grupos locales), abra el menú contextual y elija New (Nuevo), Local Group (Grupo local).
6. En Action, elija Update.
7. En Group name, elija Administrators (built-in).
8. En Miembro, elija Agregar... y especifique los usuario o grupos de Active Directory a los que se asignarán derechos de administrador local en la instancia en streaming. En Action, seleccione Add to this group y, a continuación, OK.
9. Para aplicar este GPO a otro OUs, seleccione la OU adicional, abra el menú contextual y elija Vincular un GPO existente.

10. Desplácese para encontrar el nombre del GPO nuevo o ya existente especificado en el paso 2 y, a continuación, elija OK (Aceptar).
11. Repita los pasos 9 y 10 para ver otros OUs que deban tener esta preferencia.
12. Elija OK (Aceptar) para cerrar el cuadro de diálogo New Local Group Properties (Propiedades de nuevo grupo local).
13. Elija OK (Aceptar) de nuevo para cerrar la GPMC.

Para aplicar la nueva preferencia al GPO, detenga y reinicie los constructores de imágenes o las flotas en ejecución. Los usuarios y grupos de Active Directory que ha especificado en el paso 8 obtienen automáticamente derechos de administrador local para los constructores de imágenes y las flotas de la OU a la que está vinculado el GPO.

Utilice el grupo de administradores local del WorkSpace para crear imágenes

Si desea conceder a los usuarios o grupos de Active Directory derechos de administrador local para una imagen, puede añadir manualmente estos usuarios o grupos al grupo de administradores locales de la imagen.

Los usuarios o grupos de Active Directory a los que se conceden derechos de administrador local deben existir ya.

1. Conéctate al WorkSpace que utilizas para crear imágenes. WorkSpace Debe estar en ejecución y unido a un dominio.
2. Elija Start (Inicio), Administrative Tools (Herramientas administrativas) y, a continuación, haga doble clic en Computer Management (Administración de equipos).
3. En el panel de navegación izquierdo, seleccione Local Users and Groups y abra la carpeta Groups.
4. Abra el grupo Administrators y seleccione Add....
5. Seleccione todos los usuarios o grupos de Active Directory a los que se asignarán derechos de administrador local y elija OK. Elija OK (Aceptar) de nuevo para cerrar el cuadro de diálogo Administrator Properties (Propiedades de Administradores).
6. Cierre la utilidad Administración de equipos.
7. Para iniciar sesión como usuario de Active Directory y comprobar si ese usuario tiene derechos de administrador local WorkSpaces, seleccione Admin Commands, Cambie de usuario y, a continuación, introduzca las credenciales del usuario correspondiente.

Bloqueo de la sesión en streaming cuando el usuario está inactivo

WorkSpaces Los grupos se basan en una configuración que se configura en la GPMC para bloquear la sesión de transmisión después de que el usuario esté inactivo durante un período de tiempo específico. Para utilizar la GPMC, primero tendrá que hacer lo siguiente:

- Obtenga acceso a un ordenador o a una EC2 instancia que esté unida a su dominio.
- Instalar la GPMC. Para obtener más información, consulte Installing or Removing Remote Server Administration Tools for Windows 7 en la documentación de Microsoft.
- Inicia sesión como usuario del dominio con permisos de creación GPOs. Enlace GPOs al enlace correspondiente OUs.

Para bloquear automáticamente la instancia de streaming cuando el usuario está inactivo

1. En el directorio o en un controlador de dominio, abra el símbolo del sistema como administrador, escriba `gpmc.msc` y, a continuación, pulse INTRO.
2. En el árbol de la consola de la izquierda, seleccione la OU donde creará el nuevo GPO o usará uno ya existente y, a continuación, realice una de las operaciones siguientes:
   - Cree un nuevo GPO; para ello, abra el menú contextual (haga clic con el botón derecho) y elija Create a GPO in this domain and link it here (Crear un GPO en este dominio y vincularlo aquí). En Name, proporcione un nombre descriptivo para este GPO.
   - Seleccione un GPO existente.
3. Abra el menú contextual del GPO y elija Edit (Editar).
4. En User Configuration (Configuración de usuario), expanda Policies (Políticas), Administrative Templates (Plantillas administrativas), Control Panel (Panel de control) y, a continuación, elija Personalization (Personalización).
5. Haga doble clic en Enable screen saver (Habilitar protector de pantalla).
6. En la opción de política Enable screen saver (Habilitar protector de pantalla), elija Enabled (Habilitado).
7. Seleccione Aplicar y, después, Aceptar.
8. Haga doble clic en Force specific screen saver (Aplicar un protector de pantalla específico).
9. En la opción de política Force specific screen saver (Aplicar un protector de pantalla específico), elija Enabled (Habilitado).

10. En Screen saver executable name (Nombre del ejecutable del protector de pantalla), escriba **`scrnsave.scr`**. Cuando esta opción está habilitada, el sistema muestra un protector de pantalla negro en el escritorio del usuario.
11. Seleccione Aplicar y, después, Aceptar.
12. Haga doble clic en Password protect the screen saver (Proteger el protector de pantalla mediante contraseña).
13. En la opción de política Password protect the screen saver (Proteger el protector de pantalla mediante contraseña), elija Enabled (Habilitado).
14. Seleccione Aplicar y, después, Aceptar.
15. Haga doble clic en Screen saver timeout (Tiempo de espera del protector de pantalla).
16. En la opción de política Screen saver timeout (Tiempo de espera del protector de pantalla), elija Enabled (Habilitado).
17. En Seconds (Segundos), especifique el tiempo que los usuarios deben estar inactivos antes de que se aplique el protector de pantalla. Para establecer el tiempo de inactividad en 10 minutos, especifique 600 segundos.
18. Seleccione Aplicar y, después, Aceptar.
19. En el árbol de la consola, en User Configuration (Configuración de usuario), expanda Policies (Políticas), Administrative Templates (Plantillas administrativas), System (Sistema) y, a continuación, elija Ctrl+Alt+Del Options (Opciones de Ctrl+Alt+Supr).
20. Haga doble clic en Remove Lock Computer (Quitar el bloqueo de equipos).
21. En la opción de política Remove Lock Computer (Quitar el bloqueo de equipos), elija Disabled (Deshabilitado).
22. Seleccione Aplicar y, después, Aceptar.

Configuración de WorkSpaces grupos para usar confianzas de dominio

WorkSpaces Los grupos admiten entornos de dominio de Active Directory en los que los recursos de red, como servidores de archivos, aplicaciones y objetos informáticos, residen en un dominio y los objetos de usuario residen en otro. No es necesario que la cuenta de servicio de dominio utilizada para las operaciones de objetos de equipo esté en el mismo dominio que los objetos WorkSpaces de equipo del grupo.

Cuando cree la configuración del directorio, especifique una cuenta de servicio con los permisos pertinentes para administrar objetos de equipo en el dominio de Active Directory donde se

encuentran los servidores de archivos, las aplicaciones, los objetos de equipo y otros recursos de red.

Las cuentas de Active Directory de usuario final deben tener los permisos "Allowed to Authenticate" para los elementos siguientes:

- WorkSpaces Agrupa los objetos del ordenador
- Controladores de dominio para el dominio

Para obtener más información, consulte Concesión de permisos para crear y administrar objetos de equipo de Active Directory.

Más información

Para obtener más información relacionada con este tema, consulte los siguientes recursos:

- Microsoft Active Directory: información sobre el uso AWS Directory Service.

Paquetes e imágenes para piscinas WorkSpaces

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 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 WorkSpace y lo has personalizado, puedes crear una imagen personalizada a partir de él WorkSpace para usarla con WorkSpaces Pool. WorkSpaces Pool no admite Linux.

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 crear nuevos WorkSpaces grupos para asegurarse de que los nuevos WorkSpaces del grupo tengan la misma configuración coherente (hardware y software).

Si necesita realizar actualizaciones de software o instalar software adicional en el suyo WorkSpaces, puede actualizar su paquete personalizado y usarlo para reconstruirlo WorkSpaces.

WorkSpaces Pools admite varios sistemas operativos (OS), protocolos de transmisión y paquetes diferentes. En la siguiente tabla se 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 del ciclo de vida o fecha de retirada
Windows Server 2019	Incluido	DCV	Valor, estándar, rendimiento, potencia, PowerPro	9 de enero de 2029
Windows Server 2022	Incluido	DCV	Estándar, rendimiento, potencia, gráficos. PowerPro G4dn, .G4dn GraphicsPro	14 de octubre de 2031

> **Note**
>
> - No se garantiza que las versiones del sistema operativo que el vendedor ya no admite funcionen ni cuentan con soporte técnico. AWS

Temas

- Opciones de paquetes para WorkSpaces piscinas
- Cree una imagen y un paquete personalizados para WorkSpaces piscinas
- Administra imágenes y paquetes personalizados para piscinas WorkSpaces
- Uso de scripts de sesión para administrar la experiencia de transmisión de los usuarios

Opciones de paquetes para WorkSpaces piscinas

Antes de seleccionar un paquete para usarlo con WorkSpaces Pool, asegúrese de que el paquete que desea seleccionar sea compatible con su WorkSpaces protocolo, sistema operativo, red y tipo de cómputo. 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. Para obtener más información sobre protocolos, consulte Protocolos para WorkSpaces uso personal. Para obtener más información sobre las redes, consulte Requisitos de red de clientes para WorkSpaces Personal.

Los siguientes paquetes públicos se pueden usar con WorkSpaces Pool. Para obtener información sobre los paquetes disponibles WorkSpaces, consulta Amazon WorkSpaces Bundles. Valor, estándar, rendimiento, potencia, PowerPro

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
- Correo electrónico

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
- Correo electrónico
- 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
- Correo electrónico
- 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.

PowerPro paquete

Este paquete está especialmente indicado para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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 Graphics.G4DN

Este paquete ofrece un alto nivel de rendimiento gráfico y un nivel moderado de rendimiento de CPU y memoria, WorkSpaces y es ideal para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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 (computer-aided design/computer-fabricación asistida)

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)

Este paquete ofrece un alto nivel de rendimiento gráfico, rendimiento de CPU y memoria para usted, WorkSpaces y es ideal para lo siguiente:

- Navegación web
- Procesamiento de textos
- Correo electrónico
- 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 (computer-aided design/computer-fabricación asistida)
- 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.

Cree una imagen y un paquete personalizados para WorkSpaces piscinas

WorkSpaces Pool solo admite imágenes y paquetes de Windows. Si ha lanzado un Windows o WorkSpace lo ha personalizado, puede crear una imagen personalizada y paquetes personalizados a partir de ella. 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.

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 uniforme (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**
>
> - Los volúmenes de almacenamiento de 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

- Requisitos para crear imágenes personalizadas de Windows
- 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 incluye con las imágenes WorkSpaces personalizadas de Windows

Requisitos para crear imágenes personalizadas de Windows

> **Note**
>
> Actualmente, Windows define 1 GB como 1.073.741.824 bytes. Debe asegurarse de que tengan más de 12.884.901.888 bytes (o 12 GiB) libres en la unidad C y 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.
- 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 y componentes del servicio necesarios”.
  - Windows PowerShell versión 3.0 o posterior
  - Servicios de Escritorio remoto
  - AWS Controladores PV
  - Administración remota de Windows (WinRM)
  - Agentes y controladores PCo IP de Teradici
  - Agentes y controladores de STXHD
  - AWS y certificados WorkSpaces
  - Agente de Skylight
- WorkSpaces Los grupos solo admiten un tamaño máximo de volumen raíz de paquete o imagen de 200 GB. Al crear una imagen personalizada de Windows, asegúrese de que esté por debajo del tamaño del volumen raíz de 200 GB.

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
- 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 la cuota, utilice el formulario de límites de WorkSpaces .
- Asegúrate de no intentar crear una imagen a partir de una imagen cifrada 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 Personal.
- En el caso de Windows WorkSpaces, no configure ningún objeto de política de grupo (GPOs) 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 cualquier personalización en el perfil de usuario y aplicarla después de la creación de la imagen. GPOs GPOs se pueden modificar o revertir fácilmente y, por lo tanto, son menos propensas a errores que las personalizaciones realizadas en el perfil de usuario predeterminado.
- Asegúrese de actualizar los controladores de dependencia de la red, como los controladores ENA y PV NVMe, en su WorkSpaces ordenador. Debe hacerlo al menos una vez cada seis meses.

Para obtener más información, consulte Install or upgrade Elastic Network Adapter (ENA) driver , Controladores NVMe de AWS for Windows instances y Upgrade PV drivers on Windows instances.

- Asegúrese de actualizar periódicamente los agentes EC2 Config, EC2 EC2 Launch y Launch V2 a las versiones más recientes. Debe hacerlo al menos una vez cada seis meses. Para obtener más información, consulta Update EC2 Config and EC2 Launch.

(Opcional) Paso 1: especificar un formato de nombre de equipo personalizado para la imagen

Para las imágenes WorkSpaces lanzadas a partir de sus imágenes personalizadas, puede especificar un prefijo personalizado para el formato del nombre del equipo en lugar de utilizar el formato de nombre del equipo predeterminado. De forma predeterminada, el formato del nombre del equipo para Windows 10 WorkSpaces es `DESKTOP-XXXXX` y para Windows 11 WorkSpaces,`WORKSPA-XXXXX`. Complete el siguiente procedimiento para especificar un prefijo personalizad.

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.

   Para acceder a la `C:` unidad 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 del equipo WorkSpaces creado a partir del paquete personalizado empezarán por`EC2AMAZ-`*`xxxxxxx`*.

Sysprep ignora los valores `<RegisteredOrganization>` y `<RegisteredOwner>` de la sección `<settings pass="oobeSystem">`.

4. Guarde los cambios en el archivo `Unattend.xml`.

Paso 2: ejecutar el comprobador de imágenes

Para confirmar que su Windows WorkSpace cumple los requisitos para la creación de imágenes, le recomendamos que ejecute la aplicación Image Checker. 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. El verificador de imágenes solo está disponible para Windows. WorkSpaces

> **Important**
>
> - WorkSpace Debe superar todas las pruebas realizadas por el verificador de imágenes antes de poder utilizarlo para la creación de imágenes.
> - Antes de ejecutar el comprobador de imágenes, compruebe que las actualizaciones acumulativas y de seguridad de Windows más recientes 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`. 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 que WorkSpace haya superado 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 Windows 10 que se han actualizado de una versión de Windows 10 a una versión más reciente de Windows 10 (una feature/version actualización 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 AWS Support Centro para reparar su EC2 Config o EC2 Launch.

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 el 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 la versión 1.2 de TLS debe estar habilitada

Para configurar SSL/TLS para Windows, consulte Cómo habilitar TLS 1.2 en la documentación de Microsoft Windows.

Solo puede existir un perfil de usuario en el 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 es compatible con los sistemas Windows que se han actualizado de una versión de Windows 10 a una versión más reciente de Windows 10 (una feature/version actualización de Windows).

Para crear imágenes, utilice una WorkSpace que no se haya actualizado a feature/version 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*" }
```

- Algunos objetos de política de grupo (GPOs) restringen el acceso a la huella digital del certificado RDP cuando lo solicitan el servicio EC2 Config o los scripts de EC2 lanzamiento durante la configuración de la instancia de Windows. Antes de intentar crear una imagen, muévela WorkSpace a una nueva unidad organizativa (OU) cuya herencia esté bloqueada y no GPOs se haya 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 la WorkSpace imagen, complete el siguiente procedimiento para crear la imagen y el paquete personalizados mediante la WorkSpaces consola. Para crear una imagen mediante programación, utilice la acción de la CreateWorkspaceImage API. Para obtener más información, consulta CreateWorkspaceImagela referencia de la WorkSpaces API de Amazon. 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.

Para crear una imagen personalizada y un paquete personalizado mediante la WorkSpaces consola

1. Si todavía está conectado a WorkSpace, desconéctese seleccionando Amazon WorkSpaces y Disconnect en la aplicación WorkSpaces cliente.
2. Abre la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
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.
5. Aparece un mensaje en el que se le pide que reinicie (reinicie) el suyo 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 en WorkSpaces Personal 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.

   No utilice el carácter especial de guión (`-`) en la descripción. Se producirá 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.
9. Introduzca un nombre y una descripción para el paquete y, a continuación, haga lo siguiente:
   - En el tipo de hardware del paquete, elige el hardware que se va a usar al iniciar el juego WorkSpaces desde este paquete personalizado.
   - Las combinaciones de tamaños disponibles por defecto para el volumen raíz son de 200 GB cada una WorkSpace.
10. Para confirmar que el paquete se ha creado, seleccione Paquetes y compruebe que el paquete aparezca en la lista.

¿Qué se incluye con las imágenes WorkSpaces personalizadas de Windows

Al crear una imagen desde un dispositivo Windows WorkSpace, se incluye todo el contenido de la `C` unidad.

- 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\

Administra imágenes y paquetes personalizados para piscinas WorkSpaces

El proceso de administración de imágenes y paquetes personalizados es el mismo entre WorkSpaces Personal y WorkSpaces Pool. Para obtener más información sobre cómo administrar las imágenes y los paquetes, consulte la siguiente documentación en la sección WorkSpaces Personal de esta guía:

> **Note**
>
> La principal diferencia entre los paquetes personalizados que puedes usar para WorkSpaces Personal y los que puedes usar para WorkSpaces Pool es el sistema operativo y el paquete público básico que se puede usar. Para ver los sistemas operativos y los paquetes compatibles con WorkSpaces Pool, consulte.
>
> 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 disponibles WorkSpaces se denominan paquetes públicos. Para obtener más información sobre los distintos paquetes públicos disponibles WorkSpaces, consulta Amazon WorkSpaces Bundles.
>
> En la siguiente tabla se proporciona información sobre las licencias, los protocolos de transmisión y los paquetes compatibles con cada sistema operativo.

Windows Server 2019	Incluido	DCV	Valor, estándar, rendimiento, potencia, PowerPro
Windows Server 2022	Incluido	DCV	Estándar, rendimiento, potencia, gráficos. PowerPro G4dn, .G4dn GraphicsPro
Sistema operativo	Licencias	Protocolos de transmisión	Paquetes compatibles

> **Note**
>
> - No se garantiza que las versiones del sistema operativo que el vendedor ya no admite funcionen ni cuentan con soporte técnico. AWS

- Actualizar un paquete personalizado para WorkSpaces Personal.
- Copiar una imagen personalizada en WorkSpaces Personal.
- Compartir o dejar de compartir una imagen personalizada en Personal WorkSpaces .
- Eliminar un paquete o una imagen personalizados en WorkSpaces Personal.

Uso de scripts de sesión para administrar la experiencia de transmisión de los usuarios

WorkSpaces Pool proporciona scripts de sesión en instancia. Puede utilizar estas secuencias de comandos para ejecutar sus propias secuencias de comandos personalizados cuando se produzcan eventos específicos en las sesiones de transmisión. Por ejemplo, puede usar scripts personalizados para preparar el entorno de WorkSpaces Pools antes de que comiencen las sesiones de streaming de sus usuarios. También puede usar secuencias de comandos personalizados para limpiar las instancias de transmisión después de que los usuarios hayan finalizado las sesiones de transmisión.

Los scripts de sesión se especifican dentro de una WorkSpace imagen. Estos scripts se ejecutan en el contexto del usuario o del sistema. Si los scripts de sesión utilizan la salida estándar para escribir los mensajes de información, error o depuración, estos se pueden guardar, si lo desea, en un bucket de Amazon S3 de su cuenta de Amazon Web Services.

Contenido

- Ejecución de scripts antes de que empiecen las sesiones de streaming
- Ejecución de scripts después de finalizar las sesiones de streaming
- Creación y especificación de scripts de sesión
- Archivo de configuración de scripts de sesión
- Uso de PowerShell archivos de Windows
- Registro de la salida de los scripts de sesión

- Uso del almacenamiento persistente con los scripts de sesión
- Habilitación del almacenamiento en buckets de Amazon S3 de los registros de los scripts de sesión

Ejecución de scripts antes de que empiecen las sesiones de streaming

Puede configurar los scripts para que se ejecuten durante un máximo de 60 segundos antes de se lancen las aplicaciones de los usuarios y empiecen las sesiones de streaming. Esto le permite personalizar el entorno de WorkSpaces Pools antes de que los usuarios comiencen a transmitir sus aplicaciones. Cuando se ejecutan scripts de sesión, aparece un rotador de carga a los usuarios. Cuando los scripts finalizan correctamente o transcurre el tiempo de espera máximo, empieza la sesión de streaming de los usuarios. Si los scripts no se completan correctamente, se muestra un mensaje de error para los usuarios. Sin embargo, no se impide a los usuarios que usen la sesión de streaming.

Cuando se especifica un nombre de archivo en una instancia de Windows, debe utilizar una doble barra oblicua inversa. Por ejemplo:

```
C:\\Scripts\\Myscript.bat
```

Si no utiliza una doble barra oblicua inversa, aparecerá un mensaje de error para informarle de que el archivo `.json` no tiene el formato correcto.

> **Note**
>
> Cuando los scripts finalizan correctamente, deben devolver un valor de 0. Si los scripts devuelven un valor distinto de 0, WorkSpaces muestra el mensaje de error al usuario.

Al ejecutar scripts antes de que comiencen las sesiones de transmisión, tiene lugar el siguiente proceso:

1. Los usuarios se conectan a un WorkSpace WorkSpaces grupo que no está unido a un dominio. Se conectan mediante SAML 2.0.
2. Tiene lugar uno de los siguientes procesos:
   - Si está habilitada la persistencia de la configuración de las aplicaciones para los usuarios, se descarga y monta el archivo VHD (disco duro virtual) de configuración de la aplicación, en el

que se almacenan las personalizaciones y los ajustes de Windows de los usuarios. En este caso se requiere un inicio de sesión de usuario de Windows.

Para obtener información sobre la persistencia de la configuración de las aplicaciones, consulte Habilite la persistencia de la configuración de la aplicación para los usuarios de sus WorkSpaces grupos.

- Si la persistencia de la configuración de las aplicaciones no está habilitada, el usuario de Windows ya ha iniciado sesión.

3. Se inician los scripts de sesión. Si el almacenamiento persistente está habilitado para los usuarios, también comienza el montaje del conector de almacenamiento. Para obtener más información acerca del almacenamiento persistente, consulte Habilitar y administrar el almacenamiento persistente para WorkSpaces grupos.

> **Note**
>
> No es preciso que haya finalizado el montaje del conector de almacenamiento para que se inicie la sesión de streaming. Si los scripts de sesión finalizan antes que el montaje del conector de almacenamiento, se inicia la sesión de streaming.
> Para obtener información acerca de la monitorización del estado del montaje de los conectores de almacenamiento, consulte Uso del almacenamiento persistente con los scripts de sesión.

4. Los scripts de sesión finalizan o se agota el tiempo de espera.
5. Se inicia la sesión de streaming de los usuarios.

Ejecución de scripts después de finalizar las sesiones de streaming

También puede configurar los scripts para que se ejecuten después de que finalicen las sesiones de streaming. Por ejemplo, puede ejecutar un script cuando los usuarios seleccionen Finalizar sesión en la barra de herramientas del WorkSpaces cliente o cuando alcancen la duración máxima permitida para la sesión. También puede usar estos scripts de sesión para limpiar el entorno de WorkSpaces antes de que termine una instancia de streaming. Por ejemplo, puede usar scripts para liberar los bloqueos de archivos o cargar los archivos de registro. Cuando se ejecutan scripts después de que finalicen las sesiones de streaming, tiene lugar el siguiente proceso:

1. Finaliza la sesión WorkSpaces de streaming de tus usuarios.
2. Se inician los scripts de finalización de sesión.

3. Los scripts de finalización de sesión finalizan o se agota el tiempo de espera.
4. Se produce el cierre de sesión del usuario de Windows.
5. En paralelo, se produce uno de los siguientes casos o ambos, si procede:
   - Si está habilitada la persistencia de la configuración de las aplicaciones para los usuarios, se desmonta y se carga a un bucket de Amazon S3 de la cuenta el archivo VHD de configuración de la aplicación, en el que se almacenan las personalizaciones y los ajustes de Windows de los usuarios.
   - Si el almacenamiento persistente está habilitado para los usuarios, el conector de almacenamiento lleva a cabo una sincronización final y se desmonta.
6. WorkSpace Se da por finalizada.

Creación y especificación de scripts de sesión

Complete el siguiente procedimiento para crear y especificar los scripts de sesión para WorkSpaces In a WorkSpaces Pool.

1. Conéctese a la ventana WorkSpaces desde la que va a crear una imagen personalizada.
2. Cree el directorio `/AWSEUC/SessionScripts` si aún no existe.
3. Cree un archivo de configuración `/AWSEUC/SessionScripts/config.json` si aún no existe, mediante la plantilla de configuración del script de sesión.
4. Navegue hasta `C:\AWSEUC\SessionScripts` y abra el archivo de configuración `config.json`.

   Para obtener información acerca de los parámetros de los scripts de sesión, consulte Archivo de configuración de scripts de sesión.
5. Una vez que haya terminado de realizar cambios, guarde y cierre el archivo `config.json`.
6. Complete los pasos para crear una imagen a partir de WorkSpace. Para obtener más información, consulte Cree una imagen y un paquete personalizados para WorkSpaces piscinas.

Archivo de configuración de scripts de sesión

Para localizar el archivo de configuración de los scripts de sesión en una instancia de Windows, vaya a `C:\AWSEUC\SessionScripts\config.json`. El archivo tiene el formato siguiente.

> **Note**
>
> El archivo de configuración tiene formato JSON. Compruebe que cualquier texto que escriba en este archivo esté en formato JSON válido.

```
{
  "SessionStart": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  },
  "SessionTermination": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  }
}
```

Puede utilizar los siguientes parámetros en el archivo de configuración de scripts de sesión.

`SessionStart/SessionTermination`

Los scripts de sesión que se ejecutarán en el evento de sesión apropiado basados en el nombre del objeto.

Tipo: cadena

Obligatorio: no

Valores permitidos: **`SessionStart`**, **`SessionTermination`**

`WaitingTime`

La duración máxima de los scripts de sesión, en segundos.

Tipo: entero

Obligatorio: no

Restricciones: la duración máxima es de 60 segundos. Si los scripts de sesión no han finalizado antes de cumplirse este plazo, se detendrán. Si necesita un script para continuar con la ejecución, láncelo como un proceso independiente.

`Executables`

Los detalles para ejecutar los scripts de sesión.

Tipo: cadena

Obligatorio: sí

Restricciones: el número máximo de scripts que se pueden ejecutar por evento de sesión es de 2 (uno para el contexto del usuario y otro para el contexto del sistema).

`Context`

El contexto en el que se ejecutará el script de sesión.

Tipo: cadena

Obligatorio: sí

Valores permitidos: **`user`**, **`system`**

`Filename`

La ruta completa del script de sesión que se ejecutará. Si no se especifica este parámetro, el script de sesión no se ejecuta.

Tipo: cadena

Obligatorio: no

Restricciones: la longitud máxima del nombre de archivo y su ruta completa es de 1000 caracteres.

Valores permitidos: **`.bat`**, **`.exe`** y **`.sh`**

> **Note**
>
> También puede utilizar PowerShell archivos de Windows. Para obtener más información, consulte Uso de PowerShell archivos de Windows.

`Arguments`

Los argumentos del script de sesión o del archivo ejecutable.

Tipo: cadena

Obligatorio: no

Limitaciones de longitud: la longitud máxima de 1000 caracteres.

`S3LogEnabled`

Cuando el valor de este parámetro se establece en **`True`**, se crea un bucket de S3 dentro de la cuenta de Amazon Web Services para almacenar los registros creados por el script de sesión. De forma predeterminada, este valor se establece en **`True`**. Para obtener más información, consulte la sección Registro de la salida de los scripts de sesión más adelante en este tema.

Tipo: Booleano

Obligatorio: no

Valores permitidos: **`True`**, **`False`**

Uso de PowerShell archivos de Windows

Para usar PowerShell archivos de Windows, especifique la ruta completa al PowerShell archivo en el `filename` parámetro:

```
"filename":
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
```

A continuación, especifique el script de sesión en el parámetro **`arguments`**:

```
"arguments": "-File \"C:\\path\\to\\session\\script.ps1\"",
```

Por último, compruebe que la política de PowerShell ejecución permita que el PowerShell archivo se ejecute.

Registro de la salida de los scripts de sesión

Cuando esta opción está habilitada en el archivo de configuración, WorkSpaces Pool captura automáticamente el resultado del script de sesión que se escribe en la salida estándar. Esta salida se carga en un bucket de Amazon S3 de la cuenta. Puede revisar los archivos de registro con fines de solución de problemas o depuración.

> **Note**
>
> Los archivos de registro se cargan cuando el script de sesión devuelve un valor o cuando transcurre el tiempo establecido en **`WaitingTime`**, lo que ocurra primero.

Uso del almacenamiento persistente con los scripts de sesión

Cuando el almacenamiento WorkSpaces persistente está activado, el almacenamiento comienza a montarse cuando se ejecutan los scripts de inicio de sesión. Si el script depende del montaje del almacenamiento persistente, puede esperar a que los conectores estén disponibles. WorkSpaces mantiene el estado de montaje de los conectores de almacenamiento del registro de Windows en Windows WorkSpaces, en la siguiente clave:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\AWSEUC\Storage\<provided user
                name>\<Storage connector>
```

Los valores de la clave del registro son los siguientes:

- Nombre de usuario proporcionado: el ID de usuario proporcionado a través del modo de acceso. Los modos de acceso y el valor de cada uno de ellos son los siguientes:
  - Grupo de usuarios: la dirección de correo electrónico del usuario
  - URL de streaming: el valor de UserID
  - SAML: el valor de NameID Si el nombre de usuario incluye una barra (por ejemplo, el SAMAccount nombre de un usuario de dominio), la barra se sustituye por un carácter «-».
- Conector de almacenamiento: el conector de la opción de almacenamiento persistente que se ha habilitado para el usuario. Los valores del conector de almacenamiento son los siguientes:
  - HomeFolder

Cada clave de registro del conector de almacenamiento contiene un valor MountStatusDWORD. En la siguiente tabla se enumeran los valores posibles de MountStatus.

> **Note**
>
> Para ver estas claves del Registro, debe tener Microsoft .NET Framework versión 4.7.2 o posterior instalado en la imagen.

Valor	Descripción
0	El conector de almacenamiento no se ha habilitado para este usuario
1	El montaje del conector de almacenamiento está en curso
2	El conector de almacenamiento se ha montado correctam ente
3	Se ha producido un error al montar el conector de almacenamiento

Valor	Descripción
4	El montaje del conector de almacenamiento está habilitado, pero aún no está montado

Habilitación del almacenamiento en buckets de Amazon S3 de los registros de los scripts de sesión

Cuando habilita el registro de Amazon S3 en la configuración del script de sesión, WorkSpaces Pool captura el resultado estándar del script de sesión. La salida se carga periódicamente en un bucket de S3 de la cuenta de Amazon Web Services. Para cada AWS región, WorkSpaces Pool crea un segmento en su cuenta que es exclusivo para su cuenta y la región.

No es necesario realizar ninguna tarea de configuración para administrar estos buckets de S3. El WorkSpaces servicio los gestiona en su totalidad. Los archivos de registro que se almacenan en cada bucket se cifran en tránsito mediante puntos de enlace SSL de Amazon S3 y en reposo, mediante claves de cifrado administradas por Amazon S3. Los nombres de los buckets siguen el formato específico que se indica a continuación:

```
wspool-logs-<region-code>-<account-id-without-hyphens>-random-identifier
```

<region-code>

Este es el código de AWS región en el que se crea el WorkSpaces pool con el almacenamiento en bucket de Amazon S3 habilitado para los registros de scripts de sesión.

<account-id-without-hyphens>

Su identificador de cuenta de Amazon Web Services. El ID aleatorio garantiza que no haya ningún conflicto con otros buckets en esa región. La primera parte del nombre del bucket, `wspool-logs`, no cambia entre cuentas o regiones.

Por ejemplo, si especifica los scripts de sesión en una imagen de la región EE.UU. Oeste (Oregón) (`us-west-2`) en el número de cuenta`123456789012`, WorkSpaces Pool crea un bucket de Amazon S3 en su cuenta de esa región con el nombre que se muestra. Este bucket solo lo puede eliminar un administrador con permisos suficientes.

```
wspool-logs-us-west-2-1234567890123-abcdefg
```

Al deshabilitar scripts de sesión, no se eliminarán los archivos de registro almacenados en el bucket de S3. Para eliminar permanentemente los archivos de registro, usted u otro administrador con los permisos adecuados deben hacerlo mediante la consola o la API de Amazon S3. WorkSpaces Pools añade una política de bucket que evita la eliminación accidental del bucket.

Cuando se habilitan los scripts de sesión, se crea una carpeta única para cada sesión de streaming que se inicia.

La ruta de la carpeta donde se almacenan los archivos de registro en el bucket de S3 en la cuenta utiliza la siguiente estructura:

```
<bucket-name>/<stack-name>/<fleet-name>/<access-mode>/<user-id-SHA-256-hash>/<session-id>/SessionScriptsLogs/<session-event>
```

<bucket-name>

El nombre del bucket de S3 en el que se almacenan los scripts de sesión. El formato del nombre se describe anteriormente en esta sección.

<stack-name>

El nombre de la pila de la que procede la sesión.

<fleet-name>

El nombre del WorkSpaces grupo en el que se ejecuta el script de la sesión.

<access-mode>

El método de identidad del usuario: `custom` para la WorkSpaces API o la CLI, `federated` para SAML y `userpool` para los usuarios del grupo de usuarios.

<user-id-SHA-256-hash>

El nombre de carpeta específico del usuario. Este nombre se ha creado utilizando una cadena hexadecimal con hasta SHA-256 en minúsculas generada a partir del identificador de usuario.

<session-id>

El identificador de la sesión de streaming del usuario. Cada sesión de streaming del usuario genera un identificador único.

<session-event>

El evento que generó el registro de script de sesión. Los valores del evento son: `SessionStart` y `SessionTermination`.

La siguiente estructura de carpetas de ejemplo se aplica a una sesión de streaming que se inicia desde la pila de prueba y la flota de prueba. La sesión utiliza la API del ID de usuario`testuser@mydomain.com`, a partir de un Cuenta de AWS ID de `123456789012` y el grupo de configuración `test-stack` de la región EE.UU. Oeste (Oregón) (`us-west-2`):

```
wspool-logs-us-west-2-1234567890123-abcdefg/test-stack/test-fleet/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13/05yd1391-4805-3da6-
f498-76f5x6746016/SessionScriptsLogs/SessionStart/
```

Esta estructura de carpetas de ejemplo contiene un archivo de registro para un script de inicio de sesión del contexto del usuario y un archivo de registro para un script de inicio de sesión del contexto del sistema, si procede.

Monitorización de WorkSpaces grupos

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de sus WorkSpaces grupos.

Contenido

- WorkSpaces Métricas y dimensiones de los pools

WorkSpaces Métricas y dimensiones de los pools

Amazon WorkSpaces envía la siguiente información sobre dimensiones y métricas de WorkSpaces Pools a Amazon CloudWatch.

WorkSpaces Pools envía las métricas CloudWatch una vez por minuto. El espacio de nombres de `AWS/Workspaces` incluye las siguientes métricas.

Métricas de uso de grupos

Métrica	Descripción
`ActiveUserSessionCapacity`	El número de sesiones de usuario que se utilizan actualmente para las sesiones de streaming. Unidades: recuento

Métrica	Descripción
	Estadísticas válidas: promedio, mínimo, máximo
`ActualUserSessionCapacity`	El número total de sesiones de grupos que están disponibles para la transmisión o que se están transmitiendo actualmente. `ActualUserSessionCapacity = AvailableUserSessionCapacity + ActiveUserSessionCapacity` Unidades: recuento Estadísticas válidas: promedio, mínimo, máximo
`AvailableUserSessionCapacity`	El número de sesiones de grupos inactivas disponibles actualmente para la transmisión del usuario. `AvailableUserSessionCapacity = ActualUserSessionCapacity - ActiveUserSessionCapacity` Unidades: recuento Estadísticas válidas: promedio, mínimo, máximo
`PendingUserSessionCapacity`	El número de sesiones que se están aprovisionando para el grupo. Representa el número adicional de sesiones de transmisión que el grupo puede admitir una vez finalizado el aprovisionamiento. Unidades: recuento Estadísticas válidas: promedio, mínimo, máximo

Métrica	Descripción
`UserSessionsCapacityUtilization`	El porcentaje de sesiones de un grupo que se están utilizando, mediante la siguiente fórmula. `UserSessionCapacityUtilization = (ActiveUserSessionCapacity / ActualUserSessionCapacity) * 100` La supervisión de esta métrica ayuda a tomar decisiones sobre cómo aumentar o disminuir el valor de la capacidad deseada de un grupo. Unidad: porcentaje Estadísticas válidas: promedio, mínimo, máximo
`DesiredUserSessionCapacity`	El número total de sesiones que se están ejecutando o están pendientes. Esto representa el número total de sesiones de transmisión simultáneas que puede admitir el grupo en un estado estable. `DesiredUserSessionCapacity = ActualUserSessionCapacity + PendingUserSessionCapacity` Unidades: recuento Estadísticas válidas: promedio, mínimo, máximo
`InsufficientCapacityError`	Número de solicitudes de sesión que se han rechazado por falta de capacidad. Puedes configurar alarmas para usar esta métrica para recibir notificaciones de los usuarios que esperan una sesión de streaming. Unidades: recuento Estadísticas válidas: promedio, mínimo, máximo, suma

Habilitar y administrar el almacenamiento persistente para WorkSpaces grupos

WorkSpaces Pools admite carpetas de inicio para el almacenamiento persistente. Como administrador de WorkSpaces grupos, debe saber cómo realizar las siguientes tareas para habilitar y administrar el almacenamiento persistente para sus usuarios.

Contenido

- Habilite y administre las carpetas principales para los usuarios de sus WorkSpaces grupos

Habilite y administre las carpetas principales para los usuarios de sus WorkSpaces grupos

Al habilitar las carpetas principales para los WorkSpaces grupos, los usuarios pueden acceder a una carpeta de almacenamiento persistente durante sus sesiones de streaming. Los usuarios no tienen que realizar ninguna configuración adicional para tener acceso a su carpeta de inicio. Los datos almacenados por los usuarios en sus carpetas de inicio se guardan automáticamente en un bucket de Amazon Simple Storage Service de la cuenta de Amazon Web Services y están disponibles para los usuarios en sesiones posteriores.

Los archivos y carpetas se cifran en tránsito mediante puntos de conexión SSL de Amazon S3. Los archivos y carpetas se cifran en reposo mediante claves de cifrado administradas por Amazon S3.

Las carpetas principales se almacenan WorkSpaces en WorkSpaces grupos en las siguientes ubicaciones predeterminadas:

- Para una sesión única, non-domain-joined Windows WorkSpaces: `C:\Users\PhotonUser\My Files\Home Folder`
- Windows unido a un dominio: WorkSpaces `C:\Users\%username%\My Files\Home Folder`

Como administrador, utilice la ruta aplicable si configura las aplicaciones para guardar en la carpeta de inicio. En algunos casos, los usuarios no podrán encontrar su carpeta de inicio, ya que algunas aplicaciones no reconocen el redireccionamiento que muestra la carpeta de inicio como una carpeta de nivel superior en el explorador de archivos. En este caso, los usuarios pueden tener acceso a su carpeta de inicio desplazándose a ese directorio en el explorador de archivos.

Contenido

- Archivos y directorios asociados a aplicaciones con un uso de computación intensivo
- Habilite las carpetas de inicio para los usuarios de sus WorkSpaces grupos
- Administrar las carpetas de inicio

Archivos y directorios asociados a aplicaciones con un uso de computación intensivo

Durante las sesiones de streaming de WorkSpaces Pools, guardar archivos y directorios de gran tamaño asociados a aplicaciones con un uso intensivo de recursos informáticos en un almacenamiento persistente puede llevar más tiempo que guardar los archivos y directorios necesarios para las aplicaciones de productividad básicas. Por ejemplo, es posible que las aplicaciones tarden más en guardar una gran cantidad de datos o en modificar con frecuencia los mismos archivos que si guardaran los archivos creados por aplicaciones que realicen una sola acción de escritura. También es posible que se tarde más en guardar muchos archivos pequeños.

Si sus usuarios guardan los archivos y directorios asociados a aplicaciones con un uso intensivo de recursos informáticos y las opciones de almacenamiento persistente de WorkSpaces Pools no funcionan como se esperaba, le recomendamos que utilice una solución de bloqueo de mensajes de servidor (SMB) como Amazon FSx for Windows File Server o una AWS Storage Gateway puerta de enlace de archivos. A continuación, se muestran ejemplos de archivos y directorios asociados a aplicaciones con un uso intensivo de recursos de computación que son más adecuados para su uso con estas soluciones de SMB:

- Carpetas de espacio de trabajo para entornos de desarrollo integrados () IDEs
- Archivos de bases de datos locales
- Carpetas de espacio de almacenamiento temporal creadas por aplicaciones de simulación gráfica

Para obtener más información, consulte File gateways en la Guía del usuario de AWS Storage Gateway .

Habilite las carpetas de inicio para los usuarios de sus WorkSpaces grupos

Antes de habilitar las carpetas de inicio, debe hacer lo siguiente:

- Compruebe que tiene los permisos AWS Identity and Access Management (IAM) correctos para las acciones de Amazon S3.
- Utilice una imagen que se haya creado a partir de una imagen AWS base publicada el 18 de mayo de 2017 o posteriormente.

- Habilite la conectividad de red con Amazon S3 desde su nube privada virtual (VPC) a través de la configuración del acceso a Internet o de un punto de conexión de VPC para Amazon S3. Para obtener más información, consulte Redes y acceso para WorkSpaces piscinas y Uso de puntos de enlace de VPC de Amazon S3 para funciones de grupos WorkSpaces .

Puede activar o desactivar las carpetas principales al crear un directorio (consulteConfigurar SAML 2.0 y crear un directorio de WorkSpaces grupos) o después de crearlo mediante la opción AWS Management Console for WorkSpaces Pools. Para cada región de AWS , se crea una copia de seguridad de las carpetas de inicio en un bucket de Amazon S3.

La primera vez que habilita las carpetas principales para un directorio de WorkSpaces grupos en una AWS región, el servicio crea un bucket de Amazon S3 en su cuenta de esa misma región. El mismo bucket se utiliza para almacenar el contenido de las carpetas de inicio de todos los usuarios y todos los directorios de esa región. Para obtener más información, consulte Almacenamiento en buckets de Amazon S3.

Cómo habilitar las carpetas de inicio al crear un directorio

- Siga las instrucciones de Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos y asegúrese de que la opción Habilitar carpetas de inicio esté seleccionada.

Cómo habilitar las carpetas de inicio para un directorio existente

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación de la izquierda, seleccione Directorios y elija el directorio para el que desea habilitar las carpetas de inicio.
3. Debajo de la lista de directorios, elija Almacenamiento y seleccione Habilitar carpetas de inicio.
4. En el cuadro de diálogo Habilitar carpetas de inicio, elija Habilitar.

Administrar las carpetas de inicio

Contenido

- Deshabilitación de las carpetas de inicio
- Almacenamiento en buckets de Amazon S3
- Sincronización del contenido de la carpeta de inicio
- Formatos de las carpetas de inicio

- Recursos adicionales

Deshabilitación de las carpetas de inicio

Puede deshabilitar las carpetas de inicio para un directorio sin perder el contenido del usuario ya almacenado en esas carpetas. La deshabilitación de carpetas de inicio para un directorio tiene los siguientes efectos:

- Los usuarios que se conectan a sesiones de transmisión activas para el directorio reciben un mensaje de error. Se les informa de que ya no pueden almacenar contenido en su carpeta de inicio.
- Las carpetas de inicio no aparecen para ninguna sesión nueva que use el directorio con las carpetas de inicio deshabilitadas.
- Si se deshabilitan las carpetas de inicio para un directorio, no se deshabilitan para los demás.
- Incluso si las carpetas principales están deshabilitadas en todos los directorios, WorkSpaces Pools no elimina el contenido del usuario.

Para restaurar el acceso a las carpetas de inicio del directorio, vuelva a habilitar las carpetas de inicio. Para ello, siga los pasos que se han descrito anteriormente en este tema.

Cómo deshabilitar las carpetas de inicio al crear un directorio

- Siga las instrucciones de Configurar SAML 2.0 y crear un directorio de WorkSpaces gruposy asegúrese de que la opción Habilitar carpetas de inicio esté desactivada.

Cómo deshabilitar las carpetas de inicio para un directorio existente

1. Abra la WorkSpaces consola en la https://console.aws.amazon.com/workspaces/versión 2/home.
2. En el panel de navegación de la izquierda, seleccione Directorios y elija el directorio para el que desea habilitar las carpetas de inicio.
3. Debajo de la lista de directorios, elija Almacenamiento y elimine la selección de Habilitar carpetas de inicio.
4. En el cuadro de diálogo Deshabilitar carpetas de inicio, escriba `CONFIRM` (en mayúsculas) para confirmar la elección y, a continuación, elija Deshabilitar.

Almacenamiento en buckets de Amazon S3

WorkSpaces Pools administra el contenido de los usuarios almacenado en las carpetas principales mediante los buckets de Amazon S3 creados en su cuenta. Para cada AWS región, WorkSpaces Pools crea un depósito en su cuenta. Todo el contenido del usuario generado desde las sesiones de transmisión de los directorios de esa región se almacena en ese bucket. El servicio administra totalmente los buckets sin intervención o configuración alguna por parte del administrador. Los nombres de los buckets siguen el formato específico que se indica a continuación:

```
wspool-home-folder-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

Dónde *<region-code>* está el código de AWS región en el que se creó el directorio y *<account-id-without-hyphens>* es el ID de su cuenta de Amazon Web Services, y *>random-identifier<* es un número identificador aleatorio generado por el WorkSpaces servicio. La primera parte del nombre del bucket, `wspool-home-folder-`, no cambia entre cuentas o regiones.

Por ejemplo, si habilita las carpetas de inicio para directorios de la región de Oeste de EE. UU. (Oregón) (us-west-2) en el número de cuenta 123456789012, el servicio crea un bucket de Amazon S3 en esa región con el nombre que se muestra. Este bucket solo lo puede eliminar un administrador con permisos suficientes.

```
wspool-home-folder-us-west-2-123456789012
```

Como se ha mencionado anteriormente, la deshabilitación de las carpetas de inicio para los directorios no eliminará ningún contenido del usuario almacenado en el bucket de Amazon S3. Para eliminar de forma permanente el contenido de los usuarios, un administrador con acceso adecuado debe hacerlo desde la consola de Amazon S3. WorkSpaces Pools añade una política de bucket que evita la eliminación accidental del bucket.

Sincronización del contenido de la carpeta de inicio

Cuando las carpetas principales están habilitadas, WorkSpaces Pools crea una carpeta única para cada usuario en la que almacenar su contenido. La carpeta se crea como un prefijo exclusivo de Amazon S3 que utiliza un hash del nombre de usuario dentro de un bucket de S3 para su región y cuenta de Amazon Web Services. Una vez que WorkSpaces Pools crea la carpeta de inicio en Amazon S3, copia el contenido al que se ha accedido en esa carpeta del bucket de S3 al WorkSpace. Esto permite al usuario acceder rápidamente al contenido de su carpeta principal, desde WorkSpace el WorkSpace Pool, durante su sesión de streaming. Los cambios que realice en

el contenido de la carpeta principal de un usuario en un bucket de S3 y que el usuario realice en el contenido de su carpeta principal WorkSpace en un contenedor del WorkSpace Pool se sincronizan entre Amazon S3 y WorkSpaces Pools de la siguiente manera.

1. Al principio de la sesión de streaming de WorkSpaces Pools de un usuario, WorkSpaces Pools cataloga los archivos de la carpeta de inicio que están almacenados para ese usuario en el bucket de Amazon S3 de su cuenta y región de Amazon Web Services.
2. El contenido de la carpeta de inicio de un usuario también se almacena WorkSpace en los WorkSpaces grupos desde los que transmite. Cuando un usuario accede a su carpeta principal en WorkSpace, se muestra la lista de archivos catalogados.
3. WorkSpaces Pools descarga un archivo del bucket de S3 WorkSpace solo después de que el usuario utilice una aplicación de streaming para abrir el archivo durante la sesión de streaming.
4. Una vez que WorkSpaces Pools descarga el archivo en el WorkSpace, la sincronización se produce cuando se accede al archivo
5. Si el usuario cambia el archivo durante la sesión de streaming, WorkSpaces Pools carga la nueva versión del archivo desde el WorkSpace bucket de S3 de forma periódica o al final de la sesión de streaming. Sin embargo, el archivo no se vuelve a descargar del bucket de S3 durante la sesión de streaming.

En las siguientes secciones se describe el comportamiento de sincronización al añadir, reemplazar o eliminar el archivo de la carpeta principal de un usuario en Amazon S3.

Contenido

- Sincronización de los archivos que añada a la carpeta principal de un usuario en Amazon S3
- Sincronización de los archivos que reemplace en la carpeta principal de un usuario en Amazon S3
- Sincronización de los archivos que elimine de la carpeta principal de un usuario en Amazon S3

Sincronización de los archivos que añada a la carpeta principal de un usuario en Amazon S3

Si añades un archivo nuevo a la carpeta principal de un usuario en un bucket de S3, WorkSpaces Pools cataloga el archivo y lo muestra en la lista de archivos de la carpeta principal del usuario en unos minutos. Sin embargo, el archivo no se descarga del bucket de S3 al depósito de S3 WorkSpace hasta que el usuario lo abra con una aplicación durante la sesión de streaming.

Sincronización de los archivos que reemplace en la carpeta principal de un usuario en Amazon S3

Si un usuario abre un archivo en su carpeta principal del WorkSpace WorkSpace pool durante su sesión de streaming y tú sustituyes el mismo archivo de su carpeta principal en un bucket de S3 por una nueva versión durante la sesión de streaming activa del usuario, la nueva versión del archivo no se descarga inmediatamente en el WorkSpace. La nueva versión se descarga del bucket de S3 al depósito de S3 WorkSpace solo después de que el usuario inicie una nueva sesión de streaming y vuelva a abrir el archivo.

Sincronización de los archivos que elimine de la carpeta principal de un usuario en Amazon S3

Si un usuario abre un archivo en su carpeta principal del WorkSpace WorkSpace grupo durante su sesión de streaming y tú eliminas el archivo de su carpeta principal en un bucket de S3 durante la sesión de streaming activa de ese usuario, el archivo se eliminará del repositorio WorkSpace después de que el usuario realice una de las siguientes acciones:

- Abrir de nuevo la carpeta de inicio
- Actualizar la carpeta de inicio

Formatos de las carpetas de inicio

La jerarquía de la carpeta de un usuario depende de cómo inicie este una sesión de transmisión, tal y como se describe en las siguientes secciones.

SAML 2.0

Para las sesiones creadas mediante federación SAML, la estructura de carpetas es la siguiente:

```
bucket-name/user/federated/user-id-SHA-256-hash/
```

En este caso, *`user-id-SHA-256-hash`* es el nombre de carpeta creado con una cadena hexadecimal hash SHA-256 en minúsculas generada a partir del valor del atributo SAML `NameID` pasado a la solicitud de federación SAML. Para diferenciar a los usuarios que tienen el mismo nombre pero pertenecen a dos dominios diferentes, envíe la solicitud SAML con `NameID` en el formato `domainname\username`. Para obtener más información, consulte Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos.

La siguiente estructura de carpetas de ejemplo se aplica al acceso de la sesión usando la federación SAML con `NameID` SAMPLEDOMAIN\testuser y el ID de cuenta 123456789012 en la Región de Oeste de EE. UU. (Oregón):

```
wspool-home-folder-us-west-2-123456789012/user/
federated/8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901
```

Cuando una parte o la totalidad de la cadena NameID está en mayúscula (como ocurre con el nombre *SAMPLEDOMAIN* de dominio en el ejemplo), WorkSpaces Pools genera el valor hash en función de las mayúsculas utilizadas en la cadena. En este ejemplo, el valor hash de SAMPLEDOMAIN\ testuser es 8 A642F511609454D344D53 A71190E44 B8 FDE0C507012A9901. DD9 CB861 FED2 AF9 En la carpeta de ese usuario, este valor se muestra en minúsculas, tal como se indica a continuación: 8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901.

Puede identificar la carpeta de un usuario generando el valor hash SHA-256 del `NameID` mediante bibliotecas de programación de código abierto o sitios web disponibles online.

Recursos adicionales

Para obtener más información acerca de cómo administrar los buckets de Amazon S3 y las prácticas recomendadas, consulte los siguientes temas en Guía del usuario de Amazon Simple Storage Service:

- Puede proporcionar acceso sin conexión a los datos de los usuarios con políticas de Amazon S3. Para obtener más información, consulte Amazon S3: permite a los usuarios de IAM obtener acceso a su directorio principal de S3, mediante programación y en la consola en la Guía del usuario de IAM.
- Puede habilitar el control de versiones de archivos para el contenido almacenado en los buckets de Amazon S3 que utilizan los WorkSpaces grupos. Para obtener más información, consulte Uso del control de versiones.

Habilite la persistencia de la configuración de la aplicación para los usuarios de sus WorkSpaces grupos

WorkSpaces Pools admite la configuración de aplicaciones persistente para los directorios basados en Windows. Esto significa que las personalizaciones de aplicaciones de los usuarios y la configuración de Windows se guardan automáticamente después de cada sesión de streaming y se aplican durante la siguiente sesión. Entre los ejemplos de configuración de aplicaciones persistentes que los usuarios pueden configurar se incluyen, entre otras, favoritos del explorador, configuración, sesiones de página web, perfiles de conexión de aplicaciones, complementos y personalizaciones de

la interfaz de usuario. Estos ajustes se guardan en un depósito de Amazon Simple Storage Service (Amazon S3) de su cuenta, dentro de la región en la que está habilitada AWS la persistencia de los ajustes de la aplicación. Están disponibles en cada sesión de streaming de WorkSpaces Pools.

> **Note**
>
> Es posible que se apliquen cargos estándar de Amazon S3 a los datos almacenados en su bucket de S3. Para obtener más información, consulte Precios de Amazon S3.

Contenido

- Cómo funciona la persistencia de configuración de aplicaciones
- Habilitación de la persistencia de configuración de la aplicación
- Administre la configuración de la aplicación VHDs para sus usuarios

Cómo funciona la persistencia de configuración de aplicaciones

La configuración de aplicación persistente se guarda en un archivo VHD (disco duro virtual). Este archivo se crea la primera vez que un usuario transmite una aplicación desde un directorio en la que la persistencia de configuración de la aplicación esté habilitada. Si el WorkSpace grupo asociado al directorio se basa en una imagen que contiene la configuración predeterminada de la aplicación y de Windows, la configuración predeterminada se utilizará para la primera sesión de streaming del usuario.

Cuando la sesión de streaming finaliza, el VHD se desmonta y se carga en un bucket de Amazon S3 en su cuenta. El depósito se crea cuando se habilita la configuración persistente de la aplicación por primera vez para un directorio de una AWS región. El depósito es exclusivo de tu AWS cuenta y de la región. El VHD se cifra en tránsito mediante puntos de enlace SSL de Amazon S3 y, en reposo, mediante AWS Managed. CMKs

El VHD se monta WorkSpace en ambos lados. `C:\Users\%username%` `D:\%username%` Si no WorkSpace está unido a un dominio de Active Directory, el nombre de usuario de Windows es PhotonUser. Si WorkSpace está unido a un dominio de Active Directory, el nombre de usuario de Windows es el del usuario que ha iniciado sesión.

La persistencia de la configuración de la aplicación no funciona en distintas versiones del sistema operativo. Por ejemplo, si habilita la persistencia de la configuración de la aplicación para un

WorkSpace grupo que usa una imagen de Windows Server 2019, si actualiza el WorkSpace grupo para usar una imagen que ejecute un sistema operativo diferente (como Windows Server 2022), la configuración de las sesiones de transmisión anteriores no se guardará para los usuarios del directorio. En cambio, después de actualizar el WorkSpace grupo para usar la nueva imagen, cuando los usuarios inician una sesión de transmisión desde un WorkSpace, se crea un nuevo perfil de usuario de Windows. Sin embargo, si aplica una actualización al mismo sistema operativo en la imagen, se guardan las personalizaciones y la configuración de los usuarios de las sesiones de streaming anteriores. Cuando se aplican actualizaciones del mismo sistema operativo a una imagen, se utiliza el mismo perfil de usuario de Windows cuando los usuarios inician una sesión de streaming desde WorkSpace.

> **Important**
>
> WorkSpaces Los pools admiten aplicaciones que dependen de la API de protección de datos de Microsoft solo cuando WorkSpace están unidos a un dominio de Microsoft Active Directory. En los casos en que a no WorkSpace está unido a un dominio de Active Directory, el usuario de Windows, PhotonUser, es diferente en cada uno de ellos WorkSpace. Debido a la forma en que funciona el modelo de seguridad DPAPI, las contraseñas de los usuarios no se mantienen para aplicaciones que utilizan DPAPI en esta situación. En los casos en los que WorkSpaces están unidos a un dominio de Active Directory y el usuario es un usuario de dominio, el nombre de usuario de Windows es el del usuario que ha iniciado sesión y las contraseñas de los usuarios se conservan en las aplicaciones que utilizan DPAPI.

WorkSpaces Pools guarda automáticamente todos los archivos y carpetas de esta ruta, excepto las siguientes carpetas:

- Contactos
- Escritorio
- Documentos
- Descargas
- Enlaces
- Imágenes
- Juegos guardados
- Búsquedas
- Videos

Los archivos y carpetas creados fuera de estas carpetas se guardan dentro del VHD y se sincronizan a Amazon S3. El tamaño máximo predeterminado de los VHD es de 5 GB para los pools. El tamaño del VHD guardado es el tamaño total de los archivos y carpetas que contiene. WorkSpaces Pools guarda automáticamente el `HKEY_CURRENT_USER` subárbol de registro para el usuario. Para los usuarios nuevos (usuarios cuyos perfiles no existen en Amazon S3), WorkSpaces Pools crea el perfil inicial con el perfil predeterminado. Este perfil se crea en la siguiente ubicación del generador de imágenes: `C:\users\default`.

> **Note**
>
> Se debe descargar todo el VHD WorkSpace antes de que pueda comenzar una sesión de streaming. Por este motivo, un VHD que contiene una gran cantidad de datos puede retrasar el inicio de la sesión de streaming. Para obtener más información, consulte Prácticas recomendadas para habilitar la persistencia de configuración de la aplicación.

Al habilitar la persistencia de la configuración de la aplicación, debe especificar un grupo de configuración. El grupo de ajustes determina qué ajustes de aplicación guardados se utilizan para una sesión de streaming desde este directorio. WorkSpaces Pools crea un nuevo archivo VHD para el grupo de configuración que se almacena por separado en el bucket de S3 de su AWS cuenta. Si el mismo grupo de configuración se comparte entre directorios, se utiliza la misma configuración de la aplicación en cada directorio. Si un directorio requiere su propia configuración de la aplicación, especifíquele un grupo de configuración único.

Habilitación de la persistencia de configuración de la aplicación

Contenido

- Requisitos previos para habilitar la persistencia de configuración de la aplicación
- Prácticas recomendadas para habilitar la persistencia de configuración de la aplicación
- Cómo habilitar la persistencia de configuración de la aplicación

Requisitos previos para habilitar la persistencia de configuración de la aplicación

Para habilitar la persistencia de la configuración de aplicaciones, debe hacer primero lo siguiente:

- Utilice una imagen que se haya creado a partir de una imagen base publicada a más tardar AWS el 7 de diciembre de 2017.

- Habilite la conectividad de red con Amazon S3 desde su nube privada virtual (VPC) a través de la configuración del acceso a Internet o de un punto de conexión de VPC para Amazon S3. Para obtener más información, consulte la sección Carpetas de inicio y puntos de enlace de la VPC en Redes y acceso para WorkSpaces piscinas.

Prácticas recomendadas para habilitar la persistencia de configuración de la aplicación

Para habilitar la persistencia de la configuración de la aplicación sin proporcionarle acceso a Internet WorkSpaces, utilice un punto de conexión de VPC. Este punto final debe estar en la VPC a la que están conectados sus WorkSpaces WorkSpaces grupos internos. Debe adjuntar una política personalizada para permitir que los WorkSpaces grupos accedan al punto final. Para obtener información acerca de cómo crear la política personalizada, consulte la sección Carpetas de inicio y puntos de enlace de la VPC en Redes y acceso para WorkSpaces piscinas. Para obtener más información sobre los puntos de conexión de Amazon S3, consulte Puntos de conexión de VPC y Puntos de conexión para Amazon S3 en la Guía del usuario de Amazon VPC.

Cómo habilitar la persistencia de configuración de la aplicación

Puede activar o desactivar la persistencia de la configuración de la aplicación al crear un directorio o después de crearlo mediante la WorkSpaces consola. Para cada región de AWS , la configuración persistente de la aplicación se almacena en un bucket de S3 en su cuenta.

La primera vez que habilita la persistencia de la configuración de la aplicación en un directorio de una AWS región, WorkSpaces Pools crea un bucket de S3 en su AWS cuenta de la misma región. El mismo depósito almacena el archivo VHD de configuración de la aplicación para todos los usuarios y todos los directorios de esa AWS región. Para obtener más información, consulte Almacenamiento en buckets de Amazon S3 en Administre la configuración de la aplicación VHDs para sus usuarios.

Cómo habilitar la persistencia de la configuración de la aplicación mientras se crea un directorio

- Siga las instrucciones de Configurar SAML 2.0 y crear un directorio de WorkSpaces gruposy asegúrese de que la opción Enable Application Settings Persistence (Habilitar persistencia de la configuración de la aplicación) esté seleccionada.

Cómo habilitar la persistencia de la configuración de la aplicación para un directorio existente

1. Abra la WorkSpaces consola en la versión https://console.aws.amazon.com/workspaces/v2/home.

2. En el panel de navegación de la izquierda, seleccione Grupos y elija el grupo para el que desea habilitar la persistencia de la aplicación.
3. Elija Editar en la sección Configuración de la página.
4. En la sección Persistencia de la aplicación de la página, seleccione Habilitar persistencia de configuración de la aplicación.
5. Seleccione Save changes (Guardar cambios).

Las nuevas sesiones de streaming tienen ahora habilitada la persistencia de la configuración de la aplicación.

Administre la configuración de la aplicación VHDs para sus usuarios

Contenido

- Almacenamiento en buckets de Amazon S3
- Restablecimiento de la configuración de la aplicación de un usuario
- Habilitación del control de versiones de objeto de Amazon S3 y reversión de la configuración de la aplicación de un usuario
- Aumento del tamaño del VHD de configuración de la aplicación

Almacenamiento en buckets de Amazon S3

Al habilitar la persistencia de la configuración de las aplicaciones, las personalizaciones de las aplicaciones de sus usuarios y la configuración de Windows se guardan automáticamente en un archivo de disco duro virtual (VHD) que se almacena en un bucket de Amazon S3 creado en su AWS cuenta. Para cada AWS región, WorkSpaces Pools crea un depósito en su cuenta que es exclusivo para su cuenta y para la región. Todas las configuraciones de la aplicación configuradas por los usuarios se almacenan en el bucket para dicha región.

No necesita realizar ninguna tarea de configuración para administrar estos depósitos de S3; el servicio WorkSpaces Pools los administra completamente. El archivo VHD que se almacena en cada depósito se cifra en tránsito mediante los puntos de enlace SSL de Amazon S3 y en reposo mediante AWS Managed. CMKs Los nombres de los buckets siguen el formato específico que se indica a continuación:

```
wspool-app-settings-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

region-code

Este es el código de AWS región en el que se crea el directorio con la persistencia de la configuración de la aplicación.

account-id-without-hyphens

El ID AWS de tu cuenta. El identificador aleatorio garantiza que no haya conflicto con otros buckets en esa región. La primera parte del nombre del bucket, `wspool-app-settings`, no cambia entre cuentas o regiones.

Por ejemplo, si habilita la persistencia de la configuración de la aplicación para los directorios de la región EE.UU. Oeste (Oregón) (us-west-2) en el número de cuenta 123456789012, WorkSpaces Pools crea un bucket de Amazon S3 en su cuenta de esa región con el nombre que se muestra. Este bucket solo lo puede eliminar un administrador con permisos suficientes.

```
wspool-app-settings-us-west-2-1234567890123-abcdefg
```

Al deshabilitar la persistencia de la configuración de la aplicación, no se elimina ninguna información almacenada en el depósito de S3. VHDs Para eliminar la configuración de forma permanente VHDs, usted u otro administrador con los permisos adecuados deben hacerlo mediante la consola o la API de Amazon S3. WorkSpaces Pools añade una política de bucket que evita la eliminación accidental del bucket.

Cuando la persistencia de la configuración de la aplicación está habilitada, se crea una única carpeta para cada grupo de configuración para almacenar el archivo VHD de configuración. La jerarquía de la carpeta en el bucket de S3 depende de cómo lance este una sesión de streaming, como se describe en la siguiente sección.

La ruta para la carpeta donde el VHD de configuración está almacenado en el bucket de S3 en su cuenta utiliza la siguiente estructura:

```
bucket-name/Windows/prefix/settings-group/access-mode/user-id-SHA-256-hash
```

bucket-name

El nombre del bucket de S3 en el que se almacena la configuración de la aplicación de los usuarios. El formato del nombre se describe anteriormente en esta sección.

prefix

El prefijo específico de la versión de Windows. Por ejemplo, v4 para Windows Server 2012 R2.

settings-group

El valor del grupo de configuración. Este valor se aplica a uno o varios directorios que comparten la misma configuración de la aplicación.

access-mode

El método de identidad del usuario: `custom` para la API o CLI de WorkSpaces grupos, `federated` para SAML y `userpool` para los usuarios del grupo de usuarios.

user-id-SHA-256-hash

El nombre de carpeta específico del usuario. Este nombre se ha creado utilizando una cadena hexadecimal con hasta SHA-256 en minúsculas generada a partir del ID de usuario.

El siguiente ejemplo de estructura de carpetas se aplica a una sesión de streaming a la que se accede mediante la API o la CLI con un Cuenta de AWS identificador de `testuser@mydomain.com` usuario`123456789012`, un identificador y el grupo `test-stack` de configuración de la región EE.UU. Oeste (Oregón) (us-west-2):

```
wspool-app-settings-us-west-2-1234567890123-abcdefg/Windows/v4/test-stack/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13
```

Puede identificar la carpeta de un usuario generando el valor hash SHA-256 en minúsculas del ID de usuario mediante bibliotecas de programación de código abierto o sitios web disponibles online.

Restablecimiento de la configuración de la aplicación de un usuario

Para restablecer la configuración de la aplicación de un usuario, debe buscar y eliminar el VHD y el archivo de metadatos asociado del bucket de S3 de su cuenta. AWS Asegúrese de no hacerlo durante una sesión de streaming activa del usuario. Tras eliminar el VHD del usuario y el archivo de metadatos, la próxima vez que el usuario inicie una sesión desde una instancia de streaming que tenga habilitada la persistencia de la configuración de la aplicación, WorkSpaces Pools creará un nuevo VHD de configuración para ese usuario.

Para restablecer la configuración de la aplicación de un usuario

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. En la lista Bucket name (Nombre de bucket), elija el bucket de S3 que contiene el VHD de configuración de la aplicación que desea restablecer.
3. Localice la carpeta que contiene el VHD. Para obtener más información acerca de cómo navegar por la estructura de carpetas del bucket de S3, consulte Almacenamiento de bucket de Amazon S3 anteriormente en este tema.
4. En la lista Name (Nombre), seleccione la casilla de verificación que se encuentra junto al VHD y la REG, elija More (Más) y, a continuación, seleccione Delete (Eliminar).
5. En el cuadro de diálogo Delete objects (Eliminar objetos), compruebe que aparecen el VHD y la REG y, a continuación, elija Delete (Eliminar).

La próxima vez que el usuario realice una transmisión desde un grupo en el que esté habilitada la persistencia de la configuración de la aplicación con el grupo de configuración correspondiente, se creará un nuevo VHD de configuración de la aplicación. Este VHD se guarda en el bucket de S3 al final de la sesión.

Habilitación del control de versiones de objeto de Amazon S3 y reversión de la configuración de la aplicación de un usuario

Puede utilizar el control de versiones de objetos y las políticas de ciclo de vida de Amazon S3 para administrar la configuración de la aplicación de los usuarios cuando los usuarios la cambian. Con el control de versiones de Amazon S3, puede preservar, recuperar y restaurar cada versión del VHD de configuración. Esto permite recuperarse fácilmente tanto de las acciones de usuario no deseadas como de los errores de las aplicaciones. Cuando el control de versiones está habilitado, después de cada sesión de streaming, una nueva versión del VHD de configuración de la aplicación se sincroniza con Amazon S3. La nueva versión no sobrescribe la versión anterior, por tanto si se produce un problema con la configuración de sus usuarios, puede volver a una versión anterior del VHD.

> **Note**
>
> Cada versión del VHD de configuración de la aplicación se guarda en Amazon S3 como un objeto independiente y se cobra en función de ello.

El control de versiones de objetos no está habilitado de forma predeterminada en el bucket de S3, por lo que debe habilitarlo de forma explícita.

Para habilitar el control de versiones para el VHD de configuración de su aplicación

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Bucket name (Nombre de bucket), elija el bucket de S3 que contiene el VHD de configuración de la aplicación en el que desea habilitar el control de versiones de objeto.
3. Seleccione Propiedades.
4. Elija Versioning (Control de versiones), Enable versioning (Habilitar control de versiones) y, a continuación, Save (Guardar).

Para caducar las versiones anteriores de la configuración de la aplicación VHDs, puede utilizar las políticas de ciclo de vida de Amazon S3. Para obtener más información, consulte How Do I Create a Lifecycle Policy for an S3 Bucket? en la Guía del usuario de Amazon Simple Storage Service.

Para volver al VHD de configuración de la aplicación de un usuario

Puede volver a una versión anterior del VHD de configuración de la aplicación de un usuario eliminando las versiones más actuales del VHD desde el bucket de S3 aplicable. No lo haga cuando este usuario tenga una sesión de streaming activa.

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Bucket name (Nombre de bucket), elija el bucket de S3 que contiene la versión de VHD de configuración de la aplicación del usuario a la que desea volver.
3. Localice y seleccione la carpeta que contiene el VHD. Para obtener información acerca de cómo navegar por la estructura de carpetas del bucket de S3, consulte Almacenamiento de bucket de Amazon S3 anteriormente en este tema.

   Al seleccionar la carpeta, se muestran el VHD de configuración y el archivo de metadatos asociado.
4. Para mostrar una lista de las versiones de los archivos VHD y de metadatos, elija Show (Mostrar).
5. Localice la versión del VHD a la que desea volver.
6. En la lista Name (Nombre), seleccione las casillas de verificación situadas junto a las versiones más recientes de los archivos de metadatos asociados y VHD, elija More (Más) y, a continuación, Delete (Eliminar).
7. Compruebe que el archivo VHD de configuración de la aplicación al que desea volver y el archivo de metadatos asociado son las versiones más recientes de estos archivos.

La próxima vez que el usuario realice una transmisión desde un grupo en el que esté habilitada la persistencia de la configuración de la aplicación con el grupo de configuración correspondiente, se mostrará la versión anterior de la configuración del usuario.

Aumento del tamaño del VHD de configuración de la aplicación

El tamaño máximo predeterminado del VHD es de 5 GB para los pools. Si un usuario requiere espacio adicional para la configuración de la aplicación, puede descargar el archivo VHD de configuración de la aplicación correspondiente a un equipo Windows para ampliarlo. A continuación, reemplace el VHD actual en el bucket de S3 por el mayor. No lo haga cuando este usuario tenga una sesión de streaming activa.

> **Note**
>
> Para reducir el tamaño físico del disco duro virtual (VHD), vacíe la papelera de reciclaje antes de finalizar una sesión. Esto también reducirá los tiempos de carga y descarga y mejorará la experiencia general del usuario.

Para aumentar el tamaño del VHD de configuración de la aplicación

> **Note**
>
> El archivo VHD completo se debe descargar antes de que un usuario pueda transmitir aplicaciones. Un aumento del tamaño del archivo VHD de configuración de la aplicación puede aumentar el tiempo necesario para que los usuarios comiencen las sesiones de streaming de la aplicación.

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Bucket name (Nombre de bucket), elija el bucket de S3 que contiene el VHD de configuración de la aplicación que ampliar.
3. Localice y seleccione la carpeta que contiene el VHD. Para obtener más información sobre cómo navegar por la estructura de carpetas del bucket de S3, consulte Almacenamiento en buckets de Amazon S3 que aparece anteriormente en este tema.

   Al seleccionar la carpeta, se muestran el VHD de configuración y el archivo de metadatos asociado.

4. Descargue el archivo `Profile.vhdx` en un directorio en el equipo de Windows. No cierre el navegador una vez que se complete la descarga, ya que volverá a utilizar el navegador a continuación para cargar el VHD ampliado.
5. Para utilizar Diskpart para aumentar el tamaño del VHD a 7 GB, abra el símbolo del sistema como administrador y escriba los siguientes comandos.

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
expand vdisk maximum=7000
```

6. A continuación, escriba los siguientes comandos de Diskpart para encontrar y asociar el VHD y mostrar la lista de volúmenes:

```
elect vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
attach vdisk
```

```
list volume
```

En la salida, anote el número de volumen con la etiqueta "AwsEucUsers». En el siguiente paso, seleccione este volumen para que lo pueda ampliar.

7. Escriba el siguiente comando en el que *<volume-number>* es el número de la salida del volumen de la lista.

```
select volume <volume-number>
```

8. Escriba el siguiente comando:

```
extend
```

9. Escriba los comandos siguientes para confirmar que el tamaño de la partición en el VHD ha aumentado según lo previsto (7 GB en este ejemplo):

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
list volume
```

10. Escriba el siguiente comando para desconectar el VHD de forma que se pueda cargar:

```
detach vdisk
```

11. Vuelva al navegador con la consola de Amazon S3, seleccione Cargar, Agregar archivos y, a continuación, seleccione el VHD ampliado.
12. Seleccione Cargar.

Una vez cargado el VHD, la próxima vez que el usuario realice una transmisión desde un grupo en el que la persistencia de configuración de la aplicación esté habilitada con el grupo de aplicaciones correspondiente, estará disponible el VHD de configuración de la aplicación mayor.

WorkSpaces Códigos de notificación de solución de problemas de piscinas

A continuación, se muestran los códigos de notificación y los pasos de resolución de problemas con la unión de dominios que es posible que encuentre al configurar y utilizar Active Directory con WorkSpaces.

DOMAIN_JOIN_ERROR_ACCESS_DENIED

Mensaje: se deniega el acceso.

Resolución: la cuenta de servicio especificada en el directorio no tiene permisos para crear el objeto de equipo ni para volver a utilizar uno ya existente. Valide los permisos e inicie el WorkSpaces grupo.

DOMAIN_JOIN_ERROR_LOGON_FAILURE

Mensaje: el nombre de usuario o la contraseña es incorrecto.

Resolución: la cuenta de servicio especificada en el directorio tiene un nombre de usuario o una contraseña no válidos. Actualice las credenciales en el AWS Secrets Manager secreto configurado en el directorio y vuelva a iniciar el WorkSpaces grupo.

DOMAIN_JOIN_NERR_PASSWORD_EXPIRED

Mensaje: la contraseña de este usuario ha vencido.

Solución: la contraseña de la cuenta de servicio que figura en el AWS Secrets Manager secreto ha caducado. Primero, detenga la WorkSpaces piscina. A continuación, cambie la contraseña del secreto especificado en el WorkSpaces directorio. A continuación, inicie la WorkSpaces piscina.

DOMAIN_JOIN_ERROR_DS_MACHINE_ACCOUNT_QUOTA_EXCEEDED

Mensaje: su equipo no se ha podido incorporar al dominio. Ha superado el número máximo de cuentas de equipos para las que tiene permiso de creación en este dominio. Póngase en contacto con el administrador del sistema para restablecer o aumentar este límite.

Resolución: la cuenta de servicio especificada en el directorio no tiene permisos para crear el objeto de equipo ni para volver a utilizar uno ya existente. Valide los permisos e inicie el WorkSpaces grupo.

DOMAIN_JOIN_ERROR_INVALID_PARAMETER

Mensaje: un parámetro es incorrecto. Este error se devuelve si el parámetro `LpName` es NULL o si el parámetro `NameType` se especifica como `NetSetupUnknown` o un tipo de nombre desconocido.

Resolución: este error puede producirse cuando el nombre distinguido de la OU es incorrecto. Valide la OU e inténtelo de nuevo. Si sigue apareciendo este error, póngase en contacto con AWS Support. Para obtener más información, consulte el Centro de AWS Support.

DOMAIN_JOIN_ERROR_MORE_DATA

Mensaje: hay más datos disponibles.

Resolución: este error puede producirse cuando el nombre distinguido de la OU es incorrecto. Valide la OU e inténtelo de nuevo. Si sigue apareciendo este error, ponte en contacto con AWS Support. Para obtener más información, consulte el Centro de AWS Support.

DOMAIN_JOIN_ERROR_NO_SUCH_DOMAIN

Mensaje: el dominio especificado no existe o no se pudo contactar con él.

Resolución: la instancia de streaming no ha podido ponerse en contacto con el dominio de Active Directory. Confirme la VPC, la subred y la configuración del grupo de seguridad para garantizar la conectividad de red.

DOMAIN_JOIN_NERR_WORKSTATION_NOT_STARTED

Mensaje: el servicio de la estación de trabajo no se ha iniciado.

Resolución: se ha producido un error al comenzar el servicio de la estación de trabajo. Asegúrese de que el servicio esté habilitado en su imagen. Si sigue apareciendo este error, ponte en contacto con AWS Support. Para obtener más información, consulte el Centro de AWS Support.

DOMAIN_JOIN_ERROR_NOT_SUPPORTED

Mensaje: no se admite la solicitud. Este error se devuelve si se ha especificado un equipo remoto en el parámetro `lpServer` y la llamada no se admite en dicho equipo remoto.

Solución: póngase en contacto AWS Support para obtener ayuda. Para obtener más información, consulte el Centro de AWS Support.

DOMAIN_JOIN_ERROR_FILE_NOT_FOUND

Mensaje: el sistema no puede encontrar el archivo especificado.

Resolución: este error se produce cuando se proporciona un nombre distinguido de una unidad organizativa (OU) no válida. El nombre distinguido debe comenzar con **`OU=`**. Valide el nombre distinguido de la OU e inténtelo de nuevo.

DOMAIN_JOIN_INTERNAL_SERVICE_ERROR

Mensaje: The account already exists (La cuenta ya existe).

Solución: este error puede producirse en los siguientes escenarios:

- Si el problema no está relacionado con los permisos, compruebe si hay errores en los registros de Netdom y asegúrese de haber proporcionado la OU correcta.
- La cuenta de servicio especificada en el directorio no tiene permisos para crear el objeto de equipo ni para volver a utilizar uno ya existente. Si este es el caso, valide los permisos e inicie el WorkSpaces grupo.
- Una vez WorkSpaces creado el objeto de ordenador, se mueve desde la unidad organizativa en la que se creó. En este caso, el primer WorkSpaces grupo se crea correctamente, pero se produce un error en cualquier WorkSpaces grupo nuevo que utilice el objeto de ordenador. Cuando Active Directory busca el objeto de equipo en la OU especificada y detecta que existe un objeto con el mismo nombre en otra parte del dominio, la unión al dominio no se realiza correctamente.

- El nombre de la unidad organizativa especificada en el WorkSpaces directorio incluye espacios antes o después de las comas del directorio. En este caso, cuando un WorkSpaces grupo intenta volver a unirse al dominio de Active Directory, WorkSpaces no puede hacer un ciclo correcto de los objetos del equipo y la unión del dominio no se realiza correctamente. Para resolver este problema en un WorkSpaces grupo, haga lo siguiente:

  1. Detenga la WorkSpaces piscina.
  2. Edite la configuración del dominio de Active Directory del WorkSpaces grupo para eliminar el directorio y la unidad organizativa del directorio a los que está unido el WorkSpaces grupo.
  3. Actualice el WorkSpaces directorio para especificar una unidad organizativa que no contenga espacios.
  4. Edite la configuración del dominio de Active Directory del WorkSpaces grupo para especificar el directorio con la OU de directorio actualizada.

  Para resolver este problema en un WorkSpaces grupo, haga lo siguiente:

  1. Elimine el WorkSpaces grupo.
  2. Actualice el WorkSpaces directorio para especificar una unidad organizativa que no contenga espacios.
  3. Cree un nuevo WorkSpaces grupo y especifique el directorio con la OU de directorio actualizada.

WORKSPACES_POOL_SESSION_RESERVATION_ERROR

Mensaje: Actualmente no tenemos capacidad suficiente para las sesiones solicitadas en las zonas de disponibilidad [us-west-1] de las subredes asociadas a su grupo. WorkSpaces Estamos trabajando para aprovisionar capacidad adicional. Mientras tanto, cambie o asocie una subred diferente mediante una de las siguientes opciones AZs [us-west-2, us-west-3].

Solución: espere hasta que EC2 tenga suficiente capacidad o actualice las subredes de otras subredes del directorio. AZs

INSUFFICIENT_CAPACITY_ERROR_WORKSPACES_POOL_AZ

Mensaje: Actualmente no tenemos capacidad suficiente para las sesiones solicitadas en la zona de disponibilidad (AZs) [<impacted az>]. Estamos trabajando para aprovisionar capacidad adicional. Mientras tanto, cambie o asocie otra subred AZs a su WorkSpaces grupo utilizando otra.

Solución: espere a que Amazon EC2 tenga suficiente capacidad o actualice las subredes de otras AZs subredes del directorio.

INVALID_CUSTOMER_SUBNET_CIDR_BLOCK

Mensaje: Your subnet includes use of an unavailable CIDR range. Please update your subnets outside of the current /18 range.”.

Solución: espere hasta que EC2 tenga suficiente capacidad o actualice las subredes de otras AZs subredes del directorio.

Seguridad en Amazon WorkSpaces

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables WorkSpaces, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio 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 cuando se utiliza WorkSpaces. Le muestra cómo configurarlo para WorkSpaces cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus WorkSpaces recursos.

Contenido

- Protección de datos en Amazon WorkSpaces
- Administración de identidad y acceso para WorkSpaces
- Validación de conformidad para Amazon WorkSpaces
- Resiliencia en Amazon WorkSpaces
- Seguridad de la infraestructura en Amazon WorkSpaces
- Gestión de actualizaciones en WorkSpaces

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. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres 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, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. 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. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza 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 140-3 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, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

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 con WorkSpaces o Servicios de AWS utiliza la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de

texto 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 WorkSpaces el cifrado de terminales FIPS, consulteConfigure la autorización de FedRAMP o el cumplimiento de las normas SRG del DoD para personal WorkSpaces .

Cifrado en reposo

Puede cifrar sus volúmenes de almacenamiento WorkSpaces mediante AWS KMS Key from. AWS Key Management Service Para obtener más información, consulte WorkSpaces Cifrado en WorkSpaces modo personal.

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 EC2 usuario de Amazon.

Cifrado en tránsito

En el PCo caso de la IP, los datos en tránsito se cifran mediante el cifrado TLS 1.2 y la firma de solicitudes SigV4. El protocolo PCo IP 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 los cifrados AES-128 y AES-256, pero el cifrado predeterminado 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 PCo IP para Windows WorkSpaces o modificando la configuración de seguridad PCo IP en el `pcoip-agent.conf` archivo para Amazon Linux. WorkSpaces

Para obtener más información sobre la administración de políticas de grupo para Amazon WorkSpaces, consulte Configure los ajustes de seguridad PCo IP enAdministre su Windows WorkSpaces en WorkSpaces Personal. Para obtener más información sobre la modificación del `pcoip-agent.conf` archivo, consulte Controle el comportamiento del agente PCo IP en Amazon Linux WorkSpaces la configuración de seguridad PCo IP en la documentación de Teradici.

Para DCV, los datos en tránsito de transmisión y control se cifran mediante el cifrado TLS 1.3 para el tráfico UDP y el cifrado TLS 1.2 para el tráfico TCP, con cifrados AES-256.

Administración de identidad y acceso para WorkSpaces

De forma predeterminada, los usuarios de IAM no tienen permisos para los WorkSpaces recursos y las operaciones. Para permitir que los usuarios de IAM administren WorkSpaces los recursos, debe crear una política de IAM que les conceda permisos de forma explícita y adjuntar la política a los usuarios o grupos de IAM que necesiten esos permisos.

> **Note**
>
> Amazon WorkSpaces no admite el aprovisionamiento de credenciales de IAM en un WorkSpace (por ejemplo, con un perfil de instancia).

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en 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 aceptar. Siga las instrucciones descritas en 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 añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

A continuación se enumeran recursos adicionales de IAM:

- Para obtener más información sobre las políticas de IAM, consulte Políticas y permisos en la Guía del usuario de IAM.
- Para obtener más información sobre IAM, consulte Administración de identidades y acceso (IAM) y la Guía del usuario de IAM.

- Para obtener más información sobre recursos, acciones y claves de contexto de condiciones WorkSpaces específicos para su uso en las políticas de permisos de IAM, consulte 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 de AWS. También puede utilizar el simulador de política de IAM para probar si una política permitiría o denegaría una solicitud específica a AWS.

Contenido

- Ejemplos de políticas
- Especifique WorkSpaces los recursos en una política de IAM
- Cree el rol workspaces_ DefaultRole
- Cree el rol de servicio AmazonWorkSpaces PCAAccess
- AWS políticas gestionadas para WorkSpaces
- Acceso a las instancias de streaming WorkSpaces y a los scripts de las mismas

Ejemplos de políticas

Los siguientes ejemplos muestran declaraciones de políticas que puedes usar para controlar los permisos que los usuarios de IAM tienen en Amazon WorkSpaces.

Ejemplo 1: conceder acceso para realizar tareas WorkSpaces personales y grupales

La siguiente declaración de política otorga a un usuario de IAM permiso para realizar tareas WorkSpaces personales y de grupos.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
```

```
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys",
                "secretsmanager:ListSecrets",
                "tag:GetResources",
```

```
                "sso-directory:SearchUsers",
                "sso:CreateApplication",
                "sso:DeleteApplication",
                "sso:DescribeApplication",
                "sso:DescribeInstance",
                "sso:GetApplicationGrant",
                "sso:ListInstances",

                "sso:PutApplicationAssignmentConfiguration",
                "sso:PutApplicationAuthenticationMethod",
                "sso:PutApplicationGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

Ejemplo 2: Conceder acceso para realizar tareas WorkSpaces personales

La siguiente declaración de política concede a un usuario de IAM permiso para realizar todas las tareas WorkSpaces personales.

Si bien Amazon admite WorkSpaces plenamente los `Resource` elementos `Action` y cuando utiliza la API y las herramientas de línea de comandos, para utilizar Amazon WorkSpaces desde el 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

JSON

```
{
  "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",
        "secretsmanager:ListSecrets",
        "sso-directory:SearchUsers",
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationGrant",
        "sso:ListInstances",

        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Ejemplo 3: Conceder acceso para realizar tareas de WorkSpaces Pools

La siguiente declaración de política otorga a un usuario de IAM permiso para realizar todas las tareas de WorkSpaces Pools.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": [
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "secretsmanager:ListSecrets",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
```

```
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-
role/workspaces.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_WorkSpacesPool",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "workspaces.application-
autoscaling.amazonaws.com"
                }
            }
        }
    ]
}
```

Ejemplo 4: Realizar todas las WorkSpaces tareas para BYOL WorkSpaces

La siguiente declaración de política otorga a un usuario de IAM permiso para realizar todas WorkSpaces las tareas, incluidas las EC2 tareas de Amazon necesarias para crear Bring Your Own License (BYOL). WorkSpaces

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
```

```
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:ModifyImageAttribute",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

Especifique WorkSpaces los recursos en una política de IAM

Para especificar un WorkSpaces recurso en el `Resource` elemento de la declaración de política, utilice el nombre de recurso de Amazon (ARN) del recurso. Usted controla el acceso a sus WorkSpaces recursos al permitir o denegar los permisos para usar las acciones de la API que se especifican en el `Action` elemento de su declaración de política de IAM. WorkSpaces define ARNs los paquetes WorkSpaces, los grupos de IP y los directorios.

WorkSpace ARN

Un WorkSpace ARN tiene la sintaxis que se muestra en el siguiente ejemplo.

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

region

La región en la que WorkSpace se encuentra (por ejemplo,`us-east-1`).

account_id

El ID de la AWS cuenta, sin guiones (por ejemplo,`123456789012`).

identificador_espacio_trabajo

El ID de WorkSpace (por ejemplo,`ws-a1bcd2efg`).

El siguiente es el formato del `Resource` elemento de una declaración de política que identifica un elemento específico WorkSpace.

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

Puede usar el `*` comodín para especificar todos los WorkSpaces que pertenecen a una cuenta específica en una región específica.

WorkSpace piscina ARN

Un WorkSpace ARN de grupo tiene la sintaxis que se muestra en el siguiente ejemplo.

```
arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier
```

region

La región en la que WorkSpace se encuentra (por ejemplo,`us-east-1`).

account_id

El ID de la AWS cuenta, sin guiones (por ejemplo,`123456789012`).

workspacespool_identifier

El ID del WorkSpace grupo (por ejemplo,`ws-a1bcd2efg`).

El siguiente es el formato del `Resource` elemento de una declaración de política que identifica un elemento específico WorkSpace.

```
"Resource":
 "arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier"
```

Puede usar el `*` comodín para especificar todos los WorkSpaces que pertenecen a una cuenta específica en una región específica.

ARN de imagen

El ARN WorkSpace de una imagen 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 WorkSpace imagen (por ejemplo,`us-east-1`).

account_id

El ID de la AWS cuenta, sin guiones (por ejemplo,`123456789012`).

identificador_paquete

El ID de la WorkSpace imagen (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 WorkSpace se encuentra (por ejemplo,`us-east-1`).

account_id

El ID de la AWS cuenta, sin guiones (por ejemplo,`123456789012`).

identificador_paquete

El ID del WorkSpace paquete (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 WorkSpace se encuentra (por ejemplo,`us-east-1`).

account_id

El ID de la AWS cuenta, 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 WorkSpace se encuentra (por ejemplo,`us-east-1`).

account_id

El ID de la AWS cuenta, 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`).

account_id

El ID de la AWS cuenta, 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"
```

Cree el rol workspaces_ DefaultRole

Antes de poder registrar un directorio mediante la API, debe comprobar que existe un rol denominado `workspaces_DefaultRole`. Esta función la crea la configuración rápida o, si lanzas una WorkSpace con AWS Management Console, y otorga a Amazon WorkSpaces permiso para acceder a AWS recursos específicos en tu nombre. Si este rol no existe, puede crearlo mediante el siguiente procedimiento.

Para crear el rol workspaces_ DefaultRole

1. Inicie sesión en la consola de AWS Management Console IAM y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación de la izquierda, seleccione Roles.
3. Seleccione 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 Adjuntar políticas de permisos, seleccione las políticas AWS AmazonWorkSpacesServiceAccessAmazonWorkSpacesSelfServiceAccessadministradas y AmazonWorkSpacesPoolServiceAccess. Para obtener más información sobre estas políticas administradas, consulte AWS políticas gestionadas para WorkSpaces.
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 Siguiente: etiquetas.
11. En la página Add tags (optional) [Agregar etiquetas (opcional)], añada las etiquetas que correspondan.
12. Elija 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 Crear rol.
16. En la página de resumen del DefaultRole rol workspaces_, seleccione la pestaña 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 Actualizar política de confianza.

Cree el rol de servicio AmazonWorkSpaces PCAAccess

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 habilitas la autenticación basada en certificados en un directorio mediante el AWS Management Console, y otorga a Amazon WorkSpaces permiso para acceder a AWS Private CA los recursos en tu 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 AmazonWorkSpaces PCAAccess servicio mediante el AWS CLI

1. Cree un archivo JSON llamado `AmazonWorkSpacesPCAAccess.json` con el siguiente texto.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Ajuste la `AmazonWorkSpacesPCAAccess.json` ruta según sea necesario y ejecute los siguientes AWS CLI comandos para crear el rol de servicio y adjuntar la política AmazonWorkspacesPCAAccessgestionada.

```
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
```

AWS políticas gestionadas para WorkSpaces

El uso de políticas AWS administradas hace que añadir permisos a usuarios, grupos y roles sea más fácil 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. Usa políticas AWS administradas para empezar rápidamente. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios pueden añadir permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. 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.

AWS política gestionada: AmazonWorkSpacesAdmin

Esta política proporciona acceso a las acciones WorkSpaces administrativas de Amazon. Proporciona los siguientes permisos:

- `workspaces`- Permite el acceso para realizar acciones administrativas en los recursos WorkSpaces personales y de WorkSpaces Pools.
- `kms`: Permite acceder a la lista y descripción de claves KMS, así como a la lista de alias.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonWorkSpacesAdmin",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaceImage",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspacesPool",
                "workspaces:CreateStandbyWorkspaces",
                "workspaces:DeleteTags",
                "workspaces:DeregisterWorkspaceDirectory",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesPools",
                "workspaces:DescribeWorkspacesPoolSessions",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:ModifyStreamingProperties",
                "workspaces:ModifyWorkspaceCreationProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:RebootWorkspaces",
```

```
                "workspaces:RebuildWorkspaces",
                "workspaces:RegisterWorkspaceDirectory",
                "workspaces:RestoreWorkspace",
                "workspaces:StartWorkspaces",
                "workspaces:StartWorkspacesPool",
                "workspaces:StopWorkspaces",
                "workspaces:StopWorkspacesPool",
                "workspaces:TerminateWorkspaces",
                "workspaces:TerminateWorkspacesPool",
                "workspaces:TerminateWorkspacesPoolSession",
                "workspaces:UpdateWorkspacesPool"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AmazonWorkspaces PCAAccess

Esta política administrada proporciona acceso a los recursos de AWS Certificate Manager Private Certificate Authority (Private CA) de su AWS cuenta para la autenticación basada en certificados. Se incluye en la AmazonWorkSpaces PCAAccess función y proporciona los siguientes permisos:

- `acm-pca`- Permite el acceso a una CA AWS privada para gestionar la autenticación basada en certificados.

JSON

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

AWS política gestionada: AmazonWorkSpacesSelfServiceAccess

Esta política proporciona acceso al WorkSpaces servicio de Amazon para realizar acciones de WorkSpaces autoservicio iniciadas por un usuario. Se incluye en el rol `workspaces_DefaultRole` y proporciona los siguientes permisos:

- `workspaces`- Permite a los usuarios acceder a las capacidades de WorkSpaces gestión de autoservicio.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AmazonWorkSpacesServiceAccess

Esta política proporciona acceso a la cuenta del cliente al WorkSpaces servicio de Amazon para lanzar un WorkSpace. Se incluye en el rol `workspaces_DefaultRole` y proporciona los siguientes permisos:

- `ec2`- Permite el acceso para gestionar EC2 los recursos de Amazon asociados a WorkSpace, como las interfaces de red.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AmazonWorkSpacesPoolServiceAccess

Esta política se usa en workspaces_DefaultRole, que se WorkSpaces utiliza para acceder a los recursos necesarios en la cuenta de cliente AWS de Pools. WorkSpaces Para obtener más información, consulte Cree el rol workspaces_ DefaultRole . Proporciona los siguientes permisos:

- `ec2`- Permite el acceso para gestionar EC2 los recursos de Amazon asociados a un WorkSpaces pool, como subredes VPCs, zonas de disponibilidad, grupos de seguridad y tablas de enrutamiento.
- `s3`: permite el acceso para realizar las acciones necesarias en los buckets de Amazon S3 para los registros, la configuración de las aplicaciones y la característica de carpeta de inicio.

Commercial Regiones de AWS

La siguiente política de JSON se aplica al anuncio Regiones de AWS.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

AWS GovCloud (US) Regions

La siguiente política JSON se aplica a las AWS GovCloud (US) Regions comerciales.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

WorkSpaces actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas WorkSpaces desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
the section called “AmazonWorkSpacesPoolServiceAcces”: Añadió una nueva política.	WorkSpaces se ha añadido una nueva política gestionada para conceder permisos para ver Amazon EC2 VPCs y los recursos relacionados, y para ver y gestionar los buckets de	24 de junio de 2024

Cambio	Descripción	Fecha
	Amazon S3 para WorkSpaces grupos.	
the section called “AmazonWorkSpacesAdmin”: política actualizada	WorkSpaces agregó varias acciones para los WorkSpaces grupos a la política WorkSpacesAdmin administrada de Amazon, lo que permitió a los administradores acceder a administrar los recursos de los WorkSpace grupos.	24 de junio de 2024
the section called “AmazonWorkSpacesAdmin”: política actualizada	WorkSpaces agregó la `workspaces:RestoreWorkspace` acción a la política WorkSpacesAdmin gestionada por Amazon, otorgando a los administradores acceso a la restauración WorkSpaces.	25 de junio de 2023
the section called “AmazonWorkspacesPCAAccess”: Añadió una nueva política.	WorkSpaces se agregó una nueva política administrada para otorgar `acm-pca` permiso para administrar la CA AWS privada a fin de administrar la autenticación basada en certificados.	18 de noviembre de 2022
WorkSpaces comenzó a rastrear los cambios	WorkSpaces comenzó a realizar un seguimiento de los cambios de sus políticas WorkSpaces gestionadas.	1 de marzo de 2021

Acceso a las instancias de streaming WorkSpaces y a los scripts de las mismas

Las aplicaciones y los scripts que se ejecutan en las instancias de WorkSpaces streaming deben incluir AWS credenciales en sus solicitudes de AWS API. Puede crear un rol de IAM para administrar estas credenciales. Un rol de IAM especifica un conjunto de permisos que puedes usar para acceder a AWS los recursos. Sin embargo, este rol no se asocia de manera exclusiva a una persona. En su lugar, puede asumirlo cualquier usuario que lo necesite.

Puede aplicar un rol de IAM a una instancia de WorkSpaces streaming. Cuando la instancia de streaming cambia al rol (lo asume), el rol proporciona credenciales de seguridad temporales. La aplicación o los scripts utilizan estas credenciales para realizar acciones de API y tareas de administración en la instancia de streaming. WorkSpaces administra el cambio de credenciales temporal por usted.

Contenido

- Mejores prácticas para usar las funciones de IAM con WorkSpaces instancias de streaming
- Configuración de un rol de IAM existente para usarlo con WorkSpaces instancias de streaming
- Cómo crear un rol de IAM para usarlo con WorkSpaces instancias de streaming
- Cómo utilizar el rol de IAM con instancias de WorkSpaces streaming

Mejores prácticas para usar las funciones de IAM con WorkSpaces instancias de streaming

Cuando utilices funciones de IAM con instancias de WorkSpaces streaming, te recomendamos que sigas estas prácticas:

- Limita los permisos que concedes a las acciones y los recursos de la AWS API.

  Siga los principios de privilegios mínimos al crear y adjuntar políticas de IAM a las funciones de IAM asociadas a las instancias de WorkSpaces streaming. Cuando utilices una aplicación o un script que requiera acceso a acciones o recursos de la AWS API, determina las acciones y los recursos específicos que se requieren. A continuación, cree políticas que permitan a la aplicación o al script realizar únicamente tales acciones. Para obtener más información, consulte Concesión de mínimos privilegios en la Guía del usuario de IAM.
- Cree una función de IAM para cada WorkSpaces recurso.

Crear un rol de IAM único para cada WorkSpaces recurso es una práctica que sigue los principios de privilegios mínimos. Esto también le permite modificar los permisos de un recurso sin que ello afecte a otros recursos.

- Límite dónde se pueden utilizar las credenciales.

  Las políticas de IAM le permiten definir las condiciones en las que el rol de IAM se puede utilizar para acceder a un recurso. Por ejemplo, puede incluir condiciones para especificar un rango de direcciones IP desde el que pueden proceder las solicitudes. Esto impide que las credenciales se utilicen fuera de su entorno. Para obtener más información, consulte Utilizar condiciones de política para mayor seguridad en la Guía del usuario de IAM.

Configuración de un rol de IAM existente para usarlo con WorkSpaces instancias de streaming

En este tema se describe cómo configurar un rol de IAM existente para poder usarlo con. WorkSpaces

Requisitos previos

El rol de IAM que desee utilizar WorkSpaces debe cumplir los siguientes requisitos previos:

- La función de IAM debe estar en la misma cuenta de Amazon Web Services que la instancia de WorkSpaces streaming.
- El rol de IAM no puede ser un rol de servicio.
- La política de relaciones de confianza asociada a la función de IAM debe incluir el WorkSpaces servicio como principal. Un principal es una entidad AWS que puede realizar acciones y acceder a los recursos. La política también debe incluir la acción `sts:AssumeRole`. Esta configuración de política WorkSpaces se define como una entidad de confianza.

- Si va a aplicar la función de IAM a WorkSpaces, WorkSpaces debe ejecutar una versión del WorkSpaces agente publicada a partir del 3 de septiembre de 2019. Si va a aplicar la función de IAM a WorkSpaces, WorkSpaces debe utilizar una imagen que utilice una versión del agente publicada en la misma fecha o después.

Para permitir que el director del WorkSpaces servicio asuma una función de IAM existente

Para realizar los siguientes pasos, debe iniciar sesión en la cuenta como un usuario de IAM que tenga los permisos necesarios para enumerar y actualizar los roles de IAM. Si no tiene los permisos necesarios, pida al administrador de su cuenta de Amazon Web Services que realice estos pasos en su cuenta o que le conceda los permisos requeridos.

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. En la lista de roles de su cuenta, elija el nombre del rol que desee modificar.
4. Elija la pestaña Relaciones de confianza y, a continuación, Editar relación de confianza.
5. En Policy Document (Documento de política), compruebe que la política de relación de confianza incluya la acción `sts:AssumeRole` para la entidad principal del servicio `workspaces.amazonaws.com`:

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "workspaces.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Cuando haya terminado de editar la política de confianza, elija Update Trust Policy (Actualizar política de confianza) para guardar los cambios.
7. El rol de IAM que haya seleccionado se mostrará en la WorkSpaces consola. Este rol concede permisos a las aplicaciones y los scripts para realizar acciones de la API y tareas de administración en las instancias de streaming.

Cómo crear un rol de IAM para usarlo con WorkSpaces instancias de streaming

En este tema se describe cómo crear un nuevo rol de IAM para que pueda usarlo con WorkSpaces

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
3. En Seleccionar el tipo de entidad de confianza, elija Servicio de AWS .
4. En la lista de AWS servicios, elija WorkSpaces.
5. En Seleccione su caso de uso, ya está seleccionada la opción WorkSpaces — Permite que las WorkSpaces instancias llamen a los AWS servicios en su nombre. Elija Siguiente: permisos.
6. Si es posible, seleccione la política que desea utilizar para la política de permisos o elija Create policy (Crear política) para abrir una pestaña nueva del navegador y crear una política nueva desde cero. Para obtener más información, consulte el paso 4 del procedimiento Crear políticas de IAM (consola) en la Guía del usuario de IAM.

   Después de crear la política, cierre esa pestaña y vuelva a la pestaña original. Seleccione la casilla de verificación situada junto a las políticas de permisos que WorkSpaces desee tener.
7. (Opcional) Configure un límite de permisos. Se trata de una característica avanzada que está disponible para los roles de servicio, pero no para los roles vinculados a servicios. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
8. Elija Siguiente: etiquetas. Opcionalmente, puede asociar etiquetas como pares de clave-valor. Para obtener más información, consulte Etiquetado de usuarios y roles de IAM en la Guía del usuario de IAM.
9. Elija Siguiente: Revisar.
10. En Nombre de rol, escriba un nombre de rol único en su cuenta de Amazon Web Services. Como otros AWS recursos pueden hacer referencia al rol, no puedes editar el nombre del rol una vez creado.
11. En Role description (Descripción del rol), conserve la descripción del rol predeterminada o escriba una nueva.
12. Revise el rol y, a continuación, elija Crear rol.

Cómo utilizar el rol de IAM con instancias de WorkSpaces streaming

Después de crear un rol de IAM, puede aplicarlo al WorkSpaces momento del lanzamiento. WorkSpaces También puede aplicar un rol de IAM a uno existente. WorkSpaces

Al aplicar un rol de IAM a WorkSpaces, WorkSpaces recupera las credenciales temporales y crea el perfil de credenciales workspaces_machine_role en la instancia. Las credenciales temporales son válidas durante 1 hora y las nuevas credenciales se recuperan cada hora. Las credenciales anteriores no vencen, por lo que puede utilizarlas mientras sean válidas. Puede usar el perfil de credenciales para llamar a AWS los servicios mediante programación mediante la interfaz de línea de AWS comandos (AWS CLI), AWS las herramientas o el AWS SDK con el idioma que prefiera. PowerShell

Cuando realice llamadas a la API, especifique workspaces_machine_role como el perfil de credenciales. De lo contrario, la operación falla debido a los permisos insuficientes.

WorkSpaces asume la función especificada mientras se aprovisiona la instancia de streaming. Como WorkSpaces utiliza la interfaz de red elástica que está conectada a la VPC para las llamadas a la AWS API, la aplicación o el script deben esperar a que la interfaz de red elástica esté disponible antes de realizar las llamadas a la AWS API. Si las llamadas a la API se realizan antes de que la interfaz de red elástica esté disponible, las llamadas fallan.

Los siguientes ejemplos muestran cómo se puede utilizar el perfil de credenciales workspaces_machine_role para describir las instancias de streaming (instancias) EC2 y crear el cliente Boto. Boto es el SDK de Amazon Web Services (AWS) para Python.

Describa las instancias de streaming (EC2 instancias) mediante la AWS CLI

```
aws ec2 describe-instances --region us-east-1 --profile workspaces_machine_role
```

Describa las instancias de streaming (EC2 instancias) mediante AWS herramientas para PowerShell

Debe usar AWS Tools para la PowerShell versión 3.3.563.1 o posterior, con el Amazon Web Services SDK para .NET versión 3.3.103.22 o posterior. Puede descargar el instalador de AWS Herramientas para Windows, que incluye AWS Herramientas para PowerShell y el SDK de Amazon Web Services para .NET, desde el PowerShell sitio web AWS Herramientas para.

```
Get-EC2Instance -Region us-east-1 -ProfileName workspaces_machine_role
```

Creación del cliente Boto mediante el AWS SDK para Python

```
session = boto3.Session(profile_name=workspaces_machine_role')
```

Validación de conformidad para Amazon WorkSpaces

Los auditores externos evalúan la seguridad y el cumplimiento de Amazon WorkSpaces como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para ver una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulta los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad y . Para obtener información general, consulta Programas de conformidad de AWS.

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Para obtener más información acerca de WorkSpaces FedRAMP, consulte. Configure la autorización de FedRAMP o el cumplimiento de las normas SRG del DoD para personal WorkSpaces

Su responsabilidad de cumplimiento al WorkSpaces utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- 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 las consideraciones en materia de arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Diseño de arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden utilizar AWS para crear aplicaciones compatibles con la HIPAA.
- AWS Recursos de cumplimiento Recursos de : esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de los recursos con las reglas de la guía para AWS Config desarrolladores: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en Amazon WorkSpaces

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. 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 demora. 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 uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Amazon WorkSpaces también ofrece la redirección entre regiones, una función que funciona con las políticas de enrutamiento de conmutación por error del Sistema de nombres de dominio (DNS) para redirigir a WorkSpaces los usuarios a una alternativa WorkSpaces en otra AWS región cuando la principal WorkSpaces no está disponible. Para obtener más información, consulte Redirección entre regiones para Personal WorkSpaces .

Seguridad de la infraestructura en Amazon WorkSpaces

Como servicio gestionado, Amazon WorkSpaces está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a WorkSpaces través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) 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 principal de IAM. También puedes utilizar AWS

Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Contenido

- Aislamiento de red
- Aislamiento en hosts físicos
- Autorización de usuarios corporativos
- Cree y transmita desde puntos finales de VPC de interfaz
- Realice solicitudes a la WorkSpaces API de Amazon a través de un punto final de interfaz de VPC
- Cree una política de puntos de conexión de VPC para Amazon WorkSpaces
- Conecte su red privada a su VPC

Aislamiento de red

Una nube privada virtual (VPC) es una red virtual en su propia área aislada lógicamente en la nube. AWS Puede implementarla WorkSpaces en una subred privada de su VPC. Para obtener más información, consulte Configurar una VPC para personal 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 WorkSpace acceso a dispositivos de confianza con certificados válidos. Para obtener más información, consulte Restrinja el acceso a dispositivos de confianza para WorkSpaces uso personal.

Aislamiento en hosts físicos

Los diferentes WorkSpaces en el mismo host físico están aislados unos de otros a través del hipervisor. Es como si estuvieran en hosts físicos distintos. Cuando WorkSpace se elimina a, el hipervisor limpia la memoria que se le ha asignado (se establece en cero) antes de asignarla a una nueva. WorkSpace

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 Personal.

Para controlar aún más el acceso a su WorkSpaces, utilice la autenticación multifactorial. Para obtener más información, consulte Cómo habilitar la autenticación multifactor para AWS los servicios.

Cree y transmita desde puntos finales de VPC de interfaz

Una nube privada virtual (VPC) es una red virtual en su propia área, aislada lógicamente en la nube de Amazon Web Services. Si utiliza Amazon Virtual Private Cloud para alojar sus AWS recursos, puede establecer una conexión privada entre su VPC y. WorkSpaces Puede utilizar esta conexión para poder WorkSpaces comunicarse con los recursos de su VPC sin tener que pasar por la Internet pública.

Los puntos finales de la interfaz funcionan con una tecnología que le permite mantener el tráfico de streaming dentro de una VPC que especifique mediante direcciones IP privadas. AWS PrivateLink Cuando utilizas la VPC con un túnel de Direct AWS Connect o de red privada AWS virtual, puedes mantener el tráfico de streaming dentro de tu red.

Puede usar un punto de enlace de VPC en su AWS cuenta para restringir todo el tráfico de streaming entre su Amazon VPC y WorkSpaces la red. AWS Después de crear el punto final, configure el WorkSpaces directorio para usarlo.

Requisitos previos y limitaciones

Antes de configurar los puntos finales de la VPC WorkSpaces, tenga en cuenta los siguientes requisitos previos y limitaciones.

- Por el momento, la función solo está disponible para uso personal WorkSpaces . WorkSpaces Los grupos no admiten puntos de conexión de VPC para la transmisión.
- La función de punto de conexión de VPC está disponible exclusivamente para el uso de WorkSpaces Amazon DCV. Al configurar un punto de enlace de VPC para un directorio, los usuarios no pueden transmitir desde Amazon DCV a través de Internet. Sin embargo, puede habilitar la transmisión por Internet para PCo IP WorkSpaces en el mismo directorio durante la configuración del punto final de la VPC.
- Actualmente, la función solo admite puntos finales de IPv4 VPC. IPv6 y no se admiten los puntos finales de VPC de Dualstack.

- Para mantener el tráfico de streaming dentro de su VPC, utilice un punto final de VPC de streaming. Sus WorkSpaces clientes requieren conectividad a Internet para la autenticación de los usuarios. Habilite el acceso saliente en el puerto 443 (tanto UDP como TCP) para el tráfico de autenticación. Además, debe añadir los dominios y las direcciones IP necesarios a la lista de permitidos en función del método de autenticación que haya elegido. Para obtener una lista completa de los dominios de cada categoría, consulta Dominios y direcciones IP para añadirlos a tu lista de dominios permitidos.
  - CAPTCHA
  - Configuración de directorios
  - Puntos finales de autenticación con tarjeta inteligente anteriores a la sesión, si utiliza una tarjeta inteligente
  - Páginas de inicio de sesión del usuario
  - Agente de WS
  - WorkSpaces Puntos finales para el inicio de sesión único (SSO) de SAML
- La red a la que están conectados los dispositivos de sus usuarios debe poder enrutar el tráfico al punto final de la VPC.
- Debe tener una política de permisos de IAM para el usuario de IAM o el rol de IAM de su AWS cuenta para poder realizar la acción de API. `ec2:DescribeVpcEndpoints`
- WorkSpaces Los puntos finales de VPC de streaming actualmente no admiten el cifrado FIPS. Si ya has habilitado el cifrado FIPS para un directorio, debes inhabilitar el cifrado FIPS antes de configurar un punto final de VPC.
- AWS La integración de Global Accelerator (AGA) no está disponible cuando se transmite a través de un punto final de VPC.
- Cuando se configura un punto final de VPC para un directorio, los grupos de control de acceso IP especificados para el directorio ya no se aplican.

Configuración del punto final de VPC para la transmisión WorkSpaces

Para configurar un punto final de VPC para la WorkSpaces transmisión, complete los siguientes pasos:

Paso 1: Crear el grupo de seguridad

En este paso, crea un grupo de seguridad que permite a WorkSpaces los clientes comunicarse con el punto de conexión de VPC que va a crear.

1. En el panel de navegación de la EC2 consola de Amazon, ve a Red y seguridad y, a continuación, a Grupos de seguridad.
2. Selecciona Crear grupo de seguridad.
3. En Detalles básicos, ingresa lo siguiente:
   - Para el nombre del grupo de seguridad: introduzca un nombre único que identifique el grupo de seguridad.
   - Para la descripción: introduzca un texto que describa el propósito del grupo de seguridad.
   - Para la VPC: elija la VPC en la que se encuentra el punto final de la VPC.
4. Ve a Reglas de entrada y selecciona Agregar regla para crear reglas de entrada para el tráfico TCP.
5. Introduzca lo siguiente:
   - Para Tipo: selecciona TCP personalizado.
   - Para el rango de puertos: introduzca los siguientes números de puerto:`443,4195`.
   - Para el tipo de fuente: elija Personalizado.
   - Para el origen: introduzca el rango CIDR de IP privado u otro grupo de seguridad IDs desde el que los usuarios se conectan al punto final de la VPC. Asegúrese de permitir el tráfico entrante únicamente desde el origen de la IPv4 dirección.
6. Repita los pasos 4 y 5 para cada rango de CIDR o grupo de seguridad.
7. Vaya a Reglas de entrada y seleccione Agregar regla para crear reglas de entrada para el tráfico UDP.
8. Introduzca lo siguiente:
   - Para Tipo: selecciona UDP personalizado.
   - Para el rango de puertos: introduzca los siguientes números de puerto: 443, 4195.
   - Para el tipo de fuente, elija Personalizado.
   - Para la fuente: introduzca el mismo rango de CIDR IP privado o el mismo grupo de seguridad que IDs ingresó en el paso 5.
9. Repita los pasos 7 y 8 para cada UDP personalizado.
10. Selecciona Crear grupo de seguridad.

Paso 2: Crear el punto de conexión de VPC

En Amazon VPC, un punto de enlace de VPC le permite conectar su VPC a los servicios compatibles. AWS En este ejemplo, configuras Amazon VPC para que tus WorkSpaces usuarios puedan hacer streaming desde ella. WorkSpaces

1. Abra la Consola de Amazon VPC.
2. En el panel de navegación, vaya a Endpoints y, a continuación, a Create Endpoints.
3. Seleccione Crear punto de conexión.
4. Asegúrese de lo siguiente:
   - Categoría de servicio: asegúrese de que AWS los servicios estén seleccionados.
   - Nombre del servicio: selecciona com.amazonaws. ***Region***.prod.highlander.
   - VPC: elija una VPC en la que crear el punto final de la interfaz. Puede elegir una VPC diferente a la VPC con WorkSpaces recursos siempre que la red dirija el tráfico al punto final de la VPC.
   - Habilitar el nombre de DNS privado: la casilla de verificación está seleccionada. Si los usuarios utilizan un proxy de red para acceder a instancias de streaming, deshabilite cualquier almacenamiento en caché de proxy en los nombres de dominio y DNS asociados al punto de conexión privado. El nombre DNS del punto final de la VPC debe estar permitido a través del proxy.
   - Tipo de IP del registro DNS: elija IPv4. Actualmente no se admiten los tipos de IP de registro IPv6 DNS y Dualstack. Si seleccionas Dualstack o IPv6 , no podrás hacer streaming desde el punto de conexión de la WorkSpaces VPC.
   - Subredes: elija las subredes (zonas de disponibilidad) para crear el punto final de la VPC. Se recomienda elegir al menos dos subredes.
   - Tipo de dirección IP: elija IPv4.
   - Panel de grupos de seguridad: seleccione el grupo de seguridad que creó anteriormente.
5. (Opcional) En el panel Etiquetas, puede crear una o más etiquetas.
6. Seleccione Crear punto final.

Cuando el punto de conexión esté listo para usar, el valor de la columna Status (Estado) cambia a Available (Disponible).

Paso 3: Configurar el WorkSpaces directorio para usar el punto final de la VPC

Debe configurar el WorkSpaces directorio para usar el punto de enlace de VPC que creó para la transmisión.

1. Abra la WorkSpaces consola en la misma AWS región que el punto final de la VPC.
2. En el panel de navegación, selecciona Directorios y, a continuación,.
3. Seleccione el directorio que desee usar.
4. Ve a la sección de puntos finales de la VPC y, a continuación, a Editar.
5. En el cuadro de diálogo Editar punto de enlace de VPC, en Streaming Endpoint, seleccione el punto de enlace de VPC que ha creado.
6. Si lo desea, puede habilitar la opción Permitir que los usuarios con PCo IP WorkSpaces transmitan desde Internet.

   > **Note**
   >
   > Cuando está habilitada, los usuarios pueden transmitir desde su PCo IP WorkSpaces a través de Internet pública. De lo contrario, no se podrá acceder a la PCo IP WorkSpaces del directorio, ya que la PCo IP WorkSpaces no admite el punto final de la VPC para la transmisión.

7. Seleccione Guardar.

El tráfico de las nuevas sesiones de streaming se enrutará a través de este punto final de VPC. Sin embargo, el tráfico de las sesiones de streaming actuales sigue dirigiéndose a través del punto de conexión especificado anteriormente.

> **Note**
>
> Los usuarios con DCV WorkSpaces no pueden transmitir a través de la Internet pública cuando se especifica un punto final de VPC.

Realice solicitudes a la WorkSpaces API de Amazon a través de un punto final de interfaz de VPC

Puede conectarse directamente a los puntos de enlace de la WorkSpaces API de Amazon a través de un punto de enlace de interfaz en su nube privada virtual (VPC) en lugar de conectarse a través de Internet. Cuando utiliza un punto de enlace de interfaz de VPC, la comunicación entre su VPC y el punto de enlace de la WorkSpaces API de Amazon se lleva a cabo de forma completa y segura dentro de la red. AWS

> **Note**
>
> Esta función solo se puede utilizar para conectarse a los puntos de enlace de la WorkSpaces API. Para conectarse a WorkSpaces través de los WorkSpaces clientes, se requiere conectividad a Internet, tal y como se describe enRequisitos de dirección IP y puerto para WorkSpaces Personal.

Los puntos de enlace de la WorkSpaces API de Amazon son compatibles con los puntos de enlace de la interfaz Amazon Virtual Private Cloud (Amazon VPC) que funcionan con la tecnología de. AWS PrivateLink Cada punto final de la VPC está representado por una o más interfaces de red (también conocidas como interfaces de red elásticas o ENIs) con direcciones IP privadas en las subredes de la VPC.

El punto de enlace de la interfaz de VPC conecta su VPC directamente al punto de enlace de la WorkSpaces API de Amazon sin necesidad de una puerta de enlace a Internet, un dispositivo NAT, una conexión de VPN o una conexión. AWS Direct Connect Las instancias de tu VPC no necesitan direcciones IP públicas para comunicarse con el punto de enlace de la WorkSpaces API de Amazon.

Puede crear un punto final de interfaz para conectarse a Amazon WorkSpaces con los comandos AWS Management Console o AWS Command Line Interface (AWS CLI). Para obtener instrucciones, consulte Creating an Interface Endpoint.

Tras crear un punto de enlace de VPC, puede utilizar los siguientes comandos de CLI de ejemplo que utilizan el `endpoint-url` parámetro para especificar los puntos de enlace de la interfaz con el punto de enlace de la 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 WorkSpaces API de Amazon que la CLI y el WorkSpaces SDK de Amazon utilizan de forma predeterminada (https://api.workspaces). *Region*.amazonaws.com) se resuelve en tu punto final de VPC.

El punto de enlace de la WorkSpaces API de Amazon admite puntos de enlace de VPC en todas AWS las regiones en las que están disponibles Amazon VPC y Amazon. WorkSpaces Amazon WorkSpaces admite la realización de llamadas a todos sus públicos APIs dentro de su VPC.

Para obtener más información AWS PrivateLink, consulte la AWS PrivateLink documentación. 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 enlace de las WorkSpaces API de Amazon por región, consulta los puntos de enlace de las WorkSpaces API.

> **Note**
>
> Los puntos de enlace de la WorkSpaces API de Amazon no AWS PrivateLink son compatibles con los puntos de enlace de la WorkSpaces API de Amazon con el Estándar Federal de Procesamiento de Información (FIPS).

Cree una política de puntos de conexión de VPC para Amazon WorkSpaces

Puedes crear una política para los puntos de enlace de Amazon VPC para que Amazon especifique WorkSpaces lo siguiente:

- La entidad principal 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**
>
> Las políticas de puntos de enlace de VPC no son compatibles con los puntos de enlace de Amazon con el Estándar Federal de Procesamiento de Información (FIPS). WorkSpaces

El siguiente ejemplo de política de punto de enlace de VPC especifica que todos los usuarios que tienen acceso al punto de enlace de la interfaz de VPC pueden invocar el punto de enlace alojado en Amazon denominado. WorkSpaces `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 enlace WorkSpaces alojados en Amazon distintos de. `ws-f9abcdefg`
- Realizar una acción en cualquier recurso que no sea el especificado (WorkSpace ID:`ws-f9abcdefg`).

> **Note**
>
> En este ejemplo, los usuarios pueden seguir realizando otras acciones de la WorkSpaces API de Amazon desde fuera de la VPC. Para restringir las llamadas a la API a las que se

realizan desde la VPC, consulte Administración de identidad y acceso para WorkSpaces para obtener información sobre el uso de políticas basadas en la identidad para controlar el acceso a los puntos de enlace de las API de Amazon. WorkSpaces

Conecte su red privada a su VPC

Para llamar a la WorkSpaces API de Amazon a través de su VPC, debe conectarse desde una instancia que esté dentro de la VPC o conectar su red privada a su VPC mediante () o. AWS Virtual Private Network AWS VPN AWS Direct Connect Para más información, consulte Conexiones VPN en la Guía del usuario de Amazon Virtual Private Cloud (Amazon VPC). Para obtener más información AWS Direct Connect, consulte Crear una conexión en la Guía del AWS Direct Connect usuario.

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 WorkSpaces personal.

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.

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.

Recurso	Predeterminado/a	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

Recurso	Predeterminado/a	Descripción	Ajustable
		recomenda mos migrar tu paquete WorkSpace s a Graphics. G4DN. Para obtener más informaci ón, consulte Migrar un WorkSpace archivo en WorkSpaces Personal.	
GeneralPurpose4 x grande WorkSpaces	1	El número máximo de GeneralPu rpose .4xlarge WorkSpaces en esta cuenta en la región actual.	Sí
GeneralPurpose.8x grande WorkSpaces	1	El número máximo de GeneralPu rpose .8xlarge WorkSpaces en esta cuenta en la región actual.	Sí
Gráficos. G4dn WorkSpaces	0	El número máximo de WorkSpaces Graphics.g4dn en esta cuenta en la región actual.	Sí

Recurso	Predeterminado/a	Descripción	Ajustable
GraphicsPro WorkSpaces	0	El número máximo de GraphicsPro WorkSpaces en esta cuenta en la región actual. (el GraphicsPro paquete estará disponible end-of-life el 31 de octubre de 2025). Considere la posibilidad de utilizar otros paquetes compatibles como reemplazo.)	Sí
GraphicsPro.g4dn WorkSpaces	0	El número máximo de GraphicsPro .g4dn WorkSpaces en esta cuenta en la región actual.	Sí
En espera WorkSpaces	5	El número máximo de WorkSpaces en esta cuenta en la región actual.	Sí
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

Recurso	Predeterminado/a	Descripción	Ajustable
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
Grupos de control de acceso a direcciones IP por directorio	25	El número máximo de grupos de control de acceso a direccion es 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

Recurso	Predeterminado/a	Descripción	Ajustable
WorkSpaces Piscinas	10	El número máximo de WorkSpaces grupos de esta cuenta en la región actual.	Sí
Instancias de streaming de Value de uso general para WorkSpaces grupos	10	El número máximo de instancias de streaming de valor de uso general que se pueden usar para los WorkSpaces grupos de esta cuenta en la región actual.	Sí
Instancias de streaming estándar de uso general para WorkSpaces grupos	10	El número máximo de instancias estándar de uso general que se pueden usar para los WorkSpaces grupos de esta cuenta en la región actual.	Sí
Instancias de streaming de rendimiento de uso general para WorkSpaces grupos	10	El número máximo de instancias de streaming de rendimiento de uso general que se pueden usar para los WorkSpaces grupos de esta cuenta en la región actual.	Sí

Recurso	Predeterminado/a	Descripción	Ajustable
Instancias de streaming de Power de uso general para WorkSpaces grupos»	10	El número máximo de instancias de streaming de Power de uso general que se pueden usar para los WorkSpaces grupos de esta cuenta en la región actual.	Sí
Instancias de PowerPro streaming de uso general para WorkSpaces grupos»	10	El número máximo de instancias de PowerPro streaming de uso general que se pueden usar para los WorkSpaces grupos de esta cuenta en la región actual.	Sí
Instancias de streaming Graphics. G4DN xlarge para grupos WorkSpaces	0	El número máximo de instancias de streaming xlarge de Graphics.g4dn que se pueden usar para los grupos de esta cuenta en la región actual. WorkSpaces	Sí

Recurso	Predeterminado/a	Descripción	Ajustable
Instancias de streaming Graphics. G4DN 4xlarge para grupos WorkSpaces	0	El número máximo de instancias de streaming de Graphics.G4DN 4xlarge que se pueden usar para los grupos de esta cuenta en la región actual. WorkSpaces	Sí
WorkSpaces Instancias gestionadas principales	1 000	El número máximo de instancias gestionadas WorkSpaces principales de esta cuenta en la región actual.	Sí

Limitación de la API

La tarifa permitida es de dos llamadas por segundo. Para obtener más información, consulte Excepciones de limitación.

Política de fin de vida útil de las aplicaciones WorkSpaces cliente

La política de WorkSpaces fin de vida útil (EOL) de Amazon se aplica a versiones principales específicas (y a todas sus versiones secundarias) de WorkSpaces clientes para WorkSpaces Personal y WorkSpaces Pools.

El ciclo de vida de una versión de WorkSpaces cliente 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 WorkSpaces cliente y dura un tiempo fijo. Durante la fase de soporte general, el equipo de WorkSpaces soporte proporciona 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 WorkSpaces cliente.

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 funciones se implementan únicamente para las versiones más recientes del WorkSpaces cliente. No se implementan para las versiones más antiguas. Durante la fase de orientación técnica, si es necesaria una corrección, la AWS programará para la próxima versión que esté disponible para el público y tendrá la opción de actualizar a la última WorkSpaces versión 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. Tras la fecha de fin de vida, no se proporcionará ningún otro tipo de asistencia o mantenimiento. AWS detiene las pruebas para detectar problemas de compatibilidad. Para continuar con el soporte, debe actualizar a la última versión del WorkSpaces cliente.

Consulte esta tabla para obtener más información acerca de la compatibilidad con versiones específicas.

> **Important**
>
> Support para las siguientes versiones finalizará el 31 de marzo de 2025. Asegúrese de actualizar a una versión de cliente compatible antes de que lleguen a su fin de vida para evitar la interrupción del servicio.
>
> - Windows 3.x, 4.x y 5.0-5.22.0

- Linux 4.x, 2023.x y 2024.0-2024.5 para Ubuntu 20.04
- Linux 2023.x y 2024.0-2024.5 para Ubuntu 22.04
- macOS 3.x, 4.x y 5.1-5.22.0
- Android 3.x, 4.x y 5.0.0

Cliente de Windows	Soporte general	Orientación técnica	EOL	Notas
5.22.1+	3 de septiembre de 2024			Compatible
5,0-5,22,0	2 de junio de 2022	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
4.x	30 de junio de 2021	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
3.x	25 de noviembre de 2019	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance

Cliente de Windows	Soporte general	Orientación técnica	EOL	Notas
				su fecha de fin de vida.

Cliente de Linux	Soporte general	Orientación técnica	EOL	Notas
2024.6+ para Ubuntu 22.04	6 de septiembre de 2024			Compatible
2024.6+ para Ubuntu 20.04	6 de septiembre de 2024			Compatible
2024.0-2024.5 para Ubuntu 22.04	28 de febrero de 2024	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
2024.0-2024.5 para Ubuntu 20.04	24 de agosto de 2023	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
2023.x para Ubuntu 22.04	24 de agosto de 2023	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes

Cliente de Linux	Soporte general	Orientación técnica	EOL	Notas
				de que esta versión alcance su fecha de fin de vida.
2023.x para Ubuntu 20.04	24 de agosto de 2023	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
4.x para Ubuntu 20.04	27 de octubre de 2022	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.

Cliente para macOS	Soporte general	Orientación técnica	EOL	Notas
5.22.1+	3 de septiembre de 2024			Compatible
5.1-5.22.0	30 de junio de 2022	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta

Cliente para macOS	Soporte general	Orientación técnica	EOL	Notas
				versión alcance su fecha de fin de vida.
4.x	5 de agosto de 2021	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
3.x	25 de noviembre de 2019	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.

Cliente para iPad	Soporte general	Orientación técnica	EOL	Notas
2.x	2019			Compatible

Cliente de Android	Soporte general	Orientación técnica	EOL	Notas
5.0.1+	6 de noviembre de 2024			Compatible

Cliente de Android	Soporte general	Orientación técnica	EOL	Notas
5.0.0	26 de febrero de 2024	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
4.x	12 de mayo de 2022	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.
3.x	30 de junio de 2021	21 de noviembre de 2024	31 de marzo de 2025	Asegúrese de actualizar a la última versión del cliente antes de que esta versión alcance su fecha de fin de vida.

Acceso web	Soporte general
Google Chrome	Versión actual, más las dos versiones principales más recientes

Acceso web	Soporte general
Firefox	Versión actual, más las dos versiones principales más recientes
Microsoft Edge	Versión actual, más las dos versiones principales más recientes

Versiones de cliente no compatibles

Los siguientes WorkSpaces clientes 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 compatible
Windows	5.10	19 de junio de 2023	1 de octubre de 2023	1 de octubre de 2023	No compatible
Windows	5.9	9 de mayo de 2023	1 de octubre de 2023	1 de octubre de 2023	No compatible
Windows	2.x	2018	31 de marzo de 2023	31 de agosto de 2023	No compatible
Ubuntu	4.x para Ubuntu 18.04	12 de agosto de 2021	31 de marzo de 2023	31 de agosto de 2023	No compatible
Ubuntu	3.x para Ubuntu 18.04	25 de noviembre de 2019	31 de marzo de 2023	31 de agosto de 2023	No compatible
macOS	2.x	2019	31 de marzo de 2023	31 de agosto de 2023	No compatible

Sistema operativo	Versión del cliente	Soporte general	Orientación técnica	EOL	Notas
macOS	1.x	2018	31 de marzo de 2023	31 de agosto de 2023	No compatible
iPad	1.x	2018	31 de marzo de 2023	31 de agosto de 2023	No compatible
Android	2.x	2019	31 de marzo de 2023	31 de agosto de 2023	No compatible
Android	1.x	2018	31 de marzo de 2023	31 de agosto de 2023	No compatible

EOL FAQs

Estoy usando una versión de un WorkSpaces cliente que ha alcanzado su EOL. ¿Qué debo hacer para actualizar a una versión compatible?

Vaya a la página de descargas del WorkSpaces cliente para descargar e instalar una versión totalmente compatible de WorkSpaces.

¿Puedo usar una versión del WorkSpaces cliente que haya alcanzado su fin de vida con una versión compatible? WorkSpace

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, póngase en contacto con el equipo de AWS soporte para obtener más información.

Estoy usando una versión de un WorkSpaces cliente que ha alcanzado su fin de vida. ¿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 .

Estoy usando una versión de WorkSpaces cliente compatible en un sistema operativo que ha alcanzado su EOL. ¿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 ofrecen asistencia a WorkSpaces los clientes que utilizan sistemas operativos que han alcanzado su fin de vida. Utilice un sistema operativo compatible para garantizar que sus WorkSpaces clientes cuenten con el soporte necesario.

Extensión SDK compatible con DCV

El DCV permite un acceso remoto de alto rendimiento a WorkSpaces las instancias para una amplia gama de cargas de trabajo y casos de uso. Con el SDK de extensión Amazon DCV, los desarrolladores pueden personalizar la WorkSpaces experiencia de DCV para los usuarios finales, lo que incluye:

- 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 SDK de Amazon DCV, consulte la documentación de Amazon DCV Extension SDK. Puede encontrar el propio SDK en el GitHub repositorio del SDK de Amazon DCV Extension. Además, también puede encontrar ejemplos de integración del SDK en el GitHub repositorio de muestras del SDK de Amazon DCV Extension.

Los siguientes son compatibles WorkSpaces con.

- Protocolo de transmisión: DCV
- WorkSpaces Cliente de Windows: Windows: 5.9.0.4110 y superior.

> **Note**
>
> WorkSpaces Los clientes de Android e iOS y el acceso web no son compatibles con el SDK de extensión DCV.

- WorkSpaces compatibles: servidores Windows, Linux y Ubuntu

Historial de documentos para WorkSpaces

En la siguiente tabla se describen los cambios importantes en el WorkSpaces servicio y en la Guía de WorkSpaces administración de Amazon a partir del 1 de enero de 2018. Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

Para recibir notificaciones sobre estas actualizaciones, puedes suscribirte a la WorkSpaces fuente RSS.

Cambio	Descripción	Fecha
Modos de ejecución	El modo de funcionamiento de un WorkSpaces pool determina su disponibilidad inmediata y su método de pago. Puede elegir entre los dos modos de ejecución al crear un WorkSpaces grupo.	15 de mayo de 2025
Directorio de Microsoft Entra ID	Se admite la integración entre regiones entre el IAM Identity Center. WorkSpaces	27 de febrero de 2025
Directorio de Microsoft Entra ID	Puede crear un directorio de Microsoft Entra ID dedicado.	26 de agosto de 2024
Microsoft Visual Studio	Los paquetes de Microsoft Visual Studio son compatibl es con la opción Administrar aplicaciones.	1 de agosto de 2024
Extensión de redirecci onamiento de WebRTC de Amazon DCV	Puede instalar la extensión de redireccionamiento de WebRTC de Amazon DCV para utilizar el redirecci onamiento de WebRTC.	1 de agosto de 2024

WorkSpaces Pools ya está disponible en AWS GovCloud (US) Region	WorkSpaces Pools ofrece escritorios virtuales no persistentes diseñados para los usuarios que necesitan acceso bajo demanda a entornos de escritorio altamente seleccionados alojados en una infraestructura efímera.	23 de julio de 2024
WorkSpaces Pools ya está disponible	WorkSpaces Pools ofrece escritorios virtuales no persistentes diseñados para los usuarios que necesitan acceso bajo demanda a entornos de escritorio altamente seleccionados alojados en una infraestructura efímera.	27 de junio de 2024
AmazonWorkSpacesAdmin actualización de políticas gestionadas y nueva política gestionada AmazonWorkSpacesPoolServiceAccess	WorkSpaces actualizó la política AmazonWorkSpacesAdmin administrada y agregó la nueva política AmazonWorkSpacesPoolServiceAccess administrada.	27 de junio de 2024
AmazonWorkSpacesAdmin actualización de política gestionada	WorkSpaces añadió los espacios de trabajo: RestoreWorkspace acción a la política AmazonWorkSpacesAdmin gestionada, que permitía a los administradores acceder a la restauración. WorkSpaces	17 de julio de 2023

Extensión SDK compatible con DCV	Con el SDK de extensión de Amazon DCV, los desarroll adores pueden personalizar la WorkSpaces experiencia de DCV para los usuarios finales.	25 de mayo de 2023
Versiones del agente de host de DCV	Información sobre la versión de DCV.	8 de mayo de 2023
Amazon WorkSpaces se lanzó en AWS GovCloud (este de EE. UU.)	Amazon WorkSpaces está disponible en el AWS GovCloud este de EE. UU.	3 de mayo de 2023
Soporte para WorkSpaces cámaras web de Amazon	Amazon WorkSpaces ahora admite audio y vídeo (AV) en tiempo real al redirigir sin problemas la entrada de vídeo de la cámara web local a los WorkSpaces escritorios Windows mediante DCV.	5 de abril de 2021
Compatibilidad con tarjetas WorkSpaces inteligentes de Amazon con la aplicación cliente WorkSpaces macOS	Ahora puede utilizar la aplicación cliente Amazon WorkSpaces macOS con tarjetas inteligentes Common Access Card (CAC) y personal Identity Verification (PIV). La compatibilidad con tarjetas inteligentes está disponible cuando se WorkSpaces utiliza DCV.	5 de abril de 2021

Gestión de WorkSpaces paquetes de Amazon APIs	La gestión de WorkSpace s paquetes de Amazon ya APIs está disponible. Estas acciones de la API admiten las operaciones de creación, eliminación y asociación de imágenes para WorkSpaces paquetes.	15 de marzo de 2021
Amazon WorkSpaces se lanzó en Asia Pacífico (Mumbai)	Amazon WorkSpaces está disponible en la región Asia Pacífico (Bombay).	8 de marzo de 2021
Tarjetas inteligentes	Amazon WorkSpaces ahora admite la autenticación con tarjeta inteligente previa a la sesión (inicio de sesión) y durante la sesión en Windows y Linux WorkSpaces en la región AWS GovCloud (EE. UU. Oeste).	1 de diciembre de 2020
DCV	El DCV ya está disponible tanto para Windows 10 con licencia incluida (Windows Server 2016) como para Windows 10 en todos los tipos de paquetes, excepto WorkSpaces en Graphics y. GraphicsPro El DCV también está disponible para Linux WorkSpaces en la región (EE. UU.-Oeste). AWS GovCloud	1 de diciembre de 2020

Compartir imágenes personalizadas	Ahora puede compartir WorkSpaces imágenes personalizadas en todas AWS las cuentas. Una vez que se ha compartido una imagen, la cuenta del destinatario puede copiarla y utilizarla para crear paquetes para lanzar nuevos WorkSpaces.	1 de octubre de 2020
Redireccionamiento entre regiones	Ahora puedes usar la redirección entre regiones, una función que funciona con las políticas de enrutamiento del Sistema de Nombres de Dominio (DNS) para redirigir a los usuarios a una alternativa WorkSpaces cuando la principal WorkSpaces no esté disponible.	10 de septiembre de 2020
Suscríbase a Microsoft Office 2016 o 2019 para BYOL WorkSpaces	Ahora puede suscribirse a Microsoft Office Professional 2016 o 2019, que se proporciona con la licencia Bring Your Own Windows License (BYOL) WorkSpaces. AWS	3 de septiembre de 2020
Automatización BYOL en China (Ningxia)	Puede utilizar la automatización Bring Your Own License (BYOL) para simplificar el proceso de uso de sus licencias de escritorio de Windows 10 WorkSpaces en China (Ningxia).	2 de abril de 2020

Comprobador de imágenes	La herramienta Image Checker te ayuda a determina r si tu Windows WorkSpace cumple con los requisitos para la creación de imágenes. El comprobador de imágenes realiza una serie de pruebas con las WorkSpace que desea utilizar para crear la imagen y proporciona instrucciones sobre cómo resolver cualquier problema que encuentre.	30 de marzo de 2020
Migración WorkSpaces	La función de WorkSpace s migración de Amazon le permite migrar WorkSpace de un paquete a otro y, al mismo tiempo, conservar los datos del volumen de usuarios. Puede usar esta función para migrar WorkSpaces de la experiencia de escritorio de Windows 7 a la experienc ia de escritorio de Windows 10. También puede usar esta función para migrar WorkSpaces de un paquete público o personalizado a otro.	9 de enero de 2020

PrivateLink integración para Amazon WorkSpaces APIs	Puede conectarse directamente a los puntos de enlace de la WorkSpaces API de Amazon a través de un punto de enlace de interfaz en su Virtual Private Cloud (VPC) en lugar de conectarse a través de Internet. Cuando utiliza un punto de enlace de interfaz de VPC, la comunicación entre su VPC y el punto de enlace de la WorkSpaces API de Amazon se lleva a cabo de forma completa y segura dentro de la red. AWS	25 de noviembre de 2019
Cliente Linux para Amazon WorkSpaces	Los usuarios ahora pueden usar el cliente Linux para acceder a sus WorkSpaces.	25 de noviembre de 2019
Amazon WorkSpaces se lanza en China (Ningxia)	Amazon WorkSpaces está disponible en la región China (Ningxia).	13 de noviembre de 2019
Restaure WorkSpaces al último estado saludable conocido	Puede utilizar la función de restauración para volver WorkSpace a su último estado de funcionamiento conocido.	18 de septiembre de 2019

Cifrado de puntos de conexión de FIPS	Para cumplir con el Programa federal de gestión de riesgos y autorizaciones (FedRAMP) o la Guía de requisitos de seguridad de la computación en nube (SRG) del Departamento de Defensa (DoD), puede configurar WorkSpaces Amazon para que utilice el cifrado de puntos finales de los estándares federales de procesamiento de información (FIPS) a nivel de directorio.	12 de septiembre de 2019
WorkSpace Copie imágenes	Puede copiar las imágenes dentro de la misma región o en otras regiones.	27 de junio de 2019
Capacidades de WorkSpace administración de autoservicio para los usuarios	Puede habilitar las capacidades WorkSpace de administración de autoservicio para que sus usuarios tengan más control sobre su experiencia.	19 de noviembre de 2018
Automation de BYOL	Puede utilizar la automatización Bring Your Own License (BYOL) para simplificar el proceso de uso de sus licencias de escritorio de Windows 7 y Windows 10 para su. WorkSpaces	16 de noviembre de 2018
PowerPro y paquetes GraphicsPro	Los GraphicsPro paquetes PowerPro y ya están disponibles para. WorkSpaces	18 de octubre de 2018

Supervise los inicios de sesión correctos WorkSpace	Puede utilizar los eventos de Amazon CloudWatch Events para supervisar los WorkSpace inicios de sesión correctos y responder a ellos.	17 de septiembre de 2018
Acceso web para Windows 10 WorkSpaces	Los usuarios ahora pueden usar el cliente de acceso web para acceder a una experienc ia de escritorio en WorkSpace ejecución de Windows 10.	24 de agosto de 2018
Inicio de sesión con URI	Puede usar identificadores de recursos uniformes (URIs) para proporcionar a los usuarios acceso a sus WorkSpaces.	31 de julio de 2018
Amazon Linux WorkSpaces	Puede aprovisionar Amazon Linux WorkSpaces para sus usuarios.	26 de junio de 2018
Grupos de control de acceso a direcciones IP	Puede controlar las direccion es IP desde las que los usuarios pueden acceder a sus WorkSpaces.	30 de abril de 2018
Actualizaciones locales	Puede actualizar el BYOL de Windows 10 WorkSpaces a una versión más reciente de Windows 10.	9 de marzo de 2018

Actualizaciones anteriores

En la siguiente tabla se describen las incorporaciones importantes al WorkSpaces servicio de Amazon y su documentación establecidas antes del 1 de enero de 2018.

Cambio	Descripción	Fecha
Opciones de computación flexibles	Puedes cambiar 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 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 a los que tiene acceso WorkSpaces. Además, puede restringir el acceso WorkSpaces a dispositi vos de confianza (también conocidos como dispositivos gestionados).	19 de junio de 2017
Confianzas entre bosques	Puede establecer una relación de confianza entre su Microsoft AD AWS administrado y su dominio de Microsoft Active Directory local y, a continuación, aprovisionar a WorkSpaces los usuarios del dominio local.	9 de febrero de 2017
Paquetes de Windows Server 2016	WorkSpaces ofrece paquetes que incluyen una experiencia de escritorio de Windows 10, con la tecnología de Windows Server 2016.	29 de noviembre de 2016
Acceso web	Puede acceder a Windows WorkSpaces desde un navegador web mediante WorkSpaces Web Access.	18 de noviembre de 2016
Por hora WorkSpaces	Puede configurarlo WorkSpaces para que a los usuarios se les facture por hora.	18 de agosto de 2016
BYOL de Windows 10	Puede llevar 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 rastrear su. WorkSpaces	17 de mayo de 2016
Registros guardados	Cada vez que ingresas un nuevo código de registro, el WorkSpaces cliente lo guarda. Esto facilita el cambio entre WorkSpaces diferentes directorios o regiones.	28 de enero de 2016
BYOL para Windows 7, cliente Chromebook, cifrado WorkSpace	Puede llevar su licencia de escritorio de Windows 7 a WorkSpaces (BYOL), usar el cliente Chromebook y usar el cifrado. WorkSpace	1 de octubre de 2015
CloudWatch supervisión	Se agregó información sobre el CloudWatch monitoreo.	28 de abril de 2015
Reconexión automática de sesiones	Se agregó información sobre la función de reconexión automática de sesiones en las aplicaciones cliente WorkSpaces de escritorio.	31 de marzo de 2015
Direcciones IP públicas	Puede asignar automáticamente una dirección IP pública a su WorkSpaces.	23 de enero de 2015
WorkSpaces lanzado 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	Puedes crear una imagen a partir de una imagen WorkSpace que hayas personalizado y un WorkSpace paquete personalizado a partir de la imagen.	28 de octubre de 2014

Cambio	Descripción	Fecha
PCoSoporte para clientes IP zero	Puede acceder a los dispositivos cliente con WorkSpaces PCo IP cero.	15 de octubre de 2014
WorkSpaces lanzado en Asia Pacífico (Tokio)	WorkSpaces está disponible en la región Asia-Pacífico (Tokio).	26 de agosto de 2014
Compatibilidad con impresoras locales	Puede habilitar la compatibilidad con impresoras locales para su 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 coloquen las cuentas de las WorkSpace máquinas y un dominio independiente en el que se creen las cuentas de las WorkSpace máquinas.	7 de julio de 2014
Añadir grupos de seguridad	Puede añadir un grupo de seguridad a su WorkSpaces.	7 de julio de 2014
WorkSpaces lanzado en Asia Pacífico (Sídney)	WorkSpaces está disponible en la región Asia-Pacífico (Sídney).	15 de mayo de 2014
WorkSpaces lanzado en Europa (Irlanda)	WorkSpaces está disponible en la región 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.