Linux Virtual Delivery Agent 2507 LTSR

Importante:

La estrategia del ciclo de vida del producto para las versiones actuales (CR) y las versiones de servicio a largo plazo (LTSR) se describe en Hitos del ciclo de vida.

El Virtual Delivery Agent (VDA) de Linux permite el acceso a las aplicaciones y escritorios virtuales de Linux desde cualquier lugar y desde cualquier dispositivo donde esté instalada la aplicación Citrix Workspace™.

Puede entregar aplicaciones y escritorios virtuales basados en distribuciones de Linux compatibles. Instale el software VDA en sus máquinas virtuales (VM) Linux, configure el Delivery Controller y, a continuación, utilice Citrix Studio para poner las aplicaciones y los escritorios a disposición de los usuarios.

Novedades

La Actualización Acumulativa 2 (CU2) es la última versión del Agente de entrega virtual de Linux 2507 LTSR. CU2 añade más de seis correcciones en comparación con la versión inicial 2507 LTSR y CU1 del Agente de entrega virtual de Linux.

Actualización acumulativa 2 (CU2)

Fecha de lanzamiento: August 18, 2026

Novedades

Se requiere una nueva versión de .NET

A partir de esta versión, debe instalar .NET Runtime 10 en algunas distribuciones de Linux compatibles antes de instalar el Linux VDA. Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde la fuente integrada. De lo contrario, instale .NET desde la fuente de paquetes de Microsoft. Consulte más detalles en los requisitos del sistema.

Compatibilidad con RHEL y Rocky Linux 9.8, Debian 12.15, AlmaLinux 9.8 (limitado)

El Linux VDA ahora es compatible con las siguientes distribuciones de Linux:

- RHEL 9.8
- Rocky Linux 9.8
- Debian 12.15
- AlmaLinux 9.8 (limitado)

Para obtener más información sobre las distribuciones de Linux compatibles, consulte Requisitos del sistema.

Mover archivos de socket de $HOME y /tmp al directorio de tiempo de ejecución del SO

Los archivos de socket de dominio Unix creados anteriormente en $HOME o /tmp ahora se colocan en `/run/user/<uid>` (directorio de tiempo de ejecución de systemd), con un respaldo automático a `/var/xdl/user/<uid>` o `/var/xdl/user` cuando no estén disponibles. Las

sesiones en directorios de inicio de solo lectura o montados en NFS ya no fallan, y systemd limpia automáticamente los archivos de socket cuando finalizan las sesiones.

Problemas resueltos

- Cuando utiliza el cliente Mac con Linux VDA y el nombre del dispositivo de la cámara web contiene caracteres especiales, la cámara web no funciona y puede provocar que la aplicación se bloquee.
- Cuando utiliza Linux VDA con autenticación FAS y redirección de tarjeta inteligente en la sesión en la versión 2511 o posterior, las aplicaciones pueden dejar de responder o tardar mucho más en iniciarse.
- Cuando se vuelve a conectar a una sesión de Linux VDA desconectada que utiliza autenticación con tarjeta inteligente, y la ventana de LogonUI se cierra o la conexión ICA se interrumpe, la sesión se vuelve irrecuperable y muestra una pantalla gris en los intentos de reconexión posteriores.
- Cuando la conexión de red de un cliente se interrumpe y luego se vuelve a conectar mediante Auto Client Reconnect (ACR), las sesiones de Linux VDA pueden bloquearse o cerrarse inesperadamente.
- Cuando un Linux VDA se vuelve a conectar mientras el Servicio de autenticación federada (FAS) está en uso, un retraso en la autenticación puede causar fallos de autenticación e impedir el registro del VDA.
- Cuando varios usuarios inician sesión en un Linux VDA simultáneamente, el servicio ctxhdx puede detenerse inesperadamente, lo que provoca inestabilidad en la sesión o fallos de conexión.
- Cuando utiliza Linux VDA 2507 LTSR CU1 en Red Hat Enterprise Linux 8 con una GPU NVIDIA dedicada, las sesiones pueden bloquearse aleatoriamente debido a fallos de GNOME y errores de memoria.
- Cuando actualiza máquinas Linux VDA en Azure o crea un nuevo catálogo, los inicios de sesión pueden fallar durante 45 minutos a dos horas debido al inicio retrasado de Xorg y a los servicios de red no preparados.
- Cuando actualiza Linux VDA de la versión 2402 a la 2507 en un entorno implementado con MCS, el servicio de tarjeta inteligente (ctxscardsd.service) se inicia y luego se detiene inmediatamente después del arranque, lo que impide la autenticación con tarjeta inteligente.
- Cuando una sesión 3D de Linux VDA se vuelve a conectar después de que el sistema se reanude de la hibernación, la reconexión falla y la sesión se cierra.

- Cuando actualiza Linux VDA a la versión 2507, el servicio de tarjeta inteligente se inicia y luego se detiene después del arranque, lo que impide la autenticación con tarjeta inteligente.
- En Linux VDA versión 2402 o anterior con AppStream 2 y un gestor de visualización Xfce o MATE, la aplicación Citrix Workspace no se muestra en modo de pantalla completa en una configuración de varios monitores.
- Cuando se vuelve a conectar a una sesión de Linux VDA después de que su ticket del Servicio de autenticación federada (FAS) caduque o se vuelva a emitir, un error de "Inicio de sesión no válido" le impide volver a conectarse a su sesión existente.
- Cuando utiliza métodos de entrada coreanos en una sesión ICA de Ubuntu VDA, la tecla de cambio de teclado coreano/inglés no funciona como se espera.

Actualización acumulativa 1 (CU1)

Fecha de lanzamiento: December 16, 2025

Novedades

Soporte para Debian 12.12, AlmaLinux 9.6

El VDA de Linux ahora es compatible con las siguientes distribuciones de Linux: Debian 12.12 AlmaLinux 9.6 (Limitado) Para obtener más información sobre las distribuciones de Linux compatibles, consulte Requisitos del sistema.

Soporte para la redirección USB en máquinas virtuales de Azure

Con esta versión, nos complace anunciar la compatibilidad con la redirección USB para máquinas virtuales de Azure que ejecutan Canonical Ubuntu 22.04 y 24.04. Dado que estas plataformas no incluyen ciertos controladores de kernel USB de forma predeterminada, ahora ofrecemos una solución flexible que le permite compilar y cargar los módulos de controlador de kernel necesarios para dispositivos USB específicos.

Para obtener más detalles, consulte Redirección de dispositivos USB

Recopilación y carga de registros AOT

A partir de esta versión, Linux VDA admite la recopilación y carga de registros AOT a un servidor de registros centralizado, lo que permite una mejor solución de problemas en todos los componentes de Citrix.

Para obtener más detalles, consulte Recopilación de registros AOT

Integrar VDA de Linux no unido a un dominio con Red Hat IdM

A partir de esta versión, Linux VDA ofrece una solución de integración verificada en laboratorio con Red Hat Identity Management (IdM) para entornos no unidos a un dominio. Esto proporciona una mayor flexibilidad para implementaciones sin una integración directa entre Linux VDA y los dominios tradicionales de Active Directory.

Para obtener más detalles, consulte Integrar VDA de Linux no unido a un dominio con Red Hat IdM

Problemas resueltos

- Cuando utiliza la redirección USB en entornos de Azure con Ubuntu 24.04, la creación del módulo del kernel USB podría fallar.
- Al desinstalar el agente Linux VDA 2507, el proceso podría no completarse correctamente.
- Podría encontrar un problema de "Inicio de sesión no válido" con FAS al usar LVDA 2507 en RHEL 8.10.
- Cuando utiliza VDI de Ubuntu, los binarios pueden vincularse incorrectamente a las bibliotecas de Citrix en /opt/Citrix/VDA/lib64 en lugar de a las bibliotecas del sistema, como /usr/lib
- Al volver a conectarse a un escritorio publicado de Citrix después de la autenticación con tarjeta inteligente, la sesión puede fallar en Debian 12, Ubuntu 22.04, RHEL 8.10 y 9.6.
- Podría experimentar un error de registro al usar RHEL 8.10 en un Linux VDA.
- Cuando utiliza controladores NVIDIA más recientes que la versión 555 con Citrix VDA 24.02 LTSR CU2, una biblioteca que falta puede causar problemas de compatibilidad.
- Cuando utiliza la redirección del portapapeles con VDA de Linux, la función de copiar y pegar puede fallar intermitentemente entre Linux y Windows.
- Al usar LVDA 2507 con autenticación FAS, el certificado de usuario FAS puede fallar al decodificarse, lo que puede impedir un procesamiento posterior y terminar la sesión.

Novedades

Novedades en 2507 LTSR

Compatibilidad con Debian 12.11, RHEL y Rocky Linux 9.6

El VDA de Linux ahora es compatible con las siguientes distribuciones de Linux:

- Debian 12.11

- RHEL 9.6
- Rocky Linux 9.6

Para obtener más información sobre las distribuciones de Linux compatibles, consulte Requisitos del sistema.

Funcionalidades de implementación de Smartcard y FAS actualizadas

Se han actualizado las funcionalidades de implementación de Smartcard y FAS, con notas adicionales específicas para las plataformas Linux Rocky8/9, Ubuntu 24.04, Debian 12/11 y SLES 15.6. Para obtener más información, consulte Distribuciones compatibles con Smartcard y Distribución compatible con FAS.

Actualizar las funcionalidades de implementación de SSSD + FAS + MCS

Se han actualizado las funcionalidades de implementación de SSSD + FAS + MCS, con notas adicionales específicas para las plataformas RHEL y Rocky Linux. Para obtener más información, consulte Crear VDA de Linux con FAS habilitado mediante MCS.

Permitir diferentes tipos de inicio de sesión durante la reconexión de la sesión

Anteriormente, la reconexión de la sesión requería el mismo tipo de inicio de sesión que la sesión original. Con esta mejora, los usuarios pueden reconectarse utilizando un tipo de inicio de sesión diferente. Esta funcionalidad solo se aplica a los métodos de autenticación de nombre de usuario/contraseña y FAS. Establezca la clave del registro local para habilitar esta función:

```
HKLM\System\CurrentControlSet\Control\Citrix\AccessControl\Login -t
REG_DWORD -v allowReconnectCredChange -d 0x00000001
```

Tiempo de espera de visualización del banner de inicio de sesión configurable

El período de tiempo de espera de visualización del banner de inicio de sesión ahora es configurable. Anteriormente, el banner de inicio de sesión avanzaba automáticamente después de 60 segundos de inactividad. Con esta función, ahora puede personalizar el período de tiempo de espera del banner de inicio de sesión. Consulte Fondos personalizados y mensajes de banner en las pantallas de inicio de sesión de la sesión.

Soporte para seleccionar la distribución del teclado en la interfaz de usuario de inicio de sesión

Agregue un selector de distribución del teclado a la interfaz de inicio de sesión, lo que le permite cambiar entre diferentes idiomas de entrada. Esta función garantiza que pueda introducir su

nombre de usuario y contraseña correctamente, configurando una distribución de teclado adecuada.

Asignación de unidades de cliente optimizada

Se optimizan las siguientes capacidades de CDM:

- Eficiencia mejorada de la transferencia de archivos y compatibilidad con la carga de archivos grandes (>4 GB).
- Impacto minimizado del progreso de `ctxcdm` bloqueado. La carpeta vinculada de CDM se cambia a `$Home/ctxmnt/drives`. Consulte Asignación de unidades de cliente.

Compatibilidad con el registro CNAME en la consulta LDAPS

Anteriormente, Linux VDA no admitía el registro CNAME en el flujo de trabajo de consulta LDAPS. A partir de la versión 2507, el registro CNAME en la consulta LDAPS es compatible de forma predeterminada.

Compatibilidad con la configuración de varios dominios

Una nueva variable de entorno, `CTX_EASYINSTALL_TRUSTED_DOMAINS`, ya está disponible para Easyinstall, y `TRUSTED_DOMAINS` para MCS. Puede especificar una lista de dominios de confianza. Los scripts actualizarán automáticamente `krb5.conf` y detectarán automáticamente los servidores LDAP en esos dominios de confianza si no se especifica la lista de servidores LDAP.

Mejoras en la GUI de Easy Install

La GUI de Easy Install ahora presenta un diseño de componentes reestructurado, que incluye un nuevo botón de selección de tipo de instalación que le permite elegir entre varias opciones. Puede configurar fácilmente los ajustes de la base de datos con una página dedicada a la configuración de la base de datos. El nuevo tipo de instalación “no unido a un dominio” y el tipo de instalación rápida de prueba de concepto (POC) ofrecen más flexibilidad para varios entornos. Puede guardar y cargar configuraciones, personalizar ajustes opcionales y agilizar el proceso de configuración de instalaciones completas y POC con una configuración mínima. Para obtener más información, consulte Crear VDA unidos a un dominio mediante Easy Install.

Compatibilidad con la visualización de más métricas de sesión en Director

Compatibilidad con la visualización de más métricas de sesión en Director para Diagnosticar problemas de rendimiento de la sesión.

Herramienta de línea de comandos de diagnóstico de audio

La herramienta de línea de comandos de diagnóstico de audio se ha mejorado en la versión 2507 para proporcionar información de diagnóstico adicional. Para obtener más información, consulte Herramienta de línea de comandos de diagnóstico de audio.

Mejorador de calidad de audio para el modo tolerante a pérdidas de EDT

A partir de la versión 2507, el mejorador de calidad de audio está habilitado de forma predeterminada para el audio adaptable a través del modo tolerante a pérdidas de EDT para audio.

Novedades en versiones anteriores

Para conocer las nuevas funciones incluidas en las versiones que se lanzaron después de la **LTSR** 1912 hasta la **CR** 2411, consulte Historial de novedades.

Problemas resueltos

- Es posible que el VDA de Linux de MCS deje de estar registrado después de un cierto período de tiempo si no puede actualizar la contraseña de la máquina.
- Podría experimentar corrupción de archivos al transferir archivos grandes (4 GB o más) a un VDA de Linux.
- Es posible que las sesiones de usuario aparezcan como "desconocidas" y no se puedan volver a conectar después de actualizar a LVDA 2402CU1.

Historial de novedades

Este artículo proporciona información sobre las nuevas funciones incluidas en las versiones que se publicaron después de la 1912 LTSR hasta la 2503 CR.

Novedades de la versión 2503

Compatibilidad con RHEL 9.5, Rocky Linux 9.5 y Debian 12.9

El VDA de Linux ahora es compatible con las siguientes distribuciones de Linux:

- RHEL 9.5
- Rocky Linux 9.5
- Debian 12.9

Para obtener más información sobre las distribuciones de Linux compatibles, consulte Requisitos del sistema.

El VDA de Linux no unido a un dominio se extiende a la implementación de CVAD local mediante el aprovisionamiento de MCS

Anteriormente, los VDA de Linux no unidos a un dominio solo estaban disponibles para implementaciones de Citrix DaaS. Ahora, con la tecnología de aprovisionamiento de MCS, se pueden extender a implementaciones de CVAD locales. Esta función es efectiva a partir de CVAD 2411 y Linux VDA 2411. Para obtener más detalles, consulte Crear VDA de Linux no unidos a un dominio mediante MCS.

Compatibilidad ampliada con el escritorio MATE

El VDA de Linux ahora es compatible con el entorno de escritorio MATE en todas las distribuciones compatibles de Red Hat Enterprise Linux (RHEL) 9.x y Rocky Linux 9.x. Para obtener más información, consulte Requisitos del sistema.

Xorg sin raíz ahora está deshabilitado de forma predeterminada

Red Hat ha abordado la vulnerabilidad de seguridad CVE-2024-31083 que afecta a los servidores Xorg. Para obtener más información, consulte Xorg sin raíz.

Secure HDX™ ya está disponible de forma general

Puede cifrar sesiones ICA® de extremo a extremo entre la aplicación Citrix Workspace™ (cliente) y el VDA (host de sesión).

La función de cifrado de extremo a extremo (E2EE) no permite que ningún elemento de red intermedio, incluido Citrix Gateway, descifre el tráfico ICA. Mejora la postura de seguridad de su entorno y es fácil de configurar y administrar. Para obtener más información, consulte HDX seguro.

HDX Direct

Al acceder a los recursos entregados por Citrix, HDX Direct permite que los dispositivos cliente internos y externos establezcan una conexión directa segura con el host de sesión si la comunicación directa es posible. Para obtener más información, consulte HDX Direct para Linux.

Compatibilidad con WebSocket para la comunicación entre VDA unidos a un dominio y Delivery Controllers

Esta función le permite configurar la comunicación WebSocket entre VDA unidos a un dominio y Delivery Controllers, lo que ofrece una alternativa a Windows Communication Foundation (WCF).

Para obtener más información, consulte Comunicación WebSocket entre VDA y Delivery Controllers.

Métodos de inicio de sesión personalizables

El VDA de Linux ahora le permite controlar cómo inician sesión los usuarios cuando no utilizan el inicio de sesión único (SSO). Puede personalizar la experiencia de inicio de sesión eligiendo qué métodos de autenticación se muestran. Anteriormente, la pantalla de inicio de sesión sin SSO siempre mostraba la autenticación con contraseña y con tarjeta inteligente en una lista desplegable. Ahora, puede configurar el VDA de Linux para que ofrezca:

- Solo autenticación con contraseña
- Solo autenticación con tarjeta inteligente
- Combinación de autenticación con contraseña y tarjeta inteligente, con cualquiera de las opciones presentada de forma predeterminada.

Puede personalizar fácilmente el método de inicio de sesión ajustando la siguiente configuración del registro en el VDA:

`System\CurrentControlSet\Control\Citrix\login\NSSOLogonType`

Para obtener más información, consulte Personalizar la pantalla de inicio de sesión.

Inicio de sesión mejorado sin SSO para aplicaciones seamless

La experiencia de inicio de sesión para aplicaciones seamless cuando el SSO está deshabilitado se ha mejorado considerablemente. Anteriormente, los usuarios experimentaban largos tiempos de inicio de sesión al iniciar la aplicación y una ventana de inicio de sesión a pantalla completa mal dimensionada. Ahora, aparece rápidamente un cuadro de inicio de sesión de tamaño proporcional en el centro de la pantalla, ajustándose dinámicamente para adaptarse al espacio de ventana disponible.

Autenticación de usuario mejorada

El VDA de Linux ahora admite usuarios con varios nombres principales de usuario (UPN). Al consultar LDAP con el SID del usuario, el sistema puede identificar y autenticar correctamente a

los usuarios con varios UPN asociados a su cuenta. Esta mejora proporciona una experiencia de inicio de sesión más flexible, fiable y fácil de usar para los usuarios del VDA de Linux.

Autenticación secundaria para fallos de SSO de FAS

El VDA de Linux ahora proporciona una mayor resistencia al inicio de sesión al ofrecer un método de autenticación secundaria específicamente cuando falla el inicio de sesión único (SSO) del Servicio de autenticación federada (FAS). Anteriormente, si el SSO de FAS encontraba problemas, los usuarios no podían autenticarse, lo que provocaba fallos en el inicio de la sesión. Con esta función, si el SSO de FAS encuentra problemas, se pide a los usuarios que introduzcan manualmente sus credenciales para la autenticación por contraseña. Para habilitar la función, ejecute el siguiente comando:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\AccessControl\Login\Global"
-t "REG_DWORD" -v "SecondaryAuthEnabled" -d "0x00000001" --force
```

Para obtener más información, consulte Habilitar la autenticación secundaria para fallos de SSO de FAS.

Bloqueo del escritorio al extraer la tarjeta inteligente

Esta versión introduce una mejora de seguridad que bloquea automáticamente el escritorio cuando un usuario que ha iniciado sesión extrae su tarjeta inteligente del lector durante una sesión activa. Esta mejora se puede lograr mediante la siguiente configuración del registro en el VDA:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LocalPolicies\SecurityOptions`

Para obtener más información, Configuración de extracción de tarjetas inteligentes.

Compatibilidad con JUMBO_ICONS

El VDA de Linux ahora es compatible con JUMBO_ICONS. Esta mejora garantiza que las sesiones de aplicaciones publicadas sin interrupciones se muestren correctamente con los iconos de alta resolución adecuados en la aplicación Citrix Workspace para clientes Mac.

El modo tolerante a pérdidas para audio ahora está habilitado de forma predeterminada

Para obtener más información, consulte Funciones de audio.

Compatibilidad con el modo tolerante a pérdidas para gráficos

El modo tolerante a pérdidas se ha revisado a fondo para garantizar que la sesión siga siendo interactiva cuando se detecta pérdida de paquetes. Para obtener más información, consulte Modo tolerante a pérdidas para gráficos.

Función Intelligent Build to Lossless

Intelligent Build to Lossless es una mejora de nuestra función Build to Lossless existente, diseñada para ofrecer una experiencia más inteligente y eficiente. Con Intelligent Build to Lossless, los administradores ya no necesitan configurar manualmente Build to Lossless, y se aplica automáticamente de forma dinámica en la sesión en los monitores que lo requieren. Cuando la necesidad disminuye, Thinwire lo desactiva sin problemas, volviendo a la codificación regular para un rendimiento óptimo. Esta función solo es aplicable con una GPU (HDX 3D Pro). Para usar esta función, la configuración **Usar códec de vídeo para la compresión** debe ser **Usar cuando se prefiera** (predeterminado), y la **Calidad visual** NO debe ser **Siempre sin pérdidas**.

Mejora de la sincronización del portapapeles

Esta versión introduce una función de almacenamiento en búfer del portapapeles para mejorar la sincronización del portapapeles entre el cliente y la sesión VDA. Anteriormente, seleccionar texto dentro de la sesión VDA podía sobrescribir los datos del portapapeles copiados en el cliente, lo que impedía a los usuarios pegar esos datos en el VDA. Este problema ocurre cuando el modo de actualización de selección PRINCIPAL está configurado como 'Selection changes are updated on both the client and host' o 'Client selection changes are not updated on the host'. Este problema se ha resuelto.

La función de almacenamiento en búfer del portapapeles está deshabilitada de forma predeterminada. Para habilitarla, ejecute el siguiente comando dentro de la sesión VDA:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "BufferData" -d "0x00000001" --force
```

Nota:

Esta función se aplica solo a datos de texto y BMP. La funcionalidad de copia de archivos no se ve afectada.

Compatibilidad mejorada con ratón y trackpad

Hemos mejorado el manejo de los eventos de ratón sin procesar para un desplazamiento más fluido del trackpad y una mejor compatibilidad con los botones laterales del ratón en varios dispositivos cliente.

Actualizaciones de VDA simplificadas (versión preliminar)

Anteriormente, la actualización de los VDA requería una intervención manual completa. La versión 2503 simplifica las actualizaciones de VDA para implementaciones de DaaS mediante la introducción del Agente de actualización de VDA. Las actualizaciones a partir de la versión 2503 se pueden realizar posteriormente directamente desde una ruta de archivo compartida o local. Para obtener más información, consulte Actualizaciones de VDA.

Novedades de la versión 2411

Estabilidad de sesión mejorada

El proceso de sesión de usuario (`ctxgfx`) ahora está desacoplado del servicio `ctxhdx`. Anteriormente, una sesión de usuario activa o desconectada podía finalizar si se reiniciaba el servicio `ctxhdx`. Con esta actualización, la sesión de usuario ahora puede mantener su estado incluso si se reinicia el servicio `ctxhdx`, lo que mejora la estabilidad general de la sesión.

Esta función está habilitada de forma predeterminada. Si se ha deshabilitado, puede volver a habilitarla mediante el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\HDXSessionRecovery" -t "REG_DWORD" -v
"EnableSessionRecovery" -d "0x1" --force
```

Compatibilidad con Ubuntu 24.04, Debian 12.7, Debian 11.11 y SUSE 15.6

El VDA de Linux ahora es compatible con las siguientes distribuciones de Linux:

- Ubuntu 24.04
- Debian 12.7
- Debian 11.11
- SUSE 15.6

Para obtener más información sobre las distribuciones de Linux compatibles, consulte Requisitos del sistema.

Dependencia de OpenJDK actualizada de la versión 11 a la versión 17

En esta versión, la dependencia de OpenJDK se ha actualizado de la versión 11 a la versión 17. OpenJDK 17 se instala automáticamente como dependencia al instalar el VDA de Linux. Para obtener más información, consulte Instalar el VDA de Linux manualmente.

Compatibilidad mejorada con la versión de PostgreSQL

El VDA de Linux ahora admite el uso de una versión personalizada de PostgreSQL, independientemente de la versión proporcionada por su distribución de Linux. Le recomendamos que utilice una versión de PostgreSQL que sea al menos tan reciente como la proporcionada por su distribución de Linux. Para usar eficazmente una versión personalizada de PostgreSQL, asegúrese de que `/etc/xdl/db.conf` esté configurado correctamente para la nueva versión. Para obtener más información, consulte las instrucciones de especificación de la base de datos en los artículos de instalación, por ejemplo, Paso 7: Especificar una base de datos para usar y Paso 1g: Instalar y especificar una base de datos para usar.

Xorg sin privilegios de root

El VDA de Linux ahora admite la ejecución de Xorg con privilegios de usuario que no son de root, también conocido como Xorg "sin privilegios de root". Xorg sin privilegios de root es una mejora de seguridad significativa en comparación con la ejecución como root. Para obtener más información, consulte Xorg sin privilegios de root.

La cuenta de servicio "ctxsrvr" se ha movido a una nueva ubicación

A partir de esta versión, la cuenta de servicio de Citrix "ctxsrvr" se ha movido de **/home/ctxsrvr** a **/var/lib/ctxsrvr**.

Función mejorada de copiar y pegar archivos

Esta versión incluye mejoras en la función de copiar y pegar archivos, destinadas a admitir caracteres especiales en los nombres de archivo. Para obtener más información, consulte Copiar y pegar archivos.

Funcionalidad de teclado multiplataforma mejorada

Esta versión aborda problemas con la funcionalidad del teclado al compartir sesiones entre el VDA de Linux y el VDA de Windows. Para obtener más información, consulte Uso compartido de pantalla HDX.

Capacidad de cámara web mejorada

Esta versión incluye varias mejoras en la funcionalidad de la cámara web:

- Negociación mejorada de la resolución y los FPS de la cámara web durante la creación del dispositivo.
- Proceso optimizado de creación y eliminación de la cámara web.
- Se ha añadido compatibilidad con la autorreparación del servicio de cámara web en la sesión.

Compatibilidad con PipeWire en Ubuntu 24.04

El VDA de Linux ahora extiende la compatibilidad con PipeWire a Ubuntu 24.04, donde es el servicio de audio predeterminado. Para obtener más información, consulte Funciones de audio.

La compatibilidad con varios dispositivos de audio y el modo tolerante a pérdidas para el audio ya están disponibles de forma general

La compatibilidad con varios dispositivos de audio ahora está habilitada de forma predeterminada. El modo tolerante a pérdidas para el audio ahora se puede habilitar mediante una configuración de directiva en lugar del registro. Para obtener más información, consulte Funciones de audio.

Mejorador de la calidad de audio para audio adaptable (versión preliminar)

A partir de la versión 2411, hemos introducido el mejorador de la calidad de audio para audio adaptable como una función de vista previa. Esta mejora gestiona eficazmente los períodos cortos de pérdida de paquetes e interrupciones reconstruyendo inteligentemente el audio a partir de muestras anteriores, evitando así una degradación notable de la calidad. Además, recupera de forma adaptativa los paquetes de audio perdidos solo cuando es necesario. El mejorador de la calidad de audio se habilita y deshabilita automáticamente en función de los cambios sostenidos en la pérdida de paquetes, optimizando la calidad de reproducción y grabación de audio tanto en condiciones de red buenas como malas. Para obtener más información, consulte Funciones de audio.

Compatibilidad con más directivas de reconexión automática de clientes

El VDA de Linux ahora admite las siguientes directivas, además de la directiva de reconexión automática de clientes, para controlar la reconexión automática de sesiones.

- Autenticación de reconexión automática del cliente
- Registro de reconexión automática del cliente
- Tiempo de espera de reconexión automática del cliente

Para obtener descripciones detalladas de las directivas, consulte Configuración de la directiva de reconexión automática de clientes.

> **Nota:**

> Cuando el registro de reconexión automática de clientes está habilitado, el VDA de Linux escribe las reconexiones automáticas de clientes directamente en el registro del sistema. Este comportamiento difiere de Windows, donde los registros se escriben en el registro de eventos.

> Para obtener una lista de las directivas que admite el VDA de Linux, consulte Lista de compatibilidad de directivas.

Novedades en 2407

Soporte para RHEL 9.4 / 8.10, Rocky Linux 9.4 / 8.10 y Debian 12.5 / 11.9

El VDA de Linux ahora es compatible con las siguientes distribuciones de Linux:

- RHEL 9.4
- Rocky Linux 9.4
- RHEL 8.10
- Rocky Linux 8.10
- Debian 12.5
- Debian 11.9

Para obtener más información sobre las distribuciones de Linux compatibles, consulte Requisitos del sistema.

Se requiere un nuevo tiempo de ejecución de .NET

Además del tiempo de ejecución de .NET, debe instalar .ASP.NET Core Runtime en todas las distribuciones de Linux compatibles antes de instalar o actualizar el VDA de Linux. La versión 6 es necesaria para Amazon Linux 2. La versión 8 es necesaria para otras distribuciones.

Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde la fuente integrada. De lo contrario, instale .NET desde la fuente de paquetes de Microsoft. Para obtener más información, consulte `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

Inscripción basada en tokens ampliada a entornos locales (versión preliminar)

Esta versión amplía la función de inscripción basada en tokens a entornos locales. Al crear VDA no unidos a un dominio mediante la instalación sencilla, ahora puede:

- Inscribir VDA no unidos a un dominio con un catálogo de máquinas de controladores de entrega tanto en la nube como locales.
- Utilice Citrix Web Studio™ para crear un catálogo de máquinas vacío y generar un token de inscripción.

Para obtener más información, consulte Crear un VDA de Linux no unido a un dominio mediante la instalación sencilla (vista previa).

SSSD designado como método predeterminado para unir dominios

SSSD es ahora el método predeterminado para unir dominios, reemplazando a Winbind. Este cambio afecta al comportamiento de la configuración cuando se ejecuta ctxsetup.sh o el script de instalación sencilla (ctxinstall.sh) en modo interactivo. Para obtener más información, consulte Crear VDA unidos a un dominio mediante la instalación sencilla.

Delegar a los administradores de paquetes la gestión de los archivos de configuración durante las actualizaciones

Esta versión delega en los administradores de paquetes **rpm** o **dpkg** la gestión de los archivos de configuración durante las actualizaciones. Además, esta versión aborda algunos problemas señalados por RPMlint y reconstruye el paquete RPM para cumplir mejor con los requisitos de RPMlint. Para obtener más información, consulte Paso 13: Actualizar el VDA de Linux (opcional).

Compatibilidad con la configuración de extracción de tarjetas inteligentes

Ahora puede determinar qué sucede cuando se extrae la tarjeta inteligente de un usuario que ha iniciado sesión del lector de tarjetas inteligentes durante una sesión editando el registro en el VDA de Linux. Para obtener más información, consulte Configuración de extracción de tarjetas inteligentes.

Capacidad para evitar que impresoras cliente específicas se redirijan a sesiones HDX™

Ahora puede evitar que impresoras cliente específicas se redirijan a sesiones HDX configurando la directiva de Citrix **Asignación y compatibilidad de controladores de impresora**. Para obtener más información, consulte Asignación y compatibilidad de controladores de impresora.

Modo tolerante a pérdidas para audio (vista previa)

Ahora se admite el audio a través del protocolo tolerante a pérdidas Enlightened Data Transport (EDT). Esta función mejora la experiencia del usuario para la transmisión en tiempo real cuando los usuarios se conectan a través de redes con alta latencia y pérdida de paquetes. Cuando esta función está habilitada, el transporte adaptable en Citrix Virtual Apps and Desktops utiliza el protocolo de transporte tolerante a pérdidas EDT para una mejor experiencia de audio. Esta función está deshabilitada de forma predeterminada. Para obtener más información, consulte Modo tolerante a pérdidas para audio (vista previa) en el artículo Funciones de audio.

Ocultación de pérdida de paquetes implementada para mejorar el rendimiento del audio (vista previa)

A partir de la versión 2407, se mejora el mecanismo de búfer de fluctuación y se añade la ocultación de pérdida de paquetes (PLC) para el códec de audio adaptable. PLC ayuda a reconstruir los paquetes de datos perdidos. Esta mejora ayuda a aumentar la tolerancia a la pérdida de paquetes y la tolerancia a la fluctuación, lo que mejora el rendimiento del audio para el modo tolerante a pérdidas (EDT con pérdidas) para el audio.

Para habilitar esta función, también debe habilitar la función Modo tolerante a pérdidas para audio (vista previa). Para obtener más información, consulte Ocultación de pérdida de paquetes para mejorar el rendimiento del audio (vista previa) en el artículo Funciones de audio.

Compatibilidad con PipeWire en Debian 12.5, RHEL 9.x y Rocky Linux 9.x

El VDA de Linux ahora es compatible con PipeWire en Debian 12.5, RHEL 9.x y Rocky Linux 9.x, donde es el servicio de audio predeterminado. Para obtener más información, consulte Funciones de audio.

Rendimiento gráfico mejorado

Esta versión mejora el rendimiento gráfico al actualizar JPEG Turbo a la versión 3 (V3) en el VDA de Linux.

Detalles del proceso de inicio de sesión mostrados en la interfaz de usuario de inicio de sesión

Los usuarios de la sesión ahora pueden ver los siguientes detalles del proceso de inicio de sesión en la interfaz de usuario de inicio de sesión cuando abren una sesión de VDA de Linux:

- **Evaluando la configuración de la directiva de grupo de Citrix®**
- **Autenticando el acceso del usuario**

- **Iniciando el entorno de escritorio** (en el caso de una sesión de escritorio virtual) o **Iniciando la ventana de la aplicación** (en el caso de una sesión de aplicación virtual)

Compatibilidad con la sincronización del diseño del teclado para los entornos de escritorio KDE y XFCE

Esta versión amplía la función de sincronización dinámica del diseño del teclado a los entornos de escritorio XFCE y KDE Plasma 5. Para obtener más información, consulte Sincronización dinámica del diseño del teclado.

Establecer evdev como la regla predeterminada de la extensión de teclado X (XKB)

Para crear una mejor experiencia de usuario con un comportamiento del teclado más receptivo y predecible, el VDA de Linux ahora especifica evdev como la regla XKB predeterminada para la configuración del teclado.

Para obtener más información, consulte Configuración de la extensión de teclado X (XKB).

Optimización del rendimiento de las consultas LDAP

Con la nueva versión, se elimina la comunicación innecesaria con el servidor LDAP y se utiliza una clave de consulta indexada para lograr un mejor rendimiento de las consultas LDAP y reducir los costes.

Escalabilidad mejorada de VDA para Cloud Connectors

Esta versión implementa mejoras en la escalabilidad de VDA para que cada Citrix Cloud Connector (4 vCPU, 10 GB de memoria) pueda ahora admitir 6000 VDA de Linux. Para obtener más información, consulte Consideraciones de tamaño y escala para Cloud Connectors.

El rendimiento adaptativo de HDX ahora está habilitado de forma predeterminada

Para obtener más información, consulte Rendimiento adaptativo de HDX.

> **Nota:**
>
> Ofrecemos un artículo completo de mejores prácticas para los clientes interesados en usar Ansible para la administración de implementaciones. Para obtener más información, consulte Administrar su implementación con Ansible.

Novedades de 2402 LTSR

Compatibilidad con RHEL 8.9, Rocky Linux 8.9, RHEL 9.3 y Rocky Linux 9.3

El VDA de Linux ahora es compatible con las siguientes distribuciones de Linux:

- RHEL 8.9
- Rocky Linux 8.9
- RHEL 9.3
- Rocky Linux 9.3

Para obtener más información, consulte Requisitos del sistema.

Se requiere una nueva versión de .NET

A partir de esta versión, debe instalar .NET Runtime 8.0 en todas las distribuciones de Linux compatibles, excepto RHEL 7.9 y Amazon Linux 2, antes de instalar el VDA de Linux. Para RHEL 7.9 y Amazon Linux 2, continúe instalando .NET Runtime 6.0.

Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde el feed integrado. De lo contrario, instale .NET desde el feed de paquetes de Microsoft.

Soporte de Xfce para RHEL, Rocky Linux y Ubuntu

Ahora puede usar el entorno de escritorio **Xfce** en las sesiones de VDA alojadas en RHEL 8/9, Rocky Linux 8/9 y Ubuntu 20.04/22.04.

Para obtener más información, consulte Requisitos del sistema.

Soporte de tarjeta inteligente y Servicio de autenticación federada (FAS) extendido a VDA de Linux unidos a Quest

El soporte de tarjeta inteligente y FAS ahora también está disponible para los VDA de Linux que están unidos a un dominio mediante Quest. Esta función se ha probado completamente en las distribuciones RHEL, CentOS y Ubuntu que el VDA de Linux admite para la autenticación con tarjeta inteligente y FAS.

Para obtener más información, consulte Tarjetas inteligentes y Servicio de autenticación federada.

Capacidad para comprobar qué dependencias están instaladas

Hemos ampliado las capacidades de **XDPing** para que ahora pueda usar **XDPing** para comprobar qué dependencias están instaladas en el VDA de Linux. Para ello, ejecute el ejecutable de

XDPing para mostrar las dependencias instaladas o guardarlas en una ruta específica mientras las muestra.

Para obtener más información, consulte Tareas que se pueden realizar con **XDPing**.

Soporte para nuevos dispositivos de destino de streaming de Linux

Hemos ampliado el streaming de Linux a las siguientes distribuciones:

- SUSE 15.5

Para obtener más información, consulte Crear VDA de Linux con Citrix Provisioning y Streaming de dispositivos de destino de Linux en la documentación de Citrix Provisioning.

Desglose de la duración del inicio de sesión

Esta función muestra la duración de cada paso que el proceso de inicio de sesión del usuario tarda en Citrix Director y Monitor. Le ayuda a solucionar problemas de inicio de sesión de forma más eficaz. El proceso de inicio de sesión del usuario se desglosa en fases como **conexión HDX**, **Autenticación** y **GPO**. Para obtener más información, consulte Fases del proceso de inicio de sesión y Métricas de VM Linux y sesiones Linux.

Vista previa dinámica de ventanas para aplicaciones publicadas

Ahora puede previsualizar el contenido en pantalla de las ventanas de las aplicaciones publicadas. Por ejemplo, puede abrir varias ventanas de sesiones de Google Chrome mediante la aplicación Citrix Workspace™ para Windows y, a continuación, pasar el ratón por encima del icono de Chrome en la barra de tareas para previsualizar el contenido.

La función depende de la directiva **Vista previa dinámica de ventanas** que puede configurar en Citrix Studio. Para obtener más información, consulte Vista previa dinámica de ventanas y Lista de compatibilidad de directivas.

Nuevas utilidades optimizadas de consulta de métricas de sesión

Esta versión presenta una nueva utilidad de consulta de métricas de sesión (**ctxsession**) para alinearse con el VDA de Windows y proporcionar una experiencia de usuario de Windows. Con esta utilidad, puede acceder a más métricas de sesión.

Esta versión también optimiza la información de ayuda y añade control de acceso para las utilidades de consulta de métricas de sesión heredadas, incluidas **ctxqsession**, **ctxquser**, **ctxqfull** y **ctxquery**. Anteriormente, cuando no había control de acceso, cualquier usuario del VDA de Linux que hubiera iniciado sesión podía consultar las métricas de todas las sesiones a través

de una de las herramientas. Ahora, con el control de acceso añadido, los usuarios solo pueden consultar las métricas de sus propias sesiones y solo los usuarios root y del grupo **ctxadm** tienen permiso para consultar las métricas de sesión de otros usuarios.

Para obtener más información, consulte Utilidades de consulta de métricas de sesión.

Novedades en 2311

Compatibilidad con SUSE 15.5 y Debian 11.7

El VDA de Linux ahora es compatible con SUSE 15.5 y Debian 11.7. Para obtener más información, consulte Requisitos del sistema.

Rendimiento adaptativo HDX

El VDA de Linux ahora es compatible con el rendimiento adaptativo de HDX. Esta función ajusta de forma inteligente el rendimiento máximo de las sesiones ICA al modificar los búferes de salida, lo que mejora la experiencia del usuario. Para obtener más información, consulte el artículo Rendimiento adaptativo de HDX.

Compatibilidad con AOMedia Video 1 (AV1)

Esta versión presenta un nuevo códec, AV1, que le permite recibir imágenes de mayor calidad con la misma utilización de ancho de banda y más FPS con anchos de banda más bajos. AV1 utiliza un ancho de banda por fotograma inferior en comparación con H.264/H.265. Para obtener más información, consulte Configuración y ajuste de gráficos.

> **Sugerencia:**
>
> Para usar HDX 3D Pro con una GPU NVIDIA, debe instalar una versión del controlador de gráficos NVIDIA que sea compatible con la versión 8 de NVIDIA Capture SDK. Para obtener más información, consulte la documentación de NVIDIA Capture SDK.

Estado de los gráficos disponible en la bandeja del sistema

Los usuarios de la sesión ahora pueden ver el estado de los gráficos haciendo clic en el icono de la bandeja del sistema en sus sesiones.

Para obtener más información, consulte Bandeja del sistema.

Compatibilidad con varios dispositivos de audio (versión preliminar)

Esta versión introduce una función de redirección de audio. La función permite que varios dispositivos de audio de la máquina cliente donde está instalada la aplicación Citrix Workspace se redirijan a la sesión remota de Linux VDA.

Con la función habilitada:

- Todos los dispositivos de audio locales de la máquina cliente se muestran en una sesión. En lugar de CitrixAudioSink (salida de audio) o CitrixAudioSource (entrada de audio), los dispositivos de audio aparecen con sus respectivos nombres de dispositivo. Puede seleccionar un dispositivo de audio en una aplicación en una sesión o usar el dispositivo de audio predeterminado durante una sesión, que también es el dispositivo de audio predeterminado de la máquina cliente. Si es necesario, puede cambiar el dispositivo de audio predeterminado desde la configuración del sistema de la máquina cliente. Una vez actualizado el dispositivo de audio predeterminado de la máquina cliente, el nuevo dispositivo aparece como el dispositivo de audio predeterminado en la sesión.
- Los dispositivos de audio dentro de las sesiones se actualizan dinámicamente cuando se conecta o se quita uno.

Para obtener más información, consulte Compatibilidad con varios dispositivos de audio.

Inscripción basada en tokens (versión preliminar)

Ahora puede inscribir VDA no unidos a un dominio en un catálogo de máquinas y autenticar estos VDA en el plano de control de Citrix Cloud™ mediante un archivo de token.

La inscripción basada en tokens es la más adecuada para los casos de uso en los que prepara máquinas (físicas o virtuales) por su cuenta utilizando tecnología de aprovisionamiento™ que no es de Citrix. Ofrece los siguientes beneficios:

- Elimina la necesidad de instalar y mantener Cloud Connectors.
- Elimina la dependencia de AD para la autenticación de usuarios y máquinas, lo que permite la autenticación para máquinas no unidas a un dominio.

Para obtener más información, consulte Crear un Linux VDA no unido a un dominio mediante la instalación sencilla (versión preliminar).

Mejoras en la instalación sencilla

Hemos refactorizado y simplificado la función de instalación sencilla para mejorar su experiencia. Ahora puede:

- Crear VDA no unidos a un dominio mediante la **instalación sencilla**. Esta función está en versión preliminar. Para obtener más información, consulte Crear un VDA de Linux no unido a un dominio mediante la instalación sencilla (versión preliminar).
- Ejecutar el script de instalación sencilla (ctxinstall.sh) a través de todos o módulos específicos. Para obtener instrucciones sobre la ejecución modular, ejecute **ctxinstall.sh -h** para consultar la información de ayuda donde se proporcionan ejemplos. Para obtener más información sobre ctxinstall.sh, consulte la sección ctxinstall.sh del artículo Crear VDA unidos a un dominio mediante la instalación sencilla.
- Comprender mejor el archivo ctxinstall.conf.tmpl donde las variables se agrupan según los casos de uso.

Programa de recopilación de datos de Linux VDA

Ahora participa automáticamente en el programa de recopilación de datos después de instalar el Linux VDA. El programa de recopilación de datos recopila estadísticas y datos de uso y los envía a Citrix Analytics para ayudar a mejorar la calidad y el rendimiento de los productos de Citrix. Para inhabilitar el programa y ver más detalles, consulte Programa de recopilación de datos de Linux VDA.

Nuevas métricas disponibles para sesiones de Linux

Esta versión añade dos nuevas métricas para las sesiones de Linux en Citrix Director y Monitor:

- **Latencia de ICA®**

  La latencia de ICA es básicamente la latencia de red. Esta métrica indica si la red es lenta.

- **Directivas**

  Todas las directivas que están en vigor para la sesión actual se muestran en la ficha Directivas de la vista **Detalles de la sesión**.

Para obtener más información, consulte Métricas de VM de Linux y sesiones de Linux.

El control de congestión EDT mejorado ya está disponible de forma general

Se introduce un nuevo algoritmo de control de congestión para optimizar el protocolo Enlightened Data Transport (EDT). Esta implementación permite que EDT logre un mayor rendimiento y reduzca la latencia para una experiencia de usuario mejorada. Esta función está habilitada de forma predeterminada. Para obtener más información, consulte Transporte adaptable.

Rendezvous V2 de forma predeterminada

El Protocolo Rendezvous está inhabilitado de forma predeterminada. Cuando el Protocolo Rendezvous está habilitado, Rendezvous V2, en lugar de V1, surte efecto.

La detección de MTU de EDT ahora está habilitada en el VDA de forma predeterminada

La detección de MTU permite a EDT determinar automáticamente la unidad de transmisión máxima (MTU) al establecer una sesión. Esto evita la fragmentación de paquetes EDT que podría provocar una degradación del rendimiento o un error al establecer una sesión. Para obtener más información, consulte (/es-es/linux-virtual-delivery-agent/2311/configure/session/adaptive-transport.html).

HDX seguro (versión preliminar)

Puede cifrar las sesiones ICA de extremo a extremo entre la aplicación Citrix Workspace (cliente) y el VDA (host de sesión).

La función de cifrado de extremo a extremo (E2EE) no permite que ningún elemento de red intermedio, incluido Citrix Gateway, descifre el tráfico ICA. Mejora la postura de seguridad de su entorno y es fácil de configurar y administrar. Para obtener más información, consulte (/es-es/linux-virtual-delivery-agent/2311/configure/session/secure-hdx.html).

Novedades de la versión 2308

La versión 2308 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con RHEL 8.8, Rocky Linux 8.8, RHEL 9.2 y Rocky Linux 9.2

Linux VDA ahora es compatible con las siguientes distribuciones de Linux:

- RHEL 8.8
- Rocky Linux 8.8
- RHEL 9.2
- Rocky Linux 9.2

Para obtener más información, consulte (/es-es/linux-virtual-delivery-agent/2308/system-requirements.html).

Aceleración de GPU compartida en un VDA de Linux multisesión

Ahora puede habilitar la aceleración de GPU compartida en un VDA de Linux multisesión para acelerar las aplicaciones 3D de OpenGL. Para obtener más información, consulte Aceleración de GPU compartida en un VDA de Linux multisesión.

Se pueden copiar y pegar formatos de datos específicos entre la sesión y el cliente

Ahora puede permitir que se copien y peguen formatos de datos específicos entre la sesión de VDA y el dispositivo cliente. Esta función se logra mediante las directivas de Citrix. Para obtener más información, consulte Redirección del portapapeles.

Compatibilidad extendida con Quest

Hemos ampliado la compatibilidad con Quest a RHEL 8.X, Rocky Linux 8.x, RHEL 9.x y Rocky Linux 9.x. Para obtener más información, consulte la sección **Paquetes de integración de Active Directory** en Requisitos del sistema.

Captura del servidor y renderizado del cliente para la redirección de contenido del explorador

Hemos ampliado la redirección de contenido del explorador para admitir el escenario de captura del servidor y renderizado del cliente. En este escenario, la aplicación Citrix Workspace (el cliente) se pone en contacto con el servidor web y obtiene contenido de él a través del VDA mediante un canal virtual (**CTXPFWD**). Esta opción es útil cuando el cliente no tiene acceso al servidor web (por ejemplo, clientes ligeros). Reduce el consumo de CPU y RAM en el VDA, pero se consume ancho de banda en el canal virtual de ICA. Para obtener más información, consulte redirección de contenido del explorador.

Control de congestión EDT mejorado (versión preliminar)

Se introduce un nuevo algoritmo de control de congestión para optimizar el protocolo Enlightened Data Transport (EDT). Esta implementación permite que EDT logre un mayor rendimiento y reduzca la latencia para una experiencia de usuario mejorada. Esta función está deshabilitada de forma predeterminada. Para obtener más información, consulte Transporte adaptable.

Más elementos de menú en la bandeja del sistema

Hemos ampliado la herramienta de la bandeja del sistema de uso compartido de pantalla para incluir más elementos de menú. Actualmente, los usuarios de la sesión pueden hacer clic en el icono de la bandeja del sistema para acceder a todos los siguientes elementos de menú y realizar las acciones correspondientes:

- Uso compartido de pantalla
- Cambio de entorno de escritorio
- Control deslizante de calidad gráfica
- CQI en tiempo real

Para obtener más información, consulte Bandeja del sistema.

Codificación de hardware H.265 mejorada

Hemos ampliado la codificación de hardware H.265 para permitir la compresión sin pérdidas para toda la pantalla y el códec de hardware H.265 con pérdidas para las regiones que cambian activamente. Para obtener más información, consulte Configuración y ajuste de gráficos.

Mejora de XDPing para admitir comprobaciones de problemas de SQLite y RC4

Hemos ampliado el alcance de las pruebas individuales y las comprobaciones del estado de registro de VDA que la herramienta **XDPing** de Linux puede realizar para incluir pruebas de SQLite y comprobaciones de problemas de RC4, respectivamente. Para obtener más información, consulte **XDPing**.

Realm probado exhaustivamente para Amazon Linux 2, RHEL 7.9 y CentOS 7.9

El uso de **realm** para unir una VM de Linux a un dominio de Active Directory ahora se ha probado exhaustivamente para Amazon Linux 2, RHEL 7.9 y CentOS 7.9. Aún puede usar el comando **net ads** para unir las VM de Linux que se ejecutan en Amazon Linux 2, RHEL 7.9 y CentOS 7.9 a un dominio de Active Directory.

Para obtener más información, consulte Instalar el VDA de Linux en Amazon Linux 2, CentOS, RHEL y Rocky Linux manualmente.

Novedades de la versión 2305

La versión 2305 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con SQLite

SQLite ahora es totalmente compatible. Puede especificar SQLite o PostgreSQL para usar editando **/etc/xdl/db.conf** después de instalar el paquete VDA de Linux. Para obtener más información sobre cómo especificar una base de datos para usar, consulte los artículos de instalación sencilla y instalación manual.

> **Nota:**

> La herramienta **XDPing** de Linux no realiza pruebas de SQLite.

Mejoras en el inicio de sesión de la sesión

Esta versión mejora la experiencia de inicio de sesión de la sesión desde los siguientes aspectos:

- Permite a los usuarios alternar la visibilidad de las contraseñas y los códigos PIN, lo que facilita a los usuarios detectar entradas incorrectas.
- Muestra el mensaje del banner de inicio de sesión y el cuadro de diálogo de autenticación en pantallas separadas.
- Muestra el proceso de inicio de sesión y requiere contraseñas o códigos PIN para las reconexiones de sesión en escenarios sin SSO.
- Si los usuarios inician sesión en sesiones VDA con credenciales diferentes de las utilizadas para iniciar sesión en la aplicación Citrix Workspace, los cuadros de diálogo de autenticación se muestran por separado. Los usuarios pueden identificar fácilmente cuándo se introducen credenciales erróneamente.
- Agrega compatibilidad con las siguientes combinaciones de métodos de autenticación de usuario en escenarios sin SSO:

APLICACIÓN CITRIX WORKSPACE	SESIÓN VDA
FAS	nombre de usuario
FAS	tarjeta inteligente

Para obtener más información, consulte Fondos personalizados y mensajes de banner en las pantallas de inicio de sesión y Autenticación sin SSO.

Más claves de registro disponibles para la configuración del directorio principal temporal

Esta versión introduce dos claves de registro más que ayudan con la configuración del directorio principal temporal:

- CheckUserHomeMountPoint
- CheckMountPointRetryTime

Para obtener más información, consulte Inicio de sesión con un directorio principal temporal.

Compatibilidad con la autenticación Fast Identity Online (FIDO2) (versión preliminar)

Ahora puede configurar la autenticación FIDO2 para acceder a sitios web mediante Google Chrome alojado en el VDA de Linux. Para obtener más información, consulte FIDO2 (versión preliminar).

Soporte de compresión sin pérdidas H.264 para HDX 3D PRO

El soporte de compresión sin pérdidas H.264 ya está disponible para la aceleración de hardware HDX 3D PRO mediante GPU NVIDIA. Para obtener más información, consulte Compresión sin pérdidas H.264.

Soporte de comodines extendido para especificar URL a redirigir

Al especificar URL cuyo contenido se puede redirigir al cliente, ahora puede usar el comodín `*` para representar todos los componentes de la URL excepto el protocolo. Para obtener más información, consulte Redirección de contenido del explorador.

Soporte para la copia de seguridad y comparación de datos de VDA mediante XDPing

Para fines de solución de problemas, hemos agregado un módulo de copia de seguridad de VDA a la herramienta **XDPing**. Este módulo le permite hacer una copia de seguridad de los datos clave de un VDA en cualquier momento, como la configuración, la base de datos y los datos de permisos binarios. Puede hacer una copia de seguridad de los datos clave del VDA cuando se esté ejecutando correctamente. En caso de que el VDA falle más tarde, haga una copia de seguridad de otra copia de los datos y compare las dos copias de datos para facilitar la solución de problemas. Para obtener más información, consulte **XDPing**.

Soporte de SSSD para usar MCS para crear VDA de RHEL 8.x/9.x y Rocky Linux 8.x/9.x

Ahora puede usar System Security Services Daemon (SSSD) para unirse a dominios de Active Directory al usar MCS para crear VDA de RHEL 8.x/9.x y Rocky Linux 8.x/9.x.

> **Nota:**

> Para usar un VDA de RHEL 8.x/9.x o Rocky Linux 8.x/9.x que se esté ejecutando actualmente y que esté conectado al dominio mediante SSSD como VM de plantilla para MCS, asegúrese de que:

- El VDA se instala manualmente y no mediante la instalación fácil. La instalación fácil usa **Adcli** para RHEL 8.x/9.x y Rocky Linux 8.x/9.x, y la combinación de SSSD y **Adcli** no es compatible con MCS.
- Un servidor Samba está configurado para usar SSSD para la autenticación de AD. Para obtener más información, consulte el artículo de Red Hat en `<https://access.redhat.com/solutions/3802321>`.

Para obtener más información, consulte Crear VDA de Linux mediante MCS.

Soporte para nuevos dispositivos de destino de streaming de Linux

Hemos extendido el streaming de Linux a las siguientes distribuciones:

- RHEL 8.7
- Rocky Linux 8.7
- SUSE 15.4

Para obtener más información, consulte Crear VDA de Linux con Citrix Provisioning y Dispositivos de destino de Linux de streaming en la documentación de Citrix Provisioning.

Novedades en 2303

La versión 2303 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con RHEL 9.1 y Rocky Linux 9.1

Hemos añadido RHEL 9.1 y Rocky Linux 9.1 como distribuciones compatibles. Para obtener más información, consulte Requisitos del sistema.

Compatibilidad con nuevos dispositivos de destino de streaming de Linux

Hemos ampliado el streaming de Linux a las siguientes distribuciones:

- RHEL 9.1
- RHEL 9.0
- Rocky Linux 9.1
- Rocky Linux 9.0

Para obtener más información, consulte Dispositivos de destino de Linux de streaming en la documentación de Citrix Provisioning.

Mejoras en la instalación sencilla

Hemos mejorado la función de instalación sencilla y la experiencia de usuario para los modos silencioso e interactivo. A continuación, se muestra una lista de las principales mejoras que hemos realizado:

- Se ha añadido **/opt/Citrix/VDA/sbin/ctxinstall.conf** como archivo de configuración para la instalación sencilla, para establecer, guardar y sincronizar los valores de todas las variables de entorno necesarias para la GUI y ctxinstall.sh.
- Se ha añadido la validación de las configuraciones de variables para mejorar la solidez.
- Se han añadido opciones de comando para ejecutar ctxinstall.sh. Para obtener más información, utilice el comando de ayuda **ctxinstall.sh -h**.

Para obtener más información sobre el uso de la instalación sencilla, consulte Crear VDA unidos a un dominio mediante la instalación sencilla.

Mejoras de XDPing

Hemos añadido un módulo de análisis en la herramienta **XDPing** para comprobar y analizar el estado de registro de su VDA. Para comprobar el estado de registro del VDA, ejecute el comando **sudo /opt/Citrix/VDA/bin/xdping -a**.

También hemos ampliado las categorías de prueba de **XDPing** para incluir las comprobaciones de dependencia, Kerberos y PAM. Para realizar las comprobaciones específicas, ejecute los comandos **sudo /opt/Citrix/VDA/bin/xdping -T dependency,kerberos,pam**.

Para obtener más información, consulte **XDPing**, Federated Authentication Service y Tarjetas inteligentes.

Novedades de la versión 2301

La versión 2301 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con RHEL 8.7, Rocky Linux 8.7 y SUSE 15.4

Hemos añadido RHEL 8.7, Rocky Linux 8.7 y SUSE 15.4 como distribuciones compatibles. Para obtener más información, consulte Requisitos del sistema.

> **Nota:**

> SUSE 15.3 está obsoleto a partir de esta versión. Para ejecutar Linux VDA en SUSE 15.4, realice una nueva instalación del VDA.

Compatibilidad con Wayland (versión preliminar)

Linux VDA ahora es compatible con Wayland en GNOME en RHEL 9.0, Rocky Linux 9.0 y Ubuntu 22.04. Para obtener más información, consulte Wayland (versión preliminar).

Todas las impresoras cliente ahora se pueden asignar a una sesión de Linux VDA

Anteriormente, solo la impresora predeterminada de un dispositivo cliente podía asignarse a una sesión de Linux VDA. A partir de esta versión, puede asignar todas las impresoras de un dispositivo cliente a una sesión de Linux VDA. Para obtener más información, consulte Prácticas recomendadas de impresión y Impresión de PDF.

Asignación dinámica de unidades cliente y redirección de carpetas cliente

Anteriormente, las unidades conectadas al cliente después de iniciar una sesión no se asignaban a la sesión. Para que esas unidades fueran accesibles en la sesión, tenía que desconectar y volver a conectar la sesión. A partir de esta versión, las unidades conectadas al cliente en cualquier momento durante una sesión se pueden asignar automáticamente. Además, esta versión introduce la redirección de carpetas cliente que le permite redirigir dinámicamente una parte personalizada de una unidad local en el cliente a la sesión. Para obtener más información, consulte Asignación de unidades cliente.

Novedades en 2212

La versión 2212 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con RHEL 9.0 y Rocky Linux 9.0

Hemos añadido RHEL 9.0 y Rocky Linux 9.0 como distribuciones compatibles. Para obtener más información, consulte Requisitos del sistema.

Mejoras en la redirección de dispositivos USB

Hemos realizado las siguientes mejoras para la redirección de dispositivos USB:

- Ahora usamos USB/IP como el nuevo controlador de host virtual para la redirección de dispositivos USB. Dado que, en la mayoría de los casos, el módulo del kernel USB/IP se lanza con la versión 3.17 del kernel de Linux y posteriores, no es necesario compilar el módulo del kernel de forma predeterminada.

- Hemos añadido compatibilidad con puertos USB 3.0. Ahora puede insertar dispositivos USB 3.0 en puertos USB 3.0 de un dispositivo cliente.
- Hemos optimizado las transferencias masivas y aumentado la velocidad de transferencia. La mejora es más notable en entornos de alta latencia.
- Hemos ampliado la redirección de dispositivos USB a más dispositivos USB, como el **dispositivo USB TD-RDF5A Transcend** y el dispositivo USB compuesto **Yubico YubiKey OTP+FIDO+CCID**.

Para obtener más información, consulte Redirección de dispositivos USB.

Aceleración de hardware para GPU no virtualizadas específicas de NVIDIA

En la documentación de Linux VDA, las GPU no virtualizadas se refieren a:

- GPU utilizadas en escenarios de acceso remoto a PC
- GPU pasadas desde un hipervisor

Para que los gráficos HDX 3D Pro se rendericen con un rendimiento superior, ahora habilitamos la aceleración de hardware para GPU no virtualizadas específicas de NVIDIA. Para las GPU no virtualizadas específicas, consulte la sección de hardware compatible de las notas de la versión de NVIDIA Linux Capture SDK.

Para obtener más información, consulte GPU no virtualizadas.

Sustitución de pam_krb5 por SSSD para la autenticación con tarjeta inteligente y FAS

Anteriormente, para usar la autenticación con tarjeta inteligente o el Servicio de autenticación federada (FAS) en RHEL 8 y Rocky Linux 8, tenía que compilar el módulo pam_krb5 manualmente. A partir de esta versión, ya no es necesario realizar este paso manual para las máquinas RHEL 8 y Rocky Linux 8 entregadas en modo VDI. Para obtener más información, consulte Servicio de autenticación federada y Tarjetas inteligentes.

Ampliación de la GUI de instalación sencilla para incluir la configuración de MCS

Anteriormente, solo podía configurar las variables de MCS editando el archivo `/etc/xdl/mcs/mcs.conf`. Esta versión amplía la GUI de instalación sencilla para incluir la configuración de MCS, de modo que también puede configurar las variables de MCS mediante la GUI. Después de hacer clic en **Implementar** en la GUI, las variables que configure en la GUI anulan las variables que configure en el archivo `/etc/xdl/mcs/mcs.conf`. Para obtener más información, consulte Paso 3: Preparar una imagen maestra.

Compatibilidad con la grabación de sesiones de Linux (versión preliminar)

Ahora puede grabar y reproducir sesiones alojadas en un VDA de Linux. Para obtener más información, consulte Grabación de sesiones (versión preliminar).

Opciones de base de datos ahora disponibles (versión preliminar)

Ahora puede usar SQLite además de PostgreSQL. Puede especificar SQLite o PostgreSQL para usar editando `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para ello, complete los siguientes pasos:

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.
2. Edite `/etc/xdl/db.conf` para especificar una base de datos que usar.
3. Ejecute cualquiera de los siguientes scripts según su método de instalación:

- `/opt/Citrix/VDA/sbin/ctxinstall.sh` o `/opt/Citrix/VDA/bin/easyinstall` si utiliza la instalación fácil
- `/opt/Citrix/VDA/sbin/ctxsetup.sh` si instala el VDA de Linux manualmente
- `/opt/Citrix/VDA/sbin/deploymcs.sh` si utiliza MCS para crear VDA de Linux

> **Nota:**
>
> - Recomendamos usar SQLite solo para el modo VDI.
> - Para instalaciones manuales, debe instalar SQLite y PostgreSQL manualmente antes de poder alternar entre ellos. Para la instalación fácil y MCS, puede alternar entre SQLite y PostgreSQL sin tener que instalarlos manualmente.
> - También puede usar `/etc/xdl/db.conf` para configurar el número de puerto para PostgreSQL.

> Para obtener más información, consulte los artículos de instalación.

Novedades de la versión 2210

La versión 2210 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Aceleración de hardware de GPU mejorada para HDX 3D Pro

Hemos mejorado la eficiencia de la transferencia de datos entre la GPU y la memoria del sistema Linux. También hemos reducido la latencia en la representación de gráficos 3D y la codificación de hardware. Estas mejoras optimizan la utilización de los recursos de hardware y mejoran en gran medida el rendimiento de los fotogramas por segundo (FPS). Para obtener más información, consulte Codificación de hardware H.264.

Compatibilidad con límites de tamaño en las transferencias de datos a través del portapapeles

Puede especificar el tamaño máximo (en KB) de los datos del portapapeles que los usuarios pueden transferir entre un cliente y una sesión virtual de Linux durante una única operación de copiar y pegar. Para ello, utilice las siguientes configuraciones de directiva:

- Limitar el tamaño de transferencia del Portapapeles de cliente a sesión
- Limitar el tamaño de transferencia del portapapeles de sesión a cliente

Para obtener más información sobre la configuración de directivas, consulte la sección Redirección del portapapeles del cliente de Configuración de directivas de ICA.

Para obtener información sobre la configuración de directivas que admite el VDA de Linux, consulte la lista de compatibilidad de directivas.

Compatibilidad con nuevos dispositivos de destino de streaming de Linux

Hemos ampliado el streaming de Linux a las siguientes distribuciones:

- RHEL 8.6
- Rocky Linux 8.6
- Ubuntu 22.04

Para obtener más información, consulte Dispositivos de destino de streaming de Linux en la documentación de Citrix Provisioning.

Mejora de los scripts de shell

Hemos mejorado los scripts de shell para que sean más fáciles de mantener y hemos movido las siguientes plantillas de configuración de `/etc/xdl/mcs/` a `/etc/xdl/ad_join/`:

- winbind_krb5.conf.tmpl
- winbind_smb.conf.tmpl

- sssd.conf.tmpl
- sssd_krb5.conf.tmpl
- sssd_smb.conf.tmpl
- centrify_krb5.conf.tmpl
- centrify_smb.conf.tmpl

La instalación fácil también utiliza las plantillas de configuración relevantes para los métodos específicos de unión a dominios.

Novedades de la versión 2209

La versión 2209 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con RHEL 8.6, Rocky Linux 8.6 y Ubuntu 22.04

Hemos añadido RHEL 8.6, Rocky Linux 8.6 y Ubuntu 22.04 como distribuciones compatibles.

Compatibilidad con la autenticación federada para VDA de Ubuntu y SUSE unidos a SSSD y PBIS

Hemos ampliado la compatibilidad de **Federated Authentication Service (FAS)** a los siguientes tipos de VDA:

- VDA de Ubuntu unidos al dominio mediante SSSD y PBIS
- VDA de SUSE unidos al dominio mediante SSSD.

Ahora puede usar FAS para autenticar a los usuarios que inician sesión en esos VDA. Para obtener más información, consulte Federated Authentication Service.

Entornos de escritorio personalizados por usuarios de sesión

Los usuarios de sesión ahora pueden personalizar sus entornos de escritorio. Para habilitar esta función, debe instalar los entornos de escritorio en el VDA con antelación. Para obtener más información, consulte Custom desktop environments by session users.

Firma GPG

Hemos firmado el paquete de Linux VDA con GPG para que pueda verificar la integridad del paquete de Linux VDA mediante la clave pública.

Para obtener la clave pública:

1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.

2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Haga clic en **Components** para buscar y descargar la clave pública.

Para verificar la integridad del paquete Linux VDA mediante la clave pública:

- Para un paquete RPM, importe la clave pública a la base de datos RPM y ejecute los siguientes comandos:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

- Para un paquete DEB, importe la clave pública a la base de datos DEB y ejecute los siguientes comandos:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Novedades de la versión 2207

La versión 2207 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con más métodos de autenticación de usuario en escenarios sin SSO

Anteriormente, con el inicio de sesión único (SSO) inhabilitado, los usuarios podían iniciar sesión en la aplicación Citrix Workspace y en las sesiones con diferentes nombres de usuario. A partir de esta versión, los usuarios pueden iniciar sesión con nombres de usuario o tarjetas inteligentes. Para obtener más información, consulte Autenticación sin SSO.

Opciones adicionales para configurar la marca de agua de la sesión

Hemos agregado nuevas opciones a la directiva **Texto personalizado de marca de agua**, lo que le permite personalizar aún más las marcas de agua de la sesión. Por ejemplo, puede establecer **Texto personalizado de marca de agua** en **<image=path to a PNG image on the VDA>** para crear una marca de agua PNG. Para obtener más información, consulte Marca de agua de sesión.

Compatibilidad con hipervisor KVM

Kernel-based Virtual Machine (KVM) es la tecnología de virtualización de código abierto líder para Linux. Forma parte de Linux y permite convertir máquinas Linux en hipervisores para que puedan alojar varias máquinas virtuales (VM) aisladas. El Linux VDA funciona correctamente en hipervisores KVM. Sin embargo, los hipervisores KVM no son compatibles para su uso con MCS para crear máquinas virtuales.

Copia y pegado de archivos disponible para todas las distribuciones de Linux compatibles

Anteriormente, la **función de copiar y pegar archivos** solo estaba disponible para Debian 10, RHEL 7.9 y Ubuntu 18.04. A partir de esta versión, la función se extiende a todas las distribuciones de Linux compatibles con Linux VDA. Para obtener más información, consulte Copiar y pegar archivos.

Novedades de la versión 2206

La versión 2206 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con Debian 11.3

Hemos añadido Debian 11.3 como distribución compatible.

Compatibilidad con la autenticación de usuarios con credenciales de Azure AD

Linux VDA ahora puede integrarse con Azure Active Directory (AD) para proporcionar autenticación de usuarios. Con esta función, los usuarios pueden iniciar sesión en escritorios Linux no unidos a un dominio utilizando sus credenciales de Azure AD. Para obtener más información, consulte Autenticación con Azure Active Directory.

Visualización del estado de la batería del cliente

Linux VDA ahora puede redirigir y mostrar el estado de la batería de los dispositivos cliente en escritorios virtuales. Esta función está habilitada de forma predeterminada. Para obtener más información, consulte Visualización del estado de la batería del cliente.

Mejoras de varios monitores para VDA de acceso con PC remoto que utilizan tarjetas gráficas que no son vGPU

Esta versión aborda los siguientes problemas que se producen cuando los usuarios acceden a sesiones de acceso con PC remoto:

- El monitor del PC remoto no se puede apagar. Mostrar el contenido de la sesión puede suponer un riesgo de seguridad.
- Los monitores pueden mostrar artefactos cuando se utilizan varios monitores para acceder a sesiones de acceso con PC remoto.

Para obtener más información, consulte Tarjetas gráficas que no son vGPU.

Fondos personalizados y mensajes de banner en las pantallas de inicio de sesión

Ahora puede personalizar las pantallas de inicio de sesión con fondos personalizados y mensajes de banner. Para obtener más información, consulte Fondos personalizados y mensajes de banner en las pantallas de inicio de sesión.

Escalado automático de DPI

El VDA de Linux ahora admite el escalado automático de DPI. Cuando un usuario abre un escritorio virtual o una sesión de aplicación, el valor de DPI de la sesión cambia automáticamente para coincidir con la configuración de DPI del lado del cliente. Para obtener más información, consulte Escalado automático de DPI.

Consultas LDAP más rápidas

Además de consultar cada servidor LDAP en modo de sondeo, el VDA de Linux ahora puede consultar servidores LDAP en un bosque de varios dominios simultáneamente. Para habilitar las consultas LDAP más rápidas, habilite **Catálogo global** en un controlador de dominio y especifique el número de puerto LDAP relevante como 3268. Para obtener información sobre cómo especificar servidores LDAP y puertos LDAP, consulte la descripción de la variable CTX_XDL_LDAP_LIST en el artículo de instalación del VDA de Linux según su distribución.

Puerto FAS personalizado

Anteriormente, el VDA de Linux estaba codificado para comunicarse con los servidores FAS a través del puerto 80. A partir de esta versión, puede personalizar el puerto FAS en el lado del VDA de Linux a través de CTX_XDL_FAS_LIST en ctxsetup.sh. Para obtener más información, consulte el artículo de instalación del VDA de Linux según su distribución.

Novedades de la versión 2204

La versión 2204 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Codificación de hardware ampliada a códec selectivo

Anteriormente disponible solo para toda la pantalla, la codificación de hardware H.264 ahora admite el uso selectivo para regiones que cambian activamente. Esta función descarga el consumo de compresión de vídeo de la CPU al hardware y mejora la calidad de imagen y el número de fotogramas por segundo (FPS). Para obtener información sobre cómo habilitar esta función, consulte Configuración y ajuste de gráficos.

Compatibilidad con el inicio de sesión con un directorio de inicio temporal

A partir de esta versión, puede especificar un directorio de inicio temporal para los casos en que el punto de montaje en el VDA de Linux falle. Con un directorio de inicio temporal especificado, aparece un mensaje durante el inicio de sesión de una sesión cuando el punto de montaje falla. Los datos del usuario se almacenan entonces en el directorio de inicio temporal. Para obtener más información, consulte Inicio de sesión con un directorio de inicio temporal.

Compatibilidad con proxy SOCKS5 para el tráfico HDX de Rendezvous

El VDA de Linux ahora amplía la compatibilidad con proxy SOCKS5 para establecer conexiones Rendezvous. Para obtener más información, consulte Rendezvous V1 y Rendezvous V2.

Compatibilidad con proxy transparente para Rendezvous

El proxy HTTP transparente ahora es compatible con Rendezvous. Si utiliza un proxy transparente en su red, no se requiere ninguna configuración adicional en el VDA.

Compatibilidad con el escritorio GNOME Classic

Esta versión añade GNOME Classic como una opción de escritorio que puede especificar a través de `CTX_XDL_DESKTOP _ENVIRONMENT` en ctxsetup.sh. Para obtener más información, consulte el artículo de instalación de VDA de Linux GNOME Classic según su distribución.

Agrupación de botones de la barra de tareas de aplicaciones

Anteriormente, todos los botones de la barra de tareas de las aplicaciones publicadas que se ejecutaban en la misma sesión se combinaban en un único grupo. A partir de esta versión, cada aplicación aparece como un único botón en la barra de tareas, incluso cuando hay varias ventanas abiertas para una aplicación.

Novedades de la versión 2203

La versión 2203 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Compatibilidad total con Rendezvous V2

Al utilizar el servicio Citrix Gateway, el protocolo Rendezvous permite que el tráfico omita los Citrix Cloud Connectors y se conecte directa y de forma segura con el plano de control de Citrix Cloud.

Hay dos tipos de tráfico a considerar: 1) tráfico de control para el registro de VDA y la intermediación de sesiones; 2) tráfico HDX.

Rendezvous V1 permite que el tráfico HDX omita los Cloud Connectors, pero aún requiere que los Cloud Connectors actúen como proxy para todo el tráfico de control para el registro de VDA y la intermediación de sesiones.

Las máquinas unidas a un dominio AD estándar y las máquinas no unidas a un dominio son compatibles con el uso de Rendezvous V2 con VDA de Linux de sesión única y de varias sesiones. Con las máquinas no unidas a un dominio, Rendezvous V2 permite que tanto el tráfico HDX como el tráfico de control omitan los Cloud Connectors.

Para obtener más información, consulte Rendezvous V2.

La GUI de instalación sencilla ya está disponible

Anteriormente, solo podía operar una interfaz de línea de comandos para usar la instalación sencilla. Esta versión ofrece una GUI de instalación sencilla que le guía a través de las siguientes operaciones:

- Comprobar el entorno del sistema
- Instalar dependencias
- Unir el VDA a un dominio especificado
- Configurar el entorno de tiempo de ejecución

Para usar la GUI de instalación sencilla, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su VDA. Para obtener más información, consulte la sección **Modo interactivo** del artículo Instalación rápida mediante la instalación sencilla (recomendado).

Mejora de gráficos HDX

Thinwire ahora puede mejorar el número de fotogramas por segundo (FPS) al paralelizar ciertas tareas, con el inconveniente de un consumo general de CPU ligeramente superior. Esta función está inhabilitada de forma predeterminada. Para obtener más información, consulte la sección Procesamiento paralelo del artículo Configurar gráficos.

Novedades de la versión 2201

La versión 2201 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con el escritorio MATE en SUSE 15.3 y SUSE 15.2

Ahora puede especificar MATE como escritorio predeterminado para las sesiones de SUSE 15.3 y SUSE 15.2. Para obtener más información sobre los entornos de escritorio, consulte los artículos de instalación.

Función de duplicación de sesiones ampliada a todas las distribuciones admitidas

La función de duplicación de sesiones permite a los administradores de dominio ver las sesiones ICA de los usuarios en una intranet. Anteriormente disponible solo para RHEL 7.x y Ubuntu 16.04, la función ahora se extiende a todas las distribuciones compatibles con Linux VDA. Para obtener más información, consulte Duplicar sesiones.

Creación de usuarios locales con atributos especificados en VDA no unidos a un dominio

Cuando abre una sesión alojada en un VDA no unido a un dominio, el VDA crea automáticamente un usuario local con atributos predeterminados. El VDA crea el usuario local basándose en el nombre de usuario que utilizó para iniciar sesión en la aplicación Citrix Workspace. Ahora puede especificar atributos de usuario, incluidos el identificador de usuario (UID), el identificador de grupo (GID), el directorio principal y el shell de inicio de sesión del usuario. Para obtener más información, consulte VDA no unidos a un dominio.

Compatibilidad con Transport Layer Security (TLS) 1.3

El VDA de Linux ahora es compatible con TLS 1.3. El script `enable_vdassl.sh` en el directorio /opt/Citrix/VDA/sbin le permite habilitar TLS y establecer la versión mínima de TLS. Para obtener más información, consulte Proteger sesiones de usuario con TLS.

> **Nota:**
>
> A partir de esta versión, debe instalar .NET Runtime 6.0 antes de instalar el VDA de Linux.

Novedades de la versión 2112

La versión 2112 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con Amazon Linux 2 (versión preliminar)

Hemos añadido Amazon Linux 2 como distribución compatible. Para obtener más información, consulte Requisitos del sistema.

Compatibilidad total con el uso compartido de pantalla de HDX

El uso compartido de pantalla de HDX ahora es totalmente compatible. Puede compartir la pantalla de su escritorio virtual con los usuarios de la sesión en otros escritorios virtuales. La función de uso compartido de pantalla está inhabilitada de forma predeterminada. Para obtener más información, consulte Uso compartido de pantalla de HDX.

Conexión Rendezvous a través de un proxy HTTP

El VDA de Linux ahora admite el establecimiento de conexiones Rendezvous a través de un proxy HTTP que utiliza TCP como protocolo de transporte para ICA. Para obtener más información, consulte Protocolo Rendezvous.

Autenticación de proxy Rendezvous

Un VDA de Linux unido a un dominio ahora puede autenticarse en un servidor proxy para conexiones Rendezvous. Para obtener más información, consulte Protocolo Rendezvous.

Compatibilidad con audio adaptable

El audio adaptable está habilitado de forma predeterminada. Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en el VDA. El audio adaptable ajusta dinámicamente las tasas de bits de muestreo de audio en función de las condiciones de la red para proporcionar una experiencia de audio de primera calidad. Para obtener más información, consulte Audio adaptable.

Compatibilidad con nuevos dispositivos de destino de streaming de Linux

Para el streaming de Linux, ahora se admiten los siguientes sistemas operativos:

- SUSE Linux Enterprise Server 15 SP2 (SUSE 15.2)
- SUSE Linux Enterprise Server 15 SP3 (SUSE 15.3)

Para obtener más información, consulte Streaming Linux target devices en la documentación de Citrix Provisioning.

Mejora de la sincronización de la distribución del teclado

Con **KeyboardLayout** establecido en **Server Default** en el archivo WFCLIENT.ini, la distribución del teclado seleccionada anteriormente se mantiene después de volver a conectarse a una sesión.

Mejora de la entrada de teclado

Hemos resuelto varios problemas y hemos añadido compatibilidad con más caracteres especiales y accesos directos.

Novedades de la versión 2110

La versión 2110 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con SUSE 15.3 y SUSE 15.2

Hemos añadido SUSE Linux Enterprise Server 15 SP3 (SUSE 15.3) y SUSE Linux Enterprise Server 15 SP2 (SUSE 15.2) como distribuciones compatibles. Para obtener más información, consulte Requisitos del sistema.

Compatibilidad con la compresión de vídeo de cámara web HDX para SUSE 15.3, SUSE 15.2 y SUSE 12.5

Los usuarios de aplicaciones de videoconferencia que se ejecutan en sesiones de SUSE 15.3, SUSE 15.2 y SUSE 12.5 ahora pueden usar sus cámaras web con la compresión de vídeo de cámara web HDX. Para obtener más información, consulte Compresión de vídeo de cámara web HDX.

Compatibilidad con FAS para máquinas virtuales creadas con MCS mediante PowerBroker Identity Services (PBIS)

Ahora puede usar FAS para autenticar a los usuarios que inician sesión en un Linux VDA creado con MCS que se unió a un dominio de Windows mediante PBIS. Para obtener más información, consulte Configurar Federated Authentication Service y Habilitar FAS en una máquina virtual creada con MCS.

Se añaden dos variables de entorno a ctxfascfg.sh

Hemos agregado las siguientes variables a ctxfascfg.sh:

- CTX_FAS_KDC_HOSTNAME: Especifica el nombre de host del Centro de distribución de claves (KDC) cuando se selecciona PBIS.
- CTX_FAS_PKINIT_KDC_HOSTNAME: Especifica el nombre de host del KDC de PKINIT, que es igual a CTX_FAS_KDC_HOSTNAME a menos que se especifique lo contrario.

Para obtener más información, consulte Ejecutar ctxfascfg.sh.

Inicio de sesión con credenciales diferentes a las utilizadas para iniciar sesión en la aplicación Citrix Workspace

Después de iniciar sesión en la aplicación Citrix Workspace, puede usar credenciales diferentes para iniciar sesiones de Citrix Virtual Apps™ and Desktops. Para habilitar esta función, ejecute el siguiente comando en su VDA de Linux:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
"REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
```

Con la función habilitada, se le pedirán las credenciales al iniciar las sesiones. La función es compatible con las siguientes distribuciones:

- RHEL 8.4 / CentOS 8 (2105)
- RHEL 7.9 / CentOS 7.9
- Ubuntu 16.04
- Debian 10.9
- SUSE 15.3
- SUSE 15.2

Novedades de la versión 2109

La versión 2109 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con el uso compartido de pantalla HDX (versión preliminar)

Ahora, Linux VDA le permite compartir la pantalla de su escritorio virtual con los usuarios de la sesión en otros escritorios virtuales. La función de uso compartido de pantalla está inhabilitada de forma predeterminada. Para obtener más información, consulte Uso compartido de pantalla HDX.

Kit de desarrollo de software (SDK) de canal virtual de Citrix para Linux VDA (versión preliminar)

Ya está disponible el SDK de canal virtual de Citrix para Linux VDA. Con el SDK de canal virtual, puede escribir aplicaciones del lado del servidor para ejecutarlas en el VDA. Para obtener más información, consulte la documentación del SDK de canal virtual de Citrix para Linux VDA.

El SDK de canal virtual de Citrix para Linux VDA está disponible para su descarga en la página de descarga de Citrix Virtual Apps and Desktops. Expanda la versión adecuada de Citrix Virtual Apps and Desktops y haga clic en **Componentes** para seleccionar la descarga de Linux VDA.

Compatibilidad con FAS para VDA que utilizan PBIS

Ahora puede usar FAS para autenticar a los usuarios que inician sesión en un Linux VDA que se unió a un dominio de Windows mediante PowerBroker Identity Services (PBIS). Cuando seleccione PBIS al ejecutar ctxfascfg.sh, introduzca el nombre de host del Centro de distribución de claves (KDC) cuando el script se lo solicite. Para obtener más información, consulte Configurar el servicio de autenticación federada.

Compatibilidad con la transmisión de Linux para RHEL 8.4, RHEL 7.9 y SUSE 12.5

Con la función de transmisión de Linux con Citrix Provisioning, puede aprovisionar escritorios virtuales Linux directamente en el entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Usar Citrix Provisioning para crear máquinas virtuales Linux.

Compatibilidad con la sincronización del diseño del teclado para el escritorio MATE

Hemos ampliado la compatibilidad con la sincronización del diseño del teclado al escritorio MATE. Cada vez que cambie el diseño del teclado en su dispositivo cliente, el diseño de su VDA donde instaló el entorno de escritorio MATE hará lo mismo. Para obtener más información, consulte Sincronización dinámica del diseño del teclado.

Utilidad de consulta de datos de sesión

Ahora proporcionamos una utilidad (`ctxsdcutil`) que puede usar para consultar datos de sesión en cada Linux VDA. Para consultar los siguientes datos de todas las sesiones o de una sesión específica alojada en un VDA, ejecute el comando `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]`. El argumento `[-c]` significa consultar datos cada segundo.

- **Ancho de banda de la sesión de entrada**
- **Ancho de banda de la sesión de salida**
- **Velocidad de línea de la sesión de salida**
- **Latencia - Última registrada**
- **Tiempo de ida y vuelta**
- **Ancho de banda de ThinWire de salida**
- **Ancho de banda de audio de salida**
- **Ancho de banda de impresora de salida**

- **Ancho de banda de unidad de entrada**
- **Ancho de banda de unidad de salida**

Nuevas métricas de sesión de Linux disponibles

Hemos agregado las siguientes métricas para que pueda rastrear, agregar y visualizar el rendimiento de sus sesiones de Linux:

- **Duración del inicio de sesión**

  La duración del inicio de sesión es una medida del proceso de inicio de sesión desde el momento en que un usuario se conecta desde la aplicación Citrix Workspace hasta el momento en que una sesión está lista para usarse. Puede ver esta métrica en la ficha Monitor de Citrix DaaS. Monitor está disponible como la consola Director para supervisar y solucionar problemas de implementaciones de Citrix Virtual Apps and Desktops Current Release y LTSR.

- **Recuento de reconexiones automáticas de sesión**

  Ahora puede ver el número de reconexiones automáticas en una sesión de Linux a través de la vista **Tendencias** de Citrix Director y Monitor. La reconexión automática se habilita cuando las directivas de **Fiabilidad de la sesión** o **Reconexión automática de clientes** están en vigor. Para obtener más información sobre las reconexiones de sesión, consulte Sesiones. Para obtener más información sobre las directivas, consulte Configuración de directivas de reconexión automática de clientes y Configuración de directivas de fiabilidad de la sesión.

Para obtener más información, consulte Supervisar máquinas virtuales Linux y sesiones Linux.

Novedades de la versión 2107

La versión 2107 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con Centrify para máquinas RHEL 7/CentOS 7 y RHEL 8/CentOS 8 creadas con MCS

Hemos agregado compatibilidad con Centrify para unir máquinas RHEL 7/CentOS 7 y RHEL 8/CentOS 8 creadas con MCS a dominios de Windows. Para obtener más información, consulte Usar Machine Creation Services (MCS) para crear máquinas virtuales Linux.

Recompilación simplificada del módulo del kernel para la redirección USB

Ahora proporcionamos `ctxusbcfg.sh` en el archivo de código fuente de Linux VDA, citrix-linux-vda-sources.zip. El script ayuda a simplificar la creación de los módulos del kernel VHCI (`usb-vhci-hcd.ko` y `usb-vhci-iocif.ko`) con y sin la opción DKMS (Dynamic Kernel Module

Support). DKMS ayuda a recompilar los módulos del kernel VHCI automáticamente cuando se actualiza un kernel. Para obtener más información, consulte Configurar la redirección USB.

Compatibilidad con RHEL 8.4 y CentOS 8 (2105)

Hemos agregado RHEL 8.4 y CentOS 8 (2105) como distribuciones compatibles. Para obtener más información, consulte Requisitos del sistema.

Compatibilidad con tarjetas inteligentes para Debian

Puede usar una tarjeta inteligente conectada al dispositivo cliente para la autenticación al iniciar sesión en una sesión de escritorio virtual Linux. Esta versión le permite además usar tarjetas inteligentes en sesiones de Debian 10.7. Para obtener más información, consulte Compatibilidad con tarjetas inteligentes.

Novedades de la versión 2106

La versión 2106 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Actualización automática de Linux VDA

Esta función ayuda a actualizar automáticamente el software de Linux VDA, de forma inmediata o a una hora programada. Es beneficiosa porque no tiene privilegios de administrador de las máquinas virtuales en Azure. Para obtener más información, consulte Actualización automática de Linux VDA.

Soporte para Machine Creation Services™ (MCS) en Nutanix AHV

Ahora puede usar MCS para crear máquinas virtuales Linux en Nutanix AHV. Para obtener más información, consulte Usar MCS para crear máquinas virtuales Linux en Nutanix AHV.

Compatibilidad con PBIS para unir máquinas creadas con MCS a dominios de Windows

Hemos agregado compatibilidad con PBIS para unir máquinas creadas con MCS a dominios de Windows. Para obtener más información, consulte Usar Machine Creation Services (MCS) para crear máquinas virtuales Linux.

Compatibilidad con la compresión de vídeo de la cámara web HDX

Los usuarios de aplicaciones de videoconferencia que se ejecutan en sesiones de Linux VDA ahora pueden usar sus cámaras web con la compresión de vídeo de la cámara web HDX. La compresión de vídeo de la cámara web HDX también se denomina modo de cámara web **optimizado**. Este tipo de compresión de vídeo de la cámara web envía el vídeo H.264

directamente a la aplicación de videoconferencia que se ejecuta en la sesión virtual. La compresión de vídeo de la cámara web HDX utiliza la tecnología de marco multimedia que forma parte del sistema operativo cliente para interceptar el vídeo de los dispositivos de captura, transcodificarlo y comprimirlo. Esta función está habilitada de forma predeterminada. Le recomendamos que utilice siempre la compresión de vídeo de la cámara web HDX si es posible. Para obtener más información, consulte Compresión de vídeo de la cámara web HDX.

Control deslizante de calidad gráfica

Hemos incluido un control deslizante de calidad gráfica en la herramienta de indicador de estado gráfico que se ejecuta en sus sesiones virtuales de Linux. El control deslizante ayuda a encontrar el equilibrio adecuado entre la calidad de imagen y la interactividad. Para obtener más información, consulte el Control deslizante de calidad gráfica.

Compatibilidad con la evaluación de directivas para usuarios de Secure Browser que han iniciado sesión durante las reconexiones de sesión de CGP

El VDA de Linux ahora admite la evaluación y aplicación, durante las reconexiones de sesión de CGP, de directivas específicas del usuario que usted configure en el servicio Secure Browser. Se admiten las siguientes directivas:

- Portapapeles
  - Redirección del Portapapeles del cliente
  - Modo de actualización de la selección del portapapeles
  - Modo de actualización de la selección principal
- Impresión
  - Redirección de impresoras de cliente
  - Crear automáticamente impresora universal PDF
- Transferencia de archivos
  - Permitir la transferencia de archivos entre el escritorio y el cliente
  - Descargar archivo del escritorio
  - Cargar archivo al escritorio

Compatibilidad con la transmisión de Linux para RHEL 8.3 y Ubuntu 18.04

La transmisión de Linux para RHEL 8.3 y Ubuntu 18.04 ahora es totalmente compatible. Con la función de transmisión de Linux con Citrix Provisioning, puede aprovisionar escritorios virtuales

Linux directamente en el entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Usar Citrix Provisioning para crear máquinas virtuales Linux.

Novedades de la versión 2104

La versión 2104 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con VDA de Linux no unidos a un dominio en Citrix DaaS™

Ahora puede usar MCS para crear VDA de Linux no unidos a un dominio en Citrix DaaS (anteriormente, servicio Citrix Virtual Apps and Desktops).

OpenJDK 11 es un requisito

Linux VDA ahora requiere la presencia de OpenJDK 11. Entre las distribuciones de Linux que admite Linux VDA, solo Ubuntu 16.04 requiere que instale OpenJDK 11 manualmente. En las demás distribuciones compatibles, OpenJDK 11 se instala automáticamente como una dependencia al instalar Linux VDA.

Cambios en XDPing

La ejecución de `ctxsetup.sh` ya no instala `XDPing`. Puede ejecutar `sudo /opt/Citrix/VDA/bin/xdping` para instalar `XDPing`. Este comando también crea un entorno virtual de **Python3** que es necesario para `XDPing`. Para obtener más información, consulte **XDPing**

Compatibilidad con tarjetas inteligentes para Ubuntu

Los usuarios pueden usar una tarjeta inteligente conectada al dispositivo cliente para la autenticación al iniciar sesión en una sesión de escritorio virtual Linux. Esta versión le permite además usar la autenticación de paso a través de tarjeta inteligente en sesiones de Ubuntu 20.04, Ubuntu 18.04 y Ubuntu 16.04. Para obtener más información, consulte Autenticación de paso a través mediante tarjetas inteligentes.

Compatibilidad con el escritorio MATE

Hemos agregado compatibilidad con el escritorio ligero MATE en CentOS, RHEL, Ubuntu y Debian. Ahora puede especificar el escritorio MATE o GNOME a través de una nueva variable disponible en los scripts ctxinstall.sh, ctxsetup.sh y deploymcs.sh. Si deja la variable sin especificar, se utiliza el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de esta variable en mate. Para obtener más información, consulte Instalación sencilla y los artículos de instalación manual, como Instalar Linux Virtual Delivery Agent para RHEL/CentOS.

Compatibilidad con PBIS para RHEL 8, CentOS 8 y SUSE 12.5

Hemos añadido compatibilidad con PBIS para unir máquinas RHEL 8, CentOS 8 y SUSE 12.5 a dominios de Windows.

Novedades de la versión 2103

La versión 2103 de Linux VDA incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con Debian 10.7 y CentOS 8.3

Hemos añadido Debian 10.7 y CentOS 8.3 como distribuciones compatibles. Para obtener más información, consulte Requisitos del sistema, Instalar Linux Virtual Delivery Agent para Debian e Instalar Linux Virtual Delivery Agent para RHEL/CentOS.

Compatibilidad con SSSD para unir máquinas SUSE a dominios de Windows

Hemos añadido compatibilidad con SSSD para unir máquinas SUSE a dominios de Windows.

Una sola imagen de Linux VDA para casos de uso unidos y no unidos a un dominio

Ahora ofrecemos una sola imagen para crear Linux VDA unidos y no unidos a un dominio en Citrix Virtual Apps and Desktops Standard para Azure. Esta función simplifica la preparación y el mantenimiento de las imágenes. Para obtener más información, consulte Crear Linux VDA en Citrix Virtual Apps and Desktops Standard para Azure.

Mejora de la transferencia de archivos

Hemos mejorado la función de transferencia de archivos rediseñando la barra de progreso, acelerando la velocidad de descarga y resolviendo algunos errores. También hemos aumentado el número de archivos que se pueden transferir a la vez de 10 a 100. Para obtener más información, consulte Transferencia de archivos.

Compatibilidad para configurar temporizadores de conexión de sesión en Citrix Studio

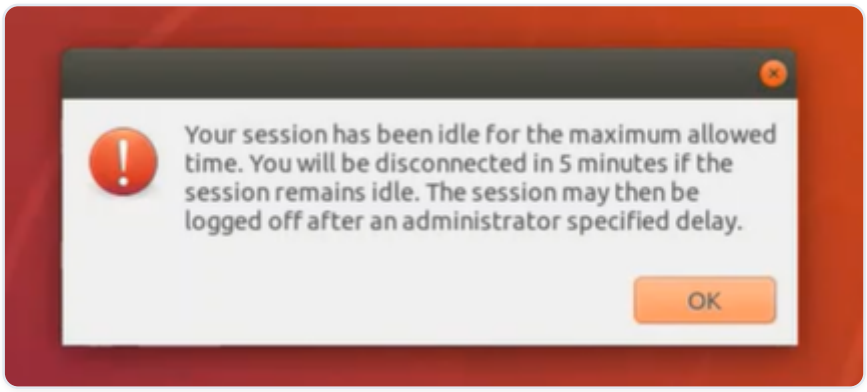
Anteriormente, solo podía configurar límites de tiempo para sesiones inactivas y desconectadas a través de `/opt/Citrix/VDA/bin/ctxcfg` por separado en cada VDA y para cada VDA. Esta versión añade las siguientes directivas para que configure los temporizadores de conexión de sesión en Citrix Studio:

- **Temporizador de inactividad de sesión**: Determina si se debe aplicar un límite de tiempo a las sesiones inactivas.

- **Intervalo del temporizador de inactividad de sesión**: Establece un límite de tiempo para las sesiones inactivas. Si el **Temporizador de inactividad de sesión** está configurado como **Habilitado** y una sesión activa no ha recibido ninguna entrada de usuario durante el tiempo establecido, la sesión se desconecta.
- **Temporizador de sesión desconectada**: Determina si se debe aplicar un límite de tiempo a las sesiones desconectadas.
- **Intervalo del temporizador de sesión desconectada**: Establece un intervalo antes de que se cierre una sesión desconectada.

Cuando actualice cualquiera de las configuraciones de directiva, asegúrese de que sean coherentes en toda la implementación. Para obtener más información sobre las directivas, consulte la Lista de compatibilidad de directivas.

Aparece un mensaje de advertencia cuando expira el límite de tiempo para las sesiones inactivas. Consulte la siguiente captura de pantalla para ver un ejemplo. Al pulsar **Aceptar** se cierra el mensaje de advertencia, pero no se puede mantener la sesión activa. Para mantener la sesión activa, proporcione una entrada de usuario para restablecer el temporizador de inactividad.



Nuevas métricas para máquinas virtuales Linux y sesiones Linux disponibles en Citrix Director

Esta versión añade nuevas métricas para máquinas virtuales Linux y sesiones Linux en Citrix Director.

Nueva métrica para cada máquina virtual Linux:

- El número de núcleos de CPU
- Tamaño de la memoria
- Capacidad del disco duro
- Utilización actual e histórica de CPU y memoria

Nueva métrica para cada sesión Linux:

- Tiempo de inactividad

Para obtener más información, consulte Supervisar máquinas virtuales Linux y sesiones Linux en Citrix Director.

Mejora de FAS para Linux VDA

Ahora proporcionamos salidas de registro más detalladas y le permitimos especificar una ruta que contenga tanto el certificado raíz como todos los certificados intermedios al ejecutar el script ctxfascfg.sh. Para obtener información de configuración, consulte Configurar el servicio de autenticación federada.

Compatibilidad con la transmisión de Linux para RHEL 8.3 y Ubuntu 18.04.5 (versión preliminar)

Con la función de transmisión de Linux de Citrix Provisioning, puede aprovisionar escritorios virtuales Linux directamente en el entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Transmisión de Linux.

Novedades de 2012

La versión 2012 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Detección de MTU de Enlightened Data Transport (EDT)

EDT determina automáticamente la unidad de transmisión máxima (MTU) al establecer una sesión. Esto evita la fragmentación de paquetes EDT que podría provocar una degradación del rendimiento o un fallo al establecer una sesión. Para obtener más información, consulte Detección de MTU de EDT.

Compatibilidad con el enlace de canal LDAP

Anteriormente, el VDA de Linux no podía registrarse con un Delivery Controller™ cuando el enlace de canal estaba habilitado en Active Directory. Esta versión del VDA de Linux admite el enlace de canal para aumentar la seguridad de las comunicaciones con los controladores de dominio de Active Directory. Asegúrese de crear un entorno virtual de **Python3** antes de habilitar el enlace de canal en el VDA de Linux.

XDPing integrado con el VDA de Linux

La herramienta **XDPing** de Linux es una aplicación basada en línea de comandos que automatiza el proceso de comprobación de problemas de configuración comunes en un entorno VDA de

Linux. Anteriormente, tenía que descargar **XDPing** de la página CTX202015 e instalar la herramienta por separado del VDA de Linux. A partir de esta versión, `XDPing` está integrado con el VDA de Linux y se puede instalar automáticamente al instalar el VDA de Linux.

Compatibilidad con RHEL 7.9, RHEL 8.3

Hemos añadido RHEL 7.9 y RHEL 8.3 como distribuciones compatibles.

Compatibilidad con Ubuntu 20.04

Ubuntu 20.04 es totalmente compatible en esta versión.

Soporte para el protocolo Rendezvous

El VDA de Linux ahora es compatible con el protocolo Rendezvous. En entornos que utilizan el servicio Citrix Gateway, el protocolo Rendezvous permite que las sesiones HDX omitan el Citrix Cloud Connector™ y se conecten directa y de forma segura al servicio Citrix Gateway.

Soporte para Machine Creation Services (MCS) en Google Cloud Platform (GCP)

Puede usar MCS para crear máquinas virtuales Linux en GCP.

Wake on LAN disponible para máquinas Linux

La funcionalidad integrada de Wake on LAN ya está disponible para máquinas Linux.

> **Nota:**
>
> A partir de esta versión, debe instalar .NET Core Runtime 3.1 antes de instalar el VDA de Linux.

Novedades de 2009

La versión 2009 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Soporte para RHEL 8.2

Citrix añadió RHEL 8.2 como distribución compatible.

Soporte para Ubuntu 20.04 (versión preliminar)

Puede distribuir el VDA de Linux en Ubuntu 20.04.

Soporte para la redirección de contenido del explorador

A partir de esta versión, el VDA de Linux admite la redirección de contenido del explorador en Google Chrome. La redirección de contenido del explorador permite renderizar páginas web de la lista de permitidos en el lado del cliente. Para obtener más información, consulte Redirección de contenido del explorador.

Soporte para marcas de agua de sesión

El VDA de Linux ahora admite marcas de agua de sesión. Puede especificar una marca de agua que es una capa de texto para mostrar sobre toda la pantalla de la sesión sin cambiar el contenido del documento original. Las marcas de agua de sesión basadas en texto ayudan a disuadir y permiten rastrear el robo de datos. Esta información rastreable aparece en el escritorio de la sesión como un elemento disuasorio para aquellos que utilizan fotografías y capturas de pantalla para robar datos. Para obtener más información, consulte Marca de agua de sesión.

Soporte para VDA de Linux no unidos a un dominio en Citrix Virtual Apps and Desktops Standard para Azure

Ahora puede crear VDA de Linux no unidos a un dominio en Citrix Virtual Apps and Desktops Standard para Azure para entregar aplicaciones y escritorios virtuales a cualquier dispositivo desde Microsoft Azure. Para obtener más información, consulte Crear VDA de Linux en Citrix DaaS Standard para Azure y Citrix Virtual Apps and Desktops Standard para Azure.

Política disponible para configurar la sincronización dinámica del diseño del teclado y la sincronización de la interfaz de usuario del IME del cliente

Anteriormente, para habilitar o deshabilitar las funciones de sincronización dinámica del diseño del teclado y sincronización de la interfaz de usuario del IME del cliente, tenía que editar el registro en cada VDA de destino. A partir de esta versión, puede usar la directiva **Sincronización del diseño del teclado del cliente y mejora del IME** para configurar las funciones. Esta directiva tiene prioridad sobre la configuración del registro y se puede aplicar a los objetos de usuario y máquina que especifique o a todos los objetos de su sitio. Para obtener más información, consulte Sincronización dinámica del diseño del teclado y Sincronización de la interfaz de usuario del IME del cliente.

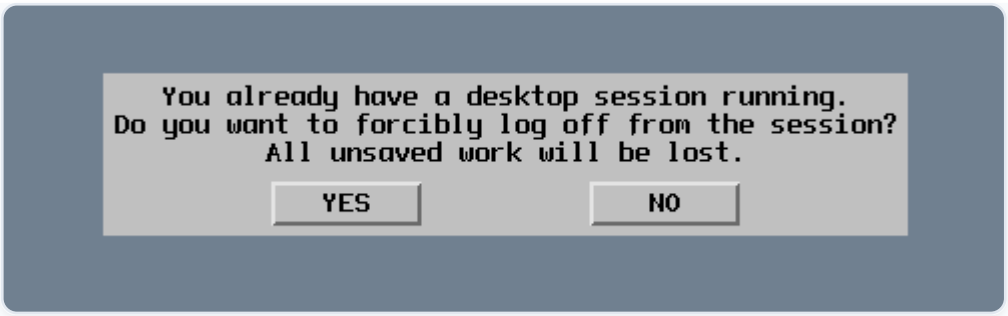
Mensaje proporcionado al abrir una sesión de escritorio adicional desde un VDA

Puede abrir una sesión de escritorio desde un VDA a través de Citrix HDX, RDP y conexiones directas a la consola. Sin embargo, los intentos de abrir una sesión de escritorio HDX adicional desde el mismo VDA de Ubuntu fallaron antes de esta versión. El problema se produjo en los VDA de Ubuntu que tienen instalado el escritorio GNOME. Como mejora, un cierre de sesión forzado

de su sesión de escritorio actual en el siguiente mensaje le permite continuar con la nueva sesión de escritorio. El mensaje aparece cada vez que abre una sesión de escritorio adicional desde un VDA, independientemente de la plataforma Linux en la que esté instalado el VDA.

Nota:

- Si hace clic en **SÍ** en el mensaje cuando inicia sesión en el VDA a través de gdm3, la pantalla de su escritorio de consola aparece en negro y aparentemente no responde. Puede usar Ctrl+Alt+F1 para volver a la ventana de inicio de sesión del VDA.
- El mensaje permanece flotando durante 30 segundos. Después de eso, la respuesta se establece en **NO** automáticamente.



Novedades de 2006

La versión 2006 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con idiomas

El VDA de Linux ahora está disponible en italiano. Para obtener más información, consulte Compatibilidad de idiomas para productos Citrix.

Soporte para SUSE 12 SP5

A partir de esta versión, Citrix añadió SUSE 12 SP5 como distribución compatible.

Mejora de la asignación de unidades de cliente

Esta versión mejora la asignación de unidades de cliente para acelerar las transferencias de archivos entre el VDA de Linux y el dispositivo cliente, especialmente en condiciones de alta latencia de red.

Compatibilidad con copiar y pegar archivos entre sesiones y clientes

Con Citrix Virtual Apps and Desktops 2006 y Citrix Workspace app 1903 o posterior para Windows, los usuarios ahora pueden copiar y pegar archivos entre una sesión y un cliente local. Las funciones de copiar y pegar se realizan mediante el menú contextual o los métodos abreviados de teclado. Para obtener más información, consulte Copia y pegado de archivos.

> **Nota:**
>
> A partir de esta versión, debe instalar .NET Core Runtime 2.1 antes de instalar el VDA de Linux.

Novedades de la versión 2003

La versión 2003 del VDA de Linux incluye las siguientes funciones y mejoras nuevas:

Compatibilidad con RHEL 8

A partir de esta versión, Citrix añadió RHEL 8 como distribución compatible.

Integración con el servicio de telemetría de Citrix

El servicio de telemetría de Citrix (**ctxtelemetry**) está integrado en el software VDA de Linux. Ahora puede ejecutar Citrix Scout desde el Delivery Controller para recopilar registros sobre el VDA de Linux. Para obtener más información, consulte Citrix Scout.

Compatibilidad con el canal virtual NSAP ligero

El VDA de Linux añade compatibilidad con el canal virtual NSAP. Todos los datos de HDX Insight se obtienen exclusivamente del canal virtual NSAP y se envían sin comprimir, lo que mejora la escalabilidad y el rendimiento. Para obtener más información, consulte HDX Insight.

Descarga automática

Citrix añadió la descarga automática como una mejora para las transferencias de archivos. Está disponible para la aplicación Citrix Workspace para HTML5 y para Chrome. Esta mejora proporciona el directorio **Guardar en mi dispositivo** en el VDA. Los archivos que descargue o mueva al directorio **Guardar en mi dispositivo** se transfieren automáticamente al dispositivo cliente. Para obtener más información, consulte Transferencia de archivos.

Compatibilidad con NVIDIA Tesla T4

Se admite NVIDIA Tesla T4.

Problemas conocidos

- BCR no funciona con la última Extensión de redirección del navegador de Citrix.

Debian 12.11 no funciona con el controlador Nvidia 570. Según la documentación oficial de Nvidia, el controlador 570 publicado es compatible con versiones de Debian inferiores o iguales a Debian 12.8. Consulte la documentación del centro de datos

- La sesión de varios monitores podría colgarse si se reproducen varios vídeos en monitores separados con HDX™ 3D pro habilitado.

Avisos de terceros

Linux Virtual Delivery Agent Version 2507 LTSR (Descarga en PDF)

Esta versión del VDA de Linux puede incluir software de terceros con licencia bajo los términos definidos en el documento.

Obsoleto

Los anuncios de este artículo le informan con antelación sobre las plataformas, los productos Citrix® y las funciones que se están eliminando gradualmente para que pueda tomar decisiones comerciales oportunas. Citrix supervisa el uso y los comentarios de los clientes para determinar cuándo se retiran. Los anuncios pueden cambiar en versiones posteriores y es posible que no incluyan todas las funciones o características obsoletas. Para obtener más información sobre el soporte del ciclo de vida del producto, consulte el artículo Política de soporte del ciclo de vida del producto.

Elementos obsoletos y eliminaciones

La siguiente tabla muestra las plataformas, los productos Citrix y las funciones que están obsoletas o eliminadas. Los elementos **obsoletos** no se eliminan de inmediato. Citrix sigue siendo compatible con ellos en esta versión, pero se eliminarán en una futura versión Current Release. Los elementos **eliminados** se quitan o ya no son compatibles en el VDA de Linux.

> **Nota:**
>
> A partir de la versión 2503, el soporte para las versiones secundarias de Debian anteriores a la más reciente queda obsoleto automáticamente sin previo aviso.

ELEMENTO	OBSOLETO ANUNCIADO EN	ELIMINADO EN
Soporte para SUSE 15.6	2507	2511
Debian 11.x	2503	2511
Soporte para RHEL 8.8, 9.2, 9.5	2503	2507

ELEMENTO	OBSOLETO ANUNCIADO EN	ELIMINADO EN
Soporte para Rocky Linux 8.8, 9.2, 9.5	2503	2507
Soporte para Amazon Linux 2	2407	2503
Soporte para RHEL 9.3, RHEL 8.9	2407	2411
Soporte para Rocky Linux 9.3, Rocky Linux 8.9	2407	2411
Soporte para Ubuntu 20.04	2407	2503
Soporte para SUSE 15.5	2407	2411
Soporte para Debian 11.7/11.3	2407	2407
Soporte para RHEL 9.0, RHEL 8.6	2402	2407
Soporte para Rocky Linux 9.0, Rocky Linux 8.6	2402	2407
Soporte para RHEL 7.9, CentOS 7.9	2402	2407
Soporte para SUSE 15.4	2308	2311
Soporte para Rocky Linux 9.1, Rocky Linux 8.7	2305	2308
Soporte para RHEL 9.1, RHEL 8.7	2305	2308
Soporte para RHEL 8.4	2303	2308
Soporte para Ubuntu 18.04	2212	2305

ELEMENTO	OBSOLETO ANUNCIADO EN	ELIMINADO EN
Soporte para SUSE 15.3	2210	2301
Soporte para Debian 10.9	2206	2210
Soporte para SUSE 15.2	2206	2209
Soporte para RHEL 8.2	2206	2209
Soporte para RHEL 8.1, RHEL 8.3	2203	2206
Soporte para RHEL 7.8, CentOS 7.8	2203	2204
Soporte para CentOS 8.x	2110	2201
Soporte para SUSE 12.5	2109	2204
Soporte para Ubuntu 16.04	2109	2203
Soporte para RHEL 7.7, CentOS 7.7	2006	2009
Soporte para SUSE 12.3	2006	2006
Soporte para RHEL 6.10, CentOS 6.10	2003	2003
Soporte para RHEL 6.9, CentOS 6.9	1909	1909
Soporte para RHEL 7.5, CentOS 7.5	1903	1903
Soporte para RHEL 7.4, CentOS 7.4	1811	1811
Soporte para RHEL 6.8, CentOS 6.8	1811	1811

ELEMENTO	OBSOLETO ANUNCIADO EN	ELIMINADO EN
Soporte para RHEL 7.3, CentOS 7.3	7.18	7.18
Soporte para RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

Funciones en Technical Preview

Las funciones en Technical Preview están disponibles para su uso en entornos de no producción o de producción limitada, y para dar a los clientes la oportunidad de compartir sus comentarios. Citrix® no acepta casos de soporte para las funciones en Technical Preview, pero agradece los comentarios para mejorarlas. Citrix podría actuar en función de los comentarios basándose en su gravedad, criticidad e importancia.

Lista de funciones en Technical Preview

La siguiente tabla enumera las funciones en Technical Preview, junto con sus descripciones y las versiones en las que estuvieron disponibles por primera vez.

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
Actualizaciones de VDA simplificadas	Anteriormente, la actualización de los VDA requería una intervención manual completa. La versión 2503 introduce el Agente de actualización de VDA, que permite las actualizaciones a partir de la versión 2503 directamente desde una ruta de archivo compartida o local, eliminando el requisito anterior de una intervención manual compleja. Para obtener más información, consulte	2503	N/D

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	Actualizaciones de VDA.		
Inscripción basada en tokens ampliada a entornos locales	Al crear VDA no unidos a un dominio mediante la instalación sencilla, puede inscribir VDA no unidos a un dominio en un catálogo de máquinas de controladores de entrega tanto en la nube como locales. Puede usar Citrix Web Studio para crear un catálogo de máquinas vacío y generar un token de inscripción. Para obtener más información, consulte Crear un VDA Linux no unido a un dominio mediante la instalación sencilla.	2407	2507
Modo tolerante a pérdidas para audio	El audio es compatible con el protocolo tolerante a pérdidas Enlightened Data Transport (EDT). Esta función mejora la experiencia del usuario para la transmisión en tiempo real cuando	2407	2411

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	los usuarios se conectan a través de redes con alta latencia y pérdida de paquetes. Cuando esta función está habilitada, Adaptive Transport en Citrix Virtual Apps and Desktops utiliza el protocolo de transporte tolerante a pérdidas EDT para una mejor experiencia de audio. Esta función está deshabilitada de forma predeterminada. Para obtener más información, consulte Modo tolerante a pérdidas para audio en el artículo Funciones de audio.		
Mejorador de calidad de audio para audio adaptable	A partir de la versión 2411, hemos introducido el Mejorador de calidad de audio para audio adaptable como función de vista previa. Esta mejora gestiona eficazmente los períodos cortos de pérdida de paquetes e interrupciones	2411	2507

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	reconstruyendo inteligentemente el audio a partir de muestras anteriores, evitando así una degradación notable de la calidad. Además, recupera de forma adaptativa los paquetes de audio perdidos solo cuando es necesario. El Mejorador de calidad de audio se habilita y deshabilita en función de los cambios sostenidos en la pérdida de paquetes, optimizando la reproducción y grabación de audio tanto en condiciones de red buenas como malas. Para obtener más información, consulte Funciones de audio.		
Compatibilidad con varios dispositivos de audio	La función permite redirigir varios dispositivos de audio de la máquina cliente donde está instalada la aplicación Citrix Workspace a la sesión remota de Linux VDA. Con la	2311	2411

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	función habilitada, todos los dispositivos de audio locales de la máquina cliente se muestran en una sesión. En lugar de CitrixAudioSink (salida de audio) o CitrixAudioSource (entrada de audio), los dispositivos de audio aparecen con sus respectivos nombres de dispositivo. Puede seleccionar un dispositivo de audio en una aplicación en una sesión o usar el dispositivo de audio predeterminado durante una sesión, que también es el dispositivo de audio predeterminado de la máquina cliente. Si es necesario, puede cambiar el dispositivo de audio predeterminado desde la configuración del sistema de la máquina cliente. Una vez actualizado el dispositivo de audio predeterminado de la máquina cliente, el nuevo dispositivo		

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	aparece como el dispositivo de audio predeterminado en la sesión. Además, los dispositivos de audio dentro de las sesiones se actualizan dinámicamente cuando conecta o desconecta uno. Para obtener más información, consulte Compatibilidad con varios dispositivos de audio.		
Inscripción basada en tokens	La función le permite inscribir VDA no unidos a un dominio en un catálogo de máquinas y autenticar estos VDA en el plano de control de Citrix Cloud mediante un archivo de token. La inscripción basada en tokens es la más adecuada para los casos de uso en los que prepara máquinas (físicas o virtuales) por su cuenta utilizando tecnología de aprovisionamiento que no es de Citrix. Elimina la necesidad	2311	2507

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	de instalar y mantener Cloud Connectors y elimina la dependencia de AD para la autenticación de usuarios y máquinas, lo que permite la autenticación para máquinas no unidas a un dominio. Para obtener más información, consulte Crear un VDA Linux no unido a un dominio mediante la instalación sencilla.		
Secure HDX	Puede cifrar las sesiones ICA de extremo a extremo entre la aplicación Citrix Workspace (cliente) y el VDA (host de sesión). La función de cifrado de extremo a extremo (E2EE) no permite que ningún elemento de red intermedio, incluido Citrix Gateway, descifre el tráfico ICA. Mejora la postura de seguridad de su entorno y es fácil de configurar y administrar. Para obtener más	2311	2503

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	información, consulte HDX seguro.		
Control de congestión EDT mejorado	Se introduce un nuevo algoritmo de control de congestión para optimizar el protocolo Enlightened Data Transport (EDT). Esta implementación permite que EDT logre un mayor rendimiento y reduzca la latencia para una experiencia de usuario mejorada. Esta función está inhabilitada de forma predeterminada. Para obtener más información, consulte Transporte adaptable.	2308	2311
Compatibilidad con la autenticación Fast Identity Online (FIDO2)	Ahora puede configurar la autenticación FIDO2 para acceder a sitios web mediante Google Chrome alojado en el VDA de Linux. Para obtener más información, consulte FIDO2 (versión preliminar).	2305	N/D

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
Compatibilidad con la grabación de sesiones de Linux en el almacenamiento local	Puede grabar y reproducir sesiones alojadas en un VDA de Linux. Para obtener más información, consulte Grabar sesión en el almacenamiento local.	2212	2507
Opciones de base de datos	Puede usar SQLite además de PostgreSQL. Puede especificar SQLite o PostgreSQL para usar editando `/etc/xdl/db.conf` después de instalar el paquete de VDA de Linux. Para obtener más información, consulte los artículos de instalación.	2212	2305
Compatibilidad con Amazon Linux 2	Amazon Linux 2 se agrega como distribución compatible. Para obtener más información, consulte Requisitos del sistema.	2112	2203
Uso compartido de pantalla HDX	El VDA de Linux le permite compartir la pantalla de su escritorio virtual con los usuarios de la	2109	2112

FUNCIÓN DE TECHNICAL PREVIEW	DESCRIPCIÓN	DISPONIBLE A PARTIR DE LA VERSIÓN	VERSIÓN DE DISPONIBILIDAD GENERAL (GA)
	sesión en otros escritorios virtuales. La función de compartir pantalla está inhabilitada de forma predeterminada. Para obtener más información, consulte Uso compartido de pantalla HDX.		
Compatibilidad con Ubuntu 20.04	Puede instalar el VDA de Linux en Ubuntu 20.04.	2009	2012

Requisitos del sistema

La versión actual del Virtual Delivery Agent (VDA) de Linux está alineada con Citrix Virtual Apps and Desktops. También es compatible con versiones anteriores de Citrix Virtual Apps and Desktops que aún no han llegado al final de su ciclo de vida. Para obtener información sobre el ciclo de vida de los productos de Citrix y para saber cuándo Citrix deja de dar soporte a versiones específicas de productos, consulte la Matriz del ciclo de vida de los productos de Citrix.

El proceso de configuración de los VDA de Linux difiere ligeramente del de los VDA de Windows. Cualquier conjunto de servidores de Delivery Controller™ puede intermediar escritorios Windows y Linux.

Los requisitos del sistema para los componentes no cubiertos aquí (como la aplicación Citrix Workspace™) se describen en sus respectivos conjuntos de documentación.

Para obtener información sobre el uso de una versión actual (CR) en un entorno de servicio a largo plazo (LTSR) y otras preguntas frecuentes, consulte el artículo del Centro de conocimientos.

Distribuciones de Linux compatibles, versiones de Xorg y entornos de escritorio

Para ver una matriz de las distribuciones de Linux, las versiones de Xorg y los entornos de escritorio que admite esta versión del VDA de Linux, consulte la siguiente tabla. Para obtener más información, consulte XorgModuleABIVersions.

DISTRIBUCIÓN DE LINUX	VERSIÓN DE XORG	ESCRITORIO COMPATIBLE
AlmaLinux 9.8/9.6	1.20	GNOME, MATE, Xfce
Debian 12.15	1.20	GNOME, GNOME Classic, KDE, MATE, Xfce
Debian 11.11	1.20	GNOME, GNOME Classic, KDE, MATE
RHEL 9.8/9.6/9.4	1.20	GNOME, MATE, Xfce

DISTRIBUCIÓN DE LINUX	VERSIÓN DE XORG	ESCRITORIO COMPATIBLE
RHEL 8.10	1.20	GNOME, GNOME Classic, MATE, Xfce
Rocky Linux 9.8/9.6/9.4	1.20	GNOME, MATE, Xfce
Rocky Linux 8.10	1.20	GNOME, GNOME Classic, KDE, MATE, Xfce
SUSE 15.6	1.20	GNOME, GNOME Classic, MATE
Ubuntu 22.04	1.21	GNOME, GNOME Classic, KDE, MATE, Xfce
Ubuntu 24.04	1.21	GNOME (se requiere Mutter 46.2-1 o posterior), GNOME Classic (se requiere Mutter 46.2-1 o posterior), KDE, MATE, Xfce

Importante:

La biblioteca de gráficos Mesa (específicamente versiones superiores a la 24.1.0) está causando problemas de visualización con ciertas aplicaciones del sistema (como el Administrador de archivos, la Configuración y la Calculadora) en los escritorios virtuales de Ubuntu 24.04. Hay dos soluciones disponibles, según si ya ha actualizado Mesa. Para obtener más información, consulte Problemas conocidos.

Nota:

- La compatibilidad con AlmaLinux 9.8/9.6 se limita a la instalación manual.
- Cuando caduque el soporte de su proveedor de SO, Citrix podría tener una capacidad limitada para solucionar problemas. Para plataformas obsoletas o eliminadas, consulte Obsoleto.

- Se debe instalar al menos un escritorio. Puede especificar un entorno de escritorio para usar en las sesiones mediante el script ctxinstall.sh o ctxsetup.sh.
- Según la documentación de Red Hat Enterprise Linux, GNOME es el único entorno de escritorio disponible en RHEL 9. Sin embargo, también puede usar el entorno de escritorio Xfce en RHEL 9 y Rocky Linux 9 si tiene instalado el repositorio EPEL.
- No utilice `HWE kernel` ni `HWE Xorg` en Ubuntu.
- A veces, las modificaciones de terceros en el kernel pueden provocar la falta de módulos necesarios para el VDA de Linux. En este caso, debe compilar e instalar el módulo del kernel necesario. Asegúrese de que el arranque seguro esté deshabilitado mientras instala el nuevo módulo del kernel.
- El formato de su nombre de usuario debe cumplir con las reglas de sintaxis `systemd` de su administrador de pantalla actual. Para obtener más información sobre la sintaxis del nombre de usuario `systemd`, consulte Sintaxis del nombre de usuario/grupo.

Requisitos de .Net

A partir de CU2, debe instalar .NET Runtime 10.0 en todas las distribuciones de Linux compatibles, como Alma 9.x, Debian 12.x, RHEL y Rocky Linux 8.x, 9.x, Ubuntu 22.04, 24.04, SUSE 15.6;

Para Debian 11.x, continúe instalando .NET Runtime 8.0;

- Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde el feed integrado. De lo contrario, instale .NET desde el feed de paquetes de Microsoft. Para obtener más información, consulte Instalar .NET en distribuciones de Linux - .NET.
- Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde el feed integrado. De lo contrario, instale .NET desde el feed de paquetes de Microsoft. Para obtener más información, consulte: Instalar .NET en distribuciones de Linux - .NET..

Puertos de red

Para obtener información completa sobre los puertos de red, consulte Puertos de comunicación utilizados por las tecnologías de Citrix.

Plataformas de host y entornos de virtualización compatibles

- Servidores bare metal
- Amazon Web Services (AWS)
- XenServer (anteriormente Citrix Hypervisor™)
- Google Cloud Platform (GCP)
- Máquina virtual basada en kernel (KVM)
- Microsoft Azure
- Microsoft Hyper-V
- Hipervisor VMware vSphere
- Nutanix AHV

> **Nota:**
>
> En todos los casos, la arquitectura de procesador compatible es x86-64.

> A partir de la versión 2203, puede alojar el VDA de Linux en Microsoft Azure, AWS y GCP para Citrix Virtual Apps and Desktops™ así como Citrix DaaS. Para agregar estas conexiones de host de nube pública a su implementación de Citrix Virtual Apps and Desktops, necesita la licencia Citrix Universal Hybrid Multi-Cloud (HMC).

Paquetes de integración de Active Directory

El VDA de Linux admite los siguientes paquetes y productos de integración de Active Directory:

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
AlmaLinux 9.8/9.6	Sí	Sí	No	No	No
Debian 12.15/11.11	Sí	Sí	Sí	Sí	Sí
RHEL 9.8/9.6/9.4, Rocky Linux	Sí	Sí	Sí	No	Sí (Quest v4.1 y posterior)

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
9.8/9.6/9.4/8.10					
RHEL 8.10	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y posterior)
SUSE 15.6	Sí	Sí	Sí	Sí	Sí
Ubuntu 24.04	Sí	Sí	Sí	No	Sí
Ubuntu 22.04	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y posterior)

Consideraciones de tamaño y escala para Cloud Connectors

Cuando conecte los VDA de Linux al plano de control con Citrix Cloud™ Connectors, tenga en cuenta lo siguiente, según las pruebas internas de Citrix:

- Cada Citrix Cloud Connector™ (4 vCPU, 10 GB de memoria) puede admitir 6000 VDA de Linux.
- Implemente dos Cloud Connectors en cada ubicación de recursos para alta disponibilidad y también implemente un máximo de 6000 VDA de Linux en cada ubicación de recursos.

Consideraciones sobre la base de datos

- Recomendamos usar SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una fácil instalación y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el VDA de Linux utiliza PostgreSQL de forma predeterminada.
- Para instalaciones manuales, debe instalar SQLite, PostgreSQL o ambos manualmente. Si instala tanto SQLite como PostgreSQL, puede especificar uno de ellos para usarlo editando **/etc/xdl/db.conf** después de instalar el paquete VDA de Linux.

HDX™ 3D Pro

HDX 3D Pro en Citrix Virtual Apps™ and Desktops permite escritorios y aplicaciones acelerados por GPU. Para garantizar una buena experiencia gráfica en 3D, recomendamos que considere cuidadosamente el ancho de banda de la red, la latencia y otras condiciones de infraestructura relacionadas. Por ejemplo, implemente el VDA y la aplicación Citrix Workspace en la misma región siempre que sea posible.

Hipervisores

Para el VDA de Linux, HDX 3D Pro es compatible con los siguientes hipervisores:

- XenServer® (anteriormente Citrix Hypervisor)
- VMware vSphere Hypervisor
- Nutanix AHV
- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

> **Nota:**
>
> Los hipervisores son compatibles con ciertas distribuciones de Linux.

GPU

Para el VDA de Linux, HDX 3D Pro admite los siguientes tipos de GPU:

vGPU de NVIDIA

Para saber qué tarjetas GPU de NVIDIA admite su distribución de Linux, vaya a la matriz de compatibilidad de productos de NVIDIA y consulte las columnas **Hypervisor or Bare-Metal OS**, **Software Product Deployment**, **Hardware Supported** y **Guest OS Support**.

Asegúrese de instalar el controlador vGPU más reciente para su tarjeta GPU. Actualmente, el VDA de Linux admite hasta vGPU 19. Para obtener más información, consulte NVIDIA Virtual GPU Software Supported GPUs.

GPU no virtualizadas

En la documentación del VDA de Linux, las GPU no virtualizadas se refieren a:

- GPU utilizadas en escenarios de Acceso con PC remoto
- GPU transferidas desde un hipervisor

GPU de NVIDIA que admiten el SDK de captura de NVIDIA para Linux

Para las GPU de NVIDIA que admiten el SDK de captura de NVIDIA para Linux, habilite HDX 3D Pro estableciendo **CTX_XDL_HDX_3D_PRO** en **Y** al instalar el VDA de Linux. No se requiere ninguna configuración adicional. La aceleración de hardware está habilitada de forma predeterminada después de habilitar HDX 3D Pro.

> **Sugerencia:**
>
> Para usar HDX 3D Pro con una GPU de NVIDIA, debe instalar una versión del controlador de gráficos de NVIDIA que admita la versión 8 del SDK de captura de NVIDIA. Para obtener más información, consulte la documentación del SDK de captura de NVIDIA.

Descripción general de la instalación

Esta sección le guía a través de los siguientes procedimientos:

- Preparar la instalación
- Crear VDA unidos a un dominio mediante la instalación sencilla
- Crear VDA de Linux no unidos a un dominio mediante MCS
- Crear un VDA de Linux no unido a un dominio mediante la instalación sencilla (versión preliminar)
- Crear VDA de Linux mediante MCS
- Crear VDA de Linux unidos a un dominio con FAS habilitado mediante MCS
- Crear VDA de Linux mediante Citrix Provisioning
- Crear VDA de Linux en Citrix DaaS Standard para Azure
- Instalar el VDA de Linux manualmente
    - Instalar el VDA de Linux en Amazon Linux 2, CentOS, RHEL y Rocky Linux manualmente
    - Instalar el VDA de Linux en SUSE manualmente
    - Instalar el VDA de Linux en Ubuntu manualmente
    - Instalar el VDA de Linux en Debian manualmente

Preparar la instalación

Este artículo presenta un método para seleccionar un método de instalación adecuado en función de sus circunstancias específicas y le dirige a la guía de instalación pertinente. Para obtener información sobre la planificación de las implementaciones de Citrix Virtual Apps and Desktops y Citrix DaaS, consulte Prepararse para la instalación y Primeros pasos: Planificar y crear una implementación respectivamente.

Antes de empezar a instalar el VDA, tenga en cuenta lo siguiente:

- verificar que la implementación de destino es oficialmente compatible consultando los requisitos del sistema para Linux VDA.
- Decida si quiere conectar sus VDA a un dominio o no.

- Consulte el enlace adecuado de la siguiente tabla, según su método de aprovisionamiento y su decisión de unirse a un dominio:

	SCRIPT DE INSTALACIÓN FÁCIL	MACHINE CREATION SERVICES™ (MCS)	CITRIX PROVISIONING	MANUAL PURO
Unido a un dominio	Crear VDA unidos a un dominio mediante la instalación fácil	Crear VDA de Linux mediante Machine Creation Services (MCS)	Crear VDA de Linux mediante Citrix Provisioning	Instalar el VDA de Linux manualmente
No unido a dominio	Crear un VDA de Linux no unido a un dominio mediante la instalación fácil	Crear VDA de Linux no unidos a un dominio mediante MCS	No compatible	No compatible

Nota:

- MCS NO es compatible con los casos de uso de acceso con PC remoto.
- Para el aprovisionamiento masivo, puede usar MCS, Citrix Provisioning™ o automatización de terceros por su cuenta. Para la automatización de terceros, tiene la opción de incorporar el script de instalación fácil (recomendado) o automatizar los pasos de instalación puramente manuales dentro de su script.
- Para una prueba de concepto (POC) rápida en una sola VM, le recomendamos que use la instalación fácil.
- También puede ejecutar el script de instalación fácil (ctxinstall.sh -s) para actualizar rápidamente sus variables de entorno, como CTX_XDL_DDC_LIST y CTX_XDL_LDAP_LIST.
- Ofrecemos un artículo completo de mejores prácticas para los clientes interesados en usar Ansible para la gestión de la implementación. Para obtener más información, consulte Administrar su implementación con Ansible.

Crear VDA unidos a un dominio mediante la instalación sencilla

Importante:

- Para instalaciones nuevas, le recomendamos que consulte este artículo para una instalación rápida. Este artículo explica cómo instalar y configurar el VDA de Linux mediante la instalación sencilla. La instalación sencilla ahorra tiempo y trabajo, y es menos propensa a errores que la instalación manual. Le ayuda a configurar un entorno de ejecución del VDA de Linux instalando los paquetes necesarios y personalizando los archivos de configuración automáticamente.
- Para crear VDA no unidos a un dominio, puede usar tanto Machine Creation Services (MCS) como la instalación sencilla. Para obtener más información, consulte Crear VDA de Linux no unidos a un dominio mediante MCS y Crear un VDA de Linux no unido a un dominio mediante la instalación sencilla.
- Para obtener información sobre las funciones disponibles para los VDA no unidos a un dominio, vaya a VDA no unidos a un dominio.

Paso 1: Preparar la información de configuración y la máquina Linux

Recopile la siguiente información de configuración necesaria para la instalación sencilla:

- Nombre de host: nombre de host de la máquina en la que se va a instalar el VDA de Linux.
- Dirección IP del servidor de nombres de dominio.
- Dirección IP o nombre de cadena del servidor NTP.
- Nombre de dominio: el nombre NetBIOS del dominio.
- Nombre de ámbito: el nombre de ámbito de Kerberos.
- Nombre de dominio completo (FQDN) del dominio.
- Método de integración de Active Directory (AD): actualmente, la instalación sencilla es compatible con SSSD, Winbind, Centrify, PBIS y Quest. La instalación sencilla solo es compatible con Quest para RHEL y Rocky Linux.
- Nombre de usuario: el nombre del usuario que une la máquina al dominio.
- Contraseña: la contraseña del usuario que une la máquina al dominio.
- OU – La unidad organizativa. Opcional.

Importante:

- Para instalar el VDA de Linux, verificar que los repositorios se hayan agregado correctamente en la máquina Linux.
- Para iniciar una sesión, verificar que el sistema X Window y los entornos de escritorio estén instalados.
- Por motivos de seguridad, la instalación fácil no guarda la contraseña de unión al dominio. Cada vez que ejecute el script de instalación fácil (ctxinstall.sh) en modo interactivo, debe introducir la contraseña de unión al dominio manualmente. En modo silencioso, debe establecer la contraseña de unión al dominio en **/Citrix/VDA/sbin/ctxinstall.conf** o exportar la contraseña. Le recomendamos que no utilice la cuenta de administrador para la unión al dominio. En su lugar, delegue los permisos de unión al dominio a un usuario de Active Directory que no sea la cuenta de administrador. Para ello, delegue el control en el controlador de dominio mediante el **Asistente para la delegación de control**.

Paso 2: Preparar el hipervisor

Se requieren algunos cambios al ejecutar el VDA de Linux como máquina virtual en un hipervisor compatible. Realice los siguientes cambios según la plataforma de hipervisor en uso. No se requieren cambios si ejecuta la máquina Linux en hardware físico.

Corregir la sincronización de la hora en XenServer (anteriormente Citrix Hypervisor™)

Cuando la función de sincronización de hora de XenServer® está habilitada, dentro de cada máquina virtual Linux paravirtualizada, experimenta problemas con NTP y XenServer. Ambos intentan administrar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con NTP. Este caso requiere deshabilitar la sincronización de hora del host. No se requieren cambios en el modo HVM.

Si está ejecutando un kernel de Linux paravirtualizado con las herramientas de XenServer VM instaladas, puede comprobar si la función de sincronización de hora de XenServer está presente y habilitada desde la máquina virtual Linux:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve 0 o 1:

- 0 - La función de sincronización de hora está habilitada y debe deshabilitarse.
- 1 - La función de sincronización de hora está deshabilitada y no se requiere ninguna otra acción.

Si el archivo /proc/sys/xen/independent_wallclock no está presente, los siguientes pasos no son necesarios.

Si está habilitada, deshabilite la función de sincronización de hora escribiendo 1 en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Para que este cambio sea permanente y persistente después de reiniciar, edite el archivo **/etc/sysctl.conf** y agregue la línea:

`xen.independent_wallclock = 1`

Para verificar estos cambios, reinicie el sistema:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux con los Servicios de integración de Linux de Hyper-V instalados pueden aplicar la función de sincronización horaria de Hyper-V para usar la hora del sistema operativo host. Para asegurarse de que el reloj del sistema permanezca preciso, debe habilitar esta función junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para la configuración de una máquina virtual Linux, seleccione **Servicios de integración**.
3. Asegúrese de que **Sincronización de hora** esté seleccionada.

> **Nota:**
>
> Este enfoque es diferente de VMware y XenServer (anteriormente Citrix Hypervisor), donde la sincronización horaria del host está deshabilitada para evitar conflictos con NTP. La sincronización horaria de Hyper-V puede coexistir y complementar la sincronización horaria de NTP.

Corregir la sincronización horaria en ESX y ESXi

Cuando la función de sincronización horaria de VMware está habilitada, dentro de cada máquina virtual Linux paravirtualizada experimentará problemas con el NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con el NTP. Este caso requiere deshabilitar la sincronización horaria del host.

Si está ejecutando un kernel de Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Edite la configuración de la máquina virtual Linux.
3. En el cuadro de diálogo **Propiedades de la máquina virtual**, abra la ficha **Opciones**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Avanzado**, desactive **Synchronize guest time with host**.

Paso 3: Instalar .NET

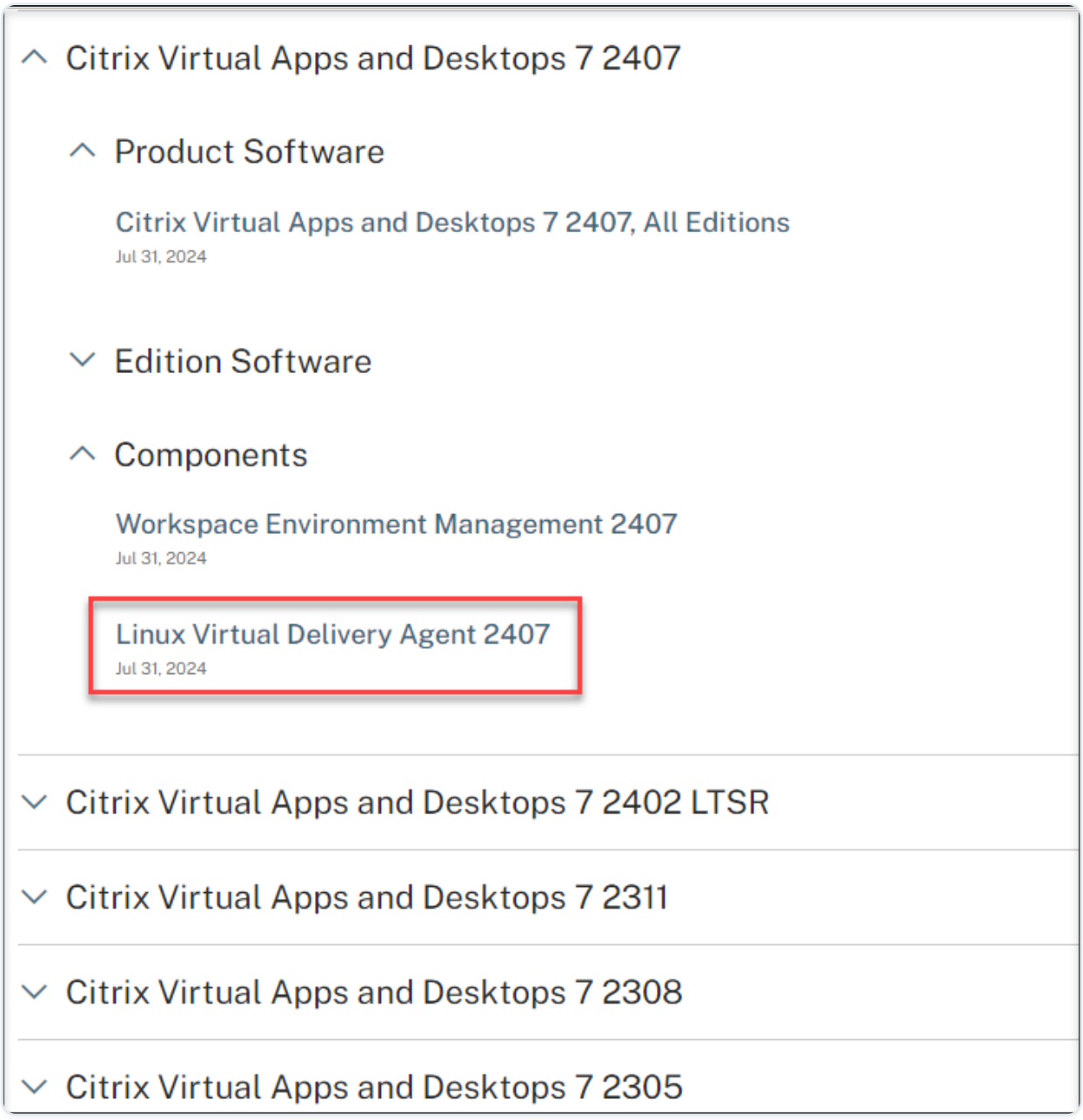
Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Después de instalar .NET, ejecute el comando **which dotnet** para encontrar la ruta de tiempo de ejecución.

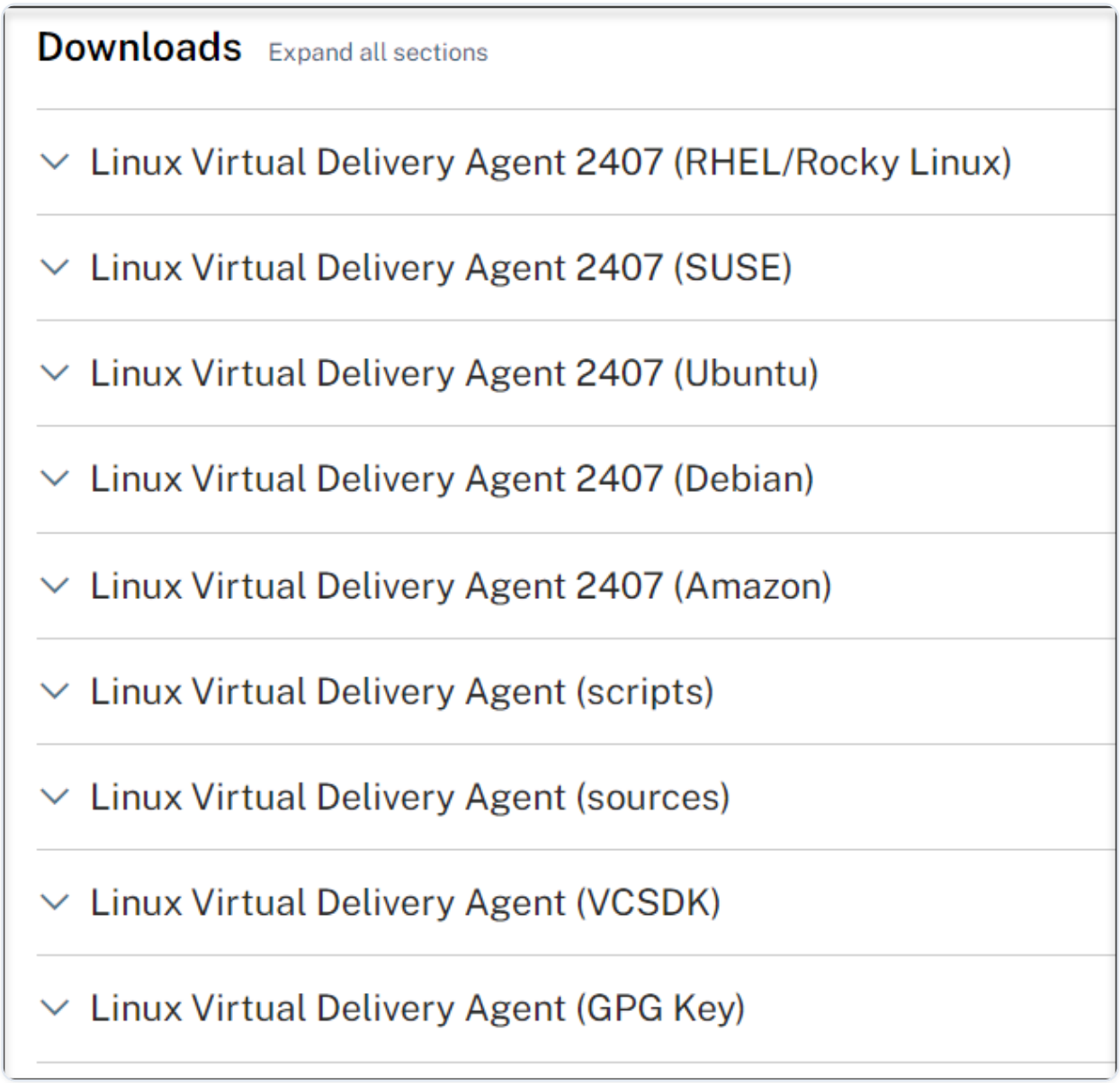
Según la salida del comando, establezca la ruta del binario de tiempo de ejecución de .NET. Por ejemplo, si la salida del comando es /aa/bb/dotnet, utilice /aa/bb como ruta del binario de .NET.

Paso 4: Descargar el paquete VDA de Linux

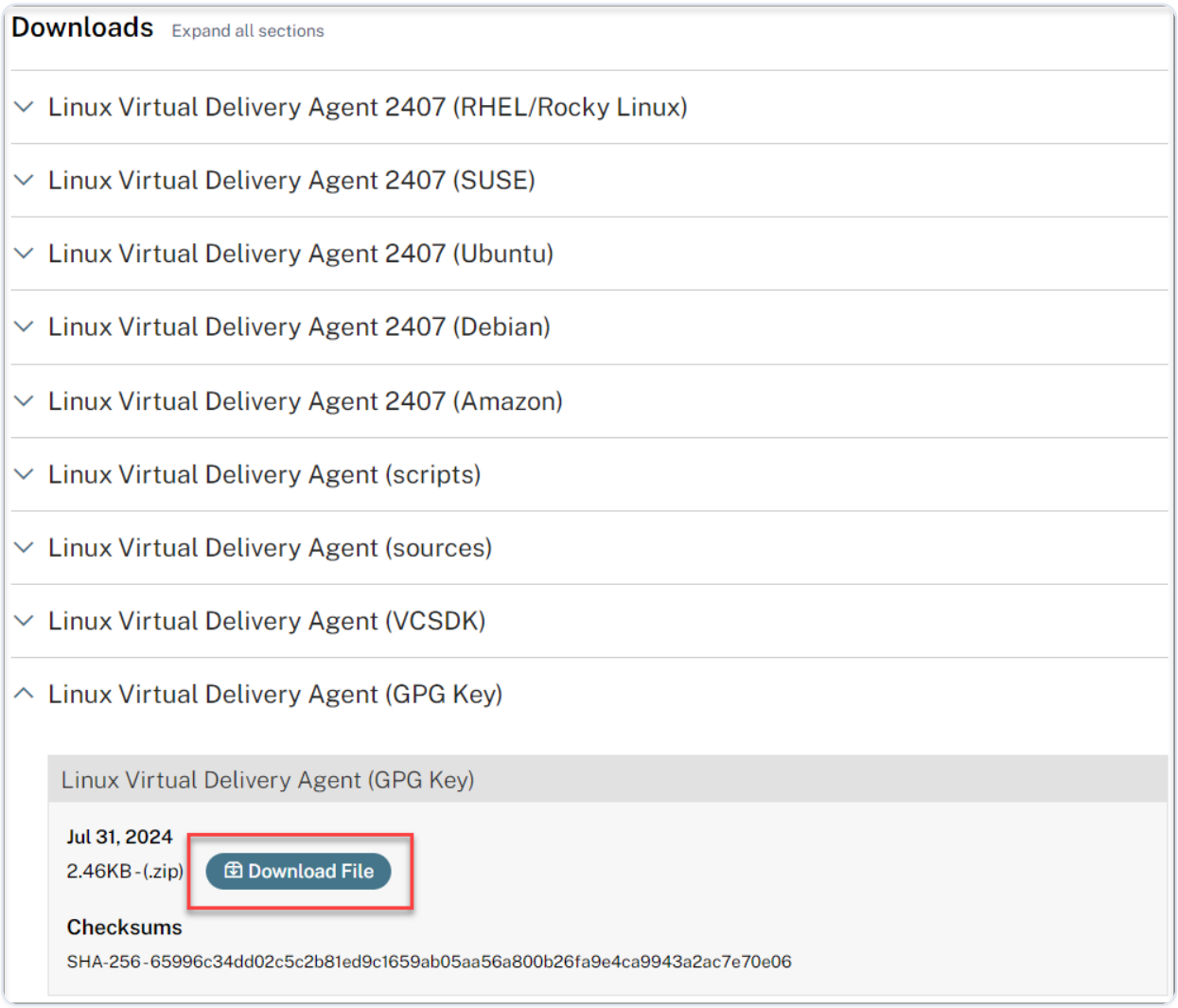
1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Expanda **Components** para encontrar el VDA de Linux. Por ejemplo:



4. Haga clic en el enlace del VDA de Linux para acceder a las descargas del VDA de Linux.



5. Descargue el paquete VDA de Linux que coincida con su distribución de Linux.
6. Descargue la clave pública GPG que puede utilizar para verificar la integridad del paquete VDA de Linux. Por ejemplo:



Para verificar la integridad del paquete de Linux VDA mediante la clave pública:

- Para un paquete RPM, ejecute los siguientes comandos para importar la clave pública en la base de datos RPM y comprobar la integridad del paquete:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

- Para un paquete DEB, ejecute los siguientes comandos para importar la clave pública en la base de datos DEB y comprobar la integridad del paquete:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Paso 5: Instalar el paquete de Linux VDA

Para configurar el entorno para el Linux VDA, ejecute los siguientes comandos.

Para distribuciones RHEL y Rocky Linux:

Nota:

- Para RHEL, instale el repositorio EPEL antes de poder instalar el Linux VDA correctamente. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en `<https://docs.fedoraproject.org/es-es/epel/>`.
- Antes de instalar el Linux VDA en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.

```
sudo yum -y localinstall <PATH>/<Linux VDA RPM>
```

Nota:

Después de instalar el Linux VDA en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojado en GCP, la conexión Ethernet podría perderse y el Linux VDA podría quedar inaccesible después de un reinicio de la VM. Para solucionar el problema, establezca una contraseña de root al iniciar sesión en la VM por primera vez y asegúrese de que puede iniciar sesión en la VM como root. Luego, ejecute los siguientes comandos en la consola después de reiniciar la VM:

```
nmcli dev connect eth0

systemctl restart NetworkManager
```

Para distribuciones Ubuntu/Debian:

```
sudo dpkg -i <PATH>/<Linux VDA deb>

sudo apt-get install -f
```

Nota:

- Para instalar las dependencias necesarias para una distribución Debian 11, añada la línea `deb http://deb.debian.org/debian/ bullseye main` al archivo /etc/apt/sources.list.
- Para Ubuntu 24.04/22.04 en GCP, deshabilite RDNS. Para ello, añada la línea **rdns = false** debajo de en /etc/krb5.conf.

Para distribuciones SUSE:

1. Para SUSE 15.6 en AWS, Azure y GCP, asegúrese de que:
   - Está utilizando **libstdc++6** versión 12 o posterior.
   - El parámetro **Default_WM** en **/etc/sysconfig/windowmanager** está establecido en **"gnome"**.
2. Ejecute el siguiente comando para instalar el VDA de Linux:

   ```
   zypper -i install <PATH>/<Linux VDA RPM>
   ```

Paso 6: Instalar los controladores NVIDIA GRID

Para habilitar HDX™ 3D Pro, debe instalar los controladores NVIDIA GRID en su hipervisor y en las máquinas VDA.

Para instalar y configurar NVIDIA GRID Virtual GPU Manager (el controlador de host) en los hipervisores específicos, consulte las siguientes guías:

- XenServer
- VMware ESX
- Nutanix AHV

Para instalar y configurar los controladores de VM invitada de NVIDIA GRID, siga estos pasos generales:

1. Asegúrese de que la VM invitada esté apagada.
2. En el panel de control del hipervisor, asigne una GPU a la VM.
3. Inicie la VM.

4. Instale el controlador de VM invitada (de su proveedor de la nube o de NVIDIA) en la VM.

Paso 7: Especificar una base de datos para usar

Puede alternar entre SQLite y PostgreSQL después de instalar el paquete de VDA de Linux. Para ello, complete los siguientes pasos:

> **Nota:**
>
> - Recomendamos usar SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
> - Para la instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, Linux VDA usa PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).
> - También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

1. (Opcional) Para usar una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, instale la versión especificada manualmente e inicie el servicio PostgreSQL.
2. Edite **/etc/xdl/db.conf** para especificar una base de datos que usar. A continuación, se muestra un ejemplo del archivo **db.conf**:

```
# database configuration file for Linux VDA



## database choice

# possible choices are:

#     SQLite
```

```
#     PostgreSQL

# default choice is PostgreSQL

DbType="PostgreSQL"




## database port

# specify database port for the database.

# if not specified, default port will be used:

# SQLite: N/A

# PostgreSQL: 5432

DbPort=5432




## PostgreSQL customized

# only the following value means true, otherwise false:

#     true

#     yes

#     y

#     YES

#     Y

# default is false

DbCustomizePostgreSQL=false
```

```
## PostgreSQL service name

# specify the service name of PostgreSQL for Linux VDA

# default is "postgresql"

DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

3. Ejecute **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** o **/opt/Citrix/VDA/bin/easyinstall**.

Paso 8: Ejecute la instalación sencilla para configurar el entorno y el VDA para completar la instalación

Después de instalar el paquete Linux VDA, configure el entorno de ejecución mediante el script ctxinstall.sh o la GUI.

Nota:

Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional **en_US.UTF-8** esté instalada en su sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando **sudo locale-gen en_US.UTF-8**. Para Debian, edite el archivo **/etc/locale.gen** descomentando la línea **# en_US.UTF-8 UTF-8** y, a continuación, ejecute el comando **sudo locale-gen**.

ctxinstall.sh

ctxinstall.sh es el script de instalación sencilla para realizar algunas configuraciones previas y establecer las variables de entorno de ejecución de VDA.

- Solo el usuario root puede ejecutar este script.
- La instalación sencilla utiliza /opt/Citrix/VDA/sbin/ctxinstall.conf como archivo de configuración para establecer, guardar y sincronizar los valores de todas las variables de entorno utilizadas. Le recomendamos que lea la plantilla (ctxinstall.conf.tmpl) detenidamente y, a continuación,

personalice su propio ctxinstall.conf. Cuando cree el archivo de configuración por primera vez, utilice cualquiera de las siguientes formas:

  - Copiando el archivo de plantilla /opt/Citrix/VDA/sbin/ctxinstall.conf.tmpl y guardándolo como /opt/Citrix/VDA/sbin/ctxinstall.conf.
  - Al ejecutar ctxinstall.sh. Cada vez que ejecuta ctxinstall.sh, su entrada se guarda en /opt/Citrix/VDA/sbin/ctxinstall.conf.

- Easy install admite la ejecución modular. Los módulos incluyen la comprobación previa, la instalación, la configuración de dominio, la configuración y la verificación.
- Los detalles de depuración de este script se pueden encontrar en /var/log/xdl/ctxinstall.log.

Para obtener más información, utilice el comando de ayuda **ctxinstall.sh -h**.

> **Nota:**
>
> - Siguiendo el principio de privilegio mínimo, asegúrese de que solo el usuario root pueda leer **/opt/Citrix/VDA/sbin/ctxinstall.conf** porque la contraseña de unión al dominio podría estar establecida en el archivo.
> - La desinstalación del VDA de Linux elimina los archivos de **/opt/Citrix/VDA**. Le recomendamos que haga una copia de seguridad de **/opt/Citrix/VDA/sbin/ctxinstall.conf** antes de desinstalar el VDA.

> Puede ejecutar ctxinstall.sh en modo interactivo o en modo silencioso. Antes de ejecutar el script, establezca las siguientes variables de entorno:

- **CTX_XDL_NON_DOMAIN_JOINED='y\|n'** – Si se une la máquina a un dominio. El valor predeterminado es 'n'. Para escenarios unidos a un dominio, establézcalo en 'n'.
- **CTX_XDL_AD_INTEGRATION='sssd\|winbind\|centrify\|pbis\|quest'** – El VDA de Linux requiere la configuración de Kerberos para autenticarse con los Delivery Controllers. La configuración de Kerberos se determina a partir de la herramienta de integración de Active Directory instalada y configurada en el sistema.
- **CTX_XDL_DDC_LIST='<list-ddc-fqdns\>'** – El VDA de Linux requiere una lista de nombres de dominio completos (FQDN) de Delivery Controller separados por espacios para registrarse en un Delivery Controller. Se debe especificar al menos un FQDN o CNAME.

- **CTX_XDL_VDI_MODE='y\|n'** – Si se configura la máquina como un modelo de entrega de escritorio dedicado (VDI) o un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca el valor en **'y'**.
- **CTX_XDL_HDX_3D_PRO='y\|n'** – El VDA de Linux admite HDX 3D Pro, un conjunto de tecnologías de aceleración de GPU diseñadas para optimizar la virtualización de aplicaciones con gráficos enriquecidos. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única), es decir, CTX_XDL_VDI_MODE=**'y'**.
- **CTX_XDL_START_SERVICE='y\|n'** – Determina si los servicios del VDA de Linux se inician cuando se completa la configuración.
- **CTX_XDL_REGISTER_SERVICE='y\|n'** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES='y\|n'** – Los servicios del VDA de Linux requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos necesarios (por defecto, los puertos 80 y 1494) automáticamente en el firewall del sistema para Linux Virtual Desktop.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/kde/mate/xfce/'<none\>'** – Especifica el entorno de escritorio GNOME, GNOME Classic, KDE, MATE o **Xfce** que se utilizará en las sesiones. Si lo establece en **'<none\>'**, se utiliza el escritorio predeterminado configurado en el VDA.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET para admitir el nuevo servicio de agente de broker (**ctxvda**). La ruta predeterminada es **'/usr/bin'**.
- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP.
- **CTX_XDL_SITE_NAME=<dns-name\>** – El VDA de Linux detecta servidores LDAP a través de DNS. Para limitar los resultados de la búsqueda de DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_LDAP_LIST='<list-ldap-servers\>'** – El VDA de Linux consulta DNS para detectar servidores LDAP. Si DNS no puede proporcionar registros de servicio LDAP, puede proporcionar una lista de FQDN de LDAP separados por espacios con puertos LDAP. Por ejemplo, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Para habilitar consultas LDAP más rápidas dentro de un bosque de Active Directory, habilite el Catálogo global en un controlador de dominio y especifique el número de puerto LDAP relevante como 3268. Esta variable se establece en **'<none\>'** de forma predeterminada.

- **CTX_XDL_SEARCH_BASE=search-base-set** – El VDA de Linux consulta LDAP a través de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=mycompany,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_SUPPORT_DDC_AS_CNAME='y\|n'** – El VDA de Linux admite la especificación de un nombre de Delivery Controller mediante un registro CNAME de DNS.
- **CTX_EASYINSTALL_DNS='<ip-address-of-dns\>'** – La dirección IP de DNS.
- **CTX_EASYINSTALL_HOSTNAME=host-name** – El nombre de host del servidor VDA de Linux.
- **CTX_EASYINSTALL_NTPS=address-of-ntps** – La dirección IP o el nombre de cadena del servidor NTP.
- **CTX_EASYINSTALL_REALM=realm-name** – El nombre del reino de Kerberos.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_USERNAME=domain-user-name** – El nombre del usuario que une la máquina al dominio.
- **CTX_EASYINSTALL_PASSWORD=password** – La contraseña del usuario que une la máquina al dominio.

Nota:

Le recomendamos que no utilice la cuenta de administrador para unir el dominio. En su lugar, delegue los permisos de unión al dominio a un usuario de Active Directory que no sea la cuenta de administrador. Para ello, delegue el control en el controlador de dominio mediante el **Asistente para la delegación de control**.

Las siguientes cuatro variables son opcionales. Aunque no estén configuradas, ctxinstall.sh no se abortará en modo silencioso y no se le pedirá la entrada del usuario en modo interactivo. Puede configurarlas solo exportando sus valores o editando **/Citrix/VDA/sbin/ctxinstall.conf**.

- **CTX_EASYINSTALL_NETBIOS_DOMAIN=netbios-domain-name** – El nombre de dominio NetBIOS suele ser el primer componente del nombre de dominio DNS separado por un punto (.). De lo contrario, personalice un nombre de dominio NetBIOS diferente. Esta variable es opcional.

- **CTX_EASYINSTALL_OU=ou-value** – Los valores de OU varían según los diferentes métodos de integración de **AD**. Para ver un ejemplo de valores de OU, consulte la tabla en la sección Consideraciones de este artículo. Esta variable es opcional.
- **CTX_EASYINSTALL_TRUSTED_DOMAINS=trusted-domains** – Para entornos multidominio, especifique una lista de dominios de confianza separados por espacios (por ejemplo, "mycompany1.com mycompany2.com"). Esto actualiza los dominios de confianza en /etc/krb5.conf y permite la detección automática de servidores LDAP en esos dominios si no se especifica **CTX_XDL_LDAP_LIST**. Esta variable es opcional.

> **Nota**
>
> SSSD solo admite dominios de confianza en un único bosque de Active Directory.

- **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=centrify-local-path** – Easy install ayuda a descargar el paquete de Centrify de Internet. Sin embargo, si Centrify ya está instalado, puede obtener el paquete de Centrify de un directorio local definido por esta variable. Esta variable es opcional.
- **CTX_EASYINSTALL_PBIS_LOCAL_PATH= pbis-local-path** – Easy install ayuda a descargar el paquete de PBIS de Internet. Sin embargo, si PBIS ya está instalado, puede obtener el paquete de PBIS de un directorio local definido por esta variable. Esta variable es opcional.
- **CTX_EASYINSTALL_QUEST_LOCAL_PATH=quest-local-path** - La ruta local que contiene el ejecutable vastool. Si no se establece, se utiliza la ruta predeterminada /opt/quest/bin. Esta variable es opcional.
- **CTX_XDL_DJ_ENROLLMENT_TOKEN_FILE=`'<none>'`** - La ruta completa al archivo de token de inscripción para conexiones WebSocket a los Delivery Controllers. Esta variable es opcional.
- **CTX_XDL_ENROLLMENT_TOOL_USING_LDAPS='n'** - Determina si VdaEnrollmentTool utiliza LDAPS para consultar los SID de los equipos. Si utiliza LDAPS, asegúrese de que los servidores LDAP sean verificables con certificados del sistema local. Esta variable es opcional.

Consideraciones

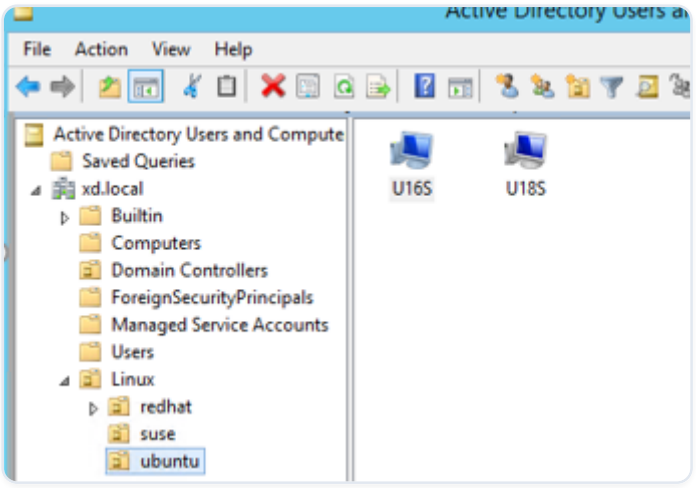
- El nombre de dominio NetBIOS suele ser el primer componente del nombre de dominio DNS separado por un punto (.). Para personalizar un nombre de dominio NetBIOS diferente en su

entorno, establezca la variable de entorno **CTX_EASYINSTALL_NETBIOS_DOMAIN** en **/opt/Citrix/VDA/sbin/ctxinstall.conf**.

- Para unir su VDA a una OU específica, haga lo siguiente:

  a. Asegúrese de que la OU específica exista en el controlador de dominio.

  Para ver un ejemplo de OU, consulte la siguiente captura de pantalla:



  b. Establezca la variable de entorno **CTX_EASYINSTALL_OU** en **/opt/Citrix/VDA/sbin/ctxinstall.conf**.

  Los valores de OU varían según los diferentes métodos de AD. La siguiente tabla muestra los nombres de OU de ejemplo de la captura de pantalla anterior. Puede utilizar cualquier otro nombre de OU en su organización.

OS	WINBIND	SSSD	CENTRIFY	PBIS
Debian	`"Linux/debian"`	`"Linux/debian"`	`"XD.LOCAL/Linux/debian"`	`"Linux/debian"`
RHEL 9.8/9.6/9.4, Rocky Linux 9.8/9.6/9.4	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	N/D	N/D
RHEL 8.x	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	`"XD.LOCAL/Linux/redhat"`	`"Linux/redhat"`

OS	WINBIND	SSSD	CENTRIFY	PBIS
Rocky Linux 8.x	`"OU=redhat, OU=Linux"`	`"OU=redhat, OU=Linux"`	N/D	N/D
SUSE	`"Linux/ suse"`	`"Linux/ suse"`	`"XD.LOCAL/ Linux/suse"`	`"Linux/ suse"`
Ubuntu	`"Linux/ ubuntu"`	`"Linux/ ubuntu"`	`"XD.LOCAL/ Linux/ ubuntu"`	`"Linux/ ubuntu"`

- Centrify no admite la configuración DNS puramente **IPv6**. Se requiere al menos un servidor DNS que utilice **IPv4** en /etc/resolv.conf para que **adclient** encuentre los servicios de AD correctamente.

  Registro:

  ```
  ADSITE    : Check that this machine's subnet is in a site known by AD
    : Failed

          : This machine's subnet is not known by AD.

          : We guess you should be in the site Site1.
  ```

  Este problema es exclusivo de Centrify y su configuración. Para resolver este problema, haga lo siguiente:

  a. Abra **Administrative Tools** en el controlador de dominio.

  b. Seleccione **Active Directory Sites and Services**. c. Agregue una dirección de subred adecuada para **Subnets**.

- La instalación fácil admite **IPv6** puro a partir de Linux VDA 7.16. Se aplican las siguientes condiciones previas y limitaciones:

  - Su repositorio de Linux debe estar configurado para garantizar que su máquina pueda descargar los paquetes necesarios a través de redes **IPv6** puras.
  - Centrify no es compatible con redes **IPv6** puras.

> **Nota:**

> Si su red es **IPv6** pura y toda su entrada está en formato **IPv6** adecuado, el VDA se registra con el Delivery Controller™ a través de **IPv6**. Si su red tiene una configuración híbrida de **IPv4** e **IPv6**, el tipo de la primera dirección IP de DNS determina si se utiliza **IPv4** o **IPv6** para el registro.

- Puede especificar un entorno de escritorio para usar en las sesiones mediante la variable CTX_XDL_DESKTOP_ENVIRONMENT, como se describió anteriormente. También puede cambiar entre entornos de escritorio ejecutando comandos o usando la bandeja del sistema. Para obtener más información, consulte Comandos de cambio de escritorio y Bandeja del sistema.
- Si elige Centrify como método para unirse a un dominio, el script ctxinstall.sh requiere el paquete de Centrify. Formas en que ctxinstall.sh puede obtener el paquete de Centrify:
  - La instalación fácil ayuda a descargar el paquete de Centrify de Internet automáticamente. Las siguientes son las URL para cada distribución:

    Para RHEL: wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz>`

    Para SUSE: wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-suse12-x86_64.tgz>`

    Para Ubuntu/Debian: wget `<https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-deb9-x86_64.tgz>`
  - Obtenga el paquete de Centrify de un directorio local si Centrify ya está instalado. Para designar el directorio del paquete de Centrify, establezca **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=/home/mydir** en **/opt/Citrix/VDA/sbin/ctxinstall.conf**. Por ejemplo:

    ```
    ls  -ls  /home/mydir

        9548 -r-xr-xr-x. 1 root root  9776688 May 13  2016 adcheck-
    rhel4-x86_64

        4140 -r--r--r--. 1 root root  4236714 Apr 21  2016
    centrifyda-3.3.1-rhel4-x86_64.rpm

        33492 -r--r--r--. 1 root root 34292673 May 13  2016
    ```

```
centrifydc-5.3.1-rhel4-x86_64.rpm

    4 -rw-rw-r--. 1 root root     1168 Dec  1  2015 centrifydc-
install.cfg

    756 -r--r--r--. 1 root root   770991 May 13  2016 centrifydc-
ldapproxy-5.3.1-rhel4-x86_64.rpm

    268 -r--r--r--. 1 root root   271296 May 13  2016 centrifydc-
nis-5.3.1-rhel4-x86_64.rpm

    1888 -r--r--r--. 1 root root  1930084 Apr 12  2016 centrifydc-
openssh-7.2p2-5.3.1-rhel4-x86_64.rpm

    124 -rw-rw-r--. 1 root root   124543 Apr 19  2016 centrify-
suite.cfg

    0 lrwxrwxrwx. 1 root root       10 Jul  9  2012 install-
express.sh -> install.sh

    332 -r-xr-xr--. 1 root root   338292 Apr 10  2016 install.sh

    12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-notes-
agent-rhel4-x86_64.txt

    4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-notes-
da-rhel4-x86_64.txt

    4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-notes-
nis-rhel4-x86_64.txt

    12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-notes-
openssh-rhel4-x86_64.txt
```

- Si elige PBIS como método para unirse a un dominio, el script ctxinstall.sh requiere el paquete de PBIS. Formas en que ctxinstall.sh puede obtener el paquete de PBIS:
    - La instalación fácil ayuda a descargar el paquete de PBIS de Internet automáticamente. Por ejemplo, las siguientes son las URL para cada distribución:

      Para RHEL 8, SUSE 15.6: wget `<https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh>`

Debian y Ubuntu: wget `<https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh>`

- Obtenga una versión específica del paquete PBIS de Internet. Para ello, cambie las líneas "pbisDownloadRelease" y "pbisDownloadExpectedSHA256" en el archivo /opt/Citrix/VDA/sbin/ctxinstall.sh.

  Para ver un ejemplo, consulte la siguiente captura de pantalla:



- Obtenga el paquete PBIS de un directorio local si PBIS ya está instalado. Para designar el directorio del paquete PBIS, establezca la variable de entorno **CTX_EASYINSTALL_PBIS_LOCAL_PATH** en **/opt/Citrix/VDA/sbin/ctxinstall.conf**.

Modo interactivo

Para ejecutar el script **ctxinstall.sh** en modo interactivo, utilice el comando **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** sin la opción **-S**. Escriba el valor de la variable correspondiente en cada solicitud de la interfaz de línea de comandos. Si una variable ya está establecida, ctxinstall.sh le pedirá confirmación en caso de que desee cambiarla.

Modo silencioso

En modo silencioso, debe establecer las variables anteriores mediante **/opt/Citrix/VDA/sbin/ctxinstall.conf** o el comando export. Después, ejecute **ctxinstall.sh -S** (tenga en cuenta que la letra **S** aquí está en **mayúsculas**). Si no se establecen todas las variables requeridas o algún valor no es válido, **ctxinstall.sh** aborta la ejecución, a menos que haya valores predeterminados.

El valor exportado para cada variable sobrescribe el valor en **/Citrix/VDA/sbin/ctxinstall.conf**, a menos que no esté establecido. Todos los valores actualizados se guardan en **/Citrix/VDA/sbin/ctxinstall.conf**, excepto la contraseña de unión al dominio. Por lo tanto, en modo silencioso, debe establecer la contraseña de unión al dominio en **/Citrix/VDA/sbin/ctxinstall.conf** o exportar la contraseña.

```
export CTX_XDL_NON_DOMAIN_JOINED='n'

export CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest

export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'

export CTX_XDL_VDI_MODE='y|n'
```

```
export CTX_XDL_HDX_3D_PRO='y|n'

export CTX_XDL_START_SERVICE='y|n'

export CTX_XDL_REGISTER_SERVICE='y|n'

export CTX_XDL_ADD_FIREWALL_RULES='y|n'

export CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|
xfce|'<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'

export CTX_XDL_VDA_PORT='<port-number>'

export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'

export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'

export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'

export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'

export CTX_EASYINSTALL_DNS='<ip-address-of-dns>'

export CTX_EASYINSTALL_HOSTNAME='<host-name>'

export CTX_EASYINSTALL_NTPS='<address-of-ntps>'

export CTX_EASYINSTALL_REALM='<realm-name>'

export CTX_EASYINSTALL_FQDN='<ad-fqdn-name>'

export CTX_EASYINSTALL_USERNAME='<domain-user-name>'

export CTX_EASYINSTALL_PASSWORD='<password>'

export CTX_EASYINSTALL_NETBIOS_DOMAIN='<netbios-domain>'

export CTX_EASYINSTALL_OU='<organization-unit>'
```

```
sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh -S
```

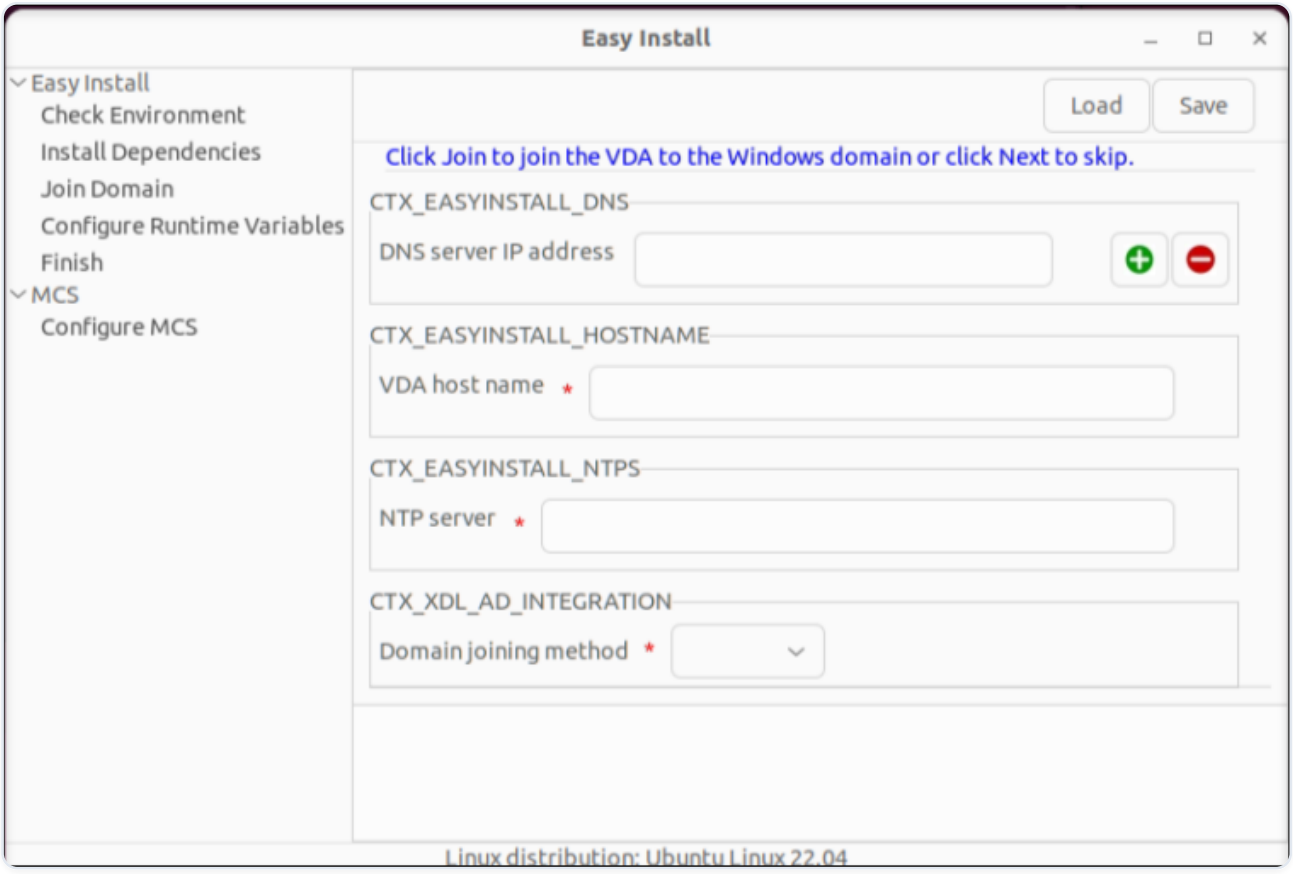
Al ejecutar el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que crea. Le recomendamos que cree un archivo de script de shell a partir de los comandos anteriores con **#\!/bin/bash** como primera línea.

Alternativamente, puede especificar todas las variables mediante un solo comando.

Para configurar las variables de entorno de ejecución de VDA (las que comienzan con '**CTX_XDL_**'), puede ejecutar **ctxinstall.sh -s** (tenga en cuenta que la letra **s** aquí está en **minúsculas**).

GUI

Puede utilizar la instalación fácil a través de una GUI. Ejecute el comando **/opt/Citrix/VDA/bin/easyinstall** en el entorno de escritorio de su VDA y, a continuación, siga las instrucciones de la GUI de instalación fácil.



La GUI de instalación fácil le guía a través de las siguientes operaciones:

- Comprobar el entorno del sistema
- Configurar la base de datos

- Instalar dependencias
- Unir el VDA a un dominio especificado
- Configurar el entorno de tiempo de ejecución

> **Sugerencia:**

> Haga clic en **Guardar** para guardar la configuración de las variables en un archivo local en la ruta que especifique. Haga clic en **Cargar** para cargar la configuración de las variables desde un archivo que especifique.

Paso 9: Ejecutar XDPing

Ejecute `sudo /opt/Citrix/VDA/bin/xdping` para comprobar si hay problemas de configuración comunes en un entorno VDA de Linux. Para obtener más información, consulte **XDPing**.

Paso 10: Ejecutar el VDA de Linux

Iniciar el VDA de Linux:

Para iniciar los servicios del VDA de Linux:

```
sudo systemctl start ctxhdx.service



sudo systemctl start ctxvda.service
```

Detener el VDA de Linux:

Para detener los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda.service



sudo systemctl stop ctxhdx.service
```

> **Nota:**

> Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que detuvo.

> **Reiniciar el VDA de Linux:**

Para reiniciar los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda.service



sudo systemctl restart ctxhdx.service



sudo systemctl start ctxvda.service
```

Comprobar el estado del VDA de Linux:

Para comprobar el estado de ejecución de los servicios del VDA de Linux:

```
sudo systemctl status ctxvda.service



sudo systemctl status ctxhdx.service
```

Paso 11: Crear catálogos de máquinas

El proceso para crear catálogos de máquinas y agregar máquinas VDA de Linux es similar al enfoque tradicional de VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Para crear catálogos de máquinas que contengan máquinas VDA de Linux, existen algunas restricciones que diferencian el proceso de la creación de catálogos de máquinas para máquinas VDA de Windows:

- Para el sistema operativo, seleccione:
  - La opción **Multi-session OS** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **Single-session OS** para un modelo de entrega de escritorios dedicados VDI.
- No mezcle máquinas VDA de Linux y Windows en el mismo catálogo de máquinas.

Nota:

Las primeras versiones de Citrix Studio no admitían la noción de un "sistema operativo Linux". Sin embargo, seleccionar la opción **Windows Server OS** o **Server OS** implica un modelo de entrega de escritorios compartidos alojados equivalente. Seleccionar la opción **Windows Desktop OS** o **Desktop OS** implica un modelo de entrega de un solo usuario por máquina.

Sugerencia:

Si quita y vuelve a unir una máquina al dominio de Active Directory, debe quitar y volver a agregar la máquina al catálogo de máquinas.

Paso 12: Crear grupos de entrega

El proceso para crear un grupo de entrega y agregar catálogos de máquinas que contengan máquinas VDA de Linux es casi idéntico al de las máquinas VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear grupos de entrega.

Para crear grupos de entrega que contengan catálogos de máquinas Linux VDA, se aplican las siguientes restricciones:

- Asegúrese de que los usuarios y grupos de AD que seleccione se hayan configurado correctamente para iniciar sesión en las máquinas Linux VDA.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No mezcle el grupo de entrega con catálogos de máquinas que contengan máquinas Windows.

Importante:

La publicación de aplicaciones es compatible con Linux VDA versión 1.4 y posteriores. Sin embargo, Linux VDA no admite la entrega de escritorios y aplicaciones a la misma máquina.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2503.

Paso 13: Actualizar el Linux VDA (opcional)

El Linux VDA admite actualizaciones desde la versión más reciente. Por ejemplo, puede actualizar el Linux VDA de 2308 a 2311 y de 1912 LTSR a 2203 LTSR.

Nota:

- La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de realizar una actualización, asegúrese de hacer una copia de seguridad de los archivos.
- A partir de la versión 2407, el Linux VDA delega en los administradores de paquetes **rpm** o **dpkg** la gestión de los archivos de configuración durante las actualizaciones. A continuación, se describe cómo interactúan rpm y dpkg con los cambios en los archivos de configuración:
  - **rpm**: de forma predeterminada, conserva la versión local y guarda la nueva versión del paquete con una extensión **.rpmnew**.
  - **dpkg**: le pide interactivamente que elija cómo proceder. Para actualizar el Linux VDA de forma silenciosa, conservando el archivo de configuración local y guardando la nueva versión del paquete como **.dpkg-new** o **.dpkg-dist**, utilice el siguiente comando:

    ```
    dpkg --force-confold -i package.deb  # Always keep your version, then save new package's version as *.dpkg-new or *.dpkg-dist
    ```

Para distribuciones RHEL y Rocky Linux:

```
sudo yum -y localinstall <PATH>/<Linux VDA RPM>
```

Nota:

Antes de actualizar el Linux VDA en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.

Para distribuciones SUSE:

```
sudo zypper -i install <PATH>/<Linux VDA RPM>
```

Para distribuciones de Ubuntu/Debian:

```
sudo dpkg -i <PATH>/<Linux VDA deb>



sudo apt-get install -f
```

Solución de problemas

Utilice la información de esta sección para solucionar problemas que puedan surgir al usar la función de instalación sencilla.

Error al unirse a un dominio mediante SSSD

Puede producirse un error al intentar unirse a un dominio, con una salida similar a la siguiente (verificar los registros para la impresión en pantalla):

`Step 6: join Domain!Enter ctxadmin's password:Failed to join domain: failed to lookup DC info for domain 'CITRIXLAB.LOCAL' over rpc: The network name cannot be found`

/var/log/xdl/vda.log:

```
2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service successfully
obtained the following list of 1 delivery controller(s) with which to
register: 'CTXDDC.citrixlab.local (10.158.139.214)'.

2016-11-04 02:11:52.362 [ERROR] -
RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register
```

```
with http://CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar.
Error: General security error (An error occurred in trying to obtain a
TGT: Client not found in Kerberos database (6))

2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
connect to the delivery controller 'http://CTXDDC.citrixlab.local:80/
Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')

Check the following:- The system clock is in sync between this machine and
the delivery controller.

-  The Active Directory provider (e.g. winbind daemon) service is running
and correctly configured.

-  Kerberos is correctly configured on this machine.

If the problem persists, please refer to Citrix Knowledge Base article
CTX117248 for further information.

Error Details:

Exception 'General security error (An error occurred in trying to obtain a
TGT: Client not found in Kerberos database (6))' of type 'class
javax.xml.ws.soap.SOAPFaultException'.

2016-11-04 02:11:52.362 [INFO ] -
RegistrationManager.AttemptRegistrationWithSingleDdc: The current time for
this VDA is Fri Nov 04 02:11:52 EDT 2016.

Ensure that the system clock is in sync between this machine and the
delivery controller.

Verify the NTP daemon is running on this machine and is correctly
configured.

2016-11-04 02:11:52.364 [ERROR] - Could not register with any controllers.
Waiting to try again in 120000 ms. Multi-forest - false

2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
register with any controllers in the last 470 minutes.
```

/var/log/messages:

`Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Failed to initialize credentials using keytab [MEMORY:/etc/krb5.keytab]: Client 'RH-WS-68$@CITRIXLAB.LOCAL' not found in Kerberos database. Unable to create GSSAPI-encrypted LDAP connection.Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Client 'RH-WS-68$@CITRIXLAB.LOCAL' not found in Kerberos database`

Para resolver este problema:

1. Ejecute el comando `rm -f /etc/krb5.keytab`.
2. Ejecute el comando `net ads leave $REALM -U $domain-administrator`.
3. Quite el catálogo de máquinas y el grupo de entrega en el Delivery Controller.
4. Run /opt/Citrix/VDA/sbin/ctxinstall.sh.
5. Cree el catálogo de máquinas y el grupo de entrega en el Delivery Controller.

Las sesiones de escritorio de Ubuntu muestran una pantalla gris

Este problema ocurre cuando se inicia una sesión que luego se bloquea en un escritorio en blanco. Además, la consola de la máquina también muestra una pantalla gris al iniciar sesión con una cuenta de usuario local.

Para resolver este problema:

1. Ejecute el comando `sudo apt-get update`.
2. Ejecute el comando `sudo apt-get install unity lightdm`.
3. Agregue la siguiente línea a `/etc/lightdm/lightdm.conf`:

   `greeter-show-manual-login=true`

Los intentos de iniciar las sesiones de escritorio de Ubuntu fallan debido a la falta de un directorio de inicio

/var/log/xdl/hdx.log:

```
2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)



2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent: Session
started for user ctxadmin.
```

```
2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
Login Process died: normal.



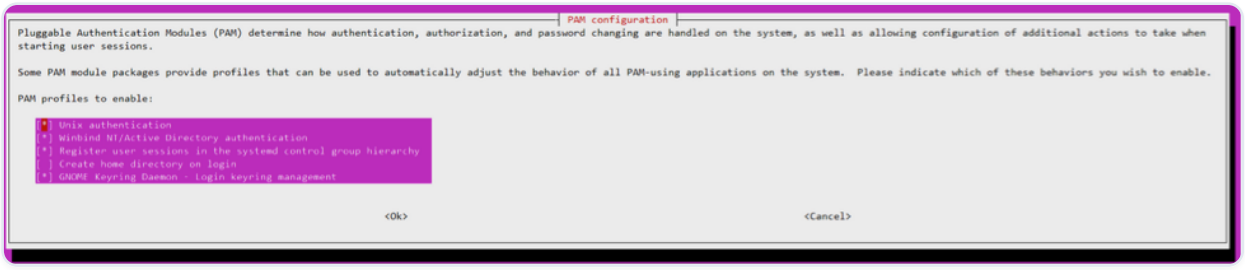
2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting normally.
```

Sugerencia:

La causa principal de este problema es que el directorio de inicio no se crea para el administrador del dominio.

Para resolver este problema:

1. Desde la línea de comandos, escriba **pam-auth-update**.
2. En el cuadro de diálogo resultante, verificar que **Create home directory login** esté seleccionado.



La sesión no se inicia o finaliza rápidamente con un error de dbus

/var/log/messages (para RHEL o CentOS):

```
Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
CITRIXLAB\ctxadmin.



Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0
```

```
Oct 27 04:17:18 CentOS7 gnome-session[19146]: ERROR: Failed to connect to
system bus: Exhausted all available authentication mechanisms (tried:
EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available: EXTERNAL,
DBUS_COOKIE_SHA1, ANONYMOUS)#012aborting...



Oct 27 04:17:18 CentOS7 gnome-session: gnome-session[19146]: ERROR: Failed
to connect to system bus: Exhausted all available authentication
mechanisms (tried: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available:
EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS)



Oct 27 04:17:18 CentOS7 gnome-session: aborting...



Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.



Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
CITRIXLAB\ctxadmin.
```

O, alternativamente para las distribuciones de Ubuntu, utilice el registro /var/log/syslog:

```
Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
Stale PID file, overwriting.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] bluez5-
util.c: Failed to get D-Bus connection: Did not receive a reply. Possible
causes include: the remote application did not send a reply, the message
bus security policy blocked the reply, the reply timeout expired, or the
network connection was broken.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] hashmap.c:
Assertion 'h' failed at pulsecore/hashmap.c:116, function
```

```
pa_hashmap_free(). Aborting.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
util.c: Failed to connect to system bus: Did not receive a reply. Possible
causes include: the remote application did not send a reply, the message
bus security policy blocked the reply, the reply timeout expired, or the
network connection was broken.



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
times: [ [pulseaudio] core-util.c: Failed to connect to system bus: Did
not receive a reply. Possible causes include: the remote application did
not send a reply, the message bus security policy blocked the reply, the
reply timeout expired, or the network connection was broken.]



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-
ctxgfx[24693]: Exiting normally
```

Algunos grupos o módulos no surten efecto hasta que se reinicia el sistema. Si los mensajes de error de **dbus** aparecen en el registro, le recomendamos que reinicie el sistema y lo intente de nuevo.

SELinux impide que SSHD acceda al directorio de inicio

El usuario puede iniciar una sesión, pero no puede iniciar sesión.

/var/log/xdl/ctxinstall.log:

```
Jan 25 23:30:31 yz-rhel72-1 setroubleshoot[3945]: SELinux is preventing /
usr/sbin/sshd from setattr access on the directory /root. For complete
SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698-963a79f16b81



Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/sbin/
sshd from setattr access on the directory /root.
```

```
*****  Plugin catchall_boolean (89.3 confidence) suggests
******************


If you want to allow polyinstantiation to enabled


   Then you must tell SELinux about this by enabling the
'polyinstantiation_enabled' boolean.


You can read 'None' man page for more details.


    Do


       setsebool -P polyinstantiation_enabled 1


*****  Plugin catchall (11.6 confidence) suggests
*************************


If you believe that sshd should be allowed setattr access on the root
directory by default.


Then you should report this as a bug.


You can generate a local policy module to allow this access.
```

```
      Do


       allow this access for now by executing:


       # grep sshd /var/log/audit/audit.log | audit2allow -M mypol


# semodule -i mypol.pp
```

Para resolver este problema:

1. Deshabilite SELinux realizando el siguiente cambio en /etc/selinux/config.

   SELINUX=disabled
2. Reinicie el VDA.

Crear VDA de Linux no unidos a un dominio mediante MCS

Este artículo le guía a través del uso del método de Machine Creation Services (MCS) para crear un VDA de Linux no unido a un dominio con un catálogo de máquinas en Citrix DaaS o Citrix Virtual Apps and Desktops™ 2411 y versiones posteriores.

Importante:

- Para clientes de Citrix DaaS™:
  - Puede implementar VDA no unidos a un dominio en una nube pública o en el centro de datos local. Los VDA no unidos a un dominio son administrados por el plano de control en Citrix DaaS.
  - Para crear VDA no unidos a un dominio, los clientes que utilizan el servicio Citrix Gateway deben asegurarse de que Rendezvous V2 esté habilitado. Los Cloud

Connectors solo son necesarios si planea aprovisionar máquinas en hipervisores locales o si desea utilizar Active Directory como proveedor de identidades en Workspace.

- Para clientes de CVAD:
  - Habilite la función WebSocket en el DDC siguiendo las instrucciones a continuación:

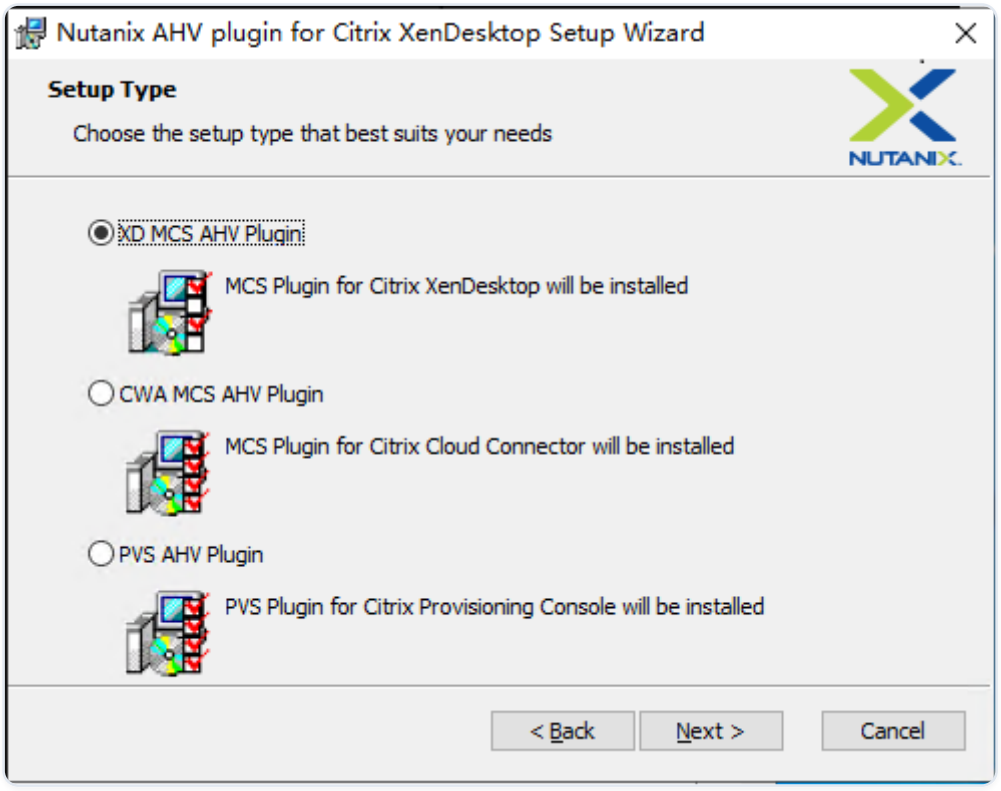
    Abra PowerShell y ejecute el siguiente comando, luego reinicie el DDC New-ItemProperty `"HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force`
- Para crear VDA no unidos a un dominio, puede usar tanto MCS como la instalación sencilla. Para obtener más información, consulte Crear VDA de Linux no unidos a un dominio mediante MCS y Crear un VDA de Linux no unido a un dominio mediante instalación sencilla.
- MCS no es compatible con servidores bare metal.
- Las siguientes funciones están disponibles para VDA de Linux no unidos a un dominio:
  - Crear usuarios locales con atributos especificados en VDA no unidos a un dominio
  - Autenticación sin SSO
  - Autenticación con Azure Active Directory
  - Rendezvous V2

(Solo para Nutanix) Paso 1: Instale y registre el complemento Nutanix AHV

Obtenga el paquete del complemento Nutanix AHV de Nutanix. Instale y registre el complemento en su entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte la guía de instalación del complemento Nutanix Acropolis MCS, disponible en el Portal de soporte de Nutanix.

Paso 1a: Instale y registre el complemento Nutanix AHV para Delivery Controllers locales

Después de instalar Citrix Virtual Apps™ and Desktops, seleccione e instale el **XD MCS AHV Plugin** en sus Delivery Controllers.



Paso 1b: Instale y registre el complemento Nutanix AHV para Delivery Controllers en la nube

Seleccione e instale el **CWA MCS AHV Plugin** para Citrix Cloud™ Connectors. Instale el complemento en todos los Citrix Cloud Connectors que estén registrados con el inquilino de Citrix Cloud. Debe registrar los Citrix Cloud Connectors incluso cuando presten servicio a una ubicación de recursos sin AHV.

Paso 1c: Complete los siguientes pasos después de instalar el complemento

- verificar que se ha creado una carpeta de Nutanix Acropolis en `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.
- Ejecute el comando `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`.
- Reinicie los servicios Citrix Host, Citrix Broker y Citrix Machine Creation Services™ en sus Delivery Controllers locales o reinicie el servicio Citrix RemoteHCLServer Service en los Citrix Cloud Connectors.

> **Sugerencia:**

> Recomendamos que detenga y luego reinicie los servicios Citrix Host, Citrix Broker y Machine Creation Services al instalar o actualizar el complemento Nutanix AHV.

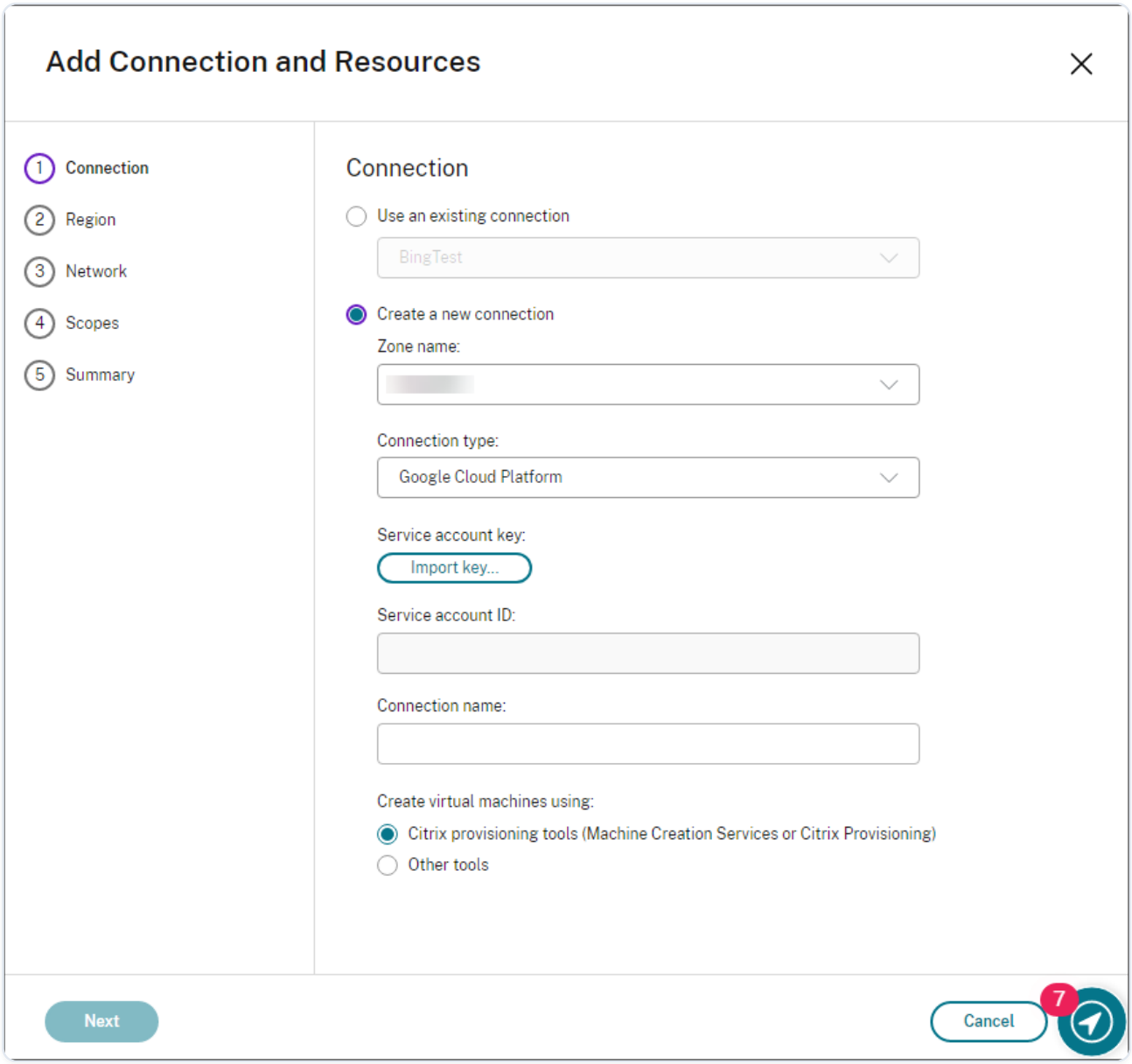
Paso 2: Crear una conexión de host

Los hosts son hipervisores o servicios en la nube que se utilizan en sus ubicaciones de recursos. Este paso le permite especificar la información que DaaS utiliza para comunicarse con las VMs en un host. La información detallada incluye la ubicación de los recursos, el tipo de host, las credenciales de acceso, el método de almacenamiento a utilizar y qué redes pueden usar las VMs en el host.

> **Importante:**
>
> Los recursos de host (almacenamiento y red) de su ubicación de recursos deben estar disponibles antes de crear una conexión.

1. Inicie sesión en Citrix Cloud.
2. En el menú superior izquierdo, seleccione **My Services > DaaS**.
3. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel izquierdo.
4. Seleccione **Agregar conexiones y recursos** en la barra de acciones.
5. El asistente le guiará por las siguientes páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página de **Resumen**.

Paso 2a: Conexión



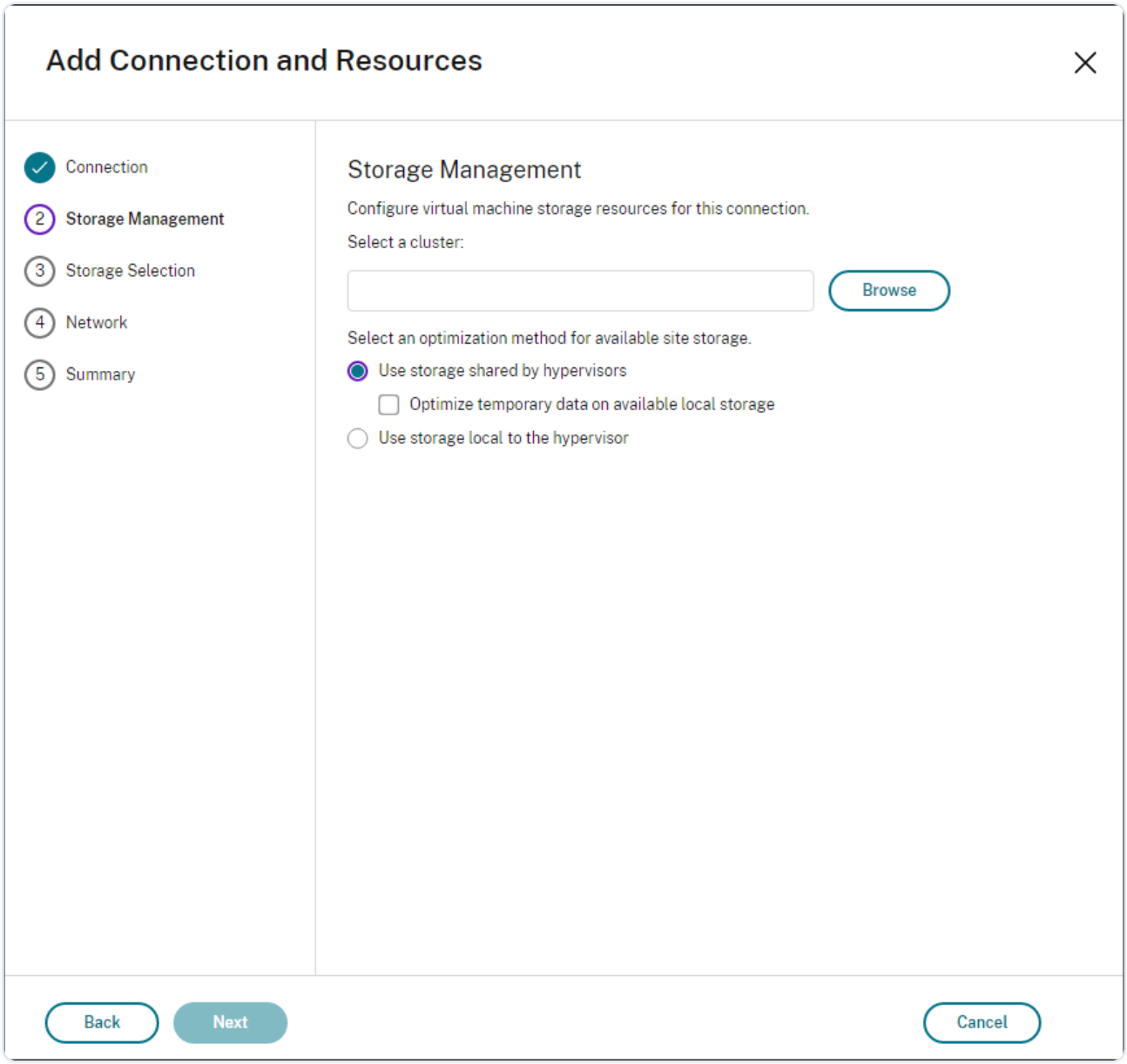
En la página **Conexión**:

- Para crear una conexión, seleccione **Crear una conexión nueva**. Para crear una conexión basada en la misma configuración de host que una conexión existente, seleccione **Usar una conexión existente** y, a continuación, elija la conexión pertinente.
- Seleccione una zona en el campo **Nombre de la zona**. Las opciones son todas las ubicaciones de recursos que configuró.
- Seleccione un hipervisor o un servicio en la nube en el campo **Tipo de conexión**. Las opciones son hipervisores y servicios en la nube que tienen sus plug-ins instalados correctamente en la zona. Alternativamente, puede usar el comando de PowerShell `Get-HypHypervisorPlugin -ZoneUid` para obtener la lista de plug-ins de hipervisor disponibles con la zona seleccionada.

- Introduzca un nombre de conexión. Este nombre aparece en la pantalla de **Administrar**.
- Elija la herramienta para crear máquinas virtuales: Machine Creation Services o Citrix Provisioning.

La información de la página **Conexión** difiere según el host (tipo de conexión) que utilice. Por ejemplo, al usar Azure Resource Manager, puede usar una entidad de servicio existente o crear una.

Paso 2b: Administración del almacenamiento



Para obtener información sobre los tipos y métodos de administración del almacenamiento, consulte Almacenamiento de host.

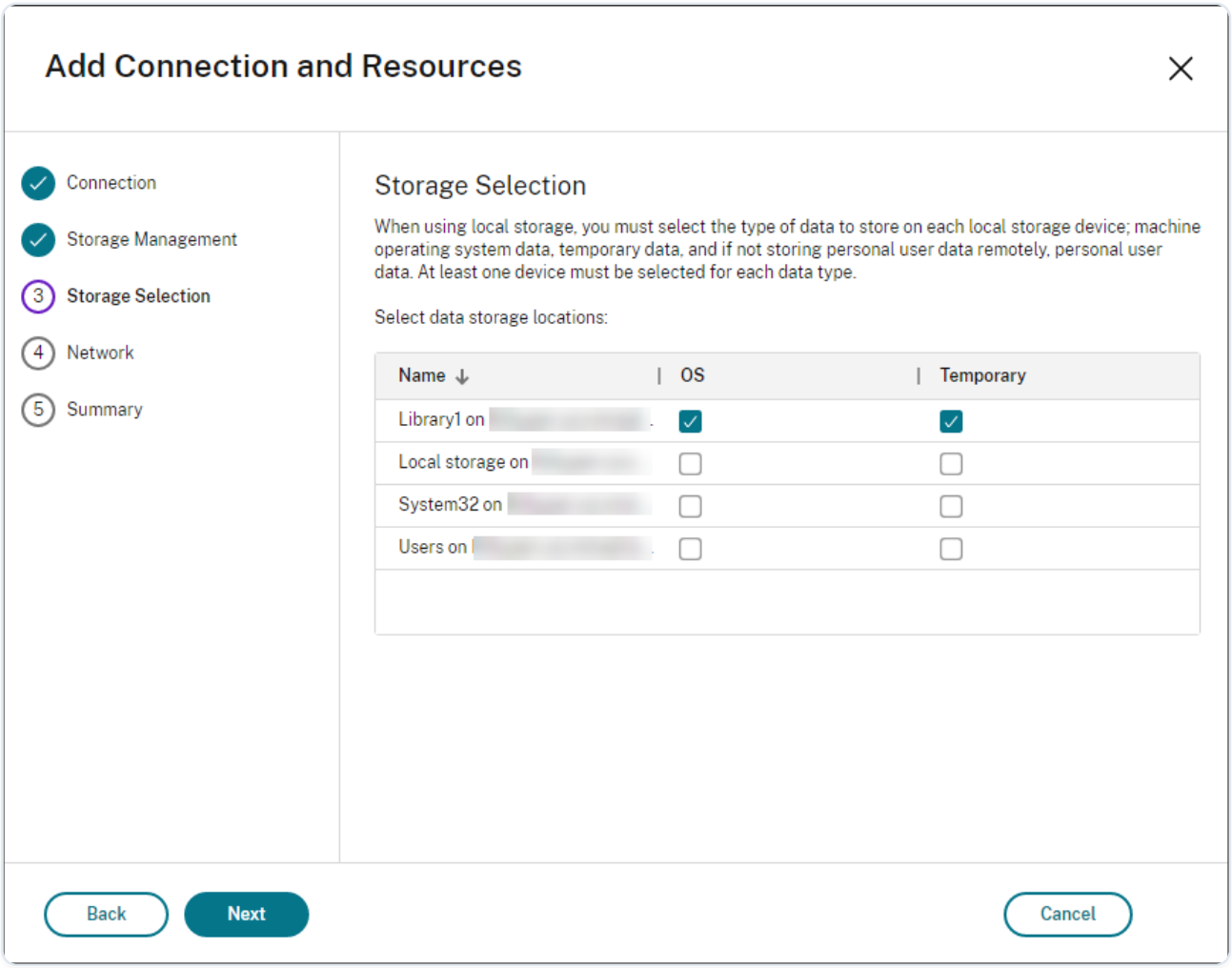
Si va a configurar una conexión a un host Hyper-V o VMware, busque y seleccione un nombre de clúster. Otros tipos de conexión no solicitan un nombre de clúster.

Seleccione un método de administración del almacenamiento: almacenamiento compartido por hipervisores o almacenamiento local del hipervisor.

- Si elige el almacenamiento compartido por hipervisores, indique si desea mantener los datos temporales en el almacenamiento local disponible. (Puede especificar tamaños de almacenamiento temporal no predeterminados en los catálogos de máquinas que utilizan esta conexión). **Excepción:** Al usar volúmenes compartidos de clúster (CSV), Microsoft System Center Virtual Machine Manager no permite crear discos de caché de datos temporales en el almacenamiento local. Los intentos de configurar esa configuración de administración de almacenamiento en la consola de **Administrar** fallan.

Si utiliza almacenamiento compartido en un grupo de Citrix Hypervisor, indique si desea usar IntelliCache para reducir la carga en el dispositivo de almacenamiento compartido. Consulte Entornos de virtualización de Citrix Hypervisor.

Paso 2c: Selección de almacenamiento



Para obtener más información sobre la selección del almacenamiento, consulte Almacenamiento de host.

Seleccione al menos un dispositivo de almacenamiento de host para cada tipo de datos disponible. El método de administración del almacenamiento que seleccionó en la página anterior afecta a los tipos de datos disponibles para la selección en esta página. Debe seleccionar al menos un dispositivo de almacenamiento para cada tipo de datos compatible antes de poder pasar a la siguiente página del asistente.

La parte inferior de la página **Selección de almacenamiento** contiene más opciones de configuración si eligió el almacenamiento compartido por hipervisores y habilitó **Optimizar datos temporales en el almacenamiento local disponible**. Puede seleccionar qué dispositivos de almacenamiento local (en el mismo grupo de hipervisores) usar para los datos temporales.

Se muestra el número de dispositivos de almacenamiento seleccionados actualmente (en el gráfico, "1 dispositivo de almacenamiento seleccionado"). Cuando pasa el ratón por encima de esa entrada, aparecen los nombres de los dispositivos seleccionados (a menos que no haya dispositivos configurados).

1. Seleccione **Seleccionar** para cambiar los dispositivos de almacenamiento que se van a usar.
2. En el cuadro de diálogo **Seleccionar almacenamiento**, marque o desmarque las casillas de verificación del dispositivo de almacenamiento y, a continuación, seleccione **Aceptar**.

Paso 2d: Región

(Aparece solo para algunos tipos de host). La selección de la región indica dónde se implementarán las VM. Lo ideal es elegir una región cercana a donde los usuarios acceden a sus aplicaciones.

Paso 2e: Red

Introduzca un nombre para los recursos. Este nombre aparece en la consola de **Administrar** para identificar la combinación de almacenamiento y red asociada a la conexión. Seleccione una o varias redes que utilicen las máquinas virtuales.

Algunos tipos de conexión (como Azure Resource Manager) también enumeran las subredes que utilizan las máquinas virtuales. Seleccione una o varias subredes.

Paso 2f: Resumen

Revise sus selecciones; si desea realizar cambios, vuelva a las páginas anteriores del asistente. Cuando termine la revisión, seleccione **Finalizar**.

Recuerde: Si almacena datos temporales localmente, puede configurar valores no predeterminados para el almacenamiento de datos temporales al crear el catálogo que contiene las máquinas que utilizan esta conexión.

> **Nota:**
>
> No se muestra un ámbito para los administradores con acceso total. Para obtener más información, consulte Administradores, roles y ámbitos.
>
> Para obtener más información, consulte Crear y administrar conexiones.

Paso 3: Preparar una imagen maestra

> **Sugerencia:**
>
> Puede usar una sola imagen para crear VDA unidos a un dominio y VDA no unidos a un dominio.

(Solo para XenServer (anteriormente Citrix Hypervisor™)) Paso 3a: Instalar las herramientas de máquina virtual de XenServer

Instale las herramientas de máquina virtual de XenServer en la máquina virtual de plantilla para que cada máquina virtual utilice la CLI de xe o XenCenter. El rendimiento de la máquina virtual puede ser lento si no instala las herramientas. Sin las herramientas, no puede hacer lo siguiente:

- Apagar, reiniciar o suspender una máquina virtual de forma limpia.
- Ver los datos de rendimiento de la máquina virtual en XenCenter.
- Migrar una máquina virtual en ejecución (a través de `XenMotion`).
- Crear instantáneas o instantáneas con memoria (puntos de control), y revertir a instantáneas.
- Ajustar el número de vCPU en una máquina virtual Linux en ejecución.

1. Descargue el archivo XenServer VM Tools para Linux desde la página de descargas de XenServer o la página de descargas de Citrix Hypervisor según la versión del hipervisor en uso.
2. Copie el archivo `LinuxGuestTools-xxx.tar.gz` en su VM Linux o en una unidad compartida a la que pueda acceder la VM Linux.

3. Extraiga el contenido del archivo tar: `tar -xzf LinuxGuestTools-xxx.tar.gz`
4. Ejecute el siguiente comando para instalar el paquete `xe-guest-utilities` según su distribución de Linux.

   Para RHEL/CentOS/Rocky Linux/SUSE:

   ```
   sudo rpm -i <extract-directory>/xe-guest-utilities_{package-version}
   _x86.64.rpm
   ```

   Para Ubuntu/Debian:

   ```
   sudo dpkg -i <extract-directory>/xe-guest-utilities_{package-version}
   _amd64.deb
   ```

5. Compruebe el estado de virtualización de la VM de plantilla en la ficha **General** de XenCenter. Si las XenServer® VM Tools están instaladas correctamente, el estado de virtualización muestra **Optimizado**.

Paso 3b: Instale .NET y el paquete VDA de Linux en la VM de plantilla

> **Nota:**
>
> Para usar un VDA en ejecución como VM de plantilla, omita este paso.
>
> Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Después de instalar .NET, ejecute los siguientes comandos según su distribución de Linux para instalar el VDA de Linux:

Para RHEL/CentOS/Rocky Linux:

```
sudo yum –y localinstall <PATH>/<Linux VDA RPM>
```

> **Nota:**

Después de instalar el VDA de Linux en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, es posible que se pierda la conexión Ethernet y que el VDA de Linux sea inaccesible después de reiniciar una VM. Para solucionar el problema, ejecute los siguientes comandos antes de reiniciar la VM:

```
nmcli dev connect eth0

systemctl restart NetworkManager
```

Para Ubuntu/Debian:

```
sudo dpkg –i  <PATH>/<Linux VDA DEB>



apt-get install -f
```

Para SUSE:

```
sudo zypper –i install <PATH>/<Linux VDA RPM>
```

Paso 3c: (Solo para RHEL) Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en `<https://docs.fedoraproject.org/es-es/epel/>`.

Paso 3d: (Solo para SUSE) Instale ntfs-3g manualmente

En la plataforma SUSE, ningún repositorio proporciona ntfs-3g. Descargue el código fuente, compile e instale ntfs-3g manualmente:

1. Instale el sistema de compiladores GNU Compiler Collection (GCC) y el paquete **make**:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Descargue el paquete ntfs-3g.
3. Descomprima el paquete ntfs-3g:

```
sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
```

4. Introduzca la ruta al paquete ntfs-3g:

```
sudo cd ntfs-3g_ntfsprogs-<package version>
```

5. Instale ntfs-3g:

```
./configure

make

make install
```

Paso 3e: (Solo para Ubuntu) Edite el archivo /etc/network/interfaces

Agregue la línea `source /etc/network/interfaces.d/*` al archivo `/etc/network/interfaces`.

> **Sugerencia:**

> Es posible que el archivo `/etc/network/interfaces` no esté disponible en su máquina Ubuntu. Si el archivo no existe, primero debe instalar los paquetes **net-tools** e **ifupdown**.

Paso 3f: (Solo para Ubuntu) Apunte /etc/resolv.conf

Apunte `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf` en lugar de apuntarlo a `/run/systemd/resolve/stub-resolv.conf`:

```
unlink /etc/resolv.conf



ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

Paso 3g: Especificar una base de datos para usar

Puede alternar entre SQLite y PostgreSQL después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

Nota:

- Recomendamos usar SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el Linux VDA utiliza PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio de PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).
- También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh` . Omita este paso si es una instalación nueva.
2. Edite `/etc/xdl/db.conf` antes de ejecutar `deploymcs.sh` . El siguiente es un ejemplo de archivo **db.conf**:

```
# database configuration file for Linux VDA



## database choice

# possible choices are:

#     SQLite

#     PostgreSQL
```

```
# default choice is PostgreSQL

DbType="PostgreSQL"




## database port

# specify database port for the database.

# if not specified, default port will be used:

# SQLite: N/A

# PostgreSQL: 5432

DbPort=5432




## PostgreSQL customized

# only the following value means true, otherwise false:

#     true

#     yes

#     y

#     YES

#     Y

# default is false

DbCustomizePostgreSQL=false
```

```
## PostgreSQL service name

# specify the service name of PostgreSQL for Linux VDA

# default is "postgresql"

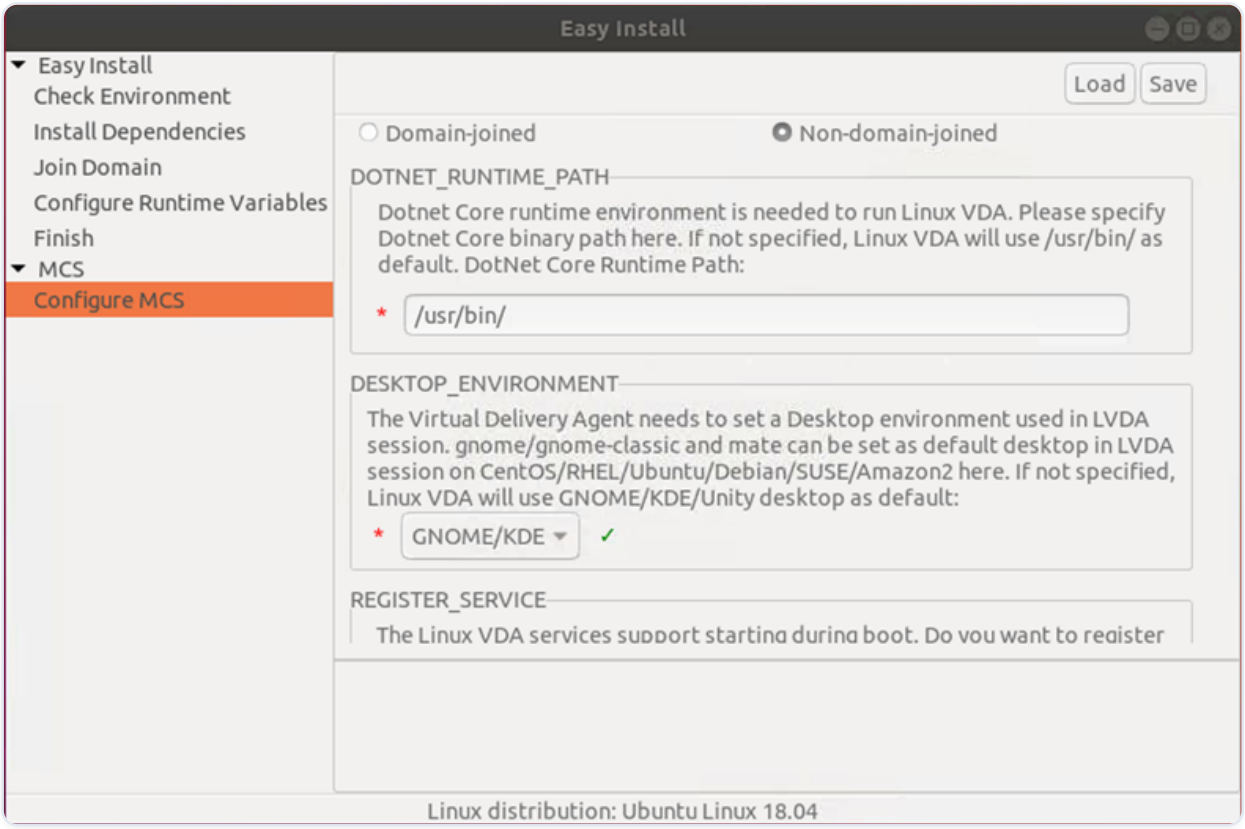
DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

Paso 3h: Configurar variables de MCS

Hay dos maneras de configurar las variables de MCS:

- Edite el archivo `/etc/xdl/mcs/mcs.conf`.
- Use la GUI de instalación sencilla. Para abrir la GUI de instalación sencilla, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su Linux VDA.



Sugerencia:

> Haga clic en **Guardar** para guardar la configuración de las variables en un archivo local en la ruta que especifique. Haga clic en **Cargar** para cargar la configuración de las variables desde un archivo que especifique.

Las siguientes son variables de MCS que puede configurar para escenarios sin unión a un dominio. Puede usar los valores predeterminados de las variables o personalizarlas según sea necesario (opcional):

`DOTNET_RUNTIME_PATH`=path-to-install-dotnet-runtime

`DESKTOP_ENVIRONMENT`=gnome | mate `REGISTER_SERVICE`=S | N

`ADD_FIREWALL_RULES`=S | N `VDI_MODE`=S | N

`START_SERVICE`=S | N

(Opcional) Paso 3i: Escribir o actualizar valores del registro para MCS

En la máquina de plantilla, agregue líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar los valores del registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina aprovisionada por MCS.

Cada línea del archivo `/etc/xdl/mcs/mcs_local_setting.reg` es un comando para establecer o actualizar un valor del registro.

Por ejemplo, puede agregar las siguientes líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar un valor del registro, respectivamente:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -v "Flags" -d "0x00000003"
```

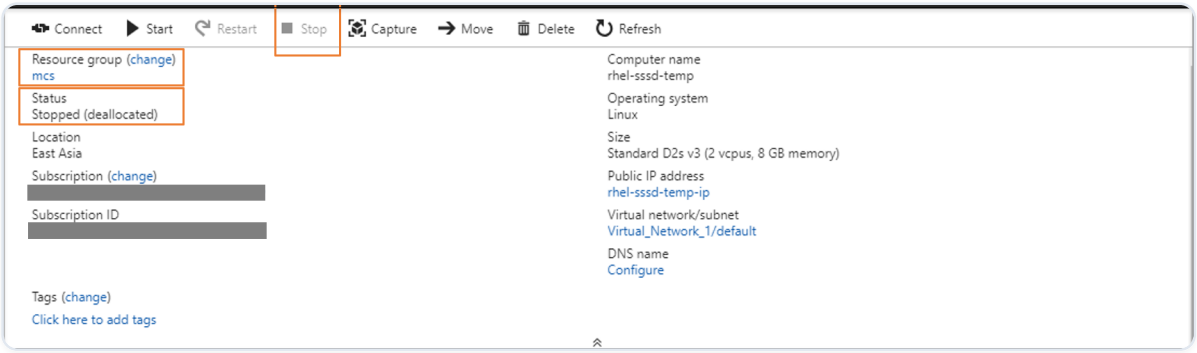
Paso 3j: Crear una imagen maestra

1. Si configura las variables de MCS editando `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura las variables de MCS mediante la GUI, haga

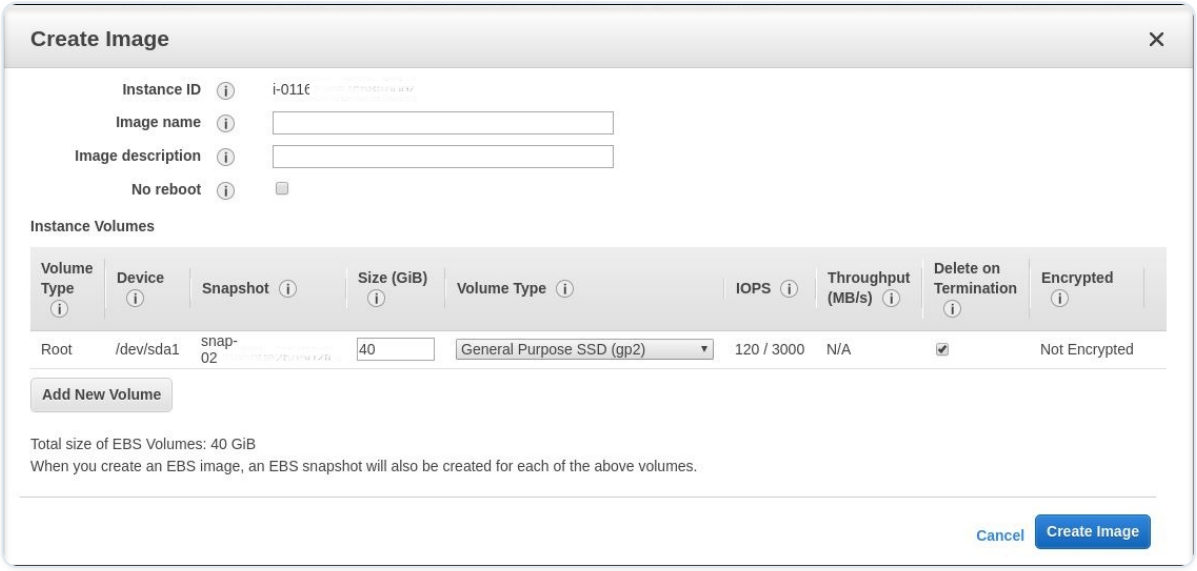
clic en **Implementar**. Después de hacer clic en **Implementar** en la GUI, las variables que configure en la GUI anularán las variables que configuró en el archivo `/etc/xdl/mcs/mcs.conf`.

2. Cree y asigne un nombre a una instantánea de su imagen maestra según la nube pública que utilice.

   - **(Para XenServer (anteriormente Citrix Hypervisor), GCP y VMware vSphere)** Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla. Cree y asigne un nombre a una instantánea de su imagen maestra.
   - **(Para Azure)** Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de Azure. Asegúrese de que el estado de energía de la VM de plantilla muestre **Detenida (desasignada)**. Recuerde aquí el nombre del grupo de recursos. Necesitará el nombre para localizar su imagen maestra en Azure.



   - **(Para AWS)** Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de AWS EC2. Asegúrese de que el estado de la instancia de la VM de plantilla muestre **Detenida**. Haga clic con el botón derecho en la VM de plantilla y seleccione **Imagen > Crear imagen**. Escriba la información y realice los ajustes necesarios. Haga clic en **Crear imagen**.



- **(Para Nutanix)** En Nutanix AHV, apague la VM de plantilla. Cree y asigne un nombre a una instantánea de su imagen maestra.

  > **Nota:**
  >
  > Debe prefijar los nombres de las instantáneas de Acropolis con `XD_` para usarlos en Citrix Virtual Apps and Desktops. Utilice la consola de Acropolis para cambiar el nombre de sus instantáneas cuando sea necesario. Después de cambiar el nombre de una instantánea, reinicie el asistente **Crear catálogo** para obtener una lista actualizada.

Paso 4a: Crear un catálogo de máquinas en DaaS

1. Inicie sesión en Citrix Cloud.
2. En el menú superior izquierdo, seleccione **Mis servicios > DaaS**.
3. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.
4. El asistente le guía para crear un catálogo de máquinas.

   En la página **Contenedor**, que es exclusiva de Nutanix, seleccione el contenedor que especificó anteriormente para la VM de plantilla.

   En la página **Imagen maestra**, seleccione la instantánea de la imagen.

   En la página **Máquinas virtuales**, compruebe el número de vCPU y el número de núcleos por vCPU. Seleccione MCS como método de implementación de máquinas y seleccione **No unido a un dominio** como identidad para las máquinas que se crearán en el catálogo.

   Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear catálogos de máquinas.

> **Nota:**
>
> Para instancias de AWS Workspace Core, consulte Crear un catálogo de instancias administradas de Amazon WorkSpaces Core

> Si el proceso de creación del catálogo de máquinas en el Delivery Controller™ tarda mucho tiempo, vaya a Nutanix Prism y encienda manualmente la máquina con el prefijo **Preparation**. Este enfoque ayuda a continuar el proceso de creación.

Paso 4b: Crear un catálogo de máquinas en CVAD

Puede crear un catálogo de máquinas no unidas a un dominio en CVAD a través de Web Studio o PowerShell; para obtener más detalles, consulte identidad de máquina no unida a un dominio

Paso 5: Crear un grupo de entrega

Un grupo de entrega es una colección de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica qué usuarios pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios. Para obtener más información, consulte Crear grupos de entrega en DaaS o Crear grupos de entrega en CVAD.

Crear un VDA de Linux no unido a un dominio mediante la instalación fácil

Este artículo le guía a través del método de instalación fácil para crear e inscribir un VDA de Linux no unido a un dominio con un catálogo de máquinas en Citrix DaaS o Citrix Virtual Apps and Desktops™ 2407 y versiones posteriores.

> **Importante:**

- Para clientes de Citrix DaaS™:
  - Puede implementar VDA no unidos a un dominio en una nube pública o en el centro de datos local. Los VDA no unidos a un dominio son administrados por el plano de control en Citrix DaaS.
  - Para crear VDA no unidos a un dominio, los clientes que utilizan el servicio Citrix Gateway deben asegurarse de que Rendezvous V2 esté habilitado. Los Cloud Connectors solo son necesarios si planea aprovisionar máquinas en hipervisores locales o si desea utilizar Active Directory como proveedor de identidades en Workspace.
- Para crear VDA no unidos a un dominio, también puede usar MCS. Para obtener más información, consulte Crear VDA de Linux no unidos a un dominio mediante MCS.

    - MCS no admite servidores bare metal.

- Las siguientes funciones están disponibles para los VDA de Linux no unidos a un dominio:

    - Crear usuarios locales con atributos especificados en VDA no unidos a un dominio
    - Autenticación sin SSO
    - Autenticación con Azure Active Directory
    - Rendezvous V2

Paso 1: Crear un catálogo de máquinas vacío

Inicie sesión en Citrix Web Studio™ y cree un catálogo de máquinas vacío sin máquinas. El VDA de Linux no admite el uso de un archivo de token para inscribirse en un catálogo de máquinas administrado por energía.

El proceso para crear catálogos de máquinas y agregar máquinas VDA de Linux es similar al enfoque tradicional de VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Para crear catálogos de máquinas que contengan máquinas VDA de Linux, existen algunas restricciones que diferencian el proceso de la creación de catálogos de máquinas para máquinas VDA de Windows:

- Para el sistema operativo, seleccione:

    - La opción **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
    - La opción **SO de sesión única** para un modelo de entrega de escritorios dedicados VDI.

- No mezcle máquinas VDA de Linux y Windows en el mismo catálogo de máquinas.
- No mezcle máquinas unidas a un dominio y máquinas no unidas a un dominio en el mismo catálogo de máquinas.
- Para crear un catálogo de máquinas de inscripción de tokens, elija **SO de sesión única** o **SO multisesión** en la página **Tipo de máquina**, y elija **“Máquinas sin administración de energía (por ejemplo, máquinas físicas)”** en la página **Administración de máquinas**.

Nota:

> Las versiones anteriores de Citrix Studio no admiten la noción de un "SO Linux". Sin embargo, seleccionar la opción **SO de Windows Server** o **SO de servidor** implica un modelo de entrega de escritorios compartidos alojados equivalente. Seleccionar la opción **SO de escritorio de Windows** o **SO de escritorio** implica un modelo de entrega de un solo usuario por máquina.

Paso 2: Crear un token de inscripción

Para crear un VDA no unido a un dominio mediante la instalación sencilla, necesita un archivo de token para inscribir el VDA en un catálogo de máquinas y autenticar el VDA en el controlador de entrega en la nube o local. El VDA de Linux no admite el uso de un archivo de token para la inscripción en un catálogo de máquinas con administración de energía.

Para crear un token de inscripción, complete los siguientes pasos en Citrix Web Studio:

> **Sugerencia:**

> En Citrix DaaS, Web Studio se conoce como Configuración completa.

1. Seleccione el catálogo de máquinas vacío que creó anteriormente y, a continuación, seleccione **Administrar tokens de inscripción** en la barra de acciones.
2. En la página **Administrar tokens de inscripción**, haga clic en **Generar** para crear un token de inscripción. También puede elegir un token existente que esté en un estado válido.
3. Siga el asistente para completar la configuración.
4. Descargue el token creado correctamente y guárdelo con el menor privilegio en una ubicación segura. Más tarde, cuando ejecute el script de instalación fácil, la variable CTX_XDL_NDJ_ENROLLMENT_TOKEN_FILE le permite especificar la ruta al archivo de token para inscribir el VDA.

Paso 3: Instalar .NET

Antes de instalar el VDA de Linux, instale .NET (/es-es/linux-virtual-delivery-agent/2507-ltsr/system-requirements.html#net-requirements) según los requisitos del sistema.

Después de instalar .NET, ejecute el comando **which dotnet** para encontrar la ruta de su tiempo de ejecución.

Según la salida del comando, establezca la ruta binaria del tiempo de ejecución de .NET. Por ejemplo, si la salida del comando es /aa/bb/dotnet, use /aa/bb como la ruta binaria de .NET.

Paso 4: Añadir certificados de CA autofirmados

Para obtener detalles sobre la configuración de certificados de CA autofirmados, consulte (/es-es/linux-virtual-delivery-agent/2507-ltsr/best-practices/configure-self-signed-certificates-for-websocket.html). Esta sección implica colocar y actualizar certificados de CA en el VDA de Linux.

- Para RHEL y Rocky Linux:

  Guarde sus certificados de CA autofirmados en el directorio **/etc/pki/ca-trust/source/anchors** en el VDA de Linux y, a continuación, ejecute el siguiente comando para actualizar los certificados:

  ```
  sudo update-ca-trust
  ```

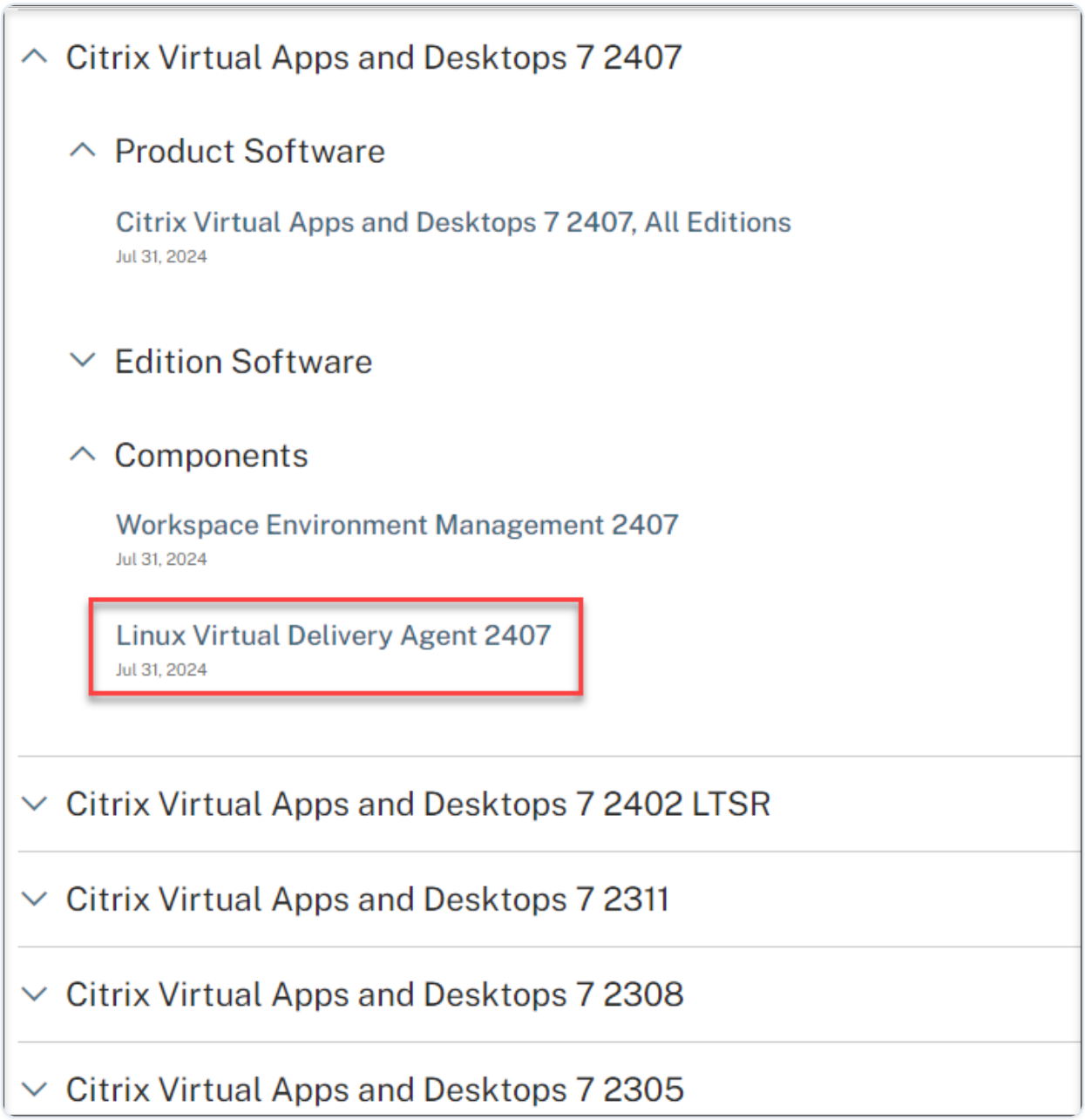
- Para SUSE, Ubuntu y Debian:

  Coloque el certificado de CA raíz en el directorio **/usr/local/share/ca-certificates**. Luego, ejecute el comando **update-ca-certificate**.

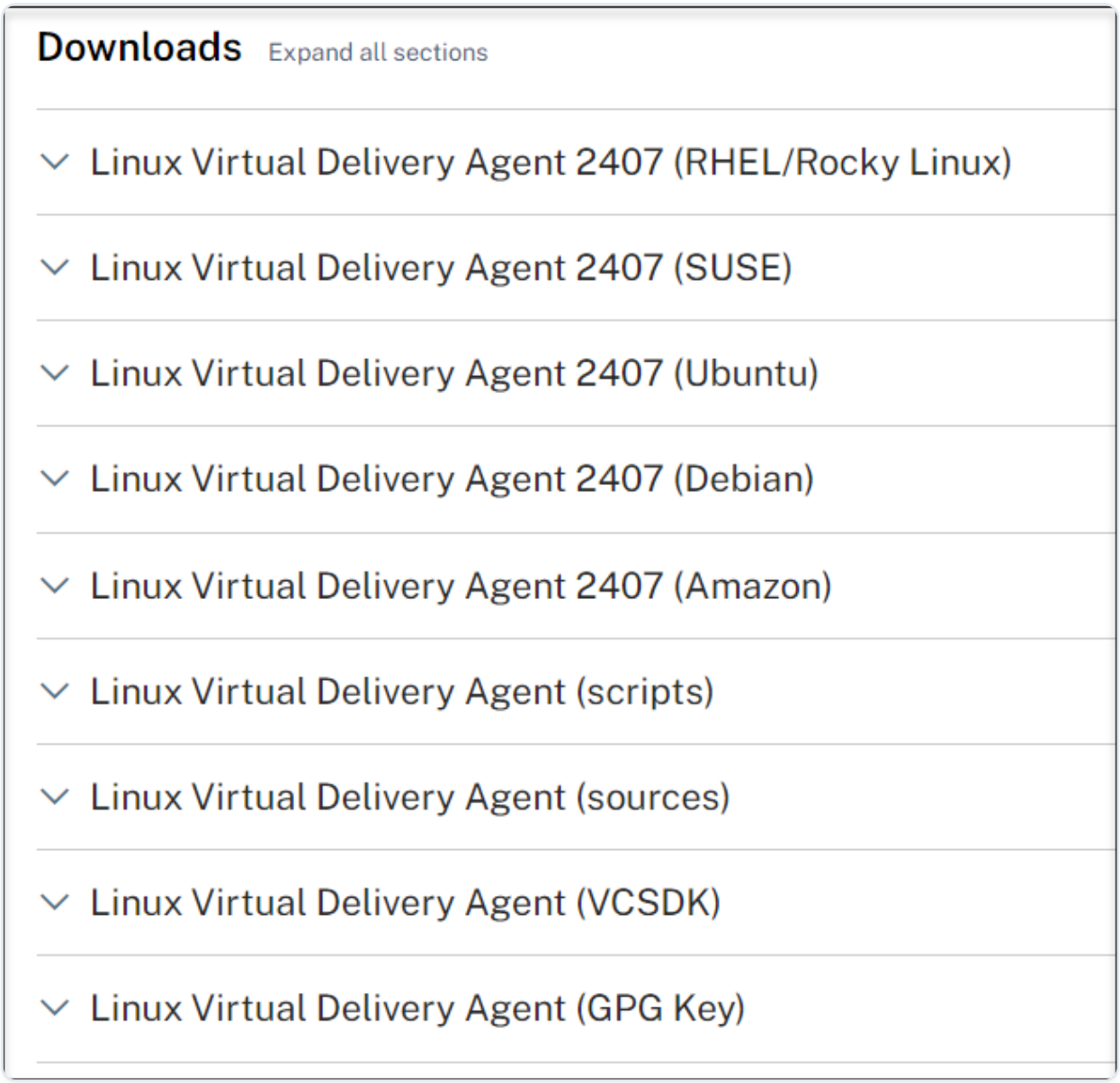
  ```
  sudo update-ca-certificates
  ```

Paso 5: Descargar el paquete del VDA de Linux

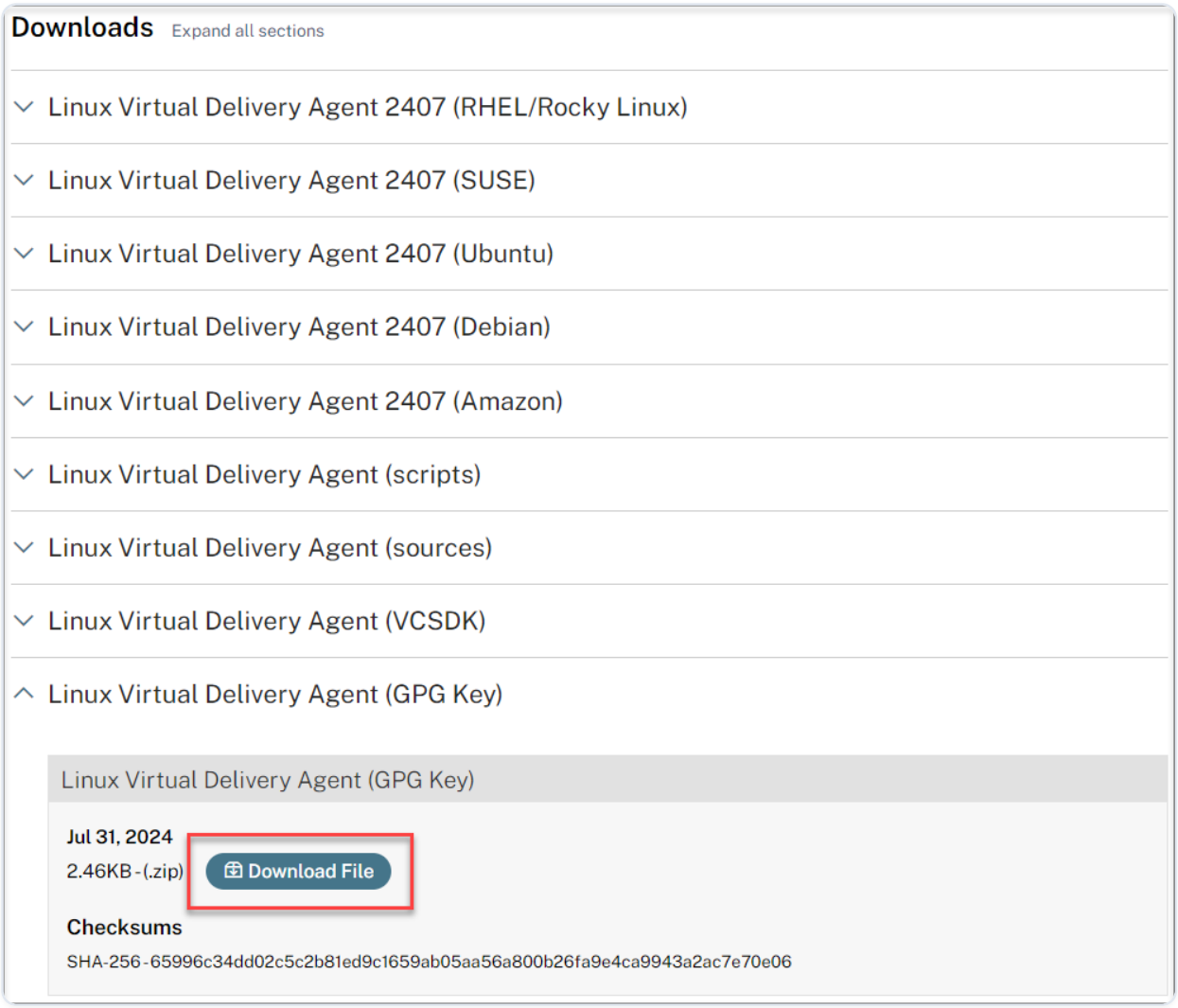
1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps™ and Desktops.
3. Expanda **Componentes** para encontrar el VDA de Linux. Por ejemplo:



4. Haga clic en el enlace de Linux VDA para acceder a las descargas de Linux VDA.



5. Descargue el paquete de Linux VDA que coincida con su distribución de Linux.
6. Descargue la clave pública GPG que puede usar para verificar la integridad del paquete de Linux VDA. Por ejemplo:



Para verificar la integridad del paquete de Linux VDA mediante la clave pública:

- Para un paquete RPM, ejecute los siguientes comandos para importar la clave pública en la base de datos RPM y comprobar la integridad del paquete:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

- Para un paquete DEB, ejecute los siguientes comandos para importar la clave pública en la base de datos DEB y comprobar la integridad del paquete:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Paso 6: Instalar el paquete de Linux VDA

Para configurar el entorno para el Linux VDA, ejecute los siguientes comandos.

Para distribuciones RHEL y Rocky Linux:

Nota:

- Para RHEL y CentOS, instale el repositorio EPEL antes de poder instalar el Linux VDA correctamente. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en `<https://docs.fedoraproject.org/es-es/epel/>`.
- Antes de instalar el Linux VDA en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.

```
sudo yum  -y localinstall   <PATH>/<Linux VDA RPM>
```

Nota:

Después de instalar el Linux VDA en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojado en GCP, la conexión Ethernet podría perderse y el Linux VDA podría quedar inaccesible después de un reinicio de la VM. Para solucionar el problema, establezca una contraseña de root al iniciar sesión en la VM por primera vez y asegúrese de poder iniciar sesión en la VM como root. Luego, ejecute los siguientes comandos en la consola después de reiniciar la VM:

```
nmcli dev connect eth0

systemctl restart NetworkManager
```

Para distribuciones Ubuntu/Debian:

```
sudo dpkg -i <PATH>/<Linux VDA deb>

sudo apt-get install -f
```

Nota:

- Para instalar las dependencias necesarias para una distribución Debian 11, agregue la línea `deb http://deb.debian.org/debian/ bullseye main` al archivo /etc/apt/sources.list.
- Para Ubuntu 24.04/22.04 en GCP, deshabilite RDNS. Para ello, agregue la línea **rdns = false** debajo de en /etc/krb5.conf.

Para distribuciones SUSE:

1. Para SUSE 15.6 en AWS, Azure y GCP, asegúrese de que:
   - Está utilizando **libstdc++6** versión 12 o posterior.
   - El parámetro **Default_WM** en **/etc/sysconfig/windowmanager** esté establecido en **"gnome"**.
2. Ejecute el siguiente comando para instalar el VDA de Linux:

   ```
   zypper -i install <PATH>/<Linux VDA RPM>
   ```

Paso 7: Instalar los controladores NVIDIA GRID

La habilitación de HDX™ 3D Pro requiere que instale los controladores NVIDIA GRID en su hipervisor y en la máquina VDA.

Para instalar y configurar NVIDIA GRID Virtual GPU Manager (el controlador de host) en los hipervisores específicos, consulte las siguientes guías:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Para instalar y configurar los controladores de VM invitada de NVIDIA GRID, realice los siguientes pasos generales:

1. Asegúrese de que la VM invitada esté apagada.
2. En el panel de control del hipervisor, asigne una GPU a la VM.
3. Inicie la VM.

4. Instale el controlador de la VM invitada (de su proveedor de la nube o NVIDIA) en la VM.

Paso 8: Especifique una base de datos para usar

Puede especificar SQLite o PostgreSQL para usar editando **/etc/xdl/db.conf** después de instalar el paquete Linux VDA.

Para ello, edite **/etc/xdl/db.conf** antes de ejecutar **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** o **/opt/Citrix/VDA/bin/easyinstall**.

> **Nota:**
>
> - Le recomendamos que use SQLite solo para el modo VDI.
> - Para la instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el Linux VDA usa PostgreSQL de forma predeterminada.
> - También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

Paso 9: Ejecute el script de instalación sencilla para configurar el entorno y el VDA para completar la instalación

Después de instalar el paquete Linux VDA, configure el entorno de ejecución mediante el script ctxinstall.sh.

> **Nota:**
>
> Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional **en_US.UTF-8** esté instalada en su sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando **sudo locale-gen en_US.UTF-8**. Para Debian, edite el archivo **/etc/locale.gen** descomentando la línea **# en_US.UTF-8 UTF-8** y, a continuación, ejecute el comando **sudo locale-gen**.

ctxinstall.sh

ctxinstall.sh es el script de instalación sencilla para realizar algunas configuraciones previas y establecer las variables de entorno de ejecución del VDA.

- Solo el usuario root puede ejecutar este script.
- Easy install utiliza /opt/Citrix/VDA/sbin/ctxinstall.conf como su archivo de configuración para establecer, guardar y sincronizar los valores de todas las variables de entorno utilizadas. Le recomendamos que lea la plantilla (ctxinstall.conf.tmpl) detenidamente y luego personalice su propio ctxinstall.conf. Cuando cree el archivo de configuración por primera vez, utilice cualquiera de las siguientes formas:
  - Copiando el archivo de plantilla /opt/Citrix/VDA/sbin/ctxinstall.conf.tmpl y guardándolo como /opt/Citrix/VDA/sbin/ctxinstall.conf.
  - Ejecutando ctxinstall.sh. Cada vez que ejecuta ctxinstall.sh, su entrada se guarda en /opt/Citrix/VDA/sbin/ctxinstall.conf.
- Easy install admite la ejecución modular. Los módulos incluyen comprobación previa, instalación, configuración de dominio, configuración y verificación.
- Los detalles de depuración de este script se pueden encontrar en /var/log/xdl/ctxinstall.log.

Para obtener más información, utilice el comando de ayuda **ctxinstall.sh -h**.

Nota:

- Siguiendo el principio de privilegio mínimo, asegúrese de que solo el usuario root pueda leer **/opt/Citrix/VDA/sbin/ctxinstall.conf** porque la contraseña de unión al dominio podría establecerse en el archivo.
- La desinstalación del Linux VDA elimina los archivos en **/opt/Citrix/VDA**. Le recomendamos que haga una copia de seguridad de **/opt/Citrix/VDA/sbin/ctxinstall.conf** antes de desinstalar el VDA.

Puede ejecutar ctxinstall.sh en modo interactivo o en modo silencioso. Antes de ejecutar el script, establezca las siguientes variables de entorno:

- **CTX_XDL_NON_DOMAIN_JOINED='y\|n'** – Si se debe unir la máquina a un dominio. El valor predeterminado es 'n'. Para escenarios sin unión a dominio, establézcalo en 'y'.
- **CTX_XDL_NDJ_ENROLLMENT_TOKEN_FILE='<path-to-token-file-on-vda-machine\>'** – Para crear un VDA sin unión a dominio mediante easy install, necesita un archivo de token para inscribir el VDA en un catálogo de máquinas del Delivery Controller. Guarde el token con el mínimo privilegio en una ubicación segura.

- **CTX_XDL_VDI_MODE='y\|n'** – Si se debe configurar la máquina como un modelo de entrega de escritorio dedicado (VDI) o un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca el valor en 'y'.
- **CTX_XDL_HDX_3D_PRO='y\|n'** – El Linux VDA admite HDX 3D Pro, un conjunto de tecnologías de aceleración de GPU diseñadas para optimizar la virtualización de aplicaciones con gráficos enriquecidos. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única), es decir, CTX_XDL_VDI_MODE='y'.
- **CTX_XDL_START_SERVICE='y\|n'** – Determina si los servicios de Linux VDA se inician cuando se completa la configuración.
- **CTX_XDL_REGISTER_SERVICE='y\|n'** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES='y\|n'** – Los servicios de Linux VDA requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema para el escritorio virtual de Linux.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate** – Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se utilizará en las sesiones. Si deja la variable sin especificar, se utiliza el escritorio predeterminado configurado en el VDA.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/kde/mate/xfce/'<none\>'** – Especifica el entorno de escritorio GNOME, GNOME Classic, KDE, MATE o Xfce que se utilizará en las sesiones. Si lo establece en '<none\>', se utiliza el escritorio predeterminado configurado en el VDA. Puede especificar un entorno de escritorio para usar en las sesiones mediante la variable CTX_XDL_DESKTOP_ENVIRONMENT. También puede cambiar entre entornos de escritorio ejecutando comandos o usando la bandeja del sistema. Para obtener más información, consulte Comandos para cambiar de escritorio y Bandeja del sistema.
- **CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime\>'** – La ruta para instalar .NET para admitir el nuevo servicio de agente de intermediación (**ctxvda**). La ruta predeterminada es '/usr/bin'.
- **CTX_XDL_VDA_PORT='<port-number\>'** – El Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP.

Modo interactivo

Para ejecutar el script **ctxinstall.sh** en modo interactivo, utilice el comando **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** sin la opción **-S**. Escriba el valor de la variable correspondiente en cada

solicitud de la interfaz de línea de comandos. Si una variable ya está establecida, **ctxinstall.sh** le pedirá confirmación en caso de que desee cambiarla.

Modo silencioso

En modo silencioso, debe establecer las variables anteriores utilizando **/opt/Citrix/VDA/sbin/ctxinstall.conf** o el comando export. Después, ejecute **ctxinstall.sh -S** (tenga en cuenta que la letra **S** aquí está en **mayúsculas**). Si no se establecen todas las variables requeridas o algún valor no es válido, **ctxinstall.sh** aborta la ejecución, a menos que haya valores predeterminados.

Si lo establece, el valor exportado para cada variable sobrescribe el valor en **/Citrix/VDA/sbin/ctxinstall.conf**. Todos los valores actualizados se guardan en **/Citrix/VDA/sbin/ctxinstall.conf**.

```
export CTX_XDL_NON_DOMAIN_JOINED='y'

export CTX_XDL_NDJ_ENROLLMENT_TOKEN_FILE='<token-file-path>'

export CTX_XDL_VDI_MODE='y|n'

export CTX_XDL_START_SERVICE='y|n'

export CTX_XDL_REGISTER_SERVICE='y|n'

export CTX_XDL_ADD_FIREWALL_RULES='y|n'

export CTX_XDL_HDX_3D_PRO='y|n'

export CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|
xfce|'<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'

export CTX_XDL_VDA_PORT='<port-number>'

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh -S
```

Al ejecutar el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que crea. Recomendamos que cree un archivo de script de shell a partir de los comandos anteriores con **#\!/bin/bash** como primera línea.

Alternativamente, puede especificar todas las variables utilizando un solo comando.

Para configurar las variables de entorno de ejecución del VDA (aquellas variables que comienzan con '**CTX_XDL_**'), puede ejecutar **ctxinstall.sh -s** (tenga en cuenta que la letra **s** aquí está en **minúsculas**).

Paso 10: Ejecute XDPing

Ejecute `sudo /opt/Citrix/VDA/bin/xdping` para comprobar si hay problemas de configuración comunes en un entorno de Linux VDA. Para obtener más información, consulte **XDPing**.

Paso 11: Ejecutar el VDA de Linux

Iniciar el VDA de Linux:

Para iniciar los servicios del VDA de Linux:

```
sudo systemctl start ctxhdx.service



sudo systemctl start ctxvda.service
```

Detener el VDA de Linux:

Para detener los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda.service



sudo systemctl stop ctxhdx.service
```

> **Nota:**

> Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que detuvo.

> **Reiniciar el VDA de Linux:**

Para reiniciar los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda.service



sudo systemctl restart ctxhdx.service



sudo systemctl start ctxvda.service
```

Comprobar el estado del VDA de Linux:

Para comprobar el estado de ejecución de los servicios del VDA de Linux:

```
sudo systemctl status ctxvda.service



sudo systemctl status ctxhdx.service
```

Paso 12: Crear grupos de entrega

El proceso para crear un grupo de entrega y añadir catálogos de máquinas que contengan máquinas VDA de Linux es casi idéntico al de las máquinas VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear grupos de entrega.

Para crear grupos de entrega que contengan catálogos de máquinas VDA de Linux, se aplican las siguientes restricciones:

- Asegúrese de que los usuarios y grupos de AD que seleccione se hayan configurado correctamente para iniciar sesión en las máquinas VDA de Linux.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No mezcle el grupo de entrega con catálogos de máquinas que contengan máquinas Windows.

Importante:

> La publicación de aplicaciones es compatible con Linux VDA versión 1.4 y posteriores. Sin embargo, el Linux VDA no admite la entrega de escritorios y aplicaciones a la misma máquina.

> Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2503.

Paso 13: Habilitar la asignación de cuentas locales

¿Qué ocurre si la asignación de cuentas locales no está habilitada?

Las sesiones alojadas en VDA no unidos a un dominio fallan al iniciar sesión, mostrando un mensaje de contraseña pero sin aceptar la contraseña correcta. Se pueden encontrar errores similares a los siguientes en el `hdx.log`:

```
2024-09-25 06:40:30.767979 [LOGIN_BOX:ERROR] <P124211:T58675:S4> citrix-
ctxlogin: PamAuthenticate: pam authentication: Authentication failure. Can
retry for user 'user3'

2024-09-25 06:40:30.768431 [LOGIN:ERROR] <P124211:T58675:S4> citrix-
ctxlogin: LoginBoxValidate: Failed to validate user 'user3'. Due to
INVALID_PASSWORD

2024-09-25 06:40:30.768947 [LOGIN_AUTH:INFO] <P124218:T58682:S4> citrix-
ctxloginui: CalLabelFormat: Update username label on LoginUI from 'user3'
to 'user3' (18)

2024-09-25 06:41:18.766196 [GFX_SLIDER:ERROR] <P124161:T58699:S4> citrix-
ctxgfx: GfxCreateSliderListener: Failed to get user home dir.
```

Habilitar la asignación de cuentas locales

Para asegurarse de que los usuarios puedan iniciar sesión en un Linux VDA no unido a un dominio, habilite la asignación de cuentas locales mediante el siguiente comando:

```
Set-BrokerDesktopGroup -Name "<your delivery group name>"
-MachineLogOnType LocalMappedAccount
```

Para una implementación local, ejecute el comando directamente en el Delivery Controller. Para una implementación de Citrix DaaS, ejecute el comando a través del SDK de PowerShell remoto de Citrix Virtual Apps y Desktops.

Crear VDA de Linux con Machine Creation Services™ (MCS)

Puede crear VDA unidos a un dominio y no unidos a un dominio mediante MCS. Si quiere crear VDA de Linux no unidos a un dominio en Citrix DaaS, también puede consultar el artículo específico Crear VDA de Linux no unidos a un dominio mediante MCS.

> **Importante:**
>
> Los siguientes son cambios importantes a partir de la versión 2212:
>
> - La variable **AD_INTEGRATION** del archivo /etc/xdl/mcs/mcs.conf o de la GUI de instalación sencilla ya no tiene un valor predeterminado. Debe establecer un valor según sea necesario. Para obtener más información, consulte la sección Paso 3i: Configurar variables de MCS de este artículo.
> - El valor válido de la entrada **UPDATE_MACHINE_PW** en /etc/xdl/mcs/mcs.conf ya no es **enabled** o **disabled**, sino **Y** o **N**. Para obtener más información, consulte la sección Automatizar las actualizaciones de contraseñas de cuentas de máquina de este artículo.

Distribuciones admitidas

	WINBIND	SSSD	CENTRIFY	PBIS
Debian 12.15/11.11	Sí	Sí	No	Sí
RHEL 9.8/9.6/9.4	Sí	Sí	Sí	No
RHEL 8.10	Sí	Sí	Sí	Sí
Rocky Linux 9.8/9.6/9.4	Sí	Sí	Sí	No

	WINBIND	SSSD	CENTRIFY	PBIS
Rocky Linux 8.10	Sí	Sí	Sí	No
SUSE 15.6	Sí	Sí	No	Sí
Ubuntu 24.04	Sí	Sí	No	Sí
Ubuntu 22.04	Sí	Sí	No	Sí

- Citrix® utiliza las siguientes versiones de Centrify para la validación inicial de funciones en las distribuciones de Linux relevantes:

DISTRIBUCIÓN DE LINUX	VERSIÓN DE CENTRIFY
RHEL 7/8	5.8.0
SUSE	5.7.1
Debian, Ubuntu	5.6.1

  El uso de otras versiones de Centrify podría causar errores. No utilice Centrify para unir una máquina de plantilla a un dominio.

- Si utiliza PBIS o Centrify para unir máquinas creadas con MCS a dominios de Windows, complete las siguientes tareas:

  - En la máquina de plantilla, configure la ruta de descarga del paquete PBIS o Centrify en el archivo `/etc/xdl/mcs/mcs.conf` o instale el paquete PBIS o Centrify directamente.
  - Antes de ejecutar `/opt/Citrix/VDA/sbin/deploymcs.sh`, cree una Unidad Organizativa (OU) que tenga permisos de escritura y de restablecimiento de contraseña para todas sus máquinas subordinadas creadas por MCS.
  - Antes de reiniciar las máquinas creadas por MCS después de que `/opt/Citrix/VDA/sbin/deploymcs.sh` termine de ejecutarse, ejecute `klist -li 0x3e4 purge` en su Delivery Controller o en su Citrix Cloud Connector, según su implementación.

- Para usar una VDA de RHEL 8.x/9.x o Rocky Linux 8.x/9.x que se esté ejecutando actualmente y que esté conectada al dominio mediante SSSD como VM de plantilla para MCS, asegúrese de que:

- La VDA se instala manualmente y no mediante la instalación sencilla. La instalación sencilla utiliza **Adcli** para RHEL 8.x/9.x y Rocky Linux 8.x/9.x, y MCS no admite la combinación de SSSD y **Adcli**.
- Un servidor Samba está configurado para usar SSSD para la autenticación de AD. Para obtener más información, consulte el artículo de Red Hat en `<https://access.redhat.com/solutions/3802321>`.

Hipervisores compatibles

- AWS
- XenServer (anteriormente Citrix Hypervisor™)
- GCP
- Microsoft Azure
- Nutanix AHV
- VMware vSphere

Pueden producirse resultados inesperados si intenta preparar una imagen maestra en hipervisores distintos de los compatibles.

Usar MCS para crear máquinas virtuales Linux

Consideraciones

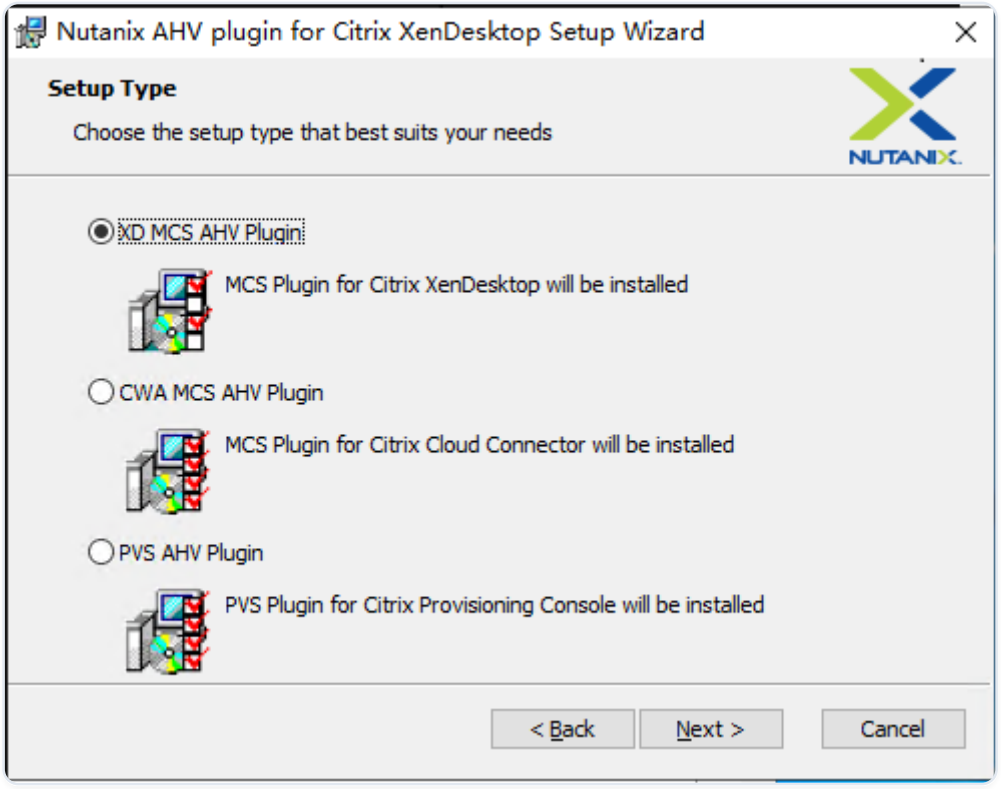
- A partir de la versión 2203, puede alojar el VDA de Linux en Microsoft Azure, AWS y GCP para Citrix Virtual Apps and Desktops™ y Citrix DaaS (anteriormente servicio Citrix Virtual Apps and Desktops). Para agregar estas conexiones de host de nube pública a su implementación de Citrix Virtual Apps and Desktops, necesita la licencia Citrix Universal Hybrid Multi-Cloud (HMC).
- Los servidores bare metal no son compatibles para su uso con MCS para crear máquinas virtuales.

(Solo para Nutanix) Paso 1: Instalar y registrar el plug-in de Nutanix AHV

Obtenga el paquete del plug-in de Nutanix AHV de Nutanix. Instale y registre el plug-in en su entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte la guía de instalación del plug-in de Nutanix Acropolis MCS, disponible en el Portal de soporte de Nutanix.

Paso 1a: Instalar y registrar el plug-in de Nutanix AHV para Delivery Controllers locales

Después de instalar Citrix Virtual Apps™ and Desktops, seleccione e instale el **XD MCS AHV Plugin** en sus Delivery Controllers.



Paso 1b: Instale y registre el complemento de Nutanix AHV para los Delivery Controllers en la nube

Seleccione e instale el **CWA MCS AHV Plugin** para los Citrix Cloud™ Connectors. Instale el complemento en todos los Citrix Cloud Connectors registrados con el inquilino de Citrix Cloud. Debe registrar los Citrix Cloud Connectors incluso si dan servicio a una ubicación de recursos sin AHV.

Paso 1c: Complete los siguientes pasos después de instalar el complemento

- verificar que se haya creado una carpeta de Nutanix Acropolis en `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.
- Ejecute el comando `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`.
- Reinicie los servicios Citrix Host, Citrix Broker y Citrix Machine Creation Services en sus Delivery Controllers locales o reinicie el servicio Citrix RemoteHCLServer en los Citrix Cloud Connectors.

> **Sugerencia:**
>
> Recomendamos que detenga y luego reinicie los servicios Citrix Host, Citrix Broker y Machine Creation Services al instalar o actualizar el complemento de Nutanix AHV.

Paso 2: Crear una conexión de host

Esta sección ofrece ejemplos sobre cómo crear una conexión de host a Azure, AWS, XenServer® (anteriormente Citrix Hypervisor), GCP, Nutanix AHV y VMware vSphere.

> **Nota:**
>
> Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.

> Para obtener más información, consulte Crear y administrar conexiones y recursos en la documentación de Citrix Virtual Apps and Desktops y Crear y administrar conexiones en la documentación de Citrix DaaS.

- Crear una conexión de host a Azure en Citrix Studio
- Crear una conexión de host a AWS en Citrix Studio
- Crear una conexión de host a XenServer en Citrix Studio
- Crear una conexión de host a GCP en Citrix Studio
- Crear una conexión de host a Nutanix en Citrix Studio
- Crear una conexión de host a VMware en Citrix Studio

Crear una conexión de host a Azure en Citrix Studio

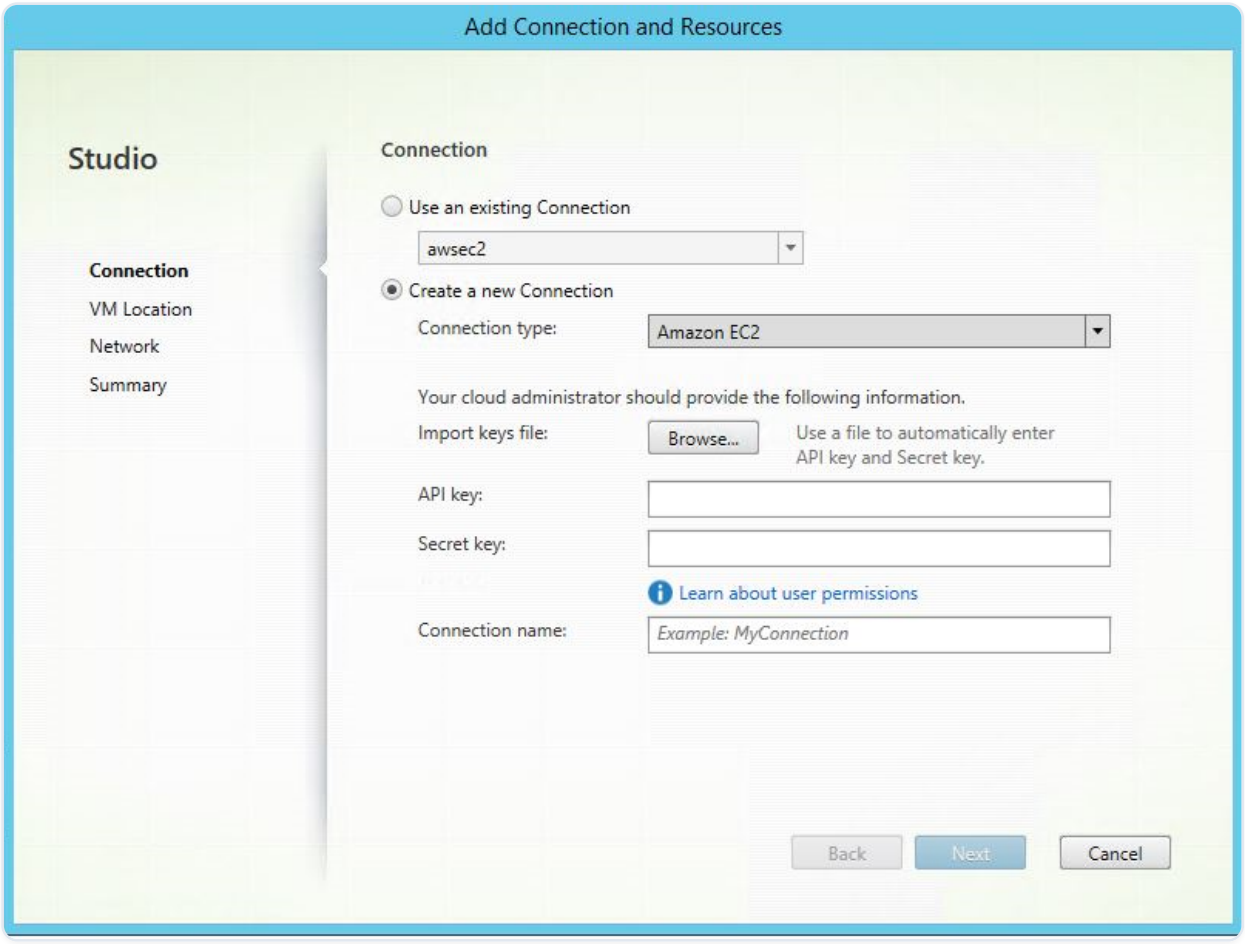
1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.

2. En el asistente **Agregar conexión y recursos**, seleccione Microsoft Azure como tipo de conexión.
3. Seleccione Microsoft Azure como tipo de conexión.
4. El asistente le guía por las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte el **Paso 2: Crear una conexión de host** en el artículo Crear VDA de Linux no unidos a un dominio con MCS.

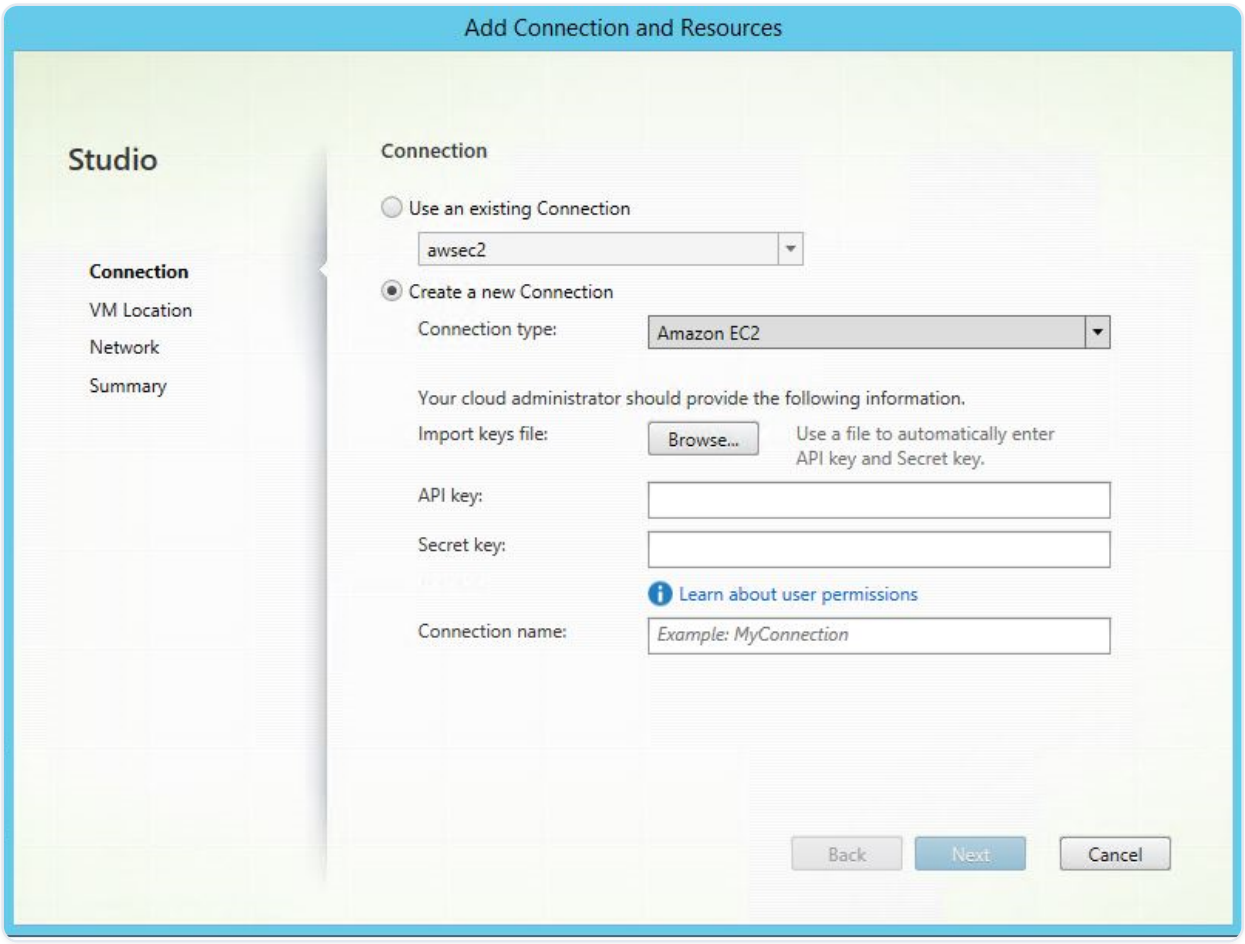
Crear una conexión de host a AWS en Citrix Studio

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione **Amazon EC2** como tipo de conexión.

   Por ejemplo, en Citrix Studio local:



3. Escriba la clave de API y la clave secreta de su cuenta de AWS y escriba el nombre de su conexión.



La **clave de API** es su ID de clave de acceso y la **clave secreta** es su clave de acceso secreta. Se consideran un par de claves de acceso. Si pierde su clave de acceso secreta, puede eliminar la clave de acceso y crear otra. Para crear una clave de acceso, haga lo siguiente:

a. Inicie sesión en los servicios de AWS.

b. Vaya a la consola de Identity and Access Management (IAM). 1 En el panel de navegación izquierdo, elija **Usuarios**.

c. Seleccione el usuario de destino y desplácese hacia abajo para seleccionar la ficha **Credenciales de seguridad**.

d. Desplácese hacia abajo y haga clic en **Crear clave de acceso**. Aparecerá una nueva ventana.

e. Haga clic en **Descargar archivo .csv** y guarde la clave de acceso en una ubicación segura.

4. El asistente le guiará por las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**.

Crear una conexión de host a XenServer en Citrix Studio

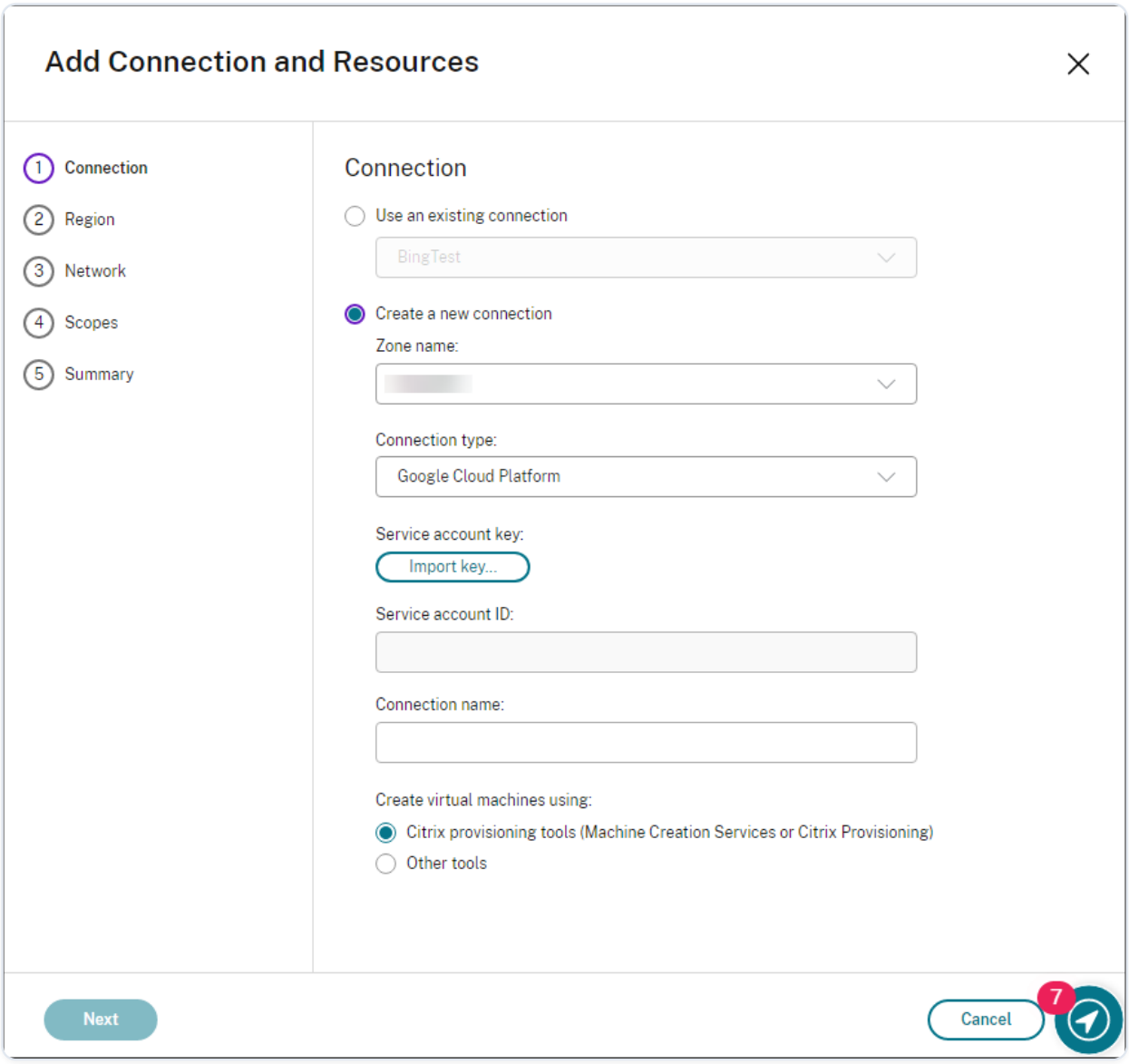
1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione XenServer (anteriormente Citrix Hypervisor) en el campo **Tipo de conexión**.
3. Escriba la dirección de conexión (la URL de XenServer) y las credenciales.
4. Introduzca un nombre de conexión.

Crear una conexión de host a GCP en Citrix Studio

Configure su entorno de GCP según Entornos de virtualización de Google Cloud Platform y, a continuación, complete los siguientes pasos para crear una conexión de host a GCP.

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione **Google Cloud Platform** como tipo de conexión.

   Por ejemplo, en la consola de Studio basada en web en Citrix Cloud:



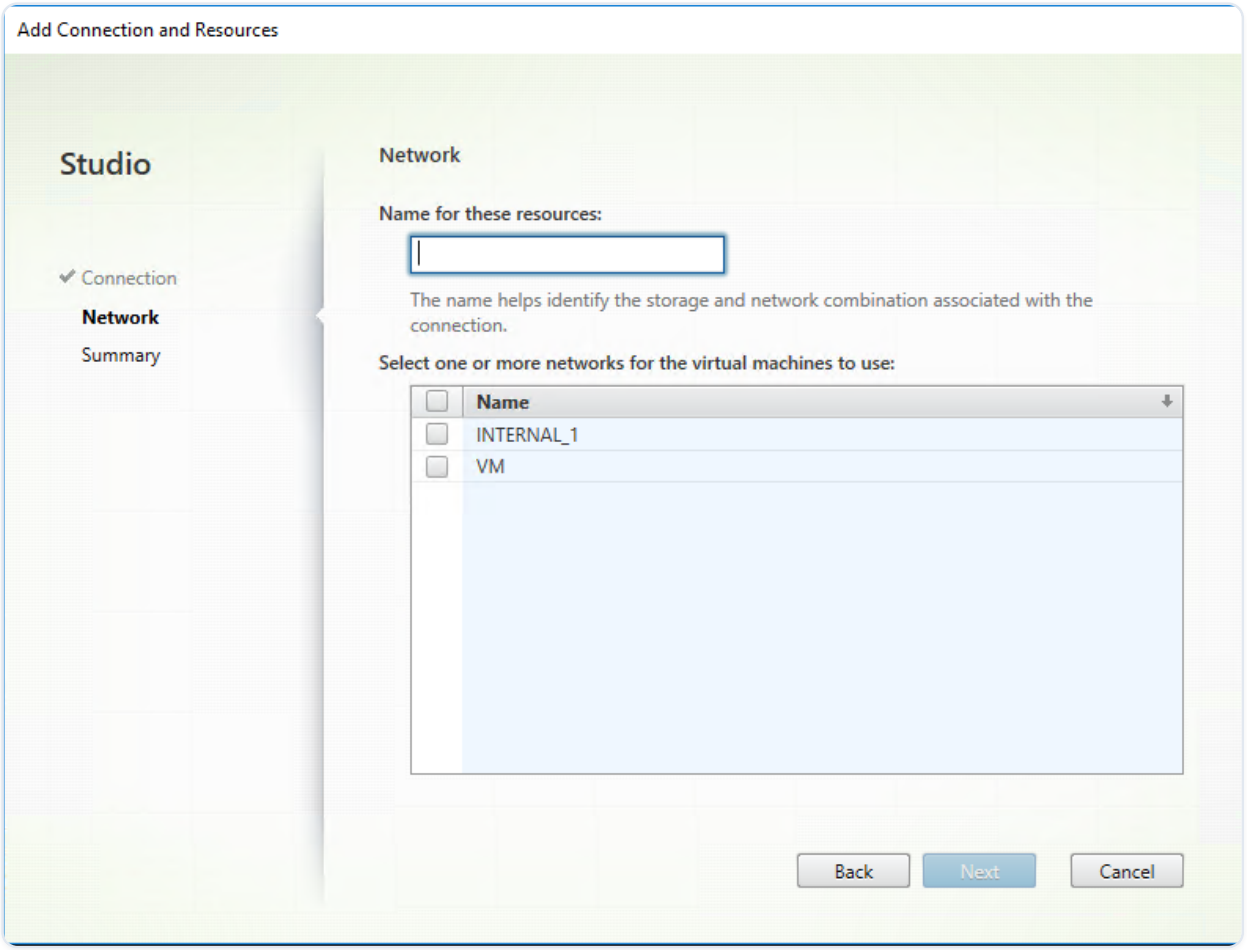
3. Importe la clave de la cuenta de servicio de su cuenta de GCP y escriba el nombre de su conexión.
4. El asistente le guía a través de las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte el **Paso 2: Crear una conexión de host** en el artículo Crear VDA de Linux no unidos a un dominio mediante MCS.

Crear una conexión de host a Nutanix en Citrix Studio

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.

2. En el asistente **Agregar conexión y recursos**, seleccione Nutanix AHV como tipo de conexión en la página **Conexión** y, a continuación, especifique la dirección del hipervisor, las credenciales y el nombre de la conexión. En la página **Red**, seleccione una red para la unidad.

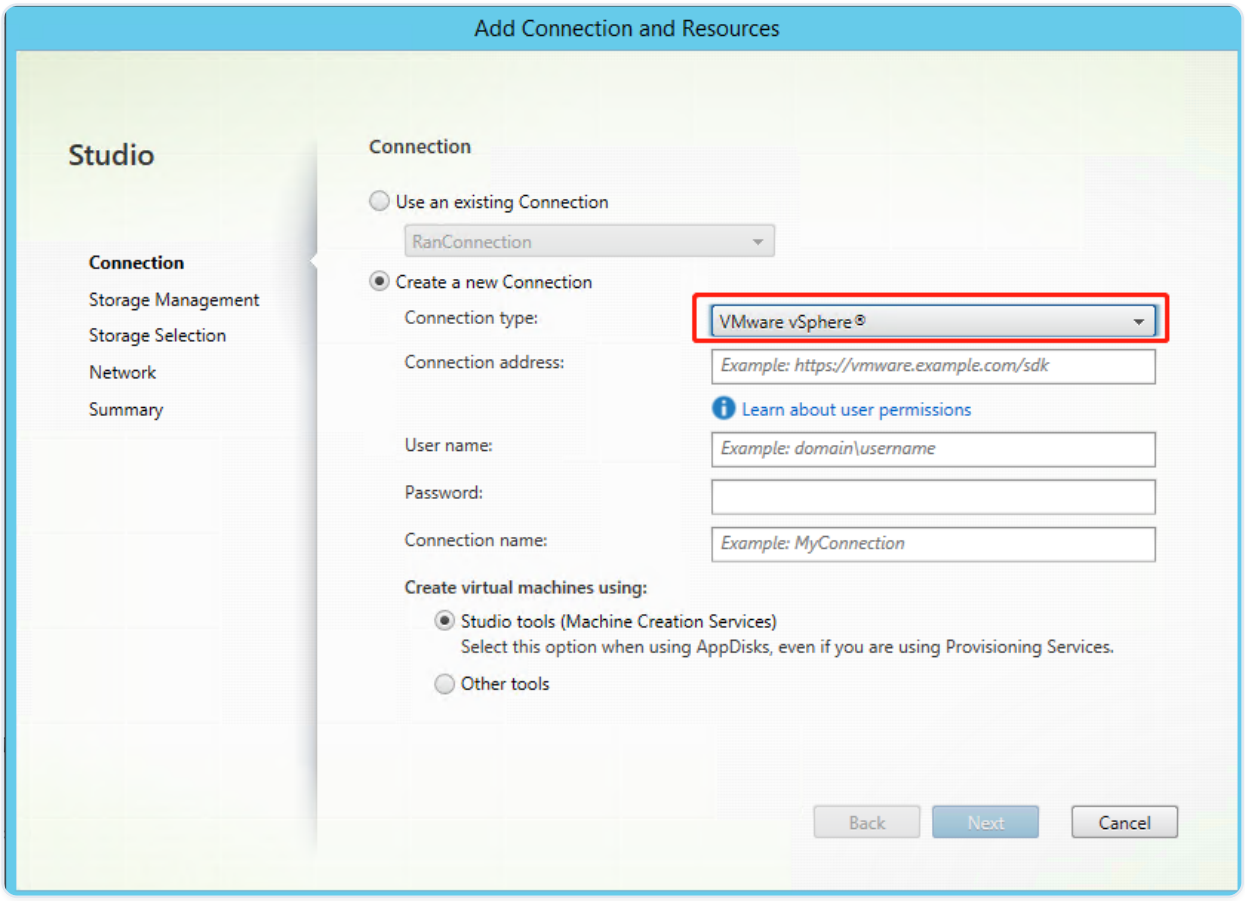
   Por ejemplo, en Citrix Studio local:



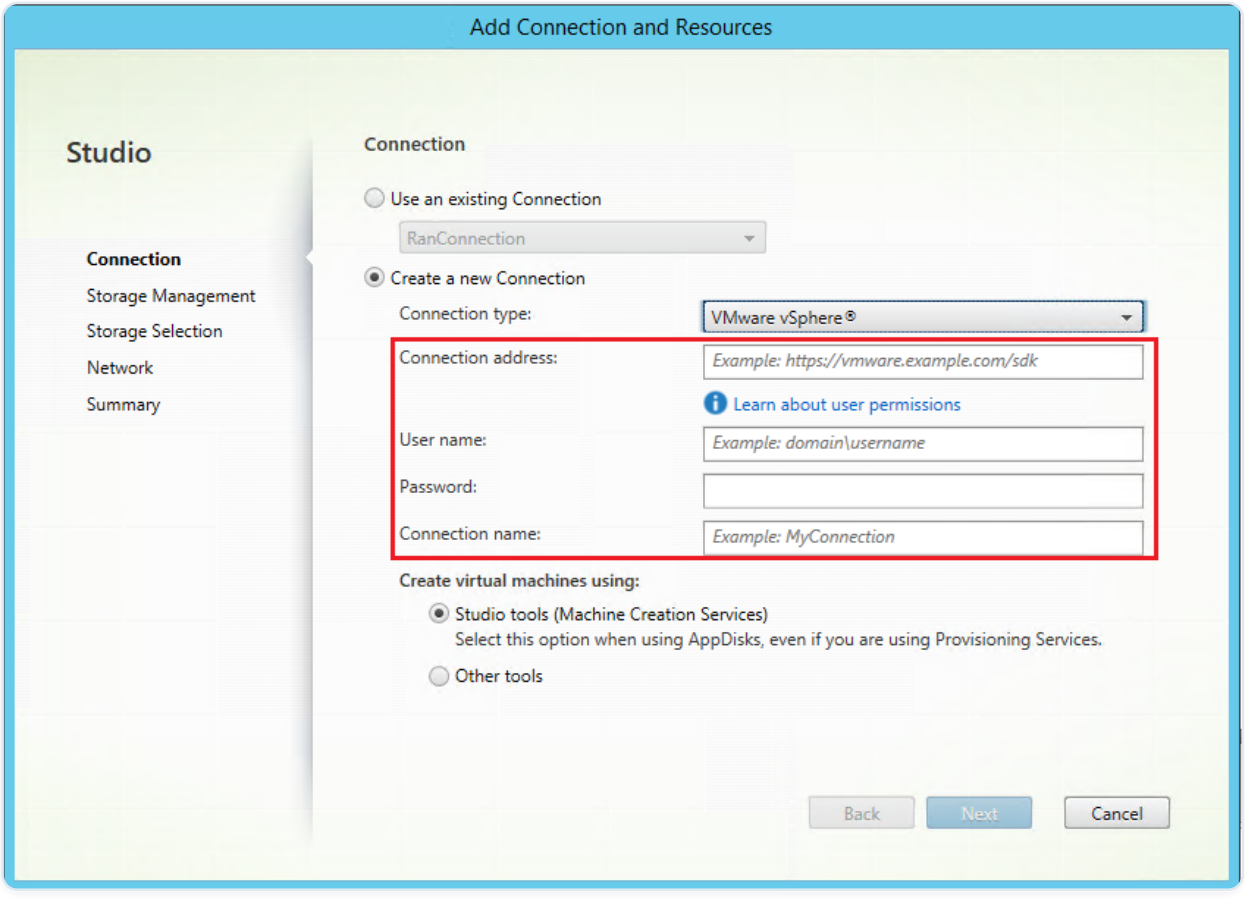
Crear una conexión de host a VMware en Citrix Studio

1. Instale vCenter Server en el entorno de vSphere. Para obtener más información, consulte VMware vSphere.
2. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
3. Elija VMware vSphere como tipo de conexión.

   Por ejemplo, en Citrix Studio local:



4. Escriba la dirección de conexión (la URL de vCenter Server) de su cuenta de VMware, sus credenciales y el nombre de su conexión.



Paso 3: Preparar una imagen maestra

(Solo para XenServer) Paso 3a: Instalar XenServer VM Tools

Instale XenServer VM Tools en la VM de plantilla para que cada VM utilice la CLI xe o XenCenter. El rendimiento de la VM puede ser lento si no instala las herramientas. Sin las herramientas, no puede hacer lo siguiente:

- Apagar correctamente, reiniciar o suspender una VM.
- Ver los datos de rendimiento de la VM en XenCenter.
- Migrar una VM en ejecución (a través de `XenMotion`).
- Crear instantáneas o instantáneas con memoria (puntos de control), y revertir a instantáneas.
- Ajustar el número de vCPU en una VM Linux en ejecución.

1. Descargue el archivo XenServer VM Tools para Linux desde la página de descargas de XenServer o la página de descargas de Citrix Hypervisor según la versión del hipervisor en uso.
2. Copie el archivo `LinuxGuestTools-xxx.tar.gz` a su VM Linux o a una unidad compartida a la que la VM Linux pueda acceder.
3. Extraiga el contenido del archivo tar: `tar -xzf LinuxGuestTools-xxx.tar.gz`
4. Ejecute el siguiente comando para instalar el paquete `xe-guest-utilities` según su distribución de Linux.

   Para RHEL/CentOS/Rocky Linux/SUSE:

   ```
   sudo rpm -i <extract-directory>/xe-guest-utilities_{package-version}
   _x86.64.rpm
   ```

   Para Ubuntu/Debian:

   ```
   sudo dpkg -i <extract-directory>/xe-guest-utilities_{package-version}
   _amd64.deb
   ```

5. Compruebe el estado de virtualización de la VM de plantilla en la pestaña **General** de XenCenter. Si XenServer VM Tools se instalan correctamente, el estado de virtualización muestra **Optimizado**.

Paso 3b: verificar las configuraciones para SUSE 15.6 en AWS, Azure y GCP

Para SUSE 15.6 en AWS, Azure y GCP, asegúrese de que:

- Está utilizando **libstdc++6** versión 12 o posterior.
- El parámetro **Default_WM** en **/etc/sysconfig/windowmanager** está establecido en **"gnome"**.

Paso 3c: Deshabilitar RDNS para Ubuntu 20.04 en GCP

En la VM de plantilla, añada la línea **rdns = false** debajo de en /etc/krb5.conf.

Paso 3d: Instalar .NET en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso. Para usar un VDA de RHEL 8.x/9.x o Rocky Linux 8.x/9.x en ejecución que esté conectado al dominio mediante SSSD como VM de plantilla, asegúrese de que:

> - El VDA se instala manualmente y no mediante la instalación fácil. La instalación fácil utiliza **Adcli** para RHEL 8.x/9.x y Rocky Linux 8.x/9.x, y la combinación de SSSD y **Adcli** no es compatible con MCS.
> - Un servidor Samba está configurado para usar SSSD para la autenticación de AD. Para obtener más información, consulte el artículo de Red Hat en `<https://access.redhat.com/solutions/3802321>`.

> Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Paso 3e: Instalar el paquete VDA de Linux en la VM de plantilla

Después de instalar .NET, ejecute los siguientes comandos según su distribución de Linux para instalar el VDA de Linux:

Para RHEL/CentOS/Rocky Linux:

> **Nota:**

> Antes de instalar el VDA de Linux en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.

```
sudo yum –y localinstall <PATH>/<Linux VDA RPM>
```

Para Ubuntu/Debian:

```
sudo dpkg –i  <PATH>/<Linux VDA DEB>



apt-get install -f
```

Para SUSE:

```
sudo zypper –i install <PATH>/<Linux VDA RPM>
```

Paso 3f: (Solo para RHEL) Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en `<https://docs.fedoraproject.org/es-es/epel/>`.

Paso 3g: (Solo para SUSE) Instale ntfs-3g manualmente

En la plataforma SUSE, ningún repositorio proporciona ntfs-3g. Descargue el código fuente, compile e instale ntfs-3g manualmente:

1. Instale el sistema de compiladores GNU Compiler Collection (GCC) y el paquete make:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Descargue el paquete ntfs-3g.
3. Descomprima el paquete ntfs-3g:

   ```
   sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
   ```

4. Introduzca la ruta al paquete ntfs-3g:

   ```
   sudo cd ntfs-3g_ntfsprogs-<package version>
   ```

5. Instale ntfs-3g:

```
./configure

make

make install
```

Paso 3h: Especifique una base de datos que usar

Puede alternar entre SQLite y PostgreSQL después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

Nota:

- Le recomendamos que use SQLite solo para el modo VDI y que use PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el Linux VDA usa PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio de PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).
- También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.
2. Edite `/etc/xdl/db.conf` antes de ejecutar `deploymcs.sh`. El siguiente es un ejemplo del archivo **db.conf**:

```
# database configuration file for Linux VDA
```

```
## database choice

# possible choices are:

#     SQLite

#     PostgreSQL

# default choice is PostgreSQL

DbType="PostgreSQL"




## database port

# specify database port for the database.

# if not specified, default port will be used:

# SQLite: N/A

# PostgreSQL: 5432

DbPort=5432




## PostgreSQL customized

# only the following value means true, otherwise false:

#     true

#     yes

#     y

#     YES
```

```
#     Y

# default is false

DbCustomizePostgreSQL=false



## PostgreSQL service name

# specify the service name of PostgreSQL for Linux VDA

# default is "postgresql"

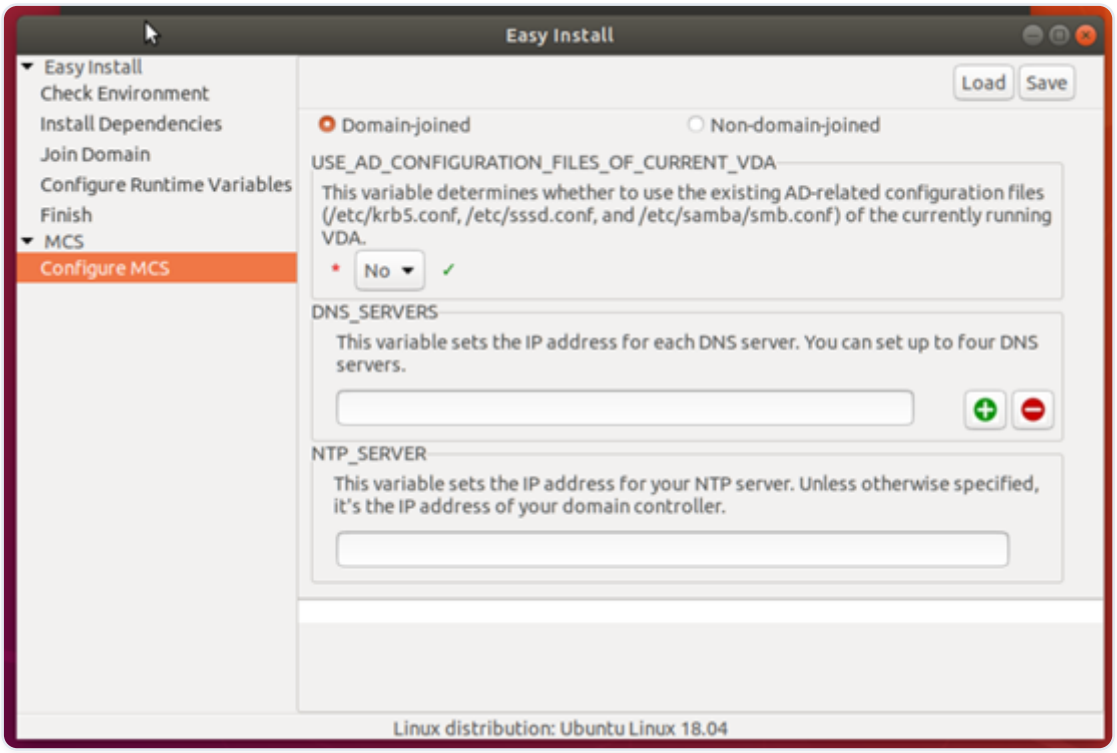
DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

Paso 3i: Configurar variables de MCS

Hay dos maneras de configurar las variables de MCS:

- Edite el archivo `/etc/xdl/mcs/mcs.conf`.
- Utilice la GUI de instalación fácil. Para abrir la GUI de instalación fácil, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su VDA de Linux.



> **Sugerencia:**
>
> Haga clic en **Guardar** para guardar la configuración de las variables en un archivo local en la ruta que especifique. Haga clic en **Cargar** para cargar la configuración de las variables desde un archivo que especifique.

Las siguientes son variables de MCS que puede configurar para escenarios sin unión a dominio y con unión a dominio:

- **Para escenarios sin unión a dominio**

  Puede usar los valores predeterminados de las variables o personalizarlas según sea necesario (opcional):

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-dotnet-runtime

  `DESKTOP_ENVIRONMENT`=gnome | mate `REGISTER_SERVICE`=Y | N

  `ADD_FIREWALL_RULES`=Y | N `VDI_MODE`=Y | N

  `START_SERVICE`=Y | N

- **Para escenarios con unión a dominio**

- `Use_AD_Configuration_Files_Of_Current_VDA`: Determina si se deben usar los archivos de configuración relacionados con AD existentes (/etc/krb5.conf, /etc/sssd.conf y /etc/samba/smb.conf) del VDA que se está ejecutando actualmente. Si se establece en Y, los archivos de configuración de las máquinas creadas con MCS son los mismos que los equivalentes del VDA que se está ejecutando actualmente. Sin embargo, aún debe configurar las variables `dns` y `AD_INTEGRATION`. El valor predeterminado es N, lo que significa que las plantillas de configuración de la imagen maestra determinan los archivos de configuración de las máquinas creadas con MCS. Para usar un VDA que se está ejecutando actualmente como VM de plantilla, establezca el valor en Y. De lo contrario, establézcalo en N.
- `dns`: Establece la dirección IP de cada servidor DNS. Puede configurar hasta cuatro servidores DNS.
- `NTP_SERVER`: Establece la dirección IP de su servidor NTP. A menos que se especifique lo contrario, es la dirección IP de su controlador de dominio.
- `WORKGROUP`: Establece el nombre del grupo de trabajo en el nombre NetBIOS (distingue mayúsculas y minúsculas) que configuró en AD. De lo contrario, MCS usa la parte del nombre de dominio que sigue inmediatamente al nombre de host de la máquina como nombre del grupo de trabajo. Por ejemplo, si la cuenta de máquina es **user1.lvda.citrix.com**, MCS usa **lvda** como nombre del grupo de trabajo, mientras que **citrix** es la opción correcta. Asegúrese de configurar el nombre del grupo de trabajo correctamente.
- `AD_INTEGRATION`: Establece SSSD, Winbind, PBIS o Centrify. Para ver una matriz de las distribuciones de Linux y los métodos de unión a dominios que admite MSC, consulte Distribuciones admitidas en este artículo.
- `TRUSTED_DOMAINS`: Para entornos de varios dominios, especifique una lista de dominios de confianza separados por espacios (por ejemplo, "mycompany1.com mycompany2.com"). Esto actualiza los dominios de confianza en /etc/krb5.conf y habilita la detección automática de servidores LDAP en esos dominios si no se especifica LDAP_LIST. Esta variable es opcional.

Nota

SSSD solo admite dominios de confianza en un único bosque de Active Directory.

- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete Server Suite Free (anteriormente Centrify Express). El valor surte efecto solo cuando se establece la variable `AD_INTEGRATION` en Centrify.
- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete Centrify Samba. El valor surte efecto solo cuando se establece la variable `AD_INTEGRATION` en Centrify.
- `PBIS_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete PBIS. El valor surte efecto solo cuando se establece la variable `AD_INTEGRATION` en PBIS.
- `UPDATE_MACHINE_PW`: Habilita o deshabilita la automatización de las actualizaciones de contraseñas de cuentas de máquina. Para obtener más información, consulte Automatizar las actualizaciones de contraseñas de cuentas de máquina.
- Variables de configuración de Linux VDA:

  `DOTNET_RUNTIME_PATH`=path-to-install-dotnet-runtime

  `DESKTOP_ENVIRONMENT`=gnome | mate `SUPPORT_DDC_AS_CNAME`=S | N

  `VDA_PORT`=port-number `REGISTER_SERVICE`=S | N

  `ADD_FIREWALL_RULES`=S | N `HDX_3D_PRO`=S | N

  `VDI_MODE`=S | N `SITE_NAME`=dns-site-name | '<none\>'

  `LDAP_LIST`='list-ldap-servers' | '<none\>' `SEARCH_BASE`=search-base-set | '<none\>'

  `FAS_LIST`='list-fas-servers' | '<none\>' `START_SERVICE`=S | N

  `TELEMETRY_SOCKET_PORT`=port-number `TELEMETRY_PORT`=port-number

(Opcional) Paso 3j: Escribir o actualizar valores del Registro para MCS

En la máquina de plantilla, agregue líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar los valores del Registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina aprovisionada por MCS.

Cada línea del archivo `/etc/xdl/mcs/mcs_local_setting.reg` es un comando para establecer o actualizar un valor del registro.

Por ejemplo, puede agregar las siguientes líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar un valor del registro, respectivamente:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -v "Flags" -d "0x00000003"
```

Nota

Para modificar la configuración de MCS, puede editar los archivos en /etc/xdl/ad_join y /etc/xdl/mcs/, pero está prohibido editar cualquier archivo en /var/xdl/mcs.

Paso 3k: Crear una imagen maestra

1. (Solo para SSSD + RHEL 8.x/9.x o Rocky Linux 8.x/9.x) Ejecute el comando `update-crypto-policies --set DEFAULT:AD-SUPPORT` y, a continuación, reinicie la VM de plantilla.
2. Si configura las variables de MCS editando `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura las variables de MCS mediante la GUI, haga clic en **Implementar**. Después de hacer clic en **Implementar** en la GUI, las variables que haya establecido en la GUI anulan las variables que haya establecido en el archivo `/etc/xdl/mcs/mcs.conf`.
3. (Si utiliza una VDA en ejecución como VM de plantilla o si se trata de un escenario sin unión a un dominio, omita este paso). En la VM de plantilla, actualice las plantillas de configuración para personalizar los archivos `/etc/krb5.conf`, `/etc/samba/smb.conf` y `/etc/sssd/sssd.conf` relevantes en todas las VM creadas.

   Para los usuarios de Winbind, actualice las plantillas `/etc/xdl/ad_join/winbind_krb5.conf.tmpl` y `/etc/xdl/ad_join/winbind_smb.conf.tmpl`.

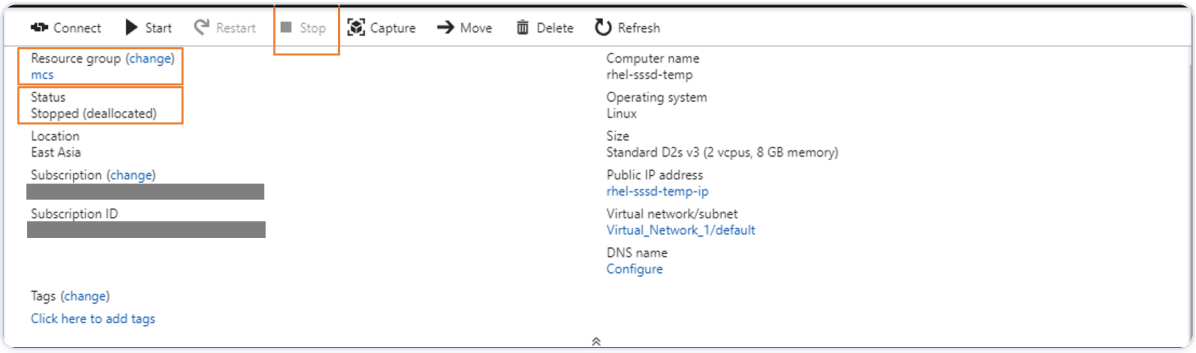
   Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/ad_join/sssd.conf.tmpl`, `/etc/xdl/ad_join/sssd_krb5.conf.tmpl` y `/etc/xdl/ad_join/sssd_smb.conf.tmpl`.

   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/ad_join/centrify_krb5.conf.tmpl` y `/etc/xdl/ad_join/centrify_smb.conf.tmpl`.

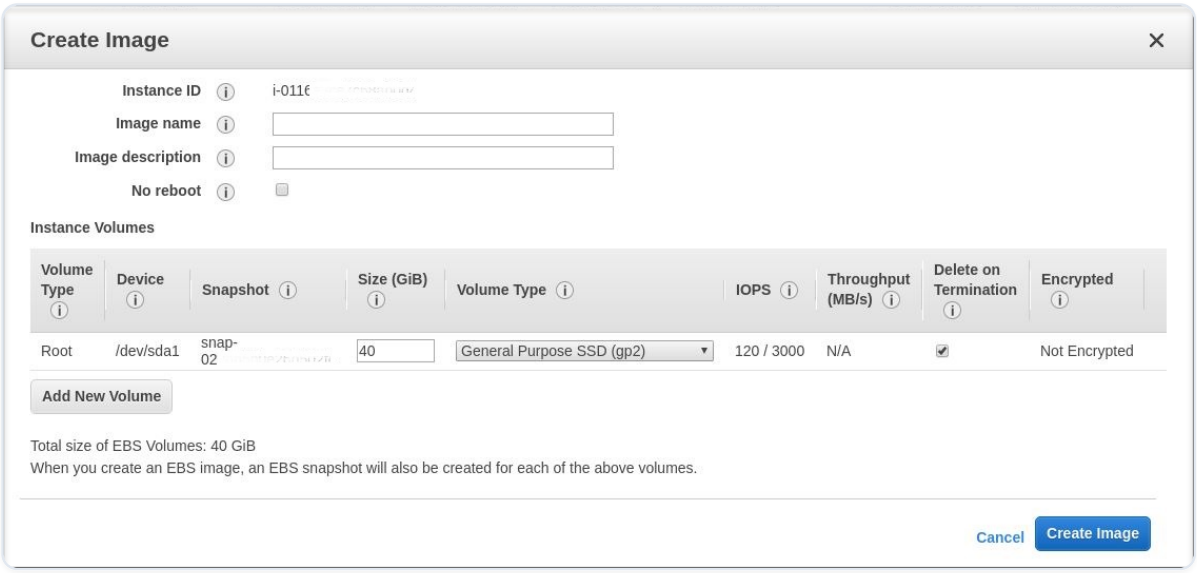
> **Nota:**
>
> Mantenga el formato existente utilizado en los archivos de plantilla y utilice variables como $WORKGROUP, $REALM, $realm, ${new_hostname} y $AD_FQDN.

4. Cree y asigne un nombre a una instantánea de su imagen maestra según la nube pública que utilice.

   - **(Para XenServer, GCP y VMware vSphere)** Instale las aplicaciones en la VM de plantilla y apáguela. Cree y asigne un nombre a una instantánea de su imagen maestra.
   - **(Para Azure)** Instale las aplicaciones en la VM de plantilla y apáguela desde el portal de Azure. Asegúrese de que el estado de energía de la VM de plantilla sea **Detenida (desasignada)**. Recuerde el nombre del grupo de recursos aquí. Necesitará el nombre para localizar su imagen maestra en Azure.



   - **(Para AWS)** Instale aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de AWS EC2. Asegúrese de que el estado de la instancia de la VM de plantilla sea **Detenida**. Haga clic con el botón derecho en la VM de plantilla y seleccione **Imagen > Crear imagen**. Introduzca la información y configure los ajustes según sea necesario. Haga clic en **Crear imagen**.



- **(Para Nutanix)** En Nutanix AHV, apague la VM de plantilla. Cree y asigne un nombre a una instantánea de su imagen maestra.

> **Nota:**
>
> Debe anteponer `XD_` a los nombres de las instantáneas de Acropolis para usarlas en Citrix Virtual Apps and Desktops. Use la consola de Acropolis para cambiar el nombre de las instantáneas cuando sea necesario. Después de cambiar el nombre de una instantánea, reinicie el asistente **Crear catálogo** para obtener una lista actualizada.

(Para GCP) Paso 3l: Configurar la conexión Ethernet en RHEL 8.x/9.x y Rocky Linux 8.x/9.x

Después de instalar el VDA de Linux en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, la conexión Ethernet podría perderse y el VDA de Linux podría quedar inaccesible después de reiniciar la VM. Para solucionar el problema, establezca una contraseña de root al iniciar sesión en la VM por primera vez y asegúrese de que puede iniciar sesión en la VM como root. A continuación, ejecute los siguientes comandos en la consola después de reiniciar la VM:

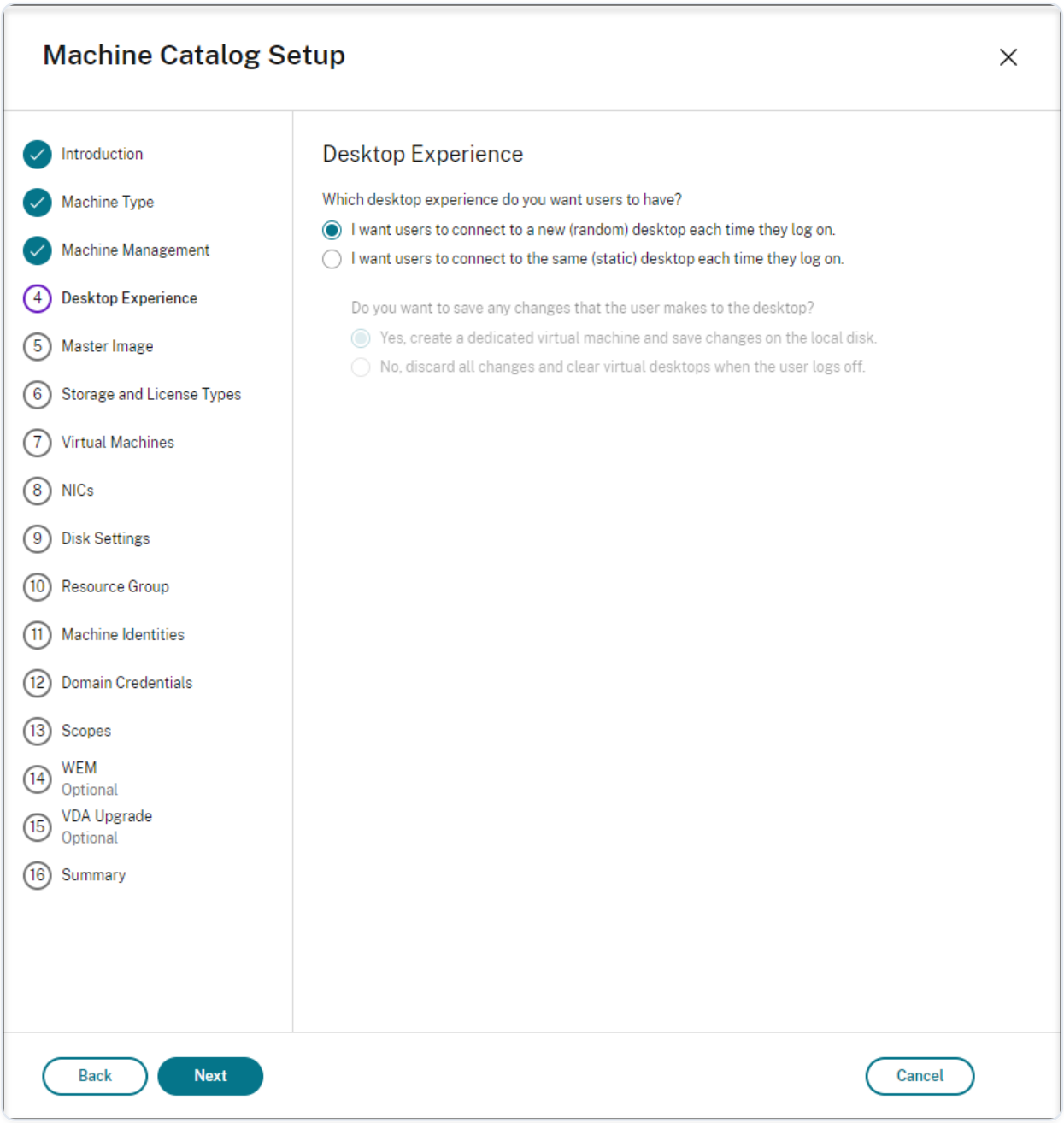
```
nmcli dev connect eth0

systemctl restart NetworkManager
```

Paso 4: Crear un catálogo de máquinas

En Citrix Studio o Web Studio, cree un catálogo de máquinas y especifique el número de VM que se crearán en el catálogo. Al crear el catálogo de máquinas, elija su imagen maestra y tenga en cuenta lo siguiente:

- En la página **Contenedor**, que es exclusiva de Nutanix, seleccione el contenedor que especificó anteriormente para la VM de plantilla.
- Al crear un catálogo que contenga máquinas con **SO de sesión única**, aparece la página **Experiencia de escritorio** y le permite determinar qué ocurre cada vez que un usuario inicia sesión.



En la página **Experiencia de escritorio**, seleccione una de las siguientes opciones:

    - Los usuarios se conectan a un escritorio nuevo (aleatorio) cada vez que inician sesión.
    - Los usuarios se conectan al mismo escritorio (estático) cada vez que inician sesión.

  Si elige la primera opción, los cambios que los usuarios realicen en el escritorio se descartarán (no persistente).

  Si elige la segunda opción y utiliza MCS para aprovisionar las máquinas, puede configurar cómo se gestionan los cambios del usuario en el escritorio:

    - Guardar los cambios del usuario en el escritorio en el disco local (persistente).
    - Descartar los cambios del usuario y borrar el escritorio virtual cuando el usuario cierre la sesión (no persistente). Seleccione esta opción si utiliza la capa de personalización del usuario.

- Al actualizar la imagen maestra de un catálogo de MCS que contiene máquinas persistentes, las máquinas nuevas que se agreguen al catálogo usarán la imagen actualizada. Las máquinas preexistentes seguirán usando la imagen maestra original.

Para obtener más información, consulte la creación de catálogos de máquinas en la documentación de Citrix Virtual Apps and Desktops y la documentación de Citrix DaaS.

> **Nota:**

> Para entornos Nutanix, si el proceso de creación del catálogo de máquinas en el Delivery Controller™ tarda mucho tiempo, vaya a Nutanix Prism y encienda manualmente la máquina con el prefijo **Preparation**. Este enfoque ayuda a continuar el proceso de creación.

Paso 5: Crear un grupo de entrega

Un grupo de entrega es una colección de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica qué usuarios pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios.

Para obtener más información, consulte la creación de grupos de entrega en la documentación de Citrix Virtual Apps and Desktops y la documentación de Citrix DaaS.

> **Nota:**

Es posible que las máquinas virtuales que cree con MCS no puedan registrarse en los Citrix Cloud Connectors y aparezcan como **Sin registrar**. El problema ocurre cuando aloja las máquinas virtuales en Azure y se une al dominio de AD con Samba Winbind. Para solucionar el problema, complete los siguientes pasos:

1. Vaya a la consola ADSI Edit, seleccione una máquina virtual sin registrar y edite el atributo **msDS-SupportedEncryptionTypes** de su cuenta de máquina.
2. Reinicie los servicios **ctxjproxy** y **ctxvda** en la máquina virtual. Si el estado de la máquina virtual cambia a **Registrada**, continúe con los pasos 3 a 5.
3. Abra el archivo **/var/xdl/mcs/ad_join.sh** en la máquina virtual de plantilla.
4. Agregue una línea de **net ads enctypes set $NEW_HOSTNAME\$ <Decimal value of encryption type attribute, for example, 28\> -U $NEW_HOSTNAME\$ -P password** después de las siguientes líneas dentro del archivo **/var/xdl/mcs/ad_join.sh**:

   ```
   if [ "$AD_INTEGRATION" == "winbind" ]; then

                   join_domain_samba

                   restart_service winbind /usr/bin/systemctl
   ```

5. Tome una nueva instantánea y cree máquinas virtuales usando la nueva plantilla.

Usar MCS para actualizar su VDA de Linux

Para usar MCS para actualizar su VDA de Linux, haga lo siguiente:

1. Asegúrese de haber instalado .NET según los requisitos del sistema antes de actualizar su VDA de Linux a la versión actual.
2. Actualice su VDA de Linux en la máquina de plantilla:

Nota:

- También puede usar la función actualización automática de VDA de Linux a través de Azure para programar actualizaciones automáticas de software. Para lograr este objetivo, agregue líneas de comando al archivo etc/xdl/mcs/mcs_local_setting.reg en

la máquina de plantilla. Por ejemplo, puede agregar las siguientes líneas de comando:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_DWORD" -v "fEnabled" -d "0x00000001" --force



create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_SZ" -v "ScheduledTime" -d "Immediately" --force



create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_SZ" -v "Url" -d "&lt;Your-Azure-Container-Url>" –force



create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_SZ" -v "CaCertificate" -d "&lt;Local-Certificate-Path-of-
PortalAzureCom>" --force
```

- A partir de la versión 2407, el VDA de Linux delega en los administradores de paquetes **rpm** o **dpkg** el manejo de los archivos de configuración durante las actualizaciones. A continuación, se describe cómo interactúan rpm y dpkg con los cambios en los archivos de configuración:
  - **rpm**: por defecto, mantiene la versión local y guarda la nueva versión del paquete con una extensión **.rpmnew**.
  - **dpkg**: le pide interactivamente que elija cómo proceder. Para actualizar el VDA de Linux de forma silenciosa, conservando su archivo de configuración local y guardando la nueva versión del paquete como **.dpkg-new** o **.dpkg-dist**, use el siguiente comando:

```
dpkg --force-confold -i package.deb  # Always keep your version, then save new package's version as *.dpkg-new or *.dpkg-dist
```

Para distribuciones RHEL y Rocky Linux:

```
sudo yum -y localinstall <PATH>/<Linux VDA RPM>
```

Nota:

Antes de actualizar el VDA de Linux en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.

Para distribuciones SUSE:

```
sudo zypper -i install <PATH>/<Linux VDA RPM>
```

Para distribuciones Ubuntu/Debian:

```
sudo dpkg -i <PATH>/<Linux VDA deb>



sudo apt-get install -f
```

3. Edite `/etc/xdl/mcs/mcs.conf` y `/etc/xdl/mcs/mcs_local_setting.reg`.
4. Tome una nueva instantánea.
5. En Citrix Studio, seleccione la nueva instantánea para actualizar su catálogo de máquinas. Espere antes de que se reinicie cada máquina. No reinicie una máquina manualmente.

Automatizar las actualizaciones de contraseñas de cuentas de máquina

Las contraseñas de las cuentas de máquina, por defecto, caducan 30 días después de la creación del catálogo de máquinas. Para evitar la caducidad de las contraseñas y automatizar las actualizaciones de las contraseñas de las cuentas de máquina, haga lo siguiente:

1. Agregue la siguiente entrada a /etc/xdl/mcs/mcs.conf antes de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh.

   `UPDATE_MACHINE_PW="Y"`

2. Después de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh, abra /etc/cron.d/mcs_update_password_cronjob para configurar la hora y la frecuencia de actualización. La configuración predeterminada actualiza las contraseñas de las cuentas de máquina semanalmente a las 2:30 a. m. del domingo.

Después de cada actualización de la contraseña de la cuenta de máquina, la caché de tickets del Delivery Controller deja de ser válida y puede aparecer el siguiente error en /var/log/xdl/jproxy.log:

`[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred. Error: Failure unspecified at GSS-API level (Mechanism level: Checksum failed)`

Para eliminar el error, borre la caché de tickets regularmente. Puede programar una tarea de limpieza de caché en todos los Delivery Controllers o en el controlador de dominio.

Crear VDA de Linux unidos a un dominio con FAS habilitado mediante Machine Creation Services™ (MCS)

> **Importante:**
>
> Los siguientes son cambios importantes a partir de la versión 2212:
>
> - La variable **AD_INTEGRATION** en el archivo /etc/xdl/mcs/mcs.conf o en la GUI de instalación sencilla ya no tiene un valor predeterminado. Debe establecer un valor según sea necesario. Para obtener más información, consulte la sección (#step-3j-configure-mcs-variables) en este artículo.
> - El valor válido de la entrada **UPDATE_MACHINE_PW** en /etc/xdl/mcs/mcs.conf ya no es **enabled** o **disabled**, sino **Y** o **N**. Para obtener más información, consulte la sección (#automate-machine-account-password-updates) en este artículo.

Distribuciones admitidas

	WINBIND	SSSD	PBIS
Debian 12.15/11.11	Sí	Sí	Sí
RHEL 9.8/9.6/9.4	Sí	Sí	No
RHEL 8.x	Sí	Sí	Sí
Rocky Linux 9.8/9.6/9.4	Sí	Sí	No
Rocky Linux 8.x	Sí	Sí	No
Ubuntu 24.04/22.04	Sí	Sí	No
SUSE 15.6	Sí	Sí	No

Nota:

Para implementaciones de RHEL 8.x/9.x o Rocky Linux 8.x/9.x, para usar el VDA unido a SSSD actual como VM de plantilla para la implementación de MCS, asegúrese de que:

- El VDA no se puede implementar mediante el script de instalación fácil, porque la combinación de SSSD y Adcli en easy-install no es compatible con MCS.

Para usar MCS para implementar un VDA unido a AD mediante el protocolo SSSD, se debe configurar un servidor Samba para la autenticación de AD. Para obtener más información, consulte el artículo de Red Hat.

Si utiliza PBIS para unir máquinas creadas con MCS a dominios de Windows, complete las siguientes tareas:

- En la máquina de plantilla, configure la ruta de descarga del paquete PBIS en el archivo `/etc/xdl/mcs/mcs.conf` o instale el paquete PBIS directamente.

- Antes de ejecutar `/opt/Citrix/VDA/sbin/deploymcs.sh`, cree una Unidad organizativa (OU) que tenga permisos de escritura y restablecimiento de contraseña para todas sus máquinas subordinadas creadas con MCS.
- Antes de reiniciar las máquinas creadas con MCS después de que `/opt/Citrix/VDA/sbin/deploymcs.sh` termine de ejecutarse, ejecute `klist -li 0x3e4 purge` en su Delivery Controller o en su Citrix Cloud Connector, según su implementación.

Hipervisores compatibles

- AWS
- XenServer (anteriormente Citrix Hypervisor™)
- GCP
- Microsoft Azure
- Nutanix AHV
- VMware vSphere

Pueden producirse resultados inesperados si intenta preparar una imagen maestra en hipervisores distintos de los compatibles.

Crear VDA de Linux con FAS habilitado mediante MCS

Esta sección describe el procedimiento para crear VDA de Linux mediante MCS y habilitar FAS mientras se prepara una imagen maestra en la VM de plantilla. Si FAS no está habilitado en la VM de plantilla, puede habilitarlo en cada VM creada con MCS más adelante consultando Habilitar FAS en una VM creada con MCS.

Consideraciones

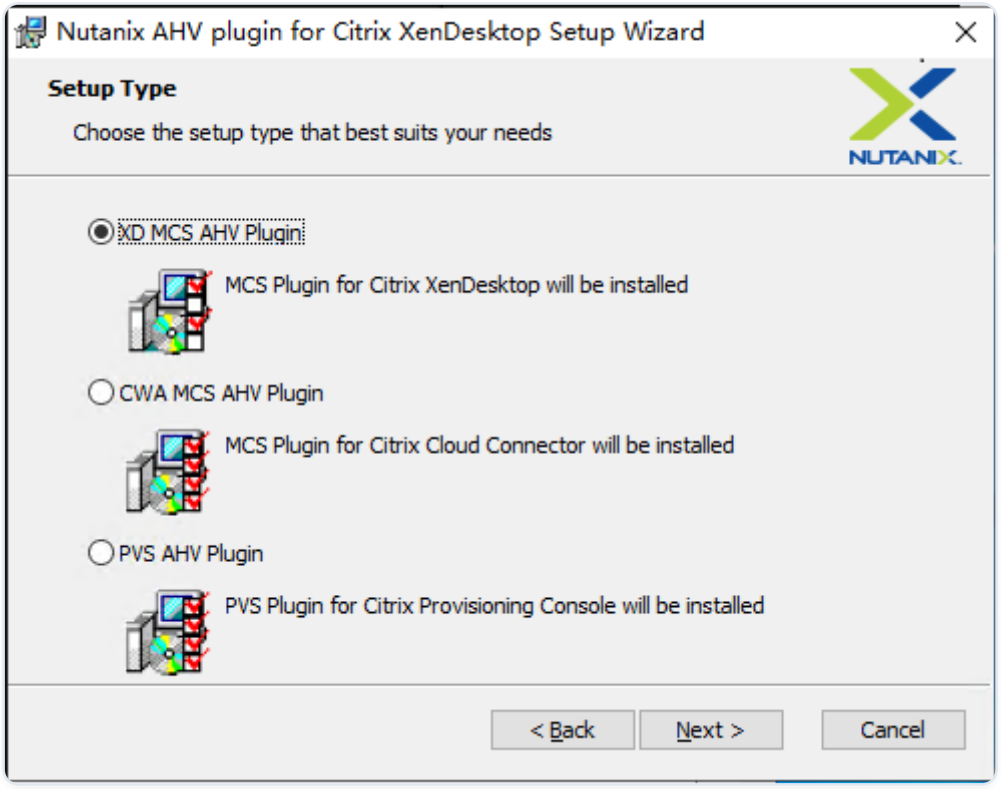
- A partir de la versión 2203, puede alojar el VDA de Linux en Microsoft Azure, AWS y GCP para Citrix Virtual Apps and Desktops™ y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops service). Para agregar estas conexiones de host de nube pública a su implementación de Citrix Virtual Apps and Desktops, necesita la licencia Citrix Universal Hybrid Multi-Cloud (HMC).
- Los servidores bare metal no son compatibles para su uso con MCS para crear máquinas virtuales.

(Solo para Nutanix) Paso 1: Instale y registre el complemento Nutanix AHV

Obtenga el paquete del complemento Nutanix AHV de Nutanix. Instale y registre el complemento en su entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte la guía de instalación del complemento Nutanix Acropolis MCS, disponible en el Portal de soporte de Nutanix.

Paso 1a: Instalar y registrar el complemento de Nutanix AHV para Delivery Controllers locales

Después de instalar Citrix Virtual Apps™ and Desktops, seleccione e instale el **XD MCS AHV Plugin** en sus Delivery Controllers.



Paso 1b: Instalar y registrar el complemento de Nutanix AHV para Delivery Controllers en la nube

Seleccione e instale el **CWA MCS AHV Plugin** para los Citrix Cloud™ Connectors. Instale el complemento en todos los Citrix Cloud Connectors registrados con el inquilino de Citrix Cloud. Debe registrar los Citrix Cloud Connectors incluso cuando presten servicio a una ubicación de recursos sin AHV.

Paso 1c: Complete los siguientes pasos después de instalar el complemento

- verificar que se ha creado una carpeta de Nutanix Acropolis en `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.

- Ejecute el comando `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`.
- Reinicie los servicios Citrix Host, Citrix Broker y Citrix Machine Creation Services en sus Delivery Controllers locales o reinicie el servicio Citrix RemoteHCLServer en los Citrix Cloud Connectors.

> **Sugerencia:**
>
> Recomendamos detener y luego reiniciar los servicios Citrix Host, Citrix Broker y Machine Creation Services al instalar o actualizar el complemento de Nutanix AHV.

Paso 2: Crear una conexión de host

Esta sección ofrece ejemplos sobre cómo crear una conexión de host a Azure, AWS, XenServer® (anteriormente Citrix Hypervisor), GCP, Nutanix AHV y VMware vSphere.

> **Nota:**
>
> Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.

> Para obtener más información, consulte Crear y administrar conexiones y recursos en la documentación de Citrix Virtual Apps and Desktops y Crear y administrar conexiones en la documentación de Citrix DaaS.

- Crear una conexión de host a Azure en Citrix Studio
- Crear una conexión de host a AWS en Citrix Studio
- Crear una conexión de host a XenServer en Citrix Studio
- Crear una conexión de host a GCP en Citrix Studio
- Crear una conexión de host a Nutanix en Citrix Studio
- Crear una conexión de host a VMware en Citrix Studio

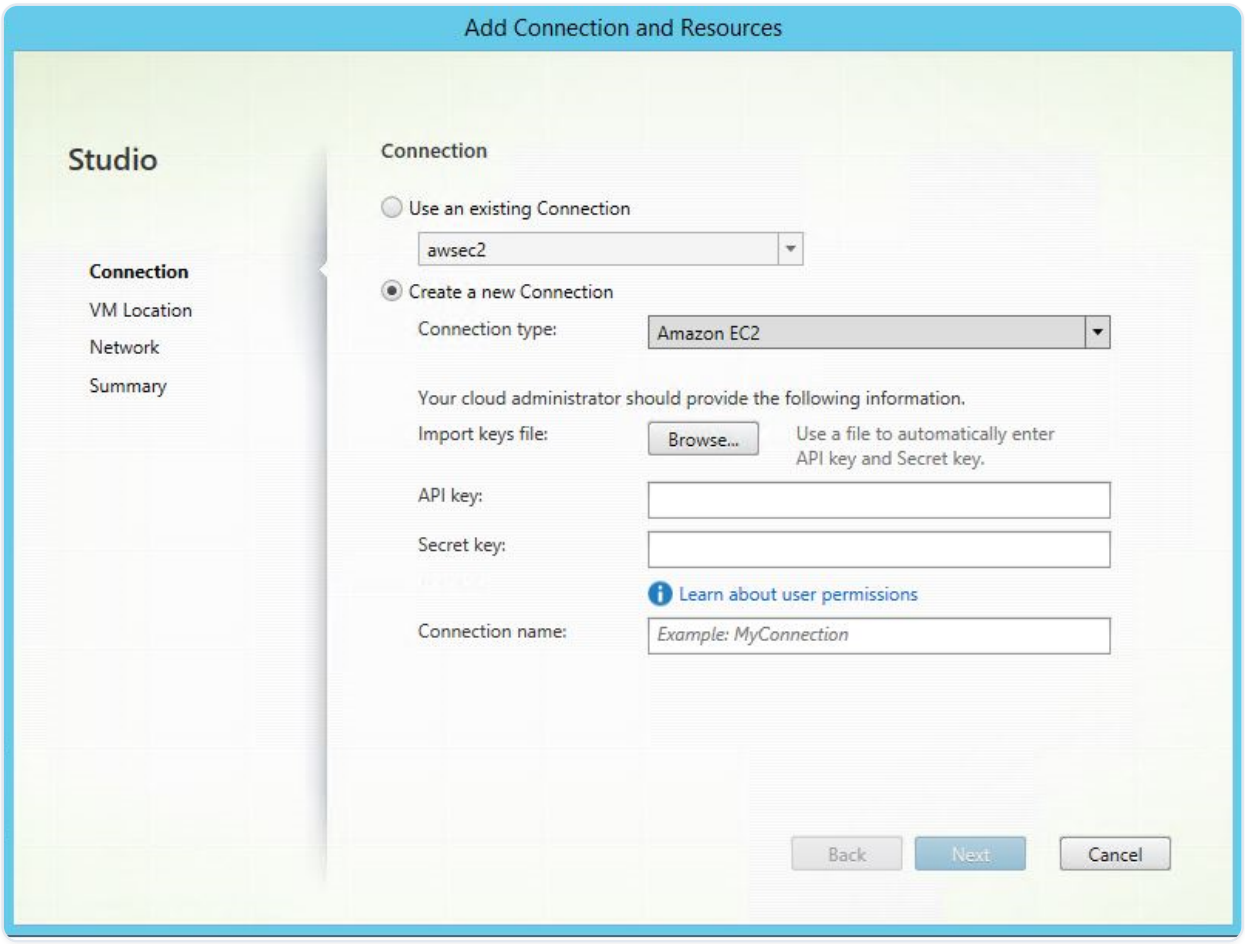
Crear una conexión de host a Azure en Citrix Studio

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione Microsoft Azure como tipo de conexión.
3. Seleccione Microsoft Azure como tipo de conexión.
4. El asistente le guiará por las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte el **Paso 2: Crear una conexión de host** en el artículo Crear VDA de Linux sin unir a un dominio mediante MCS.

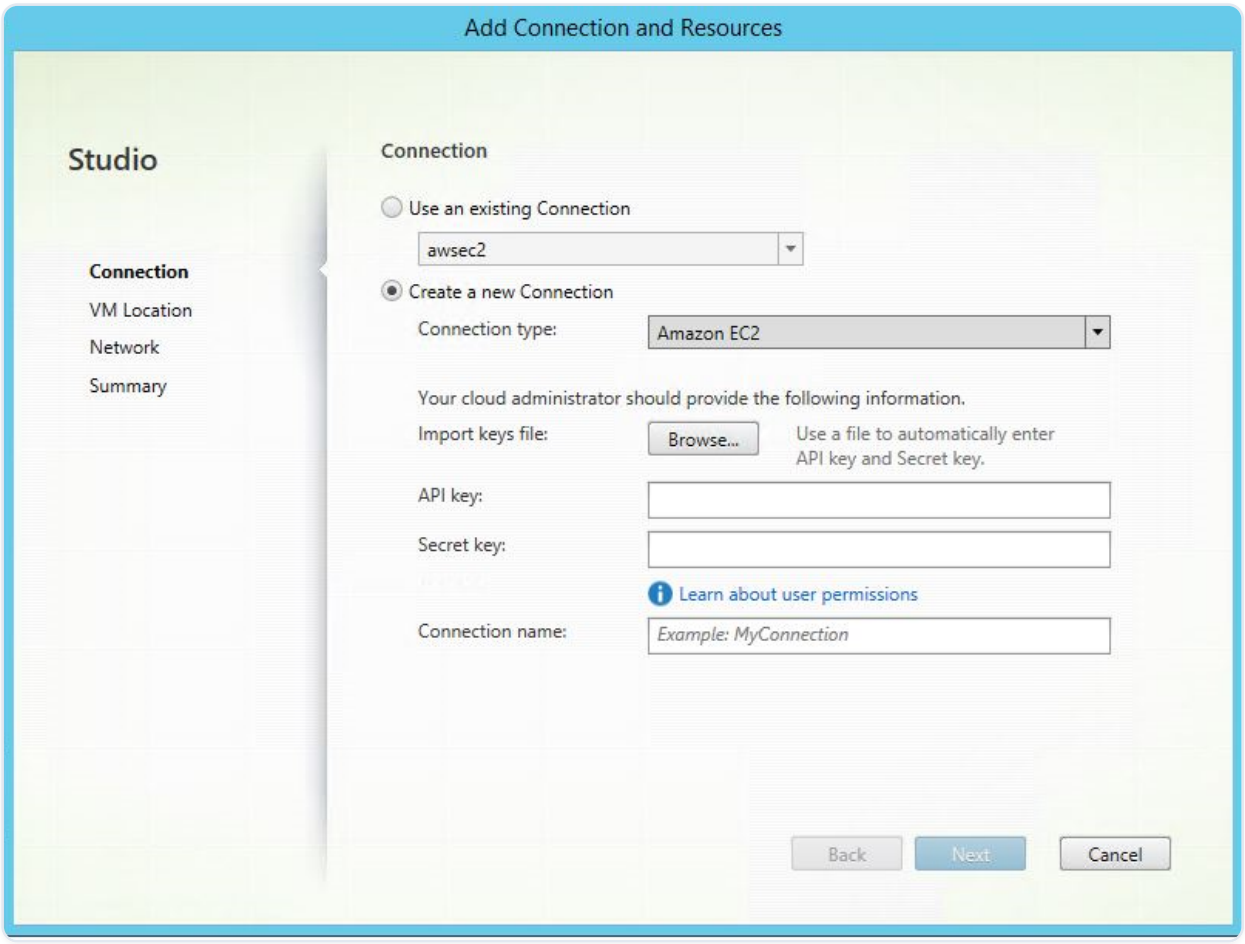
Crear una conexión de host a AWS en Citrix Studio

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione **Amazon EC2** como tipo de conexión.

   Por ejemplo, en Citrix Studio local:



3. Escriba la clave de API y la clave secreta de su cuenta de AWS y escriba el nombre de su conexión.



La **clave de API** es su ID de clave de acceso y la **clave secreta** es su clave de acceso secreta. Se consideran un par de claves de acceso. Si pierde su clave de acceso secreta, puede eliminar la clave de acceso y crear otra. Para crear una clave de acceso, haga lo siguiente:

a. Inicie sesión en los servicios de AWS.

b. Vaya a la consola de Identity and Access Management (IAM). 1 En el panel de navegación izquierdo, elija **Usuarios**.

c. Seleccione el usuario de destino y desplácese hacia abajo para seleccionar la ficha **Credenciales de seguridad**.

d. Desplácese hacia abajo y haga clic en **Crear clave de acceso**. Aparecerá una nueva ventana.

e. Haga clic en **Descargar archivo .csv** y guarde la clave de acceso en una ubicación segura.

4. El asistente le guiará por las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**.

Crear una conexión de host a XenServer en Citrix Studio

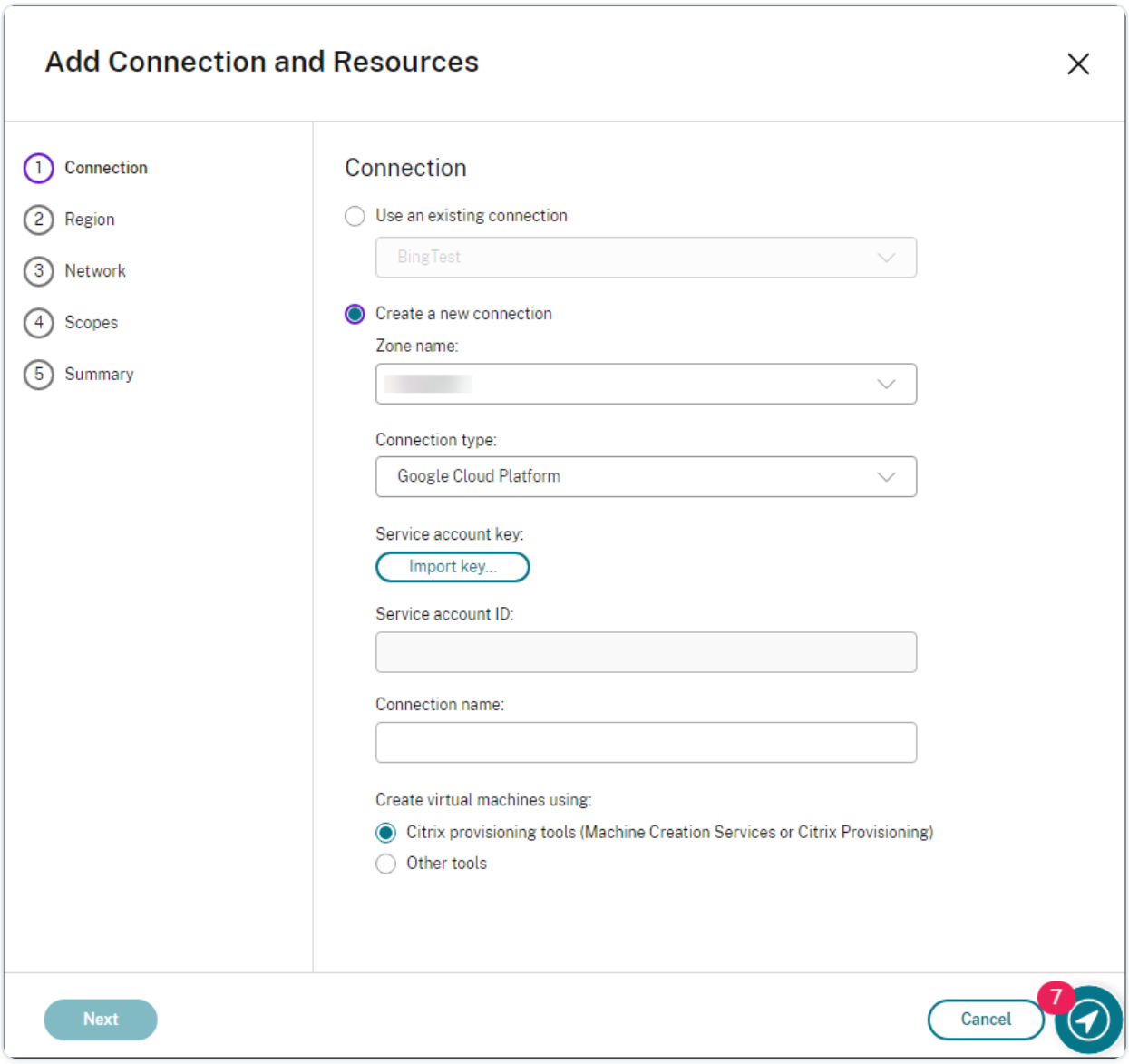
1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione XenServer (anteriormente Citrix Hypervisor) en el campo **Tipo de conexión**.
3. Escriba la dirección de conexión (la URL de XenServer) y las credenciales.
4. Introduzca un nombre de conexión.

Crear una conexión de host a GCP en Citrix Studio

Configure su entorno de GCP según Entornos de virtualización de Google Cloud Platform y, a continuación, complete los siguientes pasos para crear una conexión de host a GCP.

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione **Google Cloud Platform** como tipo de conexión.

   Por ejemplo, en la consola de Studio basada en web en Citrix Cloud:



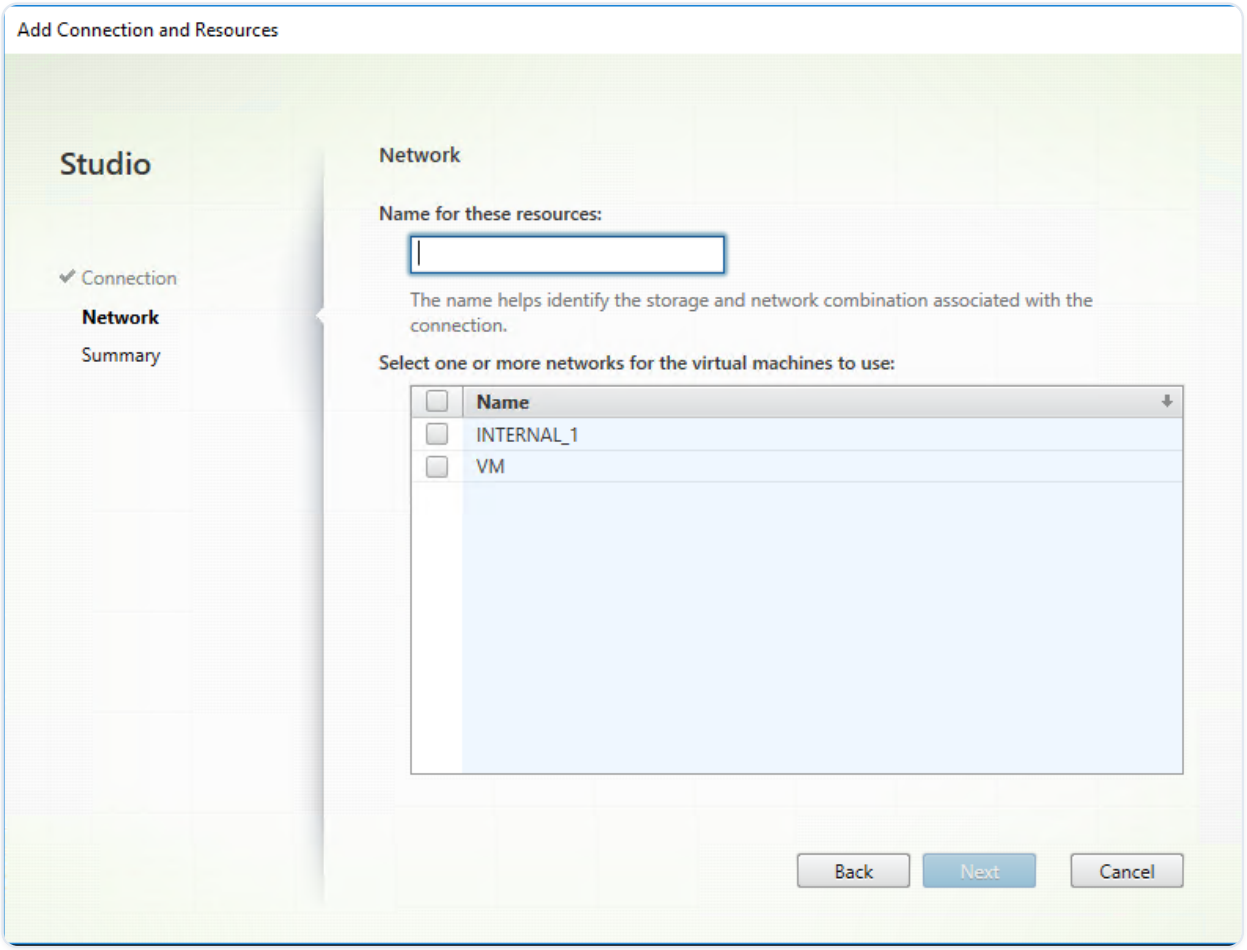
3. Importe la clave de cuenta de servicio de su cuenta de GCP y escriba el nombre de su conexión.
4. El asistente le guiará por las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte el **Paso 2: Crear una conexión de host** en el artículo Crear VDA de Linux no unidos a un dominio mediante MCS.

Crear una conexión de host a Nutanix en Citrix Studio

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.

2. En el asistente **Agregar conexión y recursos**, seleccione Nutanix AHV como tipo de conexión en la página **Conexión** y, a continuación, especifique la dirección del hipervisor, las credenciales y el nombre de la conexión. En la página **Red**, seleccione una red para la unidad.

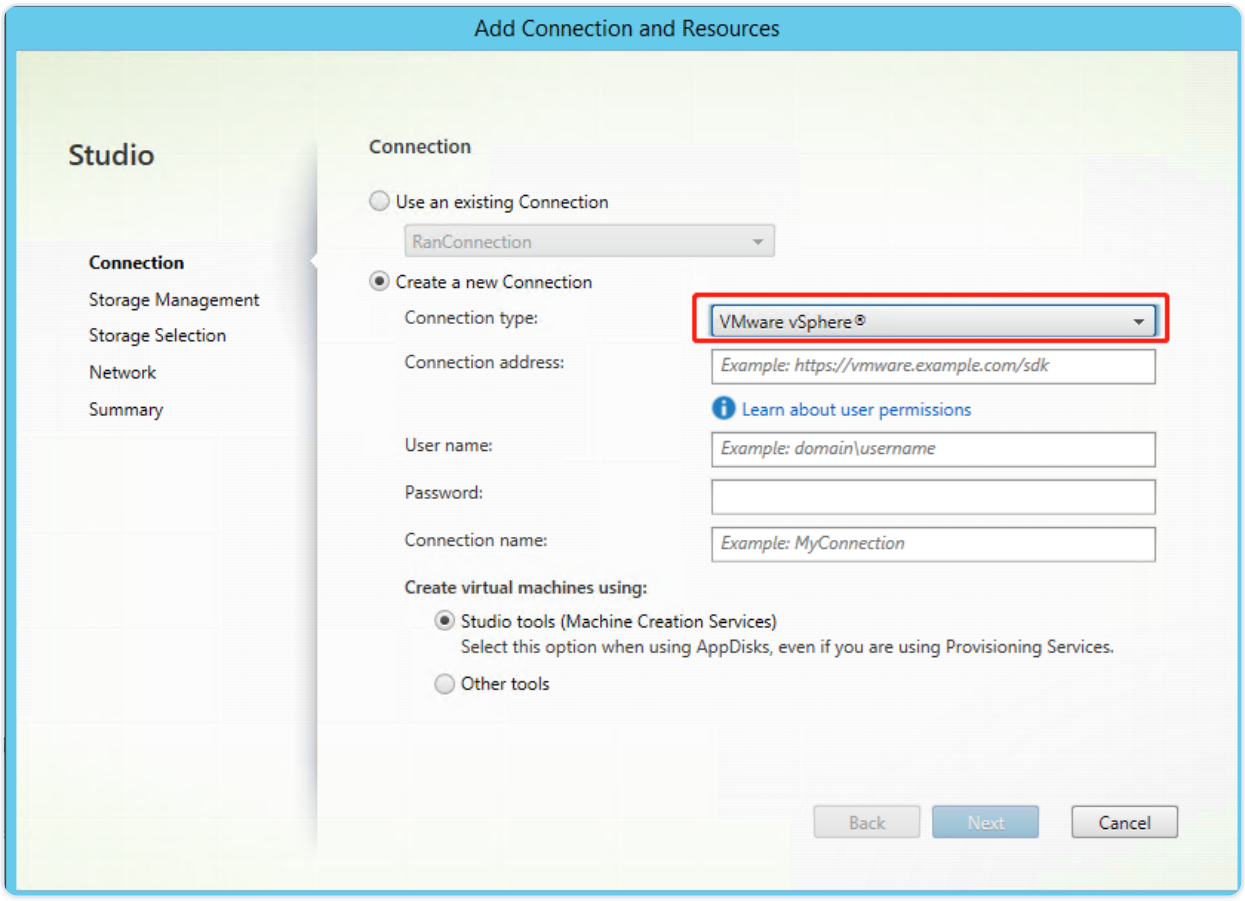
   Por ejemplo, en Citrix Studio local:



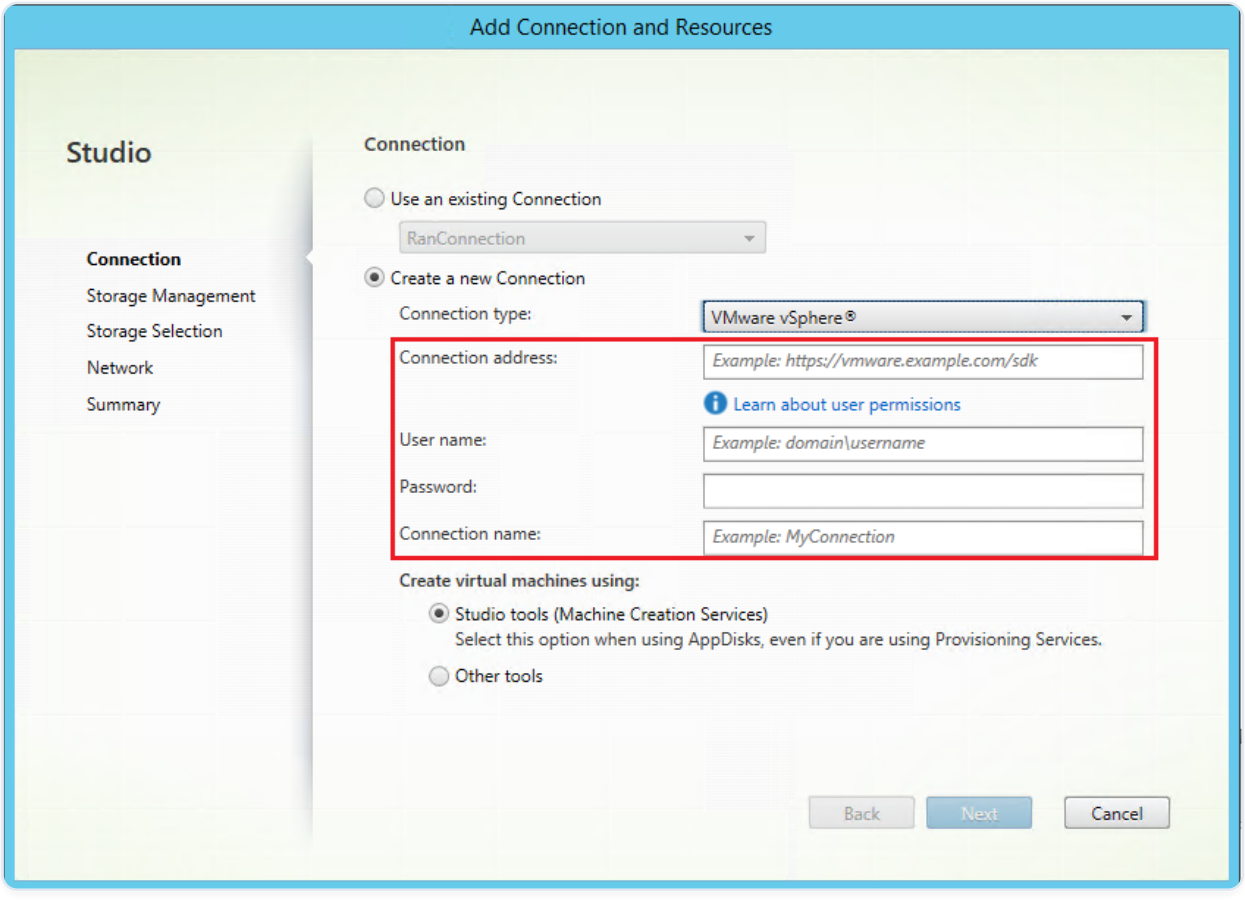
Crear una conexión de host a VMware en Citrix Studio

1. Instale vCenter Server en el entorno de vSphere. Para obtener más información, consulte VMware vSphere.
2. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud para crear una conexión de host.
3. Elija VMware vSphere como tipo de conexión.

   Por ejemplo, en Citrix Studio local:



4. Escriba la dirección de conexión (la URL del servidor vCenter) de su cuenta de VMware, sus credenciales y el nombre de su conexión.



Paso 3: Preparar una imagen maestra

(Solo para XenServer) Paso 3a: Instalar las herramientas de VM de XenServer

Instale las herramientas de VM de XenServer en la VM de plantilla para que cada VM utilice la CLI xe o XenCenter. El rendimiento de la VM puede ser lento si no instala las herramientas. Sin las herramientas, no puede hacer lo siguiente:

- Apagar, reiniciar o suspender una VM de forma limpia.
- Ver los datos de rendimiento de la VM en XenCenter.
- Migrar una VM en ejecución (a través de `XenMotion`).
- Crear instantáneas o instantáneas con memoria (puntos de control) y revertir a instantáneas.
- Ajustar el número de vCPU en una VM Linux en ejecución.

1. Descargue el archivo de herramientas de VM de XenServer para Linux desde la página de descargas de XenServer o la página de descargas de Citrix Hypervisor según la versión del hipervisor en uso.
2. Copie el archivo `LinuxGuestTools-xxx.tar.gz` en su VM Linux o en una unidad compartida a la que pueda acceder la VM Linux.
3. Extraiga el contenido del archivo tar: `tar -xzf LinuxGuestTools-xxx.tar.gz`
4. Ejecute el siguiente comando para instalar el paquete `xe-guest-utilities` según su distribución de Linux.

   Para RHEL/CentOS/Rocky Linux/SUSE:

   ```
   sudo rpm -i <extract-directory>/xe-guest-utilities_{package-version}
   _x86.64.rpm
   ```

   Para Ubuntu/Debian:

   ```
   sudo dpkg -i <extract-directory>/xe-guest-utilities_{package-version}
   _amd64.deb
   ```

5. Compruebe el estado de virtualización de la VM de plantilla en la pestaña **General** de XenCenter. Si las herramientas de XenServer VM están instaladas correctamente, el estado de virtualización muestra **Optimizado**.

Paso 3b: verificar las configuraciones para SUSE 15.5 en AWS, Azure y GCP

Para SUSE 15.5 en AWS, Azure y GCP, asegúrese de que:

- Está utilizando **libstdc++6** versión 12 o posterior.
- El parámetro **Default_WM** en **/etc/sysconfig/windowmanager** está establecido en **"gnome"**.

Paso 3c: Deshabilitar RDNS para Ubuntu 20.04 en GCP

En la VM de plantilla, añada la línea **rdns = false** debajo de en /etc/krb5.conf.

Paso 3d: Instalar .NET en la VM de plantilla

Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Paso 3e: Instalar el paquete VDA de Linux en la VM de plantilla

Después de instalar .NET, ejecute los siguientes comandos según su distribución de Linux para instalar el VDA de Linux:

Para RHEL/Rocky Linux:

> **Nota:**
>
> Antes de instalar el VDA de Linux en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.

```
sudo yum –y localinstall <PATH>/<Linux VDA RPM>
```

Para Ubuntu/Debian:

```
sudo dpkg –i  <PATH>/<Linux VDA DEB>



apt-get install -f
```

Para SUSE:

```
sudo zypper –i install <PATH>/<Linux VDA RPM>
```

Paso 3f: (Solo para RHEL) Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en `<https://docs.fedoraproject.org/es-es/epel/>`.

Paso 3g: (Solo para SUSE) Instale ntfs-3g manualmente

En la plataforma SUSE, ningún repositorio proporciona ntfs-3g. Descargue el código fuente, compile e instale ntfs-3g manualmente:

1. Instale el sistema de compilación GNU Compiler Collection (GCC) y el paquete make:

```
sudo zypper install gcc

sudo zypper install make
```

2. Descargue el paquete ntfs-3g.
3. Descomprima el paquete ntfs-3g:

```
sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
```

4. Introduzca la ruta al paquete ntfs-3g:

```
sudo cd ntfs-3g_ntfsprogs-<package version>
```

5. Instale ntfs-3g:

```
./configure

make

make install
```

Paso 3h: Una la VM a un dominio de Windows

Una la VM a un dominio de Windows. Recomendamos usar el script de instalación fácil (ctxinstall.sh) para este proceso, ya que ahorra tiempo, reduce el trabajo y es menos propenso a errores en comparación con la instalación manual. Para obtener más información, consulte Paso 8: Ejecutar la instalación fácil para configurar el entorno y el VDA para completar la instalación. Si prefiere la instalación manual, consulte los pasos 1 a 3 en los artículos de instalación manual en Instalar el VDA de Linux manualmente.

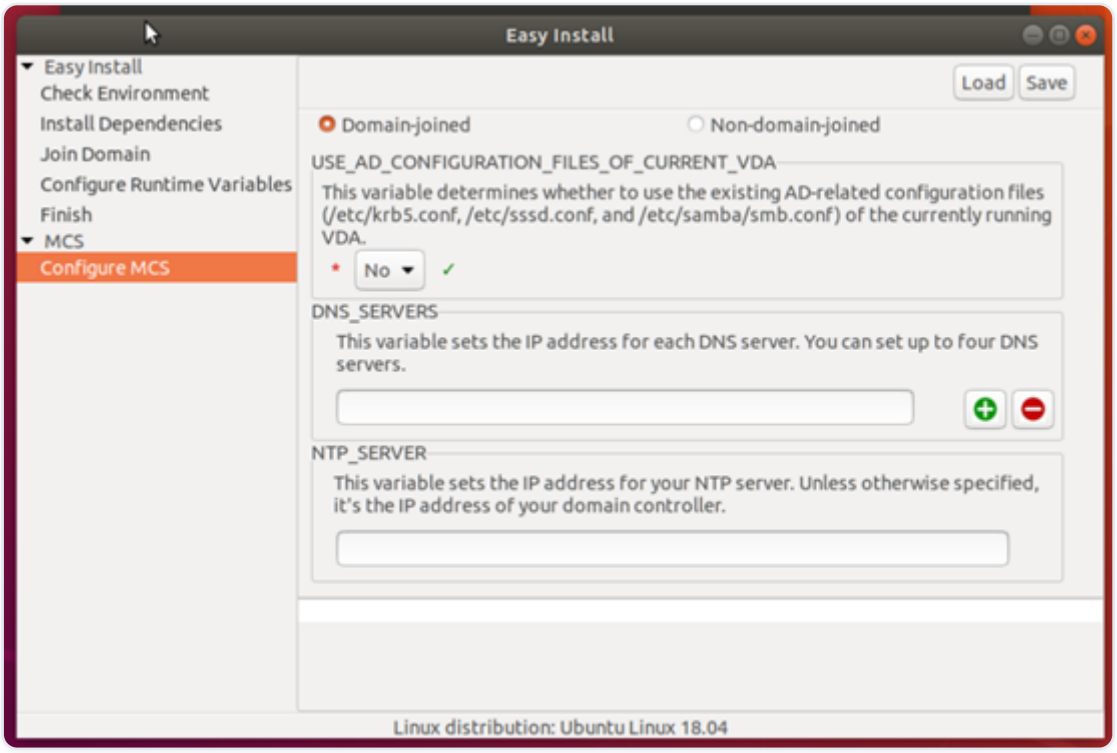
Paso 3i: Configure FAS en la VM

Para conocer los pasos detallados, consulte Configurar FAS en el VDA de Linux.

Paso 3j: Configurar variables de MCS

Hay dos formas de configurar las variables de MCS:

- Editar el archivo `/etc/xdl/mcs/mcs.conf`.
- Utilice la GUI de instalación sencilla. Para abrir la GUI de instalación sencilla, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su VDA de Linux.



> **Sugerencia:**
>
> Haga clic en **Guardar** para guardar la configuración de las variables en un archivo local en la ruta que especifique. Haga clic en **Cargar** para cargar la configuración de las variables desde un archivo que especifique.

Las siguientes son variables de MCS que puede configurar para escenarios con FAS habilitado:

```
-  `Use_AD_Configuration_Files_Of_Current_VDA`: Determines whether to use
the existing AD-related configuration files (/etc/krb5.conf, /etc/
sssd.conf, and /etc/samba/smb.conf) of the currently running VDA. Set the
```

value to Y when FAS is enabled.

- `dns`: Sets the IP address for each DNS server. You can set up to four DNS servers.

- `NTP_SERVER`: Sets the IP address for your NTP server. Unless otherwise specified, it's the IP address of your domain controller.

- `WORKGROUP`: Sets the workgroup name to the NetBIOS name (case-sensitive) that you configured in AD. Otherwise, MCS uses the part of the domain name that immediately follows the machine hostname as the workgroup name. For example, if the machine account is **user1.lvda.citrix.com**, MCS uses **lvda** as the workgroup name while **citrix** is the correct choice. Ensure that you set the workgroup name correctly.

- `AD_INTEGRATION`: Sets SSSD, Winbind, or PBIS. For a matrix of the Linux distributions and domain joining methods that MSC supports, see [Supported distributions](#distribuciones-admitidas) in this article.

- `PBIS_DOWNLOAD_PATH`: Sets the path for downloading the PBIS package. The value takes effect only when you set the `AD_INTEGRATION` variable to PBIS.

- `UPDATE_MACHINE_PW`: Enables or disables automating machine account password updates. For more information, see [Automate machine account password updates](https://docs.citrix.com/us/en/linux-virtual-delivery-agent/2507-ltsr/installation-overview/create-linux-vdas-using-mcs.html#automatizar-las-actualizaciones-de-contraseñas-de-cuentas-de-máquina).

```
-  Linux VDA configuration variables:



    `DOTNET_RUNTIME_PATH`=path-to-install-dotnet-runtime

    `DESKTOP_ENVIRONMENT`=gnome | mate

    `SUPPORT_DDC_AS_CNAME`=Y | N

    `VDA_PORT`=port-number

    `REGISTER_SERVICE`=Y | N

    `ADD_FIREWALL_RULES`=Y | N

    `HDX_3D_PRO`=Y | N

    `VDI_MODE`=Y | N

    `SITE_NAME`=dns-site-name | '&lt;none\>'

    `LDAP_LIST`='list-ldap-servers' | '&lt;none\>'

    `SEARCH_BASE`=search-base-set | '&lt;none\>'

    `START_SERVICE`=Y | N

    `TELEMETRY_SOCKET_PORT`=port-number

    `TELEMETRY_PORT`=port-number
```

Paso 3k: Escribir o actualizar valores del Registro para MCS

Agregue la siguiente línea de comandos al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para configurar las direcciones de su servidor FAS:

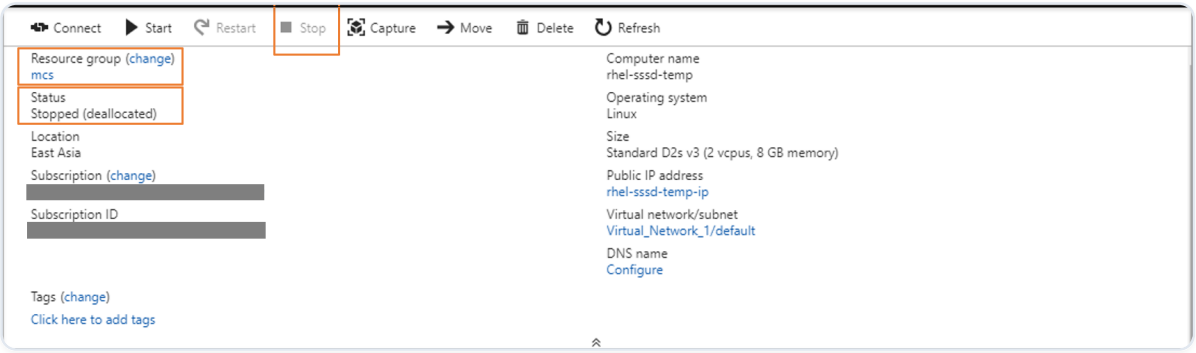
```
create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force
```

> **Nota**
>
> Para modificar la configuración de MCS, puede editar archivos en /etc/xdl/ad_join y /etc/xdl/mcs/, pero está prohibido editar cualquier archivo en /var/xdl/mcs.

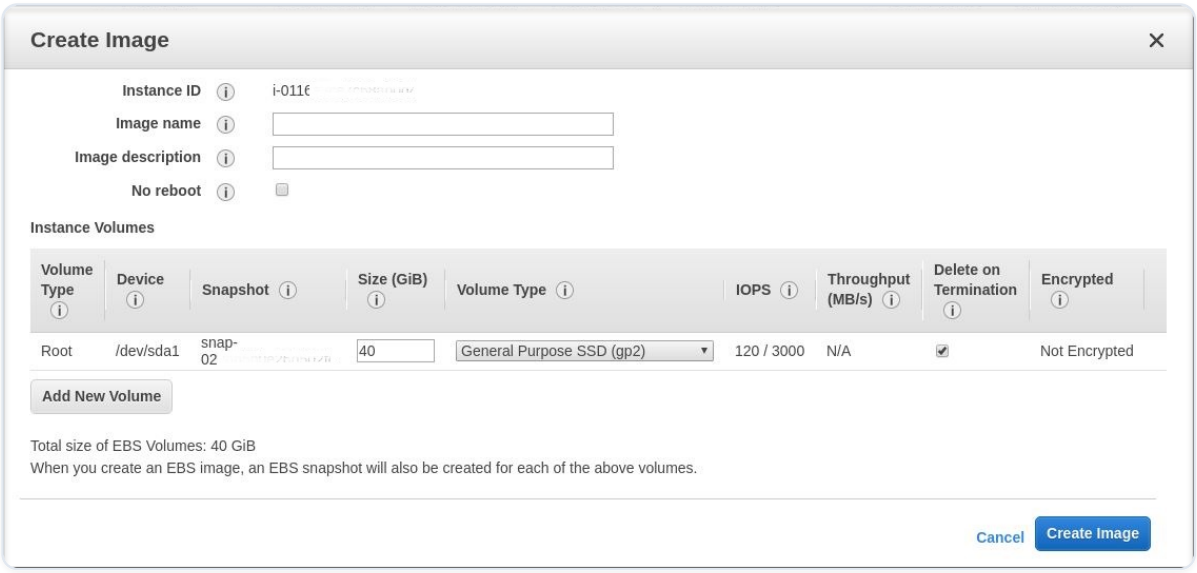
Paso 3l: Crear una imagen maestra

1. (Solo para SSSD + RHEL 8.x/9.x o Rocky Linux 8.x/9.x) Ejecute el comando `update-crypto-policies --set DEFAULT:AD-SUPPORT` y, a continuación, reinicie la VM de la plantilla.
2. Si configura las variables de MCS editando `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura las variables de MCS mediante la GUI, haga clic en **Implementar**. Después de hacer clic en **Implementar** en la GUI, las variables que configure en la GUI anularán las variables que configure en el archivo `/etc/xdl/mcs/mcs.conf`.
3. Cree y asigne un nombre a una instantánea de su imagen maestra según la nube pública que utilice.

   - **(Para XenServer, GCP y VMware vSphere)** Instale las aplicaciones en la VM de la plantilla y apague la VM de la plantilla. Cree y asigne un nombre a una instantánea de su imagen maestra.
   - **(Para Azure)** Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de Azure. Asegúrese de que el estado de energía de la VM de plantilla sea **Detenida (desasignada)**. Recuerde el nombre del grupo de recursos aquí. Necesitará el nombre para localizar su imagen maestra en Azure.

   - **(Para AWS)** Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de AWS EC2. Asegúrese de que el estado de la instancia de la VM de plantilla sea **Detenida**. Haga clic con el botón derecho en la VM de plantilla y seleccione **Imagen > Crear imagen**. Escriba la información y realice los ajustes necesarios. Haga clic en **Crear imagen**.



- **(Para Nutanix)** En Nutanix AHV, apague la VM de plantilla. Cree y asigne un nombre a una instantánea de su imagen maestra.

> **Nota:**
>
> Debe prefijar los nombres de las instantáneas de Acropolis con `XD_` para usarlos en Citrix Virtual Apps and Desktops. Utilice la consola de Acropolis para cambiar el nombre de sus instantáneas cuando sea necesario. Después de cambiar el nombre de una instantánea, reinicie el asistente **Crear catálogo** para obtener una lista actualizada.

(Para GCP) Paso 3m: Configurar la conexión Ethernet en RHEL 8.x/9.x y Rocky Linux 8.x/9.x

Después de instalar el VDA de Linux en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, la conexión Ethernet podría perderse y el VDA de Linux podría quedar inaccesible después de un reinicio de la VM. Para solucionar el problema, establezca una contraseña de root al iniciar sesión en la VM por primera vez y asegúrese de poder iniciar sesión en la VM como root. Luego, ejecute los siguientes comandos en la consola después de reiniciar la VM:

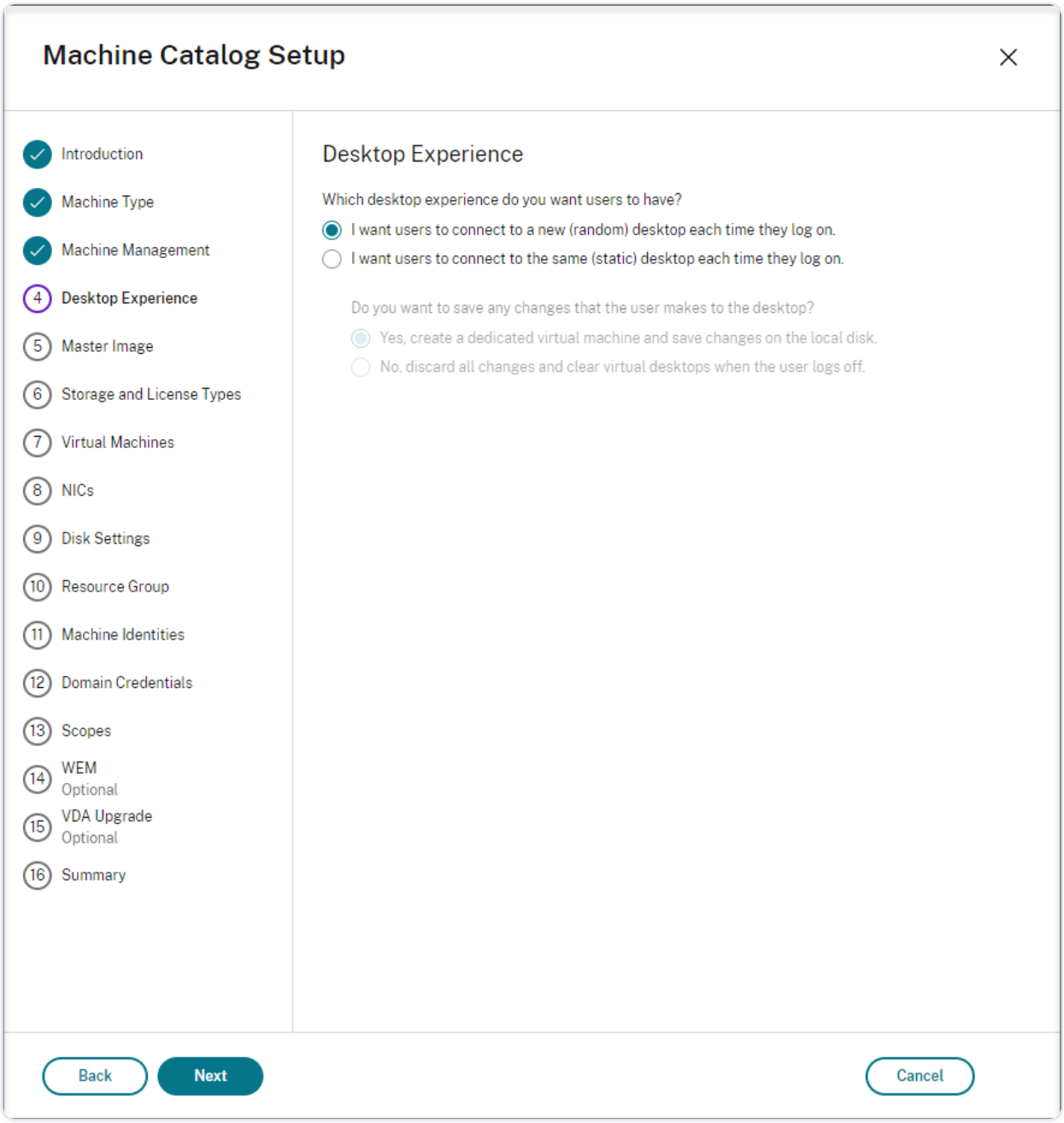
```
nmcli dev connect eth0

systemctl restart NetworkManager
```

Paso 4: Crear un catálogo de máquinas

En Citrix Studio o Web Studio, cree un catálogo de máquinas y especifique el número de VM que se crearán en el catálogo. Al crear el catálogo de máquinas, elija su imagen maestra y considere lo siguiente:

- En la página **Contenedor**, que es exclusiva de Nutanix, seleccione el contenedor que especificó anteriormente para la VM de plantilla.
- Cuando crea un catálogo que contiene máquinas de **SO de sesión única**, aparece la página **Experiencia de escritorio** y le permite determinar qué ocurre cada vez que un usuario inicia sesión.



En la página **Experiencia de escritorio**, seleccione una de las siguientes opciones:

    - Los usuarios se conectan a un escritorio nuevo (aleatorio) cada vez que inician sesión.
    - Los usuarios se conectan al mismo escritorio (estático) cada vez que inician sesión.

  Si elige la primera opción, los cambios que los usuarios realicen en el escritorio se descartarán (no persistente).

  Si elige la segunda opción y utiliza MCS para aprovisionar las máquinas, puede configurar cómo se gestionan los cambios del usuario en el escritorio:

    - Guardar los cambios del usuario en el escritorio en el disco local (persistente).
    - Descartar los cambios del usuario y borrar el escritorio virtual cuando el usuario cierra la sesión (no persistente). Seleccione esta opción si utiliza la capa de personalización del usuario.

- Al actualizar la imagen maestra de un catálogo de MCS que contiene máquinas persistentes, las máquinas nuevas que se agreguen al catálogo utilizarán la imagen actualizada. Las máquinas preexistentes seguirán utilizando la imagen maestra original.

Para obtener más información, consulte la creación de catálogos de máquinas en la documentación de Citrix Virtual Apps and Desktops y la documentación de Citrix DaaS.

> **Nota:**

> Para entornos Nutanix, si el proceso de creación del catálogo de máquinas en el Delivery Controller™ tarda mucho tiempo, vaya a Nutanix Prism y encienda manualmente la máquina con el prefijo **Preparation**. Este enfoque ayuda a continuar el proceso de creación.

Paso 5: Crear un grupo de entrega

Un grupo de entrega es una colección de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica qué usuarios pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios.

Para obtener más información, consulte la creación de grupos de entrega en la documentación de Citrix Virtual Apps and Desktops y la documentación de Citrix DaaS.

> **Nota:**

Es posible que las máquinas virtuales que cree con MCS no puedan registrarse en los Citrix Cloud Connectors y aparezcan como **No registradas**. El problema ocurre cuando aloja las máquinas virtuales en Azure y se une al dominio de AD con Samba Winbind. Para solucionar el problema, siga estos pasos:

1. Vaya a la consola de edición de ADSI, seleccione una máquina virtual no registrada y edite el atributo **msDS-SupportedEncryptionTypes** de su cuenta de máquina.
2. Reinicie los servicios **ctxjproxy** y **ctxvda** en la máquina virtual. Si el estado de la máquina virtual cambia a **Registrada**, continúe con los pasos 3 a 5.
3. Abra el archivo **/var/xdl/mcs/ad_join.sh** en la máquina virtual de plantilla.
4. Agregue una línea de **net ads enctypes set $NEW_HOSTNAME\$ <Decimal value of encryption type attribute, for example, 28\> -U $NEW_HOSTNAME\$ -P password** después de las siguientes líneas dentro del archivo **/var/xdl/mcs/ad_join.sh**:

   ```
   if [ "$AD_INTEGRATION" == "winbind" ]; then

                  join_domain_samba

                  restart_service winbind /usr/bin/systemctl
   ```

5. Tome una nueva instantánea y cree máquinas virtuales utilizando la nueva plantilla.

Automatizar las actualizaciones de contraseñas de las cuentas de máquina

Las contraseñas de las cuentas de máquina, por defecto, caducan 30 días después de la creación del catálogo de máquinas. Para evitar la caducidad de las contraseñas y automatizar las actualizaciones de las contraseñas de las cuentas de máquina, haga lo siguiente:

1. Agregue la siguiente entrada a /etc/xdl/mcs/mcs.conf antes de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh.

   `UPDATE_MACHINE_PW="Y"`

2. Después de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh, abra /etc/cron.d/mcs_update_password_cronjob para establecer la hora y la frecuencia de actualización. La configuración predeterminada actualiza las contraseñas de las cuentas de máquina semanalmente a las 2:30 AM, los domingos.

Después de cada actualización de la contraseña de la cuenta de máquina, la caché de tickets en el Delivery Controller deja de ser válida y puede aparecer el siguiente error en /var/log/xdl/jproxy.log:

```
[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred. Error: Failure unspecified at GSS-API level (Mechanism level: Checksum failed)
```

Para eliminar el error, borre la caché de tickets regularmente. Puede programar una tarea de limpieza de caché en todos los Delivery Controllers o en el controlador de dominio.

Habilitar FAS en una VM creada con MCS

Si FAS no está habilitado en la máquina de plantilla como se describió anteriormente, puede habilitar FAS en cada VM creada con MCS.

Para habilitar FAS en una VM creada con MCS, haga lo siguiente:

1. Establezca las variables en /etc/xdl/mcs/mcs.conf.

   > **Nota:**
   >
   > Establezca todas las variables necesarias en `/etc/xdl/mcs/mcs.conf` porque estas variables se invocan al iniciar la VM.

   a. Establezca el valor de `Use_AD_Configuration_Files_Of_Current_VDA` en Y.

   b. Establezca las demás variables según sea necesario, como `VDI_MODE`.

2. Agregue la siguiente línea de comandos al archivo **/etc/xdl/mcs/mcs_local_setting.reg** para configurar las direcciones de su servidor FAS:

   ```
   create -k "HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force
   ```

3. Importe el certificado de CA raíz.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   ```

4. Ejecute el script `/opt/Citrix/VDA/sbin/ctxfascfg.sh`.

Crear VDA de Linux con Citrix Provisioning™

Puede crear VDA unidos a un dominio con Citrix Provisioning.

Este artículo proporciona información sobre la transmisión de dispositivos de destino Linux. Con esta función, puede aprovisionar escritorios virtuales Linux directamente en el entorno de Citrix Virtual Apps and Desktops™.

Se admiten las siguientes distribuciones de Linux:

- Ubuntu 24.04/22.04
- RHEL 9.8/9.6/9.4/8.10
- Rocky Linux 9.8/9.6/9.4/8.10

Importante:

- Asegúrese de usar SÓLO Citrix Provisioning Server LTSR 2203 (modo BIOS + UEFI) y LTSR 2402 (modo BIOS).
- Al usar Citrix Provisioning para transmitir dispositivos de destino Linux, cree una partición de arranque independiente en la imagen de disco compartido único para que los dispositivos aprovisionados puedan arrancar según lo previsto.
- Evite formatear cualquier partición con **btrfs**. GRUB2 tiene un problema intrínseco para encontrar particiones **btrfs**. **GRUB** significa **GRand Unified Bootloader**.

Para obtener más información, consulte Streaming Linux target devices en la documentación de Citrix Provisioning.

Crear VDA de Linux en Citrix DaaS Standard para Azure

Puede crear VDA de Linux unidos a un dominio y no unidos a un dominio en Citrix DaaS Standard para Azure (anteriormente Citrix Virtual Apps and Desktops Standard para Azure) para entregar aplicaciones y escritorios virtuales a cualquier dispositivo desde Microsoft Azure. Las distribuciones de Linux compatibles con Linux VDA y Azure pueden usar esta función. Para obtener más información, consulte Citrix DaaS Standard para Azure.

Paso 1: Preparar una imagen maestra en Azure

Nota:

También puede usar la función de actualización automática de Linux VDA para programar actualizaciones de software automáticas. Para lograr este objetivo, agregue líneas de comando al archivo etc/xdl/mcs/mcs_local_setting.reg en la imagen maestra. Por ejemplo, puede agregar las siguientes líneas de comando:

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_DWORD" -v "fEnabled" -d "0x00000001" --force



create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_SZ" -v "ScheduledTime" -d "Immediately" --force



create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_SZ" -v "Url" -d "&lt;Your-Azure-Container-Url>" --force



create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t
"REG_SZ" -v "CaCertificate" -d "&lt;Local-Certificate-Path-of-
PortalAzureCom>" --force
```

1. En Azure, cree una VM de Linux de una distribución compatible.
2. Instale un entorno de escritorio en la VM de Linux si es necesario.
3. En la VM, instale .NET según su distribución de Linux.

   Además de .NET Runtime, debe instalar .ASP.NET Core Runtime en todas las distribuciones de Linux compatibles antes de instalar o actualizar el VDA de Linux. La versión 6 es necesaria para Amazon Linux 2. La versión 8 es necesaria para otras distribuciones.

   Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde la fuente integrada. De lo contrario, instale .NET desde la fuente de paquetes de Microsoft. Para obtener más información, consulte `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

4. (Solo para Ubuntu) Agregue la línea `source /etc/network/interfaces.d/*` al archivo `/etc/network/interfaces`.
5. (Solo para Ubuntu) Apunte `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf` en lugar de apuntarlo a `/run/systemd/resolve/stub-resolv.conf`:

   ```
   unlink /etc/resolv.conf



   ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

6. Instale el paquete de Linux VDA.
7. Especifique una base de datos para usar.

   Puede usar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL después de instalar el paquete de Linux VDA. Para ello, complete los siguientes pasos:

   a. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si es una instalación nueva.

   b. Edite `/etc/xdl/db.conf` antes de ejecutar `deploymcs.sh`.

   Nota:

   - Recomendamos usar SQLite solo para el modo VDI.
   - Para una instalación sencilla y MCS, puede alternar entre SQLite y PostgreSQL sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de `/etc/xdl/db.conf`, el VDA de Linux utiliza PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio de PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`). Para ver un ejemplo de archivo **db.conf**, consulte Paso 7: Especificar una base de datos para usar.

> - También puede usar `/etc/xdl/db.conf` para configurar el número de puerto de PostgreSQL.

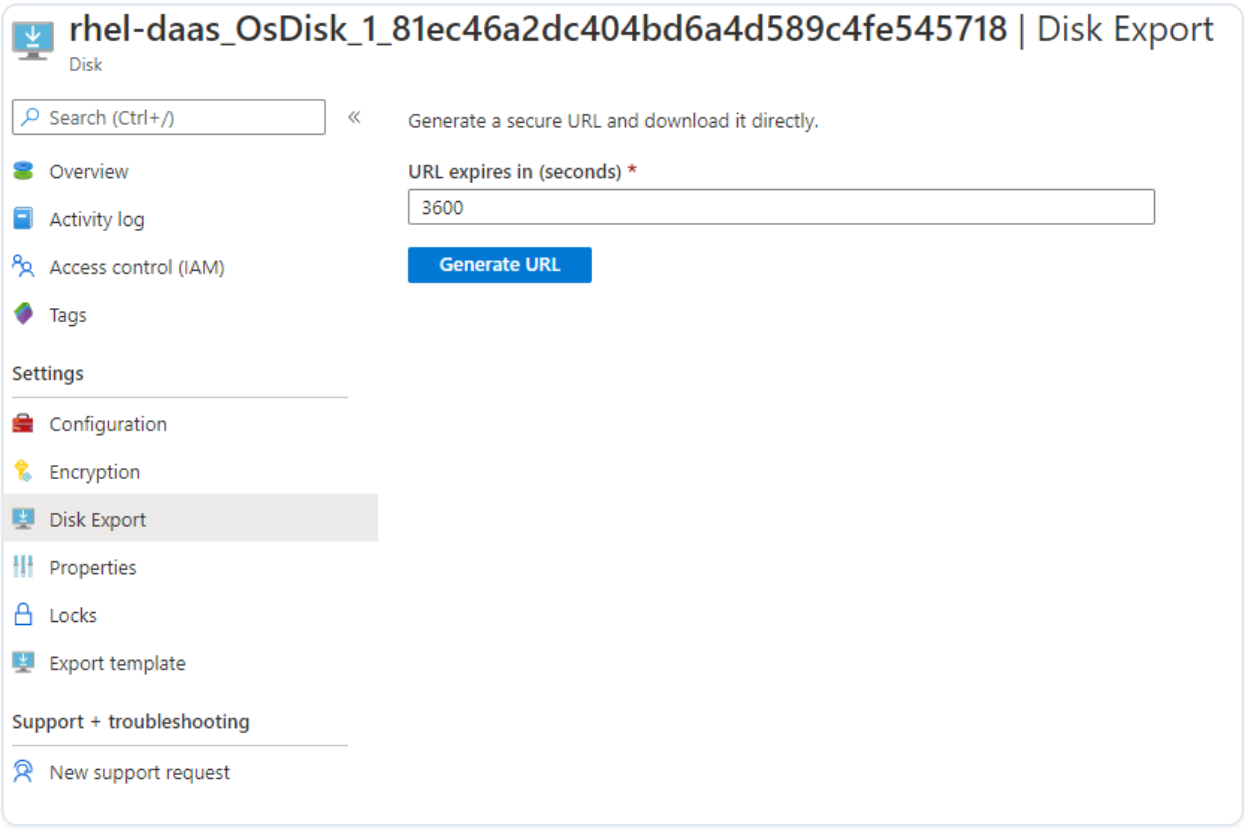
8. Cambiar las variables de MCS.

   Hay dos maneras de configurar las variables de MCS:

   - Edite el archivo `/etc/xdl/mcs/mcs.conf`.
   - Utilice la GUI de instalación sencilla. Para abrir la GUI de instalación sencilla, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su VDA de Linux.

   > **Nota:**
   >
   > Deje la variable `dns` sin especificar. Si selecciona el tipo **Estático** o **Aleatorio** al crear un catálogo de máquinas, establezca `VDI_MODE=Y`.
   >
   > Si configura las variables de MCS editando `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura las variables de MCS mediante la GUI, haga clic en **Implementar**. Después de hacer clic en **Implementar** en la GUI, las variables que haya establecido en la GUI anulan las variables que haya establecido en el archivo `/etc/xdl/mcs/mcs.conf`.

9. En Azure, detenga (o desasigne) la VM. Haga clic en **Exportar disco** para generar una URL de SAS para el archivo de disco duro virtual (VHD) que puede usar como imagen maestra para crear otras VM.



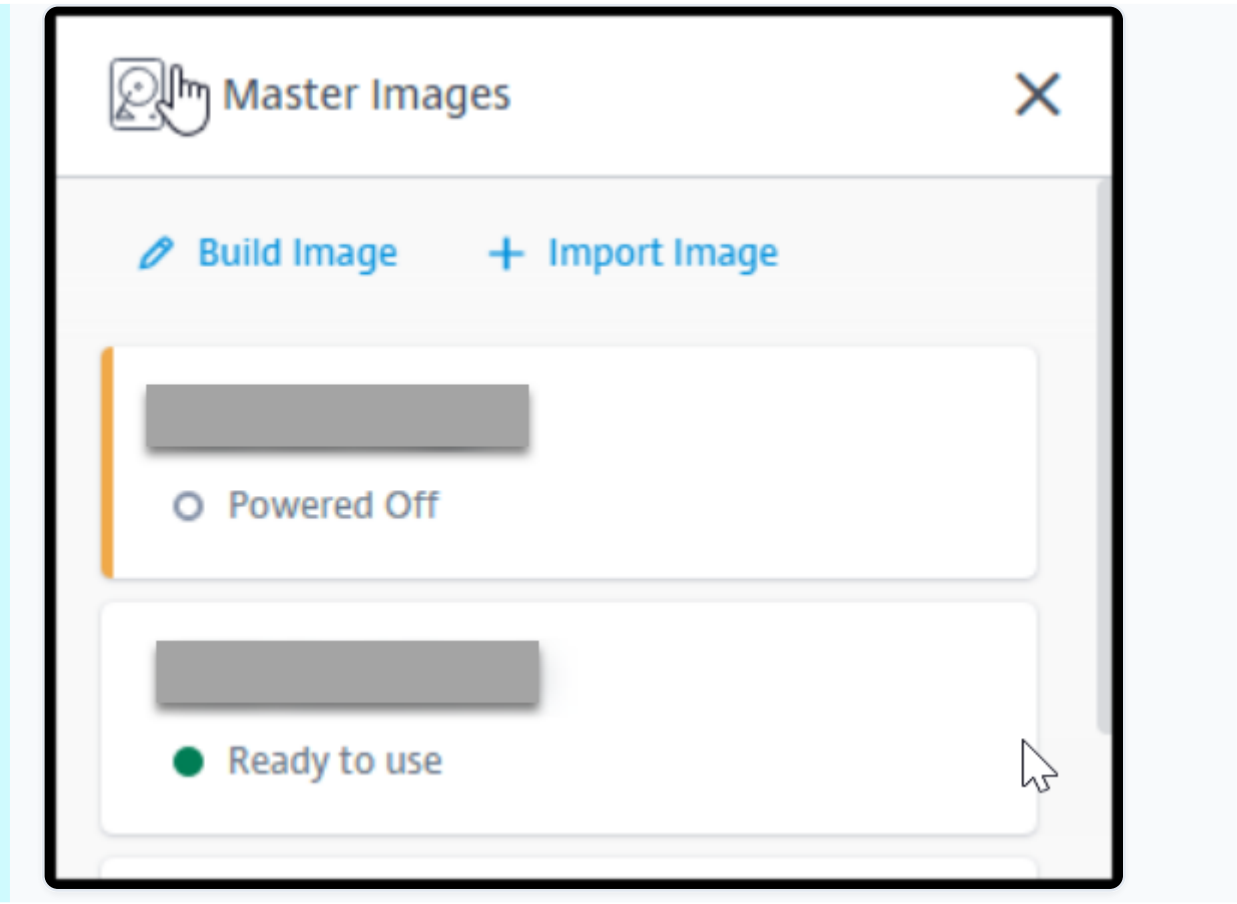
10. (Opcional) Realice la configuración de directivas de grupo en la imagen maestra. Puede usar la herramienta `ctxreg` para realizar la configuración de directivas de grupo. Por ejemplo, el siguiente comando habilita la directiva **Crear automáticamente impresora universal PDF** para la impresión de PDF.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\GroupPolicy\Defaults\PrintingPolicies" -t
"REG_DWORD" -v "AutoCreatePDFPrinter" -d "0x00000001" --force
```

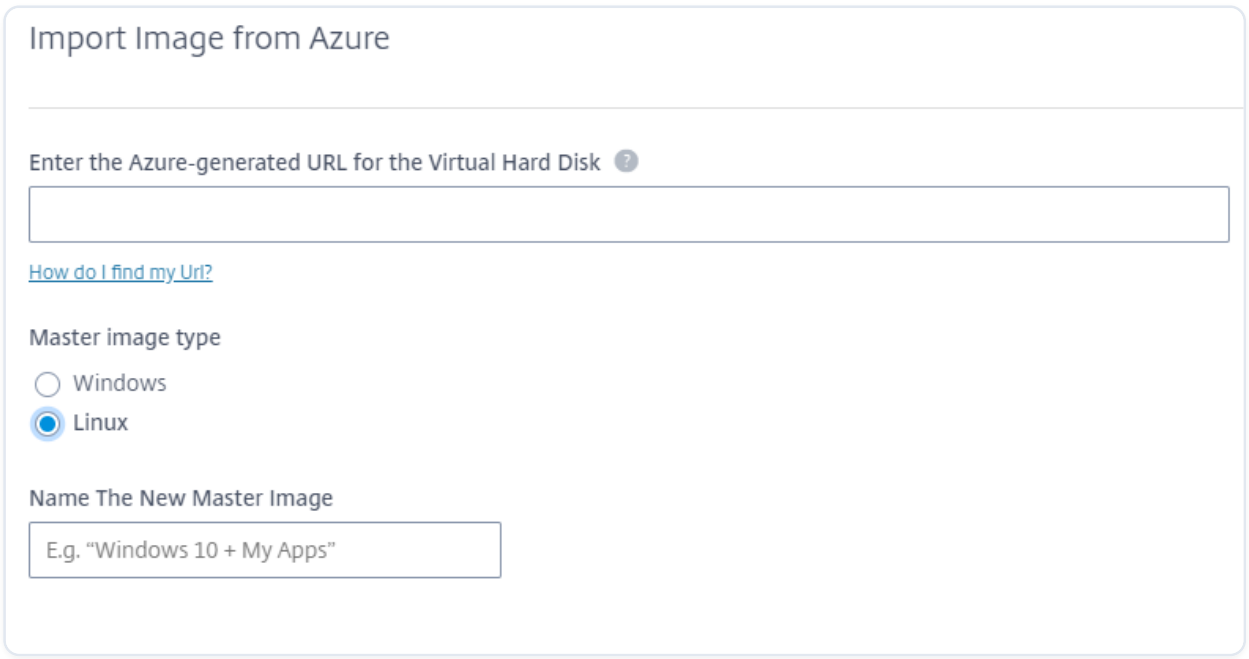
Paso 2: Importar la imagen maestra desde Azure

1. En el panel de control de Administrar, expanda **Imágenes maestras** a la derecha. La pantalla muestra las imágenes maestras que proporciona Citrix y las imágenes que usted ha creado e importado.

> **Sugerencia:**
>
> La mayoría de las actividades de administrador para este servicio se gestionan a través de los paneles **Manage** y **Monitor**. Después de crear su primer catálogo, el panel **Manage** se inicia automáticamente después de iniciar sesión en Citrix Cloud™ y seleccionar el servicio **Managed Desktops**.



2. Haga clic en **Importar imagen**.
3. Introduzca la URL SAS del archivo VHD que generó en Azure. Seleccione **Linux** para el tipo de imagen maestra.



4. Siga las instrucciones del asistente para completar la importación de la imagen maestra.

Paso 3: Crear un catálogo de máquinas

Acceda al panel **Manage** y haga clic en **Crear catálogo**. Al crear el Catálogo de máquinas, elija la imagen maestra que creó anteriormente.

> **Nota:**

> La VM utilizada como imagen maestra no es accesible a través de SSH o RDP. Para acceder a la VM, utilice la Consola serie en el portal de Azure.

Instalar el VDA de Linux manualmente

Puede instalar el VDA de Linux manualmente en las siguientes distribuciones de Linux:

- Amazon Linux 2, CentOS, RHEL y Rocky Linux
- SUSE
- Ubuntu
- Debian

Instalar el VDA de Linux en RHEL y Rocky Linux manualmente

> **Importante:**

> Para instalaciones nuevas, recomendamos usar instalación fácil para una instalación rápida. La instalación fácil ahorra tiempo y trabajo, y es menos propensa a errores que la instalación manual detallada en este artículo.

Paso 1: Preparar la información de configuración y la máquina Linux

Paso 1a: verificar la configuración de red

Asegúrese de que la red esté conectada y configurada correctamente. Por ejemplo, debe configurar el servidor DNS en el VDA de Linux.

Paso 1b: Establecer el nombre de host

Para asegurarse de que el nombre de host de la máquina se informe correctamente, cambie el archivo **/etc/hostname** para que contenga solo el nombre de host de la máquina.

`hostname`

Paso 1c: Asignar una dirección de bucle invertido al nombre de host

Para asegurarse de que el nombre de dominio DNS y el nombre de dominio completo (FQDN) de la máquina se informen correctamente, cambie la siguiente línea del archivo `/etc/hosts` para incluir el FQDN y el nombre de host como las dos primeras entradas:

```
127.0.0.1 hostname-fqdn hostname localhost localhost.localdomain localhost4 localhost4.localdomain4
```

Por ejemplo:

```
127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4
```

Elimine cualquier otra referencia a **hostname-fqdn** o **hostname** de otras entradas del archivo.

> **Nota:**

> El VDA de Linux actualmente no admite la truncación de nombres NetBIOS. El nombre de host no debe exceder los 15 caracteres.

> **Sugerencia:**

> Utilice solo caracteres a–z, A–Z, 0–9 y guiones (-). Evite los guiones bajos (_), los espacios y otros símbolos. No inicie un nombre de host con un número ni lo termine con un guion. Esta regla también se aplica a los nombres de host de Delivery Controller.

Paso 1d: Comprobar el nombre de host

verificar que el nombre de host está configurado correctamente:

```
hostname
```

Este comando devuelve solo el nombre de host de la máquina y no su nombre de dominio completo (FQDN).

verificar que el FQDN esté configurado correctamente:

```
hostname -f
```

Este comando devuelve el FQDN de la máquina.

Paso 1e: Comprobar la resolución de nombres y la accesibilidad del servicio

verificar que puede resolver el FQDN y hacer ping al controlador de dominio y a Delivery Controller™:

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

Si no puede resolver el FQDN o hacer ping a ninguna de estas máquinas, revise los pasos antes de continuar.

Paso 1f: Configurar la sincronización del reloj

Mantener una sincronización precisa del reloj entre los VDA, los Delivery Controllers y los controladores de dominio es crucial. Alojar el Linux VDA como máquina virtual (VM) puede causar problemas de desviación del reloj. Por esta razón, se prefiere sincronizar la hora con un servicio de hora remoto.

Un entorno predeterminado de RHEL utiliza el demonio Chrony (`chronyd`) para la sincronización del reloj.

CONFIGURAR EL SERVICIO CHRONY

Como usuario root, edite **/etc/chrony.conf** y añada una entrada de servidor para cada servidor de hora remoto:

```
server peer1-fqdn-or-ip-address iburst



server peer2-fqdn-or-ip-address iburst
```

En una implementación típica, sincronice la hora desde los controladores de dominio locales y no directamente desde los servidores públicos del grupo NTP. Añada una entrada de servidor para cada controlador de dominio de Active Directory en el dominio.

Elimine cualquier otra entrada de servidor listada, incluidas las direcciones IP de bucle invertido, localhost y las entradas de servidor público ***.pool.ntp.org**.

Guarde los cambios y reinicie el demonio Chrony:

```
sudo systemctl restart chronyd
```

Paso 1g: Instalar y especificar una base de datos para usar

Nota:

- Recomendamos usar SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el VDA de Linux utiliza PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).
- Para instalaciones manuales, debe instalar SQLite, PostgreSQL o ambos manualmente. Puede utilizar una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux. Si instala tanto SQLite como PostgreSQL, puede especificar uno de ellos para usar editando **/etc/xdl/db.conf** después de instalar el paquete VDA de Linux.

INSTALAR POSTGRESQL

Esta sección describe cómo instalar la versión de PostgreSQL proporcionada por su distribución de Linux. Si es necesaria una versión personalizada de PostgreSQL, puede instalarla según sus requisitos específicos.

Ejecute los siguientes comandos para instalar PostgreSQL:

```
sudo yum -y install postgresql-server



sudo yum -y install postgresql-jdbc
```

Para RHEL 8.x y RHEL 9.8/9.6/9.4, ejecute el siguiente comando para instalar `libpq` para PostgreSQL:

```
sudo yum -y install libpq
```

Ejecute el siguiente comando para inicializar la base de datos. Esta acción crea archivos de base de datos en **/var/lib/pgsql/data**.

```
sudo postgresql-setup initdb
```

Ejecute los siguientes comandos para iniciar PostgreSQL al iniciar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

Compruebe la versión de PostgreSQL usando:

```
psql --version
```

INSTALAR SQLITE

Ejecute el siguiente comando para instalar SQLite:

```
sudo yum -y install sqlite
```

ESPECIFICAR UNA BASE DE DATOS PARA USAR

Si instala tanto SQLite como PostgreSQL, puede especificar uno de ellos para usar editando **/etc/xdl/db.conf** después de instalar el paquete VDA de Linux.

1. Ejecute **/opt/Citrix/VDA/sbin/ctxcleanup.sh**. Omita este paso si es una instalación nueva.
2. Edite **/etc/xdl/db.conf** para especificar una base de datos a usar. El siguiente es un ejemplo de archivo **db.conf**:

```
# database configuration file for Linux VDA



## database choice

# possible choices are:

#     SQLite

#     PostgreSQL

# default choice is PostgreSQL

DbType="PostgreSQL"




## database port

# specify database port for the database.

# if not specified, default port will be used:

# SQLite: N/A

# PostgreSQL: 5432

DbPort=5432
```

```
## PostgreSQL customized
# only the following value means true, otherwise false:
#     true
#     yes
#     y
#     YES
#     Y
# default is false
DbCustomizePostgreSQL=false

## PostgreSQL service name
# specify the service name of PostgreSQL for Linux VDA
# default is "postgresql"
DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

3. Ejecute **ctxsetup.sh**.

Nota:

También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

Paso 2: Preparar el hipervisor

Se requieren algunos cambios al ejecutar el VDA de Linux como una VM en un hipervisor compatible. Realice los siguientes cambios según la plataforma de hipervisor en uso. No se requieren cambios si ejecuta la máquina Linux en hardware físico.

Corregir la sincronización de la hora en XenServer (anteriormente Citrix Hypervisor™)

Cuando la función de sincronización de hora de XenServer® está habilitada, dentro de cada VM Linux paravirtualizada, experimenta problemas con NTP y XenServer. Ambos intentan administrar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con NTP. Este caso requiere deshabilitar la sincronización de hora del host. No se requieren cambios en el modo HVM.

Si ejecuta un kernel de Linux paravirtualizado con las herramientas de VM de XenServer instaladas, puede comprobar si la función de sincronización de hora de XenServer está presente y habilitada desde la VM de Linux:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve 0 o 1:

- 0 - La función de sincronización de hora está habilitada y debe deshabilitarse.
- 1 - La función de sincronización de hora está deshabilitada y no se requiere ninguna acción adicional.

Si el archivo /proc/sys/xen/independent_wallclock no está presente, los siguientes pasos no son necesarios.

Si está habilitada, deshabilite la función de sincronización de hora escribiendo 1 en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Para que este cambio sea permanente y persistente después de reiniciar, edite el archivo **/etc/sysctl.conf** y agregue la línea:

`xen.independent_wallclock = 1`

Para verificar estos cambios, reinicie el sistema:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve el valor 1.

Corregir la sincronización de la hora en Microsoft Hyper-V

Las máquinas virtuales Linux con los servicios de integración de Hyper-V Linux instalados pueden aplicar la función de sincronización de hora de Hyper-V para usar la hora del sistema operativo host. Para asegurarse de que el reloj del sistema siga siendo preciso, debe habilitar esta función junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para la configuración de una máquina virtual Linux, seleccione **Integration Services**.
3. Asegúrese de que la opción **Time synchronization** esté seleccionada.

> **Nota:**
>
> Este enfoque es diferente de VMware y XenServer (anteriormente Citrix Hypervisor), donde la sincronización de la hora del host está inhabilitada para evitar conflictos con NTP. La sincronización de la hora de Hyper-V puede coexistir y complementar la sincronización de la hora de NTP.

Corregir la sincronización de la hora en ESX y ESXi

Cuando la función de sincronización de hora de VMware está habilitada, dentro de cada máquina virtual Linux paravirtualizada, experimenta problemas con el NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con el NTP. Este caso requiere inhabilitar la sincronización de la hora del host.

Si está ejecutando un kernel de Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Edite la configuración de la máquina virtual Linux.
3. En el cuadro de diálogo **Virtual Machine Properties**, abra la ficha **Options**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Avanzado**, desactive **Sincronizar la hora del invitado con la del host**.

Paso 3: Añadir la VM Linux al dominio de Windows

Los siguientes métodos están disponibles para añadir máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Quest Authentication Services
- Centrify DirectControl
- SSSD
- PBIS

Siga las instrucciones según el método elegido.

> **Nota:**
>
> Los inicios de sesión pueden fallar cuando se utiliza el mismo nombre de usuario para la cuenta local en el VDA de Linux y la cuenta en AD.

Samba Winbind

Para RHEL 9.x y Rocky Linux 9.x, ejecute el siguiente comando para evitar que **pam_winbind** cambie la propiedad del directorio raíz:

```
usermod -d /nonexistent nobody
```

Instale o actualice los paquetes necesarios:

Para RHEL 9.x/8.x y Rocky Linux 9.x/8.x:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
oddjob-mkhomedir realmd authselect
```

HABILITAR EL DEMONIO WINBIND PARA QUE SE INICIE AL ARRANCAR LA MÁQUINA

El demonio Winbind debe configurarse para iniciarse al arrancar la máquina:

```
sudo /sbin/chkconfig winbind on
```

CONFIGURAR LA AUTENTICACIÓN DE WINBIND

Configure la máquina para la autenticación Kerberos mediante Winbind:

1. Ejecute el siguiente comando.

   Para RHEL 9.x/8.x y Rocky Linux 9.x/8.x:

   ```
   sudo authselect select winbind with-mkhomedir --force
   ```

2. Abra **/etc/samba/smb.conf** y añada las siguientes entradas en la sección \[Global\], pero después de la sección generada por la herramienta `authconfig`:

   `kerberos method = secrets and keytab`

   `winbind refresh tickets = true` `winbind offline logon = no`

3. (Solo para RHEL 9.x/8.x y Rocky Linux 9.x/8.x) Abra **/etc/krb5.conf** y añada entradas en las secciones `[libdefaults]`, `[realms]` y `[domain_realm]`:

   En la sección `[libdefaults]`:

   `default_ccache_name = FILE:/tmp/krb5cc_%{uid}`

   `default_realm = REALM` `dns_lookup_kdc = true`

   En la sección `[realms]`:

   `REALM = {`

   `kdc = fqdn-of-domain-controller` `}`

   En la sección `[domain_realm]`:

   `realm = REALM`

   `.realm = REALM`

El VDA de Linux requiere el archivo keytab del sistema /etc/krb5.keytab para autenticarse y registrarse en el Delivery Controller. La configuración anterior del método Kerberos obliga a

Winbind a crear el archivo keytab del sistema cuando la máquina se une por primera vez al dominio.

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para añadir equipos al dominio.

Para añadir una VM de Linux al dominio de Windows, ejecute el siguiente comando:

```
sudo realm join -U user --client-software=winbind REALM
```

REALM es el nombre del reino Kerberos en mayúsculas, y **user** es un usuario de dominio que tiene permisos para añadir equipos al dominio.

CONFIGURAR PAM PARA WINBIND

Por defecto, la configuración del módulo PAM de Winbind (pam_winbind) no habilita el almacenamiento en caché de tickets Kerberos ni la creación de directorios de inicio. Abra **/etc/security/pam_winbind.conf** y añada o cambie las siguientes entradas en la sección \[Global\]:

`krb5_auth = yes`

`krb5_ccache_type = FILE` `mkhomedir = yes`

Asegúrese de que se eliminen los puntos y coma iniciales de cada configuración. Estos cambios requieren reiniciar el demonio de Winbind:

```
sudo systemctl restart winbind
```

> **Sugerencia:**

> El demonio `winbind` permanece en ejecución solo si la máquina está unida a un dominio.

> Abra **/etc/krb5.conf** y cambie la siguiente configuración en la sección \[libdefaults\] de tipo KEYRING a tipo FILE:

`default_ccache_name = FILE:/tmp/krb5cc_%{uid}`

Para RHEL 9.x y Rocky Linux 9.x, ejecute los siguientes comandos para resolver el problema de SELinux con Winbind:

```
ausearch -c 'winbindd' --raw | audit2allow -M my-winbindd -p /etc/selinux/
targeted/policy/policy.*



semodule -X 300 -i my-winbindd.pp
```

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en **Active Directory**.

Ejecute el comando **net ads** de **Samba** para verificar que la máquina está unida a un dominio:

```
sudo net ads testjoin
```

Ejecute el siguiente comando para verificar información adicional del dominio y del objeto de equipo:

```
sudo net ads info
```

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Para asegurarse de que Kerberos está configurado correctamente para su uso con el VDA de Linux, verificar que el archivo keytab del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las diversas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando Kerberos `kinit` para autenticar la máquina con el controlador de dominio utilizando estas claves:

```
sudo kinit -k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución de la shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utiliza el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT para la cuenta de la máquina se ha almacenado en caché utilizando:

```
sudo klist
```

Examine los detalles de la cuenta de la máquina utilizando:

```
sudo net ads status
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Utilice la herramienta **wbinfo** para verificar que los usuarios del dominio pueden autenticarse con el dominio:

```
wbinfo --krb5auth=domain\\username%password
```

El dominio especificado aquí es el nombre de dominio de AD, no el nombre de reino de Kerberos. Para el shell bash, el carácter de barra invertida (\\) debe escaparse con otra barra invertida. Este comando devuelve un mensaje que indica éxito o fracaso.

Para verificar que el módulo PAM de Winbind está configurado correctamente, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username

id -u
```

verificar que los tickets en la caché de credenciales de Kerberos son válidos y no han caducado:

```
klist
```

Salga de la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de unión al dominio.

Servicios de autenticación de Quest

CONFIGURAR QUEST EN EL CONTROLADOR DE DOMINIO

Suponga que ha instalado y configurado el software Quest en los controladores de dominio de Active Directory y que se le han concedido privilegios administrativos para crear objetos de equipo en Active Directory.

PERMITIR QUE LOS USUARIOS DEL DOMINIO INICIEN SESIÓN EN MÁQUINAS LINUX VDA

Para permitir que los usuarios del dominio establezcan sesiones HDX™ en una máquina Linux VDA:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory para esa cuenta de usuario.
2. Seleccione la pestaña **Unix Account**.
3. Marque **Unix-enabled**.
4. Establezca el **Número GID principal** en el ID de grupo de un grupo de usuarios de dominio real.

> **Nota:**
>
> Estas instrucciones son equivalentes para configurar usuarios de dominio para el inicio de sesión mediante la consola, RDP, SSH o cualquier otro protocolo de acceso remoto.

CONFIGURAR QUEST EN LINUX VDA

Solucionar la aplicación de la política de SELinux
El entorno RHEL predeterminado tiene SELinux totalmente aplicado. Esta aplicación interfiere con los mecanismos IPC de socket de dominio de Unix utilizados por Quest e impide que los usuarios de dominio inicien sesión.

La forma conveniente de solucionar este problema es deshabilitar SELinux. Como usuario root, edite **/etc/selinux/config** y cambie la configuración de **SELinux**:

`SELINUX=permissive`

Este cambio requiere un reinicio de la máquina:

```
reboot
```

Importante:

Utilice esta configuración con precaución. Volver a habilitar la aplicación de la política de SELinux después de deshabilitarla puede provocar un bloqueo completo, incluso para el usuario root y otros usuarios locales.

CONFIGURAR EL DEMONIO VAS

La renovación automática de los tickets de Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar deshabilitada.

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Este comando establece el intervalo de renovación en nueve horas (32.400 segundos), lo que es una hora menos que la vida útil predeterminada del ticket de 10 horas. Establezca este parámetro en un valor inferior en sistemas con una vida útil del ticket más corta.

CONFIGURAR PAM Y NSS

Para habilitar el inicio de sesión de usuarios de dominio a través de HDX y otros servicios como su, ssh y RDP, ejecute los siguientes comandos para configurar PAM y NSS manualmente:

```
sudo /opt/quest/bin/vastool configure pam



sudo /opt/quest/bin/vastool configure nss
```

UNIRSE AL DOMINIO DE WINDOWS

Una la máquina Linux al dominio de Active Directory utilizando el comando **vastool** de Quest:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

El usuario es cualquier usuario de dominio que tenga permisos para unir equipos al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Reinicie la máquina Linux después de unirse al dominio.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para verificar que una máquina Linux unida a Quest está en el dominio:

```
sudo /opt/quest/bin/vastool info domain
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. Si la máquina no está unida a ningún dominio, aparece el siguiente error:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Para verificar que Quest puede autenticar a los usuarios del dominio a través de PAM, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username

id -u
```

verificar que se ha creado un archivo de caché de credenciales Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets en la caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
```

Cierre la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Centrify DirectControl

UNIR UN DOMINIO DE WINDOWS

Con el agente Centrify DirectControl instalado, una la máquina Linux al dominio de Active Directory mediante el comando Centrify `adjoin`:

```
su –

adjoin -w -V -u user domain-name
```

El parámetro de usuario es cualquier usuario de dominio de Active Directory que tenga permisos para unir equipos al dominio de Active Directory. El **nombre de dominio** es el nombre del dominio al que se unirá la máquina Linux.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en Active Directory. Para verificar que una máquina Linux unida a Centrify está en el dominio:

```
su –

adinfo
```

verificar que el valor de Joined to domain es válido y que el modo CentrifyDC devuelve conectado. Si el modo se queda atascado en el estado inicial, el cliente de Centrify está experimentando problemas de conexión o autenticación con el servidor.

Hay disponible información de diagnóstico y del sistema más completa mediante:

```
adinfo --sysinfo all

adinfo –diag
```

Pruebe la conectividad con los distintos servicios de Active Directory y Kerberos.

```
adinfo --test
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

SSSD

Si utiliza SSSD, siga las instrucciones de esta sección. Esta sección incluye instrucciones para unir una máquina VDA de Linux a un dominio de Windows y proporciona orientación para configurar la autenticación Kerberos.

Para configurar SSSD en RHEL, haga lo siguiente:

1. Unir el dominio y crear un keytab de host
2. Configurar SSSD
3. Habilitar SSSD
4. verificar la configuración de Kerberos
5. verificar la autenticación de usuario

UNIR EL DOMINIO Y CREAR UN KEYTAB DE HOST

SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo keytab del sistema. En su lugar, puede usar **adcli**, **realmd** o **Samba**.

Esta sección describe el enfoque `adcli` para RHEL 8.x/9.x y Rocky Linux 8.x/9.x. Para **realmd**, consulte la documentación de RHEL. Estos pasos deben seguirse antes de configurar SSSD.

- **Adcli (RHEL 9.x/8.x y Rocky Linux 9.x/8.x):**

  Instale o actualice los paquetes necesarios:

  ```
  sudo yum -y install samba-common samba-common-tools krb5-workstation
  authconfig oddjob-mkhomedir realmd oddjob authselect
  ```

  Configure la máquina para la autenticación de **Samba** y Kerberos:

  ```
  sudo authselect select sssd with-mkhomedir --force
  ```

  Abra **/etc/krb5.conf** y agregue las entradas en las secciones y .

En la sección :

`REALM = {`

`kdc = fqdn-of-domain-controller` `}`

En la sección :

`realm = REALM` `.realm = REALM`

Únase al dominio de Windows. Asegúrese de que su controlador de dominio sea accesible y de que tenga una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
sudo realm join REALM -U user
```

REALM es el nombre del reino de Kerberos en mayúsculas y **user** es un usuario de dominio que tiene permisos para agregar equipos al dominio.

CONFIGURAR SSSD

La configuración de SSSD consta de los siguientes pasos:

- Instale el paquete **sssd-ad** en el VDA de Linux ejecutando el comando `sudo yum -y install sssd`.
- Realice cambios de configuración en varios archivos (por ejemplo, sssd.conf).
- Inicie el servicio **sssd**.

(Solo RHEL 9.x/8.x y Rocky Linux 9.x/8.x) Abra **/etc/sssd/sssd.conf** y añada las siguientes entradas en la sección :

`ad_gpo_access_control = permissive`

`full_name_format = %2$s\%1$s` `fallback_homedir = /home/%d/%u`

`# Kerberos settings` `krb5_ccachedir = /tmp`

`krb5_ccname_template = FILE:%d/krb5cc_%U`

Sustituya **ad.example.com**, **server.ad.example.com** por los valores correspondientes. Para obtener más información, consulte sssd-ad(5) - Linux man page.

Establezca la propiedad y los permisos del archivo sssd.conf:

`chown root:root /etc/sssd/sssd.conf`

`chmod 0600 /etc/sssd/sssd.conf` `restorecon /etc/sssd/sssd.conf`

HABILITAR SSSD

Para RHEL 9.x/8.x y Rocky Linux 9.x/8.x:

Ejecute los siguientes comandos para habilitar SSSD:

```
sudo systemctl restart sssd

sudo systemctl enable sssd.service

sudo chkconfig sssd on
```

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

verificar que el archivo **keytab** del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando Kerberos **kinit** para autenticar la máquina con el controlador de dominio mediante estas claves:

```
sudo kinit –k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar (**$**) debe escaparse con una barra invertida (****) para evitar la sustitución de shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utiliza el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT de la cuenta de la máquina se ha almacenado en caché mediante:

```
sudo klist
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Utilice el comando **getent** para verificar que el formato de inicio de sesión es compatible y que el NSS funciona:

```
sudo getent passwd DOMAIN\\username
```

El parámetro **DOMAIN** indica el nombre de dominio de versión corta. Si se necesita otro formato de inicio de sesión, verificar primero con el comando **getent**.

Los formatos de inicio de sesión admitidos son:

- Nombre de inicio de sesión de nivel inferior: `DOMAIN\username`
- UPN: `username@domain.com`
- Formato de sufijo NetBIOS: `username@DOMAIN`

Para verificar que el módulo PAM de SSSD está configurado correctamente, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
sudo ssh localhost –l DOMAIN\\username



id -u
```

verificar que se creó un archivo de caché de credenciales de Kerberos correspondiente para el **uid** devuelto por el comando:

```
ls /tmp/krb5cc_{uid}
```

verificar que los tickets en la caché de credenciales de Kerberos del usuario son válidos y no han caducado.

```
klist
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

PBIS

DESCARGAR EL PAQUETE PBIS NECESARIO

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

HACER EJECUTABLE EL SCRIPT DE INSTALACIÓN DE PBIS

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

EJECUTAR EL SCRIPT DE INSTALACIÓN DE PBIS

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
/opt/pbis/bin/domainjoin-cli join domain-name user
```

El **usuario** es un usuario de dominio que tiene permisos para agregar equipos al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Nota: Para establecer Bash como shell predeterminado, ejecute el comando **/opt/pbis/bin/config LoginShellTemplate/bin/bash**.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en Active Directory. Para verificar que una máquina Linux unida a PBIS está en el dominio:

```
/opt/pbis/bin/domainjoin-cli query
```

Si la máquina está unida a un dominio, este comando devuelve la información sobre el dominio de AD y la OU a los que está unida actualmente. De lo contrario, solo aparece el nombre de host.

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Para verificar que PBIS puede autenticar a los usuarios del dominio a través de PAM, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\user
```

```
id -u
```

verificar que se ha creado un archivo de caché de credenciales de Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

Salga de la sesión.

```
exit
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Paso 4: Instalar .NET

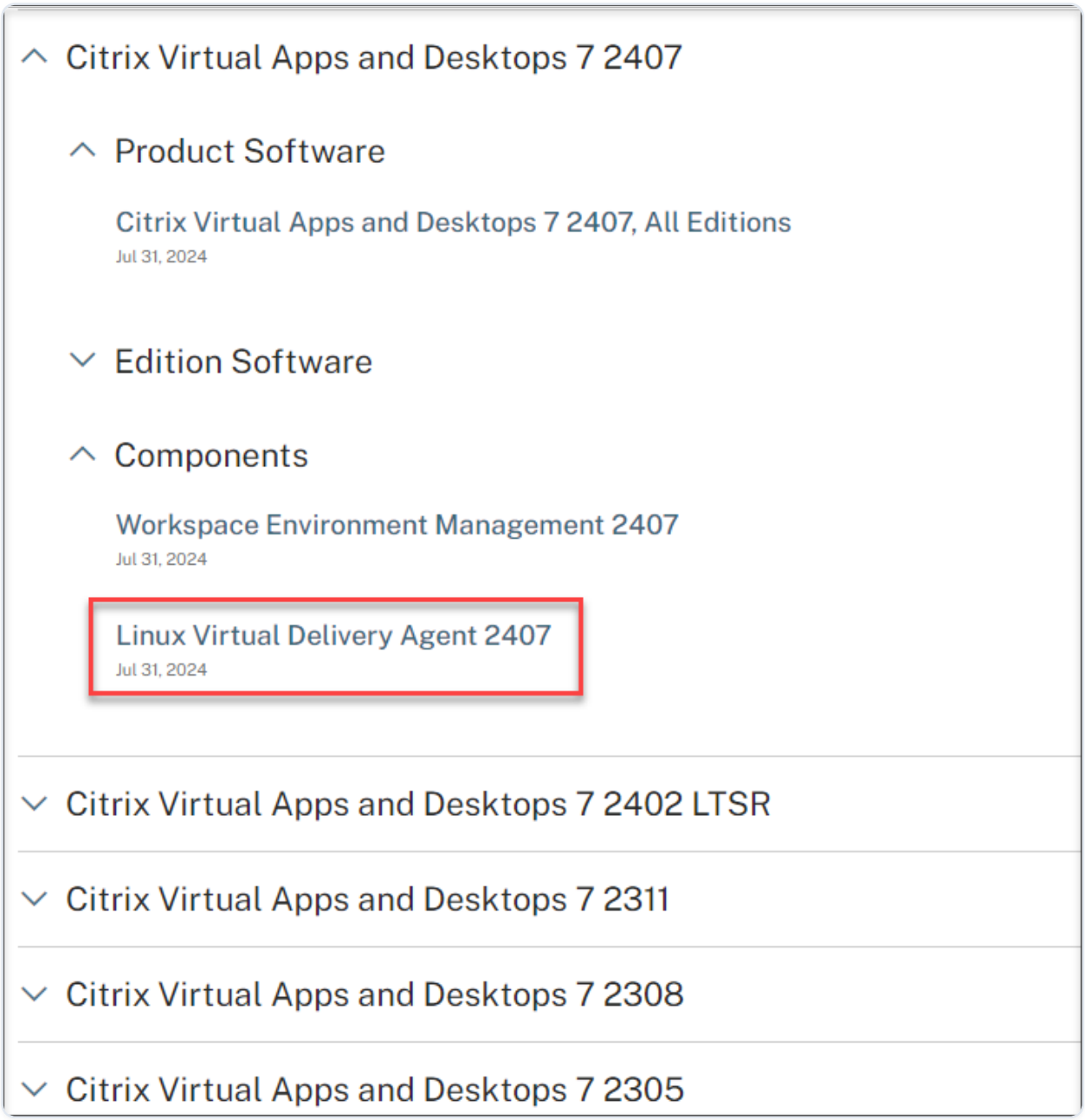
Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Después de instalar .NET, ejecute el comando **which dotnet** para encontrar la ruta de tiempo de ejecución.

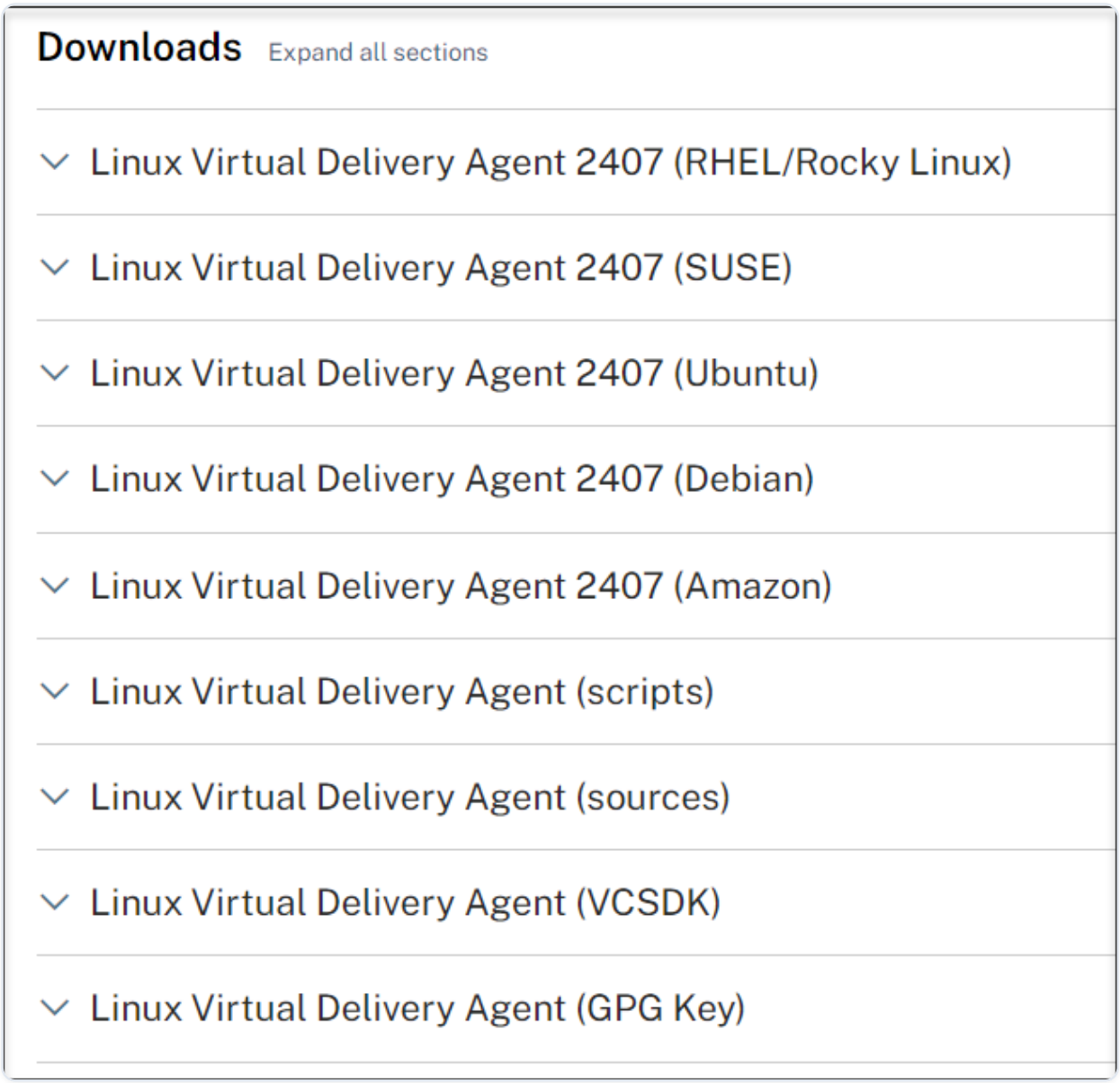
Según la salida del comando, establezca la ruta binaria de tiempo de ejecución de .NET. Por ejemplo, si la salida del comando es /aa/bb/dotnet, use /aa/bb como ruta binaria de .NET.

Paso 5: Descargar el paquete del VDA de Linux

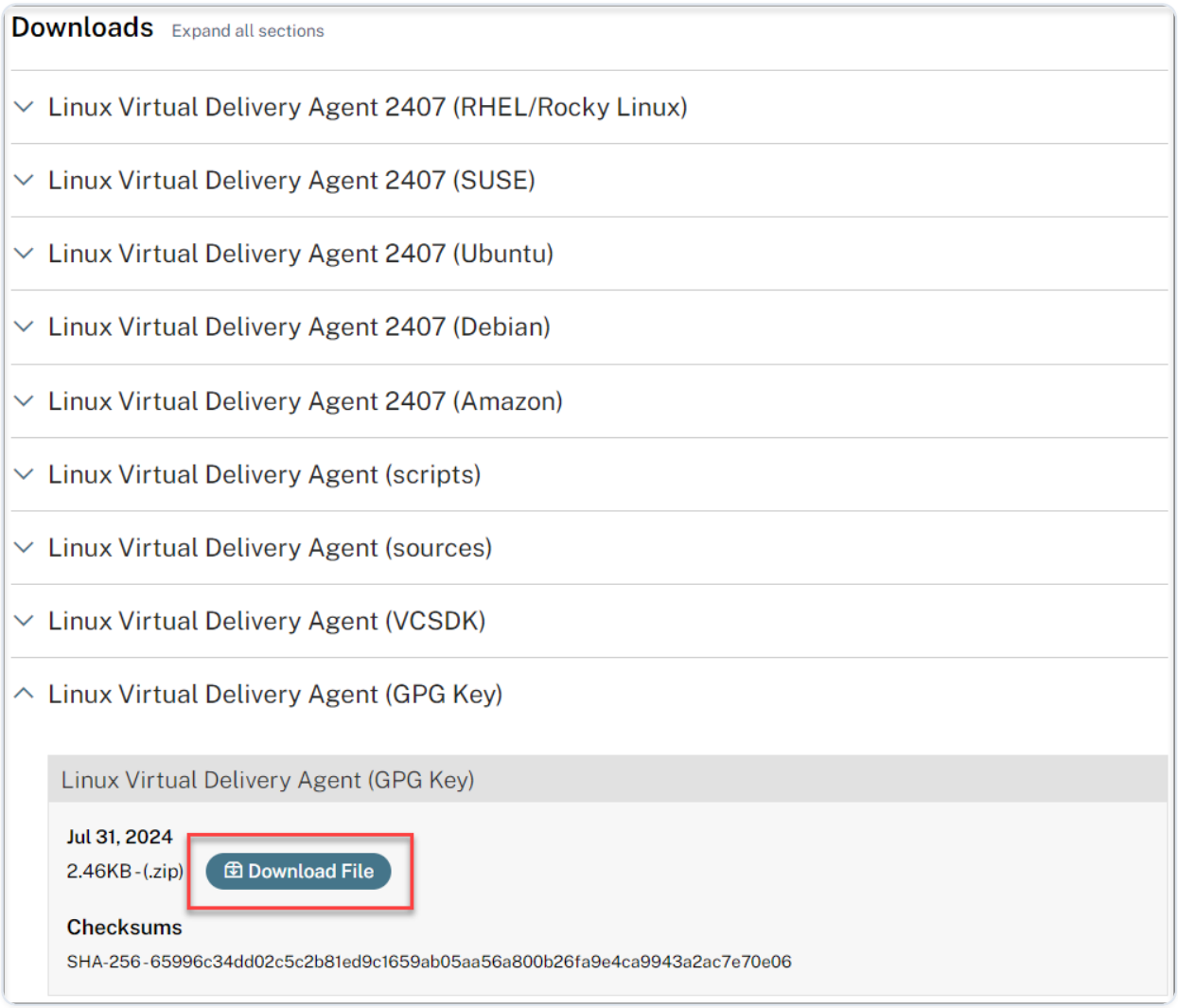
1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Expanda **Componentes** para encontrar el VDA de Linux. Por ejemplo:



4. Haga clic en el enlace del VDA de Linux para acceder a las descargas del VDA de Linux.



5. Descargue el paquete del VDA de Linux que coincida con su distribución de Linux.
6. Descargue la clave pública GPG que puede usar para verificar la integridad del paquete del VDA de Linux. Por ejemplo:



Para verificar la integridad del paquete del VDA de Linux, ejecute los siguientes comandos para importar la clave pública en la base de datos RPM y comprobar la integridad del paquete:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

Paso 6: Instalar el VDA de Linux

Puede realizar una instalación nueva o actualizar una instalación existente. El VDA de Linux admite actualizaciones desde la versión más reciente. Por ejemplo, puede actualizar el VDA de Linux de 2308 a 2311 y de 1912 LTSR a 2203 LTSR.

Paso 6a: Realizar una instalación nueva

1. (Opcional) Desinstale la versión anterior.

   Si instaló una versión anterior que no sea las dos anteriores y una versión LTSR, desinstálela antes de instalar la nueva versión.

a. Detenga los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

Nota:

Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que detuvo.

b. Desinstale el paquete:

```
sudo rpm -e XenDesktopVDA
```

Nota:

Para ejecutar un comando, se necesita la ruta completa; alternativamente, puede agregar **/opt/Citrix/VDA/sbin** y **/opt/Citrix/VDA/bin** a la ruta del sistema.

2. Descargue el paquete de Linux VDA.

   Vaya a la página de descarga de Citrix Virtual Apps and Desktops. Expanda la versión adecuada de Citrix Virtual Apps and Desktops y haga clic en **Components** para descargar el paquete de Linux VDA que coincida con su distribución de Linux.

3. Instale el software de Linux VDA mediante `Yum`.

Nota:

- Para RHEL y Rocky Linux, instale el repositorio EPEL antes de poder instalar Linux VDA correctamente. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en `<https://docs.fedoraproject.org/es-es/epel/>`.
- Antes de instalar Linux VDA en RHEL 9.4/9.2 y Rocky Linux 9.4/9.2, actualice el paquete **libsepol** a la versión 3.4 o posterior.

Para RHEL 9.x y Rocky Linux 9.x:

```
sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

Para RHEL 8.x y Rocky Linux 8.x:

```
sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

Lista de dependencias RPM para RHEL 9.x y Rocky Linux 9.x:

```
gtk2 >= 2.24.33

java-17-openjdk >= 17

tzdata-java >= 2022

ImageMagick >= 6.9

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8
```

```
dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7

ibus >= 1.5

nss-tools >= 3.44.0

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~
```

```
qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9

fuse-libs >= 2.9

pulseaudio-utils >= 15.0
```

Lista de dependencias RPM para RHEL 8.x y Rocky Linux 8.x:

```
java-17-openjdk >= 17

ImageMagick >= 6.9

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12
```

```
libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

depends_on sed >= 4.5

pulseaudio >= 14.0

pulseaudio-module-x11 >= 14.0

pulseaudio-module-bluetooth >= 14.0

alsa-plugins-pulseaudio >= 1.1.9

cups >= 1.6.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1
```

```
python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9

fuse-libs >= 2.9
```

Nota:

Para ver una matriz de las distribuciones de Linux y las versiones de Xorg que admite esta versión de Linux VDA, consulte Requisitos del sistema.

Paso 6b: Actualizar una instalación existente (opcional)

Linux VDA admite actualizaciones desde la versión más reciente. Por ejemplo, puede actualizar Linux VDA de 2308 a 2311 y de 1912 LTSR a 2203 LTSR.

Para distribuciones RHEL y Rocky Linux:

```
sudo yum -y localinstall <PATH>/<Linux VDA RPM>
```

Nota:

- La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de realizar una actualización, asegúrese de hacer una copia de seguridad de los archivos.
- Antes de actualizar el VDA de Linux en RHEL 9.x y Rocky Linux 9.x, actualice el paquete **libsepol** a la versión 3.4 o posterior.
- A partir de la versión 2407, el VDA de Linux delega en los administradores de paquetes **rpm** o **dpkg** la gestión de los archivos de configuración durante las actualizaciones. A

continuación, se describe cómo interactúan rpm y dpkg con los cambios en los archivos de configuración:

- **rpm**: por defecto, mantiene la versión local y guarda la nueva versión del paquete con una extensión `.rpmnew`.
- **dpkg**: le pide interactivamente que elija cómo proceder. Para actualizar el VDA de Linux de forma silenciosa, conservando su archivo de configuración local y guardando la nueva versión del paquete como **.dpkg-new** o **.dpkg-dist**, utilice el siguiente comando:

```
dpkg --force-confold -i package.deb  # Always keep your version,
then save new package's version as *.dpkg-new or *.dpkg-dist
```

- Reinicie la máquina VDA de Linux después de actualizar el software.

Paso 7: Instalar los controladores NVIDIA GRID

Para habilitar HDX 3D Pro, debe instalar los controladores NVIDIA GRID en su hipervisor y en las máquinas VDA.

Para instalar y configurar NVIDIA GRID Virtual GPU Manager (el controlador de host) en los hipervisores específicos, consulte las siguientes guías:

- XenServer
- VMware ESX
- Nutanix AHV

Para instalar y configurar los controladores de VM invitados de NVIDIA GRID, realice los siguientes pasos:

1. Asegúrese de que la VM invitada esté apagada.
2. En XenCenter®, asigne una GPU a la VM.
3. Inicie la VM.
4. Prepare la VM para el controlador NVIDIA GRID:

```
yum install gcc
```

```
yum install "kernel-devel-$(uname -r)"



systemctl set-default multi-user.target
```

5. Siga los pasos del documento de Red Hat Enterprise Linux para instalar el controlador NVIDIA GRID.

Nota:

Durante la instalación del controlador de GPU, seleccione la opción predeterminada ('no') para cada pregunta.

Importante:

Una vez habilitado el paso a través de GPU, la VM de Linux ya no es accesible a través de XenCenter. Use SSH para conectarse.

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Establezca la configuración correcta para la tarjeta:

`etc/X11/ctx-nvidia.sh`

Para aprovechar las grandes resoluciones y las capacidades de varios monitores, necesita una licencia NVIDIA válida. Para solicitar la licencia, siga la documentación del producto de "GRID Licensing Guide.pdf - DU-07757-001 September 2015".

Paso 8: Configurar el VDA de Linux

> **Nota:**

> Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional **en_US.UTF-8** esté instalada en su sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando **sudo locale-gen en_US.UTF-8**. Para Debian, edite el archivo **/etc/locale.gen** descomentando la línea **# en_US.UTF-8 UTF-8** y, a continuación, ejecute el comando **sudo locale-gen**.

> Después de instalar el paquete, debe configurar el VDA de Linux ejecutando el script ctxsetup.sh. Antes de realizar cualquier cambio, el script verifica el entorno y se asegura de que todas las dependencias estén instaladas. Si es necesario, puede volver a ejecutar el script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manualmente con preguntas o automáticamente con respuestas preconfiguradas. Revise la Ayuda sobre el script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

Configuración guiada

Ejecute una configuración manual con preguntas guiadas:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Configuración automatizada

Para una instalación automatizada, proporcione las opciones requeridas por el script de configuración con variables de entorno. Si todas las variables requeridas están presentes, el script no solicitará ninguna información.

Las variables de entorno admitidas incluyen:

- **CTX_XDL_NON_DOMAIN_JOINED='y\|n'** – Si se debe unir la máquina a un dominio. El valor predeterminado es 'n'. Para escenarios unidos a un dominio, establézcalo en 'n'.
- **CTX_XDL_AD_INTEGRATION='winbind\|sssd\|centrify\|pbis\|quest'** – El VDA de Linux requiere ajustes de configuración de Kerberos para autenticarse con los Delivery Controllers. La configuración de Kerberos se determina a partir de la herramienta de integración de Active Directory instalada y configurada en el sistema.
- **CTX_XDL_DDC_LIST='<list-ddc-fqdns\>'** – El VDA de Linux requiere una lista de nombres de dominio completos (FQDN) de Delivery Controller separados por espacios para registrarse con un Delivery Controller. Se debe especificar al menos un FQDN o CNAME.
- **CTX_XDL_VDI_MODE='y\|n'** – Si se debe configurar la máquina como un modelo de entrega de escritorio dedicado (VDI) o un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca el valor en **'y'**.
- **CTX_XDL_HDX_3D_PRO='y\|n'** – El VDA de Linux admite HDX 3D Pro, un conjunto de tecnologías de aceleración de GPU diseñadas para optimizar la virtualización de aplicaciones con gráficos enriquecidos. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única) - (es decir, CTX_XDL_VDI_MODE=**'y'**).
- **CTX_XDL_START_SERVICE='y\|n'** – Determina si los servicios del VDA de Linux se inician cuando la configuración está completa.
- **CTX_XDL_REGISTER_SERVICE='y\|n'** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES='y\|n'** – Los servicios del VDA de Linux requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos requeridos (por defecto los puertos 80 y 1494) automáticamente en el firewall del sistema para Linux Virtual Desktop.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/kde/mate/xfce/'<none\>'** – Especifica el entorno de escritorio GNOME, GNOME Classic, KDE, MATE o **Xfce** que se utilizará en las sesiones. Si lo establece en **'<none\>'**, se utiliza el escritorio predeterminado configurado en el VDA.

  También puede cambiar entre entornos de escritorio ejecutando comandos o utilizando la bandeja del sistema. Para obtener más información, consulte Comandos de cambio de escritorio y Bandeja del sistema.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET para admitir el nuevo servicio de agente de intermediación (ctxvda). La ruta predeterminada es **'/usr/bin'**.

- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP.
- **CTX_XDL_SITE_NAME=<dns-name\>** – El VDA de Linux descubre servidores LDAP a través de DNS. Para limitar los resultados de la búsqueda de DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_LDAP_LIST='<list-ldap-servers\>'** – El VDA de Linux consulta DNS para descubrir servidores LDAP. Si DNS no puede proporcionar registros de servicio LDAP, puede proporcionar una lista de FQDN de LDAP separados por espacios con puertos LDAP. Por ejemplo, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Para habilitar consultas LDAP más rápidas dentro de un bosque de Active Directory, habilite el Catálogo global en un controlador de dominio y especifique el número de puerto LDAP relevante como 3268. Esta variable se establece en **'<none\>'** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE=search-base-set** – El VDA de Linux consulta LDAP a través de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=mycompany,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'** – El VDA de Linux admite la especificación de un nombre de Delivery Controller mediante un registro DNS CNAME.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_NON_DOMAIN_JOINED='n'

export CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest

export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'

export CTX_XDL_VDI_MODE='y|n'

export CTX_XDL_HDX_3D_PRO='y|n'

export CTX_XDL_START_SERVICE='y|n'

export CTX_XDL_REGISTER_SERVICE='y|n'

export CTX_XDL_ADD_FIREWALL_RULES='y|n'

export CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|
```

```
xfce|'<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'

export CTX_XDL_VDA_PORT='<port-number>'

export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'

export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'

export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'

export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Al ejecutar el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que crea. Recomendamos crear un archivo de script de shell a partir de los comandos anteriores con **#\!/bin/bash** como primera línea.

Alternativamente, puede especificar todos los parámetros mediante un solo comando:

```
sudo CTX_XDL_NON_DOMAIN_JOINED='n' \

CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest \

CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \

CTX_XDL_VDI_MODE='y|n' \

CTX_XDL_HDX_3D_PRO='y|n' \

CTX_XDL_START_SERVICE='y|n' \

CTX_XDL_REGISTER_SERVICE='y|n' \

CTX_XDL_ADD_FIREWALL_RULES='y|n' \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|xfce|'<none>' \

CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \

CTX_XDL_VDA_PORT='<port-number>' \
```

```
CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \

CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \

CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \

CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Eliminar cambios de configuración

En algunos escenarios, es posible que deba eliminar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete de Linux VDA.

Revise la Ayuda sobre este script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

Para eliminar los cambios de configuración:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

Importante:

Este script elimina todos los datos de configuración de la base de datos y deja el VDA de Linux inoperativo.

Registros de configuración

Los scripts **ctxsetup.sh** y **ctxcleanup.sh** muestran errores en la consola, con información adicional escrita en el archivo de registro de configuración **/tmp/xdl.configure.log**.

Reinicie los servicios del VDA de Linux para que los cambios surtan efecto.

Paso 9: Ejecute XDPing

Ejecute `sudo /opt/Citrix/VDA/bin/xdping` para comprobar si hay problemas de configuración comunes en un entorno de Linux VDA. Para obtener más información, consulte **XDPing**.

Paso 10: Ejecutar el VDA de Linux

Después de configurar el VDA de Linux mediante el script **ctxsetup.sh**, puede ejecutar los siguientes comandos para controlar el VDA de Linux.

Iniciar el VDA de Linux:

Para iniciar los servicios del VDA de Linux:

```
sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Detener el VDA de Linux:

Para detener los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

> **Nota:**

> Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que detuvo.

> **Reiniciar el VDA de Linux:**

Para reiniciar los servicios del VDA de Linux:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx
```

```
sudo systemctl restart ctxvda
```

Comprobar el estado del VDA de Linux:

Para comprobar el estado de ejecución de los servicios del VDA de Linux:

```
sudo systemctl status ctxvda
```

```
sudo systemctl status ctxhdx
```

Paso 11: Crear catálogos de máquinas

El proceso para crear catálogos de máquinas y agregar máquinas VDA de Linux es similar al enfoque tradicional de VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Para crear catálogos de máquinas que contengan máquinas VDA de Linux, existen algunas restricciones que diferencian el proceso de la creación de catálogos de máquinas para máquinas VDA de Windows:

- Para el sistema operativo, seleccione:
  - La opción **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios dedicados VDI.
- No mezcle máquinas VDA de Linux y Windows en el mismo catálogo de máquinas.

Nota:

Las versiones anteriores de Citrix Studio no admitían la noción de un "SO Linux". Sin embargo, seleccionar la opción **SO de servidor Windows** o **SO de servidor** implica un modelo de entrega de escritorios compartidos alojados equivalente. Seleccionar la opción **SO de escritorio Windows** o **SO de escritorio** implica un modelo de entrega de un solo usuario por máquina.

Sugerencia:

Cuando vuelva a unir una máquina eliminada al dominio de Active Directory, elimine la máquina de su catálogo de máquinas y vuelva a añadirla.

Paso 12: Crear grupos de entrega

El proceso para crear un grupo de entrega y añadir catálogos de máquinas que contengan máquinas VDA de Linux es casi idéntico al de las máquinas VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear grupos de entrega.

Para crear grupos de entrega que contengan catálogos de máquinas VDA de Linux, se aplican las siguientes restricciones:

- Asegúrese de que los usuarios y grupos de AD que seleccione se hayan configurado correctamente para iniciar sesión en las máquinas VDA de Linux.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No mezcle el grupo de entrega con catálogos de máquinas que contengan máquinas Windows.

Importante:

La publicación de aplicaciones es compatible con Linux VDA versión 1.4 y posteriores. Sin embargo, el VDA de Linux no admite la entrega de escritorios y aplicaciones a la misma máquina.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2503.

Instalar el VDA de Linux en SUSE manualmente

Importante:

Para instalaciones nuevas, le recomendamos que utilice easy install para una instalación rápida. La instalación fácil ahorra tiempo y trabajo, y es menos propensa a errores que la instalación manual detallada en este artículo.

Paso 1: Preparar la información de configuración y la máquina Linux

Paso 1a: Iniciar la herramienta YaST

La herramienta YaST de SUSE Linux Enterprise se utiliza para configurar todos los aspectos del sistema operativo.

Para iniciar la herramienta YaST basada en texto:

```
su -



yast
```

Para iniciar la herramienta YaST basada en interfaz de usuario:

```
su -



yast2 &
```

Paso 1b: Configurar la red

Las siguientes secciones proporcionan información sobre la configuración de los distintos ajustes y servicios de red utilizados por el VDA de Linux. La configuración de red se realiza a través de la herramienta YaST, no a través de otros métodos como Network Manager. Estas instrucciones se basan en el uso de la herramienta YaST basada en interfaz de usuario. La herramienta YaST basada en texto se puede utilizar, pero tiene un método de navegación diferente que no se documenta aquí.

CONFIGURAR EL NOMBRE DE HOST Y EL SISTEMA DE NOMBRES DE DOMINIO (DNS)

1. Inicie la herramienta YaST basada en interfaz de usuario.
2. Seleccione **Sistema** y, a continuación, **Configuración de red**.
3. Abra la ficha **Nombre de host/DNS**.
4. Seleccione la opción **no** para **Establecer nombre de host mediante DHCP**.
5. Seleccione la opción **Usar directiva personalizada** para **Modificar configuración de DNS**.

6. Edite lo siguiente para reflejar la configuración de su red:
   - **Nombre de host estático** – Agregue el nombre de host DNS de la máquina.
   - **Servidor de nombres** – Agregue la dirección IP del servidor DNS. Normalmente es la dirección IP del controlador de dominio de AD.
   - **Lista de búsqueda de dominio** – Agregue el nombre de dominio DNS.
7. Cambie la siguiente línea del archivo `/etc/hosts` para incluir el FQDN y el nombre de host como las dos primeras entradas:

   ```
   127.0.0.1 <FQDN of the VDA> <hostname of the VDA> localhost
   ```

> **Nota:**
>
> El VDA de Linux actualmente no admite la truncación de nombres NetBIOS. Por lo tanto, el nombre de host no debe exceder los 15 caracteres. **Sugerencia:**
>
> Utilice solo caracteres a–z, A–Z, 0–9 y guiones (-). Evite los guiones bajos (_), los espacios y otros símbolos. No inicie un nombre de host con un número ni lo termine con un guion. Esta regla también se aplica a los nombres de host de Delivery Controller.

COMPROBAR EL NOMBRE DE HOST

verificar que el nombre de host esté configurado correctamente:

```
hostname
```

Este comando devuelve solo el nombre de host de la máquina y no su nombre de dominio completo (FQDN).

verificar que el FQDN esté configurado correctamente:

```
hostname -f
```

Este comando devuelve el FQDN de la máquina.

COMPROBAR LA RESOLUCIÓN DE NOMBRES Y LA ACCESIBILIDAD DEL SERVICIO

verificar que puede resolver el FQDN y hacer ping al controlador de dominio y a Delivery Controller™:

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

Si no puede resolver el FQDN o hacer ping a alguna de estas máquinas, revise los pasos antes de continuar.

Paso 1c: Configurar el servicio NTP

Es crucial mantener una sincronización horaria precisa entre los VDA, los Delivery Controllers y los controladores de dominio. Alojar el VDA de Linux como una máquina virtual (VM) puede causar problemas de desviación del reloj. Por esta razón, se prefiere mantener la hora utilizando un servicio NTP remoto. Es posible que se requieran algunos cambios en la configuración predeterminada de NTP.

Para SUSE 15.6:

1. Iniciar la herramienta YaST basada en interfaz de usuario.
2. Seleccione **Servicios de red** y, a continuación, **Configuración de NTP**.
3. En la sección **Iniciar demonio NTP**, seleccione **Ahora y al arrancar**.
4. Seleccione **Dinámico** para **Origen de configuración**.
5. Agregue los servidores NTP según sea necesario. El servicio NTP normalmente se aloja en el controlador de dominio de Active Directory.
6. Elimine o comente la siguiente línea en /etc/chrony.conf si existe.

   `include /etc/chrony.d/*.conf`

   Después de editar chrony.conf, reinicie el servicio `chronyd`.

   ```
   sudo systemctl restart chronyd.service
   ```

Paso 1d: Instalar paquetes dependientes del VDA de Linux

El software VDA de Linux para SUSE Linux Enterprise depende de los siguientes paquetes:

- Open Motif Runtime Environment 2.3.1 o posterior
- Cups 1.6.0 o posterior
- ImageMagick 6.8 o posterior

AÑADIR REPOSITORIOS

Puede obtener la mayoría de los paquetes necesarios, excepto ImageMagick, de los repositorios oficiales. Para obtener los paquetes de ImageMagick, habilite el repositorio `sle-module-desktop-applications` mediante YaST o el siguiente comando:

```
SUSEConnect -p sle-module-desktop-applications/<version number>/x86_64
```

INSTALAR EL CLIENTE KERBEROS

Instale el cliente Kerberos para la autenticación mutua entre el VDA de Linux y los Delivery Controllers:

```
sudo zypper install krb5-client
```

La configuración del cliente Kerberos depende del enfoque de integración de Active Directory que se utilice. Consulte la siguiente descripción.

INSTALAR Y ESPECIFICAR UNA BASE DE DATOS PARA USAR

Nota:

- Le recomendamos que utilice SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el VDA de Linux utiliza PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio de PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).

- Para instalaciones manuales, debe instalar SQLite, PostgreSQL o ambos manualmente. Puede utilizar una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux. Si instala tanto SQLite como PostgreSQL, puede especificar cuál usar editando **/etc/xdl/db.conf** después de instalar el paquete del VDA de Linux.

Instalar PostgreSQL

Esta sección describe cómo instalar la versión de PostgreSQL proporcionada por su distribución de Linux. Si es necesaria una versión personalizada de PostgreSQL, puede instalarla según sus requisitos específicos.

Para instalar `Postgresql`, ejecute los siguientes comandos:

```
sudo zypper install postgresql-server



sudo zypper install postgresql-jdbc
```

Ejecute los siguientes comandos para iniciar PostgreSQL al arrancar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql



sudo systemctl restart postgresql
```

Instalar SQLite

Para SUSE, ejecute el siguiente comando para instalar SQLite:

```
sudo zypper install sqlite3
```

Especifique una base de datos para usar

Si instala SQLite y PostgreSQL, puede especificar cuál de ellas usar editando **/etc/xdl/db.conf** después de instalar el paquete de Linux VDA.

1. Ejecute **/opt/Citrix/VDA/sbin/ctxcleanup.sh**. Omita este paso si se trata de una instalación nueva.
2. Edite **/etc/xdl/db.conf** para especificar una base de datos que usar. A continuación, se muestra un ejemplo del archivo **db.conf**:

```
# database configuration file for Linux VDA



## database choice

# possible choices are:

#     SQLite

#     PostgreSQL

# default choice is PostgreSQL

DbType="PostgreSQL"




## database port

# specify database port for the database.

# if not specified, default port will be used:

# SQLite: N/A

# PostgreSQL: 5432

DbPort=5432




## PostgreSQL customized
```

```
# only the following value means true, otherwise false:
#     true
#     yes
#     y
#     YES
#     Y
# default is false
DbCustomizePostgreSQL=false



## PostgreSQL service name
# specify the service name of PostgreSQL for Linux VDA
# default is "postgresql"
DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

3. Ejecute **ctxsetup.sh**.

Nota:

También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

Paso 2: Preparar el hipervisor

Se requieren algunos cambios al ejecutar el Linux VDA como una VM en un hipervisor compatible. Realice los siguientes cambios según la plataforma de hipervisor en uso. No se requieren cambios si ejecuta la máquina Linux en hardware sin sistema operativo.

Corregir la sincronización de la hora en XenServer (anteriormente Citrix Hypervisor™)

Si la función XenServer® Time Sync está habilitada, dentro de cada VM Linux paravirtualizada, experimentará problemas con NTP y XenServer. Ambos intentan administrar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, sincronice el reloj del sistema dentro de cada invitado Linux con NTP. Este caso requiere deshabilitar la sincronización de la hora del host. No se requieren cambios en el modo HVM.

Si ejecuta un kernel de Linux paravirtualizado con XenServer VM Tools instalado, puede comprobar si la función XenServer Time Sync está presente y habilitada desde la VM Linux:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve 0 o 1:

- 0 - La función de sincronización de la hora está habilitada y debe deshabilitarse.
- 1 - La función de sincronización de la hora está deshabilitada y no se requiere ninguna otra acción.

Si el archivo **/proc/sys/xen/independent_wallclock** no está presente, los siguientes pasos no son necesarios.

Si está habilitada, deshabilite la función de sincronización de hora escribiendo **1** en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Para que este cambio sea permanente y persistente después de reiniciar, edite el archivo **/etc/sysctl.conf** y añada la línea:

`xen.independent_wallclock = 1`

Para verificar estos cambios, reinicie el sistema:

```
reboot
```

Después de reiniciar, verificar que la configuración es correcta:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve el valor 1.

Corregir la sincronización de hora en Microsoft Hyper-V

Las máquinas virtuales Linux con los Servicios de integración de Linux de Hyper-V instalados pueden aplicar la función de sincronización de hora de Hyper-V para usar la hora del sistema operativo host. Para asegurarse de que el reloj del sistema permanezca preciso, habilite esta función junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para la configuración de una máquina virtual Linux, seleccione **Integration Services**.
3. Asegúrese de que **Time synchronization** esté seleccionada.

> **Nota:**
>
> Este enfoque es diferente de VMware y XenServer (anteriormente Citrix Hypervisor), donde la sincronización de hora del host está deshabilitada para evitar conflictos con NTP. La sincronización de hora de Hyper-V puede coexistir y complementar la sincronización de hora de NTP.

Corregir la sincronización de hora en ESX y ESXi

Si la función de sincronización de hora de VMware está habilitada, dentro de cada máquina virtual Linux paravirtualizada experimentará problemas con NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, sincronice el reloj del sistema dentro de cada invitado Linux con NTP. Este caso requiere deshabilitar la sincronización de hora del host.

Si está ejecutando un kernel de Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Edite la configuración de la VM de Linux.

3. En el cuadro de diálogo **Propiedades de la máquina virtual**, abra la ficha **Opciones**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Avanzado**, desactive **Sincronizar la hora del invitado con la del host**.

Paso 3: Añadir la VM de Linux al dominio de Windows

Los siguientes métodos están disponibles para añadir máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Siga las instrucciones según el método elegido.

> **Nota:**
>
> Los inicios de sesión pueden fallar cuando se utiliza el mismo nombre de usuario para la cuenta local en el VDA de Linux y para la cuenta en AD.

Samba Winbind

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para agregar máquinas al dominio:

1. Inicie YaST, seleccione **Servicios de red** y, a continuación, **Pertenencia a dominio de Windows**.
2. Realice los siguientes cambios:
   - Establezca **Dominio o grupo de trabajo** en el nombre de su dominio de Active Directory o en la dirección IP del controlador de dominio. Asegúrese de que el nombre de dominio esté en mayúsculas.
   - Marque **Usar información de SMB para la autenticación de Linux**.
     - Marque **Crear directorio personal al iniciar sesión**.
     - Marque **Inicio de sesión único para SSH**.

- Asegúrese de que **Autenticación sin conexión** no esté marcada. Esta opción no es compatible con el VDA de Linux.

3. Haga clic en **Aceptar**. Si se le pide que instale algunos paquetes, haga clic en **Instalar**.
4. Si se encuentra un controlador de dominio, le preguntará si desea unirse al dominio. Haga clic en **Sí**.
5. Cuando se le solicite, escriba las credenciales de un usuario de dominio con permiso para agregar máquinas al dominio y haga clic en **Aceptar**.
6. Reinicie los servicios manualmente o reinicie la máquina. Le recomendamos que reinicie la máquina:

```
su -

reboot
```

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en Active Directory.

Ejecute el comando **net ads** de **Samba** para verificar que la máquina está unida a un dominio:

```
sudo net ads testjoin
```

Ejecute el siguiente comando para verificar información adicional del dominio y del objeto de equipo:

```
sudo net ads info
```

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Asegúrese de que el archivo keytab del sistema se haya creado y contenga claves válidas:

```
sudo klist –ke
```

Este comando muestra la lista de claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando Kerberos `kinit` para autenticar la máquina con el controlador de dominio mediante estas claves:

```
sudo kinit -k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución de la shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utilice el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT para la cuenta de la máquina se ha almacenado en caché mediante:

```
sudo klist
```

Examine los detalles de la cuenta de la máquina mediante:

```
sudo net ads status
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Utilice la herramienta **wbinfo** para verificar que los usuarios del dominio pueden autenticarse con el dominio:

```
wbinfo --krb5auth=domain\\username%password
```

El dominio especificado aquí es el nombre de dominio de AD, no el nombre de reino de Kerberos. Para la shell bash, el carácter de barra invertida (\\) debe escaparse con otra barra invertida. Este comando devuelve un mensaje que indica éxito o fracaso.

verificar que el módulo PAM de Winbind está configurado correctamente. Para ello, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username

id -u
```

verificar que se creó un archivo de caché de credenciales de Kerberos correspondiente para el uid devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets en la caché de credenciales de Kerberos del usuario son válidos y no han caducado:

```
klist
```

Salga de la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Servicio de autenticación Quest

CONFIGURAR QUEST EN EL CONTROLADOR DE DOMINIO

Suponga que ha instalado y configurado el software Quest en los controladores de dominio y que se le han concedido privilegios administrativos para crear objetos de equipo en `Active Directory`.

PERMITIR QUE LOS USUARIOS DEL DOMINIO INICIEN SESIÓN EN MÁQUINAS VDA DE LINUX

Para permitir que los usuarios del dominio establezcan sesiones HDX™ en una máquina VDA de Linux:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory para esa cuenta de usuario.
2. Seleccione la ficha **Cuenta Unix**.
3. Marque **Habilitado para Unix**.
4. Establezca el **Número GID principal** en el ID de grupo de un grupo de usuarios de dominio real.

> **Nota:**
>
> Estas instrucciones son equivalentes para configurar usuarios de dominio para el inicio de sesión mediante la consola, RDP, SSH o cualquier otro protocolo de acceso remoto.

CONFIGURAR QUEST EN EL VDA DE LINUX

Configurar el demonio VAS

La renovación automática de los tickets Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar inhabilitada:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Este comando establece el intervalo de renovación en nueve horas (32.400 segundos), lo que es una hora menos que la duración predeterminada del ticket de 10 horas. Establezca este parámetro en un valor inferior en sistemas con una duración de ticket más corta.

Configurar PAM y NSS

Para habilitar los inicios de sesión de usuarios de dominio a través de HDX y otros servicios como su, ssh y RDP, configure PAM y NSS manualmente:

```
sudo /opt/quest/bin/vastool configure pam



sudo /opt/quest/bin/vastool configure nss
```

UNIRSE AL DOMINIO DE WINDOWS

Una la máquina Linux al dominio de Active Directory mediante el comando Quest `vastool`:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

El **usuario** es cualquier usuario de dominio que tenga permiso para unir máquinas al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Reinicie la máquina Linux después de unirse al dominio.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para verificar que una máquina Linux unida a Quest está en el dominio:

```
sudo /opt/quest/bin/vastool info domain
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. Si la máquina no está unida a ningún dominio, aparece el siguiente error:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

VERIFICAR LA AUTENTICACIÓN DE USUARIO

verificar que Quest puede autenticar a los usuarios del dominio a través de PAM. Para ello, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username

id -u
```

verificar que se creó un archivo de caché de credenciales de Kerberos correspondiente para el uid devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets de la caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
```

Cierre la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Centrify DirectControl

UNIR AL DOMINIO DE WINDOWS

Con el agente de Centrify DirectControl instalado, una la máquina Linux al dominio de Active Directory mediante el comando **adjoin** de Centrify:

```
sudo adjoin -w -V -u user domain-name
```

El **user** es cualquier usuario del dominio de Active Directory que tenga permiso para unir máquinas al dominio de Active Directory. El **domain-name** es el nombre del dominio al que se unirá la máquina Linux.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en Active Directory. Para verificar que una máquina Linux unida a Centrify está en el dominio:

```
sudo adinfo
```

verificar que el valor de **Joined to domain** es válido y que el **mode** de **CentrifyDC** devuelve **connected**. Si el modo se queda atascado en el estado inicial, el cliente de Centrify está experimentando problemas de conexión o autenticación con el servidor.

Hay disponible información de diagnóstico y del sistema más completa mediante:

```
adinfo --sysinfo all



adinfo –diag
```

Pruebe la conectividad con los distintos servicios de Active Directory y Kerberos.

```
adinfo --test
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

SSSD

Si utiliza SSSD en SUSE, siga las instrucciones de esta sección. Esta sección incluye instrucciones para unir una máquina VDA de Linux a un dominio de Windows y proporciona orientación para configurar la autenticación Kerberos.

Para configurar SSSD en SUSE, siga estos pasos:

1. Unir el dominio y crear un keytab de host
2. Configurar PAM para SSSD
3. Configurar SSSD
4. Habilitar SSSD
5. verificar la pertenencia al dominio
6. verificar la configuración de Kerberos
7. verificar la autenticación de usuario

UNIRSE AL DOMINIO Y CREAR UN KEYTAB DE HOST

SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo keytab del sistema. En su lugar, puede utilizar el enfoque de **Samba**. Complete los siguientes pasos antes de configurar SSSD.

1. Detenga y deshabilite el demonio del Servicio de Caché de Nombres (NSCD).

   ```
   sudo systemctl stop nscd

   sudo systemctl disable nscd
   ```

2. Compruebe el nombre de host y la sincronización horaria de Chrony.

   ```
   hostname

   hostname -f

   chronyc traking
   ```

3. Instale o actualice los paquetes necesarios:

```
sudo zypper install samba-client sssd-ad
```

4. Edite el archivo `/etc/krb5.conf` como usuario root para permitir que la utilidad **kinit** se comunique con el dominio de destino. Agregue las siguientes entradas en las secciones , y :

> **Nota:**
>
> Configure Kerberos según su infraestructura de AD. Las siguientes configuraciones están pensadas para el modelo de dominio único y bosque único.

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

[realms]

    REALM = {

        kdc = fqdn-of-domain-controller
```

```
        default_domain = realm


        admin_server = fqdn-of-domain-controller
    }
[domain_realm]


    .realm = REALM
```

realm es el nombre del reino de Kerberos, como example.com. **REALM** es el nombre del reino de Kerberos en mayúsculas, como EXAMPLE.COM.

5. Edite `/etc/samba/smb.conf` como usuario root para permitir que la utilidad **net** se comunique con el dominio de destino. Agregue las siguientes entradas en la sección :

```
[global]
    workgroup = domain


    client signing = yes


    client use spnego = yes


    kerberos method = secrets and keytab


    realm = REALM
```

```
    security = ADS
```

domain es el nombre corto de NetBIOS de un dominio de Active Directory, como EXAMPLE.

6. Modifique las entradas **passwd** y **group** en el archivo **/etc/nsswitch.conf** para hacer referencia a SSSD al resolver usuarios y grupos.

```
passwd: compat sss



group: compat sss
```

7. Utilice el cliente Kerberos configurado para autenticarse en el dominio de destino como Administrador.

```
kinit administrator
```

8. Utilice la utilidad **net** para unir el sistema al dominio y generar un archivo keytab del sistema.

```
net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
administrator
```

CONFIGURAR PAM PARA SSSD

Antes de configurar PAM para SSSD, instale o actualice los paquetes necesarios:

```
sudo zypper install sssd sssd-ad
```

Configure el módulo PAM para la autenticación de usuarios a través de SSSD y cree directorios de inicio para los inicios de sesión de los usuarios.

```
sudo pam-config --add  --sss

sudo pam-config --add --mkhomedir
```

CONFIGURAR SSSD

1. Edite `/etc/sssd/sssd.conf` como usuario root para permitir que el demonio SSSD se comunique con el dominio de destino. Un ejemplo de configuración de `sssd.conf` (se pueden añadir opciones adicionales según sea necesario):

```
[sssd]

    config_file_version = 2

    services = nss,pam

    domains = domain-dns-name



[domain/domain-dns-name]

    id_provider = ad

    auth_provider = ad

    access_provider = ad

    ad_domain = domain-dns-name

    ad_server = fqdn-of-domain-controller

    ldap_id_mapping = true

    ldap_schema = ad



# Kerberos settings

    krb5_ccachedir = /tmp

    krb5_ccname_template = FILE:%d/krb5cc_%U



# Comment out if the users have the shell and home dir set on the AD
```

```
side



    fallback_homedir = /home/%d/%u

    default_shell = /bin/bash



# Uncomment and adjust if the default principal SHORTNAME$@REALM is not
available



# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM



    ad_gpo_access_control = permissive
```

domain-dns-name es el nombre de dominio DNS, como example.com.

> **Nota:**
>
> **ldap_id_mapping** se establece en true para que SSSD se encargue de asignar los SID de Windows a los UID de Unix. De lo contrario, Active Directory debe poder proporcionar extensiones POSIX. **ad_gpo_access_control** se establece en **permissive** para evitar un error de inicio de sesión no válido para las sesiones de Linux. Consulte las páginas man de `sssd.conf` y `sssd-ad`.

2. Establezca la propiedad y los permisos del archivo en `sssd.conf`:

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

HABILITAR SSSD

Ejecute los siguientes comandos para habilitar e iniciar el demonio SSSD al inicio del sistema:

```
sudo systemctl enable sssd

sudo systemctl start sssd
```

VERIFICAR LA PERTENENCIA AL DOMINIO

1. Ejecute el comando `net ads` de **Samba** para verificar que la máquina está unida a un dominio:

   ```
   sudo net ads testjoin
   ```

2. Ejecute el siguiente comando para verificar información adicional del dominio y del objeto de equipo:

   ```
   sudo net ads info
   ```

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Asegúrese de que el archivo keytab del sistema se haya creado y contenga claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado.

Ejecute el comando Kerberos **kinit** para autenticar la máquina con el controlador de dominio mediante estas claves:

```
sudo kinit –k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar (**$**) debe escaparse con una barra invertida (****) para evitar la sustitución de shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utilice el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT de la cuenta de máquina se ha almacenado en caché mediante:

```
sudo klist
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

SSSD no proporciona una herramienta de línea de comandos para probar la autenticación directamente con el demonio, y solo se puede hacer a través de PAM.

Para verificar que el módulo PAM de SSSD está configurado correctamente, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

verificar que los tickets Kerberos devueltos por el comando `klist` son correctos para ese usuario y no han caducado.

Como usuario root, verificar que se creó un archivo de caché de tickets correspondiente para el uid devuelto por el comando `id -u` anterior:

```
ls /tmp/krb5cc_uid
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Step 6: Install the Linux VDA después de la verificación de unión al dominio.

PBIS

DESCARGUE EL PAQUETE PBIS NECESARIO

Por ejemplo:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

HACER QUE EL SCRIPT DE INSTALACIÓN DE PBIS SEA EJECUTABLE

Por ejemplo:

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

EJECUTAR EL SCRIPT DE INSTALACIÓN DE PBIS

Por ejemplo:

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

UNIRSE A UN DOMINIO DE WINDOWS

El controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para agregar máquinas al dominio:

```
/opt/pbis/bin/domainjoin-cli join domain-name user
```

El **usuario** es un usuario de dominio que tiene permisos para agregar máquinas al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Nota: Para establecer Bash como shell predeterminado, ejecute el comando **/opt/pbis/bin/config LoginShellTemplate/bin/bash**.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para verificar que una máquina Linux unida a PBIS está en el dominio:

```
/opt/pbis/bin/domainjoin-cli query
```

Si la máquina está unida a un dominio, este comando devuelve la información sobre el dominio de AD y la OU a los que está unida actualmente. De lo contrario, solo aparece el nombre de host.

VERIFICAR LA AUTENTICACIÓN DE USUARIO

verificar que PBIS puede autenticar a los usuarios del dominio a través de PAM. Para ello, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\user



id -u
```

verificar que se creó un archivo de caché de credenciales de Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

Cierre la sesión.

```
exit
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Paso 4: Instalar .NET

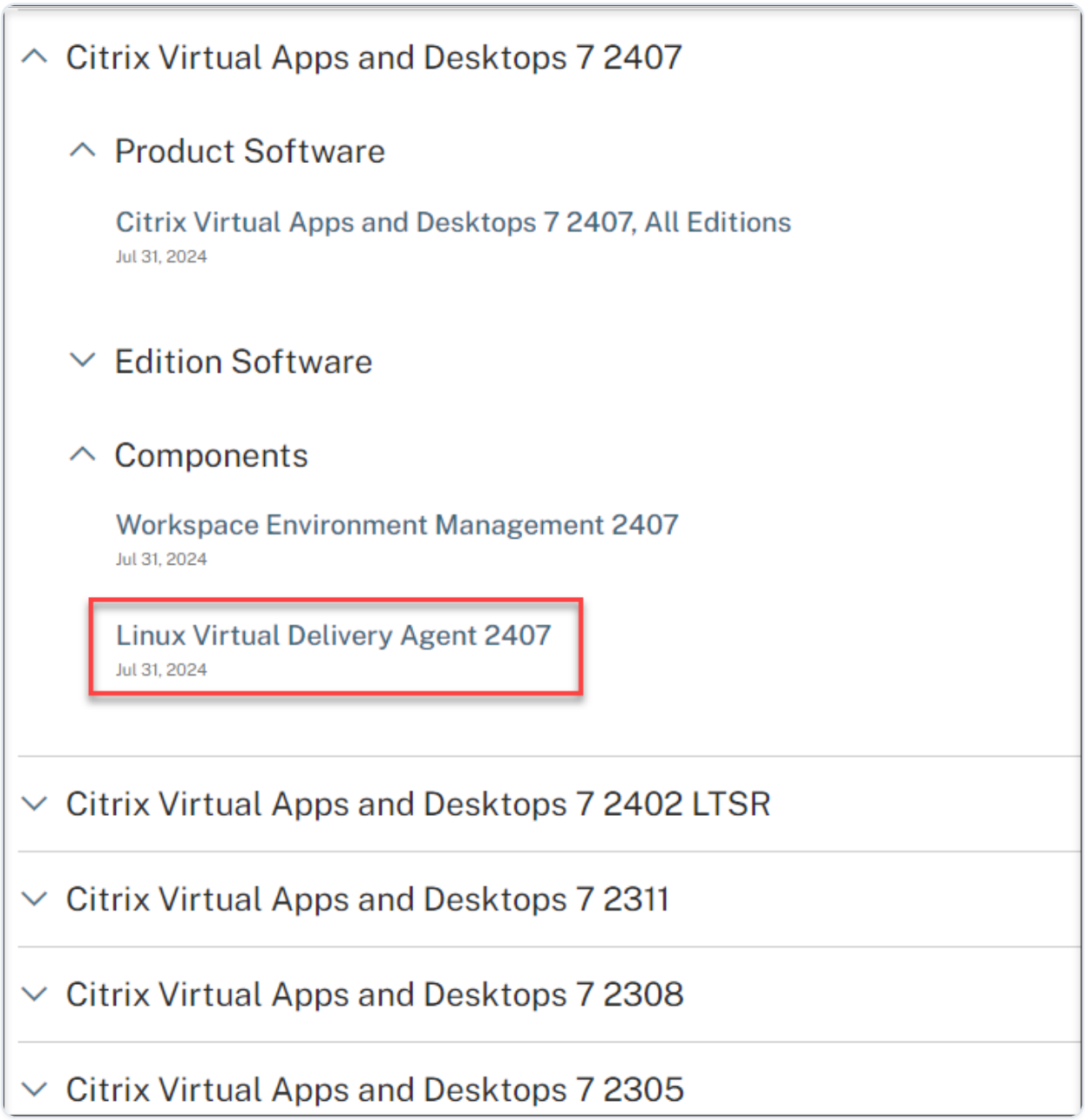
Antes de instalar el VDA de Linux, instale .NET (/es-es/linux-virtual-delivery-agent/2507-ltsr/system-requirements.html#net-requirements)

Después de instalar .NET, ejecute el comando **which dotnet** para encontrar la ruta de tiempo de ejecución.

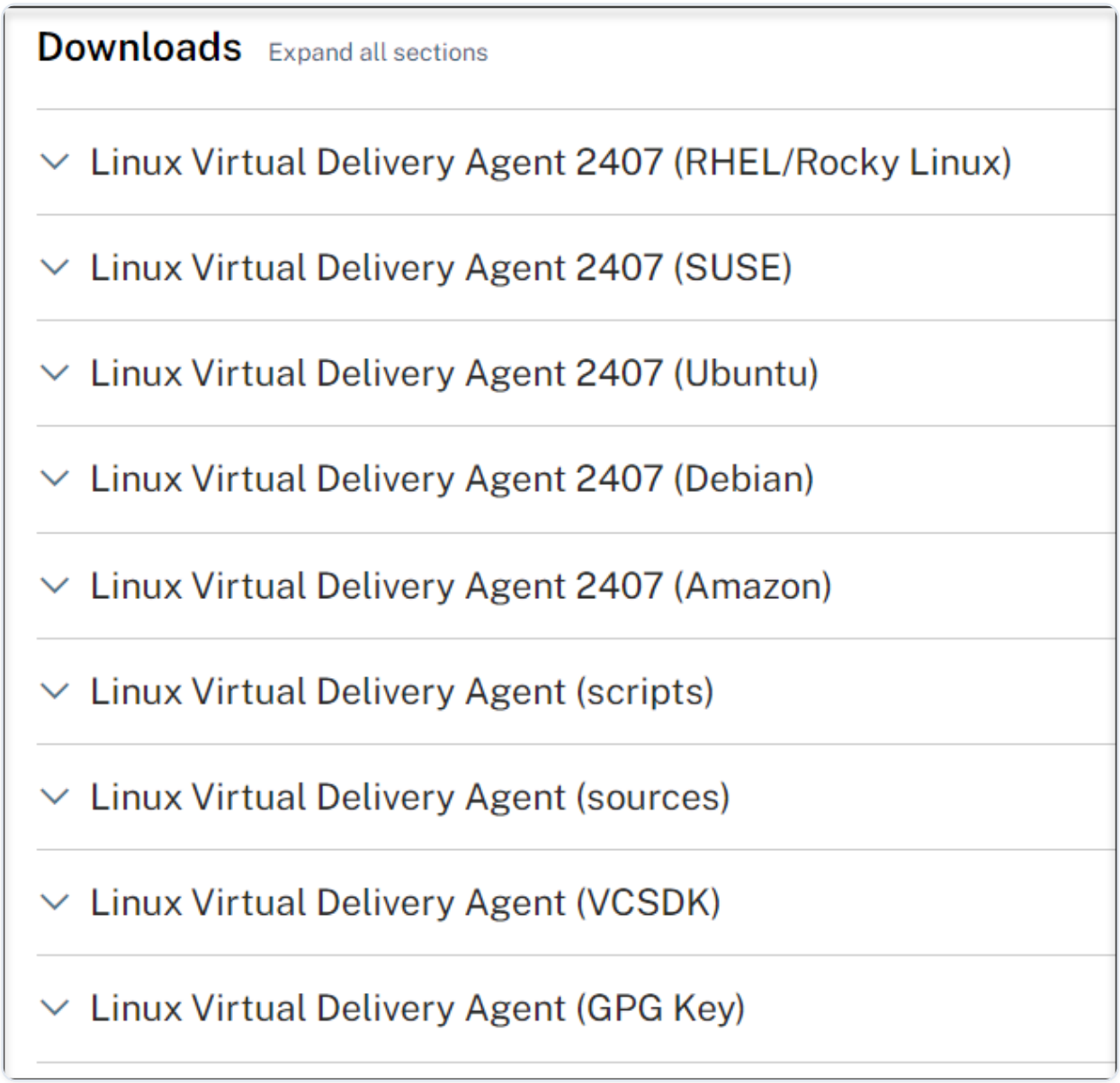
Según la salida del comando, establezca la ruta binaria de tiempo de ejecución de .NET. Por ejemplo, si la salida del comando es /aa/bb/dotnet, use /aa/bb como la ruta binaria de .NET.

Paso 5: Descargar el paquete del VDA de Linux

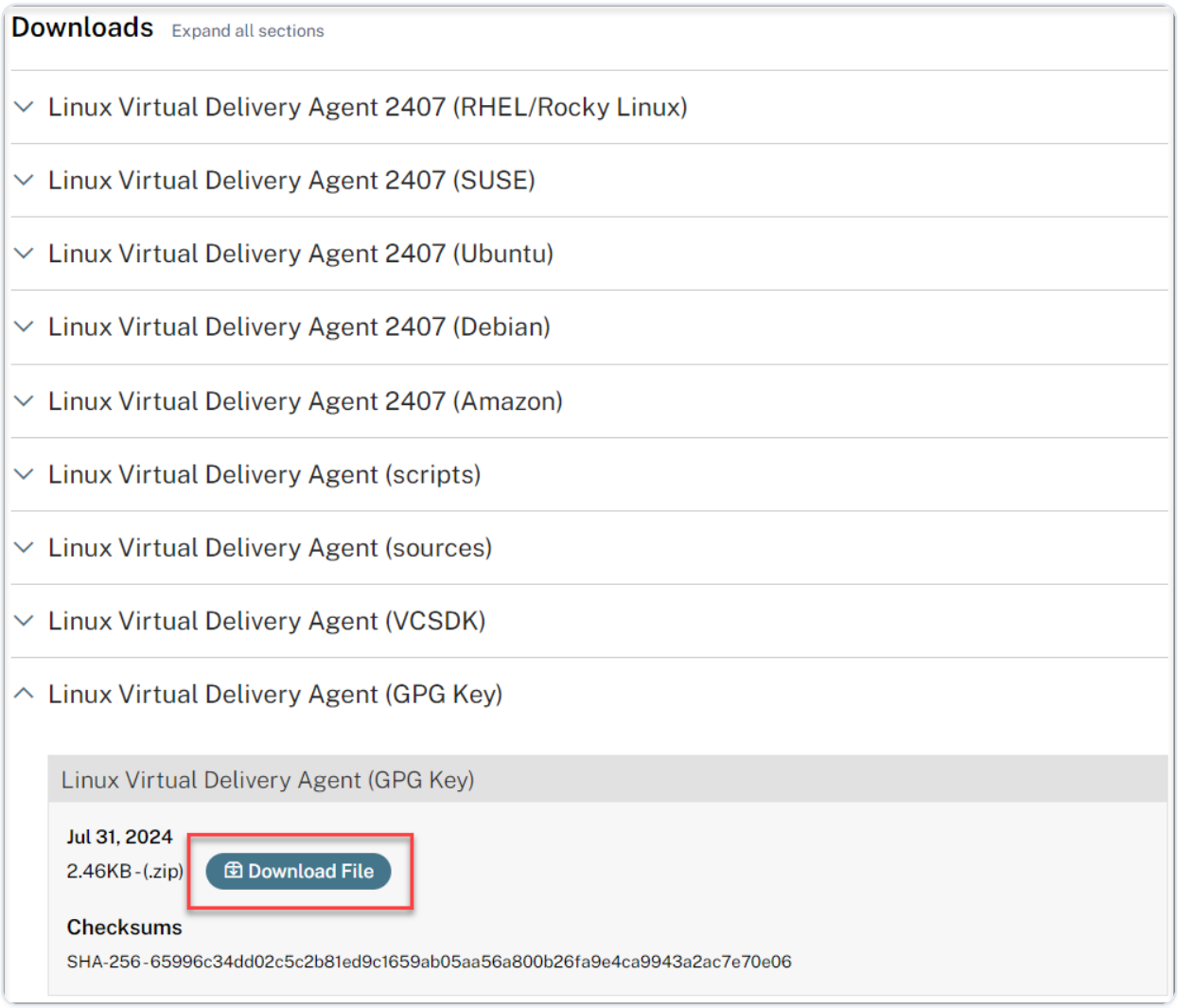
1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Expanda **Componentes** para encontrar el VDA de Linux. Por ejemplo:



4. Haga clic en el enlace del VDA de Linux para acceder a las descargas del VDA de Linux.



5. Descargue el paquete del VDA de Linux que coincida con su distribución de Linux.
6. Descargue la clave pública GPG que puede usar para verificar la integridad del paquete del VDA de Linux. Por ejemplo:



Para verificar la integridad del paquete del VDA de Linux mediante la clave pública, ejecute los siguientes comandos para importar la clave pública en la base de datos RPM y comprobar la integridad del paquete:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

Paso 6: Instalar el VDA de Linux

Paso 6a: Desinstalar la versión anterior

Si instaló una versión anterior que no sea las dos anteriores y una versión LTSR, desinstálela antes de instalar la nueva versión.

1. Detenga los servicios de Linux VDA:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

Nota:

Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que detuvo.

2. Desinstale el paquete:

```
sudo rpm -e XenDesktopVDA
```

Importante:

Se admite la actualización desde las dos últimas versiones.

Nota:

Puede encontrar los componentes instalados en **/opt/Citrix/VDA/**.

Para ejecutar un comando, se necesita la ruta completa; alternativamente, puede añadir **/opt/Citrix/VDA/sbin** y **/opt/Citrix/VDA/bin** a la ruta del sistema.

Paso 6b: Instalar el Linux VDA

Instale el software de Linux VDA mediante Zypper:

```
sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

Paso 6c: Actualizar el Linux VDA (opcional)

El Linux VDA admite actualizaciones desde la versión más reciente. Por ejemplo, puede actualizar el Linux VDA de 2308 a 2311 y de 1912 LTSR a 2203 LTSR.

> **Nota:**
>
> La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de realizar una actualización, asegúrese de hacer una copia de seguridad de los archivos.

```
sudo zypper -i install <PATH>/<Linux VDA RPM>
```

Lista de dependencias RPM para SUSE 15:

```
java-17-openjdk >= 17

ImageMagick >= 7.0

dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4
```

```
cups >= 2.2

cups-filters >= 1.25

libxml2-2 >= 2.9

libmspack0 >= 0.6

ibus >= 1.5

libQt5DBus5 >= 5.12

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1

libpython3_6m1_0 >= 3.6~

libQt5Widgets5 >= 5.12

libqrencode4 >= 4.0.0

libImlib2-1 >= 1.4.10

libgtk-2_0-0 >= 2.24

libgthread-2_0-0 >= 2.48

pulseaudio-utils >= 5.0

lsb-release >= 2.0

pkexec >= 121

cyrus-sasl-gssapi >= 2.1

libfuse2 >= 2.9
```

Importante:

> Reinicie la máquina Linux VDA después de la actualización.

Paso 7: Instalar los controladores NVIDIA GRID

Para habilitar HDX 3D Pro, debe instalar los controladores NVIDIA GRID en su hipervisor y en las máquinas VDA.

Para instalar y configurar NVIDIA GRID Virtual GPU Manager (el controlador de host) en los hipervisores específicos, consulte las siguientes guías:

- XenServer
- VMware ESX
- Nutanix AHV

Para instalar y configurar los controladores de VM invitada de NVIDIA GRID, siga estos pasos generales:

1. Asegúrese de que la VM invitada esté apagada.
2. En el panel de control del hipervisor, asigne una GPU a la VM.
3. Inicie la VM.
4. Instale el controlador de VM invitada (de su proveedor de la nube o de NVIDIA) en la VM.

Paso 8: Configurar el VDA de Linux

> **Nota:**

> Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional **en_US.UTF-8** esté instalada en su sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando **sudo locale-gen en_US.UTF-8**. Para Debian, edite el archivo **/etc/locale.gen** descomentando la línea **# en_US.UTF-8 UTF-8** y, a continuación, ejecute el comando **sudo locale-gen**.

> Después de instalar el paquete, debe configurar el VDA de Linux ejecutando el script `ctxsetup.sh`. Antes de que el script realice cualquier cambio, verifica el entorno y se asegura de que todas las dependencias estén instaladas. Si es necesario, puede volver a ejecutar el script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manualmente con indicaciones o automáticamente con respuestas preconfiguradas. Revise la Ayuda sobre el script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

Configuración guiada

Ejecute una configuración manual con preguntas guiadas:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Configuración automatizada

Para una instalación automatizada, proporcione las opciones requeridas por el script de configuración con variables de entorno. Si todas las variables requeridas están presentes, el script no solicitará ninguna información.

Las variables de entorno admitidas incluyen:

- **CTX_XDL_NON_DOMAIN_JOINED='y\|n'** – Si se debe unir la máquina a un dominio. El valor predeterminado es 'n'. Para escenarios unidos a un dominio, establézcalo en 'n'.
- **CTX_XDL_AD_INTEGRATION='winbind\|sssd\|centrify\|pbis\|quest'** – El Linux VDA requiere la configuración de Kerberos para autenticarse con los Delivery Controllers. La configuración de Kerberos se determina a partir de la herramienta de integración de Active Directory instalada y configurada en el sistema.
- **CTX_XDL_DDC_LIST='<list-ddc-fqdns\>'** – El Linux VDA requiere una lista de nombres de dominio completos (FQDN) de Delivery Controller separados por espacios para registrarse con un Delivery Controller. Se debe especificar al menos un FQDN o CNAME.
- **CTX_XDL_VDI_MODE='y\|n'** – Si se debe configurar la máquina como un modelo de entrega de escritorio dedicado (VDI) o un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca el valor en **'y'**.
- **CTX_XDL_HDX_3D_PRO='y\|n'** – El Linux VDA es compatible con HDX 3D Pro, un conjunto de tecnologías de aceleración de GPU diseñadas para optimizar la virtualización de aplicaciones con gráficos enriquecidos. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única), es decir, CTX_XDL_VDI_MODE=**'y'**.
- **CTX_XDL_START_SERVICE='y\|n'** – Determina si los servicios del Linux VDA se inician cuando la configuración está completa.

- **CTX_XDL_REGISTER_SERVICE='y\|n'** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES='y\|n'** – Los servicios del Linux VDA requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos requeridos (por defecto, los puertos 80 y 1494) automáticamente en el firewall del sistema para Linux Virtual Desktop.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate/'<none\>'** – Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se utilizará en las sesiones. Si lo establece en **'<none\>'**, se utiliza el escritorio predeterminado configurado en el VDA.

  También puede cambiar entre entornos de escritorio ejecutando comandos o utilizando la bandeja del sistema. Para obtener más información, consulte Comandos para cambiar de escritorio y Bandeja del sistema.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET para admitir el nuevo servicio de agente de broker (ctxvda). La ruta predeterminada es **'/usr/bin'**.
- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP.
- **CTX_XDL_SITE_NAME=<dns-name\>** – El VDA de Linux detecta los servidores LDAP a través de DNS. Para limitar los resultados de la búsqueda DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_LDAP_LIST='<list-ldap-servers\>'** – El VDA de Linux consulta DNS para detectar servidores LDAP. Si DNS no puede proporcionar registros de servicio LDAP, puede proporcionar una lista de FQDN de LDAP separados por espacios con puertos LDAP. Por ejemplo, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Para habilitar consultas LDAP más rápidas dentro de un bosque de Active Directory, habilite el Catálogo global en un controlador de dominio y especifique el número de puerto LDAP relevante como 3268. Esta variable se establece en **'<none\>'** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE=search-base-set** – El VDA de Linux consulta LDAP a través de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=mycompany,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_SUPPORT_DDC_AS_CNAME='y\|n'** – El VDA de Linux admite la especificación de un nombre de Delivery Controller mediante un registro DNS CNAME.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_NON_DOMAIN_JOINED='n'

export CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest

export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'

export CTX_XDL_VDI_MODE='y|n'

export CTX_XDL_HDX_3D_PRO='y|n'

export CTX_XDL_START_SERVICE='y|n'

export CTX_XDL_REGISTER_SERVICE='y|n'

export CTX_XDL_ADD_FIREWALL_RULES='y|n'

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'

export CTX_XDL_VDA_PORT='<port-number>'

export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'

export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'

export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'

export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Al ejecutar el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que crea. Le recomendamos que cree un archivo de script de shell a partir de los comandos anteriores con **#\!/bin/bash** como primera línea.

Alternativamente, puede especificar todos los parámetros mediante un solo comando:

```
sudo CTX_XDL_NON_DOMAIN_JOINED='n' \

CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest \

CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \

CTX_XDL_VDI_MODE='y|n' \

CTX_XDL_HDX_3D_PRO='y|n' \

CTX_XDL_START_SERVICE='y|n' \

CTX_XDL_REGISTER_SERVICE='y|n' \

CTX_XDL_ADD_FIREWALL_RULES='y|n' \

CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>' \

CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \

CTX_XDL_VDA_PORT='<port-number>' \

CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \

CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \

CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \

CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Eliminar cambios de configuración

En algunos escenarios, es posible que deba eliminar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete del VDA de Linux.

Revise la Ayuda sobre este script antes de continuar:

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

Para eliminar los cambios de configuración:

```
sudo /usr/local/sbin/ctxcleanup.sh
```

Importante:

Este script elimina todos los datos de configuración de la base de datos y deja el VDA de Linux inoperable.

Registros de configuración

Los scripts **ctxsetup.sh** y **ctxcleanup.sh** muestran errores en la consola, con información adicional escrita en un archivo de registro de configuración:

`/tmp/xdl.configure.log`

Reinicie los servicios de Linux VDA para que los cambios surtan efecto.

Paso 9: Ejecute XDPing

Ejecute `sudo /opt/Citrix/VDA/bin/xdping` para comprobar si hay problemas de configuración comunes en un entorno de Linux VDA. Para obtener más información, consulte **XDPing**.

Paso 10: Ejecutar el Linux VDA

Después de configurar el Linux VDA mediante el script **ctxsetup.sh**, puede ejecutar los siguientes comandos para controlar el Linux VDA.

Iniciar el Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Detener el Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda
```

```
sudo systemctl stop ctxhdx
```

Nota:

Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que detuvo.

Reiniciar el Linux VDA:

Para reiniciar los servicios de Linux VDA:

```
sudo systemctl stop ctxvda
```

```
sudo systemctl restart ctxhdx
```

```
sudo systemctl restart ctxvda
```

Comprobar el estado del Linux VDA:

Para comprobar el estado de ejecución de los servicios de Linux VDA:

```
sudo systemctl status ctxvda
```

```
sudo systemctl status ctxhdx
```

Paso 11: Crear catálogos de máquinas

El proceso para crear catálogos de máquinas y agregar máquinas VDA de Linux es similar al enfoque tradicional de VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Para crear catálogos de máquinas que contengan máquinas VDA de Linux, existen algunas restricciones que diferencian el proceso de la creación de catálogos de máquinas para máquinas VDA de Windows:

- Para el sistema operativo, seleccione:
  - La opción **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios dedicados VDI.
- No mezcle máquinas VDA de Linux y Windows en el mismo catálogo de máquinas.

> **Nota:**
>
> Las versiones anteriores de Citrix Studio no admitían la noción de un "SO Linux". Sin embargo, seleccionar la opción **SO de Windows Server** o **SO de servidor** implica un modelo de entrega de escritorios compartidos alojados equivalente. Seleccionar la opción **SO de escritorio de Windows** o **SO de escritorio** implica un modelo de entrega de un solo usuario por máquina.

> **Sugerencia:**
>
> Si quita y vuelve a unir una máquina al dominio de Active Directory, debe quitar y volver a agregar la máquina al catálogo de máquinas.

Paso 12: Crear grupos de entrega

El proceso para crear un grupo de entrega y agregar catálogos de máquinas que contengan máquinas VDA de Linux es casi idéntico al de las máquinas VDA de Windows. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear grupos de entrega.

Para crear grupos de entrega que contengan catálogos de máquinas VDA de Linux, se aplican las siguientes restricciones:

- Asegúrese de que los usuarios y grupos de AD que seleccione se hayan configurado correctamente para iniciar sesión en las máquinas VDA de Linux.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No mezcle el grupo de entrega con catálogos de máquinas que contengan máquinas Windows.

> **Importante:**
>
> La publicación de aplicaciones es compatible con Linux VDA versión 1.4 y posteriores. Sin embargo, Linux VDA no admite la entrega de escritorios y aplicaciones a la misma máquina.

> Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2503.

Instalar el VDA de Linux en Ubuntu manualmente

> **Importante:**
>
> Para instalaciones nuevas, le recomendamos que utilice instalación sencilla para una instalación rápida. La instalación sencilla ahorra tiempo y trabajo, y es menos propensa a errores que la instalación manual detallada en este artículo.

Paso 1: Preparar la información de configuración y la máquina Linux

Paso 1a: verificar la configuración de red

Asegúrese de que la red esté conectada y configurada correctamente. Por ejemplo, debe configurar el servidor DNS en el VDA de Linux.

Si utiliza un Ubuntu Live Server, realice el siguiente cambio en el archivo de configuración **/etc/cloud/cloud.cfg** antes de establecer el nombre de host:

```
preserve_hostname: true
```

Paso 1b: Establecer el nombre de host

Para asegurarse de que el nombre de host de la máquina se notifique correctamente, cambie el archivo **/etc/hostname** para que contenga solo el nombre de host de la máquina.

```
hostname
```

Paso 1c: Asignar una dirección de bucle invertido al nombre de host

Asegúrese de que el nombre de dominio DNS y el nombre de dominio completo (FQDN) de la máquina se notifiquen correctamente. La forma de hacerlo es cambiar la siguiente línea del archivo **/etc/hosts** para incluir el FQDN y el nombre de host como las dos primeras entradas:

```
127.0.0.1 hostname-fqdn hostname localhost
```

Por ejemplo:

```
127.0.0.1 vda01.example.com vda01 localhost
```

Elimine cualquier otra referencia a `hostname-fqdn` o `hostname` de otras entradas del archivo.

> **Nota:**

> Actualmente, el VDA de Linux no admite la truncación de nombres NetBIOS. Por lo tanto, el nombre de host no debe superar los 15 caracteres.

> **Sugerencia:**

> Utilice solo los caracteres a–z, A–Z, 0–9 y el guion (-). Evite los guiones bajos (_), los espacios y otros símbolos. No inicie un nombre de host con un número ni lo termine con un guion. Esta regla también se aplica a los nombres de host de Delivery Controller.

Paso 1d: Comprobar el nombre de host

verificar que el nombre de host esté configurado correctamente:

```
hostname
```

Este comando devuelve solo el nombre de host de la máquina y no su FQDN.

verificar que el FQDN está configurado correctamente:

```
hostname -f
```

Este comando devuelve el FQDN de la máquina.

Paso 1e: Deshabilitar DNS de multidifusión

La configuración predeterminada tiene habilitado el DNS de multidifusión (**mDNS**), lo que puede provocar resultados inconsistentes en la resolución de nombres.

Para deshabilitar **mDNS**, edite **/etc/nsswitch.conf** y cambie la línea que contiene:

`hosts: files mdns_minimal [NOTFOUND=return] dns`

A:

`hosts: files dns`

Paso 1f: Comprobar la resolución de nombres y la accesibilidad del servicio

verificar que puede resolver el FQDN y hacer ping al controlador de dominio y a Delivery Controller™:

```
nslookup domain-controller-fqdn



ping domain-controller-fqdn



nslookup delivery-controller-fqdn



ping delivery-controller-fqdn
```

Si no puede resolver el FQDN o hacer ping a ninguna de estas máquinas, revise los pasos antes de continuar.

Paso 1g: Configurar la sincronización del reloj (chrony)

Mantener una sincronización precisa del reloj entre los VDA, los Delivery Controllers y los controladores de dominio es crucial. Alojar el VDA de Linux como una máquina virtual (VM) puede causar problemas de desviación del reloj. Por esta razón, se prefiere sincronizar la hora con un servicio de hora remoto.

Instalar chrony:

```
apt-get install chrony
```

Como usuario root, edite **/etc/chrony/chrony.conf** y agregue una entrada de servidor para cada servidor de hora remoto:

`server peer1-fqdn-or-ip-address iburst`

`server peer2-fqdn-or-ip-address iburst`

En una implementación típica, sincronice la hora desde los controladores de dominio locales y no directamente desde los servidores públicos del grupo NTP. Agregue una entrada de servidor para cada controlador de dominio de Active Directory en el dominio.

Elimine cualquier otra entrada de **servidor** o **grupo** que aparezca, incluidas la dirección IP de bucle invertido, localhost y las entradas de servidor público ***.pool.ntp.org**.

Guarde los cambios y reinicie el demonio Chrony:

```
sudo systemctl restart chrony
```

Paso 1h: Instalar y especificar una base de datos para usar

Nota:

- Le recomendamos que utilice SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el VDA de Linux utiliza PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).
- Para instalaciones manuales, debe instalar SQLite, PostgreSQL o ambos manualmente. Puede utilizar una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux. Si instala tanto SQLite como PostgreSQL,

> puede especificar cuál usar editando **/etc/xdl/db.conf** después de instalar el paquete de Linux VDA.

INSTALAR POSTGRESQL

Esta sección describe cómo instalar la versión de PostgreSQL proporcionada por su distribución de Linux. Si es necesaria una versión personalizada de PostgreSQL, puede instalarla según sus requisitos específicos.

Ejecute los siguientes comandos para instalar PostgreSQL:

```
sudo apt-get install -y postgresql



sudo apt-get install -y libpostgresql-jdbc-java
```

Ejecute los siguientes comandos para iniciar PostgreSQL al arrancar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql



sudo systemctl restart postgresql
```

INSTALAR SQLITE

Para Ubuntu, ejecute el siguiente comando para instalar SQLite:

```
sudo apt-get install -y sqlite3
```

ESPECIFICAR UNA BASE DE DATOS PARA USAR

Si instala tanto SQLite como PostgreSQL, puede especificar cuál usar editando **/etc/xdl/db.conf** después de instalar el paquete de Linux VDA.

1. Ejecute **/opt/Citrix/VDA/sbin/ctxcleanup.sh**. Omita este paso si es una instalación nueva.
2. Edite **/etc/xdl/db.conf** para especificar una base de datos que usar. El siguiente es un ejemplo de archivo **db.conf**:

```
# database configuration file for Linux VDA



## database choice

# possible choices are:

#     SQLite

#     PostgreSQL

# default choice is PostgreSQL

DbType="PostgreSQL"




## database port

# specify database port for the database.

# if not specified, default port will be used:

# SQLite: N/A

# PostgreSQL: 5432

DbPort=5432




## PostgreSQL customized

# only the following value means true, otherwise false:

#     true

#     yes
```

```
#     y

#     YES

#     Y

# default is false

DbCustomizePostgreSQL=false



## PostgreSQL service name

# specify the service name of PostgreSQL for Linux VDA

# default is "postgresql"

DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

3. Ejecute **ctxsetup.sh**.

Nota:

También puede usar **/etc/xdl/db.conf** para configurar el número de puerto para PostgreSQL.

Paso 1i: Instalar Motif

```
sudo apt-get install -y libxm4
```

Paso 1j: Instalar otros paquetes

Para Ubuntu 24.04:

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit
```

```
sudo apt-get install -y libldap2

sudo apt-get install -y krb5-user

sudo apt-get install -y libgtk2.0-0
```

Para Ubuntu 22.04:

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit

sudo apt-get install -y libldap-2.5-0

sudo apt-get install -y krb5-user

sudo apt-get install -y libgtk2.0-0
```

Paso 2: Preparar el hipervisor

Se requieren algunos cambios al ejecutar el VDA de Linux como una VM en un hipervisor compatible. Realice los siguientes cambios según la plataforma de hipervisor en uso. No se requieren cambios si ejecuta la máquina Linux en hardware físico.

Corregir la sincronización de la hora en XenServer (anteriormente Citrix Hypervisor™)

Cuando la función de sincronización de hora de XenServer® está habilitada, dentro de cada VM Linux paravirtualizada, experimentará problemas con NTP y XenServer. Ambos intentan administrar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con el NTP. Este caso requiere deshabilitar la sincronización de hora del host. No se requieren cambios en el modo HVM.

Si está ejecutando un kernel de Linux paravirtualizado con las herramientas de VM de XenServer instaladas, puede comprobar si la función de sincronización de hora de XenServer está presente y habilitada desde la VM de Linux:

```
su -
```

```
cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve 0 o 1:

- 0 - La función de sincronización de hora está habilitada y debe deshabilitarse.
- 1 - La función de sincronización de hora está deshabilitada y no se requiere ninguna acción adicional.

Si el archivo /proc/sys/xen/independent_wallclock no está presente, los siguientes pasos no son necesarios.

Si está habilitada, deshabilite la función de sincronización de hora escribiendo 1 en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Para que este cambio sea permanente y persistente después de reiniciar, edite el archivo **/etc/sysctl.conf** y agregue la línea:

`xen.independent_wallclock = 1`

Para verificar estos cambios, reinicie el sistema:

```
su -



cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve el valor 1.

Corregir la sincronización de hora en Microsoft Hyper-V

Las máquinas virtuales Linux con los Servicios de integración de Linux de Hyper-V instalados pueden usar la función de sincronización de hora de Hyper-V para utilizar la hora del sistema operativo host. Para asegurarse de que el reloj del sistema permanezca preciso, habilite esta función junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para la configuración de una máquina virtual Linux, seleccione **Servicios de integración**.

3. Asegúrese de que la opción **Sincronización de hora** esté seleccionada.

> **Nota:**
>
> Este enfoque es diferente al de VMware y XenServer (anteriormente Citrix Hypervisor), donde la sincronización de hora del host está deshabilitada para evitar conflictos con NTP. La sincronización de hora de Hyper-V puede coexistir y complementar la sincronización de hora de NTP.

Corregir la sincronización de hora en ESX y ESXi

Cuando la función de sincronización de hora de VMware está habilitada, dentro de cada máquina virtual Linux paravirtualizada, experimentará problemas con NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con NTP. Este caso requiere deshabilitar la sincronización de hora del host.

Si está ejecutando un kernel de Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Edite la configuración de la máquina virtual Linux.
3. En el cuadro de diálogo **Virtual Machine Properties**, abra la ficha **Options**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Advanced**, desactive **Synchronize guest time with host**.

Paso 3: Agregue la máquina virtual Linux al dominio de Windows

Los siguientes métodos están disponibles para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Servicio de autenticación Quest
- Centrify DirectControl
- SSSD
- PBIS

Siga las instrucciones según el método elegido.

> **Nota:**
>
> Es posible que los inicios de sesión fallen cuando se utiliza el mismo nombre de usuario para la cuenta local en el VDA de Linux y la cuenta en AD.

Samba Winbind

INSTALAR O ACTUALIZAR LOS PAQUETES NECESARIOS

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

HABILITAR EL DEMONIO WINBIND PARA QUE SE INICIE AL ARRANCAR LA MÁQUINA

El demonio Winbind debe configurarse para que se inicie al arrancar la máquina:

```
sudo systemctl enable winbind
```

> **Nota:**
>
> Asegúrese de que el script `winbind` se encuentra en `/etc/init.d`.

CONFIGURAR KERBEROS

Abra **/etc/krb5.conf** como usuario root y realice la siguiente configuración:

> **Nota:**
>
> Configure Kerberos según su infraestructura de AD. La siguiente configuración está pensada para el modelo de dominio único y bosque único.

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM = {`

`admin_server = domain-controller-fqdn`

`kdc = domain-controller-fqdn`

`}`

`[domain_realm]`

`domain-dns-name = REALM`

`.domain-dns-name = REALM`

El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como **example.com**. El **REALM** es el nombre del reino de Kerberos en mayúsculas, como **EXAMPLE.COM**.

CONFIGURAR AUTENTICACIÓN DE WINBIND

Configure Winbind manualmente porque Ubuntu no tiene una herramienta como **authconfig** en RHEL y yast2 en SUSE.

Abra **/etc/samba/smb.conf** ejecutando el comando **vim /etc/samba/smb.conf** y, a continuación, realice la siguiente configuración:

`[global]`

`workgroup = WORKGROUP`

`security = ADS`

`realm = REALM`

`encrypt passwords = yes`

`idmap config *:range = 16777216-33554431`

`kerberos method = secrets and keytab`

`winbind refresh tickets = yes`

`template shell = /bin/bash`

WORKGROUP es el primer campo en **REALM**, y **REALM** es el nombre del reino Kerberos en mayúsculas.

CONFIGURAR NSSWITCH

Abra **/etc/nsswitch.conf** y añada **winbind** a las siguientes líneas:

`passwd: compat winbind`

`group: compat winbind`

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
sudo net ads join REALM -U user
```

Donde **REALM** es el nombre del reino Kerberos en mayúsculas, y **user** es un usuario de dominio con permisos para agregar equipos al dominio.

REINICIAR `WINBIND`

```
sudo systemctl restart winbind
```

CONFIGURAR PAM PARA WINBIND

Ejecute el siguiente comando y asegúrese de que las opciones **Autenticación Winbind NT/ Active Directory** y **Crear directorio de inicio al iniciar sesión** estén seleccionadas:

```
sudo pam-auth-update
```

> **Sugerencia:**
>
> El demonio **winbind** permanece en ejecución solo si la máquina está unida a un dominio.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA, ya sean Windows o Linux, tengan un objeto de equipo en Active Directory.

Ejecute el comando **net ads** de **Samba** para verificar que la máquina está unida a un dominio:

```
sudo net ads testjoin
```

Ejecute el siguiente comando para verificar información adicional del dominio y del objeto de equipo:

```
sudo net ads info
```

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Para verificar que Kerberos está configurado correctamente para su uso con el VDA de Linux, verificar que el archivo **keytab** del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando **kinit** de Kerberos para autenticar la máquina con el controlador de dominio utilizando estas claves:

```
sudo kinit -k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utiliza el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT para la cuenta de la máquina se ha almacenado en caché utilizando:

```
sudo klist
```

Examine los detalles de la cuenta de la máquina utilizando:

```
sudo net ads status
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Utilice la herramienta **wbinfo** para verificar que los usuarios del dominio pueden autenticarse con el dominio:

```
wbinfo --krb5auth=domain\\username%password
```

El dominio especificado aquí es el nombre de dominio de AD, no el nombre de reino de Kerberos. Para el shell bash, el carácter de barra invertida (\\) debe escaparse con otra barra invertida. Este comando devuelve un mensaje que indica éxito o fracaso.

Para verificar que el módulo PAM de Winbind está configurado correctamente, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username



id -u
```

Nota:

Para ejecutar un comando SSH correctamente, asegúrese de que SSH está habilitado y funciona correctamente.

verificar que se ha creado un archivo de caché de credenciales de Kerberos correspondiente para el uid devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets en la caché de credenciales de Kerberos del usuario son válidos y no han caducado:

```
klist
```

Salga de la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

> **Sugerencia:**
>
> Si la autenticación de usuario se realiza correctamente, pero no puede ver su escritorio al iniciar sesión con una cuenta de dominio, reinicie la máquina y vuelva a intentarlo.

Servicio de autenticación de Quest

CONFIGURAR QUEST EN EL CONTROLADOR DE DOMINIO

Suponga que ha instalado y configurado el software Quest en los controladores de dominio de Active Directory y que se le han concedido privilegios administrativos para crear objetos de equipo en `Active Directory`.

PERMITIR QUE LOS USUARIOS DEL DOMINIO INICIEN SESIÓN EN MÁQUINAS LINUX VDA

Para permitir que los usuarios del dominio establezcan sesiones HDX™ en una máquina Linux VDA:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory para esa cuenta de usuario.
2. Seleccione la ficha **Cuenta de Unix**.
3. Marque **Habilitado para Unix**.
4. Establezca el **Número de GID principal** en el ID de grupo de un grupo de usuarios de dominio real.

> **Nota:**
>
> Estas instrucciones son equivalentes para configurar usuarios de dominio para iniciar sesión mediante la consola, RDP, SSH o cualquier otro protocolo de acceso remoto.

CONFIGURAR QUEST EN LINUX VDA

Solucionar la aplicación de la política de SELinux
El entorno RHEL predeterminado tiene SELinux totalmente aplicado. Esta aplicación interfiere con los mecanismos IPC de socket de dominio Unix utilizados por Quest e impide que los usuarios del dominio inicien sesión.

La forma más cómoda de solucionar este problema es deshabilitar SELinux. Como usuario root, edite **/etc/selinux/config** y cambie la configuración de **SELinux**:

`SELINUX=disabled`

Este cambio requiere un reinicio de la máquina:

```
reboot
```

Importante:

Utilice esta configuración con precaución. Volver a habilitar la aplicación de la política de SELinux después de deshabilitarla puede provocar un bloqueo completo, incluso para el usuario root y otros usuarios locales.

Configurar el demonio VAS

La renovación automática de los tickets de Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar deshabilitada:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Este comando establece el intervalo de renovación en nueve horas (32 400 segundos), que es una hora menos que la vida útil predeterminada del ticket de 10 horas. Establezca este parámetro en un valor inferior en sistemas con una vida útil del ticket más corta.

Configurar PAM y NSS

Para habilitar el inicio de sesión de usuarios de dominio a través de HDX y otros servicios como su, ssh y RDP, ejecute los siguientes comandos para configurar PAM y NSS manualmente:

```
sudo /opt/quest/bin/vastool configure pam



sudo /opt/quest/bin/vastool configure nss
```

UNIRSE AL DOMINIO DE WINDOWS

Una la máquina Linux al dominio de Active Directory mediante el comando **vastool** de Quest:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

El usuario es cualquier usuario de dominio con permisos para unir equipos al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Reinicie la máquina Linux después de unirse al dominio.

VERIFICAR PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA, ya sean Windows o Linux, tengan un objeto de equipo en Active Directory. Para verificar que una máquina Linux unida a Quest está en el dominio:

```
sudo /opt/quest/bin/vastool info domain
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. Si la máquina no está unida a ningún dominio, aparece el siguiente error:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

VERIFICAR AUTENTICACIÓN DE USUARIO

Para verificar que Quest puede autenticar usuarios de dominio a través de PAM, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username



id -u
```

verificar que se ha creado un archivo de caché de credenciales de Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets en la caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
```

Salga de la sesión.

```
exit
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Centrify DirectControl

UNIRSE AL DOMINIO DE WINDOWS

Con el agente de Centrify DirectControl instalado, una la máquina Linux al dominio de Active Directory mediante el comando **adjoin** de Centrify:

```
su –

adjoin -w -V -u user domain-name
```

El parámetro **user** es cualquier usuario de dominio de Active Directory con permisos para unir equipos al dominio de **Active Directory**. El parámetro **domain-name** es el nombre del dominio al que se unirá la máquina Linux.

VERIFICAR PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA, ya sean Windows o Linux, tengan un objeto de equipo en **Active Directory**. Para verificar que una máquina Linux unida a Centrify está en el dominio:

```
su –



adinfo
```

verificar que el valor de **Unido al dominio** es válido y que el **modo CentrifyDC** devuelve **conectado**. Si el modo se queda atascado en el estado inicial, el cliente de Centrify está experimentando problemas de conexión o autenticación con el servidor.

Hay disponible información de diagnóstico y del sistema más completa mediante:

```
adinfo --sysinfo all



adinfo --diag
```

Pruebe la conectividad con los distintos servicios de Active Directory y Kerberos.

```
adinfo --test
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

SSSD

CONFIGURAR KERBEROS

Ejecute el siguiente comando para instalar Kerberos:

```
sudo apt-get install krb5-user
```

Para configurar Kerberos, abra **/etc/krb5.conf** como root y establezca los parámetros:

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. Las siguientes configuraciones están pensadas para el modelo de dominio único y bosque único.

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc = domain-controller-fqdn`

`}`

`[domain_realm]`

`domain-dns-name = REALM`

`.domain-dns-name = REALM`

El parámetro `domain-dns-name` en este contexto es el nombre de dominio DNS, como example.com. El *REALM* es el nombre del reino Kerberos en mayúsculas, como EXAMPLE.COM.

UNIRSE AL DOMINIO

SSSD debe configurarse para usar Active Directory como su proveedor de identidades y Kerberos para la autenticación. Sin embargo, SSSD no proporciona funciones de cliente de AD para unirse al dominio y administrar el archivo keytab del sistema. En su lugar, puede usar **adcli**, **realmd** o **Samba**.

> **Nota:**
>
> Esta sección solo proporciona información para **adcli** y **Samba**.

- **Si usa adcli para unirse al dominio, complete los siguientes pasos:**

1. Instale **adcli**.

   ```
   sudo apt-get install adcli
   ```

2. Únase al dominio con **adcli**.

   Elimine el archivo keytab del sistema antiguo y únase al dominio usando:

   ```
   su -


   rm -rf /etc/krb5.keytab
   ```

```
adcli join domain-dns-name -U user -H hostname-fqdn
```

El **usuario** es un usuario de dominio con permisos para agregar máquinas al dominio. El **hostname-fqdn** es el nombre de host en formato FQDN para la máquina.

La opción **-H** es necesaria para que **adcli** genere el SPN en el formato host/hostname-fqdn@REALM, que requiere el VDA de Linux.

3. verificar la pertenencia al dominio.

   Para las máquinas Ubuntu 22.04, ejecute el comando `adcli testjoin` para probar si las máquinas están unidas al dominio.

- **Si usa Samba para unirse al dominio, complete los siguientes pasos:**

1. Instale el paquete.

```
sudo apt-get install samba krb5-user
```

2. Configure **Samba**.

   Abra **/etc/samba/smb.conf** y realice los siguientes ajustes:

   `[global]`

   `workgroup =` *`WORKGROUP`*

   `security = ADS`

   `realm =` *`REALM`*

   `client signing = yes`

   `client use spnego = yes`

   `kerberos method = secrets and keytab`

   WORKGROUP es el primer campo en **REALM**, y **REALM** es el nombre del ámbito Kerberos en mayúsculas.

3. Una el dominio con **Samba**.

   Su controlador de dominio debe ser accesible y debe tener una cuenta de Windows con permisos para agregar equipos al dominio.

```
sudo net ads join REALM -U user
```

Donde **REALM** es el nombre del ámbito Kerberos en mayúsculas, y **user** es un usuario de dominio con permisos para agregar equipos al dominio.

CONFIGURAR SSSD

Instalar o actualizar los paquetes necesarios:

Instale los paquetes de SSSD y de configuración necesarios si aún no están instalados:

```
sudo apt-get install sssd
```

Si los paquetes ya están instalados, se recomienda una actualización:

```
sudo apt-get install --only-upgrade sssd
```

> **Nota:**
>
> De forma predeterminada, el proceso de instalación en Ubuntu configura automáticamente **nsswitch.conf** y el módulo de inicio de sesión PAM.

CONFIGURAR SSSD

Se requieren cambios en la configuración de SSSD antes de iniciar el demonio SSSD. Para algunas versiones de SSSD, el archivo de configuración **/etc/sssd/sssd.conf** no se instala de forma predeterminada y debe crearse manualmente. Como root, cree o abra **/etc/sssd/sssd.conf** y realice los siguientes ajustes:

`[sssd]`

`services = nss, pam`

`config_file_version = 2`

`domains =` *`domain-dns-name`*

`[domain/`*`domain-dns-name`*`]`

`id_provider = ad`

```
access_provider = ad

auth_provider = krb5

krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true

override_homedir = /home/%d/%u

default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```

> **Nota:**
>
> ldap_id_mapping se establece en **true** para que SSSD se encargue de asignar los SID de Windows a los UID de Unix. De lo contrario, Active Directory debe poder proporcionar extensiones POSIX. El servicio PAM `ctxhdx` se añade a ad_gpo_map_remote_interactive.

> El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como example.com. El **REALM** es el nombre del reino Kerberos en mayúsculas, como EXAMPLE.COM. No es necesario configurar el nombre de dominio NetBIOS.

> Para obtener información sobre la configuración, consulte las páginas man de sssd.conf y `sssd-ad`.

> El demonio SSSD requiere que el archivo de configuración solo tenga permisos de lectura para el propietario:

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

INICIAR EL DEMONIO SSSD

Ejecute los siguientes comandos para iniciar el demonio SSSD ahora y para habilitar que el demonio se inicie al arrancar la máquina:

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

CONFIGURACIÓN DE PAM

Ejecute el siguiente comando y asegúrese de que las opciones **SSS authentication** y **Create home directory on login** estén seleccionadas:

```
sudo pam-auth-update
```

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`.

- Si utiliza **adcli** para verificar la pertenencia al dominio, ejecute el comando `sudo adcli info domain-dns-name` para mostrar la información del dominio.
- Si utiliza **Samba** para verificar la pertenencia al dominio, ejecute el comando `sudo net ads testjoin` para verificar que la máquina está unida a un dominio y el comando `sudo net ads info` para verificar información adicional del dominio y del objeto de equipo.

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Para verificar que Kerberos está configurado correctamente para su uso con el Linux VDA, verificar que el archivo keytab del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando Kerberos `kinit` para autenticar la máquina con el controlador de dominio mediante estas claves:

```
sudo kinit -k MACHINE\$@REALM
```

Los nombres de la máquina y del dominio deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución de shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de dominio de Kerberos. Asegúrese de que se utiliza el nombre de dominio. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el TGT de la cuenta de máquina se ha almacenado en caché mediante:

```
sudo klist
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

SSSD no proporciona una herramienta de línea de comandos para probar la autenticación directamente con el demonio, y solo se puede hacer a través de PAM.

Para verificar que el módulo PAM de SSSD está configurado correctamente, inicie sesión en el Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

verificar que los tickets de Kerberos devueltos por el comando **klist** son correctos para ese usuario y no han caducado.

Como usuario root, verificar que se ha creado un archivo de caché de tickets correspondiente para el uid devuelto por el comando anterior **id -u**:

```
ls /tmp/krb5cc_uid
```

Se puede realizar una prueba similar iniciando sesión en KDE o Gnome Display Manager. Continúe con Paso 6: Instalar Linux VDA después de la verificación de unión al dominio.

PBIS

DESCARGAR EL PAQUETE PBIS NECESARIO

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

HACER EJECUTABLE EL SCRIPT DE INSTALACIÓN DE PBIS

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

EJECUTAR EL SCRIPT DE INSTALACIÓN DE PBIS

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

El **usuario** es un usuario de dominio que tiene permisos para agregar equipos al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Nota: Para establecer Bash como shell predeterminado, ejecute el comando **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**.

VERIFICAR PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para verificar que una máquina Linux unida a PBIS está en el dominio:

```
/opt/pbis/bin/domainjoin-cli query
```

Si la máquina está unida a un dominio, este comando devuelve la información sobre el dominio de AD y la OU a los que está unida actualmente. De lo contrario, solo aparece el nombre de host.

VERIFICAR AUTENTICACIÓN DE USUARIO

Para verificar que PBIS puede autenticar a los usuarios del dominio a través de PAM, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
sudo ssh localhost -l domain\\user



id -u
```

verificar que se ha creado un archivo de caché de credenciales Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

Cierre la sesión.

```
exit
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Paso 4: Instalar .NET

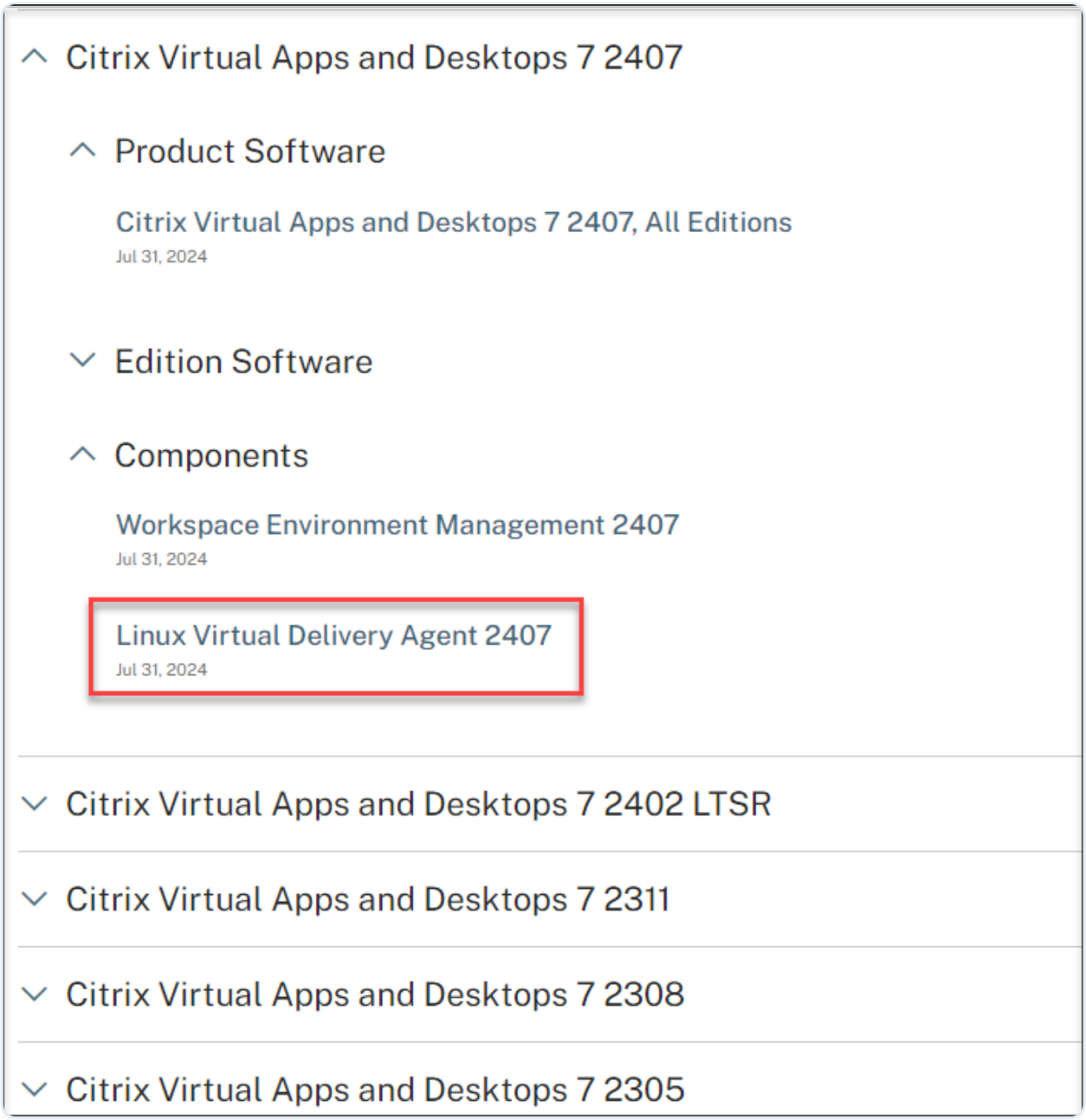
Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Después de instalar .NET, ejecute el comando **which dotnet** para encontrar la ruta de tiempo de ejecución.

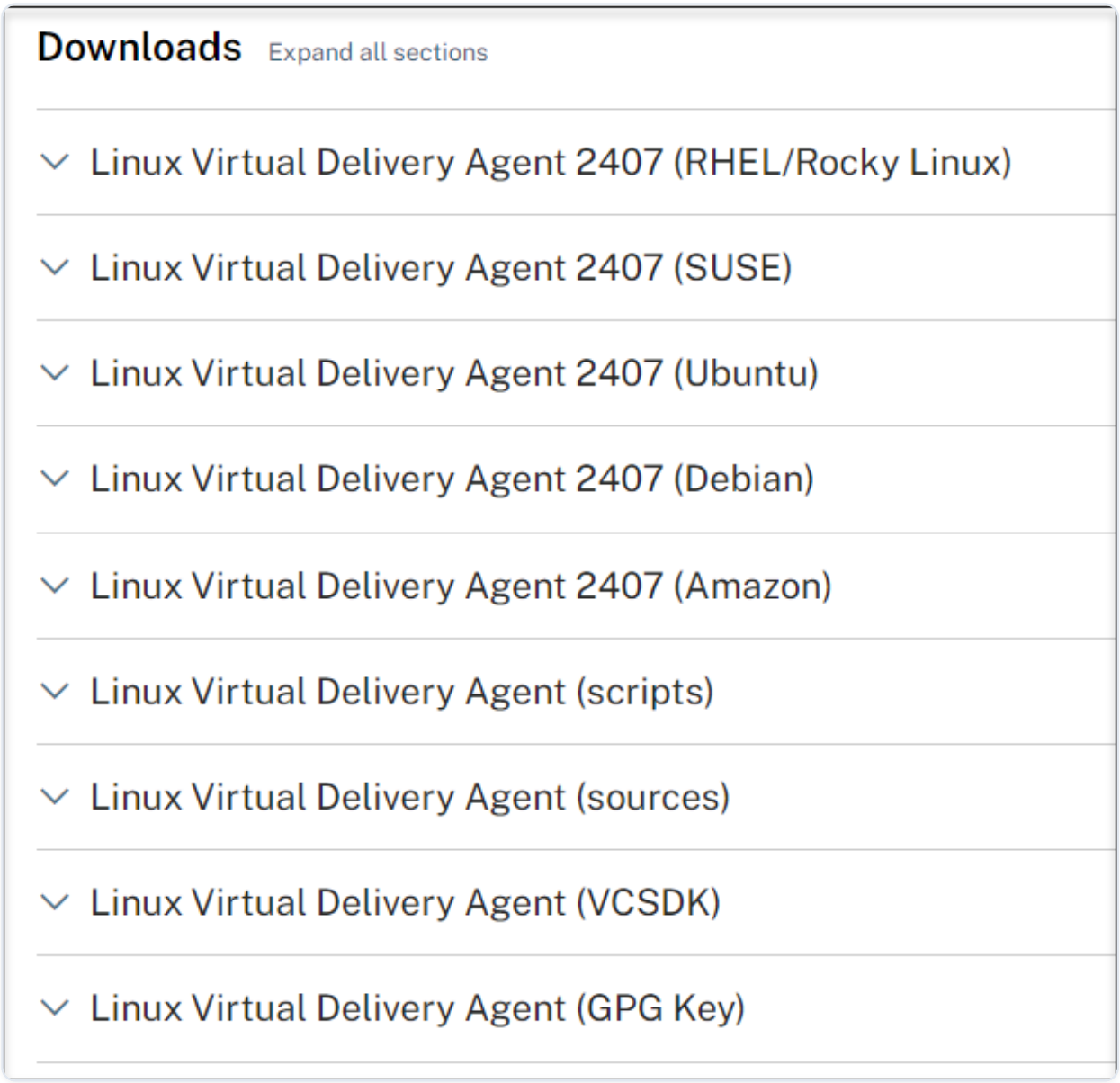
Según la salida del comando, establezca la ruta binaria de tiempo de ejecución de .NET. Por ejemplo, si la salida del comando es /aa/bb/dotnet, use /aa/bb como la ruta binaria de .NET.

Paso 5: Descargar el paquete de Linux VDA

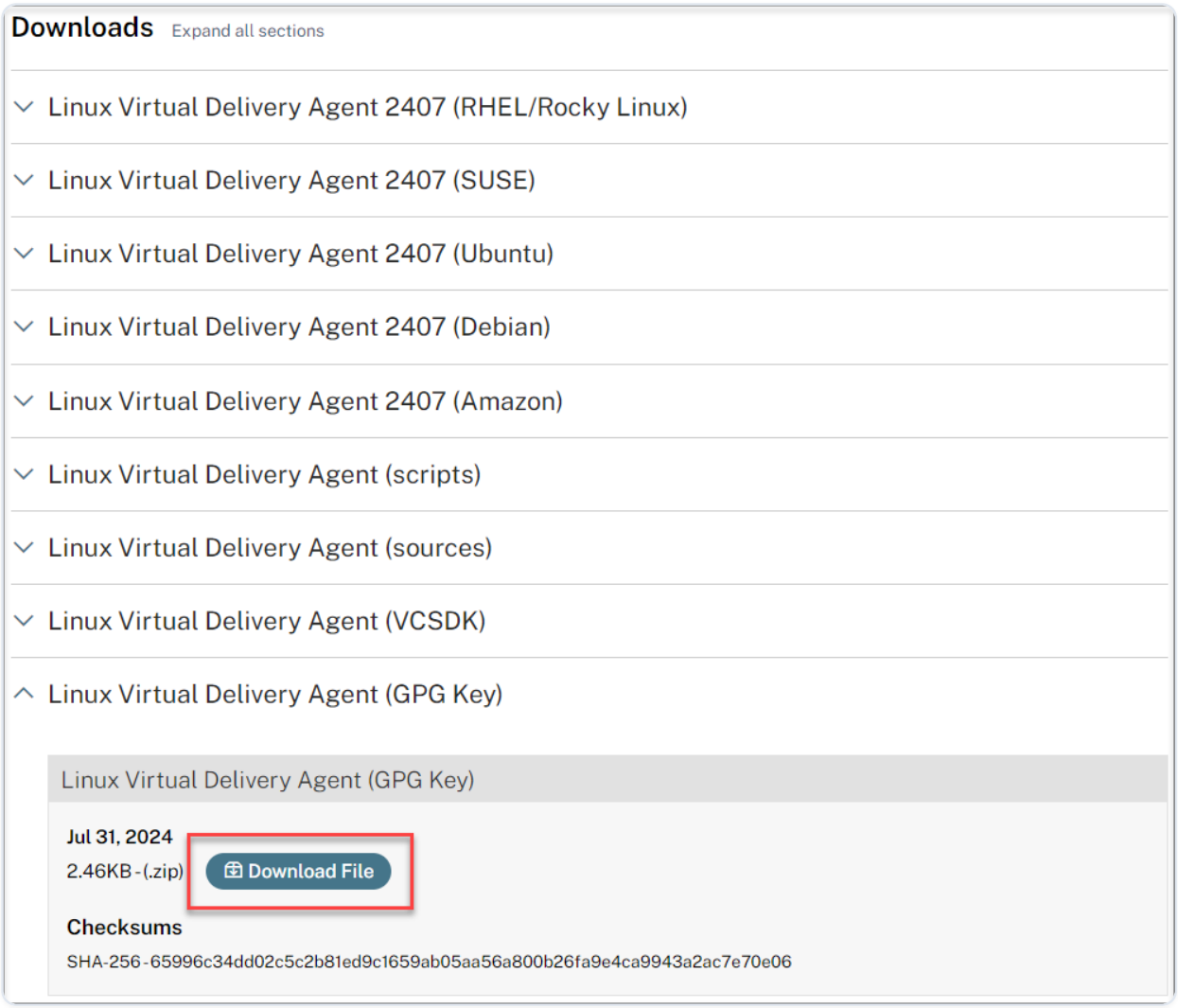
1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Expanda **Componentes** para encontrar el Linux VDA. Por ejemplo:



4. Haga clic en el enlace de Linux VDA para acceder a las descargas de Linux VDA.



5. Descargue el paquete de Linux VDA que coincida con su distribución de Linux.
6. Descargue la clave pública GPG que puede usar para verificar la integridad del paquete de Linux VDA. Por ejemplo:



Para verificar la integridad del paquete de Linux VDA, ejecute los siguientes comandos para importar la clave pública a la base de datos DEB y comprobar la integridad del paquete:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Paso 6: Instalar el Linux VDA

Paso 6a: Instalar el Linux VDA

Instale el software de Linux VDA mediante el administrador de paquetes de Debian:

```
sudo dpkg –i <PATH>/<Linux VDA DEB>

apt-get install -f
```

Nota:

Para Ubuntu 24.04/22.04 en GCP, deshabilite RDNS. Para ello, agregue la línea **rdns = false** debajo de en /etc/krb5.conf.

Lista de dependencias de Debian para Ubuntu 24.04:

```
openjdk-17-jdk >= 17

imagemagick >= 8:6.9.12

libgtkmm-3.0-1t64 >= 3.24.9

ufw >= 0.36

ubuntu-desktop >= 1.539

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.39

gtk3-nocsd >= 3

bash >= 5.2

findutils >= 4.9.0

sed >= 4.9

cups >= 2.4

libmspack0t64 >= 0.11

curl >= 8.5.0

libbsd-dev >= 0.12.1-1build1
```

```
ibus >= 1.5

libqt5dbus5 >= 5.15~

libgoogle-perftools4 >= 2.15

libpython3.12 >= 3.12~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.98

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

libimlib2 >= 1.12.1

libfuse2 >= 2.9

mutter >= 46.0

pulseaudio-utils >= 16.1
```

Lista de dependencias de Debian para Ubuntu 22.04:

```
openjdk-17-jdk >= 17

imagemagick >= 8:6.9.11

libgtkmm-3.0-1v5 >= 3.24.5

ufw >= 0.36

ubuntu-desktop >= 1.481

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8
```

```
util-linux >= 2.37

gtk3-nocsd >= 3

bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4

libmspack0 >= 0.10

ibus >= 1.5

libqt5dbus5 >= 5.15~

libgoogle-perftools4    2.9~

libpython3.10 >= 3.10~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

libimlib2 >= 1.7.4

libfuse2 >= 2.9

mutter >= 42.5
```

Nota:

Para ver una matriz de las distribuciones de Linux y las versiones de Xorg que admite esta versión de Linux VDA, consulte Requisitos del sistema.

Paso 6b: Actualizar el Linux VDA (opcional)

El Linux VDA admite actualizaciones desde la versión más reciente. Por ejemplo, puede actualizar el Linux VDA de 2308 a 2311 y de 1912 LTSR a 2203 LTSR.

```
sudo dpkg -i <PATH>/<Linux VDA deb>



sudo apt-get install -f
```

Nota:

- La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de realizar una actualización, asegúrese de hacer una copia de seguridad de los archivos.
- A partir de la versión 2407, el Linux VDA delega en los administradores de paquetes **rpm** o **dpkg** la gestión de los archivos de configuración durante las actualizaciones. A continuación, se describe cómo interactúan rpm y dpkg con los cambios en los archivos de configuración:
  - **rpm**: de forma predeterminada, conserva la versión local y guarda la nueva versión del paquete con una extensión .rpmnew.
  - **dpkg**: le pide interactivamente que elija cómo proceder. Para actualizar el Linux VDA de forma silenciosa, conservando el archivo de configuración local y guardando la nueva versión del paquete como **.dpkg-new** o **.dpkg-dist**, utilice el siguiente comando:

    ```
    dpkg --force-confold -i package.deb  # Always keep your version,
    then save new package's version as *.dpkg-new or *.dpkg-dist
    ```

Paso 7: Instalar los controladores NVIDIA GRID

Para habilitar HDX 3D Pro, debe instalar los controladores NVIDIA GRID en el hipervisor y en las máquinas VDA.

Para instalar y configurar NVIDIA GRID Virtual GPU Manager (el controlador de host) en los hipervisores específicos, consulte las siguientes guías:

- XenServer
- VMware ESX
- Nutanix AHV

Para instalar y configurar los controladores de VM invitada de NVIDIA GRID, realice los siguientes pasos generales:

1. Asegúrese de que la VM invitada esté apagada.
2. En el panel de control del hipervisor, asigne una GPU a la VM.
3. Inicie la VM.
4. Instale el controlador de la VM invitada (de su proveedor de la nube o NVIDIA) en la VM.

Paso 8: Configurar el Linux VDA

> **Nota:**

> Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional **en_US.UTF-8** esté instalada en su sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando **sudo locale-gen en_US.UTF-8**. Para Debian, edite el archivo **/etc/locale.gen** descomentando la línea **# en_US.UTF-8 UTF-8** y, a continuación, ejecute el comando **sudo locale-gen**.

> Después de instalar el paquete, debe configurar el Linux VDA ejecutando el script ctxsetup.sh. Antes de realizar cualquier cambio, el script verifica el entorno y se asegura de que todas las dependencias estén instaladas. Si es necesario, puede volver a ejecutar el script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manualmente con preguntas o automáticamente con respuestas preconfiguradas. Revise la Ayuda sobre el script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

Configuración guiada

Ejecute una configuración manual con preguntas guiadas:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Configuración automatizada

Para una instalación automatizada, las opciones requeridas por el script de configuración se pueden proporcionar con variables de entorno. Si todas las variables requeridas están presentes, el script no solicita ninguna información al usuario, lo que permite un proceso de instalación mediante script.

Las variables de entorno admitidas incluyen:

- **CTX_XDL_NON_DOMAIN_JOINED='y\|n'** – Si se une la máquina a un dominio. El valor predeterminado es 'n'. Para escenarios unidos a un dominio, establézcalo en 'n'.
- **CTX_XDL_AD_INTEGRATION='winbind\|sssd\|centrify\|pbis\|quest'** – El Linux VDA requiere la configuración de Kerberos para autenticarse con los Delivery Controllers. La configuración de Kerberos se determina a partir de la herramienta de integración de Active Directory instalada y configurada en el sistema.
- **CTX_XDL_DDC_LIST='<list-ddc-fqdns\>'** – El Linux VDA requiere una lista de Nombres de Dominio Completamente Cualificados (FQDN) de Delivery Controller, separados por espacios, para registrarse con un Delivery Controller. Se debe especificar al menos un FQDN o CNAME.
- **CTX_XDL_VDI_MODE='y\|n'** – Si se debe configurar la máquina como un modelo de entrega de escritorio dedicado (VDI) o un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca el valor en **'y'**.
- **CTX_XDL_HDX_3D_PRO='y\|n'** – El Linux VDA es compatible con HDX 3D Pro, un conjunto de tecnologías de aceleración de GPU diseñadas para optimizar la virtualización de aplicaciones con gráficos complejos. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única), es decir, CTX_XDL_VDI_MODE=**'y'**.
- **CTX_XDL_START_SERVICE='y\|n'** – Determina si los servicios del Linux VDA se inician cuando la configuración está completa.
- **CTX_XDL_REGISTER_SERVICE='y\|n'** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES='y\|n'** – Los servicios del Linux VDA requieren que las conexiones de red entrantes se permitan a través del firewall del sistema. Puede abrir los puertos necesarios (por defecto, los puertos 80 y 1494) automáticamente en el firewall del sistema para Linux Virtual Desktop.

- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/kde/mate/xfce/'<none\>'** – Especifica el entorno de escritorio GNOME, GNOME Classic, KDE, MATE o **Xfce** que se utilizará en las sesiones. Si lo establece en **'<none\>'**, se utiliza el escritorio predeterminado configurado en el VDA.

  También puede cambiar entre entornos de escritorio ejecutando comandos o usando la bandeja del sistema. Para obtener más información, consulte Comandos para cambiar de escritorio y Bandeja del sistema.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET para admitir el nuevo servicio de agente de broker (ctxvda). La ruta predeterminada es **'/usr/bin'**.
- **CTX_XDL_VDA_PORT=port-number** – El Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP.
- **CTX_XDL_SITE_NAME=<dns-name\>** – El Linux VDA descubre servidores LDAP a través de DNS. Para limitar los resultados de búsqueda de DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, establezca el valor en **'<none\>'**.
- **CTX_XDL_LDAP_LIST='<list-ldap-servers\>'** – El Linux VDA consulta DNS para descubrir servidores LDAP. Si DNS no puede proporcionar registros de servicio LDAP, puede proporcionar una lista de FQDN de LDAP separados por espacios con los puertos LDAP. Por ejemplo, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Para habilitar consultas LDAP más rápidas dentro de un bosque de Active Directory, habilite el Catálogo global en un controlador de dominio y especifique el número de puerto LDAP relevante como 3268. Esta variable se establece en **'<none\>'** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE=search-base-set** – El Linux VDA consulta LDAP a través de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=mycompany,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Si no es necesario, establezca el valor en **'<none\>'**.
- **CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'** – El Linux VDA admite la especificación de un nombre de Delivery Controller mediante un registro CNAME de DNS.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_NON_DOMAIN_JOINED='n'

export CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest
```

```
export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'

export CTX_XDL_VDI_MODE='y|n'

export CTX_XDL_HDX_3D_PRO='y|n'

export CTX_XDL_START_SERVICE='y|n'

export CTX_XDL_REGISTER_SERVICE='y|n'

export CTX_XDL_ADD_FIREWALL_RULES='y|n'

export CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|
xfce|'<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'

export CTX_XDL_VDA_PORT='<port-number>'

export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'

export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'

export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'

export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Al ejecutar el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que crea. Le recomendamos que cree un archivo de script de shell a partir de los comandos anteriores con **#\!/bin/bash** como primera línea.

Alternativamente, puede especificar todos los parámetros usando un solo comando:

```
sudo CTX_XDL_NON_DOMAIN_JOINED='n' \

CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest \

CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \

CTX_XDL_VDI_MODE='y|n' \
```

```
CTX_XDL_HDX_3D_PRO='y|n' \

CTX_XDL_START_SERVICE='y|n' \

CTX_XDL_REGISTER_SERVICE='y|n' \

CTX_XDL_ADD_FIREWALL_RULES='y|n' \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|xfce|'<none>' \

CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \

CTX_XDL_VDA_PORT='<port-number>' \

CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \

CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \

CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \

CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Eliminar cambios de configuración

En algunos casos, es posible que deba eliminar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete de Linux VDA.

Revise la Ayuda sobre este script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

Para eliminar los cambios de configuración:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

Importante:

> Este script elimina todos los datos de configuración de la base de datos y deja el Linux VDA inoperativo.

Registros de configuración

Los scripts **ctxsetup.sh** y **ctxcleanup.sh** muestran errores en la consola, con información adicional escrita en el archivo de registro de configuración **/tmp/xdl.configure.log**.

Reinicie los servicios de Linux VDA para que los cambios surtan efecto.

Desinstalar el software de Linux VDA

Para comprobar si Linux VDA está instalado y ver la versión del paquete instalado:

```
dpkg -l xendesktopvda
```

Para ver información más detallada:

```
apt-cache show xendesktopvda
```

Para desinstalar el software de Linux VDA:

```
dpkg -r xendesktopvda
```

> **Nota:**

> La desinstalación del software de Linux VDA elimina los datos de configuración de PostgreSQL asociados y otros datos de configuración. Sin embargo, el paquete de PostgreSQL y otros paquetes dependientes que se configuraron antes de la instalación de Linux VDA no se eliminan.

> **Sugerencia:**

> La información de esta sección no cubre la eliminación de paquetes dependientes, incluido PostgreSQL.

Paso 9: Ejecutar XDPing

Ejecute `sudo /opt/Citrix/VDA/bin/xdping` para comprobar si hay problemas de configuración comunes en un entorno de Linux VDA. Para obtener más información, consulte **XDPing**.

Paso 10: Ejecutar el Linux VDA

Una vez que haya configurado el Linux VDA mediante el script **ctxsetup.sh**, utilice los siguientes comandos para controlar el Linux VDA.

Iniciar el Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Detener el Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

> **Nota:**

> Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reinicia los servicios que detuvo.

> **Reiniciar el Linux VDA:**

Para reiniciar los servicios de Linux VDA:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Comprobar el estado del Linux VDA:

Para comprobar el estado de ejecución de los servicios de Linux VDA:

```
sudo systemctl status ctxvda



sudo systemctl status ctxhdx
```

Paso 11: Crear catálogos de máquinas

El proceso para crear catálogos de máquinas y agregar máquinas Linux VDA es similar al enfoque tradicional de Windows VDA. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Para crear catálogos de máquinas que contengan máquinas Linux VDA, existen algunas restricciones que diferencian el proceso de la creación de catálogos de máquinas para máquinas Windows VDA:

- Para el sistema operativo, seleccione:
  - La opción **Sistema operativo multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **Sistema operativo de sesión única** para un modelo de entrega de escritorios dedicados VDI.
- No mezcle máquinas Linux VDA y Windows VDA en el mismo catálogo de máquinas.

> **Nota:**

> Las versiones anteriores de Citrix Studio no admitían la noción de un "SO Linux". Sin embargo, seleccionar la opción **SO de Windows Server** o **SO de servidor** implica un modelo de entrega de escritorios compartidos alojados equivalente. Seleccionar la opción **SO de escritorio de Windows** o **SO de escritorio** implica un modelo de entrega de un solo usuario por máquina.

> **Sugerencia:**

> Si quita y vuelve a unir una máquina al dominio de Active Directory, debe quitar y volver a agregar la máquina al catálogo de máquinas.

Paso 12: Crear grupos de entrega

El proceso para crear un grupo de entrega y agregar catálogos de máquinas que contengan máquinas Linux VDA es casi idéntico al de las máquinas Windows VDA. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear grupos de entrega.

Para crear grupos de entrega que contengan catálogos de máquinas Linux VDA, se aplican las siguientes restricciones:

- Asegúrese de que los usuarios y grupos de AD que seleccione se hayan configurado correctamente para iniciar sesión en las máquinas Linux VDA.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No mezcle el grupo de entrega con catálogos de máquinas que contengan máquinas Windows.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2503.

Instalar Linux VDA en Debian manualmente

> **Importante:**

> Para instalaciones nuevas, le recomendamos que utilice easy install para una instalación rápida. Easy install ahorra tiempo y trabajo, y es menos propenso a errores que la instalación manual detallada en este artículo.

Paso 1: Preparar la información de configuración y la máquina Linux

Paso 1a: Establecer el nombre de host

Para asegurarse de que el nombre de host de la máquina se notifica correctamente, cambie el archivo **/etc/hostname** para que contenga solo el nombre de host de la máquina.

```
hostname
```

Paso 1b: Asignar una dirección de bucle invertido al nombre de host

Asegúrese de que el nombre de dominio DNS y el nombre de dominio completo (FQDN) de la máquina se notifiquen correctamente. Para ello, cambie la siguiente línea del archivo **/etc/hosts** para incluir el FQDN y el nombre de host como las dos primeras entradas:

```
127.0.0.1 hostname-fqdn hostname localhost
```

Por ejemplo:

```
127.0.0.1 vda01.example.com vda01 localhost
```

Quite cualquier otra referencia a `hostname-fqdn` o `hostname` de otras entradas del archivo.

> **Nota:**

> Actualmente, Linux VDA no admite la truncación de nombres NetBIOS. El nombre de host no debe superar los 15 caracteres.

> **Sugerencia:**

> Utilice solo los caracteres a–z, A–Z, 0–9 y el guion (-). Evite los guiones bajos (_), los espacios y otros símbolos. No inicie un nombre de host con un número ni lo termine con un guion. Esta regla también se aplica a los nombres de host de Delivery Controller.

Paso 1c: Comprobar el nombre de host

Reinicie la máquina y verificar que el nombre de host está configurado correctamente:

```
hostname
```

Este comando devuelve solo el nombre de host de la máquina y no su FQDN.

verificar que el FQDN está configurado correctamente:

```
hostname -f
```

Este comando devuelve el FQDN de la máquina.

Paso 1d: Deshabilitar DNS de multidifusión

La configuración predeterminada tiene el DNS de multidifusión (**mDNS**) habilitado, lo que puede provocar resultados de resolución de nombres inconsistentes.

Para deshabilitar **mDNS**, edite **/etc/nsswitch.conf** y cambie la línea:

`hosts: files mdns_minimal [NOTFOUND=return] dns`

A:

`hosts: files dns`

Paso 1e: Comprobar la resolución de nombres y la accesibilidad del servicio

verificar que puede resolver el FQDN y hacer ping al controlador de dominio y a Delivery Controller™:

```
nslookup domain-controller-fqdn



ping domain-controller-fqdn



nslookup delivery-controller-fqdn



ping delivery-controller-fqdn
```

Si no puede resolver el FQDN o hacer ping a ninguna de estas máquinas, revise los pasos antes de continuar.

Paso 1f: Configurar la sincronización del reloj (chrony)

Mantener una sincronización precisa del reloj entre los VDA, los Delivery Controllers y los controladores de dominio es crucial. Alojar el VDA de Linux como una máquina virtual (VM) puede causar problemas de desviación del reloj. Por esta razón, se prefiere sincronizar la hora con un servicio de hora remoto.

Instalar chrony:

```
apt-get install chrony
```

Como usuario root, edite **/etc/chrony/chrony.conf** y añada una entrada de servidor para cada servidor de hora remoto:

`server peer1-fqdn-or-ip-address iburst`

`server peer2-fqdn-or-ip-address iburst`

En una implementación típica, sincronice la hora desde los controladores de dominio locales y no directamente desde los servidores de grupo NTP públicos. Añada una entrada de servidor para cada controlador de dominio de Active Directory en el dominio.

Elimine cualquier otra entrada de **server** o **pool** listada, incluyendo la dirección IP de bucle invertido, localhost y las entradas de servidor público ***.pool.ntp.org**.

Guarde los cambios y reinicie el demonio Chrony:

```
sudo systemctl restart chrony
```

Paso 1g: Instalar paquetes

```
sudo apt-get install -y libsasl2-2



sudo apt-get install -y libgtk2.0-0
```

Paso 1h: Añadir repositorios para instalar las dependencias necesarias

Para Debian 11, añada la línea `deb http://deb.debian.org/debian/ bullseye main` al archivo /etc/apt/sources.list.

Paso 1i: Instalar y especificar una base de datos para usar

Nota:

- Le recomendamos que utilice SQLite solo para el modo VDI y PostgreSQL para un modelo de entrega de escritorios compartidos alojados.
- Para una instalación sencilla y MCS, puede especificar SQLite o PostgreSQL para usar sin tener que instalarlos manualmente. A menos que se especifique lo contrario a través de **/etc/xdl/db.conf**, el VDA de Linux utiliza PostgreSQL de forma predeterminada. Si necesita una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux, debe instalar la versión especificada manualmente, editar `/etc/xdl/db.conf` para reflejar la nueva versión e iniciar el servicio de PostgreSQL antes de ejecutar el script de instalación sencilla (`ctxinstall.sh`) o el script de MCS (`deploymcs.sh`).
- Para instalaciones manuales, debe instalar SQLite, PostgreSQL o ambos manualmente. Puede utilizar una versión personalizada de PostgreSQL en lugar de la versión proporcionada por su distribución de Linux. Si instala tanto SQLite como PostgreSQL, puede especificar uno de ellos para usarlo editando **/etc/xdl/db.conf** después de instalar el paquete VDA de Linux.

INSTALAR POSTGRESQL

Esta sección describe cómo instalar la versión de PostgreSQL proporcionada por su distribución de Linux. Si es necesaria una versión personalizada de PostgreSQL, puede instalarla según sus requisitos específicos.

Ejecute los siguientes comandos para instalar PostgreSQL:

```
sudo apt-get update



sudo apt-get install -y postgresql



sudo apt-get install -y libpostgresql-jdbc-java
```

Ejecute los siguientes comandos para iniciar PostgreSQL al arrancar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

INSTALAR SQLITE

Para Debian, ejecute el siguiente comando para instalar SQLite:

```
sudo apt-get install -y sqlite3
```

ESPECIFICAR UNA BASE DE DATOS PARA USAR

Si instala tanto SQLite como PostgreSQL, puede especificar uno de ellos para usarlo editando **/etc/xdl/db.conf** después de instalar el paquete VDA de Linux.

1. Ejecute **/opt/Citrix/VDA/sbin/ctxcleanup.sh**. Omita este paso si se trata de una instalación nueva.
2. Edite **/etc/xdl/db.conf** para especificar una base de datos que usar. El siguiente es un ejemplo del archivo **db.conf**:

   ```
   # database configuration file for Linux VDA



   ## database choice

   # possible choices are:

   #     SQLite

   #     PostgreSQL

   # default choice is PostgreSQL

   DbType="PostgreSQL"
   ```

```
## database port
# specify database port for the database.
# if not specified, default port will be used:
# SQLite: N/A
# PostgreSQL: 5432
DbPort=5432



## PostgreSQL customized
# only the following value means true, otherwise false:
#     true
#     yes
#     y
#     YES
#     Y
# default is false
DbCustomizePostgreSQL=false


## PostgreSQL service name
# specify the service name of PostgreSQL for Linux VDA
# default is "postgresql"
```

```
DbPostgreSQLServiceName="postgresql"
```

Para usar una versión personalizada de PostgreSQL, establezca **DbCustomizePostgreSQL** en true.

3. Ejecute **ctxsetup.sh**.

Nota:

También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

Paso 2: Preparar el hipervisor

Se requieren algunos cambios al ejecutar el VDA de Linux como una VM en un hipervisor compatible. Realice los siguientes cambios según la plataforma de hipervisor en uso. No se requieren cambios si ejecuta la máquina Linux en hardware físico.

Corregir la sincronización horaria en XenServer (anteriormente Citrix Hypervisor™)

Cuando la función de sincronización horaria de XenServer® está habilitada, dentro de cada VM Linux paravirtualizada, experimentará problemas con NTP y XenServer. Ambos intentan administrar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con NTP. Este caso requiere deshabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

Si ejecuta un kernel de Linux paravirtualizado con las herramientas de VM de XenServer instaladas, puede comprobar si la función de sincronización horaria de XenServer está presente y habilitada desde la VM de Linux:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve 0 o 1:

- 0 - La función de sincronización horaria está habilitada y debe deshabilitarse.
- 1 - La función de sincronización horaria está deshabilitada y no se requiere ninguna otra acción.

Si el archivo /proc/sys/xen/independent_wallclock no está presente, los siguientes pasos no son necesarios.

Si está habilitada, deshabilite la función de sincronización horaria escribiendo 1 en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Para que este cambio sea permanente y persistente después de reiniciar, edite el archivo **/etc/sysctl.conf** y agregue la línea:

`xen.independent_wallclock = 1`

Para verificar estos cambios, reinicie el sistema:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux con los Servicios de integración de Linux de Hyper-V instalados pueden usar la función de sincronización horaria de Hyper-V para usar la hora del sistema operativo host. Para garantizar que el reloj del sistema permanezca preciso, habilite esta función junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para la configuración de una máquina virtual Linux, seleccione **Integration Services**.
3. Asegúrese de que la opción **Time synchronization** esté seleccionada.

> **Nota:**
>
> Este enfoque es diferente al de VMware y XenServer (anteriormente Citrix Hypervisor), donde la sincronización horaria del host está deshabilitada para evitar conflictos con NTP. La sincronización horaria de Hyper-V puede coexistir y complementar la sincronización horaria de NTP.

Corregir la sincronización horaria en ESX y ESXi

Cuando la función de sincronización horaria de VMware está habilitada, dentro de cada máquina virtual Linux paravirtualizada experimentará problemas con el NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, asegúrese de que el reloj del sistema dentro de cada invitado Linux esté sincronizado con el NTP. Este caso requiere deshabilitar la sincronización horaria del host.

Si está ejecutando un kernel de Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Edite la configuración de la máquina virtual Linux.
3. En el cuadro de diálogo **Virtual Machine Properties**, abra la pestaña **Options**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Advanced**, desactive **Synchronize guest time with host**.

Paso 3: Añadir la VM Linux al dominio de Windows

Los siguientes métodos están disponibles para añadir máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Servicio de autenticación Quest
- Centrify DirectControl
- SSSD
- PBIS

Siga las instrucciones según el método elegido.

> **Nota:**

> Es posible que los inicios de sesión fallen si se utiliza el mismo nombre de usuario para la cuenta local en el VDA de Linux y la cuenta en AD.

Samba Winbind

INSTALAR O ACTUALIZAR LOS PAQUETES NECESARIOS

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

HABILITAR EL DEMONIO WINBIND PARA QUE SE INICIE AL ARRANCAR LA MÁQUINA

El demonio Winbind debe configurarse para que se inicie al arrancar la máquina:

```
sudo systemctl enable winbind
```

> **Nota:**
>
> Asegúrese de que el script `winbind` se encuentre en `/etc/init.d`.

CONFIGURAR KERBEROS

Abra **/etc/krb5.conf** como usuario root y realice la siguiente configuración:

> **Nota:**
>
> Configure Kerberos según su infraestructura de AD. La siguiente configuración está pensada para el modelo de dominio único y bosque único.

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` *`REALM`*

`.domain-dns-name` `=` *`REALM`*

El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como **example.com**. El **REALM** es el nombre del reino de Kerberos en mayúsculas, como **EXAMPLE.COM**.

CONFIGURAR LA AUTENTICACIÓN DE WINBIND

Abra **/etc/samba/smb.conf** ejecutando el comando **vim /etc/samba/smb.conf** y, a continuación, realice la siguiente configuración:

`[global]`

`workgroup =` *`WORKGROUP`*

`security = ADS`

`realm =` *`REALM`*

`encrypt passwords = yes`

`idmap config *:range = 16777216-33554431`

`kerberos method = secrets and keytab`

`winbind refresh tickets = yes`

`template shell = /bin/bash`

WORKGROUP es el primer campo en **REALM**, y **REALM** es el nombre del reino Kerberos en mayúsculas.

CONFIGURAR NSSWITCH

Abra **/etc/nsswitch.conf** y añada `winbind` a las siguientes líneas:

`passwd: files systemd winbind`

`group: files systemd winbind`

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para añadir equipos al dominio:

```
sudo net ads join <Kerberos realm name in uppercase> -U <domain user with permission to add computers to the domain>
```

REINICIAR WINBIND

```
sudo systemctl restart winbind
```

CONFIGURAR PAM PARA WINBIND

Ejecute el siguiente comando y asegúrese de que las opciones **Autenticación de Winbind NT/Active Directory** y **Crear directorio personal al iniciar sesión** estén seleccionadas:

```
sudo pam-auth-update
```

> **Sugerencia:**
>
> El demonio de **winbind** permanece en ejecución solo si la máquina está unida a un dominio.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA, ya sean Windows o Linux, tengan un objeto de equipo en `Active Directory`.

Ejecute el comando **net ads** de **Samba** para verificar que la máquina está unida a un dominio:

```
sudo net ads testjoin
```

Ejecute el siguiente comando para verificar información adicional del dominio y del objeto de equipo:

```
sudo net ads info
```

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Para verificar que Kerberos está configurado correctamente para su uso con el VDA de Linux, verificar que el archivo **keytab** del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las diversas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando Kerberos **kinit** para autenticar la máquina con el controlador de dominio utilizando estas claves:

```
sudo kinit -k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utiliza el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT para la cuenta de la máquina se ha almacenado en caché utilizando:

```
sudo klist
```

Examine los detalles de la cuenta de la máquina utilizando:

```
sudo net ads status
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Utilice la herramienta **wbinfo** para verificar que los usuarios del dominio pueden autenticarse con el dominio:

```
wbinfo --krb5auth=domain\\username%password
```

El dominio especificado aquí es el nombre de dominio de AD, no el nombre de reino de Kerberos. Para el shell bash, el carácter de barra invertida (\\) debe escaparse con otra barra invertida. Este comando devuelve un mensaje que indica éxito o fallo.

Para verificar que el módulo PAM de Winbind está configurado correctamente, inicie sesión en el VDA de Linux utilizando una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username
```

```
id -u
```

Nota:

Para ejecutar un comando SSH correctamente, asegúrese de que SSH está habilitado y funciona correctamente.

verificar que se ha creado un archivo de caché de credenciales de Kerberos correspondiente para el uid devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets en la caché de credenciales de Kerberos del usuario son válidos y no han caducado:

```
klist
```

Cierre la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola de Gnome o KDE. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Sugerencia:

Si la autenticación de usuario se realiza correctamente pero no puede mostrar su escritorio al iniciar sesión con una cuenta de dominio, reinicie la máquina e inténtelo de nuevo.

Servicio de autenticación Quest

CONFIGURAR QUEST EN EL CONTROLADOR DE DOMINIO

Suponga que ha instalado y configurado el software Quest en los controladores de dominio de Active Directory y que se le han concedido privilegios administrativos para crear objetos de equipo en `Active Directory`.

PERMITIR QUE LOS USUARIOS DE DOMINIO INICIEN SESIÓN EN MÁQUINAS LINUX VDA

Para permitir que los usuarios de dominio establezcan sesiones HDX™ en una máquina Linux VDA:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory para esa cuenta de usuario.
2. Seleccione la pestaña **Cuenta de Unix**.
3. Marque **Habilitado para Unix**.
4. Establezca el **Número GID principal** en el ID de grupo de un grupo de usuarios de dominio real.

> **Nota:**
>
> Estas instrucciones son equivalentes para configurar usuarios de dominio para el inicio de sesión mediante la consola, RDP, SSH o cualquier otro protocolo de acceso remoto.

CONFIGURAR QUEST EN LINUX VDA

Solucionar la aplicación de la política de SELinux
El entorno RHEL predeterminado tiene SELinux completamente aplicado. Esta aplicación interfiere con los mecanismos IPC de socket de dominio Unix utilizados por Quest e impide que los usuarios de dominio inicien sesión.

La forma conveniente de solucionar este problema es deshabilitar SELinux. Como usuario root, edite **/etc/selinux/config** y cambie la configuración de **SELinux**:

```
SELINUX=disabled
```

Este cambio requiere un reinicio de la máquina:

```
reboot
```

Importante:

Utilice esta configuración con precaución. Volver a habilitar la aplicación de la política de SELinux después de deshabilitarla puede provocar un bloqueo completo, incluso para el usuario root y otros usuarios locales.

Configurar el demonio VAS

La renovación automática de los tickets Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar deshabilitada:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Este comando establece el intervalo de renovación en nueve horas (32 400 segundos), lo que es una hora menos que la duración predeterminada del ticket de 10 horas. Establezca este parámetro en un valor inferior en sistemas con una duración de ticket más corta.

Configurar PAM y NSS

Para habilitar el inicio de sesión de usuarios de dominio a través de HDX y otros servicios como su, ssh y RDP, ejecute los siguientes comandos para configurar PAM y NSS manualmente:

```
sudo /opt/quest/bin/vastool configure pam



sudo /opt/quest/bin/vastool configure nss
```

UNIRSE AL DOMINIO DE WINDOWS

Una la máquina Linux al dominio de Active Directory mediante el comando Quest **vastool**:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

El usuario es cualquier usuario de dominio con permisos para unir equipos al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Reinicie la máquina Linux después de unirse al dominio.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA, ya sean Windows o Linux, tengan un objeto de equipo en Active Directory. Para verificar que una máquina Linux unida a Quest está en el dominio:

```
sudo /opt/quest/bin/vastool info domain
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. Si la máquina no está unida a ningún dominio, aparece el siguiente error:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Para verificar que Quest puede autenticar a los usuarios de dominio a través de PAM, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username



id -u
```

verificar que se ha creado un archivo de caché de credenciales Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

verificar que los tickets en la caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
```

Cierre la sesión.

```
exit
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

Centrify DirectControl

UNIR AL DOMINIO DE WINDOWS

Con el agente Centrify DirectControl instalado, una la máquina Linux al dominio de Active Directory mediante el comando Centrify `adjoin`:

```
su –

adjoin -w -V -u user domain-name
```

El parámetro **user** es cualquier usuario de dominio de Active Directory con permisos para unir equipos al dominio de Active Directory. El parámetro **domain-name** es el nombre del dominio al que se unirá la máquina Linux.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA, ya sean Windows o Linux, tengan un objeto de equipo en Active Directory. Para verificar que una máquina Linux unida a Centrify está en el dominio:

```
su –



adinfo
```

verificar que el valor de **Joined to domain** es válido y que el **CentrifyDC mode** devuelve **connected**. Si el modo se queda atascado en el estado inicial, el cliente de Centrify está experimentando problemas de conexión o autenticación con el servidor.

Hay disponible información de diagnóstico y del sistema más completa mediante:

```
adinfo --sysinfo all
```

```
adinfo --diag
```

Pruebe la conectividad con los distintos servicios de Active Directory y Kerberos.

```
adinfo --test
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de la unión al dominio.

SSSD

CONFIGURAR KERBEROS

Ejecute el siguiente comando para instalar Kerberos:

```
sudo apt-get install krb5-user
```

Para configurar Kerberos, abra **/etc/krb5.conf** como root y establezca los parámetros:

> **Nota:**
>
> Configure Kerberos según su infraestructura de AD. Las siguientes configuraciones están pensadas para el modelo de dominio único y bosque único.

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`rdns = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` *`REALM`*

`.domain-dns-name` `=` *`REALM`*

El parámetro `domain-dns-name` en este contexto es el nombre de dominio DNS, como example.com. El *REALM* es el nombre del reino de Kerberos en mayúsculas, como EXAMPLE.COM.

UNIRSE AL DOMINIO

SSSD debe configurarse para usar Active Directory como su proveedor de identidades y Kerberos para la autenticación. Sin embargo, SSSD no proporciona funciones de cliente de AD para unirse al dominio y administrar el archivo keytab del sistema. En su lugar, puede usar **adcli**, **realmd** o **Samba**.

> **Nota:**
>
> Esta sección solo proporciona información para **adcli** y **Samba**.

- **Si usa adcli para unirse al dominio, complete los siguientes pasos:**

1. Instale **adcli**.

   ```
   sudo apt-get install adcli
   ```

2. Una el dominio con **adcli**.

   Elimine el archivo keytab del sistema antiguo y una el dominio usando:

   ```
   su -


   rm -rf /etc/krb5.keytab


   adcli join domain-dns-name -U user -H hostname-fqdn
   ```

El **usuario** es un usuario de dominio con permisos para agregar máquinas al dominio. El **hostname-fqdn** es el nombre de host en formato FQDN para la máquina.

La opción **-H** es necesaria para que **adcli** genere SPN en el formato host/hostname-fqdn@REALM, que requiere el VDA de Linux.

3. verificar el keytab del sistema.

   Ejecute el comando `sudo klist -ket` para asegurarse de que el archivo keytab del sistema se haya creado.

   verificar que la marca de tiempo de cada clave coincide con la hora en que la máquina se unió al dominio.

- **Si usa Samba para unirse al dominio, complete los siguientes pasos:**

1. Instale el paquete.

   ```
   sudo apt-get install samba krb5-user
   ```

2. Configure **Samba**.

   Abra **/etc/samba/smb.conf** y realice las siguientes configuraciones:

   `[global]`

   `workgroup =` *`WORKGROUP`*

   `security = ADS`

   `realm =` *`REALM`*

   `client signing = yes`

   `client use spnego = yes`

   `kerberos method = secrets and keytab`

   WORKGROUP es el primer campo en *REALM*, y *REALM* es el nombre del reino de Kerberos en mayúsculas.

3. Una el dominio con **Samba**.

   Su controlador de dominio debe ser accesible y debe tener una cuenta de Windows con permisos para agregar equipos al dominio.

```
sudo net ads join <the Kerberos realm name in uppercase> -U <domain
user with permission to add computers to the domain>
```

CONFIGURAR SSSD

Instale o actualice los paquetes necesarios:

Instale los paquetes de SSSD y de configuración necesarios si aún no están instalados:

```
sudo apt-get install sssd
```

Si los paquetes ya están instalados, se recomienda una actualización:

```
sudo apt-get install --only-upgrade sssd
```

CONFIGURAR SSSD

Se requieren cambios en la configuración de SSSD antes de iniciar el demonio SSSD. Para algunas versiones de SSSD, el archivo de configuración **/etc/sssd/sssd.conf** no se instala de forma predeterminada y debe crearse manualmente. Como root, cree o abra **/etc/sssd/sssd.conf** y realice la siguiente configuración:

`[sssd]`

`services = nss, pam`

`config_file_version = 2`

`domains =` *`domain-dns-name`*

`[domain/` *`domain-dns-name`* `]`

`id_provider = ad`

`access_provider = ad`

`auth_provider = krb5`

`krb5_realm =` *`REALM`*

`# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days`

`krb5_renewable_lifetime = 14d`

`# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours`

`krb5_renew_interval = 1h`

`krb5_ccachedir = /tmp`

`krb5_ccname_template = FILE:%d/krb5cc_%U`

`# This ldap_id_mapping setting is also the default value`

`ldap_id_mapping = true`

`override_homedir = /home/%d/%u`

`default_shell = /bin/bash`

`ad_gpo_map_remote_interactive = +ctxhdx`

> **Nota:**
>
> ldap_id_mapping se establece en **true** para que SSSD se encargue de asignar los SID de Windows a los UID de Unix. De lo contrario, `Active Directory` debe poder proporcionar extensiones POSIX. El servicio PAM `ctxhdx` se agrega a ad_gpo_map_remote_interactive.

> El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como example.com. El *REALM* es el nombre del reino Kerberos en mayúsculas, como EXAMPLE.COM. No es necesario configurar el nombre de dominio NetBIOS.

> Para obtener información sobre los parámetros de configuración, consulte las páginas man de sssd.conf y `sssd-ad`.

> El demonio SSSD requiere que el archivo de configuración solo tenga permiso de lectura para el propietario:

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

INICIAR EL DEMONIO SSSD

Ejecute los siguientes comandos para iniciar el demonio SSSD ahora y para permitir que el demonio se inicie al arrancar la máquina:

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

CONFIGURACIÓN DE PAM

Ejecute el siguiente comando y asegúrese de que las opciones **Autenticación SSS** y **Crear directorio de inicio al iniciar sesión** estén seleccionadas:

```
sudo pam-auth-update
```

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`.

- Si utiliza **adcli** para verificar la pertenencia al dominio, ejecute el comando `sudo adcli info domain-dns-name` para mostrar la información del dominio.
- Si utiliza **Samba** para verificar la pertenencia al dominio, ejecute el comando `sudo net ads testjoin` para verificar que la máquina está unida a un dominio y el comando `sudo net ads info` para verificar información adicional del dominio y del objeto de equipo.

VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Para verificar que Kerberos está configurado correctamente para su uso con el VDA de Linux, verificar que el archivo keytab del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las diversas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando Kerberos `kinit` para autenticar la máquina con el controlador de dominio utilizando estas claves:

```
sudo kinit -k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución de shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino de Kerberos. Asegúrese de que se utiliza el nombre del reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el TGT de la cuenta de la máquina se ha almacenado en caché mediante:

```
sudo klist
```

VERIFICAR LA AUTENTICACIÓN DE USUARIO

SSSD no proporciona una herramienta de línea de comandos para probar la autenticación directamente con el demonio, y solo se puede hacer a través de PAM.

Para verificar que el módulo PAM de SSSD está configurado correctamente, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

verificar que los tickets Kerberos devueltos por el comando **klist** sean correctos para ese usuario y no hayan caducado.

Como usuario root, verificar que se haya creado un archivo de caché de tickets correspondiente para el uid devuelto por el comando anterior **id -u**:

```
ls /tmp/krb5cc_uid
```

Se puede realizar una prueba similar iniciando sesión en KDE o Gnome Display Manager. Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de unión al dominio.

PBIS

DESCARGUE EL PAQUETE PBIS NECESARIO

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

HAGA EJECUTABLE EL SCRIPT DE INSTALACIÓN DE PBIS

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

EJECUTE EL SCRIPT DE INSTALACIÓN DE PBIS

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

UNIRSE AL DOMINIO DE WINDOWS

Su controlador de dominio debe ser accesible y debe tener una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

El **usuario** es un usuario de dominio que tiene permisos para agregar equipos al dominio de Active Directory. El **nombre de dominio** es el nombre DNS del dominio, por ejemplo, example.com.

Nota: Para establecer Bash como shell predeterminado, ejecute el comando **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**.

VERIFICAR LA PERTENENCIA AL DOMINIO

El Delivery Controller requiere que todas las máquinas VDA (VDA de Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para verificar que una máquina Linux unida a PBIS está en el dominio:

```
/opt/pbis/bin/domainjoin-cli query
```

Si la máquina está unida a un dominio, este comando devuelve la información sobre el dominio de AD y la OU unidos actualmente. De lo contrario, solo aparece el nombre de host.

VERIFICAR LA AUTENTICACIÓN DE USUARIO

Para verificar que PBIS puede autenticar usuarios de dominio a través de PAM, inicie sesión en el VDA de Linux con una cuenta de usuario de dominio que no se haya utilizado antes.

```
sudo ssh localhost -l domain\\user



id -u
```

verificar que se creó un archivo de caché de credenciales de Kerberos correspondiente para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
```

Salga de la sesión.

```
exit
```

Continúe con Paso 6: Instalar el VDA de Linux después de la verificación de unión al dominio.

Paso 4: Instalar .NET

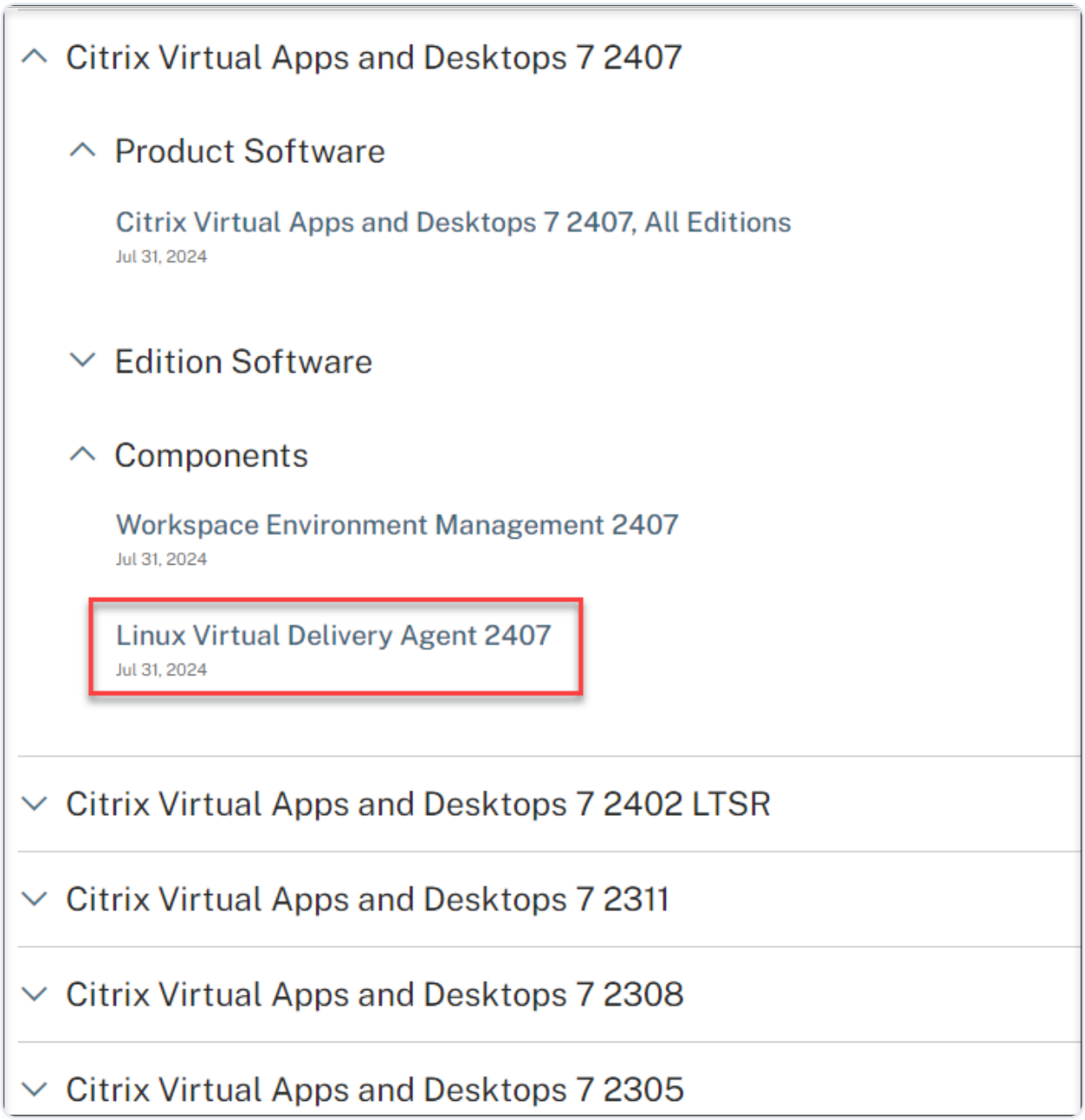
Antes de instalar el VDA de Linux, instale .NET según los requisitos del sistema

Después de instalar .NET, ejecute el comando **which dotnet** para encontrar la ruta de tiempo de ejecución.

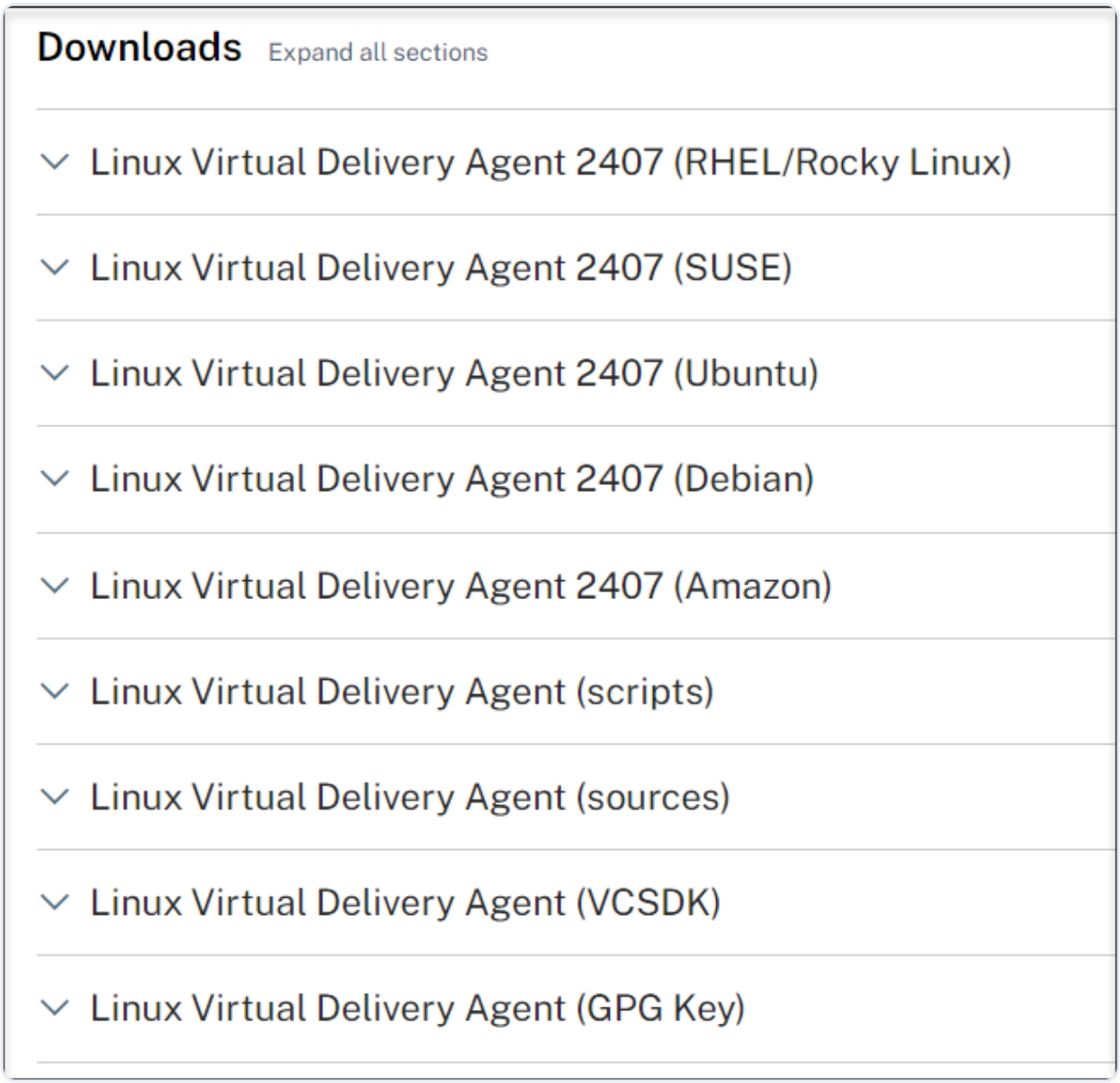
Según la salida del comando, establezca la ruta binaria de tiempo de ejecución de .NET. Por ejemplo, si la salida del comando es /aa/bb/dotnet, use /aa/bb como la ruta binaria de .NET.

Paso 5: Descargar el paquete del VDA de Linux

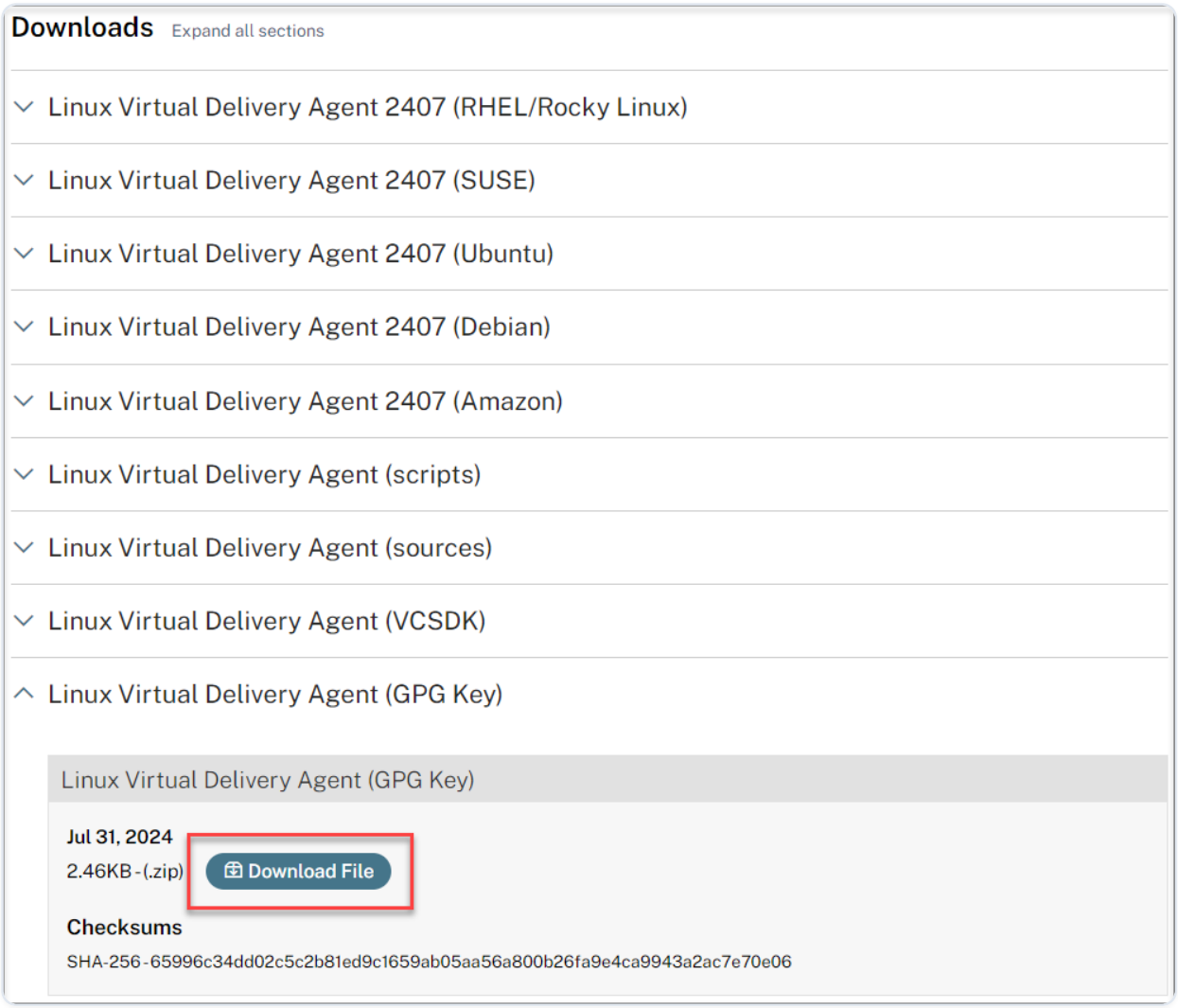
1. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Expanda **Componentes** para encontrar el VDA de Linux. Por ejemplo:



4. Haga clic en el enlace del VDA de Linux para acceder a las descargas del VDA de Linux.



5. Descargue el paquete de Linux VDA que coincida con su distribución de Linux.
6. Descargue la clave pública GPG que puede usar para verificar la integridad del paquete de Linux VDA. Por ejemplo:



Para verificar la integridad del paquete de Linux VDA, ejecute los siguientes comandos para importar la clave pública en la base de datos DEB y comprobar la integridad del paquete:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Paso 6: Instalar el VDA de Linux

Paso 6a: Instalar el VDA de Linux

Instale el software de Linux VDA mediante el administrador de paquetes de Debian:

Para Debian 12:

```
sudo dpkg -i xendesktopvda_<version>.debian12_amd64.deb
```

Para Debian 11:

```
sudo dpkg -i xendesktopvda_<version>.debian11_amd64.deb
```

Lista de dependencias para Debian 12:

```
openjdk-17-jdk >= 17

imagemagick >= 8:6.9.11

ufw >= 0.36

desktop-base >= 12.0.6

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.38

gtk3-nocsd >= 3

bash >= 5.2

findutils >= 4.9.0

sed >= 4.9

cups >= 2.4

ghostscript >= 10.0.0~

libmspack0 >= 0.11

ibus >= 1.5

libgoogle-perftools4 >= 2.10~

libpython3.11 >= 3.11~
```

```
libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.87

libqt5widgets5 >= 5.15~

mutter >= 43.8

libqrencode4 >= 4.1.1

libimlib2 >= 1.10.0

libfuse2 >= 2.9.9

pulseaudio-utils >= 16.1
```

Lista de dependencias para Debian 11:

```
libnss3-tools >= 2:3.61



libfuse2 >= 2.9



openjdk-17-jdk >= 17



imagemagick >= 8:6.9.10



ufw >= 0.36



desktop-base >= 10.0.2
```

```
libxrandr2 >= 2:1.5.1


libxtst6 >= 2:1.2.3


libxm4 >= 2.3.8


util-linux >= 2.33


gtk3-nocsd >= 3


bash >= 5.0


findutils >= 4.6.0


sed >= 4.7


cups >= 2.2


ghostscript >= 9.53~


libmspack0 >= 0.10
```

```
ibus >= 1.5


libgoogle-perftools4 >= 2.7~


libpython3.9 >= 3.9~


libsasl2-modules-gssapi-mit >= 2.1.~


libqt5widgets5 >= 5.5~


mutter >= 3.38.6~


libqrencode4 >= 4.0.0


libimlib2 >= 1.5.1
```

Nota:

Para ver una matriz de las distribuciones de Linux y las versiones de Xorg que admite esta versión del VDA de Linux, consulte Requisitos del sistema.

Paso 6b: Actualizar el VDA de Linux (opcional)

El VDA de Linux admite actualizaciones desde la versión más reciente. Por ejemplo, puede actualizar el VDA de Linux de 2308 a 2311 y de 1912 LTSR a 2203 LTSR.

```
sudo dpkg -i <PATH>/<Linux VDA deb>



sudo apt-get install -f
```

Nota:

- La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de realizar una actualización, asegúrese de hacer una copia de seguridad de los archivos.
- A partir de la versión 2407, el Linux VDA delega en los administradores de paquetes **rpm** o **dpkg** la gestión de los archivos de configuración durante las actualizaciones. A continuación, se describe cómo **rpm** y **dpkg** interactúan con los cambios en los archivos de configuración:
  - **rpm**: de forma predeterminada, mantiene la versión local y guarda la nueva versión del paquete con una extensión **.rpmnew**.
  - **dpkg**: le pide interactivamente que elija cómo proceder. Para actualizar el Linux VDA de forma silenciosa, conservando el archivo de configuración local y guardando la nueva versión del paquete como **.dpkg-new** o **.dpkg-dist**, utilice el siguiente comando:

    ```
    dpkg --force-confold -i package.deb  # Always keep your version,
    then save new package's version as *.dpkg-new or *.dpkg-dist
    ```

Paso 7: Instalar los controladores NVIDIA GRID

Para habilitar HDX 3D Pro, debe instalar los controladores NVIDIA GRID en su hipervisor y en las máquinas VDA.

Para instalar y configurar NVIDIA GRID Virtual GPU Manager (el controlador de host) en los hipervisores específicos, consulte las siguientes guías:

- XenServer
- VMware ESX

- Nutanix AHV

Para instalar y configurar los controladores de VM invitada de NVIDIA GRID, siga estos pasos generales:

1. Asegúrese de que la VM invitada esté apagada.
2. En el panel de control del hipervisor, asigne una GPU a la VM.
3. Inicie la VM.
4. Instale el controlador de VM invitada (de su proveedor de la nube o de NVIDIA) en la VM.

Paso 8: Configurar el Linux VDA

> **Nota:**

> Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional **en_US.UTF-8** esté instalada en su sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando **sudo locale-gen en_US.UTF-8**. Para Debian, edite el archivo **/etc/locale.gen** descomentando la línea **# en_US.UTF-8 UTF-8** y, a continuación, ejecute el comando **sudo locale-gen**.

> Después de instalar el paquete, debe configurar el VDA de Linux ejecutando el script ctxsetup.sh. Antes de realizar cualquier cambio, el script verifica el entorno y se asegura de que todas las dependencias estén instaladas. Si es necesario, puede volver a ejecutar el script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manualmente con indicaciones o automáticamente con respuestas preconfiguradas. Revise la Ayuda sobre el script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

Configuración guiada

Ejecute una configuración manual con preguntas guiadas:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Configuración automatizada

Para una instalación automatizada, las opciones requeridas por el script de configuración se pueden proporcionar con variables de entorno. Si todas las variables requeridas están presentes, el script no solicita ninguna información al usuario, lo que permite un proceso de instalación automatizado.

Las variables de entorno admitidas incluyen:

- **CTX_XDL_NON_DOMAIN_JOINED='y\|n'** – Si se debe unir la máquina a un dominio. El valor predeterminado es 'n'. Para escenarios unidos a un dominio, establézcalo en 'n'.
- **CTX_XDL_AD_INTEGRATION='winbind\|sssd\|centrify\|pbis\|quest'** – El VDA de Linux requiere la configuración de Kerberos para autenticarse con los Delivery Controllers. La configuración de Kerberos se determina a partir de la herramienta de integración de Active Directory instalada y configurada en el sistema.
- **CTX_XDL_DDC_LIST='<list-ddc-fqdns\>'** – El VDA de Linux requiere una lista de nombres de dominio completos (FQDN) de Delivery Controller separados por espacios para registrarse con un Delivery Controller. Se debe especificar al menos un FQDN o CNAME.
- **CTX_XDL_VDI_MODE='y\|n'** – Si se debe configurar la máquina como un modelo de entrega de escritorio dedicado (VDI) o un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca el valor en **'y'**.
- **CTX_XDL_HDX_3D_PRO='y\|n'** – El VDA de Linux admite HDX 3D Pro, un conjunto de tecnologías de aceleración de GPU diseñadas para optimizar la virtualización de aplicaciones gráficas enriquecidas. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única), es decir, CTX_XDL_VDI_MODE=**'y'**.
- **CTX_XDL_START_SERVICE='y\|n'** – Determina si los servicios del VDA de Linux se inician cuando la configuración se ha completado.
- **CTX_XDL_REGISTER_SERVICE='y\|n'** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES='y\|n'** – Los servicios del VDA de Linux requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir automáticamente los puertos requeridos (por defecto los puertos 80 y 1494) en el firewall del sistema para Linux Virtual Desktop.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/kde/mate/'<none\>'** – Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se utilizará en las

sesiones. Si lo establece en '**<none\>'**, se utiliza el escritorio predeterminado configurado en el VDA.

También puede cambiar entre entornos de escritorio ejecutando comandos o utilizando la bandeja del sistema. Para obtener más información, consulte Comandos para cambiar de escritorio y Bandeja del sistema.

- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET para admitir el nuevo servicio de agente de intermediación (ctxvda). La ruta predeterminada es **'/usr/bin'**.
- **CTX_XDL_VDA_PORT=port-number** – El Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP.
- **CTX_XDL_SITE_NAME=<dns-name\>** – El Linux VDA detecta los servidores LDAP a través de DNS. Para limitar los resultados de la búsqueda DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_LDAP_LIST='<list-ldap-servers\>'** – El Linux VDA consulta DNS para detectar servidores LDAP. Si DNS no puede proporcionar registros de servicio LDAP, puede proporcionar una lista de FQDN de LDAP separados por espacios con puertos LDAP. Por ejemplo, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Para habilitar consultas LDAP más rápidas dentro de un bosque de Active Directory, habilite el Catálogo global en un controlador de dominio y especifique el número de puerto LDAP relevante como 3268. Esta variable se establece en **'<none\>'** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE=search-base-set** – El Linux VDA consulta LDAP a través de un conjunto de bases de búsqueda en la raíz del dominio de Active Directory (por ejemplo, DC=mycompany,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Si no es necesario, establézcalo en **'<none\>'**.
- **CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'** – El Linux VDA admite la especificación de un nombre de Delivery Controller mediante un registro CNAME de DNS.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_NON_DOMAIN_JOINED='n'

export CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest

export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'

export CTX_XDL_VDI_MODE='y|n'
```

```
export CTX_XDL_HDX_3D_PRO='y|n'

export CTX_XDL_START_SERVICE='y|n'

export CTX_XDL_REGISTER_SERVICE='y|n'

export CTX_XDL_ADD_FIREWALL_RULES='y|n'

export CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|'<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'

export CTX_XDL_VDA_PORT='<port-number>'

export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'

export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'

export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'

export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Al ejecutar el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que crea. Le recomendamos que cree un archivo de script de shell a partir de los comandos anteriores con **#\!/bin/bash** como primera línea.

Alternativamente, puede especificar todos los parámetros utilizando un solo comando:

```
sudo CTX_XDL_NON_DOMAIN_JOINED='n' \

CTX_XDL_AD_INTEGRATION=sssd|winbind|centrify|pbis|quest \

CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \

CTX_XDL_VDI_MODE='y|n' \

CTX_XDL_HDX_3D_PRO='y|n' \

CTX_XDL_START_SERVICE='y|n' \
```

```
CTX_XDL_REGISTER_SERVICE='y|n' \

CTX_XDL_ADD_FIREWALL_RULES='y|n' \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|kde|mate|'<none>' \

CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \

CTX_XDL_VDA_PORT='<port-number>' \

CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \

CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \

CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \

CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \

/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Eliminar cambios de configuración

En algunos escenarios, es posible que deba eliminar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete de Linux VDA.

Revise la Ayuda sobre este script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

Para eliminar los cambios de configuración:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

Importante:

Este script elimina todos los datos de configuración de la base de datos y deja el Linux VDA inoperable.

Registros de configuración

Los scripts **ctxsetup.sh** y **ctxcleanup.sh** muestran errores en la consola, con información adicional escrita en el archivo de registro de configuración **/tmp/xdl.configure.log**.

Reinicie los servicios de Linux VDA para que los cambios surtan efecto.

Desinstalar el software de Linux VDA

Para comprobar si Linux VDA está instalado y ver la versión del paquete instalado:

```
dpkg -l xendesktopvda
```

Para ver información más detallada:

```
apt-cache show xendesktopvda
```

Para desinstalar el software de Linux VDA:

```
dpkg -r xendesktopvda
```

> **Nota:**
>
> Al desinstalar el software de Linux VDA, se eliminan los datos de configuración asociados de PostgreSQL y otros. Sin embargo, el paquete de PostgreSQL y otros paquetes dependientes que se configuraron antes de la instalación de Linux VDA no se eliminan.

> **Sugerencia:**
>
> La información de esta sección no cubre la eliminación de paquetes dependientes, incluido PostgreSQL.

Paso 9: Ejecute XDPing

Ejecute `sudo /opt/Citrix/VDA/bin/xdping` para comprobar si hay problemas de configuración comunes en un entorno de Linux VDA. Para obtener más información, consulte **XDPing**.

Paso 10: Ejecute el Linux VDA

Una vez que haya configurado el Linux VDA mediante el script **ctxsetup.sh**, utilice los siguientes comandos para controlar el Linux VDA.

Iniciar el Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Detener el Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

> **Nota:**
>
> Antes de detener los servicios **ctxvda** y **ctxhdx**, ejecute el comando **systemctl stop ctxmonitord** para detener el demonio del servicio de monitorización. De lo contrario, el demonio del servicio de monitorización reiniciará los servicios que detuvo.

Reiniciar el Linux VDA:

Para reiniciar los servicios de Linux VDA:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx
```

```
sudo systemctl restart ctxvda
```

Comprobar el estado del Linux VDA:

Para comprobar el estado de ejecución de los servicios de Linux VDA:

```
sudo systemctl status ctxvda
```

```
sudo systemctl status ctxhdx
```

Paso 11: Crear catálogos de máquinas

El proceso para crear catálogos de máquinas y añadir máquinas Linux VDA es similar al enfoque tradicional de Windows VDA. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Para crear catálogos de máquinas que contengan máquinas Linux VDA, existen algunas restricciones que diferencian el proceso de la creación de catálogos de máquinas para máquinas Windows VDA:

- Para el sistema operativo, seleccione:
  - La opción **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios dedicados VDI.
- No mezcle máquinas Linux y Windows VDA en el mismo catálogo de máquinas.

Nota:

Las primeras versiones de Citrix Studio no admitían el concepto de un "sistema operativo Linux". Sin embargo, seleccionar la opción **Windows Server OS** o **Server OS** implica un modelo de entrega de escritorios compartidos alojados equivalente. Seleccionar la opción **Windows Desktop OS** o **Desktop OS** implica un modelo de entrega de un solo usuario por máquina.

> **Sugerencia:**
>
> Si quita una máquina del dominio de Active Directory y la vuelve a unir, debe quitar la máquina del catálogo de máquinas y volver a agregarla.

Paso 12: Crear grupos de entrega

El proceso para crear un grupo de entrega y agregar catálogos de máquinas que contengan máquinas Linux VDA es casi idéntico al de las máquinas Windows VDA. Para obtener una descripción más detallada de cómo completar estas tareas, consulte Crear grupos de entrega.

Para crear grupos de entrega que contengan catálogos de máquinas Linux VDA, se aplican las siguientes restricciones:

- Asegúrese de que los usuarios y grupos de AD que seleccione se hayan configurado correctamente para iniciar sesión en las máquinas Linux VDA.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No mezcle el grupo de entrega con catálogos de máquinas que contengan máquinas Windows.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2503.

Configurar

Esta sección detalla las funciones del VDA de Linux, incluyendo la descripción de las funciones, la configuración y la solución de problemas.

Administración

Esta sección contiene los siguientes temas:

- Programa de recopilación de datos de Linux VDA
- HDX Insight
- Integración con el servicio de telemetría de Citrix
- Autoactualización de Linux VDA para Citrix DaaS Standard para Azure
- Métricas de VM de Linux y de sesión de Linux
- Recopilación de registros
- Sombreado de sesiones
- El demonio del servicio de supervisión
- Solución de problemas
- Otros
  - Compatibilidad con la aplicación Citrix Workspace para HTML5
  - Crear un entorno virtual de **Python3**
  - Integrar NIS con Active Directory
  - **IPv6**
  - LDAPS
  - **Xauthority**

Actualizaciones de VDA (vista previa)

Introducción

Anteriormente, la actualización de los VDA requería una intervención manual completa. La versión 2503 simplifica las actualizaciones de VDA para implementaciones de DaaS al introducir el Agente de actualización de VDA. Las actualizaciones a partir de la versión 2503 se pueden realizar directamente desde una ruta de archivo compartida o local.

El Agente de actualización de VDA **ctxvua** es responsable de comunicarse con el Servicio de actualización de VDA y de realizar las siguientes funciones:

- **Comprobaciones programadas**: El Agente de actualización de VDA consulta al Servicio de actualización de VDA para obtener información sobre las actualizaciones programadas cada 15 minutos.
- **Actualizaciones automatizadas**: Al recibir las instrucciones de actualización, el Agente de actualización de VDA actualiza automáticamente el VDA.
- **Informes de estado**: El Agente de actualización de VDA informa del resultado de la actualización (éxito o fallo) al Servicio de actualización de VDA.

Para obtener más información sobre el servicio de actualización de VDA, consulte Tech Brief: Citrix VDA Upgrade service. Allí encontrará una descripción general del servicio, información detallada sobre su funcionamiento y otros recursos útiles.

Consideraciones

- Los VDA de Linux se actualizan mediante comandos de administración de paquetes subyacentes (como rpm o apt), lo que refleja el proceso de actualización manual; los archivos de configuración se gestionan automáticamente durante la actualización por línea de comandos.
- A diferencia de Windows, el VDA de Linux incluye un Agente de actualización de VDA integrado. Esto simplifica el proceso de actualización, ya que el agente ya está presente. La versión del Agente de actualización de VDA está vinculada a la versión del VDA.
- De forma predeterminada, el Agente de actualización de VDA está deshabilitado. Para habilitar el agente, ejecute los siguientes comandos:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\UpdateServices\UpdateAgent" -t "REG_DWORD" -v
"fEnabled" -d "0x00000001" --force
```

```
systemctl start ctxvua.service
```

- El servicio del Agente de actualización de VDA (**ctxvua**) está deshabilitado de forma predeterminada. Puede usar **systemctl** para habilitar e iniciar este servicio.
- Como práctica recomendada, le recomendamos que pruebe las actualizaciones de VDA a fondo antes de pasarlas a producción.
- A diferencia de Windows, las actualizaciones de VDA de Linux solo se admiten desde una ruta de archivo. Esto significa que no puede usar directamente URL de Azure CDN u otros repositorios en línea. Debe administrar los paquetes de VDA usted mismo. Esto se aplica tanto a las actualizaciones de versiones principales como secundarias.
- Ignore "Latest VDA Version" y "Upgrade State" en el Servicio de actualización de VDA. Solo el "VDA Upgrade State" es relevante para Linux.
- La ruta de archivo para el paquete de VDA puede ser local a la máquina VDA o una ubicación compartida (por ejemplo, un recurso compartido de red montado en el VDA). El sistema no está diseñado para descargar el paquete automáticamente. Debe proporcionar el archivo de paquete completo.
- Especifique la ruta en el formato de ruta UNC de Windows (que comienza con ****) para pasar la validación de ruta al usar Studio o Citrix DaaS Remote PowerShell SDK. Por ejemplo, **/mnt/pkg\/\<package-name>** debe introducirse como **\\\mnt\pkg\\<package-name\>**.
- La distinción entre VDA de "servidor" y de "estación de trabajo" no se aplica a Linux. Puede usar cualquiera de las dos opciones en Studio o PowerShell sin que ello afecte a la actualización.
- No se admite la degradación de VDA.

Requisitos previos

- Plano de control: Citrix DaaS™
- Versión de VDA: 2503 o posterior

> **Nota:**
>
> Recomendamos usar el VDA CR más reciente.

- Los VDA deben tener instalado el Agente de actualización de VDA y el servicio debe estar en ejecución.
- Tiene permisos para actualizar VDA.
- La actualización de VDA se configura con la pista CR o LTSR adecuada en Studio.
- Los VDA no están en uso. (Los usuarios deben cerrar sesión en ellos).
- Los VDA no están en modo de mantenimiento. (Un administrador puede poner un VDA en modo de mantenimiento. Un VDA también puede ponerse automáticamente en modo de mantenimiento si ha superado el número máximo de intentos de registro permitidos).
- Los VDA deben pertenecer a un grupo de entrega y estar registrados en DaaS.
- El VDA de destino es compatible con el sistema operativo del VDA actual.

Actualizar VDA con Studio

Flujo de trabajo general

Un flujo de trabajo general para actualizar VDAs usando Studio es el siguiente:

1. Habilitar la actualización de VDA para un catálogo.
   - Puede habilitar la actualización de VDA al crear un catálogo.
   - Puede habilitar la actualización de VDA al editar un catálogo.
2. Actualice los VDA por catálogo. Las actualizaciones de VDA por máquina no están disponibles actualmente. Para obtener más información, consulte Configurar la actualización automática de VDA.

   > **Nota:**
   >
   > Al programar actualizaciones de VDA para un catálogo, todas las máquinas del catálogo se incluyen en el ámbito de la actualización. Por lo tanto, recomendamos hacer una copia de seguridad de esas máquinas antes de iniciar la actualización.

3. El proceso de actualización de VDA no admite la actualización de componentes adicionales ni el uso de funciones como la restauración. Omita estos dos pasos.
4. Configure las opciones de programación, incluida la hora de actualización y el umbral de fallos de actualización. El umbral de fallos probablemente determina cuántas actualizaciones fallidas se toleran antes de que el proceso se detenga o se activen las alertas.

5. Seleccione "Usar recurso compartido de archivos local" para la ubicación del instalador de VDA. Proporcione la ruta en formato UNC de Windows (por ejemplo, **\\\\server\share\path**).
6. La opción "Forzar cierre de sesión" controla cómo se gestionan las sesiones de usuario durante las actualizaciones de VDA. Si bien la interfaz de usuario de Studio solo permite cerrar sesiones desconectadas, PowerShell puede cerrar todas las sesiones (conectadas y desconectadas). El cierre de sesión no es inmediato. El Servicio de actualización de VDA inicia el cierre de sesión después de que el Agente de actualización de VDA intenta consultar la programación de actualización y encuentra sesiones desconectadas. Luego, el agente espera 15 minutos antes de volver a intentar la consulta.

Actualizar VDA con PowerShell

Puede configurar las actualizaciones de VDA mediante el SDK de PowerShell remoto en Windows. Para obtener más información sobre el SDK de PowerShell remoto, consulte Citrix DaaS Remote PowerShell SDK.

Los siguientes son los cmdlets de PowerShell:

- Get-VusCatalog

  Utilice este cmdlet para obtener detalles de un catálogo como **Name**, **Uid**, **Uuid**, **UpgradeState** (**Available**, **UpToDate**, **Scheduled**, **Unknown**), **Upgrade scheduled** y **StateId** (estado de **Upgrade scheduled**).

- Get-VusMachine

  Utilice este cmdlet para obtener detalles de una máquina como **MachineName**, **Uid**, **Uuid**, **UpgradeState** (**Available**, **UpToDate**, **Scheduled**, **Unknown**) y **StateId** (estado de **Upgrade scheduled**).

- Get-VusComponentVersion

  Utilice este cmdlet para comprobar si los VDA han notificado las versiones de los componentes. Utilice **MachineId** para filtrar los VDA. **MachineId** es el UUID de **Get-BrokerMachine**.

- New-VusMachineUpgrade

  Utilice este cmdlet para configurar las actualizaciones de VDA a nivel de máquina.

- New-VusCatalogSchedule

  Utilice este cmdlet para programar las actualizaciones de VDA a nivel de catálogo de máquinas.

Ejemplo:

```
Get-BrokerMachine -DNSName 'u22-test*'



New-VusCatalogSchedule -CatalogName "test-catalog" -UpgradeNow
-DurationInHours 2 -LogoffOption ActiveAndDisconnectedSessions
-VdaServerPackageUri "\
\root\xendesktopvda_24.11.0.1-1.ubuntu22.04_amd64.deb"



Get-VusComponent -CatalogName 'test-catalog'



Get-VusCatalog -Name 'test-catalog'
```

Solución de problemas

El núcleo del proceso de actualización gira en torno al servicio del agente de actualización de VDA (**ctxvua**). Actúa como intermediario, comunicándose con el servicio de actualización de VDA y ejecutando el script **/opt/Citrix/VDA/sbin/update_helper.sh** para operaciones relacionadas con el sistema operativo. Durante la actualización, la información sobre el proceso se almacena en el registro.

Registro

Utilice el comando **/opt/Citrix/VDA/bin/ctxreg dump |grep -i UpdateAgent** para examinar la configuración del registro relacionada con el agente de actualización de VDA. Esto puede revelar problemas de configuración o problemas con el propio proceso de actualización.

1. **Comprobar configuración:** El archivo de configuración del servicio **ctxvua** se encuentra en **/etc/xdl/updateagent**.conf. Revisar este archivo puede ayudar a identificar configuraciones erróneas.

Registros

Los siguientes archivos de registro son cruciales para la solución de problemas:

- **/var/log/xdl/vua.log**: Archivo de registro del servicio **ctxvua**. Este es el registro principal que se debe consultar para detectar problemas relacionados con el funcionamiento del agente de

actualización. El archivo de configuración del servicio **ctxvua** se encuentra en **/etc/xdl/updateagent.conf**. Revisar este archivo puede ayudar a identificar configuraciones erróneas.

- **/var/log/xdl/update_helper.log**: Archivo de registro del script **update_helper.sh**. Este registro es esencial para diagnosticar problemas relacionados con las tareas a nivel del sistema operativo durante la actualización.

Problemas comunes

Esta sección aborda problemas comunes encontrados durante las actualizaciones de VDA, centrándose específicamente en las opciones deshabilitadas en Studio y el estado de "**Actualización desconocida**".

PROBLEMA COMÚN 1: OPCIONES DE ACTUALIZACIÓN DESHABILITADAS

Síntoma: Las opciones "Establecer tipo de actualización" y "Actualizar VDA" están deshabilitadas (en gris) en Studio para un catálogo determinado.

Solución: Compruebe si el Servicio de actualización de VDA es compatible con el tipo de catálogo que está utilizando. Si no lo es, no podrá utilizar estas funciones de actualización automatizadas y deberá gestionar las actualizaciones manualmente.

PROBLEMA COMÚN 2: ESTADO "ACTUALIZACIÓN DESCONOCIDA"

Síntoma: Después de habilitar el Servicio de actualización de VDA para un catálogo de máquinas, el "Estado de actualización" permanece como "Desconocido" en lugar de cambiar a "Disponible" o "Actualizado" como se esperaba. "Actualización desconocida" es un estado transitorio. Finalmente debería actualizarse a "Disponible" o "Actualizado".

Pasos para solucionar problemas de "Actualización desconocida":

1. verificar que el Agente de actualización de VDA está informando las versiones.
   - Paso 1a: Obtener el UUID de la máquina:

     ```
     Get-BrokerMachine -DNSName '<hostname>'
     ```

   - Paso 1b: Comprobar la versión del componente informada por el agente:

     ```
     Get-VusComponentVersion -MachineId "<UUID>"
     ```

     Si el comando **Get-VusComponentVersion** devuelve un valor en blanco, significa que el Agente de actualización de VDA no ha informado su versión. Esto podría indicar que el VDA está "registrado de forma fija" (compruebe la configuración del catálogo de máquinas

y del grupo de entrega). También indica que el Agente de actualización de VDA podría no estar instalado o en ejecución en el VDA de destino.

2. verificar la sincronización del Servicio de actualización de VDA.

   Paso 2a: Comprobar si el Servicio de actualización de VDA ha sincronizado la máquina desde la base de datos del Broker:

   ```
   ```

   ```
   Get-VusEntityUnit -EntityUUID ""
   ```

   ```
   ```

   Sustituya `""` por el **EntityUUID** real si se conoce, o ejecútelo sin él para obtener todos. Si observa que está en blanco, puede indicar que la máquina no se ha sincronizado con el servidor del Servicio de actualización de VDA.

   Paso 2b: Si la máquina no se ha sincronizado, espere un tiempo para que el Servicio de actualización de VDA se sincronice. Luego, confirme que se ha establecido el "Tipo de actualización".

Referencias

- Informe técnico: Servicio de actualización de VDA de Citrix
- Actualizar VDA

Programa de recopilación de datos de Linux VDA

Participa automáticamente en el programa de recopilación de datos después de instalar el Linux VDA. El programa de recopilación de datos recopila estadísticas y datos de uso, y los envía a Citrix Analytics para ayudar a mejorar la calidad y el rendimiento de los productos de Citrix. La carga de datos se produce al iniciar una sesión.

Configuración del Registro

El programa de recopilación de datos de Linux VDA está habilitado de forma predeterminada. Puede habilitar o deshabilitar el programa mediante la siguiente configuración del Registro:

Ubicación: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nombre: **CEIPSwitch**

Valor: 1 = deshabilitado, 0 = habilitado (predeterminado)

Cuando no se especifica, el programa de recopilación de datos de Linux VDA está habilitado.

Puede ejecutar el siguiente comando para deshabilitar el programa de recopilación de datos de Linux VDA:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

Datos recopilados del Linux VDA

La siguiente tabla muestra un ejemplo de los tipos de datos recopilados.

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
GUID de la máquina	**machine_guid**	Una cadena GUID que identifica la máquina de origen de los datos
Nombre y versión del sistema operativo Linux	**os_name_version**	Una cadena que indica el nombre y la versión del sistema operativo Linux de la máquina
Solución de AD	**ad_solution**	Una cadena que indica el método de unión a un dominio de la máquina
Versión del kernel de Linux	**kernel_version**	Una cadena que indica la versión del kernel de la máquina
Tipo de GPU	**gpu_type**	Indica el tipo de GPU de la máquina VDA
Núcleos de CPU	**cpu_cores**	Un entero que indica el número de núcleos de CPU de la máquina
Frecuencia de la CPU	**cpu_frequency**	Un número de coma flotante que indica la frecuencia de la CPU en MHz

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
Tamaño de la memoria física	**memory_size**	Un entero que indica el tamaño de la memoria física en KB
Versión de LVDA	**vda_version**	Una cadena que indica la versión instalada del VDA de Linux.
Actualización o instalación nueva de LVDA	**update_or_fresh_install**	Una cadena que indica si el paquete actual del VDA de Linux se está instalando de nuevo o actualizando
Modo VDI habilitado o no	**vdi_mode**	Una cadena que indica si el modo VDI está habilitado
Método de instalación de LVDA	**install_method**	Una cadena que indica que el paquete actual de Linux VDA se ha instalado mediante MCS, PVS, instalación sencilla o instalación manual.
HDX™ 3D Pro habilitado o no	**hdx_3d_pro**	Una cadena que indica si HDX 3D Pro está habilitado en la máquina
BCR habilitado o no	**BCR**	Una cadena que indica si la redirección de contenido del explorador (BCR) está habilitada en esta máquina
Localización del sistema	**system_locale**	Una cadena que indica la configuración regional de esta máquina
ID de la granja	**farm_id**	Una cadena que indica el ID de la granja.
Tipo de virtualización de VDA	**vda_virtualization**	Una cadena que indica el hipervisor que creó el VDA

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
Clave de sesión	**session_key**	Identifica la sesión de donde provienen los datos
Tipo de recurso	**resource_type**	Una cadena que indica el tipo de recurso de la sesión iniciada: escritorio o `<appname>`
Tipo de cliente de Receiver	**receiver_type**	Un entero que indica el tipo de aplicación Citrix Workspace™ utilizada para iniciar la sesión
Versión del cliente de Receiver	**receiver_version**	Una cadena que indica la versión de la aplicación Citrix Workspace utilizada para iniciar la sesión
Recuento de impresiones	**printing_count**	Un número entero que indica el número de veces que la sesión utiliza la función de impresión
Recuento de redirecciones USB	**usb_redirecting_count**	Un número entero que indica el número de veces que la sesión utiliza un dispositivo USB
Tipo de proveedor de **Gfx**	**gfx_provider_type**	Una cadena que indica el tipo de proveedor de gráficos de la sesión
Recuento de shadowing	**shadow_count**	Un número entero que indica el número de veces que se ha realizado shadowing en la sesión
Idioma seleccionado por el usuario	**ctxism_select**	Una cadena larga compuesta que contiene todos los idiomas que los usuarios han seleccionado

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
Recuento de redirección de tarjeta inteligente	**scard_redirecting_count**	Un entero que indica el número de veces que se utiliza la redirección de tarjeta inteligente para los inicios de sesión y la autenticación de usuario para las aplicaciones en sesión
Tipo de códec de vídeo	**grahpic_video_codec_type**	Una cadena que indica qué códec de vídeo se está utilizando para Thinwire.
Tipo de credencial de inicio de sesión	**credentials_type**	Un entero que indica el tipo de credencial utilizado para iniciar sesión en el VDA de Linux
Marca de agua	**marca de agua**	Una cadena que indica si la marca de agua de la sesión está habilitada o no
Transparencia de marca de agua	**watermark_transparency**	Un entero que indica la transparencia de la marca de agua
Longitud del texto personalizado de la marca de agua	**watermark_custom_text_len**	Un entero que denota la longitud del texto personalizado de la marca de agua
MTU	**unidad máxima de transmisión**	Una cadena que indica si la Unidad Máxima de Transmisión (MTU) se utiliza en esta sesión
MTU MSS	**mtu_mss**	Un entero que denota el Tamaño Máximo de Segmento (MSS)

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
Transferencia de archivos	**transferencia de archivos**	Un entero que denota la configuración de la política de transferencia de archivos
Recuento de cargas de transferencia de archivos	**filetrans_upload_count**	Un entero que denota el número de veces que se utiliza el icono "Cargar" para las transferencias de archivos en la sesión
Recuento de descargas de transferencia de archivos	**filetrans_download_count**	Un entero que indica el número de veces que se utiliza el icono "Descargar" para las transferencias de archivos en la sesión

HDX™ Insight

Información general

El VDA de Linux admite parcialmente la función HDX Insight.

Instalación

No es necesario instalar ningún paquete dependiente.

Uso

HDX Insight analiza los mensajes ICA® que pasan por Citrix ADC entre la aplicación Citrix Workspace™ y el VDA de Linux. Todos los datos de HDX Insight se obtienen del canal virtual NSAP y se envían sin comprimir. El canal virtual NSAP está habilitado de forma predeterminada.

Los siguientes comandos inhabilitan y habilitan el canal virtual NSAP, respectivamente:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000000" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000001" --force
```

Solución de problemas

No se muestran puntos de datos

Puede haber dos causas:

- HDX Insight no está configurado correctamente.

  Por ejemplo, AppFlow® no está habilitado en Citrix ADC o se ha configurado una instancia incorrecta de Citrix ADC en Citrix ADM.

- El canal virtual de control de ICA no se ha iniciado en el VDA de Linux.

  `ps aux | grep -i ctxctl`

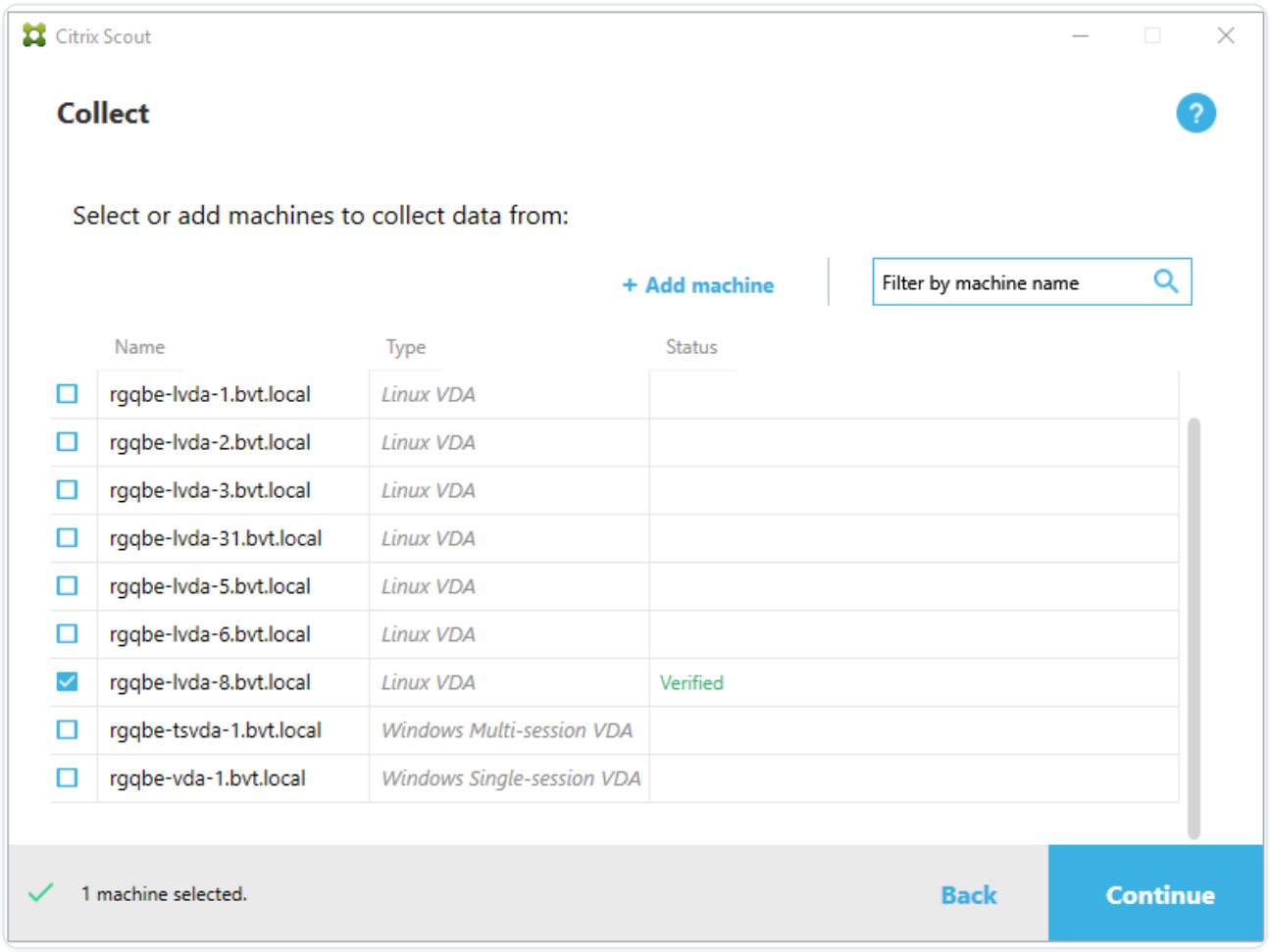
  Si `ctxctl` no se está ejecutando, póngase en contacto con su administrador para informar de un error a Citrix.

No se muestran puntos de datos de la aplicación

verificar que el canal virtual Seamless está habilitado y que se está ejecutando una aplicación Seamless.

Integración con el servicio de telemetría de Citrix

Con el servicio de telemetría de Citrix (`ctxtelemetry`) integrado con el software Linux VDA, puede ejecutar Citrix Scout, que luego utiliza el script /opt/Citrix/VDA/bin/xdlcollect.sh para recopilar registros sobre el Linux VDA.



Habilitar y deshabilitar el servicio de telemetría de Citrix

- Para habilitar el servicio, ejecute el comando **sudo systemctl enable ctxtelemetry.socket**.
- Para deshabilitar el servicio, ejecute **sudo systemctl disable ctxtelemetry.socket**.

Puertos

El servicio de telemetría de Citrix (`ctxtelemetry`), de forma predeterminada, utiliza el puerto TCP/IP 7503 para escuchar a Citrix Scout. Utiliza el puerto TCP/IP 7502 en el Delivery Controller para comunicarse con Citrix Scout.

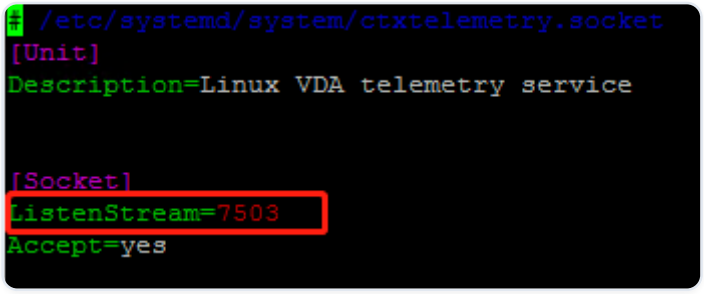
Para cambiar los puertos después de instalar el VDA, haga lo siguiente:

1. Para cambiar un puerto para comunicarse con Scout, ejecute el siguiente comando.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t REG_DWORD -v
"TelemetryServicePort" -d <port number> --force
```

2. Para cambiar el puerto de socket para escuchar a Scout, ejecute el siguiente comando para abrir y editar el archivo ctxtelemetry.socket.

```
sudo vi /etc/systemd/system/ctxtelemetry.socket
```



3. Ejecute los siguientes comandos para reiniciar el puerto de socket.

```
sudo systemctl daemon-reload

sudo systemctl stop ctxtelemetry.socket

sudo systemctl start ctxtelemetry.socket
```

4. Habilite los nuevos puertos en la configuración del firewall.

   Si utiliza Ubuntu, por ejemplo, ejecute el comando **sudo ufw allow 7503** para habilitar el puerto 7503.

Nota:

También puede ejecutar ctxsetup.sh en su lugar para automatizar los pasos 3 y 4 anteriores.

Modo de depuración

Si el servicio Citrix Telemetry no funciona como se espera, puede habilitar el modo de depuración para determinar las causas.

1. Para habilitar el modo de depuración, ejecute el siguiente comando para abrir el archivo `ctxtelemetry` y, a continuación, cambie el valor de DebugMode a 1.

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
```

```
#!/bin/sh

export PATH=/usr/lib/jvm/java-8-openjdk-amd64/jre/bin:/usr/lib/jvm/java-8-openjdk-amd64/bin:${PATH}
# Set this flag to 1 to enter debugging mode
DebugMode=1
# Set this flag to 1 to enter interactive debugging mode
InteractiveDebugMode=0
```

2. Detenga manualmente el servicio Citrix Telemetry o espere 15 minutos a que el servicio se detenga automáticamente.

```
administrator@RGQBE-LVDA-3:~$ sudo netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1447/smbd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      971/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1309/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      25158/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      998/postgres
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1447/smbd
tcp6       0      0 :::2598                 :::*                    LISTEN      28100/ctxhdx
tcp6       0      0 :::139                  :::*                    LISTEN      1447/smbd
tcp6       0      0 :::7502                 :::*                    LISTEN      1958/java
tcp6       0      0 :::7503                 :::*                    LISTEN      1/init
tcp6       0      0 :::80                   :::*                    LISTEN      1610/java
tcp6       0      0 :::1494                 :::*                    LISTEN      28100/ctxhdx
tcp6       0      0 :::22                   :::*                    LISTEN      1309/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      25158/cupsd
tcp6       0      0 :::445                  :::*                    LISTEN      1447/smbd
administrator@RGQBE-LVDA-3:~$
```

En este ejemplo, puede ejecutar los siguientes comandos para detener el servicio Citrix Telemetry.

```
sudo netstat -ntlp

Kill -9 1958
```

3. Para reiniciar el servicio Citrix Telemetry, seleccione su Linux VDA en Scout y busque telemetry-debug.log en /var/log/xdl/.

Tiempo de espera del servicio

El demonio `systemd` que abre el puerto de socket se inicia de forma predeterminada y utiliza pocos recursos. El servicio Citrix Telemetry se detiene de forma predeterminada y se inicia solo cuando hay una solicitud de recopilación de registros del Delivery Controller. Una vez completada la recopilación de registros, el servicio espera nuevas solicitudes de recopilación durante 15 minutos y se detiene de nuevo si no hay ninguna. Puede configurar el tiempo de espera mediante el siguiente comando. El valor mínimo es de 10 minutos. Si establece un valor inferior a 10 minutos, se aplicará el valor mínimo de 10 minutos. Después de configurar el tiempo de espera, detenga y reinicie el servicio.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"TelemetryServiceIdleTimeoutInMinutes" -d <number> -t REG_DWORD
```

Pruebas de verificación

Antes de que comience una recopilación, se ejecutan automáticamente pruebas de verificación para cada máquina seleccionada. Estas pruebas garantizan que se cumplen los requisitos. Si una prueba falla para una máquina, Scout muestra un mensaje con las acciones correctivas sugeridas. Para obtener más información sobre las pruebas de verificación, consulte la sección Pruebas de verificación en la documentación de Citrix Scout.

Métricas de VM y sesión de Linux

La siguiente tabla enumera las métricas disponibles para las VM de Linux y las sesiones de Linux.

MÉTRICA	VERSIÓN MÍN. DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
Duración del inicio de sesión	2402	El tiempo total de inicio de sesión está disponible con Linux VDA 2109 y versiones posteriores. Es una medida del proceso de inicio de sesión desde el momento en que un usuario se conecta desde la aplicación Citrix Workspace™ hasta que una sesión está lista para usarse. El tiempo que lleva cada fase del proceso de inicio de sesión, como la **conexión HDX™**, la **autenticación** y las **GPO**, está disponible con Linux VDA 2402	Disponible en Citrix Director y Monitor.

MÉTRICA	VERSIÓN MÍN. DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		y versiones posteriores. Para ver las métricas de duración del inicio de sesión, seleccione la ficha **Rendimiento de inicio de sesión** en la vista **Tendencias**.	
Latencia de ICA®	2311	La latencia de ICA es la latencia de red que indica si la red es lenta. Abra la vista **Detalles de la sesión** para acceder a esta métrica.	Disponible en Citrix Director y Monitor.
Directivas	2311	Todas las directivas que están en vigor para la sesión actual se muestran en la ficha **Directivas** de la vista **Detalles de la sesión**.	Disponible en Citrix Director y Monitor.
Recuento de reconexiones automáticas de sesión	2109	Para ver el número de reconexiones automáticas en una sesión, acceda a la vista **Tendencias**. Establezca las condiciones y haga clic en **Aplicar** para acotar los resultados de la búsqueda. La columna **Recuento de reconexiones automáticas de sesión** muestra el	Disponible en Citrix Director y Monitor.

MÉTRICA	VERSIÓN MÍN. DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		número de reconexiones automáticas en una sesión. La **reconexión automática** se habilita cuando las directivas de **fiabilidad de la sesión** o de **reconexión automática del cliente** están en vigor. Para obtener más información sobre las reconexiones de sesión y las directivas pertinentes, consulte los siguientes artículos. Sesiones Configuración de la directiva de reconexión automática de cliente Configuración de la directiva de fiabilidad de la sesión	
Tiempo de inactividad	2103	Para acceder a esta métrica, abra la página **Todas las sesiones** seleccionando	Disponible en Citrix Director y Monitor.

MÉTRICA	VERSIÓN MÍN. DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		Filtros > Sesiones > Todas las sesiones.	
Métricas de una VM Linux	2103	Las métricas para las VM Linux son: el número de núcleos de CPU, el tamaño de la memoria, la capacidad del disco duro y la utilización actual e histórica de la CPU y la memoria.	Disponible en Citrix Director y Monitor.
Protocolo	1909	El protocolo de transporte de una sesión Linux aparece como UDP o TCP en la vista **Detalles de la sesión**.	Disponible en Citrix Director y Monitor.
ICA RTT	1903	El tiempo de ida y vuelta (RTT) de ICA es el tiempo transcurrido desde que se pulsa una tecla hasta que la respuesta aparece en el punto final. Para obtener las métricas de RTT de ICA, cree las directivas **Cálculo de ida y vuelta de ICA** e **Intervalo de cálculo de ida y vuelta de ICA** en Citrix Studio.	Disponible en Citrix Director y Monitor.
Latencia L7	2507	La latencia de la capa de aplicación (L7) se evalúa	Disponible en Citrix Director y Monitor.

MÉTRICA	VERSIÓN MÍN. DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		mediante intercambios de sondeo y respuesta de ICA entre NetScaler o CGS y los puntos finales de CWA/VDA.	

Recopilación de registros

Descripción general del mecanismo de registro

La siguiente tabla presenta una descripción general del mecanismo de registro para el VDA de Linux.

MÓDULO DE REGISTRO	FORMATO DEL NOMBRE DEL ARCHIVO DE REGISTRO	EJEMPLO DE NOMBRE DE ARCHIVO DE REGISTRO	ÁMBITO DE REGISTRO	TAMAÑO MÁXIMO DE UN SOLO ARCHIVO	UMBRAL DE ROTACIÓN (VALORES PREDETERMINADOS)	CONFIGURACIÓN
HDX	hdx.log[.n]	hdx.log, hdx.log.1	Gráficos, inicio de sesión, audio, teclado, ratón	200 MiB	1 actual, 2 antiguos	Configurable mediante la utilidad setlog
Jproxy	jproxy.log[.n.log]	jproxy.log, jproxy.log.1.log	Registro de VDA, autenticación de usuario	20 MiB	1 actual, 10 antiguos	Configurable mediante la utilidad setlog o /etc/xdl/log4j2.xml

MÓDULO DE REGISTRO	FORMATO DEL NOMBRE DEL ARCHIVO DE REGISTRO	EJEMPLO DE NOMBRE DE ARCHIVO DE REGISTRO	ÁMBITO DE REGISTRO	TAMAÑO MÁXIMO DE UN SOLO ARCHIVO	UMBRAL DE ROTACIÓN (VALORES PREDETERMINADOS)	CONFIGURACIÓN
VDA	vda.YYYY-MM-DD.hh.mm.ss.log	vda.2024-05-06.20.18.40.log	Registro de VDA	50 MiB	1 actual, 1 antiguo	Configurable mediante la utilidad setlog o /etc/xdl/brokeragent.conf

Nota:

- El primer archivo de registro no tiene un número en su nombre, y los archivos subsiguientes se numeran con ".n", donde "n" representa el número de archivo. Por ejemplo, "hdx.log" es el primer archivo de registro HDX y "hdx.log.1" es el segundo.
- El tamaño máximo de un solo archivo de registro se mide en mebibytes (MiB).
- Un archivo de registro que se está generando y aún no ha alcanzado el tamaño máximo para un solo archivo se denomina archivo de registro "actual". Cuando un archivo de registro "actual" alcanza el tamaño máximo para un solo archivo, se transfiere y se convierte en un archivo de registro "antiguo".
- El umbral de rotación es configurable para limitar el número de archivos de registro "antiguos" que se pueden conservar. Los archivos de registro más antiguos se eliminarán cuando se alcance el límite.

Configuración del registro

Esta sección proporciona información adicional sobre la configuración del registro, complementando los detalles descritos en la tabla anterior.

Registro habilitado de forma predeterminada para el VDA de Linux

El demonio ctxlogd y la utilidad setlog se incluyen en el paquete de la versión del VDA de Linux. De forma predeterminada, el demonio ctxlogd se inicia después de instalar y configurar el VDA de Linux. Todos los demás servicios que se rastrean dependen del demonio ctxlogd. Puede detener el demonio ctxlogd si no desea mantener el VDA de Linux rastreado.

Configurar el registro del VDA mediante /etc/xdl/brokeragent.conf

> **Nota:**

> Si solo desea configurar los niveles de registro para el registro del VDA sin profundizar en otros parámetros de registro, como el tamaño máximo de un solo archivo de registro, puede usar la utilidad setlog que se describe más adelante en este artículo. De lo contrario, use /etc/xdl/brokeragent.conf.

> El archivo /etc/xdl/brokeragent.conf en el VDA está disponible para configurar el registro del VDA. Por ejemplo:

```
<!-- VDA trace settings -->
<add key="TraceProvider.Type" value="QueuedLogFileProvider"/>
<add key="TraceProvider.BaseFilename" value="/var/log/xdl/vda.log"/>
<add key="TraceProvider.AppendMode" value="true"/>
<add key="TraceProvider.SizeLimit" value="50"/>
<add key="TraceProvider.TrailCount" value="2"/>
<add key="TraceProvider.ProcessSafe" value="true"/>
<add key="TraceProvider.CategoryFilter" value="All" />
```

Configurar el registro de Jproxy mediante /etc/xdl/log4j2.xml

> **Nota:**

> Si solo desea configurar los niveles de registro para el registro de Jproxy sin profundizar en otros parámetros de registro, como el tamaño máximo de un solo archivo de registro, puede usar la utilidad setlog que se describe más adelante en este artículo. De lo contrario, use /etc/xdl/log4j2.xml.

A continuación, se muestra un ejemplo de configuración del registro de Jproxy mediante /etc/xdl/log4j2.xml, donde el parámetro **SizeBasedTriggeringPolicy** especifica el tamaño máximo para un solo archivo de registro de Jproxy y el parámetro **DefaultRollerStrategy** establece el número total de archivos de registro de Jproxy que se pueden conservar.

```
<!-- Logging Properties -->
<Properties>
    <Property name="LOG_PATTERN">%d{yyyy-MM-dd HH:mm:ss.SSS}{GMT} [%-5p] [%tid] - %m%n</Property>
    <Property name="logfile">/var/log/xdl/jproxy.log</Property>
    <Property name="perflogfile">/var/log/xdl/jproxyperf.log</Property>
</Properties>

<Appenders>

  <Console name="CONSOLE" target="SYSTEM_OUT">
    <PatternLayout pattern="${LOG_PATTERN}"/>
  </Console>

  <RollingFile name="logfile" fileName="${sys:logfile}"
    filePattern="${sys:logfile}.%i.log">
    <PatternLayout pattern="${LOG_PATTERN}"/>
    <Policies>
        <SizeBasedTriggeringPolicy size="19500KB" />
    </Policies>
    <DefaultRolloverStrategy max="10"/>
  </RollingFile>

  <RollingFile name="perflogfile" fileName="${sys:perflogfile}"
    filePattern="${sys:perflogfile}.%i.log">
    <PatternLayout pattern="${LOG_PATTERN}"/>
    <Policies>
        <SizeBasedTriggeringPolicy size="19500KB" />
    </Policies>
    <DefaultRolloverStrategy max="10"/>
  </RollingFile>
```

Configurar el registro de HDX™ mediante la utilidad setlog

La utilidad setlog reside en la ruta /opt/Citrix/VDA/bin/. Solo el usuario root tiene el privilegio de ejecutarla. Puede usar la GUI o ejecutar comandos para ver y cambiar sus opciones de configuración, incluidos los valores (ruta del archivo de registro, límite de tamaño de archivo único y umbral de rotación) y los niveles de registro. Ejecute el siguiente comando para obtener ayuda con la utilidad setlog:

```
setlog help
```

VALORES

De forma predeterminada, los registros HDX se guardan en **/var/log/xdl/hdx.log**, el límite de tamaño para un único archivo de registro HDX es de 200 MiB, y puede guardar hasta dos archivos de registro HDX "antiguos" en **/var/log/xdl/hdx.log**.

Para ver todos los valores actuales de setlog, ejecute el siguiente comando:

```
setlog values


log_path (Log Output Path) = /var/log/xdl/hdx.log


log_size (Max Log Size (MiB)) = 200


log_count (Max Old Log Files) = 2
```

Para ver o establecer un único valor de setlog, ejecute el siguiente comando:

```
setlog value <name> [<value>]
```

Por ejemplo:

```
setlog value log_size 100
```

NIVELES

De forma predeterminada, los niveles de registro se establecen en **info** (sin distinción entre mayúsculas y minúsculas).

Cuando encuentre un problema que requiera solución de problemas, le recomendamos que establezca el nivel de registro en **verbose** en la mayoría de los escenarios. Después, reproduzca el problema y recopile los registros.

Para establecer los niveles de registro (incluidos Deshabilitado, Heredado, Traza, Detallado, Información, Advertencias, Errores y Errores fatales), ejecute el siguiente comando:

```
setlog level <class> [<level>]
```

NIVEL DE REGISTRO	PARÁMETRO DE COMANDO (SIN DISTINCIÓN ENTRE MAYÚSCULAS Y MINÚSCULAS)
Deshabilitado	ninguno
Heredado	heredar
Traza	traza
Detallado	detallado
Información	información
Advertencias	Advertencia
Errores	Error
Errores graves	grave

La variable `<class>` especifica un componente del VDA de Linux. Para cubrir todos los componentes, establézcala en 'all'. Por ejemplo:

```
setlog level all error
```

Para ver todas las clases o componentes admitidos, ejecute el siguiente comando:

```
setlog levels
```

RESTAURAR VALORES PREDETERMINADOS

Revierta todos los niveles y valores a la configuración predeterminada:

```
setlog default
```

Importante:

El servicio **ctxlogd** se configura mediante el archivo **/var/xdl/.ctxlog**, que solo los usuarios raíz pueden crear. Otros usuarios no tienen permiso de escritura para este archivo. Recomendamos que los usuarios raíz no otorguen permiso de escritura a otros usuarios. El

> incumplimiento puede provocar una configuración arbitraria o maliciosa de **ctxlogd**, lo que puede afectar el rendimiento del servidor y, por lo tanto, la experiencia del usuario.

Recopilación de registros

Puede ejecutar el comando **bash /opt/Citrix/VDA/bin/xdlcollect.sh** para recopilar registros. El script Bash **xdlcollect** utilizado para recopilar registros está integrado en el software Linux VDA y se encuentra en **/opt/Citrix/VDA/bin**.

Una vez finalizada la recopilación de registros, se genera un archivo ZIP en **/tmp/xdlcollect** en el VDA.

Recopilación y carga de registros AOT

Información general

Esta característica recopila registros de **Always-On Tracing (AOT)** de los componentes del **Virtual Delivery Agent (VDA)**. Admite:

- Solución de problemas difíciles de reproducir
- Comprobaciones diarias del estado
- Gestión centralizada de registros

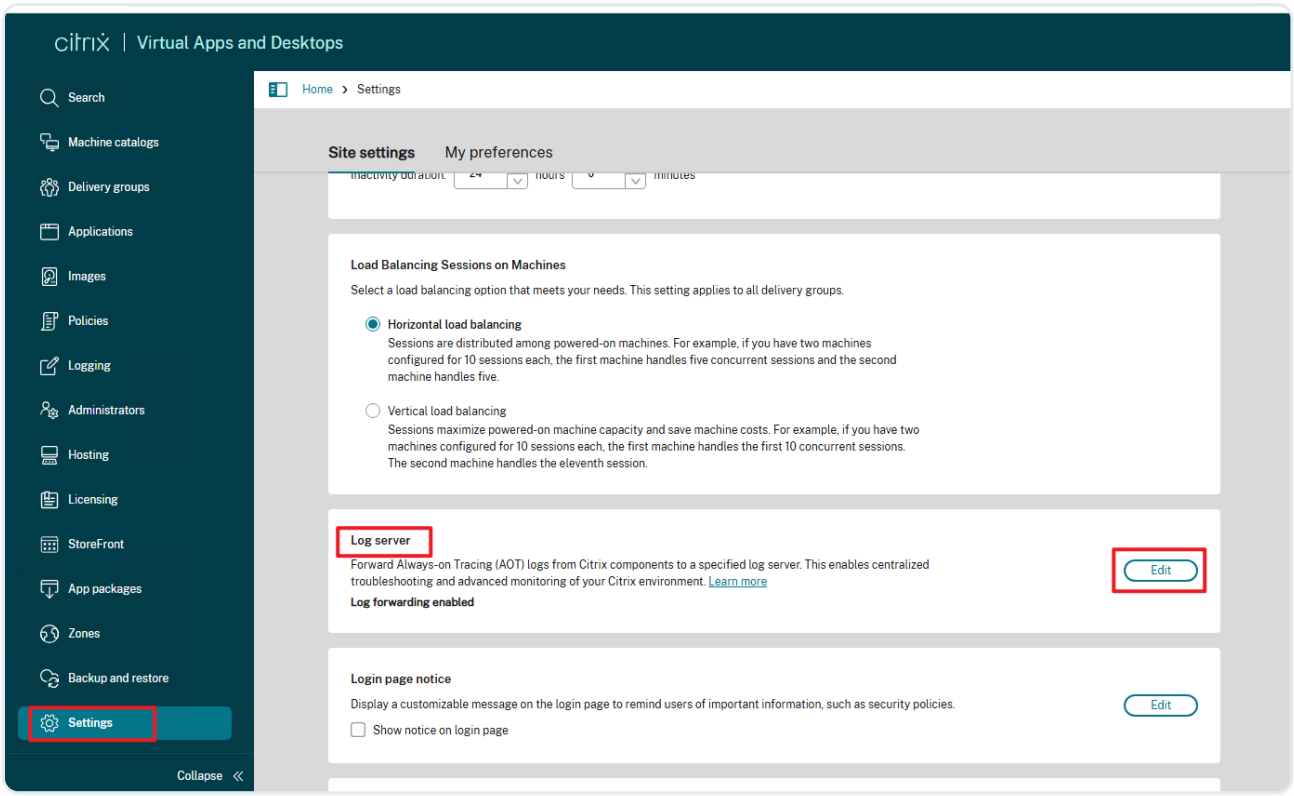
Los registros se transforman en eventos estructurados y se cargan en un **servidor de registros** centralizado para su consulta y análisis.

Configuración

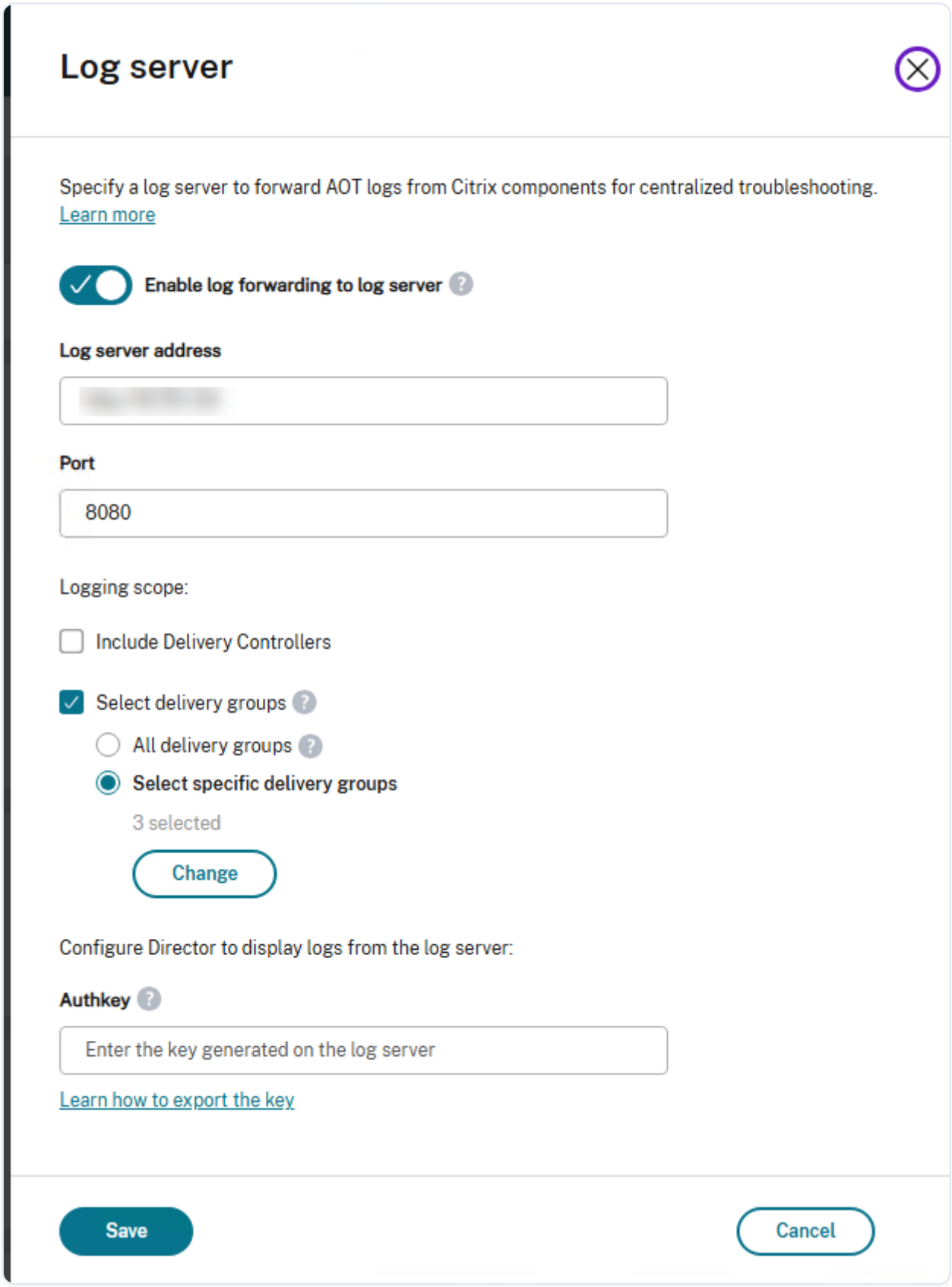
CONFIGURACIÓN DE DIRECTIVAS DE GRUPO

Para habilitar esta característica a través de la **Directiva de grupo**, asegúrese de que el **servidor de registros** esté configurado correctamente en el **Delivery Controller (DDC)**. Los pasos son los siguientes:

1. En Citrix Studio, haga clic en Configuración->Servidor de registros->Editar



1. Establezca la dirección y el puerto del servidor de registros para habilitar el reenvío de registros al servidor de registros



CONFIGURACIÓN DEL REGISTRO LOCAL

Los registros locales tienen mayor prioridad que las directivas. Para habilitar esta característica a través del registro local, ejecute los siguientes comandos en el VDA (reemplace `<ip>` y `<port>` con los suyos):

Habilitar la recopilación de datos AOT:

Establecer el punto de conexión del servidor de registros:

```
sudo /opt/Citrix/VDA/bin/ctxreg create \

  -k "HKLM\System\CurrentControlSet\Control\Citrix\AOT" \

  -t "REG_DWORD" \

  -v "EnableAotDataCollection" \

  -d "0x00000001" --force



sudo /opt/Citrix/VDA/bin/ctxreg create \

  -k "HKLM\System\CurrentControlSet\Control\Citrix\AOT" \

  -t "REG_SZ" \

  -v "AotDataStoreEndpoint" \

  -d "<http/https>://<fqdn-or-ip-address>:<port>" --force
```

Una vez que cambien la configuración de la directiva enviada desde Studio o la configuración del registro local, el servicio ctxvector aplicará automáticamente el cambio en menos de 1 minuto. No es necesario reiniciarlo manualmente.

AUTENTICACIÓN TLS

Esta función admite conexiones HTTP y HTTPS al servidor de registros. Para HTTPS, instale los certificados raíz de CA en el almacén de claves del sistema Linux. El VDA solo puede establecer una conexión HTTPS correctamente después de autenticar el certificado del servidor de registros. El servidor de registros no autentica el VDA.

Solución de problemas

El demonio **ctxlogd** falla y no se puede reiniciar el servicio **ctxlogd** cuando falta el archivo **/var/xdl/.ctxlog** (por ejemplo, si se eliminó accidentalmente).

/var/log/messages:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
configuration file.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited,
code=exited, status=1/FAILURE



Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
```

Para resolver este problema, ejecute setlog como usuario root para volver a crear el archivo **/var/xdl/.ctxlog**. Luego, reinicie el servicio **ctxlogd** del que dependen otros servicios.

Sombreado de sesión

El sombreado de sesiones permite a los administradores de dominio ver las sesiones ICA® de los usuarios en una intranet. La función utiliza noVNC para conectarse a las sesiones ICA.

> **Nota:**
>
> Para usar la función, utilice `Citrix Director` 7.16 o posterior.

Instalación y configuración

Dependencias

Se requieren dos nuevas dependencias, `python-websockify` y `x11vnc`, para el sombreado de sesiones. Instale `python-websockify` y `x11vnc` manualmente después de instalar el VDA de Linux.

Para Amazon Linux2:

Ejecute los siguientes comandos para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior):

```
sudo pip3 install websockify

sudo yum install x11vnc
```

Para RHEL 9.x/8.x y Rocky Linux 9.x/8.x:

Ejecute los siguientes comandos para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior).

```
sudo pip3 install websockify

sudo yum install x11vnc
```

Resuelva `x11vnc` habilitando los repositorios EPEL y CodeReady Linux Builder:

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-
release-latest-8.noarch.rpm



subscription-manager repos --enable "codeready-builder  -for-rhel-8-
x86_64-rpms"
```

Para Ubuntu:

Ejecute los siguientes comandos para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior):

```
sudo pip3 install websockify

sudo apt-get install x11vnc
```

Para SUSE:

Primero, habilite el módulo "SUSE Linux Enterprise Workstation Extension 15 SP6" mediante YaST o el siguiente comando **SUSEConnect**:

```
suseconnect -p sle-we/15.6/x86_64 -r <regcode>
```

Para obtener más información, consulte la documentación de SUSE: `<https://documentation.suse.com/es-es/sles/15-SP6/html/SLES-all/article-modules.html>`.

Luego, ejecute los siguientes comandos para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior):

```
sudo pip3 install websockify

sudo zypper install x11vnc
```

Para Debian 12:

Ejecute los siguientes comandos para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior):

```
apt install python3-websockify

sudo apt-get install x11vnc
```

Para Debian 11:

Ejecute los siguientes comandos para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior):

```
sudo pip3 install websockify

sudo apt-get install x11vnc
```

Puerto

La función de sombreado de sesiones selecciona automáticamente los puertos disponibles entre 6001 y 6099 para establecer conexiones desde el VDA de Linux a `Citrix Director`. Por lo tanto, el número de sesiones ICA que puede sombrear simultáneamente está limitado a 99. Asegúrese de que haya suficientes puertos disponibles para satisfacer sus requisitos, especialmente para el sombreado de varias sesiones.

Registro

La siguiente tabla enumera los registros relacionados:

REGISTRO	DESCRIPCIÓN	VALOR PREDETERMINADO
EnableSessionShadowing	Habilita o deshabilita la función de sombreado de sesiones.	1 (Habilitado)
ShadowingUseSSL	Determina si se debe cifrar la conexión entre el VDA de Linux y Citrix Director	0 (Deshabilitado)

Ejecute el comando `ctxreg` en el VDA de Linux para cambiar los valores del registro. Por ejemplo, para deshabilitar el sombreado de sesiones, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "EnableSessionShadowing" -d
"0x00000000"
```

SSL

La conexión noVNC entre el VDA de Linux y Citrix Director utiliza el protocolo WebSocket. Para el shadowing de sesiones, la elección entre `ws://` o `wss://` depende del registro "ShadowingUseSSL" mencionado anteriormente. De forma predeterminada, se elige `ws://`. Sin embargo, por motivos de seguridad, le recomendamos que utilice `wss://` e instale certificados en cada cliente de Citrix Director y en cada servidor VDA de Linux. Citrix declina toda responsabilidad de seguridad por el shadowing de sesiones del VDA de Linux al usar `ws://`.

Para habilitar SSL, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "ShadowingUseSSL" -d
"0x00000001"
```

OBTENER CERTIFICADOS SSL DE SERVIDOR Y RAÍZ

Los certificados deben estar firmados por una entidad de certificación (CA) de confianza.

Se requiere un certificado de servidor independiente (incluida la clave) para cada servidor VDA de Linux en el que desee configurar SSL. Un certificado de servidor identifica un equipo específico, por lo que debe conocer el nombre de dominio completo (FQDN) de cada servidor. Para mayor comodidad, considere la posibilidad de utilizar un certificado comodín para todo el dominio.

También se requiere un certificado raíz para cada cliente de Citrix Director que se comunica con el VDA de Linux. Los certificados raíz están disponibles en las mismas CA que emiten los certificados de servidor.

Puede instalar certificados de servidor y de cliente de las siguientes CA:

- Una CA que se incluye con su sistema operativo
- Una CA empresarial (una CA a la que su organización le da acceso)
- Una CA no incluida con su sistema operativo

Consulte al equipo de seguridad de su organización para averiguar qué métodos requieren para obtener certificados.

> **Importante:**
>
> - El nombre común de un certificado de servidor debe ser el FQDN exacto del VDA de Linux o, al menos, el comodín correcto más los caracteres de dominio. Por ejemplo, vda1.basedomain.com o *.basedomain.com.
> - Los algoritmos de hash, incluidos SHA1 y MD5, son demasiado débiles para las firmas de certificados digitales para que algunos navegadores los admitan. Por lo tanto, SHA-256 se especifica como el estándar mínimo.
> - Chrome ha dejado de aceptar certificados SSL autofirmados, considerándolos inseguros. El error `NET::ERR_CERT_COMMON_NAME_INVALID` se produce porque el certificado generado carece del campo SAN (subjectAltName). Para resolver este problema, proporcione un certificado con atributos extendidos (extensiones X509 v3) que incluyan el campo SAN.

INSTALAR UN CERTIFICADO RAÍZ EN CADA CLIENTE DE CITRIX DIRECTOR

El shadowing de sesiones utiliza el mismo almacén de certificados basado en el registro que IIS, por lo que puede instalar certificados raíz mediante IIS o el complemento Certificados de Microsoft Management Console (MMC). Cuando recibe un certificado de una CA, puede reiniciar el Asistente para certificados de servidor web en IIS y el asistente instala el certificado. Alternativamente, puede ver e importar certificados en el equipo mediante la MMC y agregar el certificado como un complemento independiente. Internet Explorer y Google Chrome importan los certificados instalados en su sistema operativo de forma predeterminada. Para Mozilla Firefox,

debe importar sus certificados de CA raíz en la pestaña **Autoridades** del Administrador de certificados.

INSTALE UN CERTIFICADO DE SERVIDOR Y SU CLAVE EN CADA SERVIDOR LINUX VDA

Asigne el nombre "shadowingcert.*" a los certificados de servidor y "shadowingkey.*" al archivo de clave (* indica el formato, por ejemplo, shadowingcert.pem y shadowingkey.key). Coloque los certificados de servidor y los archivos de clave en la ruta **/etc/xdl/shadowingssl** y protéjalos correctamente con permisos restringidos, permitiendo que solo **ctxsrvr** tenga acceso de lectura. Un nombre o una ruta incorrectos impiden que el Linux VDA encuentre un certificado o un archivo de clave específicos y, por lo tanto, provoca un error de conexión con `Citrix Director`. Los comandos son los siguientes:

```
cp <vda's-public-key> /etc/xdl/shadowingssl/shadowingcert.pem

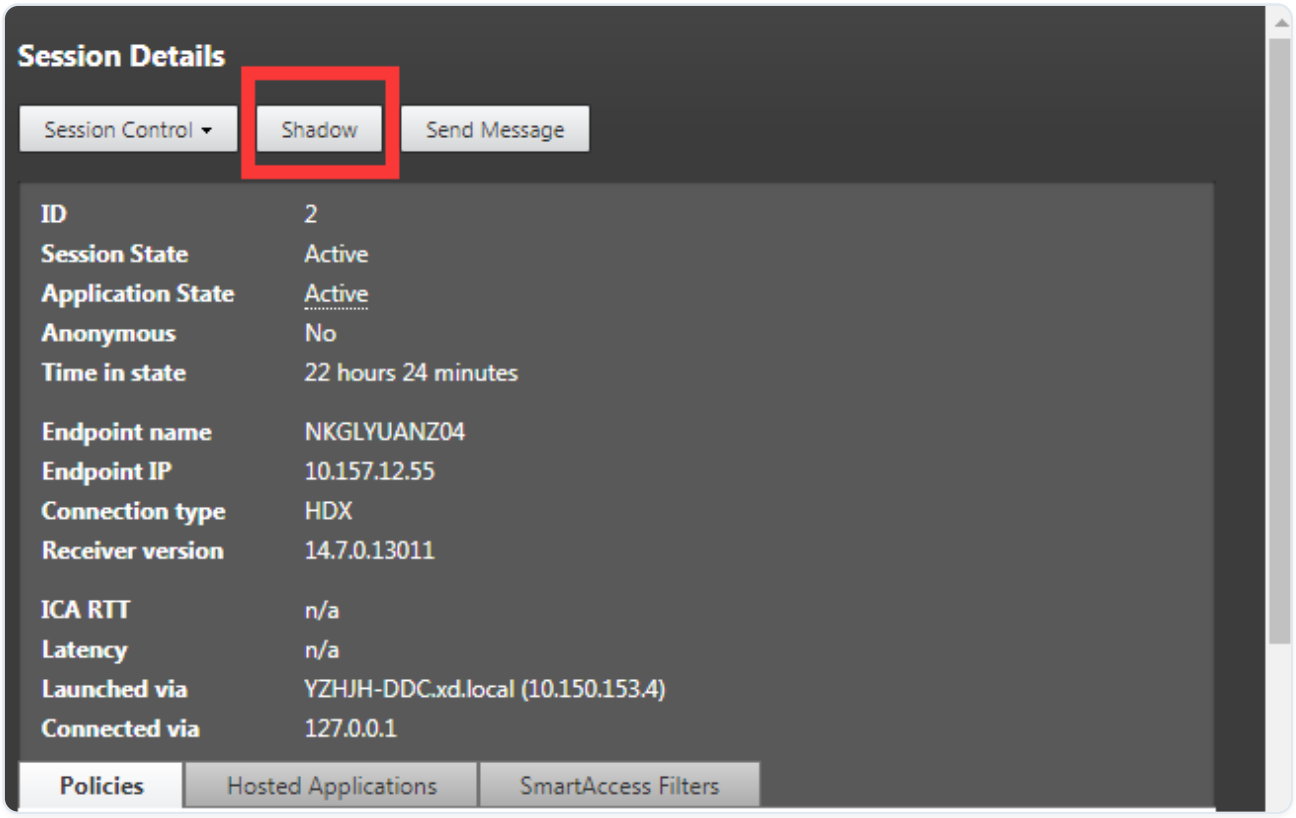
cp <vda's-server-private-key> /etc/xdl/shadowingssl/shadowingkey.key

sudo chown ctxsrvr:ctxadm  /etc/xdl/shadowingssl/shadowingcert.pem

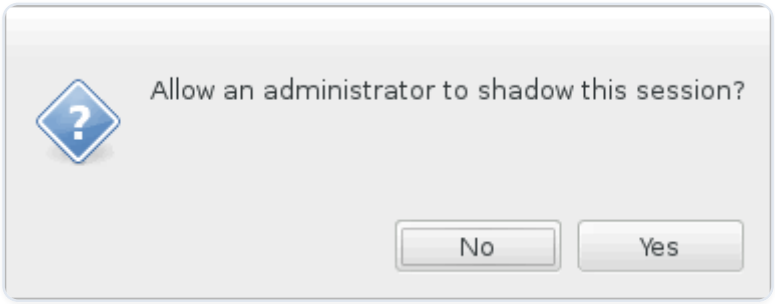
sudo chown ctxsrvr:ctxadm  /etc/xdl/shadowingssl/shadowingkey.key
```

Uso

Desde `Citrix Director`, busque la sesión de destino y haga clic en **Shadow** en la vista **Detalles de la sesión** para enviar una solicitud de shadowing al Linux VDA.



Una vez que la conexión se inicializa, aparece una confirmación en el cliente de sesión ICA (no en el cliente `Citrix Director`) para solicitar al usuario permiso para duplicar la sesión.



Si el usuario hace clic en **Sí**, aparece una ventana en el lado `Citrix Director`, indicando que la sesión ICA se está duplicando.

Para obtener más información sobre el uso, consulte la documentación de Citrix Director.

Limitaciones

- Si sus VDA están unidos a un dominio y están alojados en Microsoft Azure mediante Azure Active Directory (AAD) para la autenticación, la función de shadowing de sesiones no funciona.
- El shadowing de sesiones está diseñado para usarse solo en una Intranet. No funciona para redes externas, incluso si se conecta a través de Citrix Gateway. Citrix declina toda responsabilidad por el shadowing de sesiones de Linux VDA en una red externa.
- Con el shadowing de sesiones habilitado, un administrador de dominio solo puede ver las sesiones ICA, pero no tiene permiso para escribir o controlarlas.

- Después de que un administrador haga clic en **Shadow** desde `Citrix Director`, aparece una confirmación para solicitar al usuario permiso para duplicar la sesión. Una sesión solo se puede duplicar cuando el usuario de la sesión otorga el permiso.
- La confirmación mencionada anteriormente tiene una limitación de tiempo de espera, que es de 20 segundos. Una solicitud de shadowing falla cuando se agota el tiempo.
- Una sesión solo puede ser duplicada por un administrador. Por ejemplo, si el administrador B envía una solicitud de shadowing para una sesión que el administrador A está duplicando, la confirmación para obtener el permiso del usuario vuelve a aparecer en el dispositivo del usuario. Si el usuario acepta, la conexión de shadowing para el administrador A se detiene y se establece una nueva conexión de shadowing para el administrador B. Si un administrador envía otra solicitud de shadowing para la misma sesión, también se puede establecer una nueva conexión de shadowing.
- Para usar el shadowing de sesiones, instale `Citrix Director` 7.16 o una versión posterior.
- Un cliente `Citrix Director` utiliza un FQDN en lugar de una dirección IP para conectarse al servidor Linux VDA de destino. Por lo tanto, el cliente `Citrix Director` debe poder resolver el FQDN del servidor Linux VDA.

Solución de problemas

Si el shadowing de sesiones falla, depure tanto en el cliente `Citrix Director` como en el Linux VDA.

En el cliente de Citrix Director

A través de las herramientas de desarrollador del explorador, compruebe los registros de salida en la ficha **Console**. O bien, compruebe la respuesta de la API ShadowLinuxSession en la ficha **Network**. Si aparece la confirmación para obtener el permiso del usuario, pero la conexión no se establece, haga ping manualmente al FQDN del VDA para verificar que `Citrix Director` puede resolver el FQDN. Si hay un problema con la conexión `wss://`, compruebe sus certificados.

En el Linux VDA

1. Compruebe el archivo `/var/log/xdl/vda.log` para obtener pistas.
2. Edite el archivo `/var/xdl/sessionshadowing.sh` y cambie la variable 'logFile' para especificar un archivo de registro que se pueda seguir para obtener pistas durante el shadowing de sesiones desde el director.
3. Además, puede verificar manualmente si sus certificados funcionan correctamente con la conexión noVNC:

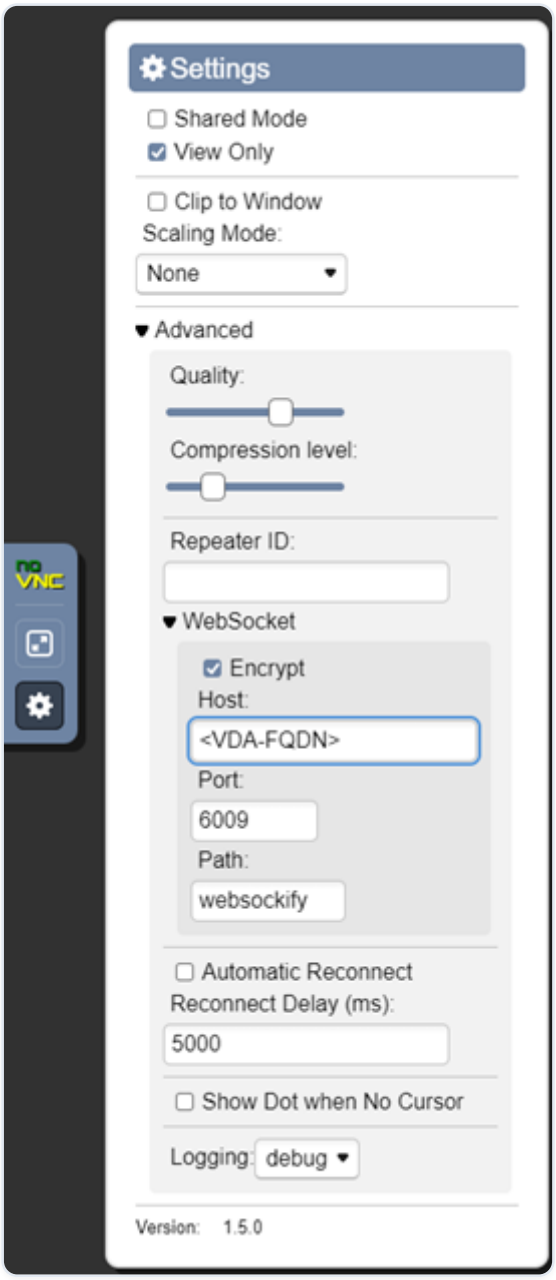
a. Ejecute **ps aux \| grep xorg** para encontrar el número de pantalla Xorg de la sesión actual **$display-num**, por ejemplo, **:3**.

b. Ejecute el siguiente comando para iniciar un servidor x11vnc y esperar una conexión entrante.

> **Nota:**
>
> Antes de ejecutar el siguiente comando, establezca las variables **$passwd**, **$port** y **$display-num**.

```
runuser -l "ctxsrvr" -s /bin/bash -c "websockify <port> -v --cert  /
etc/xdl/shadowingssl/shadowingcert.pem --key  /etc/xdl/shadowingssl/
shadowingkey.key -- x11vnc  -viewonly  -shared -passwd $passwd
-rfbport $port -display $display-num -many -o /var/log/xdl/
x11vnc.log"
```

c. Intente conectarse mediante noVNC para verificar el modo SSL de la siguiente manera. Introduzca el FQDN de su VDA y el número de puerto. En este ejemplo, el número de puerto es 6009.



d. Resuelva cualquier error impreso por Websockify en el VDA o notificado por el explorador en el cliente.

   Puntos de control clave durante el establecimiento de la conexión:

   i. Compruebe si hay alguna limitación del firewall que impida que el shadowing de sesiones abra el puerto.

   ii. verificar que ha nombrado los certificados y los archivos de clave correctamente y que los ha colocado en la ruta correcta si se trata de un escenario SSL.

   iii. verificar que quedan suficientes puertos entre 6001 y 6099 para nuevas solicitudes de shadowing.

iv. Ejecute `openssl x509 -in shadowingcert.pem -text -noout` para verificar que los certificados están configurados correctamente, prestando especial atención a los campos CN y SAN.

v. En RHEL 8, puede haber un problema por el que no se encuentre `rebind.so`. Para resolver este problema, ejecute el siguiente comando:

```
ln -s /usr/bin/rebind.so /usr/local/bin/rebind.so
```

Comunicación WebSocket entre VDAs y Delivery Controllers

Este artículo describe los pasos para establecer la comunicación WebSocket entre VDAs y Delivery Controllers, como alternativa a Windows Communication Foundation (WCF).

Paso 1: Habilitar WebSocket en los Delivery Controllers

1. Configure su sitio. Para obtener más información, consulte Crear un sitio.
2. Instale certificados TLS en cada Delivery Controller presente en su sitio. Para obtener más información, consulte Instalar certificados de servidor TLS en los Controllers.
3. Habilite la comunicación WebSocket en cada Delivery Controller™ mediante el siguiente comando:

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **Nota:**
>
> Asegúrese de reiniciar los Delivery Controllers después de habilitar WebSocket.

Paso 2: Habilitar WebSocket en los VDAs

1. Instale las entidades de certificación (CA) raíz e intermedias en los VDAs para confiar en los Delivery Controllers.
2. Habilite la comunicación WebSocket para los VDAs según el método de creación de VDA:

   - **VDAs no unidos a un dominio**:

La comunicación WebSocket está habilitada de forma predeterminada. No se requiere ninguna configuración adicional.

- **VDAs unidos a un dominio creados mediante la instalación sencilla**:

  Habilite WebSocket configurando las siguientes variables de entorno en `/opt/Citrix/VDA/sbin/ctxinstall.conf` antes de ejecutar el script de instalación sencilla (ctxinstall.sh) inicialmente.

  - **CTX_XDL_DJ_ENROLLMENT_TOKEN_FILE=<file-path\>|'<none\>'** – Controla la habilitación de WebSocket y especifica el archivo de token para el registro de VDA. El valor predeterminado es **'<none\>'**, lo que significa que WebSocket está deshabilitado. Para habilitar WebSocket en un VDA unido a un dominio, introduzca la ruta al archivo de token.
  - **CTX_XDL_ENROLLMENT_TOOL_USING_LDAPS='y|n'** – Configura la herramienta de inscripción para consultar LDAP o LDAPS. De forma predeterminada, consulta LDAP (**'n'**). Para usar LDAPS, establezca el valor en **'y'**.

- **VDA unidos a un dominio creados mediante Machine Creation Services™ (MCS)**:

  En la máquina de plantilla, abra `/etc/xdl/mcs/mcs_local_setting.reg` y añada una línea de comandos similar a la siguiente para habilitar WebSocket:

  ```
  create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD"
  -v "CbpTransportVersion2" -d "0x00000001" --force
  ```

  Este comando crea o modifica la clave de registro **CbpTransportVersion2**. De forma predeterminada, el valor es **0** (comunicación WCF). Para habilitar la comunicación WebSocket en los VDA unidos a un dominio, establezca el valor en cualquier valor distinto de cero. Después de modificar el registro, reinicie el servicio **ctxvda** para aplicar los cambios.

  > **Consejo:**
  >
  > En cualquier VDA unido a un dominio, independientemente de su método de creación, puede utilizar la clave de registro **CbpTransportVersion2** para alternar entre WCF y WebSocket.

El demonio del servicio de monitorización

El servicio de monitorización, **ctxmonitord**, es un demonio que supervisa el estado de salud del VDA de Linux. Consta de tres módulos:

- Módulo de monitorización de procesos clave: Este módulo delega en Systemd el reinicio automático de los servicios clave en caso de fallos inesperados, escanea y registra periódicamente el estado de los procesos de destino, y garantiza la limpieza oportuna de los residuos de Xorg. Los registros se almacenan en **/var/log/xdl/ms.log**.
- Módulo de integración de XDPing: Este módulo ejecuta periódicamente tareas de análisis y copia de seguridad de XDPing. Toda la salida de estas tareas se puede encontrar en **/var/log/xdl/msxdping.log**.
- Módulo de autoactualización del VDA de Linux: Para obtener más información, consulte Autoactualización del VDA de Linux a través de Azure.

Configuración

De forma predeterminada, el servicio de monitorización **ctxmonitord** se inicia automáticamente al iniciar el VDA. Con privilegios de administrador, puede configurarlo a través de /etc/xdl/ctxmonitord.conf y /etc/xdl/whitelist.conf.

ctxmonitord.conf

Este archivo de configuración especifica el comportamiento del servicio de monitorización ctxmonitord y sus módulos. De forma predeterminada, está configurado de la siguiente manera:

```
     ; This is the configuration file for ctxmonitord service




; Section 'service' configures the key process monitor module

[service]

MonitorEnable=true     ; true or false

DetectInterval=300      ; in seconds, minimum is 60
```

```
; Section 'xdping' configures the XDPing integration module

[xdping]

XdpingEnable=true      ; true or false

AnalysisInterval=600    ; in seconds, minimum is 60, 0 means disable

BackupInterval=1        ; in days, 0 means disable



; Section 'rules' configures the rules about how to monitor each key
process

; Each rule should be named as rules.<ProcessName> where <ProcessName> is
the name of the process to be monitored

; 'ProcessName' should be the name of the target process that is picked up
from whitelist.conf

; 'MonitorType' should be 'HealthCheck' or 'ResidueCleanup'. All
'MonitorType' should be 'HealthCheck' except for 'Xorg'

[rules]

[rules.ctxhdx]

ProcessName=ctxhdx

MonitorType=HealthCheck



[rules.ctxvda]

ProcessName=ctxvda

MonitorType=HealthCheck



[rules.ctxjproxy]
```

```
ProcessName=ctxjproxy

MonitorType=HealthCheck



[rules.ctxpolicyd]

ProcessName=ctxjproxy

MonitorType=HealthCheck



[rules.ctxlogd]

ProcessName=ctxlogd

MonitorType=HealthCheck



[rules.xorg]

ProcessName=Xorg

MonitorType=ResidueCleanup
```

whitelist.conf

Este archivo de configuración especifica la lista blanca de los procesos de destino que se van a supervisar. Los servicios de destino especificados en el archivo ctxmonitord.conf también deben aparecer en el archivo whitelist.conf. De forma predeterminada, está configurado de la siguiente manera:

```
ctxhdx

ctxvda

ctxjproxy

ctxlogd
```

```
ctxcdm

ctxcups

ctxpolicyd

ctxusbsd

ctxceip

ctxsdcd

ctxrunatboot

ctxgdtd

ctxbcrd

ctxfidod

ctxpfwd

ctxwcamsd

ctxcertmgr

ctxscardsd  # Except for SLES

ctxfedsd    # Only for RHEL 8/9

Xorg
```

Nota:

- Para que los cambios en los archivos ctxmonitord.conf y whitelist.conf surtan efecto, ejecute el comando **systemctl restart ctxmonitord** para reiniciar el demonio del servicio de monitorización.

- Para configurar cómo se reinician los servicios en caso de fallos inesperados, edite el archivo **/usr/lib/systemd/system/ctx*.service**. Por ejemplo, las siguientes son las opciones de reinicio predeterminadas:

```
Restart=on-failure

RestartSec=5

StartLimitInterval=60

StartLimitBurst=3
```

Solución de problemas

Este artículo describe cómo usar **XDPing** para solucionar problemas y cómo consultar las métricas de sesión con la utilidad **ctxsdcutil**.

XDPing

La herramienta **XDPing** de Linux es una aplicación de línea de comandos. Automatiza el proceso de comprobación de problemas de configuración comunes en un entorno VDA de Linux.

Instalar la herramienta XDPing de Linux

La ejecución de ctxsetup.sh no instala **XDPing**. Para instalar **XDPing**, ejecute `sudo /opt/Citrix/VDA/bin/xdping`. Este comando también crea un entorno virtual de **Python3** que es necesario para **XDPing**. Si este comando no crea un entorno virtual de **Python3**, créelo manualmente siguiendo las instrucciones en Crear un entorno virtual de **Python3**.

Para solucionar los errores de conexión SSL que pueda encontrar al usar la herramienta pip, considere agregar los siguientes hosts de confianza al archivo /etc/pip.conf:

`[global]`

`trusted-host =` `pypi.org`

`files.pythonhosted.org`

Tareas que se pueden realizar con XDPing

XDPing viene con un único ejecutable llamado **xdping** que se ejecuta desde el shell de comandos.

La siguiente tabla describe las diversas tareas que se pueden realizar con los comandos **XDPing** correspondientes:

TAREA	COMANDO XDPING	OBSERVACIONES
Para mostrar las opciones de línea de comandos	**sudo /opt/Citrix/VDA/bin/xdping -h**	N/D
Para ejecutar el conjunto completo de pruebas	**sudo /opt/Citrix/VDA/bin/xdping** (ejecute **XDPing** sin ninguna opción de línea de comandos)	La herramienta Linux **XDPing** realiza más de 150 pruebas individuales en el sistema. Para obtener más información, consulte Pruebas individuales más adelante en este artículo.
Para ejecutar una comprobación del estado de registro de VDA	**sudo /opt/Citrix/VDA/bin/xdping -a**	Para obtener más información, consulte Alcance de las comprobaciones del estado de registro más adelante en este artículo.
Para hacer una copia de seguridad de los datos clave de un VDA	**sudo /opt/Citrix/VDA/bin/xdping -b**	Para obtener más información, consulte Copia de seguridad y comparación de datos de VDA más adelante en este artículo.
Para comparar las dos últimas copias de los datos de copia de seguridad de VDA	**sudo /opt/Citrix/VDA/bin/xdping -diff**	Para obtener más información, consulte Copia de seguridad y comparación de datos de VDA más adelante en este artículo.
Para comparar dos copias específicas de los datos de copia de seguridad de VDA	**sudo /opt/Citrix/VDA/bin/xdping -diff=<un directorio de datos de copia de seguridad>:<el otro directorio de datos de copia de seguridad>**	Para obtener más información, consulte Copia de seguridad y comparación de datos de VDA más adelante en este artículo.

TAREA	COMANDO XDPING	OBSERVACIONES
Para comprobar el entorno antes de instalar el paquete Linux VDA	**sudo /opt/Citrix/VDA/bin/xdping --preflight**	N/D
Para ejecutar solo categorías de prueba específicas, por ejemplo, las pruebas de tiempo, Kerberos y base de datos	**sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos,database**	N/D
Para sondear un Delivery Controller específico	**sudo /opt/Citrix/VDA/bin/xdping -d <FQDN del Delivery Controller>**	N/D
Para mostrar qué dependencias están instaladas en el VDA	**sudo /opt/Citrix/VDA/bin/xdping --query-pkgs o sudo /opt/Citrix/VDA/bin/xdping -q**	N/D
Para mostrar qué dependencias están instaladas en el VDA y guardar los resultados de la consulta en una ruta específica	**sudo /opt/Citrix/VDA/bin/xdping -f <una ruta específica para guardar los resultados de la consulta>** o **sudo /opt/Citrix/VDA/bin/xdping --query-pkgs-to <una ruta específica para guardar los resultados de la consulta>**	N/D

PRUEBAS INDIVIDUALES

La herramienta **XDPing** de Linux realiza más de 150 pruebas individuales en el sistema, que se clasifican a grandes rasgos de la siguiente manera:

- Comprobar si se cumplen los requisitos del sistema del VDA de Linux.
- Identificar y mostrar información de la máquina, incluidas las distribuciones de Linux.
- Comprobar la compatibilidad del kernel de Linux.
- Comprobar si hay algún problema conocido de la distribución de Linux que pueda afectar al funcionamiento del VDA de Linux.

- Comprobar el modo y la compatibilidad de Security-Enhanced Linux (SELinux).
- Identificar las interfaces de red y comprobar la configuración de red.
- Comprobar el particionamiento del almacenamiento y el espacio en disco disponible.
- Comprobar la configuración del host de la máquina y del nombre de dominio.
- Comprobar la configuración de DNS y realizar pruebas de búsqueda.
- Identificar los hipervisores subyacentes y comprobar la configuración de la máquina virtual. Compatibilidad con:
  - XenServer (anteriormente Citrix Hypervisor™)
  - Microsoft HyperV
  - VMware vSphere
- Comprobar la configuración de la hora y comprobar si la sincronización de la hora de red está operativa.
- Comprobar si el servicio PostgreSQL está configurado correctamente y operativo.
- Comprobar si SQLite está configurado correctamente y operativo.
- Comprobar si el firewall está habilitado y los puertos necesarios están abiertos.
- Comprobar la configuración de Kerberos y realizar pruebas de autenticación.
- Comprobar el entorno de búsqueda LDAP para el motor del servicio de directivas de grupo.
- Comprobar si la integración de Active Directory está configurada correctamente y la máquina actual está unida al dominio. Compatibilidad con:
  - Samba Winbind
  - Servicios de autenticación Dell Quest
  - Centrify DirectControl
  - SSSD
- Comprobar la integridad del objeto de equipo Linux en Active Directory.
- Comprobar la configuración del Módulo de autenticación conectable (PAM).
- Comprobar el patrón de volcado de memoria.
- Comprobar si los paquetes requeridos por el VDA de Linux están instalados.
- Identificar el paquete VDA de Linux y comprobar la integridad de la instalación.
- Comprobar la integridad de la base de datos de registro de PostgreSQL.

- Comprobar si los servicios VDA de Linux están configurados y operativos correctamente.
- Comprobar la integridad de la configuración de VDA y HDX™.
- Sondear cada Delivery Controller™ configurado para comprobar que el servicio Broker es accesible, operativo y responde.
- Comprobar si la máquina está registrada en la granja de Delivery Controller.
- Comprobar el estado de cada sesión HDX activa o desconectada.
- Analizar los archivos de registro en busca de errores y advertencias relacionados con el VDA de Linux.
- Comprobar si la versión de Xorg es adecuada.
- Comprobar si las dependencias necesarias están instaladas.

SALIDA DE EJEMPLO

A continuación, se muestra una salida de ejemplo de la ejecución de la prueba de Kerberos:

```
sudo xdping -T kerberos

Root User ------------------------------------------------------------------
    User:          root
    EUID:          0
      Verify user is root                                              [Pass]

Kerberos -------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                        [Pass]
      Verify Kerberos version 5                                        [Pass]
    KRB5CCNAME:    [Not set]
                   Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                     [Pass]
      Verify KRB5CCNAME format                                         [Pass]
    Configuration file: /etc/krb5.conf [Exists]
```

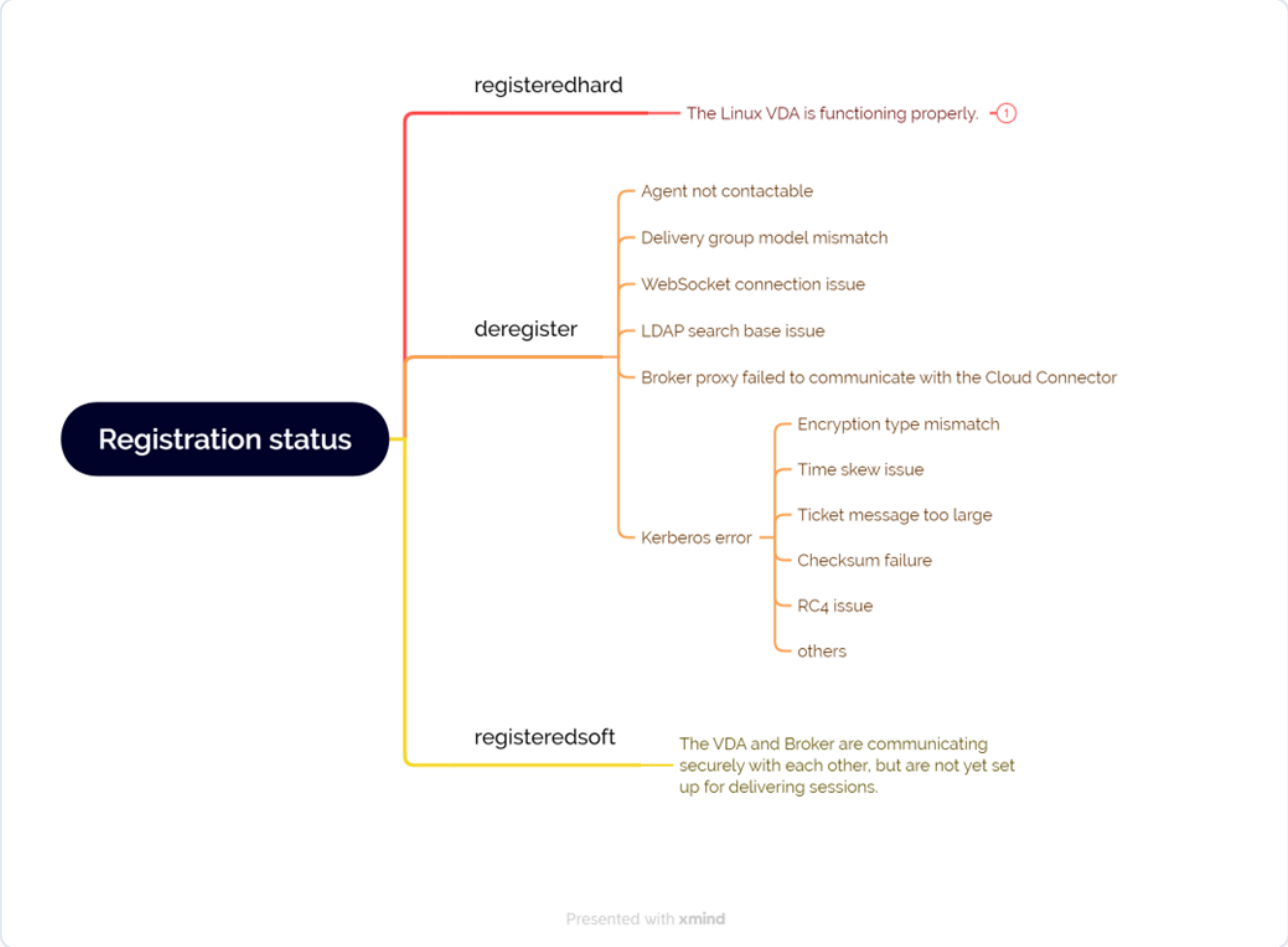
```
  Verify Kerberos configuration file found                    [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                            [Pass]
  Verify default realm set                                    [Pass]
  Verify default realm in upper-case                          [Pass]
  Verify default realm not EXAMPLE.COM                        [Pass]
  Verify default realm domain mappings                        [Pass]
  Verify default realm master KDC configured                  [Pass]
  Verify Kerberos weak crypto disabled                        [Pass]
  Verify Kerberos clock skew setting                          [Pass]
Default ccache: [Not set]
                Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                  [Pass]
  Verify default credential cache format                      [Pass]
UPN system key [MYVDA1$@[redacted]]: [MISSING]
SPN system key [host/[redacted]]: [Exists]
  Verify Kerberos system keys for UPN exist                   [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.
```

```
    Verify Kerberos system keys for SPN exist                 [Pass]
  Kerberos login: [FAILED AUTHENTICATION]
                  Keytab contains no suitable keys for MYVDA1$@[redacted]
                  while getting initial credentials
    Verify KDC authentication                                 [ERROR]
    Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
    from the KDC authentication service for the machine account UPN
    MYVDA1$@[redacted]. Check that the Kerberos configuration is
    valid and the keys in the system keytab are current.


Summary ------------------------------------------------------------------------
  The following tests did not pass:
    Verify Kerberos system keys for UPN exist                 [ERROR]
    Verify KDC authentication                                 [ERROR]
```

ALCANCE DE LAS COMPROBACIONES DEL ESTADO DE REGISTRO DEL VDA

La herramienta **XDPing** de Linux también proporciona un módulo de análisis para ayudarle a comprobar y analizar el estado de registro de su VDA. Para ver el alcance de las comprobaciones del estado de registro, consulte la siguiente captura de pantalla:



COPIA DE SEGURIDAD Y COMPARACIÓN DE DATOS DE VDA

A partir de Linux VDA 2305, la herramienta **XDPing** introduce un módulo de copia de seguridad de VDA. Este módulo le permite hacer una copia de seguridad de los datos clave de un VDA en cualquier momento, como la configuración, la base de datos y los datos de permisos binarios. Puede hacer una copia de seguridad de los datos clave de un VDA cuando se esté ejecutando correctamente. En caso de que el VDA falle más tarde, haga una copia de seguridad de otra copia de los datos y compare las dos copias de datos para facilitar la solución de problemas. La siguiente tabla describe la copia de seguridad y comparación de datos de VDA con los comandos **XDPing** correspondientes:

TAREA	COMANDO XDPING	OBSERVACIONES
Para hacer una copia de seguridad de los datos clave de un VDA	**sudo /opt/Citrix/VDA/bin/xdping -b**	Cada vez que ejecuta el comando de copia de seguridad, se genera y guarda una copia de los datos de copia de seguridad en un directorio bajo **/var/ctxbackup**. Los directorios de datos de copia de

TAREA	COMANDO XDPING	OBSERVACIONES
		seguridad se nombran con la fecha y hora actuales en formato **yyyy-mm-dd-hh_mm_ss**, por ejemplo, **2023-02-27-16_31_27**. De forma predeterminada, el número máximo de directorios de datos de copia de seguridad es 30 y la herramienta **XDPing** rota o elimina los directorios de datos de copia de seguridad antiguos cuando se supera el número. Para personalizar el número de rotación de directorios, ejecute el siguiente comando: `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent\Backup" -t "REG_DWORD" -v "MaxDirRotationCount" -d "0x0000005" --force`
Para comparar las dos últimas copias de los datos de copia de seguridad de VDA	**sudo /opt/Citrix/VDA/bin/xdping -diff**	N/D
Para comparar dos copias específicas de los datos de copia de seguridad de VDA	**sudo /opt/Citrix/VDA/bin/xdping -diff=<un directorio de datos de copia de seguridad>:<el otro directorio de datos de copia de seguridad>**	N/D

Utilidades de consulta de métricas de sesión

ctxsession

Esta utilidad proporciona una experiencia de usuario de Windows. Con esta utilidad, puede acceder a las métricas de sesión como se muestra en la siguiente captura de pantalla:

```
root@u22:~# /opt/Citrix/VDA/bin/ctxsession -v

            Session Id:    4
             Protocols:    TCP-TLS-CGP-ICA
             User Name:    st\wcx
           Client Name:    BLR3-EWS-WPD030
        Client Address:    10.109.143.143:58535
         Local Address:    10.158.180.61:443
        Remote Address:    10.109.143.143:58535
     Security Protocol:    TLSv1.2
       Security Cipher:    ECDHE-RSA-AES256-GCM-SHA384
       Cipher Strength:    256 bits
        ICA Encryption:    Basic
    Rendezvous Version:    None
       Reducer Version:    4

     ICA Statistics:
        ICA RTT: 0 ms
        Sent Bandwidth: 112 bps
        Received Bandwidth: 0 bps
```

ctxqsession, ctxquser, ctxqfull, ctxquery

Para obtener instrucciones sobre cómo usar estas utilidades, ejecute el comando de ayuda, por ejemplo:

```
root@ubuntu2204-33:~# /opt/Citrix/VDA/bin/ctxqsession --help
Usage: ctxqsession [-f short_format_options | -o long_format_options] [-m] [user user_name]
Display information about ICA connections to the local server.

Options:
    -f          Change the displayed information specified by short format options
    -o          Change the displayed information specified by long format options
    -m          Alter the column headers to remove spaces
    user        Display information about the specified user

Short format options:
    d    Client device name (client name)
    i    Session ID
    n    Session name
    p    Published application name
    P    Protocols
    S    Session state
    u    User name
    x    X display number

Long format options(comma separated):
    app      Published application name
    dev      Client device name (client name)
    id       Session ID
    proto    Protocols
    sess     Session name
    state    Session state
    user     User name
    xdpy     X display number
```

Los usuarios solo pueden consultar sus propias métricas de sesión. Solo los usuarios del grupo root y **ctxadm** tienen permiso para consultar las métricas de sesión de otros usuarios.

Utilidad ctxsdcutil

Esta utilidad ayuda a consultar las siguientes métricas de todas las sesiones o de una sesión específica alojada en un VDA. Para ello, ejecute el comando `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]`. El argumento `[-c]` significa consultar las métricas cada segundo.

- **Ancho de banda de entrada de la sesión**
- **Ancho de banda de salida de la sesión**
- **Velocidad de línea de salida de la sesión**
- **Latencia - Última registrada**
- **Tiempo de ida y vuelta**
- **Ancho de banda de salida de ThinWire**
- **Ancho de banda de salida de audio**
- **Ancho de banda de salida de la impresora**
- **Ancho de banda de entrada de la unidad**
- **Ancho de banda de salida de la unidad**

Otros

Esta sección contiene los siguientes temas:

- Compatibilidad con la aplicación Citrix Workspace para HTML5
- Crear un entorno virtual de Python3
- Integrar NIS con Active Directory
- IPv6
- LDAPS
- **Xauthority**

Compatibilidad con la aplicación Citrix Workspace™ para HTML5

Puede usar la aplicación Citrix Workspace para HTML5 para acceder directamente a las aplicaciones y escritorios virtuales Linux sin conectar su cliente a Citrix Gateway. Para obtener información sobre la aplicación Citrix Workspace para HTML5, consulte la documentación de Citrix.

Habilitar esta función

Esta función está inhabilitada de forma predeterminada. Para habilitarla, haga lo siguiente:

1. En Citrix StoreFront™, habilite la aplicación Citrix Workspace para HTML5.

   Para obtener el procedimiento detallado, consulte el Paso 1 del artículo de Knowledge Center CTX208163.

2. Habilite las conexiones WebSocket.

   a. En Citrix Studio, establezca la directiva **Conexiones de WebSockets** en **Permitido**.

      También puede configurar las demás directivas de WebSocket. Para obtener una lista completa de las directivas de WebSocket, consulte Configuración de directivas de WebSockets.

   b. En el VDA, reinicie el servicio `ctxvda` y el servicio `ctxhdx`, en este orden, para que la configuración surta efecto.

   c. En el VDA, ejecute el siguiente comando para comprobar si el agente de escucha de WebSocket se está ejecutando.

      ```
      netstat -an | grep 8008
      ```

Cuando el agente de escucha de WebSocket se está ejecutando, la salida del comando es similar a la siguiente:

```
tcp 0 0 :::8008 :::* LISTEN
```

Nota: También puede habilitar el cifrado TLS para proteger las conexiones WebSocket. Para obtener información sobre cómo habilitar el cifrado TLS, consulte Proteger las sesiones de usuario con TLS.

Crear un entorno virtual de Python3

Si se conecta a la red, la ejecución del comando `sudo /opt/Citrix/VDA/bin/xdping` puede crear un entorno virtual de Python3. Sin embargo, si los comandos no consiguen crear un entorno virtual de Python3, puede crearlo manualmente incluso sin conexión de red. Este artículo detalla los requisitos previos y los pasos para crear un entorno virtual de Python3 sin conexión de red.

Requisitos previos

- Debe tener privilegios administrativos para acceder al directorio `/opt/Citrix/VDA/sbin/ctxpython3`.
- Los archivos wheel de los paquetes `Python3` están en su lugar. Puede descargar los archivos wheel desde `<https://pypi.org/>`.

Crear un entorno virtual de Python3

Siga estos pasos para crear un entorno virtual de Python3:

1. Instale las dependencias de Python3.

   Para RHEL y Rocky Linux:

   ```
   yum -y install python3-devel krb5-devel gcc
   ```

   Nota:

   Es posible que tenga que habilitar un repositorio en particular para instalar algunas dependencias. Para RHEL 7, ejecute el comando `subscription-manager repos --enable rhel-7-server-optional-rpms`. Para RHEL 8, ejecute el comando `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms`.

Para Debian, Ubuntu:

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
libffi-dev
```

Para SUSE:

```
zypper -n install lsb-release python3-devel python3-setuptools krb5-
devel gcc libffi-devel libopenssl-devel
```

2. Crear un entorno virtual de Python3.

Nota:

Para solucionar los errores de conexión SSL que pueda encontrar al usar la herramienta pip, considere agregar los siguientes hosts de confianza al archivo /etc/pip.conf:

\> `[global]`

`trusted-host =`

\> `pypi.org`

`files.pythonhosted.org`

Para Debian, RHEL, Rocky Linux, Ubuntu:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

Para SUSE:

```
sudo ln -s /usr/lib/mit/bin/krb5-config /usr/bin/krb5-config
```

```
export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin



sudo mkdir -p /usr/lib/mit/include/gssapi/



sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/gssapi/
gssapi_ext.h



sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

3. Instale las dependencias de **XDPing**.

   Para Debian 12:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
upgrade pip



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
asn1crypto==1.5.1 cffi==1.17.1 cryptography==43.0.1 decorator==5.1.1
gssapi==1.8.3 ldap3==2.9.1 netifaces==0.11.0 packaging==24.1
pg8000==1.31.2 prettytable==3.11.0 psutil==6.0.0 pyasn1==0.6.1
pyparsing==3.1.4 python-dateutil==2.9.0.post0 scramp==1.4.5 six==1.16.0
termcolor==2.4.0 wcwidth==0.2.13



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

   Para otras distribuciones de Linux:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
upgrade pip
```

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1
gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging==21.3
pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser==2.21
pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor==1.1.0
prettytable==2.5.0



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Integrar NIS con Active Directory

Este artículo describe cómo integrar NIS con Windows Active Directory (AD) en el VDA de Linux mediante SSSD. El VDA de Linux se considera un componente de Citrix Virtual Apps and Desktops. Como resultado, se integra perfectamente en el entorno de AD de Windows.

El uso de NIS en lugar de AD como proveedor de UID y GID requiere que la información de la cuenta (combinaciones de nombre de usuario y contraseña) sea la misma en AD y NIS.

Nota:

La autenticación sigue siendo realizada por el servidor AD. NIS+ no es compatible. Si utiliza NIS como proveedor de UID y GID, los atributos POSIX del servidor de Windows ya no se utilizan.

Sugerencia:

Este método representa una forma obsoleta de implementar el VDA de Linux, que se utiliza solo para casos de uso especiales. Para una distribución RHEL, siga las instrucciones en Instalar el VDA de Linux en RHEL y Rocky Linux manualmente. Para una distribución Ubuntu, siga las instrucciones en Instalar el VDA de Linux en Ubuntu manualmente.

¿Qué es SSSD?

SSSD es un demonio del sistema. Su función principal es proporcionar acceso para identificar y autenticar recursos remotos a través de un marco común que puede proporcionar almacenamiento en caché y soporte sin conexión para el sistema. Proporciona módulos PAM y NSS, y en el futuro puede admitir interfaces basadas en D-BUS para información de usuario extendida. También proporciona una base de datos mejor para almacenar cuentas de usuario locales y datos de usuario extendidos.

Integrar NIS con AD

Para integrar NIS con AD, complete los siguientes pasos:

PASO 1: AÑADIR EL VDA DE LINUX COMO CLIENTE NIS

Configure el cliente NIS:

```
yum –y install ypbind rpcbind oddjob-mkhomedir
```

Establezca el dominio NIS:

```
ypdomainname nis.domain

echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
```

Añada la dirección IP del servidor y cliente NIS en **/etc/hosts**:

```
{NIS server IP address}   server.nis.domain nis.domain
```

Configure NIS mediante **authconfig**:

```
sudo authconfig --enablenis --nisdomain=nis.domain --
nisserver=server.nis.domain --enablemkhomedir --update
```

El **nis.domain** representa el nombre de dominio del servidor NIS. El **server.nis.domain** es el nombre de host del servidor NIS, que también puede ser la dirección IP del servidor NIS.

Configure los servicios NIS:

```
sudo systemctl start rpcbind ypbind
```

```
sudo systemctl enable rpcbind ypbind
```

Asegúrese de que la configuración de NIS sea correcta:

```
ypwhich
```

Valide que la información de la cuenta esté disponible desde el servidor NIS:

```
getent passwd nisaccount
```

> **Nota:**
>
> La **nisaccount** representa la cuenta NIS real en el servidor NIS. Asegúrese de que el UID, GID, el directorio de inicio y el shell de inicio de sesión estén configurados correctamente.

PASO 2: UNIRSE AL DOMINIO Y CREAR UN KEYTAB DE HOST CON SAMBA

SSSD no proporciona funciones de cliente de AD para unirse al dominio y administrar el archivo keytab del sistema. Existen varios métodos para lograr estas funciones, entre ellos:

- `adcli`
- `realmd`
- `Winbind`
- `Samba`

La información de esta sección describe únicamente el enfoque de Samba. Para `realmd`, consulte la documentación del proveedor de RHEL o CentOS. Estos pasos deben seguirse antes de configurar SSSD.

Unirse al dominio y crear un keytab de host con Samba:

En el cliente Linux con los archivos configurados correctamente:

- /etc/krb5.conf
- /etc/samba/smb.conf:

Configure la máquina para la autenticación de Samba y Kerberos:

```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM
--krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
```

Donde **REALM** es el nombre del reino de Kerberos en mayúsculas y **domain** es el nombre NetBIOS del dominio.

Si se requiere la búsqueda basada en DNS del servidor KDC y el nombre del reino, añada las dos opciones siguientes al comando anterior:

`--enablekrb5kdcdns --enablekrb5realmdns`

Abra **/etc/samba/smb.conf** y añada las siguientes entradas en la sección **\[Global\]**, pero después de la sección generada por la herramienta **authconfig**:

`kerberos method = secrets and keytab`

`winbind offline logon = no`

Unirse al dominio de Windows requiere que su controlador de dominio sea accesible y que tenga una cuenta de usuario de AD con permisos para agregar equipos al dominio:

```
sudo net ads join REALM -U user
```

REALM es el nombre del reino Kerberos en mayúsculas y **user** es un usuario de dominio que tiene permisos para agregar equipos al dominio.

PASO 3: CONFIGURAR SSSD

> **Nota**

> El uso de SSSD con el demonio de caché del servicio de nombres (NSCD) puede provocar un comportamiento inesperado. Para obtener más información, consulte Uso de NSCD con SSSD.

> La configuración de SSSD consta de los siguientes pasos:

- Instale los paquetes **sssd-ad** y **sssd-proxy** en la máquina cliente Linux.
- Realice cambios de configuración en varios archivos (por ejemplo, **sssd.conf**).
- Inicie el **servicio sssd**.

/etc/sssd/sssd.conf

Un ejemplo de configuración de **sssd.conf** (se pueden añadir más opciones según sea necesario):

```
[sssd]

config_file_version = 2

domains = EXAMPLE

services = nss, pam



[domain/EXAMPLE]

# Uncomment if you need offline logins

# cache_credentials = true

re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?
P<domain>.+$))|(^(?P<name>[^@\\]+)$))

id_provider = proxy

proxy_lib_name = nis

auth_provider = ad

access_provider = ad



# Should be specified as the long version of the Active Directory domain.

ad_domain = EXAMPLE.COM



# Kerberos settings

krb5_ccachedir = /tmp
```

```
krb5_ccname_template = FILE:%d/krb5cc_%U



# Uncomment if service discovery is not working

# ad_server = server.ad.example.com



# Comment out if the users have the shell and home dir set on the AD side

default_shell = /bin/bash

fallback_homedir = /home/%d/%u



# Uncomment and adjust if the default principal SHORTNAME$@REALM is not
available

# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

Sustituya **ad.domain.com**, **server.ad.example.com** por el valor correspondiente. Para obtener más detalles, consulte la página man de Linux de **sssd-ad**(5).

Establezca la propiedad y los permisos del archivo en **sssd.conf**:

`chown root:root /etc/sssd/sssd.conf`

`chmod 0600 /etc/sssd/sssd.conf` `restorecon /etc/sssd/sssd.conf`

PASO 4: CONFIGURAR NSS/PAM

RHEL/CentOS:

Utilice **authconfig** para habilitar SSSD. Instale **oddjob-mkhomedir** para asegurarse de que la creación del directorio de inicio sea compatible con SELinux:

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
```

```
sudo systemctl start sssd
```

```
sudo systemctl enable sssd
```

Sugerencia:

Al configurar los ajustes de Linux VDA, tenga en cuenta que para SSSD no hay ajustes especiales para el cliente de Linux VDA. Para soluciones adicionales en el script **ctxsetup.sh**, utilice el valor predeterminado.

PASO 5: VERIFICAR LA CONFIGURACIÓN DE KERBEROS

Para asegurarse de que Kerberos está configurado correctamente para su uso con Linux VDA, compruebe que el archivo **keytab** del sistema se ha creado y contiene claves válidas:

```
sudo klist -ke
```

Este comando muestra la lista de claves disponibles para las distintas combinaciones de nombres de entidad de seguridad y conjuntos de cifrado. Ejecute el comando Kerberos **kinit** para autenticar la máquina con el controlador de dominio utilizando estas claves:

```
sudo kinit –k MACHINE\$@REALM
```

Los nombres de la máquina y del reino deben especificarse en mayúsculas. El signo de dólar ($) debe escaparse con una barra invertida (\\) para evitar la sustitución de shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre de reino Kerberos. Asegúrese de que se utiliza el nombre de reino. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT para la cuenta de máquina se ha almacenado en caché mediante:

```
sudo klist -ke
```

PASO 6: VERIFICAR LA AUTENTICACIÓN DE USUARIO

Utilice el comando **getent** para verificar que el formato de inicio de sesión es compatible y si el NSS funciona:

```
sudo getent passwd DOMAIN\\username
```

El parámetro **DOMAIN** indica el nombre de dominio de versión corta. Si se necesita otro formato de inicio de sesión, verificar primero con el comando **getent**.

Los formatos de inicio de sesión admitidos son:

- Nombre de inicio de sesión de nivel inferior: `DOMAIN\username`
- UPN: `username@domain.com`
- Formato de sufijo NetBIOS: `username@DOMAIN`

Para verificar que el módulo PAM de SSSD está configurado correctamente, utilice una cuenta de usuario de dominio para iniciar sesión en el Linux VDA. La cuenta de usuario de dominio no se ha utilizado antes.

```
sudo ssh localhost –l DOMAIN\\username



id -u
```

Compruebe que se ha creado un archivo de caché de credenciales de Kerberos correspondiente para el **uid** devuelto por el comando:

```
ls /tmp/krb5cc_{uid}
```

Compruebe que los tickets en la caché de credenciales Kerberos del usuario son válidos y no han caducado:

```
klist
```

IPv6

El VDA de Linux es compatible con IPv6 para alinearse con Citrix Virtual Apps and Desktops. Al usar esta función, tenga en cuenta lo siguiente:

- En entornos de pila dual, se utiliza IPv4 a menos que IPv6 esté habilitado explícitamente.
- Si IPv6 está habilitado en un entorno IPv4, el VDA de Linux no funciona.

> **Importante:**
>
> - Todo el entorno de red debe ser IPv6, no solo para el VDA de Linux.
> - Centrify no es compatible con IPv6 puro.

> No se requieren tareas de configuración especiales para IPv6 al instalar el VDA de Linux.

Configurar IPv6 para el VDA de Linux

Antes de cambiar la configuración del VDA de Linux, asegúrese de que su máquina virtual Linux haya funcionado previamente en una red IPv6. Hay dos claves de registro relacionadas con la configuración de IPv6:

```
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"OnlyUseIPv6ControllerRegistration"

"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"ControllerRegistrationIPv6Netmask"
```

OnlyUseIPv6ControllerRegistration debe establecerse en 1 para habilitar IPv6 en el VDA de Linux:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
```

Si el VDA de Linux tiene más de una interfaz de red, se puede usar **ControllerRegistrationIPv6Netmask** para especificar cuál se utiliza para el registro del VDA de Linux:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ControllerRegistrationIPv6Netmask " -d "{IPv6 netmask}" --force
```

Sustituya **{IPv6 netmask}** por la máscara de red real (por ejemplo, 2000::/64).

Para obtener más información sobre la implementación de IPv6 en Citrix Virtual Apps and Desktops, consulte Compatibilidad con IPv4/IPv6.

Solución de problemas

Compruebe el entorno de red IPv6 básico y use ping6 para verificar si AD y Delivery Controller™ son accesibles.

LDAPS

LDAPS es la versión segura del Protocolo ligero de acceso a directorios (LDAP), donde las comunicaciones LDAP se cifran mediante TLS/SSL.

De forma predeterminada, las comunicaciones LDAP entre las aplicaciones cliente y servidor no están cifradas. LDAPS le permite proteger el contenido de las consultas LDAP entre el VDA de Linux y los servidores LDAP.

Los siguientes componentes del VDA de Linux tienen dependencias de LDAPS:

- Agente de broker: Registro del VDA de Linux con un Delivery Controller™
- Servicio de directivas: Evaluación de directivas

La configuración de LDAPS implica:

- Habilitar LDAPS en el servidor de Active Directory (AD)/LDAP
- Exportar la CA raíz para uso del cliente
- Habilitar/inhabilitar LDAPS en el VDA de Linux
- Configurar LDAPS para plataformas de terceros
- Configurar SSSD
- Configurar Winbind
- Configurar Centrify
- Configurar Quest

> **Nota:**

Puede ejecutar el siguiente comando para establecer un ciclo de supervisión para sus servidores LDAP. El valor predeterminado es de 15 minutos. Establézcalo en 10 minutos como mínimo.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"ListOfLDAPServersMonitorPeroid" -t "REG_DWORD" -d "0x0000000f" --
force
```

Habilitar LDAPS en el servidor AD/LDAP

Puede habilitar LDAP a través de SSL (LDAPS) instalando un certificado con el formato adecuado de una entidad de certificación (CA) de Microsoft o de una CA que no sea de Microsoft.

Sugerencia:

LDAPS se habilita automáticamente al instalar una CA raíz empresarial en un controlador de dominio.

Para obtener más información sobre cómo instalar el certificado y verificar la conexión LDAPS, consulte Cómo habilitar LDAP a través de SSL con una entidad de certificación de terceros.

Cuando tiene una jerarquía de entidad de certificación de varios niveles, no tiene automáticamente el certificado adecuado para la autenticación LDAPS en el controlador de dominio.

Para obtener información sobre cómo habilitar LDAPS para controladores de dominio mediante una jerarquía de entidad de certificación de varios niveles, consulte el artículo Certificado LDAP a través de SSL (LDAPS).

Habilitar la entidad de certificación raíz para uso del cliente

El cliente debe usar un certificado de una CA en la que confíe el servidor LDAP. Para habilitar la autenticación LDAPS para el cliente, importe el certificado de CA raíz a un almacén de claves de confianza.

Para obtener más información sobre cómo exportar la CA raíz, consulte Cómo exportar el certificado de la entidad de certificación raíz en el sitio web de soporte técnico de Microsoft.

Habilitar o deshabilitar LDAPS en el VDA de Linux

Para habilitar o deshabilitar LDAPS en el VDA de Linux, ejecute el script **enable_ldaps.sh** (mientras haya iniciado sesión como administrador). Para ejecutar el script **enable_ldaps.sh** en modo no interactivo, exporte las siguientes variables a su entorno:

```
#CTX_LDAPS_KEYSTORE_PASSWORD=



#CTX_LDAPS_LDAP_SERVERS=
```

- Para habilitar LDAP a través de SSL/TLS con el certificado de CA raíz proporcionado (se admite la vinculación de canal LDAP):

  ```
  /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
  ```

- Para volver a LDAP sin SSL/TLS

  ```
  /opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
  ```

El almacén de claves de Java dedicado a LDAPS reside en **/etc/xdl/.keystore**. Las claves de registro afectadas incluyen:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers



HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy



HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS



HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
```

```
HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
```

Configurar LDAPS para plataformas de terceros

Además de los componentes de Linux VDA, varios componentes de software de terceros que se adhieren al VDA también pueden requerir LDAP seguro, como SSSD, Winbind, Centrify y Quest. Las siguientes secciones describen cómo configurar LDAP seguro con LDAPS, STARTTLS o SASL sign and seal.

> **Sugerencia:**
>
> No todos estos componentes de software prefieren usar el puerto SSL 636 para garantizar un LDAP seguro. Y la mayoría de las veces, LDAPS (LDAP sobre SSL en el puerto 636) no puede coexistir con STARTTLS en el puerto 389.

SSSD

Configure el tráfico LDAP seguro de SSSD en el puerto 636 o en el puerto 389 según las opciones. Para obtener más información, consulte la página man de SSSD LDAP para Linux.

Winbind

La consulta LDAP de Winbind utiliza el método ADS. Winbind solo admite el método StartTLS en el puerto 389. Los archivos de configuración afectados son **/etc/samba/smb.conf** y **/etc/openldap/ldap.conf** (para Amazon Linux 2, RHEL, Rocky Linux, CentOS y SUSE) o **/etc/ldap/ldap.conf** (para Debian y Ubuntu). Cambie los archivos de la siguiente manera:

- smb.conf

  `ldap ssl = start tls`

  `ldap ssl ads = yes` `client ldap sasl wrapping = plain`

- ldap.conf

  `TLS_REQCERT never`

Alternativamente, puede configurar LDAP seguro mediante SASL GSSAPI sign and seal, pero no puede coexistir con TLS/SSL. Para usar el cifrado SASL, cambie la configuración de **smb.conf**:

`ldap ssl = off`

`ldap ssl ads = no` `client ldap sasl wrapping = seal`

Centrify

Centrify no admite LDAPS en el puerto 636. Sin embargo, proporciona cifrado seguro en el puerto 389. Para obtener más información, consulte el sitio de Centrify.

Quest

Quest Authentication Service no admite LDAPS en el puerto 636, pero proporciona cifrado seguro en el puerto 389 utilizando un método diferente.

Solución de problemas

Los siguientes problemas pueden surgir al usar esta función:

- **Disponibilidad del servicio LDAPS**

  verificar que la conexión LDAPS esté disponible en el servidor AD/LDAP. El puerto es el 636 de forma predeterminada.

- **Error en el registro de Linux VDA cuando LDAPS está habilitado**

  verificar que el servidor LDAP y los puertos estén configurados correctamente. Compruebe primero el certificado de CA raíz y asegúrese de que coincida con el servidor AD/LDAP.

- **Cambio de registro incorrecto por accidente**

  Si actualizó las claves relacionadas con LDAPS por accidente sin usar **enable_ldaps.sh**, podría romper la dependencia de los componentes de LDAPS.

- **El tráfico LDAP no está cifrado mediante SSL/TLS desde Wireshark o cualquier otra herramienta de supervisión de red**

  De forma predeterminada, LDAPS está inhabilitado. Ejecute **/opt/Citrix/VDA/sbin/enable_ldaps.sh** para forzarlo.

- **No hay tráfico LDAPS desde Wireshark ni ninguna otra herramienta de supervisión de red**

  El tráfico LDAP/LDAPS se produce cuando se registran los VDA de Linux y se evalúan las directivas de grupo.

- **Error al verificar la disponibilidad de LDAPS ejecutando ldp connect en el servidor AD**

  Utilice el FQDN de AD en lugar de la dirección IP.

- **Error al importar el certificado de CA raíz ejecutando el script /opt/Citrix/VDA/sbin/enable_ldaps.sh**

  Proporcione la ruta completa del certificado de CA y verificar que el certificado de CA raíz sea del tipo correcto. Se supone que es compatible con la mayoría de los tipos de Java Keytool admitidos. Si no aparece en la lista de compatibilidad, puede convertir el tipo primero. Recomendamos el formato PEM codificado en base64 si encuentra un problema de formato de certificado.

- **Error al mostrar el certificado de CA raíz con Keytool -list**

  Cuando habilita LDAPS ejecutando `/opt/Citrix/VDA/sbin/enable_ldaps.sh`, el certificado se importa a /etc/xdl/.keystore, y se establece la contraseña para proteger el almacén de claves. Si olvida la contraseña, puede volver a ejecutar el script para crear un almacén de claves.

Xauthority

El VDA de Linux es compatible con entornos que utilizan la funcionalidad de visualización X11 (incluidos `xterm` y `gvim`) para la comunicación remota interactiva. Esta función proporciona un mecanismo de seguridad necesario para garantizar una comunicación segura entre XClient y XServer.

Existen dos métodos para asegurar el permiso para esta comunicación segura:

- **Xhost**. De forma predeterminada, Xhost solo permite que el XClient de localhost se comunique con XServer. Si elige permitir que un XClient remoto acceda a XServer, debe ejecutar el comando Xhost para conceder permiso en la máquina específica. O bien, puede usar alternativamente **xhost +** para permitir que cualquier XClient se conecte a XServer.
- **Xauthority**. El archivo `.Xauthority` se encuentra en el directorio principal de cada usuario. Se utiliza para almacenar credenciales en cookies que usa xauth para la autenticación de XServer. Cuando se inicia una instancia de XServer (Xorg), la cookie se utiliza para autenticar las conexiones a esa pantalla específica.

Cómo funciona

Cuando se inicia Xorg, se pasa un archivo `.Xauthority` a Xorg. Este archivo `.Xauthority` contiene los siguientes elementos:

- Número de pantalla
- Protocolo de solicitud remota
- Número de cookie

Puede examinar este archivo mediante el comando `xauth`. Por ejemplo:

```
# xauth -f ~/.Xauthority



# > list



# > us01msip06:107  MIT-MAGIC-COOKIE-1  fb228d1b695729242616c5908f11624b
```

Si **XClient** se conecta a Xorg de forma remota, se deben cumplir dos requisitos previos:

- Establezca la variable de entorno **DISPLAY** en el XServer remoto.
- Obtenga el archivo `.Xauthority` que contiene uno de los números de cookie en Xorg.

Configurar Xauthority

Para habilitar **Xauthority** en el VDA de Linux para la visualización remota de X11, debe crear las dos claves de registro siguientes:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"XauthEnabled" -d "0x00000001" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"ListenTCP" -d "0x00000001" --force
```

Después de habilitar **Xauthority**, pase el archivo `.Xauthority` al **XClient** manualmente o montando un directorio de inicio compartido:

- Pase el archivo `.Xauthority` al XClient manualmente

  Después de iniciar una sesión ICA®, el VDA de Linux genera el archivo `.Xauthority` para el XClient y lo almacena en el directorio de inicio del usuario que ha iniciado sesión. Puede copiar este archivo `.Xauthority` a la máquina XClient remota y establecer las variables de entorno **DISPLAY** y **XAUTHORITY**. `DISPLAY` es el número de pantalla almacenado en el

archivo `.Xauthority` y `XAUTHORITY` es la ruta del archivo de **Xauthority**. Para ver un ejemplo, consulte el siguiente comando:

```
export DISPLAY={Display number stored in the Xauthority file}



export XAUTHORITY={the file path of .Xauthority}
```

> **Nota:**
>
> Si la variable de entorno **XAUTHORITY** no está establecida, se utiliza el archivo `~/.Xauthority` de forma predeterminada.

- Pase el archivo `.Xauthority` al XClient montando un directorio de inicio compartido

  La forma más cómoda es montar un directorio de inicio compartido para el usuario que ha iniciado sesión. Cuando el VDA de Linux inicia una sesión ICA, el archivo `.Xauthority` se crea en el directorio de inicio del usuario que ha iniciado sesión. Si este directorio de inicio se comparte con el XClient, el usuario no necesita transmitir este archivo `.Xauthority` al XClient manualmente. Una vez que las variables de entorno **DISPLAY** y **XAUTHORITY** se configuran correctamente, la GUI se muestra automáticamente en el escritorio del XServer.

Solución de problemas

Si **Xauthority** no funciona, siga los pasos de solución de problemas:

1. Como administrador con privilegios de root, recupere todas las cookies de Xorg:

   ```
   ps aux | grep -i xorg
   ```

   Este comando muestra el proceso de Xorg y los parámetros pasados a Xorg durante el inicio. Otro parámetro muestra qué archivo `.Xauthority` se utiliza. Por ejemplo:

   ```
   /var/xdl/xauth/.Xauthority110
   ```

   Muestre las cookies mediante el comando **Xauth**:

```
Xauth -f /var/xdl/xauth/.Xauthority110
```

2. Utilice el comando `Xauth` para mostrar las cookies contenidas en `~/.Xauthority`. Para el mismo número de pantalla, las cookies mostradas deben ser las mismas en los archivos `.Xauthority` de Xorg y XClient.
3. Si las cookies son las mismas, compruebe la accesibilidad del puerto de pantalla remoto utilizando la dirección IP del VDA de Linux y el número de pantalla del escritorio publicado.

   Por ejemplo, ejecute el siguiente comando en la máquina XClient:

   ```
   telnet 10.158.11.11 6160
   ```

   El número de puerto es la suma de 6000 + \<número de pantalla\>.

   Si esta operación de telnet falla, es posible que el firewall esté bloqueando la solicitud.

Audio

- Herramienta de diagnóstico de audio

Herramienta de línea de comandos de diagnóstico de audio

La herramienta de línea de comandos de diagnóstico de audio en el VDA se puede utilizar para consultar datos de sesión relacionados con las directivas de audio, la configuración y el transporte de datos.

Uso

1. Abra un símbolo del sistema y ejecute `ctxaudiosession` desde la carpeta `/opt/Citrix/VDA/bin`.
   - La ejecución de la herramienta mostrará toda la información de audio de las sesiones ICA activas y el estado de redirección de los dispositivos para el usuario actual.

Salida

La herramienta muestra varias configuraciones que pueden ayudar a diagnosticar problemas relacionados con el audio dentro de una sesión.

SECCIÓN	DESCRIPCIÓN
Información de la directiva DDC	Directivas de audio aplicadas a la sesión o sesiones actuales.
Información del Registro local	Configuración relacionada con el audio almacenada en el registro.
Información de estado	Estado del audio, versión, códecs, transporte aplicados a la sesión o sesiones actuales y números de dispositivo.
Información de dispositivos	Nombres de dispositivos, sus funciones y sus estados utilizados en la sesión.

Autenticación

Esta sección contiene los siguientes temas:

- Autenticación con Azure Active Directory
- Autenticación de inicio de sesión único de doble salto
- Servicio de autenticación federada
- Autenticación sin SSO
- Tarjetas inteligentes
- Acceso de usuarios no autenticados (anónimos)

Autenticación con Azure Active Directory

> **Nota:**
>
> Esta función solo está disponible para los VDA alojados en Azure.
>
> Según sus necesidades, puede implementar dos tipos de VDA de Linux en Azure:

- Máquinas virtuales unidas a Azure AD DS. Las máquinas virtuales están unidas a un dominio administrado de Azure Active Directory (AAD) Domain Services (DS). Los usuarios utilizan sus credenciales de dominio para iniciar sesión en las máquinas virtuales.

- Máquinas virtuales no unidas a un dominio. Las máquinas virtuales se integran con el servicio de identidad de AAD para proporcionar autenticación de usuario. Los usuarios utilizan sus credenciales de AAD para iniciar sesión en las máquinas virtuales.

Para obtener más información sobre AAD DS y AAD, consulte este artículo de Microsoft.

Este artículo le muestra cómo habilitar y configurar el servicio de identidad de AAD en VDA no unidos a un dominio.

Distribuciones compatibles

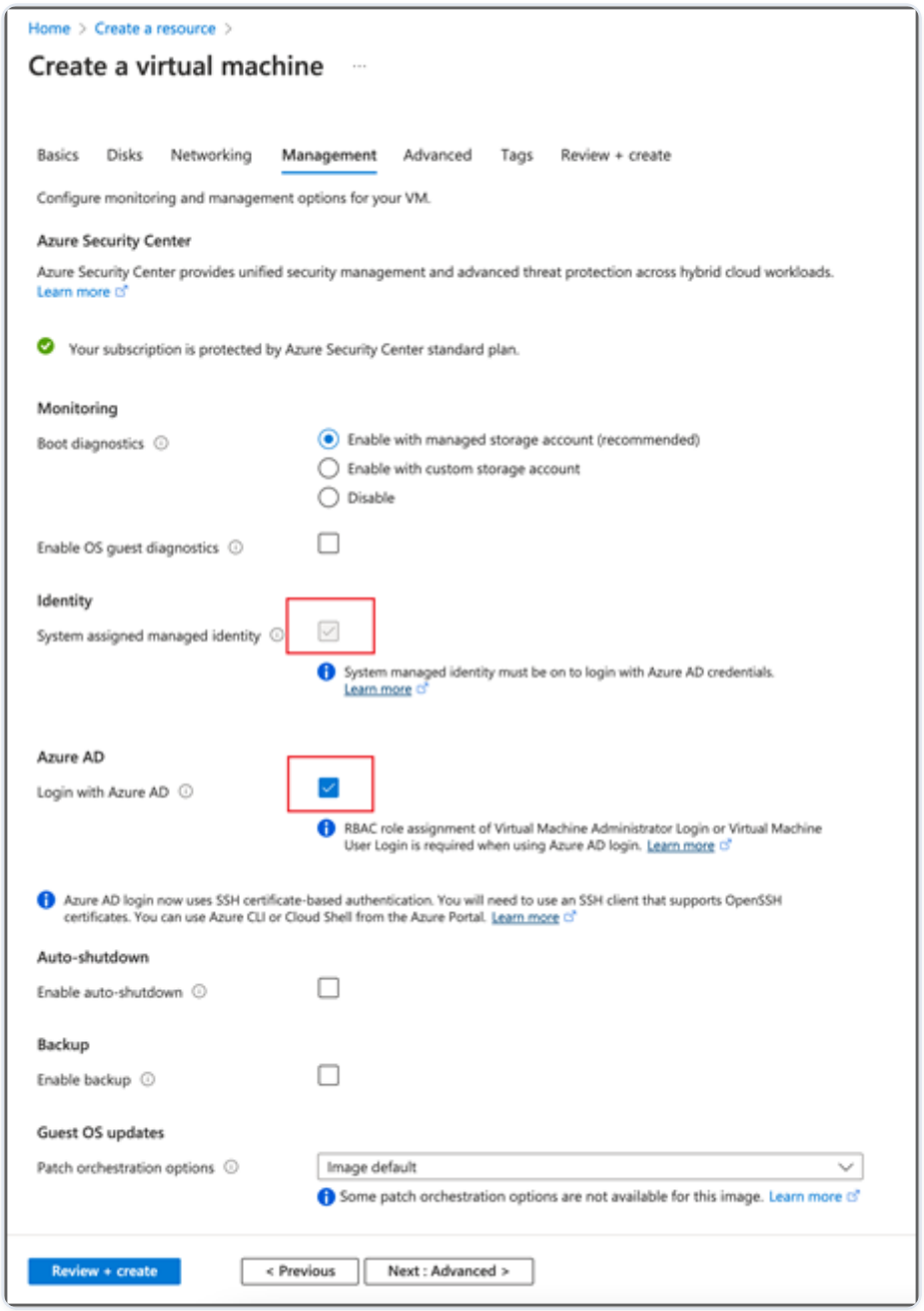
- Ubuntu 24.04, 22.04
- RHEL 8.10
- SUSE 15.6

Para obtener más información, consulte este artículo de Microsoft.

Paso 1: Crear una máquina virtual de plantilla en el portal de Azure

Cree una máquina virtual de plantilla e instale la CLI de Azure en la máquina virtual.

1. En el portal de Azure, cree una máquina virtual de plantilla. Asegúrese de seleccionar **Iniciar sesión con Azure AD** en la ficha **Administración** antes de hacer clic en **Revisar y crear**.



2. Instale la CLI de Azure en la VM de plantilla. Para obtener más información, consulte este artículo de Microsoft.

Paso 2: Preparar una imagen maestra en la VM de plantilla

Para preparar una imagen maestra, siga el **Paso 3: Preparar una imagen maestra** en Usar MCS para crear VM Linux en Azure.

Paso 3: Configurar la VM de plantilla en modo sin unión a dominio

Después de crear una imagen maestra, siga estos pasos para configurar la VM en modo sin unión a dominio:

1. Ejecute el siguiente script desde el símbolo del sistema.

```
Modify /var/xdl/mcs/mcs_util.sh
```

2. Busque `function read_non_domain_joined_info()` y, a continuación, cambie el valor de `NonDomainJoined` a `2`. Consulte el siguiente bloque de código para ver un ejemplo.

```
function read_non_domain_joined_info()

{

log "Debug: Enter read_non_domain_joined_info"

# check if websocket enabled

TrustIdentity=`cat ${id_disk_mnt_point}${ad_info_file_path} | grep '\
[TrustIdentity\]' | sed 's/\s//g'`

if [ "$TrustIdentity" == "[TrustIdentity]" ]; then

NonDomainJoined=2

fi

...

}
```

3. Guarde el cambio.
4. Apague la VM de plantilla.

Paso 4: Crear las VM Linux a partir de la VM de plantilla

Una vez que tenga lista la VM de plantilla sin unión a dominio, siga estos pasos para crear VM:

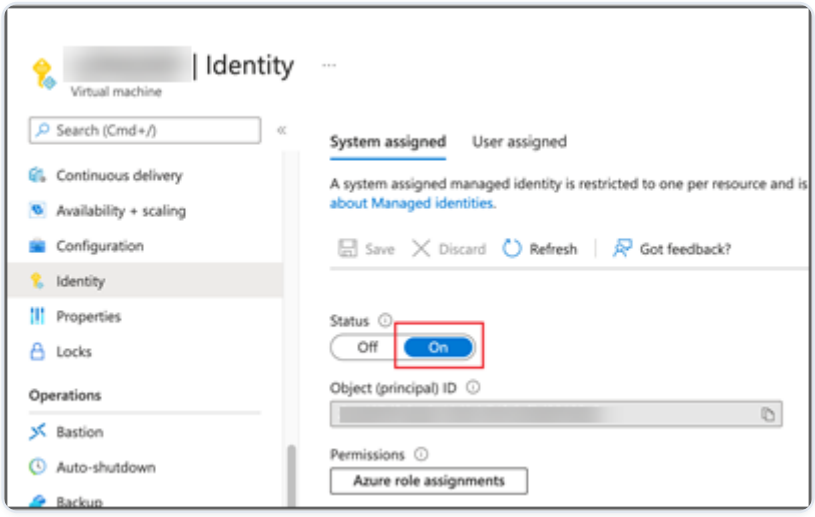
1. Inicie sesión en Citrix Cloud.
2. Haga doble clic en Citrix DaaS™ y, a continuación, acceda a la consola de administración de Configuración completa.
3. En **Catálogos de máquinas**, elija usar Machine Creation Services para crear las VM Linux a partir de la VM de plantilla. Para obtener más información, consulte el artículo de Citrix DaaS Sin unión a dominio.

Paso 5: Asignar cuentas de usuario de AAD a las VM Linux

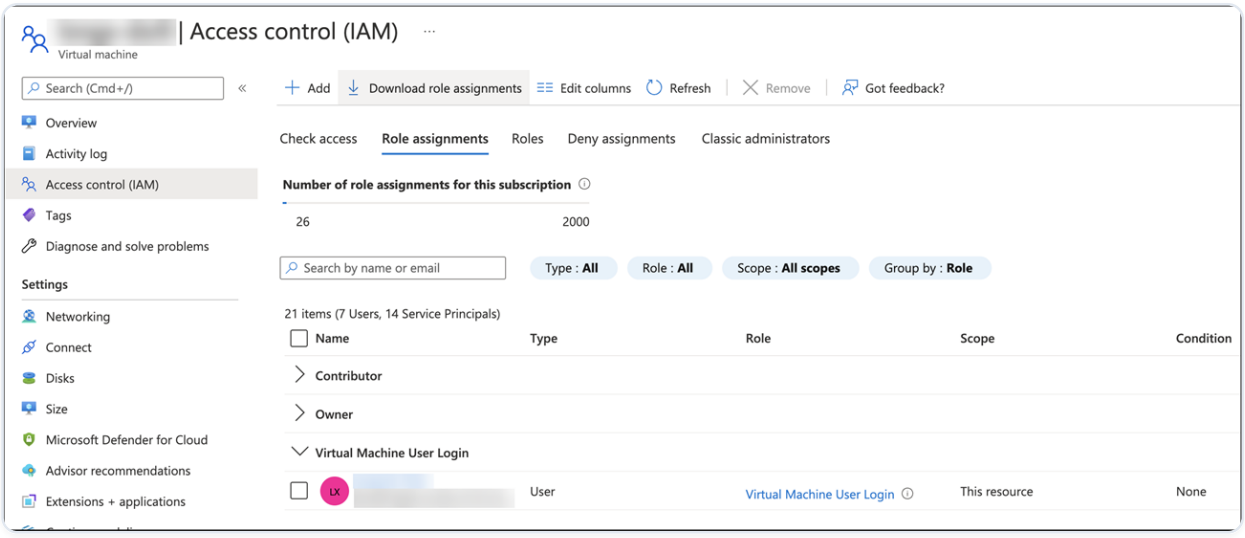
Después de crear las VM sin unión a dominio, asígneles cuentas de usuario de AAD.

Para asignar cuentas de usuario de AAD a una máquina virtual, siga estos pasos:

1. Acceda a la máquina virtual con una cuenta de administrador.
2. En la ficha **Identificar > Asignado por el sistema**, habilite **Identidad del sistema**.



3. En la ficha **Control de acceso (IAM) > Asignaciones de roles**, busque el área **Inicio de sesión de usuario de máquina virtual** y, a continuación, agregue las cuentas de usuario de AAD según sea necesario.



Iniciar sesión en VDA no unidos a un dominio

Los usuarios finales de su organización pueden iniciar sesión en un VDA no unido a un dominio de dos maneras. Los pasos detallados son los siguientes:

1. Inicie la aplicación Workspace y, a continuación, inicie sesión en el espacio de trabajo introduciendo el nombre de usuario y la contraseña de AAD. Aparecerá la página de Workspace.
2. Haga doble clic en un escritorio no unido a un dominio. Aparecerá la página de INICIO DE SESIÓN de AAD.

   La página varía en función del modo de inicio de sesión configurado en el VDA: Código de dispositivo o cuenta/contraseña de AAD. De forma predeterminada, los VDA de Linux autentican a los usuarios de AAD mediante el modo de inicio de sesión de Código de dispositivo de la siguiente manera. Como administrador, puede cambiar el modo de inicio de sesión a cuenta/contraseña de AAD si es necesario. Consulte la siguiente sección para obtener los pasos detallados.

3. Según las instrucciones en pantalla, inicie sesión en la sesión de escritorio de una de las siguientes maneras:

   - Escanee el código QR e introduzca el código.
   - Introduzca el nombre de usuario y la contraseña de AAD.

Cambiar a modo de inicio de sesión con cuenta/contraseña de AAD

De forma predeterminada, los VDA de Linux autentican a los usuarios de AAD con códigos de dispositivo. Consulte este artículo de Microsoft para obtener más información. Para cambiar el modo de inicio de sesión a *cuenta/contraseña de AAD*, siga estos pasos:

Ejecute el siguiente comando en el VDA, busque la clave `AADAcctPwdAuthEnable` y cambie su valor a `0x00000001`.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket" -t
"REG_DWORD" -v "AADAcctPwdAuthEnable" -d "0x00000001" --force
```

Nota:

> Este enfoque no funciona con cuentas de Microsoft o cuentas que tienen la autenticación de dos factores habilitada.

Autenticación de inicio de sesión único de doble salto

Las credenciales de usuario para acceder a un almacén de StoreFront se pueden inyectar en el módulo AuthManager de la aplicación Citrix Workspace para Linux y Citrix Receiver para Linux 13.10. Después de la inyección, puede usar el cliente para acceder a escritorios y aplicaciones virtuales desde una sesión de escritorio virtual de Linux, sin introducir las credenciales de usuario por segunda vez.

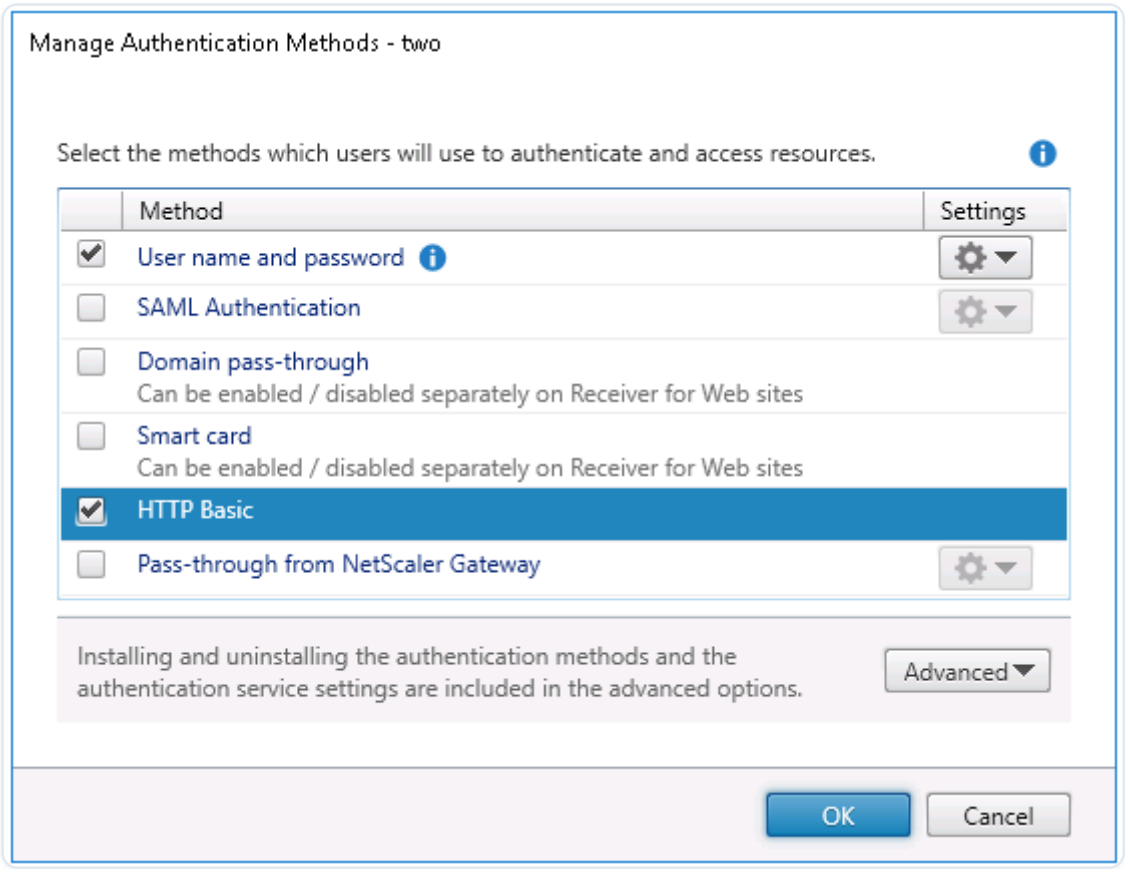
> **Nota:**
>
> Esta función es compatible con la aplicación Citrix Workspace para Linux y Citrix Receiver para Linux 13.10.

> Para habilitar la función:

1. En el VDA de Linux, instale la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10.

   Descargue la aplicación desde la página de descargas de Citrix para la aplicación Citrix Workspace o para Citrix Receiver.

   La ruta de instalación predeterminada es /opt/Citrix/ICAClient/. Si instala la aplicación en una ruta diferente, establezca la variable de entorno ICAROOT para que apunte a la ruta de instalación real.
2. En la consola de administración de Citrix StoreFront™, agregue el método de autenticación **HTTP Basic** para el almacén de destino.



3. Agregue la siguiente clave al archivo de configuración de AuthManager ($ICAROOT/config/AuthManConfig.xml) para permitir la autenticación básica HTTP:

```
<Protocols>

     <HTTPBasic>

         <Enabled>True</Enabled>

    </HTTPBasic>

</Protocols>
```

4. Ejecute los siguientes comandos para instalar el certificado raíz en el directorio especificado.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/

$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
```

5. Ejecute el siguiente comando para habilitar la función:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d
"0x00000001"
```

6. Inicie una sesión de escritorio virtual de Linux e inicie la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10 dentro de esa sesión.

   Se le pedirá una cuenta de almacén la primera vez que inicie la aplicación Citrix Workspace™. Más adelante, iniciará sesión automáticamente en el almacén que especificó anteriormente.

   Nota:

   Introduzca una URL HTTPS como cuenta de almacén.

   Introduciendo su cuenta de tienda(/en-us/linux-virtual-delivery-agent/2507-ltsr/media/store-account.png)

Servicio de autenticación federada

Puede usar el Servicio de autenticación federada (FAS) para autenticar a los usuarios que inician sesión en un VDA de Linux. El VDA de Linux utiliza el mismo entorno de Windows que el VDA de Windows para la función de inicio de sesión de FAS. Para obtener información sobre cómo configurar el entorno de Windows para FAS, consulte Servicio de autenticación federada. Este artículo proporciona información adicional específica para el VDA de Linux.

Nota:

- El VDA de Linux no admite la política de **comportamiento en la sesión**.
- El VDA de Linux utiliza conexiones cortas para transmitir datos con los servidores FAS.

Distribuciones compatibles

FAS admite distribuciones de Linux y métodos de unión a dominios limitados. Consulte la siguiente matriz:

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
Debian 12.15/11.11	Sí	Sí	Sí	Sí	Sí
RHEL 9.8/9.6/9.4	Sí	Sí	Sí	No	Sí
RHEL 8.10	Sí	Sí	Sí	Sí	Sí
Rocky Linux 9.8/9.6/9.4	Sí	Sí	Sí	No	Sí
Rocky Linux 8.10	Sí	Sí	Sí	No	Sí
SUSE 15.6	Sí	Sí	Sí	No	Sí
Ubuntu 24.04	Sí	Sí	Sí	No	Sí
Ubuntu 22.04	Sí	Sí	Sí	Sí	Sí

Nota:

1. Si el método de unión al dominio es Quest, es posible que krb5.conf no exista. En tal escenario, instale ‘krb5-pkinit’ y ‘libpam-krb5’ manualmente primero (lo que solicitará información de Kerberos y la escribirá en krb5.conf), luego ejecute el script fas ‘/opt/Citrix/VDA/sbin/ctxfascfg.sh’
2. Para rhel9 y rocky9, los clientes deben habilitar la política criptográfica ‘AD-SUPPORT’ (SHA1 también puede ser necesario si lo utiliza AD durante la autenticación Kerberos). Comando a continuación:

   ```
   update-crypto-policies --set DEFAULT:AD-SUPPORT
   ```

   ```
   update-crypto-policies --set DEFAULT:AD-SUPPORT:SHA1
   ```
3. Para Debian 11, los usuarios pueden necesitar configurar el método de resumen a 'SHA256' manualmente. Comando a continuación: /opt/Citrix/VDA/bin/ctxreg create -k

```
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialService" -t
"REG_SZ" -v "DigestMethod" -d "SHA256" --force
```

Configurar FAS en el VDA de Linux

Instalar certificados

Para la verificación de los certificados de los usuarios, instale el certificado de CA raíz y todos los certificados intermedios en el VDA. Por ejemplo, para instalar el certificado de CA raíz, obtenga el certificado raíz de AD del paso anterior de **Recuperar el certificado de CA de la CA de Microsoft (en AD)**, o descárguelo del servidor de CA raíz `http://CA-SERVER/certsrv`.

Nota:

Los siguientes comandos también se aplican a la configuración de un certificado intermedio.

Por ejemplo, para convertir un archivo DER (.crt, .cer, .der) a PEM, ejecute un comando similar al siguiente:

```
sudo openssl x509 -inform der -in root.cer -out root.pem
```

Luego, instale el certificado de CA raíz en el directorio `openssl` ejecutando un comando similar al siguiente:

```
sudo cp root.pem /etc/pki/CA/certs/
```

Nota:

No coloque el certificado de CA raíz en la ruta **/root**. De lo contrario, FAS no tendrá permiso de **lectura** para el certificado de CA raíz.

Ejecutar ctxfascfg.sh

Ejecute el script ctxfascfg.sh para configurar FAS:

```
sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
```

Puede ejecutar `ctxfascfg.sh` en modo silencioso. Antes de ejecutar el script en modo silencioso, establezca las siguientes variables de entorno:

- **CTX_FAS_ADINTEGRATIONWAY=winbind \| sssd \| centrify \| pbis \| quest**: Indica el método de integración de Active Directory, que es igual a `CTX_EASYINSTALL_ADINTEGRATIONWAY` cuando se especifica `CTX_EASYINSTALL_ADINTEGRATIONWAY`. Si no se especifica `CTX_EASYINSTALL_ADINTEGRATIONWAY`, `CTX_FAS_ADINTEGRATIONWAY` utiliza su propia configuración de valor.
- **CTX_FAS_CERT_PATH \=\<certificate path\>**: Especifica la ruta completa donde se almacenan el certificado raíz y todos los certificados intermedios.
- **CTX_FAS_KDC_HOSTNAME**: Especifica el nombre de host del Centro de distribución de claves (KDC) cuando selecciona PBIS y Quest.
- **CTX_FAS_PKINIT_KDC_HOSTNAME**: Especifica el nombre de host del KDC de PKINIT, que es igual a CTX_FAS_KDC_HOSTNAME a menos que se especifique lo contrario. Si tiene varios Delivery Controllers, agregue los nombres de host de todos los KDC del dominio a pkinit_kdc_hostname en el archivo **/etc/krb5.conf**. Para obtener más información, consulte el artículo del Centro de conocimiento CTX322129.
- **CTX_FAS_SERVER_LIST='list-fas-servers'** – Los servidores del Servicio de autenticación federada (FAS) se configuran a través de la Directiva de grupo de AD. Para obtener información sobre la configuración de la directiva de FAS en la GPO del dominio, consulte Configurar la directiva de grupo. El VDA de Linux no admite la Directiva de grupo de AD, pero puede proporcionar una lista de servidores FAS separada por punto y coma. La secuencia debe ser la misma que la configurada en la Directiva de grupo de AD. Si se elimina alguna dirección de servidor, rellene su espacio en blanco con la cadena de texto **'\<none\>'** y no modifique el orden de las direcciones de servidor. Para comunicarse correctamente con los servidores FAS, asegúrese de añadir un número de puerto coherente con el número de puerto especificado en los servidores FAS, por ejemplo, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.

  Para actualizar una instalación existente de VDA de Linux, puede ejecutar los siguientes comandos para configurar los servidores FAS y reiniciar el servicio `ctxvda` para que la configuración surta efecto.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredential
Service" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force



systemctl restart ctxjproxy



systemctl restart ctxvda
```

Para actualizar los servidores FAS a través de `ctxreg`, ejecute los siguientes comandos:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredential
Service" -v "Addresses" -d "<Your-FAS-Server-List>"



systemctl restart ctxjproxy



systemctl restart ctxvda
```

Elija el método de integración de Active Directory correcto y, a continuación, escriba la ruta correcta de los certificados (por ejemplo, `/etc/pki/CA/certs/`).

El script instala los paquetes krb5-pkinit y pam_krb5 y establece los archivos de configuración pertinentes. Para RHEL 8 y versiones posteriores, como PAM_KRB5 se ha movido al repositorio EPEL, el script intenta habilitar EPEL en esas distribuciones.

Inhabilitar FAS

Para inhabilitar FAS en el VDA de Linux, elimine todos los servidores FAS de ConfDB mediante los siguientes comandos:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "" --force
```

```
systemctl restart ctxjproxy


systemctl restart ctxvda
```

Habilitar la autenticación secundaria para errores de SSO de FAS

El VDA de Linux proporciona una mayor resistencia al inicio de sesión al ofrecer un método de autenticación secundaria específicamente cuando falla el inicio de sesión único (SSO) de FAS. Con esta función, si el SSO de FAS encuentra problemas, se pide a los usuarios que introduzcan manualmente sus credenciales para la autenticación con contraseña. Para habilitar la función, ejecute el siguiente comando:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\AccessControl\Login\Global"
-t "REG_DWORD" -v "SecondaryAuthEnabled" -d "0x00000001" --force
```

Limitación

- FAS aún no admite la pantalla de bloqueo. Si hace clic en el botón de bloqueo en una sesión, no podrá volver a iniciar sesión en la sesión utilizando FAS.
- Esta versión solo admite las implementaciones comunes de FAS resumidas en el artículo Información general de la arquitectura del Servicio de autenticación federada y no incluye **Windows 10 Azure AD Join**.

Solución de problemas

Antes de solucionar problemas de FAS, asegúrese de que:

- El VDA de Linux está instalado y configurado correctamente.
- Se puede iniciar correctamente una sesión que no sea de FAS en el almacén común mediante la autenticación con contraseña.

Si las sesiones que no son de FAS funcionan correctamente, establezca el nivel de registro de HDX de la clase **Login** en VERBOSE y el nivel de registro de VDA en TRACE. Para obtener información sobre cómo habilitar el registro de seguimiento para el VDA de Linux, consulte el artículo del Knowledge Center CTX220130.

También puede usar la herramienta **XDPing** de Linux para comprobar si hay problemas de configuración comunes que puedan existir en su entorno de VDA de Linux.

Error de configuración del servidor FAS

No se puede iniciar una sesión desde el almacén de FAS.

Compruebe **/var/log/xdl/hdx.log** y busque el registro de errores similar al siguiente:

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon
Type] Federated Authentication Logon.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start
connect to server 0



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed
to connect: Connection refused.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed
to connect to server [0], please confirm if fas service list is well
configurated in condb



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit,
43



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed
to validate fas credential
```

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
```

SOLUCIÓN

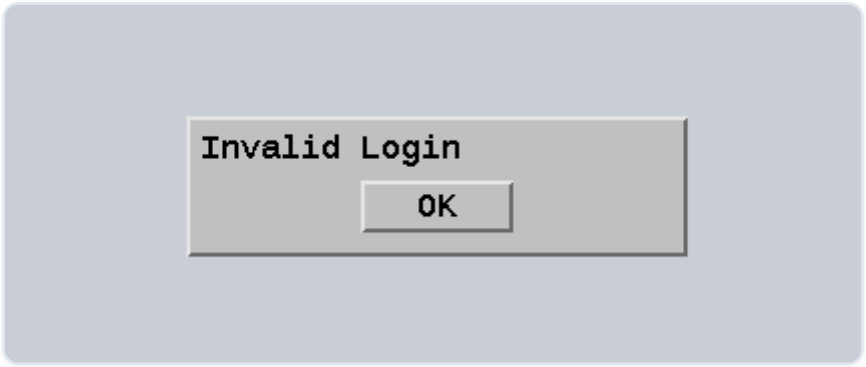
Ejecute el siguiente comando para verificar que el valor del registro de Citrix "HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\VirtualDesktopAgent\\Authentication\ \UserCredentialService" esté establecido en \<Your-FAS-Server-List\>.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
```

Si la configuración existente es incorrecta, siga el paso anterior Configurar servidores FAS para volver a configurarla.

Configuración incorrecta del certificado de CA

No se puede iniciar una sesión desde el almacén de FAS. Aparece una ventana gris y desaparece varios segundos después.



Compruebe **/var/log/xdl/hdx.log** y busque el registro de errores similar al siguiente:

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: entry



2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller: current
process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]



2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_public_certificate: entry
```

```
2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
for response...

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query to
server success

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
get_public_certificate: exit

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
input size 1888

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
cache certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: exit, 0
```

```
2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
```

SOLUCIÓN

verificar que ha configurado correctamente en `/etc/krb5.conf` la ruta completa que almacena el certificado raíz de CA y todos los certificados intermedios. La ruta completa es similar a la siguiente:

```
 [realms]

EXAMPLE.COM = {

    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

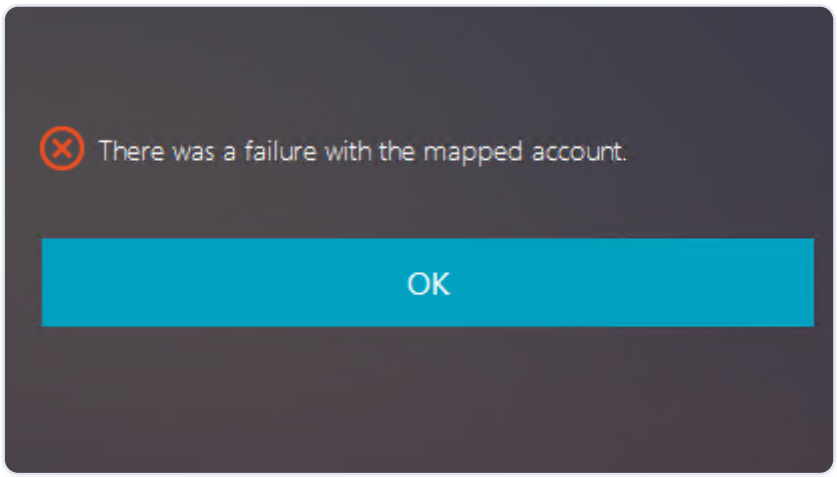
}
```

Si la configuración existente es incorrecta, siga el paso anterior Instalar certificados para configurarla de nuevo.

Alternativamente, compruebe si el certificado raíz de CA es válido.

Error de asignación de cuenta de sombra

FAS se configura mediante la autenticación SAML. El siguiente error puede ocurrir después de que un usuario de ADFS introduzca el nombre de usuario y la contraseña en la página de inicio de sesión de ADFS.



El error indica que:

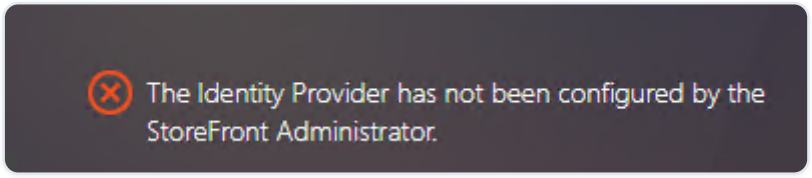
- El usuario de ADFS se ha verificado correctamente, pero no hay ningún usuario de sombra configurado en AD.

SOLUCIÓN

Configure la cuenta de sombra en AD.

ADFS no configurado

El siguiente error ocurre durante un intento de inicio de sesión en el almacén de FAS:



El problema ocurre cuando se configura el almacén de FAS para usar la autenticación SAML, pero falta la implementación de ADFS.

SOLUCIÓN

Implemente el IdP de ADFS para el Servicio de autenticación federada. Para obtener más información, consulte Implementación de ADFS del Servicio de autenticación federada.

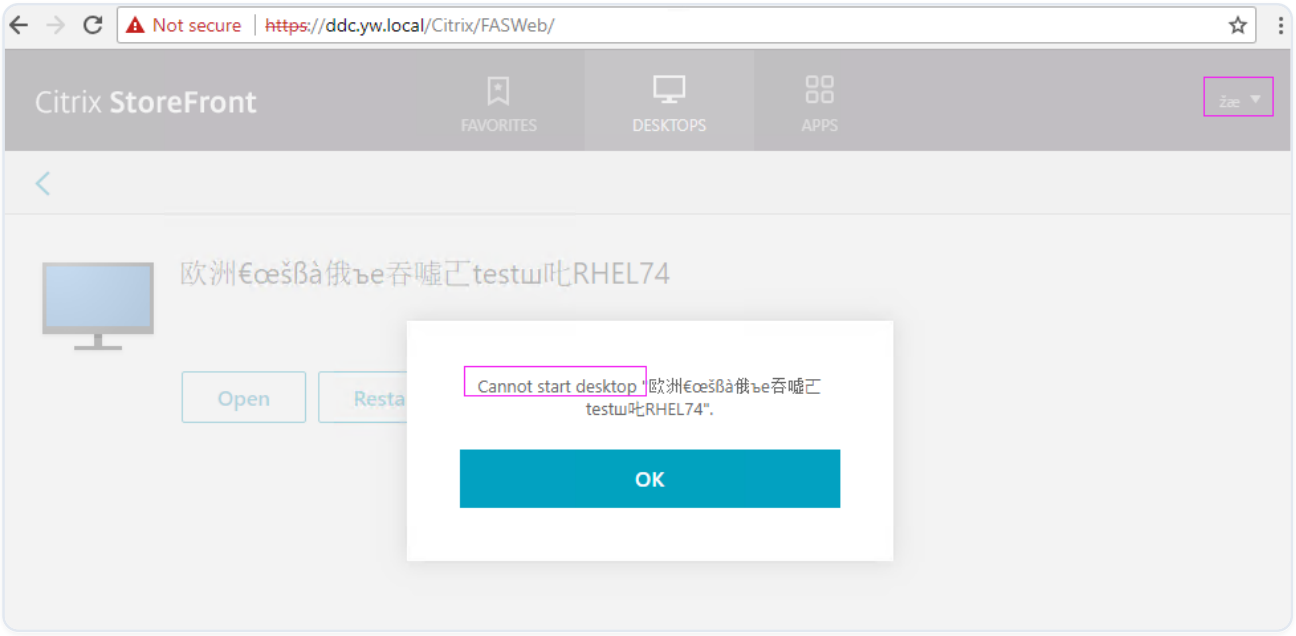
Información relacionada

- Las implementaciones comunes de FAS se resumen en el artículo Descripción general de la arquitectura del Servicio de autenticación federada.

- "Artículos "Cómo hacer" se presentan en el capítulo Configuración avanzada de Federated Authentication Service.

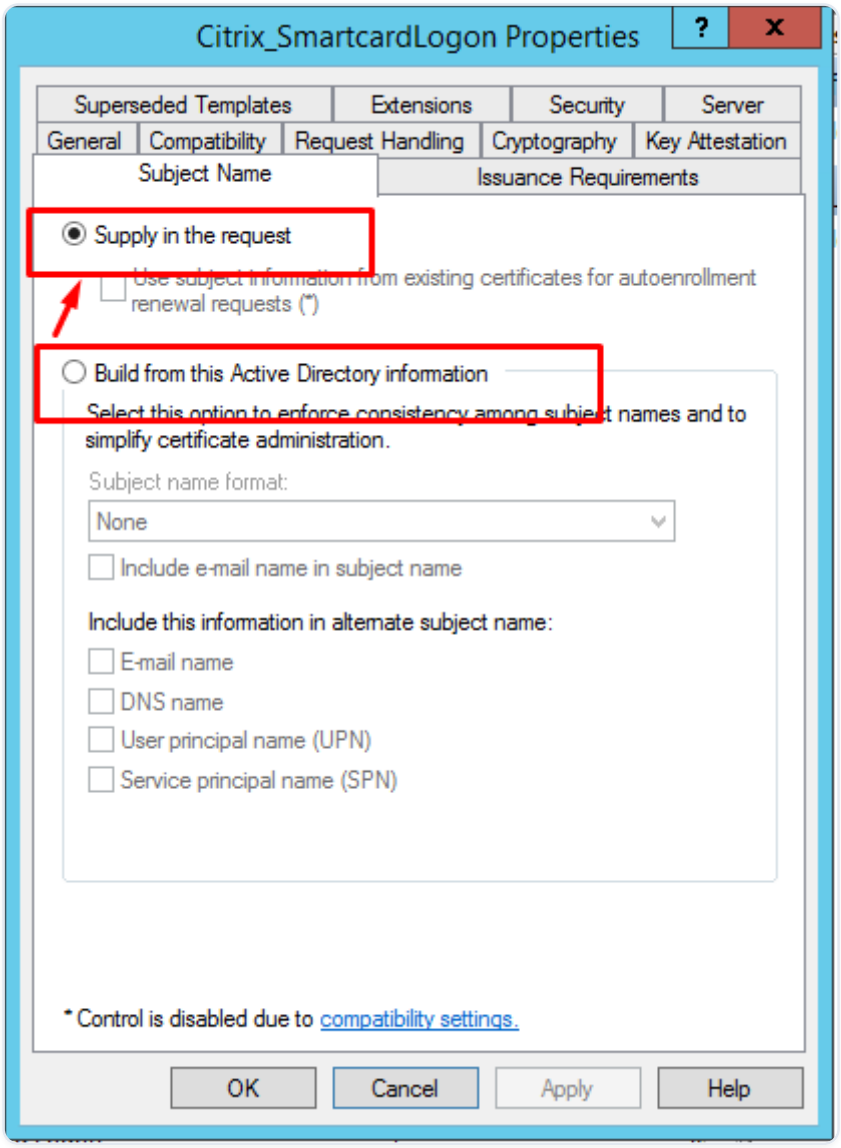
Problemas conocidos

Cuando FAS está en uso, puede fallar al intentar iniciar un escritorio publicado o una sesión de aplicación con caracteres no ingleses.



Solución alternativa

Haga clic con el botón derecho en **Administrar plantillas** en la herramienta de CA para cambiar la plantilla **Citrix_SmartcardLogon** de **Crear a partir de esta información de Active Directory** a **Suministrar en la solicitud**:



FIDO2 (vista previa)

Puede configurar la autenticación FIDO2 para acceder a sitios web mediante Google Chrome alojado en el VDA de Linux.

> **Nota:**
>
> El VDA de Linux solo admite la combinación de FIDO2 y Google Chrome.

Para configurar la autenticación FIDO2, siga estos pasos:

1. Descargue el paquete de extensión de Citrix FIDO2.
   a. Vaya a la página de descarga de Citrix Virtual Apps and Desktops.

b. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
c. Haga clic en **Components** para encontrar el VDA de Linux.
d. Haga clic en el VDA de Linux para abrir su página de descarga.
e. Descargue el paquete de orígenes.
f. Descomprima el paquete de orígenes para encontrar **FIDO2-JavaScript-Extensions.zip**.
g. Descomprima el paquete de extensión de FIDO2. Puede encontrar el directorio de extensión de FIDO2 en **extensions > chrome > fido2**.

2. Agregue la extensión de Citrix FIDO2 en Google Chrome:

a. Abra Google Chrome alojado en el VDA de Linux.
b. Haga clic en el menú de tres puntos a la derecha de la barra de direcciones y, a continuación, seleccione **Más herramientas > Extensiones**.

Localización del menú Extensiones(/en-us/linux-virtual-delivery-agent/2507-ltsr/media/more-tools-extensions.png)

c. Active el **Modo de desarrollador**.

Modo de desarrollador(/en-us/linux-virtual-delivery-agent/2507-ltsr/media/developer-mode.png)

d. Haga clic en **Cargar descomprimida** y seleccione el directorio de la extensión en **extensions > chrome > fido2**.

3. En el sitio web para el que quiera usar la autenticación FIDO2, registre una clave de seguridad FIDO2 para usar la autenticación FIDO2.

a. Inserte una clave de seguridad FIDO2 en el cliente donde está instalada la aplicación Citrix Workspace™.
b. Habilite la autenticación multifactor y añada FIDO2 como método de autenticación.

Una vez configurada la autenticación FIDO2, se le pedirá que toque la clave de seguridad para acceder al sitio web correctamente.

Autenticación sin SSO

Este artículo proporciona orientación sobre cómo habilitar la autenticación sin SSO en el VDA de Linux.

Información general

De forma predeterminada, el VDA de Linux tiene habilitado el inicio de sesión único (SSO). Los usuarios inician sesión en la aplicación Citrix Workspace™ y en las sesiones de VDA con un único conjunto de credenciales.

Para que los usuarios inicien sesión en las sesiones de VDA con un conjunto de credenciales diferente, inhabilite el SSO en el VDA de Linux. La siguiente tabla enumera las combinaciones de métodos de autenticación de usuario admitidos en escenarios sin SSO.

APLICACIÓN CITRIX WORKSPACE	SESIÓN DE VDA
nombre de usuario	nombre de usuario
tarjeta inteligente	nombre de usuario
nombre de usuario	tarjeta inteligente
FAS	nombre de usuario
FAS	tarjeta inteligente

Inhabilitar SSO

Ejecute el siguiente comando en su VDA de Linux:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
"REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
```

Personalizar la pantalla de inicio de sesión

El VDA de Linux le permite controlar cómo inician sesión los usuarios cuando no utilizan SSO. Puede personalizar la experiencia de inicio de sesión eligiendo qué métodos de autenticación se muestran. Anteriormente, la pantalla de inicio de sesión sin SSO siempre mostraba la autenticación con contraseña y con tarjeta inteligente en una lista desplegable. Ahora, puede configurar el VDA de Linux para que ofrezca:

- Solo autenticación con contraseña
- Solo autenticación con tarjeta inteligente
- Combinación de autenticación con contraseña y tarjeta inteligente, con cualquiera de las opciones presentada por defecto

Puede personalizar el método de inicio de sesión ajustando la siguiente configuración del registro en el VDA:

`System\CurrentControlSet\Control\Citrix\login\NSSOLogonType`

El valor de la clave de registro `NSSOLogonType` controla qué métodos de inicio de sesión se muestran en la pantalla de inicio de sesión del VDA de Linux para los usuarios sin SSO:

- **1**: Solo autenticación con tarjeta inteligente. Los usuarios deben iniciar sesión con su tarjeta inteligente.
- **2**: Combinación de autenticación con contraseña y tarjeta inteligente, con la autenticación con contraseña presentada por defecto
- **3**: Combinación de autenticación con contraseña y tarjeta inteligente, con la autenticación con tarjeta inteligente presentada por defecto.
- **Cualquier otro valor**: Solo autenticación con contraseña. Los usuarios inician sesión con su nombre de usuario y contraseña.

Para verificar que ha configurado correctamente la función de inicio de sesión personalizable en su VDA de Linux, siga estos pasos:

1. Habilite Non-SSO en el VDA mediante el siguiente comando:

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k
   "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
   "REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
   ```

2. Cambie el tipo de inicio de sesión predeterminado utilizando un comando similar al siguiente en el VDA:

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k
   "HKLM\System\CurrentControlSet\Control\Citrix\login" -t "REG_DWORD" -v
   "NSSOLogonType" -d "0x00000001" --force
   ```

   Como se describió anteriormente, establecer el valor de la clave de registro `NSSOLogonType` en `1` configura el VDA de Linux para mostrar solo la opción de autenticación con tarjeta inteligente en la pantalla de inicio de sesión.

3. Compruebe la pantalla de inicio de sesión para verificar que la lista desplegable muestre solo la autenticación con tarjeta inteligente que configuró.

Tarjetas inteligentes

Puede usar una tarjeta inteligente conectada al dispositivo cliente para la autenticación al iniciar sesión en una sesión de escritorio virtual de Linux. Esta función se implementa mediante la redirección de tarjetas inteligentes a través del canal virtual de tarjetas inteligentes ICA®. También puede usar la tarjeta inteligente dentro de la sesión. Los casos de uso incluyen:

- Añadir una firma digital a un documento
- Cifrar o descifrar un correo electrónico
- Autenticarse en un sitio web

El VDA de Linux utiliza la misma configuración que el VDA de Windows para esta función. Para obtener más información, consulte la sección Configurar el entorno de tarjetas inteligentes de este artículo.

> **Nota:**
>
> No se admite el uso de una tarjeta inteligente asignada dentro de una sesión de VDA de Linux para iniciar sesión en Citrix Gateway.

Compatibilidad con distribuciones de Linux y métodos de integración de AD limitados

- La autenticación de paso de tarjeta inteligente admite distribuciones de Linux y métodos de integración de AD limitados. Consulte la siguiente matriz:

	WINBIND	SSSD	CENTRIFY	QUEST
Debian 12.15/11.11	Sí	Sí	Sí	Sí
RHEL 9.8/9.6/9.4	Sí	Sí	Sí	Sí
RHEL 8.10	Sí	Sí	Sí	Sí
Rocky Linux 9.8/9.6/9.4	Sí	Sí	Sí	Sí

	WINBIND	SSSD	CENTRIFY	QUEST
Rocky Linux 8.10	Sí	Sí	Sí	Sí
Ubuntu 24.04	Sí	Sí	Sí	Sí
Ubuntu 22.04	Sí	Sí	Sí	Sí

Requisitos previos

La disponibilidad de la autenticación de paso de tarjeta inteligente depende de las siguientes condiciones:

- Su VDA de Linux puede registrarse con el Delivery Controller™ y puede abrir las sesiones de escritorio de Linux publicadas utilizando credenciales de Windows.
- Se utilizan tarjetas inteligentes compatibles con OpenSC. Para obtener más información, consulte Asegúrese de que OpenSC sea compatible con su tarjeta inteligente.

Asegúrese de que OpenSC sea compatible con su tarjeta inteligente

OpenSC es un controlador de tarjeta inteligente ampliamente utilizado en RHEL 7.4+. Como reemplazo totalmente compatible de CoolKey, OpenSC es compatible con muchos tipos de tarjetas inteligentes (consulte Compatibilidad con tarjetas inteligentes en Red Hat Enterprise Linux).

En este artículo, la tarjeta inteligente YubiKey se utiliza como ejemplo para ilustrar la configuración. YubiKey es un dispositivo USB CCID PIV todo en uno que se puede adquirir fácilmente en Amazon u otros minoristas. El controlador OpenSC es compatible con YubiKey.

Si su organización requiere otra tarjeta inteligente más avanzada, prepare una máquina física con una distribución de Linux compatible y el paquete OpenSC instalado. Para obtener información sobre la instalación de OpenSC, consulte Instalar el controlador de tarjeta inteligente. Inserte su tarjeta inteligente y ejecute el siguiente comando para verificar que OpenSC es compatible con su tarjeta inteligente:

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
```

Configuración

Prepare un certificado raíz

Se utiliza un certificado raíz para verificar el certificado de la tarjeta inteligente. Siga los pasos siguientes para descargar e instalar un certificado raíz.

1. Obtenga un certificado raíz en formato PEM, normalmente de su servidor de CA.

   Puede ejecutar un comando similar al siguiente para convertir un archivo DER (*.crt, *.cer, *.der) a PEM. En el siguiente ejemplo de comando, **certnew.cer** es un archivo DER.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   ```

2. Instale el certificado raíz en el directorio `openssl`. El archivo **certnew.pem** se utiliza como ejemplo.

   ```
   cp certnew.pem <path where you install the root certificate>
   ```

   Para crear una ruta para instalar el certificado raíz, ejecute `sudo mdkir -p <path where you install the root certificate>`.

Configurar el entorno de la tarjeta inteligente

Puede utilizar el script ctxsmartlogon.sh para configurar el entorno de la tarjeta inteligente o completar la configuración manualmente.

(OPCIÓN 1) UTILICE EL SCRIPT CTXSMARTLOGON.SH PARA CONFIGURAR EL ENTORNO DE LA TARJETA INTELIGENTE

Nota:

El script ctxsmartlogon.sh añade información de PKINIT al dominio predeterminado. Puede cambiar esta configuración a través del archivo de configuración **/etc/krb5.conf**.

Antes de utilizar tarjetas inteligentes por primera vez, ejecute el script ctxsmartlogon.sh para configurar el entorno de la tarjeta inteligente.

Sugerencia:

Si ha utilizado SSSD para la unión a un dominio, reinicie el servicio SSSD después de ejecutar ctxsmartlogon.sh. Para RHEL 8 y versiones posteriores, como PAM_KRB5 se ha movido al repositorio EPEL, el script intentará habilitar EPEL en esas distribuciones.

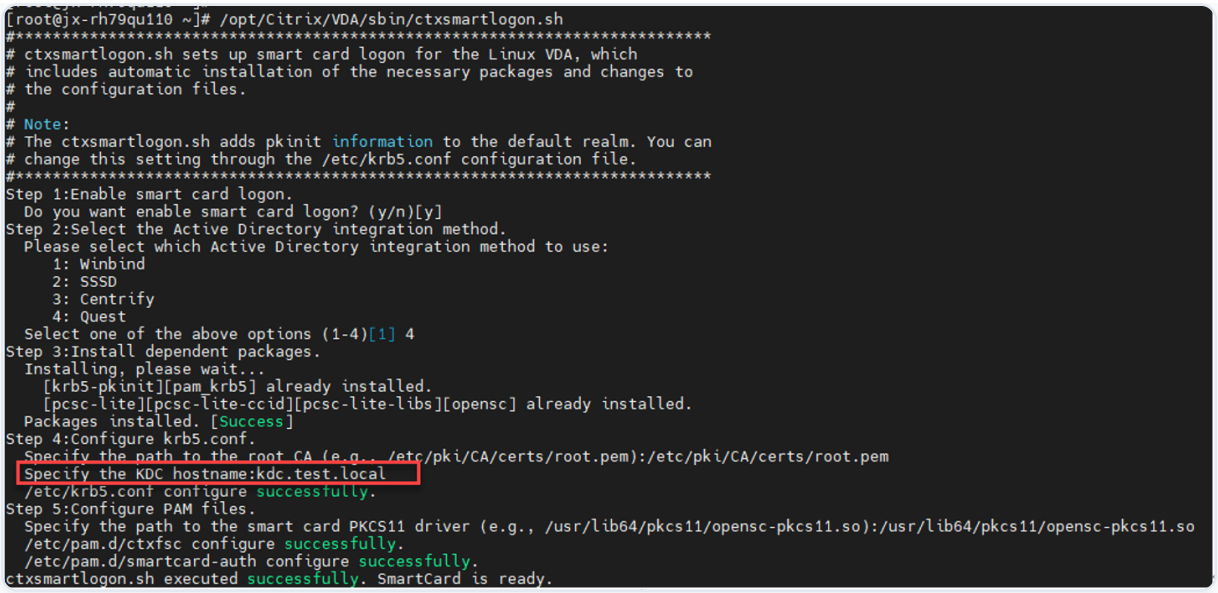
```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

Los resultados son similares a los siguientes:

```
#*******************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*******************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

Nota:

Si utiliza Quest como método de unión a un dominio, debe especificar el nombre de host del Centro de distribución de claves (KDC). Por ejemplo:



También puede deshabilitar las tarjetas inteligentes ejecutando el script ctxsmartlogon.sh:

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

Los resultados son similares a los siguientes:

```
#*******************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*******************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

(OPCIÓN 2) CONFIGURAR EL ENTORNO DE TARJETA INTELIGENTE MANUALMENTE

El VDA de Linux utiliza el mismo entorno de tarjeta inteligente que el VDA de Windows. En este entorno, se deben configurar varios componentes, incluidos el controlador de dominio, la entidad de certificación (CA) de Microsoft, Internet Information Services, Citrix StoreFront y la aplicación Citrix Workspace. Para obtener información sobre la configuración basada en la tarjeta inteligente YubiKey, consulte el artículo del Centro de conocimientos CTX206156.

Antes de pasar al siguiente paso, asegúrese de que:

- Ha configurado todos los componentes correctamente.
- Ha descargado la clave privada y el certificado de usuario en la tarjeta inteligente.

- Puede iniciar sesión correctamente en el VDA con la tarjeta inteligente.

Instalar los paquetes PC/SC Lite
PCSC Lite es una implementación de la especificación PC/SC (Personal Computer/Smart Card) en Linux. Proporciona una interfaz de tarjeta inteligente de Windows para comunicarse con tarjetas inteligentes y lectores. La redirección de tarjetas inteligentes en el VDA de Linux se implementa a nivel de PC/SC.

Ejecute el siguiente comando para instalar los paquetes PC/SC Lite:

RHEL 9.x/8.x, Rocky Linux 9.x/8.x:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Ubuntu 24.04, Ubuntu 22.04, Debian 12.x, Debian 11.11:

```
apt-get install -y libpcsclite1 libccid
```

Instalar el controlador de tarjeta inteligente
OpenSC es un controlador de tarjeta inteligente ampliamente utilizado. Si OpenSC no está instalado, ejecute el siguiente comando para instalarlo:

RHEL 9.x/8.x, Rocky Linux 9.x/8.x:

```
yum install opensc
```

Ubuntu 24.04, Ubuntu 22.04, Debian 12.x, Debian 11.11:

```
apt-get install -y opensc
```

Instalar los módulos PAM para la autenticación con tarjeta inteligente
Ejecute el siguiente comando para instalar los módulos pam_krb5 y krb5-pkinit.

RHEL 9.x/8.x, Rocky Linux 9.x/8.x:

```
yum install krb5-pkinit
```

Ubuntu 24.04, Ubuntu 22.04:

```
apt-get install libpam-krb5 krb5-pkinit
```

Debian 12.x, Debian 11.11:

```
apt-get install -y libpam-krb5 krb5-pkinit
```

El módulo pam_krb5 es un módulo de autenticación conectable. Las aplicaciones compatibles con PAM pueden usar pam_krb5 para comprobar contraseñas y obtener tickets de concesión de tickets del Centro de distribución de claves (KDC). El módulo krb5-pkinit contiene el complemento PKINIT que permite a los clientes obtener credenciales iniciales del KDC mediante una clave privada y un certificado.
Configurar el módulo pam_krb5
El módulo pam_krb5 interactúa con el KDC para obtener tickets de Kerberos mediante certificados en la tarjeta inteligente. Para habilitar la autenticación pam_krb5 en PAM, ejecute el siguiente comando:

```
authconfig --enablekrb5 --update
```

En el archivo de configuración **/etc/krb5.conf**, agregue la información de PKINIT según el dominio real.

Nota:

La opción **pkinit_cert_match** especifica las reglas de coincidencia que debe cumplir el certificado de cliente antes de que se utilice para intentar la autenticación PKINIT. La sintaxis de las reglas de coincidencia es:

component-rule …

donde **relation-operator** puede ser **&&**, lo que significa que todas las reglas de componentes deben coincidir, o **\|\|**, lo que significa que solo una regla de componente debe coincidir.

Aquí tiene un ejemplo de un archivo krb5.conf genérico:

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM


    auth_to_local = RULE:[1:$1@$0]


    pkinit_anchors = FILE:<path where you install the root certificate>/
certnew.pem


    pkinit_kdc_hostname = KDC.EXAMPLE.COM


    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature


    pkinit_eku_checking = kpServerAuth


 }
```

El archivo de configuración se parece al siguiente después de agregar la información de PKINIT.

```
CTXDEV.LOCAL = {
    kdc = [redacted]
    auth_to_local = RULE:[1:$1@$0]
    pkinit_kdc_hostname = ctx-ad.ctxdev.local
    pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

Configurar la autenticación PAM

Los archivos de configuración de PAM indican qué módulos se utilizan para la autenticación PAM. Para añadir pam_krb5 como módulo de autenticación, añada la siguiente línea al archivo **/etc/pam.d/smartcard-auth**:

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.so
```

El archivo de configuración se parece al siguiente después de la modificación si se utiliza SSSD.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

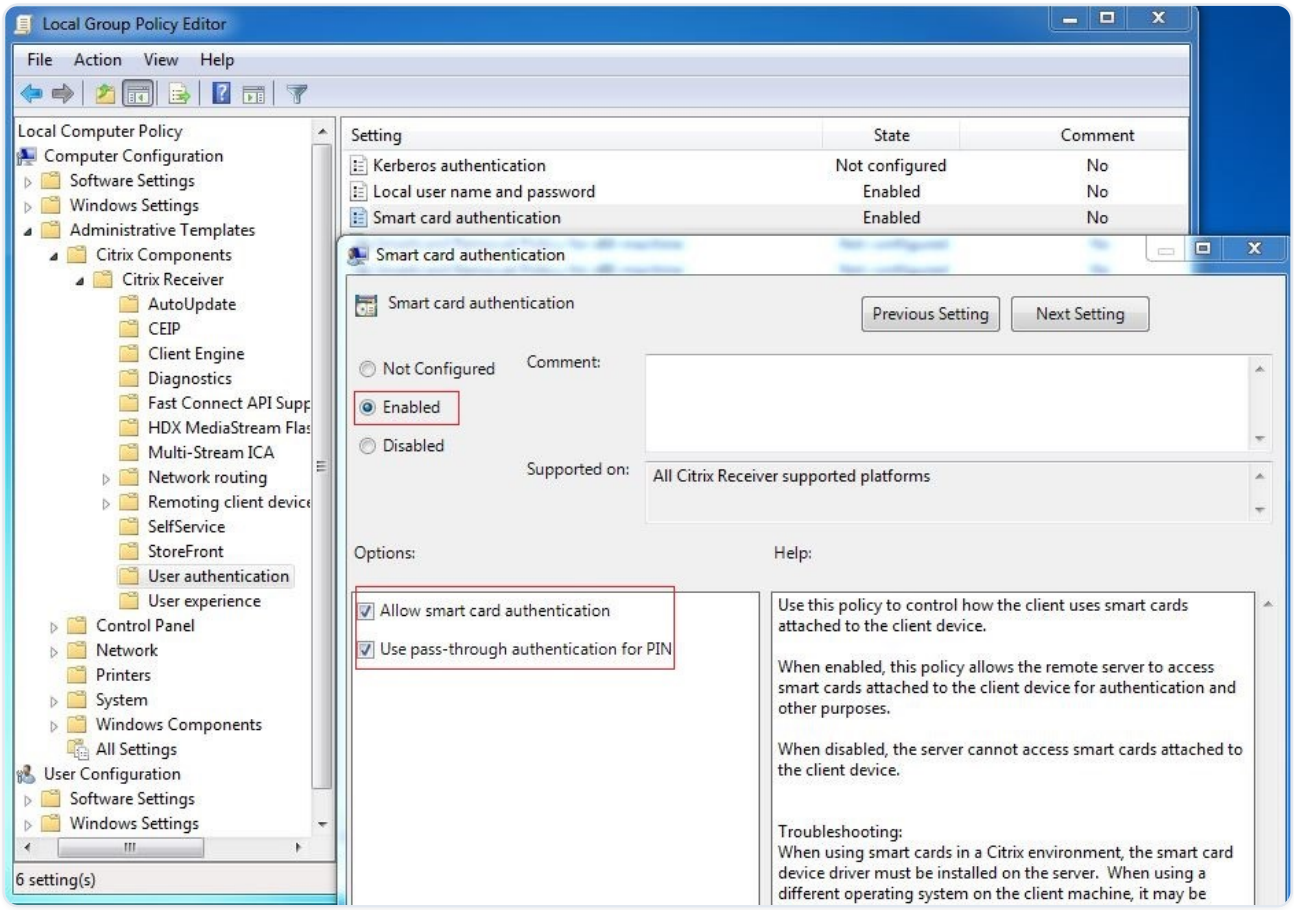
account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
account     required      pam_permit.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
#session     optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```

(Opcional) Inicio de sesión único mediante tarjetas inteligentes

El inicio de sesión único (SSO) es una función de Citrix que implementa la autenticación de paso con el lanzamiento de escritorios virtuales y aplicaciones. Esta función reduce el número de veces que los usuarios escriben su PIN. Para usar SSO con Linux VDA, configure la aplicación Citrix Workspace. La configuración es la misma que con Windows VDA. Para obtener más información, consulte el artículo del Centro de conocimientos CTX133982.

Habilite la autenticación con tarjeta inteligente de la siguiente manera al configurar la directiva de grupo en la aplicación Citrix Workspace™.



Inicio de sesión rápido con tarjeta inteligente

La tarjeta inteligente rápida es una mejora con respecto a la redirección de tarjetas inteligentes HDX basada en PC/SC existente. Mejora el rendimiento cuando las tarjetas inteligentes se utilizan en entornos WAN de alta latencia. Para obtener más información, consulte Tarjetas inteligentes.

El Linux VDA admite la tarjeta inteligente rápida en las siguientes versiones de la aplicación Citrix Workspace:

- Citrix Receiver para Windows 4.12
- Citrix Workspace app 1808 para Windows y versiones posteriores

HABILITAR EL INICIO DE SESIÓN RÁPIDO CON TARJETA INTELIGENTE EN EL CLIENTE

El inicio de sesión rápido con tarjeta inteligente está habilitado de forma predeterminada en el VDA y deshabilitado de forma predeterminada en el cliente. En el cliente, para habilitar el inicio de sesión rápido con tarjeta inteligente, incluya el siguiente parámetro en el archivo default.ica del sitio de StoreFront asociado:

```
[WFClient]

SmartCardCryptographicRedirection=On
```

DESHABILITAR EL INICIO DE SESIÓN RÁPIDO CON TARJETA INTELIGENTE EN EL CLIENTE

Para deshabilitar el inicio de sesión rápido con tarjeta inteligente en el cliente, elimine el parámetro **SmartCardCryptographicRedirection** del archivo default.ica del sitio de StoreFront asociado.

Ejecutar XDPing

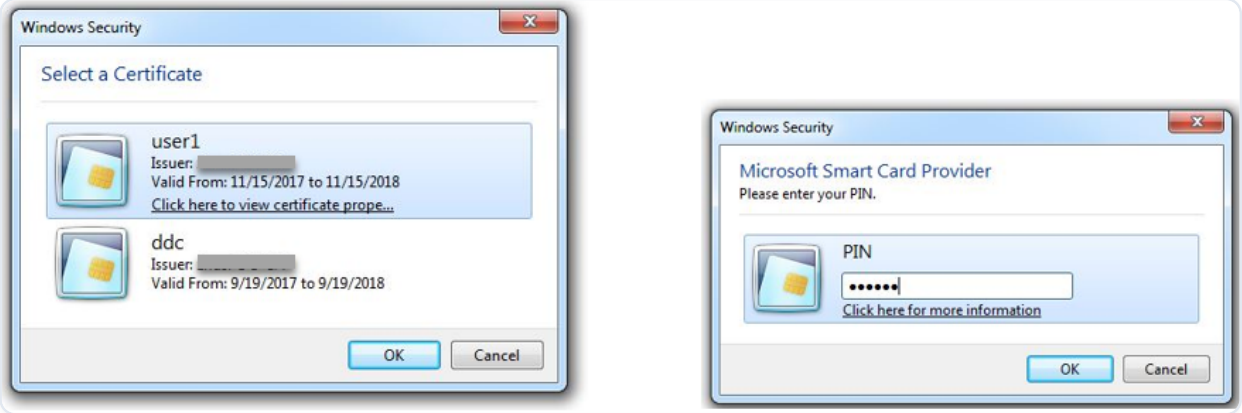
Después de completar los pasos anteriores, puede usar la herramienta **XDPing** de Linux para comprobar si hay problemas de configuración comunes que puedan existir en su entorno de VDA de Linux.

Uso

Iniciar sesión en el VDA de Linux con una tarjeta inteligente

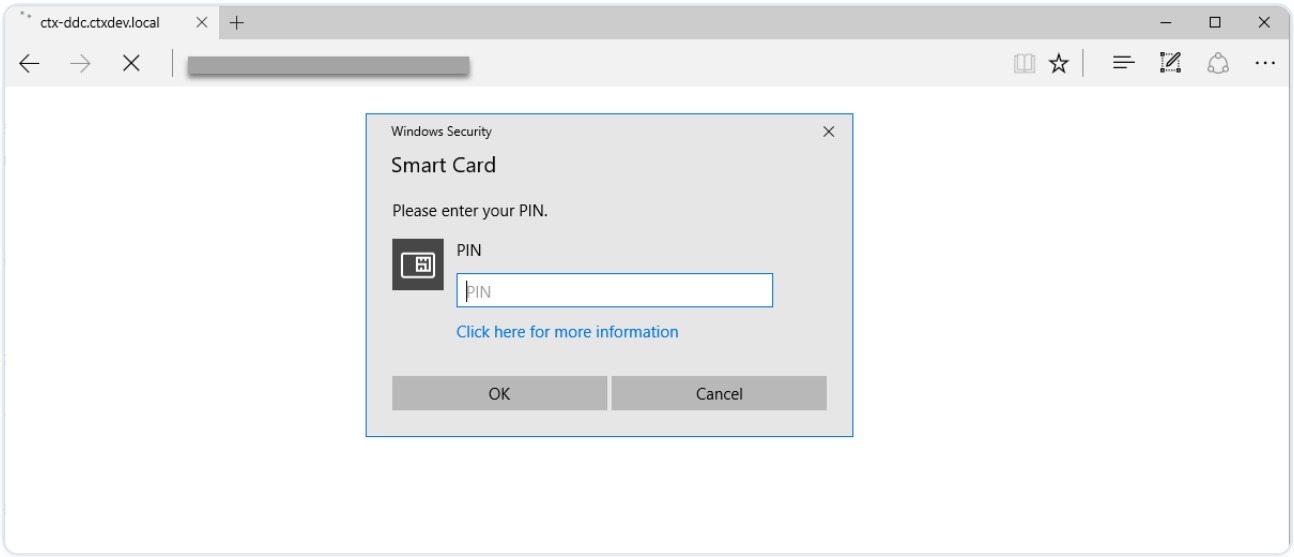
Puede usar una tarjeta inteligente para iniciar sesión en el VDA de Linux tanto en escenarios de SSO como de no SSO.

- En el escenario de SSO, inicia sesión en StoreFront™ automáticamente mediante el certificado de tarjeta inteligente y el PIN almacenados en caché. Cuando inicia una sesión de escritorio virtual de Linux en StoreFront, el PIN se pasa al VDA de Linux para la autenticación con tarjeta inteligente.
- En el escenario de no SSO, se le pedirá que seleccione un certificado y escriba un PIN para iniciar sesión en StoreFront.



Cuando inicia una sesión de escritorio virtual de Linux en StoreFront, aparece un cuadro de diálogo para iniciar sesión en el VDA de Linux de la siguiente manera. El nombre de usuario se extrae del certificado de la tarjeta inteligente y debe volver a escribir el PIN para la autenticación de inicio de sesión.

Este comportamiento es el mismo que con el VDA de Windows.



Volver a conectar a una sesión con una tarjeta inteligente

Para volver a conectar a una sesión, asegúrese de que la tarjeta inteligente esté conectada al dispositivo cliente. De lo contrario, aparecerá una ventana de almacenamiento en caché gris en el lado del VDA de Linux y se cerrará rápidamente porque la reautenticación falla si la tarjeta inteligente no está conectada. En este caso, no se proporciona ninguna otra indicación para recordarle que conecte la tarjeta inteligente.

Sin embargo, en el lado de StoreFront, si no hay una tarjeta inteligente conectada al volver a conectar a una sesión, la web de StoreFront podría mostrar una alerta como la siguiente:



Limitación

Configuración de extracción de tarjeta inteligente

Para especificar el comportamiento cuando se retira la tarjeta inteligente de un usuario con sesión iniciada del lector de tarjetas inteligentes durante una sesión, edite la siguiente clave del Registro en el VDA de Linux:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LocalPolicies\SecurityOptions

NOMBRE DEL VALOR	TIPO	PREDETERMINADO	DESCRIPCIÓN
SCardRemoveOption	REG_DWORD	0x00000000	Esta configuración determina qué sucede cuando se retira la tarjeta inteligente de un usuario con sesión iniciada del lector de tarjetas inteligentes durante una sesión. Las opciones son las siguientes.
\^	\^	\^	0 **Ninguna acción**
\^	\^	\^	1 **Cierre de sesión forzado**: El usuario cierra sesión automáticamente al retirar la tarjeta inteligente.
\^	\^	\^	2 **desconectar Session**: La sesión se desconecta sin cerrar la sesión del usuario al retirar la tarjeta inteligente. El usuario puede volver a insertar la tarjeta inteligente para volver a conectar la sesión más tarde.
\^	\^	\^	3 **Bloquear estación de trabajo**: El escritorio virtual se bloquea. El usuario puede volver a insertar la tarjeta inteligente e

NOMBRE DEL VALOR	TIPO	PREDETERMINADO	DESCRIPCIÓN
			introducir el código PIN para desbloquear la pantalla.
SCardRemoveActionDelaySeconds	REG_DWORD	15	Si la opción de eliminación se establece como **Cierre de sesión forzado** o **desconectar Session**, puede especificar un retraso de varios segundos antes de que se realice la acción. Con esta configuración, aparece un cuadro de mensaje en la sesión del usuario después de retirar la tarjeta inteligente, indicando que la sesión se cerrará forzosamente o se desconectará después de los segundos especificados. Si vuelve a insertar la tarjeta inteligente antes de ese tiempo, la sesión continúa sin interrupciones.

LIMITACIONES

El VDA de Linux solo admite un lector de tarjetas inteligentes a la vez.

Compatibilidad con otras tarjetas inteligentes y la biblioteca PKCS#11

Citrix proporciona una solución genérica de redirección de tarjetas inteligentes. Aunque solo la tarjeta inteligente OpenSC aparece en nuestra lista de compatibilidad, puede intentar usar otras tarjetas inteligentes y la biblioteca PKCS#11. Para cambiar a su tarjeta inteligente específica o a la biblioteca PKCS#11:

1. Sustituya todas las instancias de `opensc-pkcs11.so` por su biblioteca PKCS#11.
2. Para establecer la ruta de su biblioteca PKCS#11 en el registro, ejecute el siguiente comando:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v
   "PKCS11LibPath" -d "PATH"
   ```

   donde **PATH** apunta a su biblioteca PKCS#11, como `/usr/lib64/pkcs11/opensc-pkcs11.so`
3. Inhabilite el inicio de sesión rápido con tarjeta inteligente en el cliente.

Acceso de usuarios no autenticados (anónimos)

Puede permitir que los usuarios accedan a aplicaciones y escritorios sin presentar credenciales a StoreFront™ o la aplicación Citrix Workspace™. Para conceder acceso a usuarios no autenticados, debe tener un almacén de StoreFront no autenticado y habilitar el acceso para usuarios no autenticados en un grupo de entrega.

> **Nota:**
>
> El acceso de usuarios no autenticados solo se admite para VDA unidos a un dominio.
>
> El inicio previo de sesión no se admite para usuarios no autenticados. El inicio previo de sesión tampoco se admite en la aplicación Citrix Workspace para Android.

Crear un almacén de StoreFront no autenticado

1. Seleccione el nodo **Stores** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Actions**, haga clic en **Create Store**.
2. En la página **Store Name**, especifique un nombre para el almacén, seleccione **Allow only unauthenticated users to access this store** y haga clic en **Next**.

Para obtener más información, consulte Crear almacén.

Habilitar el acceso para usuarios no autenticados en un grupo de entrega

Un grupo de entrega es una colección de máquinas seleccionadas de uno o varios catálogos de máquinas. Al especificar quién puede usar las aplicaciones y los escritorios de un grupo de entrega, puede conceder acceso a usuarios no autenticados. Para obtener más información, consulte Crear grupos de entrega.

Establecer el tiempo de espera de inactividad para las sesiones de usuario no autenticadas

Las sesiones de usuario no autenticadas tienen un tiempo de espera de inactividad predeterminado de 10 minutos y se cierran automáticamente cuando el cliente se desconecta. Puede configurar un tiempo de espera de inactividad personalizado mediante la configuración del Registro **AnonymousUserIdleTime**. Por ejemplo, para establecer un tiempo de espera de inactividad personalizado de cinco minutos, ejecute el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime
 -d 0x00000005
```

Establecer el número máximo de usuarios no autenticados

Para establecer el número máximo de usuarios no autenticados, utilice la clave del Registro **MaxAnonymousUserNumber**. Esta configuración limita el número de sesiones de usuario no autenticadas que se ejecutan simultáneamente en un único VDA de Linux. Utilice la herramienta **ctxreg** para configurar esta entrada del Registro. Por ejemplo, para establecer el valor en 32, ejecute el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber
 -d  0x00000020
```

Importante:

Limite el número de sesiones de usuario no autenticadas. Demasiadas sesiones iniciadas simultáneamente pueden causar problemas en el VDA, incluida la falta de memoria disponible.

Solución de problemas

Tenga en cuenta lo siguiente al configurar sesiones de usuario no autenticadas:

- **Error al iniciar sesión en una sesión de usuario no autenticada**.

verificar que el registro se actualizó para incluir lo siguiente (establecido en 0):

```
sudo /opt/Citrix/VDA/bin/ctxreg read –k
"HKLM\System\CurrentControlSet\Control\Citrix" –v MaxAnonymousUserNumber
```

verificar que el servicio **ncsd** se está ejecutando y está configurado para habilitar la caché **passwd**:

```
ps  uax | grep nscd

cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

Establezca la variable de caché **passwd** en **no** si está habilitada y, a continuación, reinicie el servicio **ncsd**. Es posible que deba reinstalar el VDA de Linux después de cambiar esta configuración.

- **El botón de bloqueo de pantalla se muestra en una sesión de usuario no autenticada con KDE**.

El botón y el menú de bloqueo de pantalla están inhabilitados de forma predeterminada en una sesión de usuario no autenticada. Sin embargo, aún pueden mostrarse en KDE. En KDE, para inhabilitar el botón y el menú de bloqueo de pantalla para un usuario en particular, agregue las siguientes líneas al archivo de configuración **$Home/.kde/share/config/kdeglobals**. Por ejemplo:

```
[KDE Action Restrictions]

action/lock_screen=false
```

Sin embargo, si el parámetro `KDE Action Restrictions` está configurado como inmutable en un archivo `kdeglobals` global como `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals`, la configuración del usuario no tiene ningún efecto.

Para resolver este problema, modifique el archivo `kdeglobals` de todo el sistema para eliminar la etiqueta `[$i]` en la sección `[KDE Action Restrictions]`, o utilice directamente la configuración de todo el sistema para inhabilitar el botón y el menú de bloqueo de pantalla. Para obtener más información sobre la configuración de KDE, consulte la página KDE System Administration/Kiosk/Keys.

Archivo

Esta sección contiene los siguientes temas:

- Copiar y pegar archivos
- Transferencia de archivos

Copia y pegado de archivos

Los usuarios pueden copiar y pegar archivos entre una sesión y un cliente local mediante el menú contextual o los métodos abreviados de teclado. Esta función requiere Citrix Virtual Apps and Desktops™ 2006 o posterior y la aplicación Citrix Workspace™ 1903 o posterior para Windows.

Para copiar y pegar archivos correctamente, asegúrese de que:

- El número máximo de archivos no supera los 20.
- El tamaño máximo de archivo no supera los 200 MB.
- El administrador de archivos Nautilus está disponible en la máquina donde instaló el VDA de Linux.
- Los nombres de archivo contienen solo caracteres ASCII y ningún carácter especial.

Distribuciones de Linux compatibles

La **función de copiar y pegar archivos** está disponible para todas las distribuciones de Linux compatibles con el VDA de Linux.

Directivas relevantes

Las siguientes directivas de portapapeles son relevantes para configurar la función. Para obtener más información sobre las directivas de portapapeles, consulte la lista de compatibilidad de directivas.

- Redirección del Portapapeles del cliente
- Modo de actualización de la selección del portapapeles

- Modo de actualización de la selección principal

Nota:

Para inhabilitar la función de copiar y pegar archivos, establezca la directiva **Redirección del portapapeles del cliente** en **Prohibido** en Citrix Studio. Las directivas **Limitar el tamaño de transferencia del portapapeles del cliente a la sesión** y **Limitar el tamaño de transferencia del portapapeles de la sesión al cliente** controlan el tamaño del búfer del portapapeles, no el tamaño de los archivos transferidos. Para obtener más información sobre las directivas compatibles, consulte la lista de compatibilidad de directivas.

Limitaciones

- El corte no es compatible. Las solicitudes para cortar un archivo se tratan como operaciones de copia.
- Arrastrar y soltar no es compatible.
- No se admite la copia de directorios.
- La copia y pegado de archivos debe realizarse secuencialmente. Solo después de que el archivo anterior se haya copiado y pegado correctamente, se podrá copiar el siguiente archivo.

Transferencia de archivos

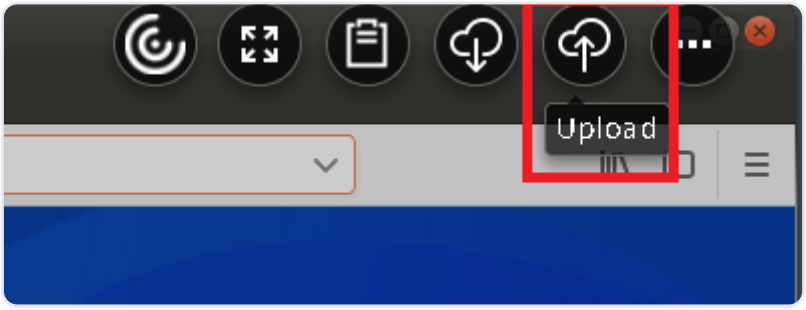
La transferencia de archivos es compatible entre el VDA de Linux y el dispositivo cliente. Esta función está disponible cuando el dispositivo cliente ejecuta un navegador web que admite el atributo de espacio aislado HTML5. El atributo de espacio aislado HTML5 permite a los usuarios acceder a escritorios y aplicaciones virtuales mediante la aplicación Citrix Workspace™ para HTML5 y para Chrome.

Nota:

La transferencia de archivos está disponible para la aplicación Citrix Workspace para HTML5 y para Chrome.

En las sesiones de aplicaciones y escritorios publicados, la transferencia de archivos permite cargar y descargar archivos entre el VDA de Linux y el dispositivo cliente. Para cargar archivos desde el dispositivo cliente al VDA de Linux, haga clic en el icono **Cargar** de la

barra de herramientas de la aplicación Citrix Workspace y seleccione el archivo deseado en los cuadros de diálogo de archivos. Para descargar archivos del VDA de Linux al dispositivo cliente, haga clic en el icono **Descargar**. Puede añadir archivos durante la carga o la descarga. Puede transferir hasta 10 archivos a la vez.



Nota:

Para cargar y descargar archivos entre el VDA de Linux y el dispositivo cliente, habilite la barra de herramientas de la aplicación Citrix Workspace. Puede usar una versión de la aplicación Citrix Workspace que le permita arrastrar y soltar archivos.

La descarga automática es una mejora para la transferencia de archivos. Los archivos que descargue o mueva al directorio **Guardar en mi dispositivo** del VDA se transfieren automáticamente al dispositivo cliente.

Nota:

La descarga automática requiere que las directivas **Transferencia de archivos para la aplicación Citrix Workspace para ChromeOS/HTML5** y **Descargar archivo para la aplicación Citrix Workspace para ChromeOS/HTML5** estén configuradas en **Permitido**.

Estos son algunos casos de uso para la descarga automática:

- Descargar archivos en **Guardar en mi dispositivo**

  En las sesiones de escritorios publicados y aplicaciones de navegador web, los archivos que descargue de sitios web se pueden guardar en el directorio **Guardar en mi dispositivo** del VDA para su transferencia automática al dispositivo cliente. Para lograr la descarga automática, establezca el directorio de descarga predeterminado del navegador web de la

sesión en **Guardar en mi dispositivo** y establezca un directorio de descarga local en el navegador web que ejecute su aplicación Citrix Workspace para HTML5 o para Chrome.

- Mover o copiar archivos a **Guardar en mi dispositivo**

  En las sesiones de escritorios publicados, elija los archivos de destino y muévalos o cópielos al directorio **Guardar en mi dispositivo** para que estén disponibles en el dispositivo cliente.

Directivas de transferencia de archivos

De forma predeterminada, la transferencia de archivos está habilitada. Utilice Citrix Studio para cambiar estas directivas, que se encuentran en **Configuración de usuario > ICA\Redirección de archivos**. Tenga en cuenta lo siguiente al utilizar las directivas de transferencia de archivos:

Transferencia de archivos para la aplicación Citrix Workspace para ChromeOS/HTML5: Permite o impide que los usuarios finales transfieran archivos entre la sesión de Citrix Virtual Apps and Desktops o la sesión de Citrix DaaS y el dispositivo del usuario final.

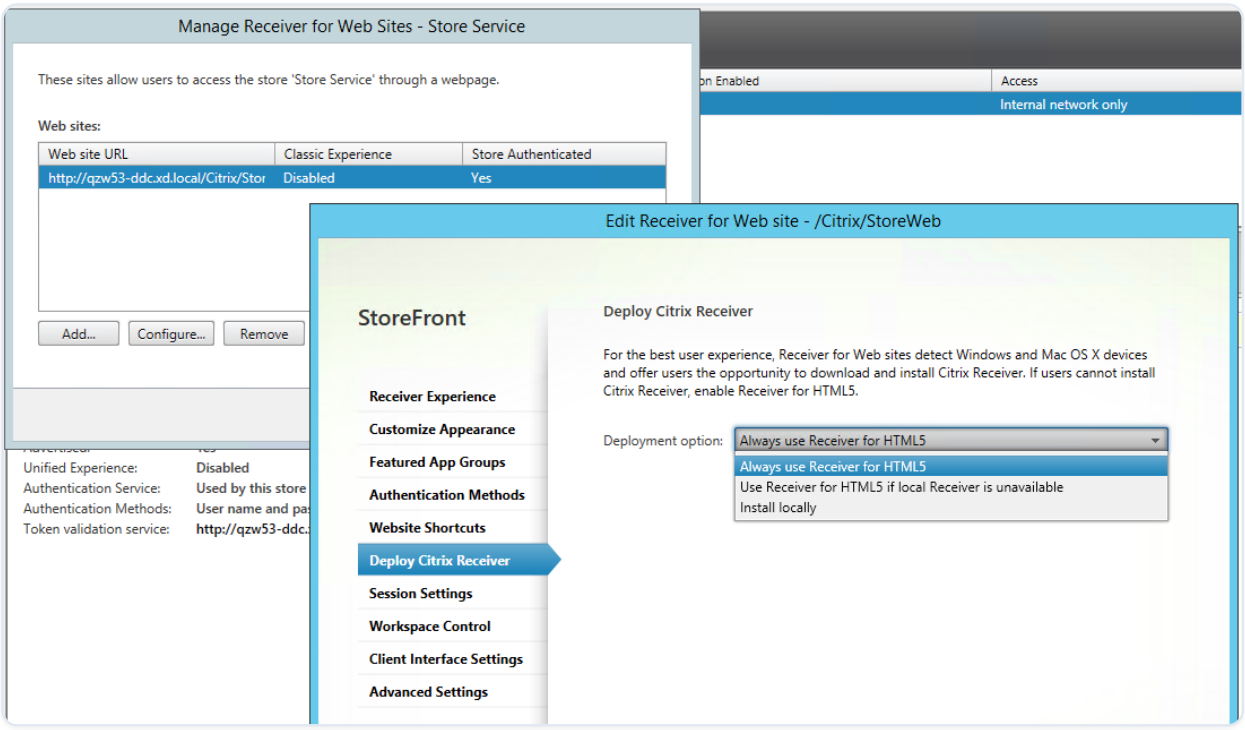
Cargar archivo para la aplicación Citrix Workspace para ChromeOS/HTML5: Permite o impide que los usuarios carguen archivos. Puede ser desde el dispositivo del usuario a una sesión de Citrix Virtual Apps and Desktops o a una sesión de Citrix DaaS.

Descargar archivo para la aplicación Citrix Workspace para ChromeOS/HTML5: Permite o impide que los usuarios descarguen archivos. Puede ser desde una sesión de Citrix Virtual Apps and Desktops o una sesión de Citrix DaaS al dispositivo del usuario.

Uso

Para usar la función de transferencia de archivos a través de la aplicación Citrix Workspace para HTML5:

1. En Citrix Studio, establezca la directiva **Conexiones de WebSockets** en **Permitido**.
2. En Citrix Studio, habilite la transferencia de archivos a través de las directivas de transferencia de archivos descritas anteriormente.
3. En la consola de administración de Citrix StoreFront, haga clic en **Tiendas**, seleccione el nodo **Administrar sitios de Receiver para Web** y habilite Citrix Receiver™ para HTML5 seleccionando la opción **Usar siempre Receiver para HTML5**.



4. Inicie un escritorio virtual o una sesión de aplicación de explorador web. Realice una o varias transferencias de archivos entre el VDA de Linux y su dispositivo cliente.

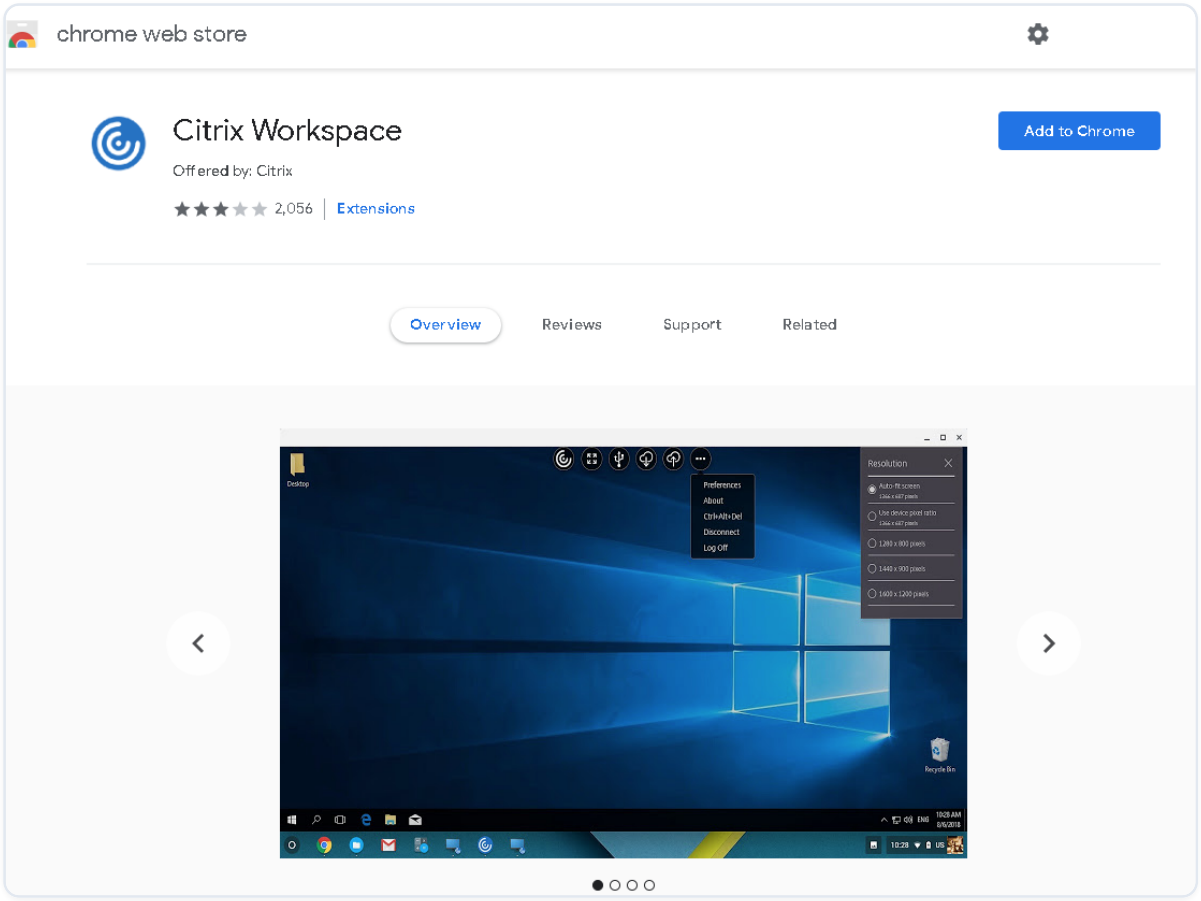
Para usar la función de transferencia de archivos a través de la aplicación Citrix Workspace para Chrome:

1. Habilite la transferencia de archivos a través de las directivas de transferencia de archivos descritas anteriormente.
2. Obtenga la aplicación Citrix Workspace de Chrome Web Store.

   Omita este paso si ya ha agregado la aplicación Citrix Workspace para Chrome a la página Aplicaciones de Chrome.

   a. Escriba **Citrix Workspace para Chrome** en el cuadro de búsqueda de Google Chrome. Haga clic en el icono de búsqueda.

   b. Entre los resultados de búsqueda, haga clic en la URL de Chrome Web Store donde está disponible la aplicación Citrix Workspace.



c. Haga clic en **Añadir a Chrome** para agregar la aplicación Citrix Workspace a Google Chrome.

3. Haga clic en la aplicación Citrix Workspace para Chrome en la página Aplicaciones de Chrome.
4. Introduzca la URL de su tienda StoreFront™ para conectarse.

   Omita este paso si ya introdujo la URL anteriormente.
5. Inicie una sesión de escritorio virtual o de aplicación. Realice una o varias transferencias de archivos entre el VDA de Linux y su dispositivo cliente.

Gráficos

Esta sección contiene los siguientes temas:

- Escalado automático de PPP
- Visualización del estado de la batería del cliente
- Configuración y ajuste de gráficos
- Uso compartido de pantalla HDX
- GPU no virtualizadas

- Marca de agua de sesión
- Visualización progresiva de Thinwire

Escalado automático de PPP

El VDA de Linux admite el escalado automático de PPP. Cuando un usuario abre un escritorio virtual o una sesión de aplicación, el valor de PPP de la sesión cambia automáticamente para coincidir con la configuración de PPP del lado del cliente.

A continuación, se presentan algunas consideraciones relacionadas con esta función:

- La función requiere que habilite la coincidencia de PPP para Citrix Workspace. En el caso de la aplicación Citrix Workspace para Windows, asegúrese de que la opción **No, usar la resolución nativa** esté seleccionada. Para obtener más información sobre cómo configurar el escalado de PPP para la aplicación Citrix Workspace para Windows, consulte Escalado de PPP.
- Para que la función funcione en escenarios de varios monitores, cada monitor debe configurarse con la misma configuración de PPP. No se admiten escenarios de PPP mixtos. Si los monitores están configurados con diferentes ajustes de PPP, el VDA de Linux aplica el valor de PPP más pequeño para todas las pantallas.
- La función está habilitada para MATE, GNOME, GNOME Classic y KDE. Al usar KDE o MATE, tenga en cuenta lo siguiente:
    - Para escritorios virtuales Linux que se ejecutan en un entorno de escritorio KDE:
        - Recomendamos usar KDE Plasma 5 o posterior.
        - Cambiar la configuración de PPP en el lado del cliente mientras las sesiones están en ejecución requiere que los usuarios cierren la sesión y vuelvan a iniciarla.
    - Para escritorios virtuales Linux que se ejecutan en un entorno de escritorio MATE:
        - Solo se admiten factores de escala de 1 y 2.
        - Cambiar la configuración de PPP en el lado del cliente mientras las sesiones están en ejecución requiere que los usuarios cierren la sesión y vuelvan a iniciarla.
- El valor de PPP de la sesión virtual cambia automáticamente según la configuración de PPP del lado del cliente. Actualmente, la función solo admite factores de escala de tipo entero, por ejemplo, 100% y 200%. Si el factor de escala configurado en el lado del cliente es de tipo

fraccional, el PPP de la sesión virtual cambia a un factor de escala entero según la siguiente tabla. Ejemplo: Si el factor de escala es 125%, el valor de PPP cambia a 100%.

FACTOR DE ESCALA DEL LADO DEL CLIENTE	PPP DE LA SESIÓN REMOTA	ESCALADO DE PANTALLA
Inferior o igual al 174%	96 (1 x 96)	100%
175%–274%	192 (2 x 96)	200%
275%–399%	288 (3 x 96)	300%
Superior o igual al 400%	384 (4 x 96)	400%

Nota:

El VDA de Linux admite un escalado de hasta el 200% para escritorios MATE.

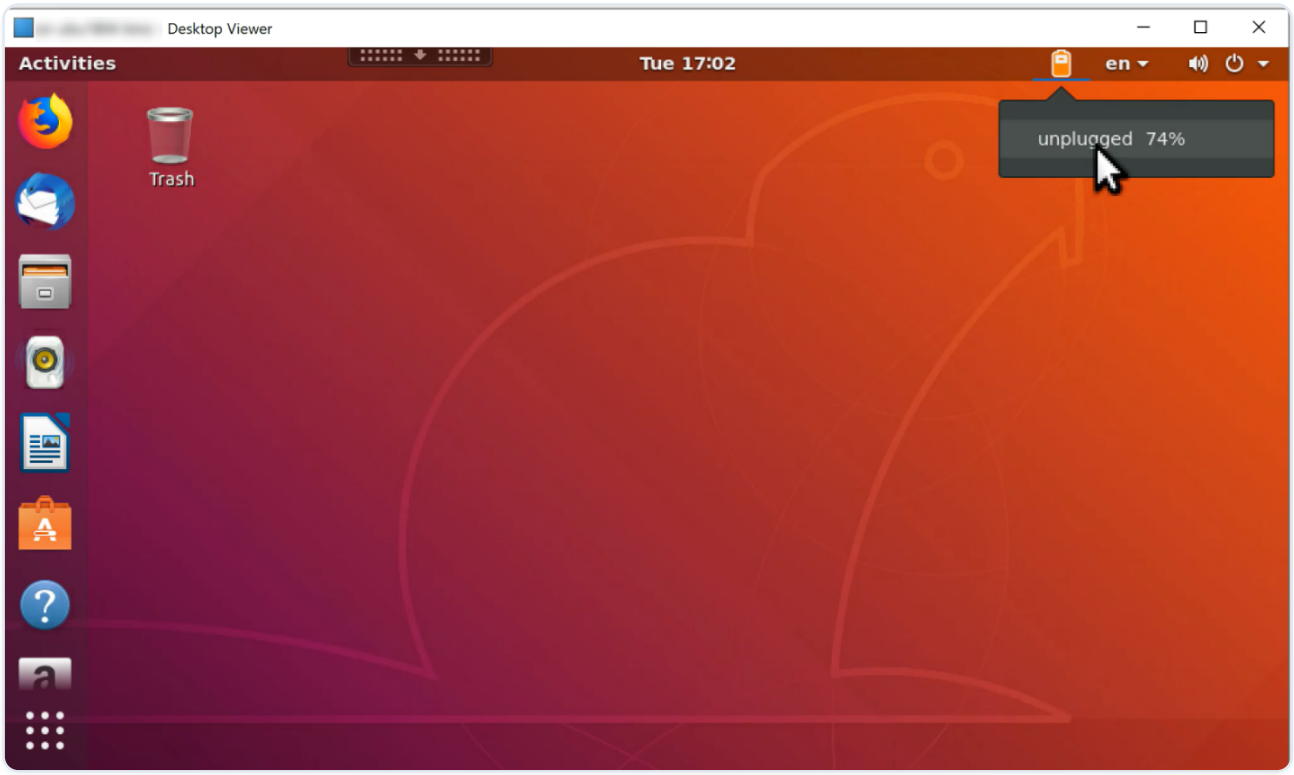
Visualización del estado de la batería del cliente

El VDA de Linux puede redirigir y mostrar el estado de la batería de los dispositivos cliente en escritorios virtuales. Esta función está habilitada de forma predeterminada y está disponible para las siguientes versiones de la aplicación Citrix Workspace™:

- Aplicación Citrix Workspace para iOS
- Aplicación Citrix Workspace para Linux
- Aplicación Citrix Workspace para Mac (la versión 2204.1 no es compatible)
- Aplicación Citrix Workspace para Windows (la versión 2204.1 no es compatible)

Información general

Cuando los usuarios abren un escritorio virtual, pueden ver un icono de batería en la bandeja del sistema de Linux. El icono de batería indica el estado de la batería de sus dispositivos cliente. Para comprobar el porcentaje de duración restante de la batería, haga clic en el icono de batería. Por ejemplo, consulte la siguiente captura de pantalla:



Los diferentes iconos de batería indican diferentes estados de la batería. Para obtener una descripción general, consulte la siguiente tabla:

ICONO DE BATERÍA	ESTADO DE CARGA	NIVEL DE DURACIÓN RESTANTE DE LA BATERÍA	PORCENTAJE DE DURACIÓN RESTANTE DE LA BATERÍA
	Cargando, indicado con un símbolo "+"	Alto, indicado con un color verde	>=80%
	Cargando, indicado con un símbolo "+"	Medio, indicado con un color ámbar	>=20% y <80%
	Cargando, indicado con un símbolo "+"	Bajo, indicado con un color rojo	< 20%
	No cargando, indicado con un símbolo "-"	Alto, indicado con un color verde	>=80%
	No cargando, indicado con un símbolo "-"	Medio, indicado con un color ámbar	>=20% y <80%

ICONO DE BATERÍA	ESTADO DE CARGA	NIVEL DE DURACIÓN RESTANTE DE LA BATERÍA	PORCENTAJE DE DURACIÓN RESTANTE DE LA BATERÍA
	No se está cargando, indicado con un símbolo "-"	Bajo, indicado con color rojo	< 20%
	Desconocido	Desconocido	Desconocido

Configuración

La visualización del estado de la batería del cliente está habilitada de forma predeterminada.

Para inhabilitar la función, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

Para habilitar la función, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000001"
```

Nota:

Los comandos anteriores afectan a la función teclado en pantalla, que comparte el canal virtual de Mobile Receiver (MRVC) con la visualización del estado de la batería del cliente.

Según su distribución, complete los pasos adicionales para habilitar la función. Para obtener más información, consulte la sección Habilitar la bandeja del sistema.

Configuración y ajuste de gráficos

Este artículo describe la configuración y el ajuste de gráficos de Linux VDA.

Para obtener más información, consulte Requisitos del sistema y la sección Información general de la instalación.

Configuración

Optimizar para cargas de trabajo de gráficos 3D

Esta configuración establece los valores predeterminados adecuados que mejor se adaptan a las cargas de trabajo con uso intensivo de gráficos. Habilite esta configuración para los usuarios cuya carga de trabajo se centre en aplicaciones con uso intensivo de gráficos. Aplique esta directiva solo en los casos en que haya una GPU disponible para la sesión. Cualquier otra configuración que anule explícitamente la configuración predeterminada establecida por esta directiva tendrá prioridad.

De forma predeterminada, **Optimizar para cargas de trabajo de gráficos 3D** está inhabilitado.

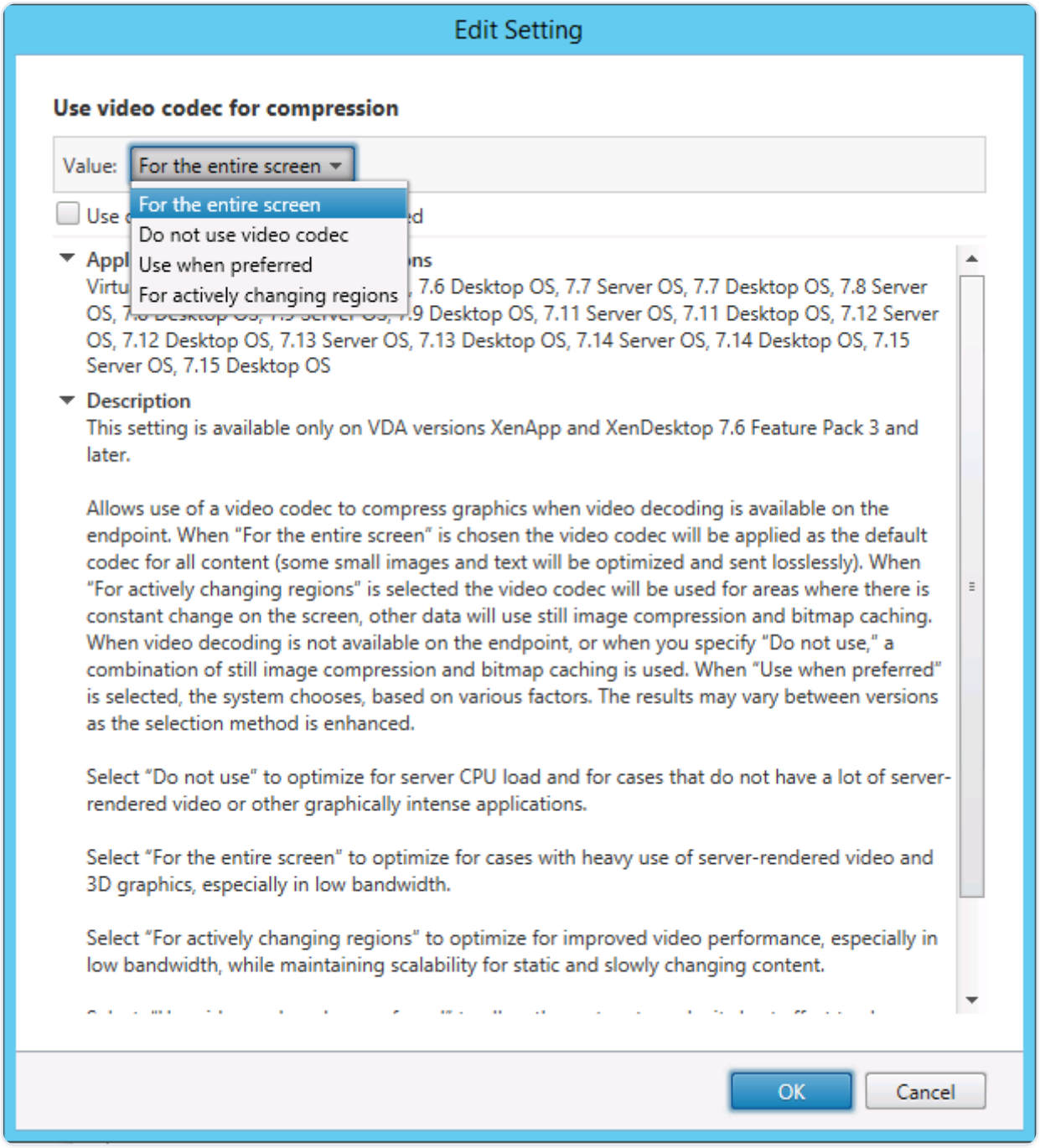
Códec de vídeo para la compresión

Thinwire es la tecnología de visualización remota utilizada en Linux VDA. Esta tecnología permite que los gráficos generados en una máquina se transmitan, normalmente a través de una red, a otra máquina para su visualización.

La directiva de gráficos Usar códec de vídeo para la compresión establece el modo de gráficos predeterminado y ofrece las siguientes opciones para diferentes casos de uso:

- **Usar cuando se prefiera**. Esta configuración es la predeterminada. No se requiere ninguna configuración adicional. Garantiza que Thinwire se seleccione para todas las conexiones de Citrix® y se optimice para la escalabilidad, el ancho de banda y una calidad de imagen superior para las cargas de trabajo de escritorio típicas.
- **Para toda la pantalla**. Ofrece Thinwire con H.264 o H.265 de pantalla completa para optimizar la experiencia del usuario y el ancho de banda, especialmente en casos de uso intensivo de gráficos 3D. La Marca de agua de sesión es compatible cuando se selecciona **Para toda la pantalla**, o cuando se selecciona **Usar cuando se prefiera** y se habilita Optimizar para cargas de trabajo de gráficos 3D.
- **Para regiones que cambian activamente**. La tecnología de visualización adaptativa de Thinwire identifica las imágenes en movimiento (vídeo, 3D en movimiento). Utiliza AV1, H.265 o H.264 solo en la parte de la pantalla donde la imagen se está moviendo. El uso selectivo del códec de vídeo AV1, H.265 o H.264 permite a HDX Thinwire detectar y codificar las partes de la pantalla que se actualizan con frecuencia. La compresión de imágenes fijas (JPEG, RLE) y el almacenamiento en caché de mapas de bits se siguen utilizando para el resto de la pantalla, incluido el texto y las imágenes fotográficas. Los usuarios obtienen el beneficio de un menor

consumo de ancho de banda y una mejor calidad para el contenido de vídeo, combinado con texto sin pérdidas o imágenes de alta calidad en otros lugares. El uso selectivo de AV1 y H.265 no es compatible cuando la directiva **Calidad visual** está establecida en **Siempre sin pérdidas** o **Compilar sin pérdidas**.



Algunas otras configuraciones de directiva, incluidas las siguientes configuraciones de directiva de visualización, se pueden utilizar para ajustar el rendimiento de la visualización remota:

- **Profundidad de color preferida para gráficos sencillos**
- **Velocidad de fotogramas de destino**
- **Calidad visual**

Codificación por hardware AV1/H.265/H.264

La directiva **Usar codificación por hardware para códec de vídeo** permite el uso de la aceleración por hardware de la GPU, si está disponible, para comprimir elementos de la pantalla con el códec de vídeo. La aceleración por hardware de la GPU optimiza la utilización de los recursos de hardware y mejora en gran medida el rendimiento de los fotogramas por segundo (FPS).

La aceleración por hardware de la GPU cubre todos los modos gráficos establecidos por la directiva **Usar códec de vídeo para la compresión**:

- **Usar cuando se prefiera**
- **Para toda la pantalla**
- **Para regiones que cambian activamente**

Para habilitar la compresión de vídeo por hardware, siga estos pasos:

1. Establezca la directiva **Usar codificación por hardware para códec de vídeo** en **Habilitado**.
2. Establezca **Usar códec de vídeo para la compresión** en **Usar cuando se prefiera**, **Para toda la pantalla** o **Para regiones que cambian activamente**. Asegúrese de que no esté establecido en **No usar códec de vídeo**.

Para que sea utilizable, el códec de vídeo AV1 o H.265 debe ser compatible y estar habilitado tanto en el VDA como en la aplicación Citrix Workspace. AV1 tiene preferencia sobre H.265 y H.264 durante la negociación del códec. Cuando AV1 no es compatible, se negocia H.265. Si AV1 y H.265 no son compatibles, las sesiones recurren al uso del códec de vídeo H.264. Si el hardware de la GPU no está disponible, el VDA recurre a la codificación basada en CPU utilizando el códec de vídeo por software.

REQUISITOS PARA LA CODIFICACIÓN POR HARDWARE AV1

VDA

- VDA: 2311 o posterior
- GPU: **NVIDIA Ada Lovelace o posterior** (Para ver una matriz de los códecs de vídeo compatibles con las GPU de NVIDIA, consulte el documento de NVIDIA en `<https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new>`.)
- Controlador de gráficos NVIDIA 522.25 o posterior (Video Codec SDK v12.0)

Cliente

- Aplicación Citrix Workspace™ 2305 para Windows o posterior

- GPU de cliente compatible con la decodificación AV1:
  - NVIDIA Ampere o posterior
  - Intel 11.ª generación / Arc o posterior
  - Serie AMD Radeon RX 6000 / Radeon Pro W6000 (RDNA2) o posterior

REQUISITOS PARA LA CODIFICACIÓN DE HARDWARE H.265

Cliente

- Citrix Receiver para Windows 4.10 a 4.12
- Citrix Workspace app 1808 para Windows y versiones posteriores

Para habilitar la codificación de hardware H.265 en su cliente, consulte Codificación de vídeo H.265.

Compresión sin pérdidas H.265/H.264

La compresión sin pérdidas H.265/H.264 está disponible para la aceleración de hardware HDX 3D PRO mediante GPU NVIDIA. La compresión sin pérdidas H.265 requiere la aplicación Citrix Workspace 2305 para Windows y versiones posteriores. La compresión sin pérdidas H.264 requiere los siguientes clientes:

- Aplicación Citrix Workspace 2303 para Windows y versiones posteriores
- Aplicación Citrix Workspace 2301 para Mac y versiones posteriores con el chip Apple M1

Para habilitar la compresión sin pérdidas H.265/H.264, siga estos pasos:

1. Establezca la directiva **Usar codificación de hardware para códec de vídeo** en **Habilitado**.
2. Establezca la directiva **Usar códec de vídeo para la compresión** en **Para toda la pantalla**.
3. Establezca la política de **Calidad visual** en **Siempre con pérdidas** o **Compilación sin pérdidas**.

Permitir compresión visualmente sin pérdidas

La política **Permitir compresión visualmente sin pérdidas** permite usar la compresión **visualmente** sin pérdidas en lugar de la compresión verdaderamente sin pérdidas para los gráficos. La compresión visualmente sin pérdidas mejora el rendimiento en comparación con la compresión verdaderamente sin pérdidas, pero tiene una pérdida menor que es imperceptible a la vista. Esta configuración cambia la forma en que se utilizan los valores de la configuración de **Calidad visual**.

La política **Permitir compresión visualmente sin pérdidas** está inhabilitada de forma predeterminada. Para habilitar la compresión **visualmente** sin pérdidas, establezca **Permitir compresión visualmente sin pérdidas** en **Habilitado** y la política de **Calidad visual** en **Compilación sin pérdidas**.

Si la política **Usar códec de vídeo para la compresión** está establecida en **No usar códec de vídeo**, la compresión **visualmente** sin pérdidas se aplica a la codificación de imágenes estáticas. Si la política **Usar códec de vídeo para la compresión** está establecida en un modo gráfico distinto de **No usar códec de vídeo**, la compresión **visualmente** sin pérdidas se aplica a la codificación H.264.

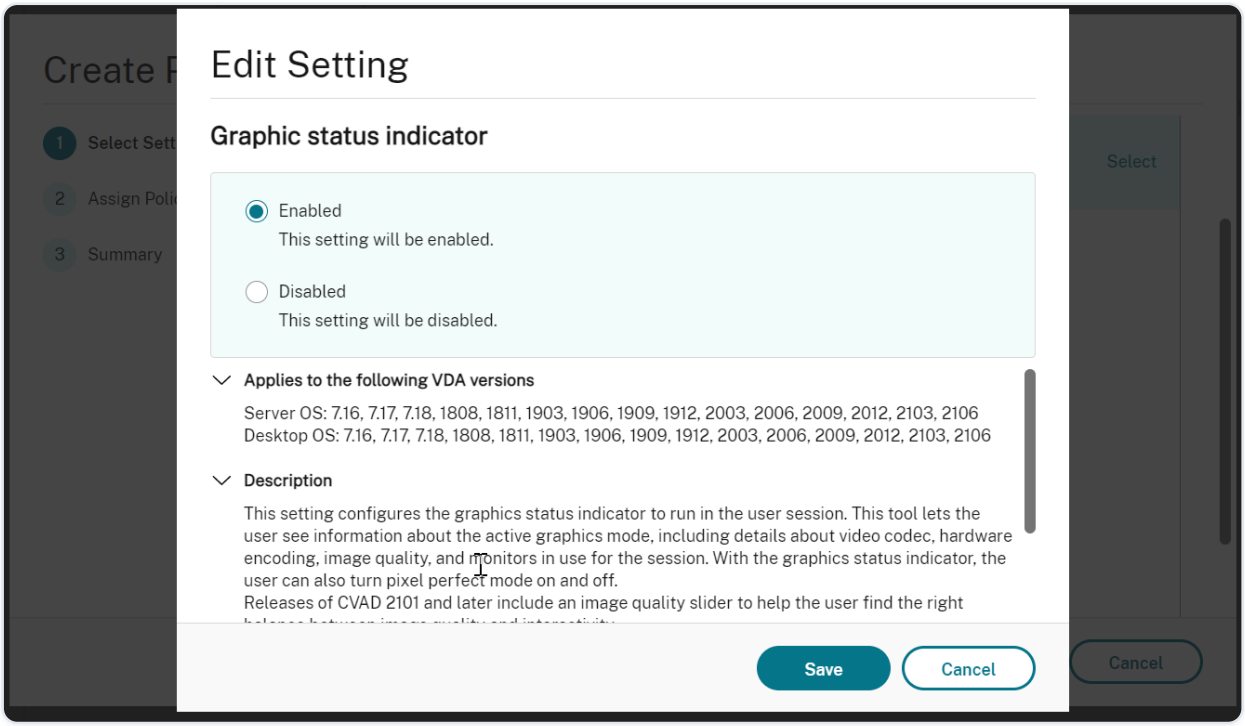
Para obtener más información sobre la configuración de las políticas de **Calidad visual** y **Usar códec de vídeo para la compresión**, consulte Configuración de la política de visualización y Configuración de la política de gráficos.

Control deslizante de calidad de gráficos

Hemos incluido un control deslizante de calidad de gráficos en la herramienta de indicador de estado de gráficos que se ejecuta en sus sesiones virtuales de Linux. El control deslizante ayuda a encontrar el equilibrio adecuado entre la calidad de imagen y la interactividad.

Para usar el control deslizante, siga estos pasos:

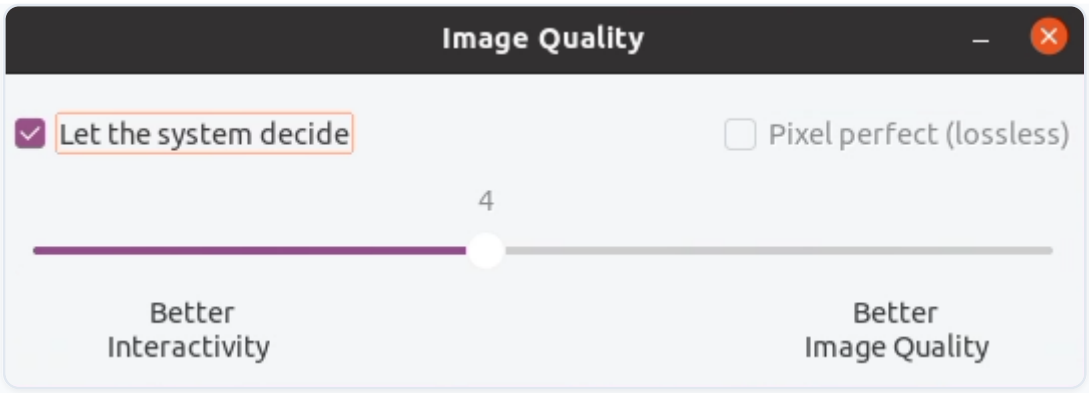
1. Habilite la política de **Indicador de estado gráfico** en Citrix Studio.



2. Abra el Terminal y ejecute el comando `ctxslider`. Aparece la interfaz de usuario del control deslizante.

   Nota:

   - Si ha establecido la política de **Calidad visual** en **Siempre sin pérdidas** o **Compilación sin pérdidas**, la interfaz de usuario del control deslizante no se muestra.
   - Puede iniciar la interfaz de usuario del control deslizante tanto desde el Terminal como desde la bandeja del sistema.

   Las siguientes opciones están ahora disponibles:

   - Para cambiar la calidad de imagen, mueva el control deslizante. El control deslizante admite un rango de 0 a 9.
   - Para usar la configuración definida por el sistema, seleccione **Dejar que el sistema decida**.
   - Para cambiar al modo sin pérdidas, seleccione **Píxel perfecto**.

Ajustar las tasas de bits promedio según las estimaciones de ancho de banda

Citrix mejora la codificación de hardware HDX™ 3D Pro ajustando las tasas de bits promedio según las estimaciones de ancho de banda.

Cuando se utiliza la codificación de hardware HDX 3D Pro, el VDA puede estimar intermitentemente el ancho de banda de la red y ajustar las tasas de bits de los fotogramas codificados en consecuencia. Esta nueva función proporciona un mecanismo para equilibrar la nitidez y la fluidez.

Esta función está habilitada de forma predeterminada. Para deshabilitarla, ejecute el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "DisableReconfigureEncoder" -d "0x00000001" --force
```

Además de usar esta función, también puede ejecutar los siguientes comandos para ajustar la nitidez y la fluidez. Los parámetros **AverageBitRatePercent** y **MaxBitRatePercent** establecen el porcentaje de uso del ancho de banda. Cuanto más altos sean los valores que establezca, más nítidos serán los gráficos y menor la fluidez. El rango de configuración recomendado es 50-100.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "AverageBitRatePercent" -d "90" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "MaxBitRatePercent" -d "100" --force
```

En el ajuste de la tasa de bits promedio, cuando la pantalla permanece inmóvil, el fotograma más reciente se mantiene en un estado de baja calidad porque no se envían nuevos fotogramas. La compatibilidad con el enfoque puede solucionar este problema reconfigurando y enviando inmediatamente el fotograma más reciente con la máxima calidad.

Para obtener una lista completa de las directivas compatibles con Linux VDA Thinwire, consulte Lista de compatibilidad de directivas.

Para obtener información sobre la configuración de la compatibilidad con varios monitores en Linux VDA, consulte CTX220128.

Procesamiento paralelo

Thinwire puede mejorar el número de fotogramas por segundo (FPS) al paralelizar ciertas tareas, con el coste de un consumo de CPU general ligeramente mayor. Esta función está deshabilitada de forma predeterminada. Para habilitar la función, ejecute el siguiente comando en su VDA:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"ParallelProcessing" -d "0x00000001" --force
```

Solución de problemas

Comprobar qué modo gráfico está en uso

Ejecute el siguiente comando para comprobar qué modo gráfico está en uso (**0** significa TW+. **1** significa códec de vídeo de pantalla completa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

El resultado se parece a:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000000" --force`

verificar que AV1 está en uso

> **Nota:**

> Para verificar qué códec de vídeo se está utilizando en la sesión actual, ejecute un comando de los que se proporcionan a continuación o compruebe el estado de los gráficos a través de la bandeja del sistema.

> Ejecute el siguiente comando para verificar que AV1 está en uso (**0** significa que no está en uso. **1** significa que está en uso):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep AV1
```

Por ejemplo, el resultado puede ser similar a:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "AV1" -d "0x00000000" --force`

verificar que H.265 está en uso

Ejecute el siguiente comando para verificar que H.265 a pantalla completa está en uso (**0** significa que no está en uso. **1** significa que está en uso):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Por ejemplo, el resultado puede ser similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H265" -d "0x00000000" --force
```

verificar que H.264 está en uso

Ejecute el siguiente comando para verificar que H.264 está en uso (**0** significa que no está en uso. **1** significa que está en uso):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

Por ejemplo, el resultado puede ser similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000000" --force
```

Comprobar qué esquema de codificación YUV está en uso

Ejecute el siguiente comando para comprobar qué esquema de codificación YUV está en uso (**0** significa YUV420. **1** significa YUV422. **2** significa YUV444):

> **Nota:**
>
> El valor de **YUVFormat** solo tiene sentido cuando se utiliza un códec de vídeo.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

Por ejemplo, el resultado puede ser similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000000" --force
```

verificar que la codificación de software YUV444 está en uso

Ejecute el siguiente comando para verificar que la codificación de software YUV444 está en uso:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

Cuando YUV444 está en uso, el resultado es similar a:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000001" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000001" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000000" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000002" --force`

verificar que HDX 3D Pro está habilitado

Ejecute los siguientes comandos para verificar que HDX 3D Pro está habilitado:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep ProductEdition



sudo /opt/Citrix/VDA/bin/ctxreg dump | grep StackSessionMode



sudo /opt/Citrix/VDA/bin/ctxreg dump | grep 3DPro
```

Cuando HDX 3D Pro está habilitado, el resultado es similar a:

`create -k "HKLM\Software\Citrix\VirtualDesktopAgent\State" -t "REG_SZ" -v "ProductEdition" -d "<PLT or ENT>" --force`

`create -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "StackSessionMode" -d "0x00000000" --force`

`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "3DPro" -d "0x00000000" --force`

Para verificar que las bibliotecas NVIDIA necesarias están cargadas para HDX 3D Pro, ejecute el comando **nvidia-smi** en el VDA de Linux. El resultado es similar a:

```
Tue Apr 12 10:42:03 2016

+-----------------------------------------------------+

| NVIDIA-SMI 361.28     Driver Version: 361.28         |

|-------------------------------+----------------------
+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr.
ECC |

| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute
M. |

|
===============================+======================+==================
===|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
N/A |

| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
Default |

+-------------------------------+----------------------
+----------------------+



+-----------------------------------------------------------------------------
----+

| Processes:                                                       GPU
Memory |

|  GPU       PID  Type  Process name
```

```
Usage      |

|
=============================================================================
===|

|    0      2164  C+G   /usr/local/bin/ctxgfx
106MiB |

|    0      2187    G   Xorg
85MiB |

+-----------------------------------------------------------------------------
----+
```

verificar que la codificación de hardware está en uso para 3D Pro

Ejecute el siguiente comando (**0** significa que no está en uso. **1** significa que está en uso):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
```

Cuando 3D Pro está en uso, el resultado es similar a:

`create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --force`

verificar que el controlador de gráficos NVIDIA GRID está instalado correctamente

Para verificar que el controlador de gráficos NVIDIA GRID está instalado correctamente, ejecute **nvidia-smi**. El resultado es similar a:

```
+-----------------------------------------------------+

| NVIDIA-SMI 352.70     Driver Version: 352.70         |

|-------------------------------+----------------------
+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr.
ECC |

| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute
M. |
```

```
|
==============================+======================+==================
===|

|   0  Tesla M60           Off  | 0000:00:05.0     Off |
Off |

| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
Default |

+------------------------------+----------------------
+----------------------+



+-----------------------------------------------------------------------------
----+

| Processes:                                                                GPU
Memory |

|  GPU       PID  Type  Process name
Usage      |

|
=============================================================================
===|

|  No running processes found
                                 |

+-----------------------------------------------------------------------------
----+
```

Establezca la configuración correcta para la tarjeta:

`etc/X11/ctx-nvidia.sh`

Problemas de redibujado en varios monitores de HDX 3D Pro

Si observa problemas de redibujado en pantallas que no son el monitor principal, compruebe que la licencia de NVIDIA GRID esté disponible.

Comprobar los registros de errores de Xorg

El archivo de registro de Xorg se denomina de forma similar a **Xorg.{DISPLAY}.log** en la carpeta **/var/log/**.

Problemas conocidos y limitaciones

Para vGPU, la consola local de XenServer (anteriormente Citrix Hypervisor™) muestra la pantalla de la sesión de escritorio de ICA

Solución alternativa: inhabilite la consola VGA local de la VM ejecutando el siguiente comando:

```
[root@xenserver® ~]# xe vgpu-param-set uuid=vgpu-uuid
extra_args=disable_vnc=1
```

Las ventanas emergentes del escritorio Gnome 3 son lentas al iniciar sesión

Es una limitación del inicio de sesión de escritorio de Gnome 3.

Algunas aplicaciones OpenGL/WebGL no se renderizan bien al cambiar el tamaño de la ventana de la aplicación Citrix Workspace

Al cambiar el tamaño de la ventana de la aplicación Citrix Workspace, se modifica la resolución de la pantalla. El controlador propietario de NVIDIA cambia algunos estados internos y puede requerir que las aplicaciones respondan en consecuencia. Por ejemplo, el elemento de la biblioteca WebGL **lightgl.js** podría generar un error que diga **Rendering to this texture is not supported (incomplete frame buffer)**.

Uso compartido de pantalla de HDX™

Información general

El VDA de Linux le permite compartir la pantalla de su escritorio virtual con los usuarios de la sesión en otros escritorios virtuales.

Nota:

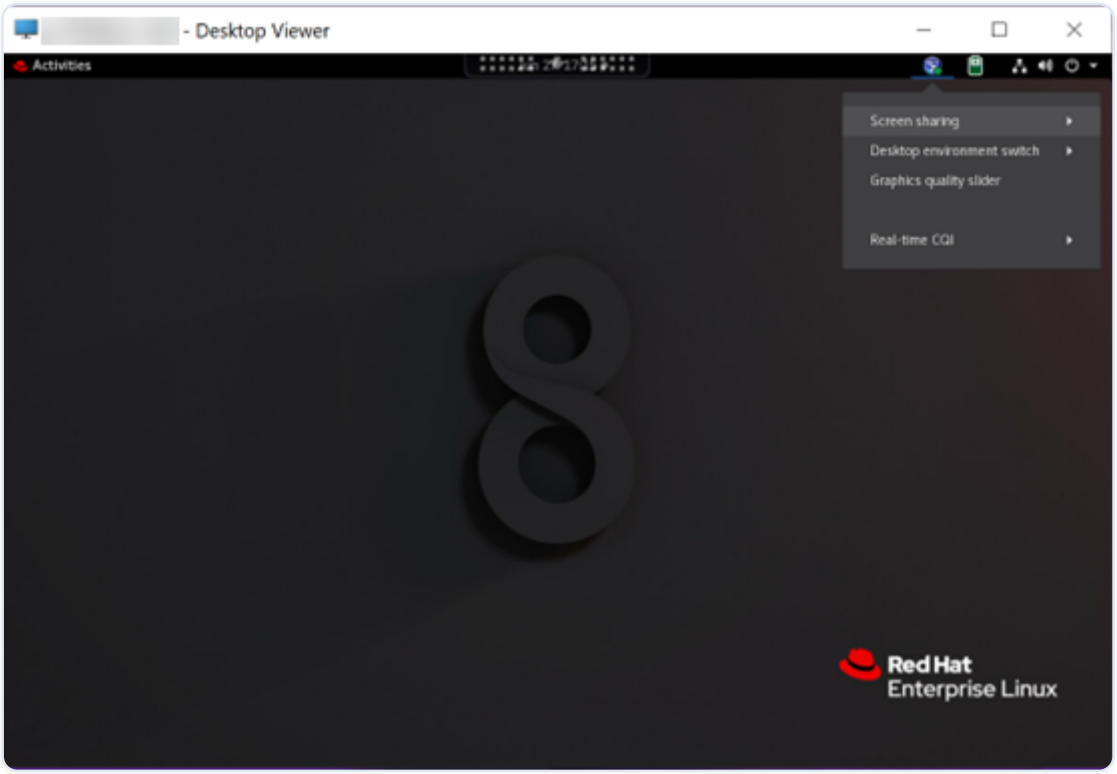
- Si el uso compartido de sesiones se produce entre varios VDA de Linux, se recomienda actualizar a la misma versión de VDA para evitar problemas de entrada de teclado.
- Si existen diferentes distribuciones de teclado entre la sesión del visor y la sesión del que comparte, la distribución de teclado del que comparte es la efectiva.

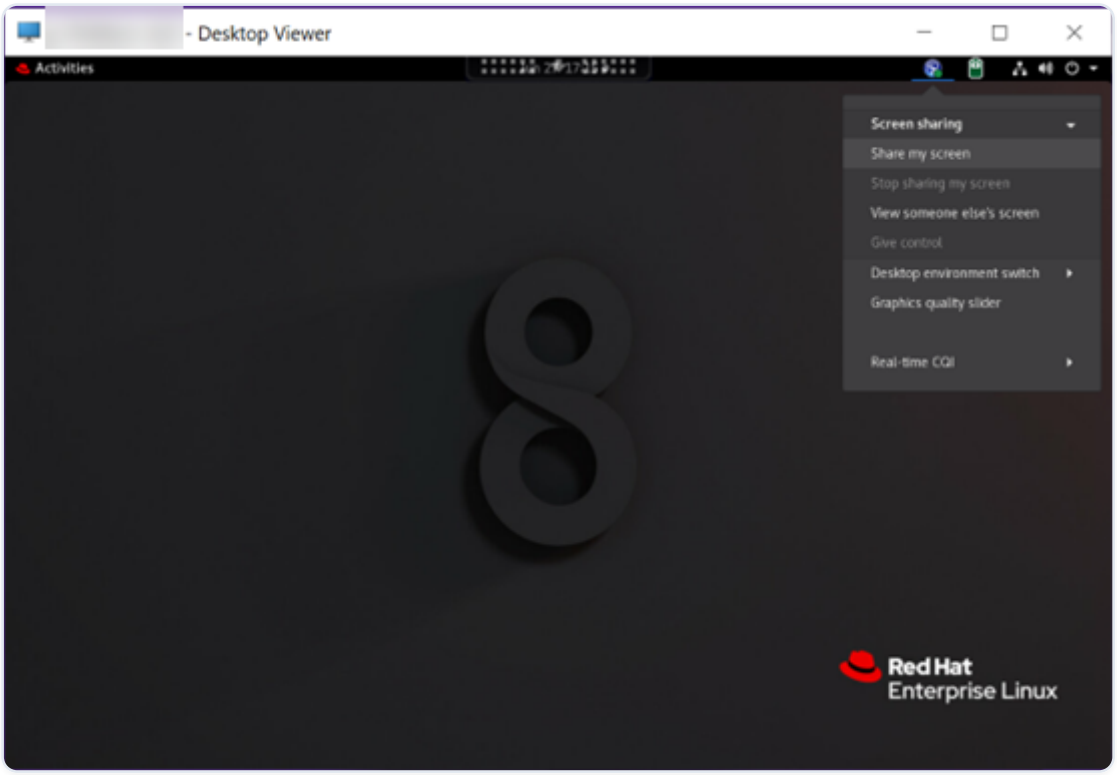
- Se recomienda que la aplicación Citrix Workspace™ del visor utilice el modo Scancode, ya que hay más limitaciones al usar el modo Unicode.
- El modo Unicode en el cliente de la aplicación Citrix Workspace puede provocar que algunos caracteres no se reconozcan.
- Al usar el modo Unicode, se recomienda que el que comparte y el visor utilicen la misma distribución de teclado para evitar una salida mixta.
- Si las combinaciones de teclas de acceso directo están activas tanto en el visor como en el que comparte, solo surten efecto en el visor.
- Si una tecla de acceso directo incluye la tecla Super, surte efecto en el visor y también se envía al que comparte.

El siguiente ejemplo le guía a través del procedimiento de compartir una pantalla y ver la pantalla de otra persona.

Para compartir una pantalla:

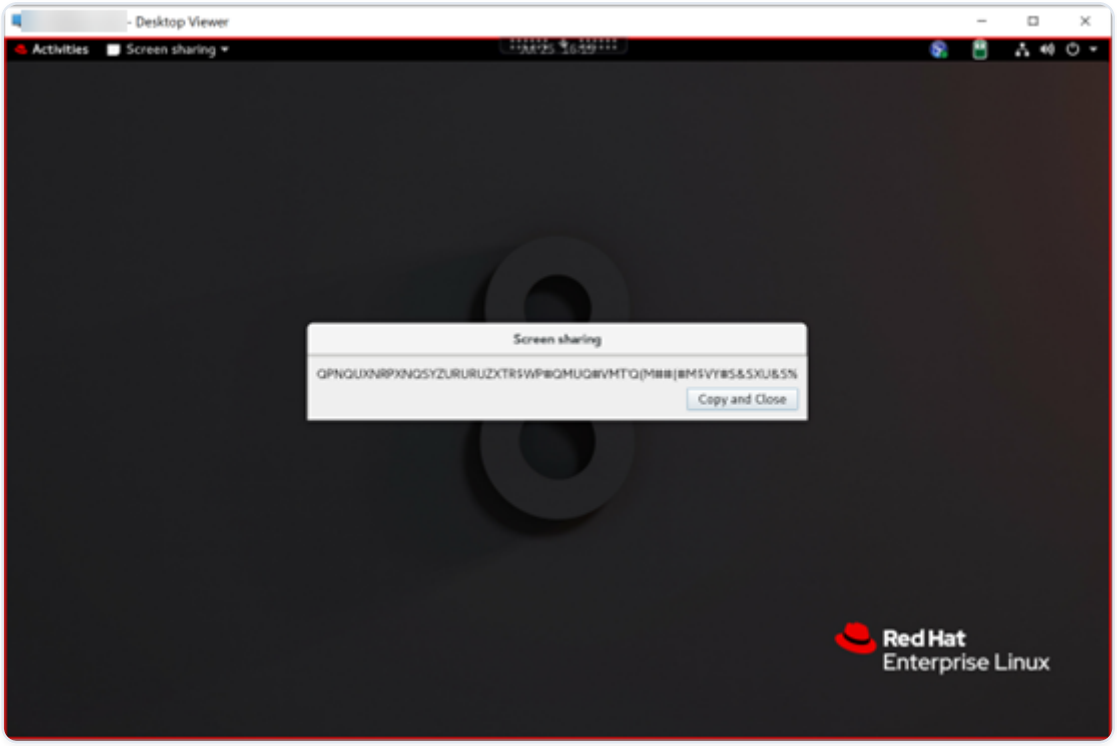
1. En el área de notificación de su escritorio virtual, haga clic en el siguiente icono de la bandeja del sistema y seleccione **Uso compartido de pantalla > Compartir mi pantalla**.





2. Haga clic en **Copiar y cerrar**.

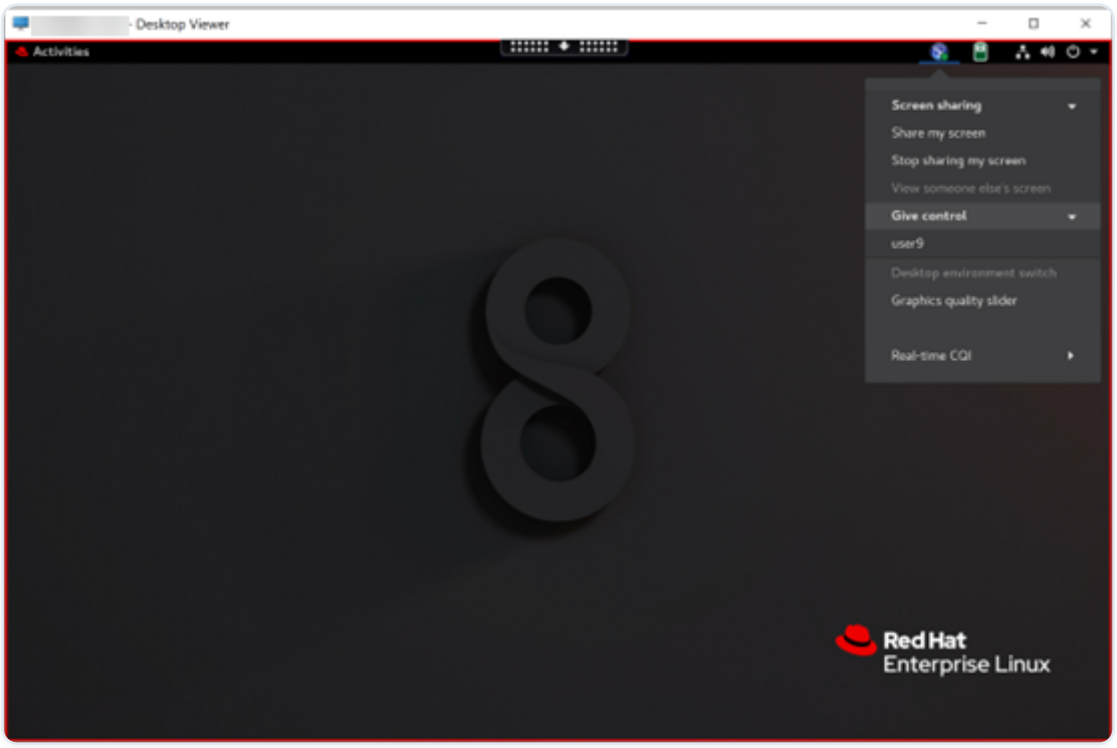
   El código actual para compartir pantalla persiste hasta que detenga y reinicie el uso compartido de su pantalla.



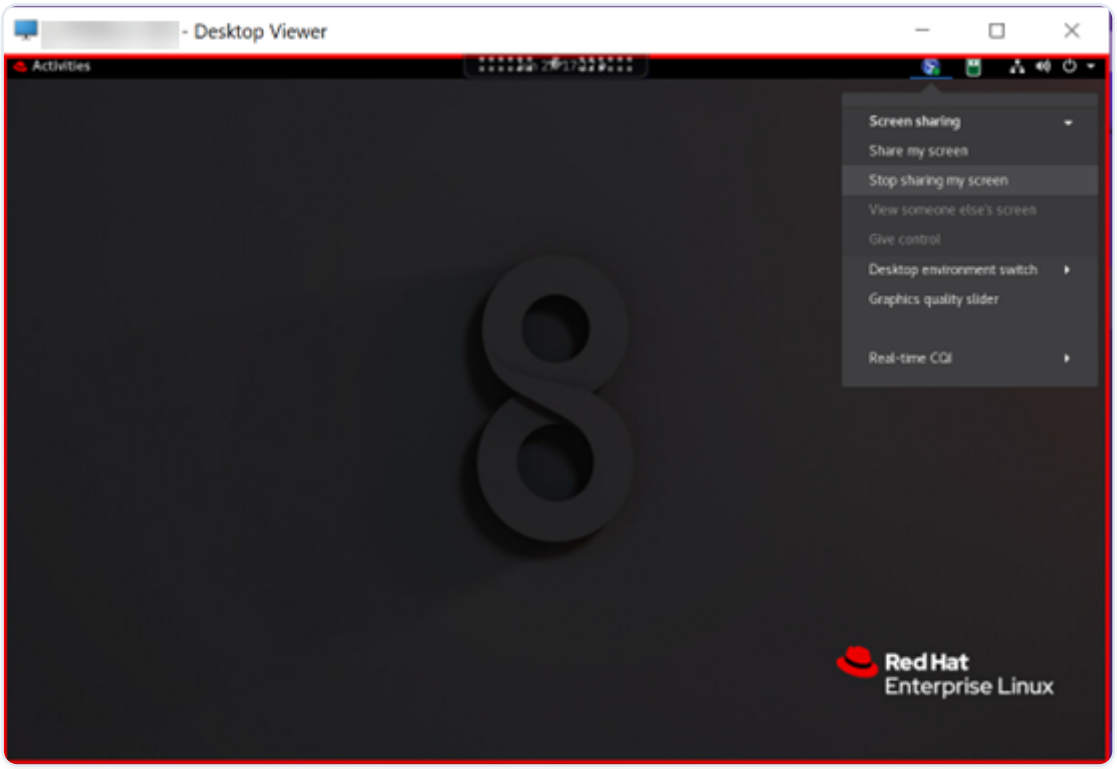
Sugerencia:

> Mientras comparte la pantalla, aparece un borde rojo alrededor de esta, lo que indica que se está compartiendo.

3. Comparta el código copiado con los usuarios de la sesión en otros escritorios virtuales con los que quiera compartir la pantalla.
4. Para permitir que un visor controle su pantalla, seleccione **Dar control** y, a continuación, el nombre del visor. Para dejar de dar control, desactive el nombre del visor.

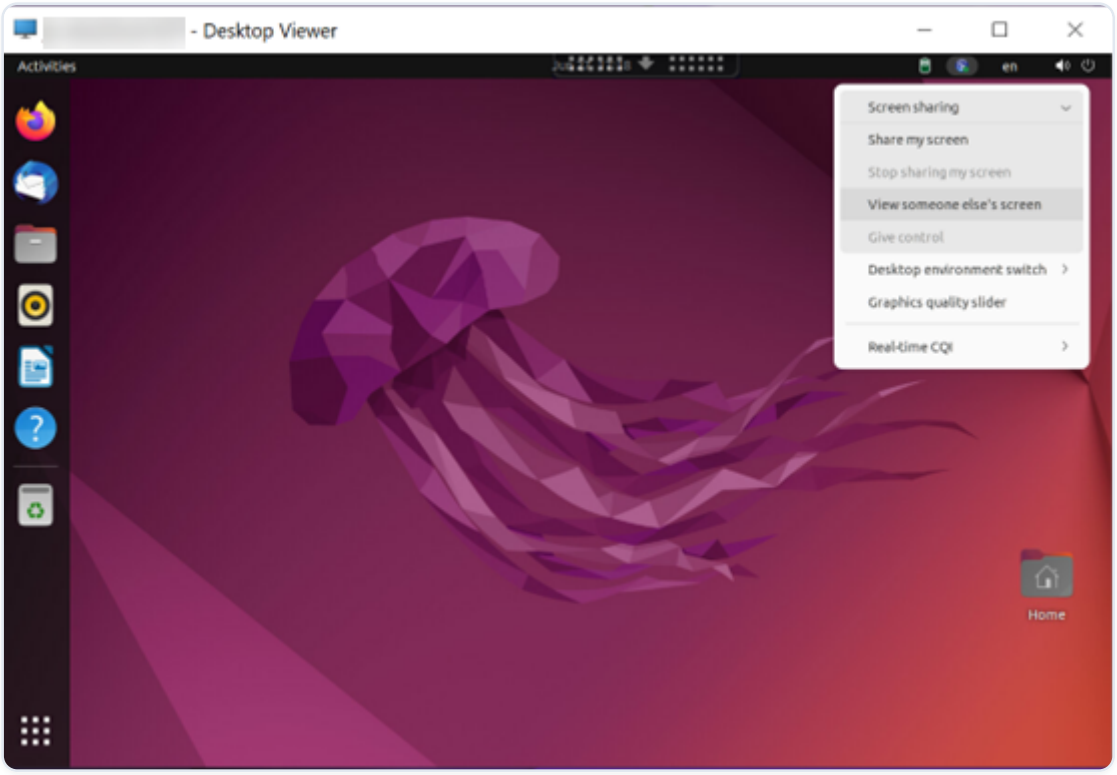


5. Para dejar de compartir la pantalla, seleccione **Dejar de compartir mi pantalla**.

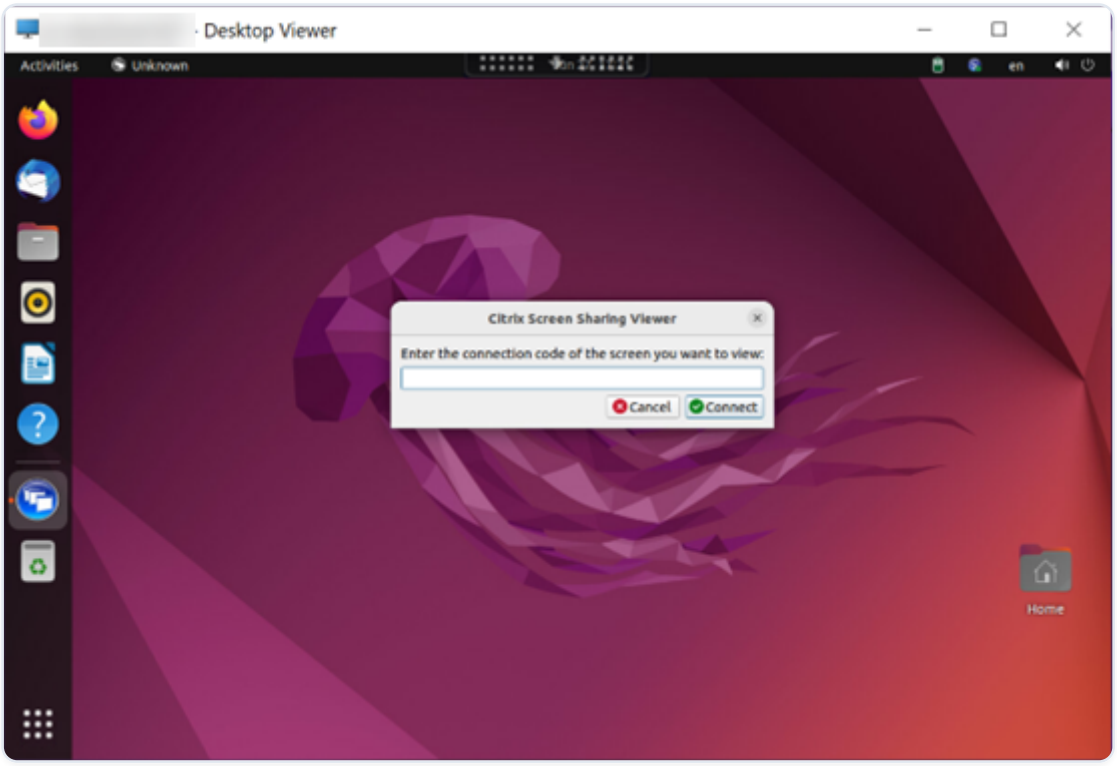


Para ver la pantalla de otra persona:

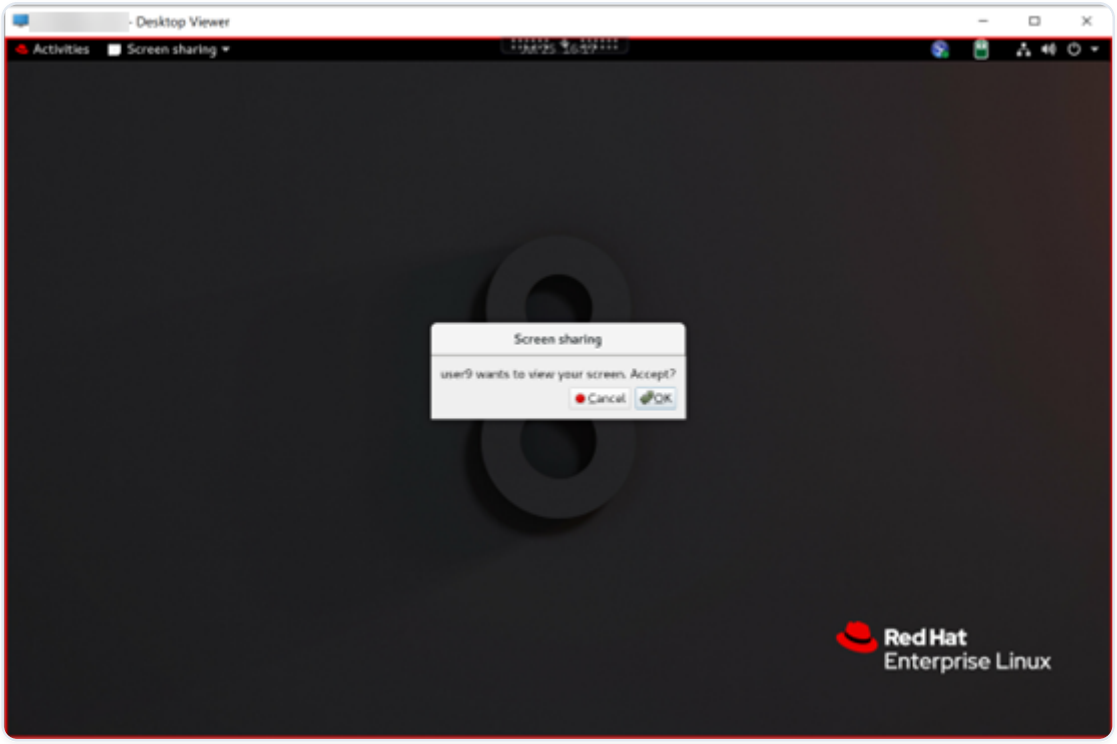
1. En el área de notificaciones de su escritorio virtual, haga clic en el icono de **uso compartido de pantalla** y seleccione **Ver la pantalla de otra persona**.



2. Introduzca el código de conexión de la pantalla que quiere ver y, a continuación, haga clic en **Conectar**.



3. Espere a que el usuario que comparte la pantalla acepte su solicitud. Por ejemplo:

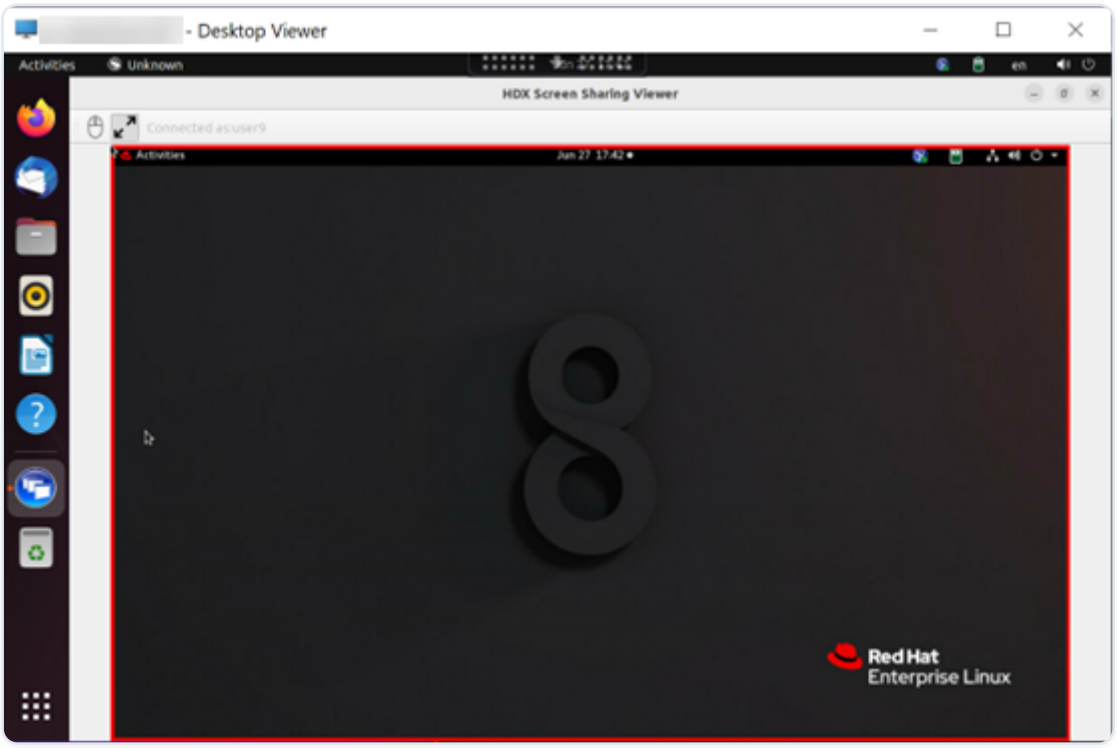


Sugerencia:

- En el lado del usuario que comparte, el sistema Linux emite una notificación de su solicitud.

- Si el compartidor no acepta su solicitud en 30 segundos, la solicitud caduca y aparece un mensaje.

4. Una vez que el compartidor de pantalla acepta su solicitud haciendo clic en **Aceptar**, la pantalla compartida aparece en su Desktop Viewer. Se conecta como visor con un nombre de usuario asignado automáticamente.

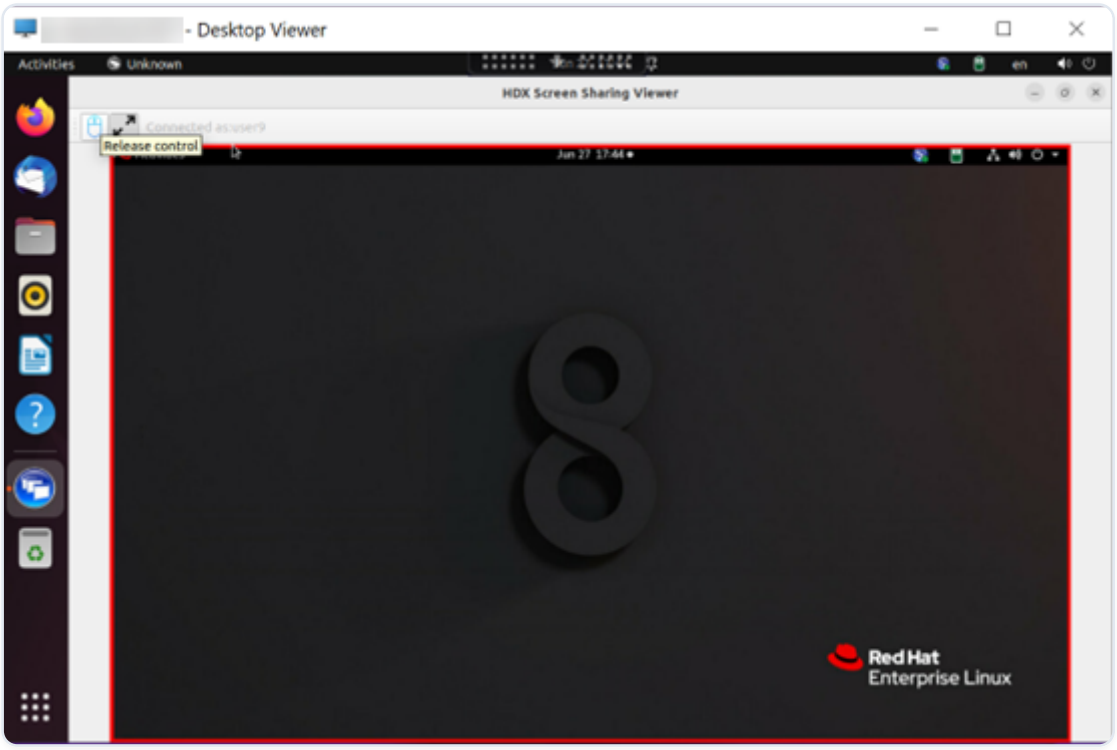


5. Para solicitar el control de la pantalla compartida, haga clic en el icono del ratón en la esquina superior izquierda.

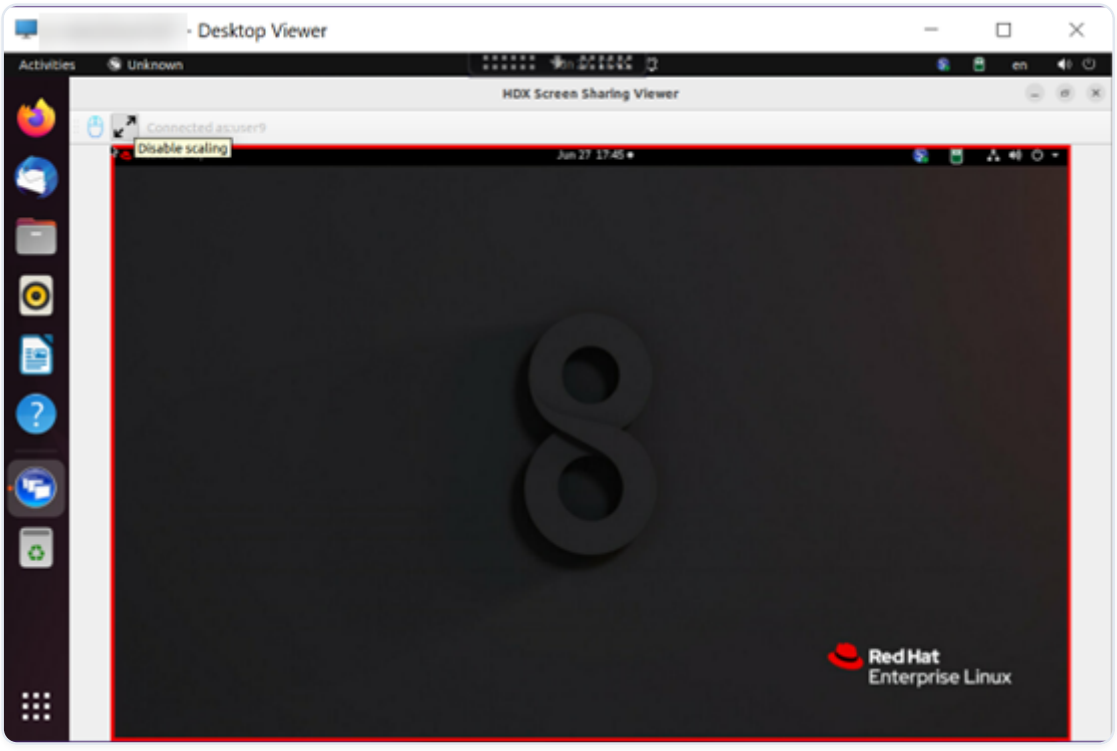
Sugerencia:

- Si el compartidor no acepta su solicitud en 30 segundos, la solicitud caduca.
- Solo un visor puede controlar una pantalla compartida a la vez.

Haga clic de nuevo en el icono del ratón para liberar el control de la pantalla compartida.



6. Para inhabilitar el escalado de pantalla o escalar al tamaño de la ventana, haga clic en el icono junto al icono del ratón.



Configuración

La función de compartir pantalla está inhabilitada de forma predeterminada. Para habilitarla, complete la siguiente configuración:

1. Habilitar la bandeja del sistema.

2. Para Citrix Virtual Apps and Desktops™ 2112 y versiones posteriores, habilite la directiva **ScreenSharing** en Citrix Studio.
3. (Opcional) Para Citrix Virtual Apps™ and Desktops 2109 y versiones anteriores, habilite el uso compartido de pantalla en el VDA de Linux ejecutando el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v
"EnableScreenSharing" -d "0x00000001"
```

4. Permita los puertos 52525–52625 en su firewall.

Consideraciones

- La función de compartir pantalla no es compatible con el códec de vídeo H.265.
- La función de compartir pantalla no está disponible para las sesiones de aplicaciones.
- Los usuarios de sesiones de escritorio pueden compartir las pantallas de sus sesiones con hasta 10 espectadores de forma predeterminada. El número máximo de espectadores se puede configurar a través de `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v "ScreenSharingViewerMaxNum" -d <hex_value>`. Cuando se alcanza el número máximo, aparece un mensaje cuando los usuarios intentan aceptar solicitudes de conexión adicionales.

Modo tolerante a pérdidas para gráficos

El modo tolerante a pérdidas para gráficos se ha reelaborado a fondo para garantizar que la sesión siga siendo interactiva cuando se detecta pérdida de paquetes. Cuando las condiciones de la red se degradan más allá de los umbrales predefinidos de ancho de banda, latencia y pérdida de paquetes, el codificador de gráficos de Citrix® cambia automáticamente a un modo más agresivo de entrega de paquetes para superar el efecto de la pérdida de paquetes. Como resultado, el uso del ancho de banda aumenta en una cantidad proporcional a la cantidad de pérdida de paquetes. Si las condiciones mejoran más tarde, el codificador de gráficos de Citrix vuelve a cambiar sin problemas. Los umbrales se pueden configurar mediante una política, siendo los valores predeterminados 300 ms de latencia y 5% de pérdida de paquetes.

Se admiten las versiones 2311 y posteriores de la aplicación Citrix Workspace™ para Windows. Se añadirá compatibilidad con otras plataformas en futuras versiones de la aplicación Citrix Workspace. Al igual que con las versiones anteriores de esta función, HDX™ Adaptive Transport (EDT) debe estar habilitado para que esta función funcione. Además, si se conecta a través de

Citrix Gateway Service, el modo tolerante a pérdidas para gráficos también debe estar habilitado en Gateway.

Compatibilidad con multimonitor

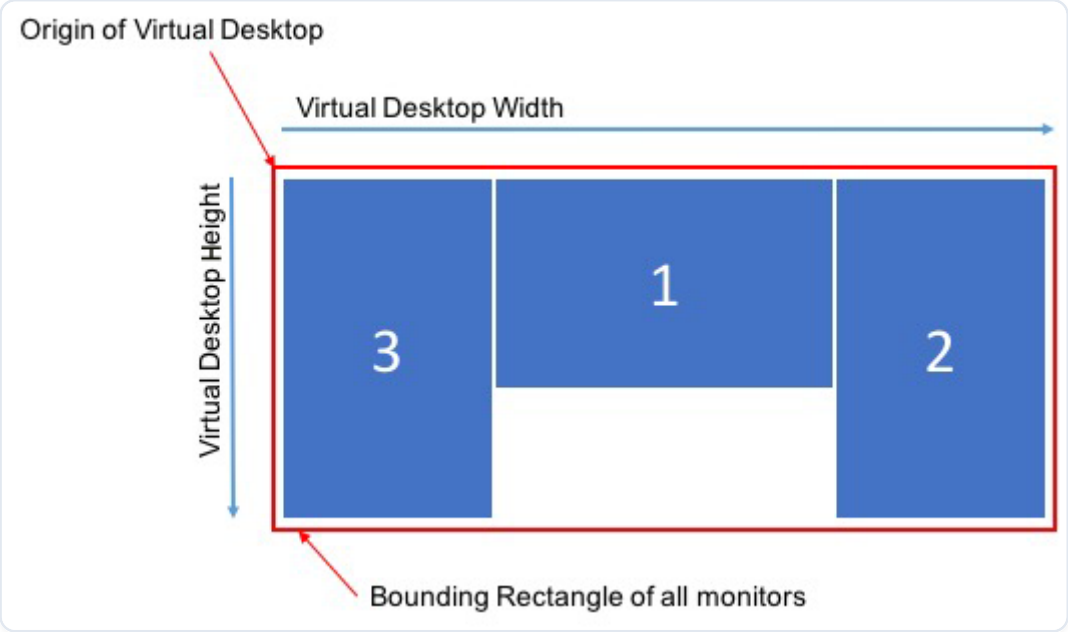
Información general

El VDA de Linux proporciona compatibilidad con varios monitores lista para usar con una resolución predeterminada de 2560×1600 por monitor. Los VDA estándar admiten hasta nueve monitores, y los VDA HDX™ 3D Pro admiten hasta cuatro monitores.

Este artículo describe cómo configurar el VDA de Linux para diferentes resoluciones y diseños de monitor.

Escritorio de sesión virtual

Al igual que el VDA de Windows, el VDA de Linux tiene el concepto de un escritorio virtual de varios monitores. Se basa en el rectángulo delimitador de todos los monitores, no en el diseño real de los monitores. Por lo tanto, el área del escritorio virtual puede ser teóricamente mayor que el área cubierta por los monitores del cliente.



Tamaño del escritorio de sesión virtual

El origen del escritorio de sesión virtual se calcula a partir de la esquina superior izquierda del rectángulo delimitador de todos los monitores. Ese punto se encuentra en X = 0, Y = 0, donde X e Y son los ejes horizontal y vertical, respectivamente.

El ancho del escritorio de sesión virtual es la distancia horizontal, en píxeles, desde el origen hasta la esquina superior derecha del rectángulo delimitador de todos los monitores.

Del mismo modo, la altura del escritorio de sesión virtual es la distancia vertical, en píxeles, desde el origen hasta la esquina inferior izquierda del rectángulo delimitador de todos los monitores.

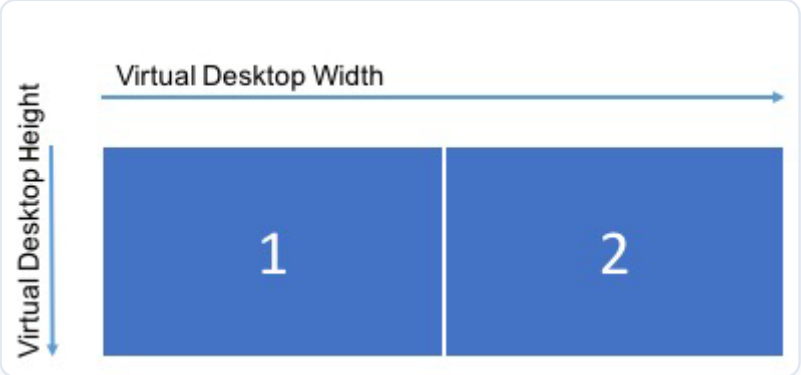
Este cálculo es importante por las siguientes razones:

- Permitir diferentes diseños de monitor de cliente
- Comprender el uso de memoria en el VDA de Linux

Permitir diferentes configuraciones de monitor de cliente

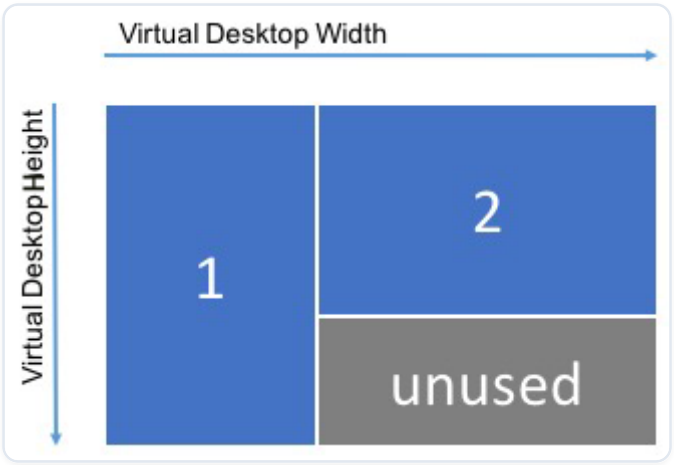
Conocer el tamaño máximo del escritorio virtual para sus diversas configuraciones de monitor de cliente le permite configurar el VDA de Linux para que sea flexible en cuanto a las configuraciones de monitor de cliente.

Considere la siguiente configuración de monitor de cliente:



El diagrama anterior muestra una configuración de varios monitores lista para usar con dos monitores, cada uno con una resolución de 2560×1600.

Ahora, considere conectarse al mismo Linux VDA con la siguiente configuración de monitor de cliente:



Si cada monitor del diagrama anterior tiene una resolución de 2560×1600, los parámetros de configuración de varios monitores listos para usar son insuficientes. La altura máxima es demasiado pequeña para acomodar el escritorio de la sesión virtual para esta disposición de monitores. Para acomodar la configuración del monitor del cliente en este ejemplo, debe establecer el escritorio virtual de Linux VDA en un tamaño de 4160×2560.

Para obtener la mayor flexibilidad en una configuración de varios monitores, busque el rectángulo delimitador más pequeño de todas las disposiciones de monitores que desee admitir. Para configuraciones con dos monitores de 2560×1600, las posibles disposiciones incluyen:

- **Monitor1** 2560×1600 y **Monitor2** 2560×1600
- **Monitor1** 1600×2560 y **Monitor2** 2560×1600
- **Monitor1** 2560×1600 y **Monitor2** 1600×2560
- **Monitor1** 1600×2560 y **Monitor2** 1600×2560

Para acomodar todas las disposiciones anteriores, necesita un escritorio de sesión virtual de 5120×2560. Es el rectángulo delimitador más pequeño que puede contener todas las disposiciones deseadas.

Si todos sus usuarios tienen solo un monitor en la disposición horizontal típica, establezca el tamaño máximo del escritorio virtual en la resolución más alta del monitor.



En este ejemplo, el escritorio virtual debe establecerse en un tamaño de 2560×1600. Dado que la configuración predeterminada es 5120×1600 y 2 monitores, se requiere un cambio de configuración para optimizar el uso de la memoria en implementaciones de un solo monitor.

> **Nota:**
>
> Si un escritorio se muestra con una resolución incorrecta en una configuración de varios monitores, ajuste la configuración de Puntos por pulgada (DPI) en la aplicación Citrix Workspace. Para obtener más información, consulte el artículo del Centro de conocimientos CTX230017.

Comprensión del uso de memoria en el VDA de Linux

Conocer el tamaño del escritorio virtual le permite calcular la cantidad de memoria utilizada por cada sesión HDX. Esta memoria es la que se asigna a cada sesión para sus datos gráficos cuando la sesión comienza. No cambia durante la vida útil de la sesión. Aunque esta memoria no es la cantidad total de memoria utilizada para la sesión, es la forma más sencilla de calcular el uso de memoria por sesión.

Para calcular cuánta memoria se asigna a cada sesión HDX, utilice la siguiente fórmula:

M = X × Y × Z,

Donde:

- **M** es la cantidad de memoria utilizada para los gráficos de la sesión.
- **X** es el ancho del escritorio de la sesión virtual.
- **Y** es la altura del escritorio de la sesión virtual.
- **Z** es la profundidad de color de la ventana de la sesión HDX. El valor está en bytes, no en bits, así que use 4 para el color de 32 bits.

> **NOTA:**
>
> La profundidad de color del servidor X se inicia y no puede cambiar durante la vida útil de la sesión (**desde el inicio de sesión, pasando por las desconexiones/reconexiones, hasta el cierre de sesión**). Por lo tanto, el VDA de Linux siempre asigna el escritorio de la sesión

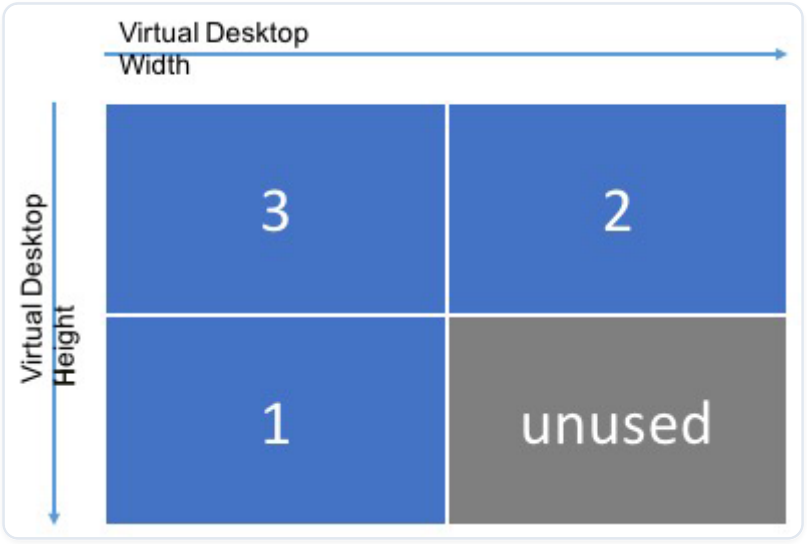
> virtual como de 32 bits y reduce la muestra a la profundidad de color solicitada para la sesión.

> Por ejemplo, para una sesión de 1024×768, la memoria utilizada es:

> 1024 × 768 × 4 / 2\^20 MB = 3 MB

> Comprender el uso de la memoria es importante para aumentar la densidad de las sesiones en cada VDA de Linux.

Considere la siguiente configuración de monitor de cliente:



Si cada monitor tiene una resolución de 2560×1600, para adaptarse a esta configuración de monitor de cliente, el tamaño del escritorio de la sesión virtual debe ser de 5120×3200. Tenga en cuenta que el área gris no se utiliza y equivale a 16.384.000 (es decir, 2560 x 1600 x 4) bytes de memoria desperdiciada.

Parámetros de configuración de varios monitores de Citrix®

Puede controlar la funcionalidad de varios monitores del VDA de Linux mediante los siguientes parámetros de configuración:

- `MaxScreenNum`

  Parámetro: HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/Thinwire/MaxScreenNum

  Descripción: Número de monitores compatibles

Tipo: DWORD

Predeterminado: 4

Máximo: 9 para VDA estándar, 4 para VDA HDX 3D Pro

- `MaxFbWidth`

  Parámetro: HKEY_LOCAL_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/MaxFbWidth

  Descripción: Ancho máximo de un escritorio de sesión virtual

  Tipo: DWORD

  Predeterminado: 5.120

  Máximo: 16.384 (8.192 x 2)

- `MaxFbHeight`

  Parámetro: HKEY_LOCAL_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/MaxFbHeight

  Descripción: Altura máxima de un escritorio de sesión virtual

  Tipo: DWORD

  Predeterminado: 1.600

  Máximo: 16.384 (8.192 x 2)

Cambio de la configuración de varios monitores del VDA de Linux

La siguiente sección describe cómo habilitar, configurar y deshabilitar la funcionalidad de varios monitores en el VDA de Linux.

Establezca el número máximo de monitores mediante:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE
\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"MaxScreenNum" -d "NumMons" --force
```

Donde `NumMons` es un valor entre 1 y 9 para VDA estándar o 1 y 4 para VDA HDX 3D Pro.

Establezca el ancho máximo de un escritorio de sesión virtual mediante:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE
\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"MaxFbWidth" -d " MaxWidth" --force
```

Donde `MaxWidth` es un valor entre `1,024` y `16,384`.

Establezca la altura máxima de un escritorio de sesión virtual mediante:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE
\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"MaxFbHeight" -d " MaxHeight" --force
```

Donde `MaxHeight` es un valor entre `1,024` y `16,384`.

GPU no virtualizadas

En la documentación de Linux VDA, las GPU no virtualizadas se refieren a:

- GPU utilizadas en escenarios de Acceso con PC remoto
- GPU pasadas desde un hipervisor

Este artículo proporciona información sobre la compatibilidad con GPU no virtualizadas.

Habilitar HDX™ 3D Pro para GPU NVIDIA que admiten el SDK de captura de NVIDIA para Linux

Para las GPU NVIDIA que admiten el SDK de captura de NVIDIA para Linux, habilite HDX 3D Pro simplemente configurando **CTX_XDL_HDX_3D_PRO** en **Y** al instalar el VDA de Linux. No se requiere ninguna configuración adicional. La aceleración de hardware se habilita de forma predeterminada después de habilitar HDX 3D Pro.

Compatible con GPU NVIDIA que no admiten el SDK de captura de NVIDIA para Linux y GPU de otros fabricantes como AMD e Intel

> **Nota:**
>
> En este escenario, solo se admite la codificación por software.

Paso 1: Establezca CTX_XDL_HDX_3D_PRO en Y al instalar el VDA de Linux

Para obtener información sobre las variables de entorno, consulte Paso 8: Ejecute la instalación sencilla para configurar el entorno y el VDA para completar la instalación.

Paso 2: Instale Xdamage

Por ejemplo, puede ejecutar **sudo apt-get install -y libxdamage1** para instalar XDamage en Ubuntu 20.04. Normalmente, XDamage existe como una extensión de XServer.

Paso 3: Habilite XDamage ejecutando el siguiente comando

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_DWORD" -v "XDamageEnabled" -d "0x00000001" --force
```

Paso 4: Modifique los archivos de configuración de Xorg

Puede encontrar los siguientes cuatro archivos de configuración de plantilla en **/etc/X11**. Según el número de monitores conectados, modifique uno de los archivos de configuración de plantilla con el número correspondiente en su nombre. Por ejemplo, si solo hay un monitor conectado, modifique el archivo de configuración de plantilla con el número 1 en su nombre, es decir, ctx-driver_name-1.conf. Si hay dos monitores conectados, modifique el archivo de configuración de plantilla con el número 2 en su nombre, es decir, ctx-driver_name-2.conf.

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

Tomando **ctx-driver_name-1.conf** como ejemplo, haga lo siguiente para modificar los archivos de configuración de plantilla:

1. Sustituya ***driver_name*** por el nombre real de su controlador.

   Por ejemplo, si el nombre de su controlador es `intel`, puede cambiar el nombre del archivo de configuración a `ctx-intel-1.conf`.

2. Agregue la información del controlador de vídeo.

   Cada archivo de configuración de plantilla contiene una sección llamada "Device", que está comentada. Esta sección describe la información del controlador de vídeo. Habilite esta

sección antes de agregar la información de su controlador de vídeo. Para habilitar esta sección:

a. Consulte la guía proporcionada por el fabricante de la GPU para obtener información de configuración. Se puede generar un archivo de configuración nativo. verificar que su GPU puede funcionar en un entorno local con el archivo de configuración nativo.

b. Copie la sección "Device" del archivo de configuración nativo en **ctx-driver_name-1.conf**.

3. Ejecute el siguiente comando para establecer la clave de registro de modo que el VDA de Linux pueda reconocer el nombre del archivo de configuración establecido en el Paso 1.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_SZ" -v "DriverName" -d "intel" --force
```

Apagado de monitor para VDA de acceso remoto a PC

El VDA de Linux admite el apagado físico del monitor para los VDA de acceso remoto a PC que utilizan GPU no virtualizadas.

Las distribuciones de Linux totalmente probadas que admiten la función incluyen Ubuntu 20.04 y Debian 11.

La función está inhabilitada de forma predeterminada. Para habilitarla, complete los dos pasos siguientes:

1. Instale el paquete `evdi-dkms` según su distribución de Linux:

```
sudo apt install evdi-dkms
```

2. Habilite la descarga de la visualización de gráficos a EVDI:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "Evdi" -d "0x00000001" --force
```

3. Si utiliza una GPU Intel, inhabilite el administrador de visualización. De lo contrario, el administrador de visualización ocupa y hace que la GPU Intel no esté disponible para las sesiones remotas de Citrix®.

```
sudo systemctl disable --now gdm
```

Solución de problemas

Salida gráfica nula o distorsionada

Si puede ejecutar aplicaciones 3D localmente y todas las configuraciones son correctas, la salida gráfica que falta o está distorsionada es el resultado de un error. Utilice /opt/Citrix/VDA/bin/setlog y establezca GFX_X11 en detallado para recopilar la información de seguimiento para la depuración.

Xorg sin privilegios de root

El VDA de Linux admite la ejecución de Xorg con privilegios de usuario que no son de root, también conocido como Xorg "sin privilegios de root". Xorg sin privilegios de root es una mejora de seguridad significativa con respecto a la ejecución como root.

Nota:

- Xorg no admite el funcionamiento sin privilegios de root en Amazon Linux 2 o RHEL 7.
- Xorg sin privilegios de root también requiere el soporte del controlador de GPU. Si utiliza un VDA de acceso remoto a PC, pruebe y verificar que su controlador de GPU sea compatible con Xorg sin privilegios de root.

Xorg sin privilegios de root está deshabilitado de forma predeterminada. Red Hat ha abordado la vulnerabilidad de seguridad CVE-2024-31083 que afecta a los servidores Xorg.

Para mantener la funcionalidad de Xorg sin privilegios de root, asegúrese de que MIT-SHM funcione en las sesiones de ICA® siguiendo estos pasos:

1. Aplique la capacidad `cap_ipc_owner` directamente al ejecutable de Xorg, no a un script de envoltura, utilizando los siguientes comandos específicos de la distribución:
   - Ubuntu, Debian: `sudo setcap 'cap_ipc_owner=+ep' /usr/lib/xorg/Xorg`
   - RHEL, Rocky: `sudo setcap 'cap_ipc_owner=+ep' /usr/libexec/Xorg`
   - SUSE: `sudo setcap 'cap_ipc_owner=+ep' /usr/libexec/Xorg /usr/bin/Xorg`
2. Habilite Xorg sin privilegios de root utilizando el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"Rootless" -d "1" --force
```

Para deshabilitar Xorg sin privilegios de root, si ya está habilitado, haga lo siguiente:

1. Ejecute el siguiente comando para deshabilitar la función:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"Rootless" -d "0" --force
```

2. Elimine la capacidad `cap_ipc_owner` del ejecutable de Xorg utilizando los comandos específicos de la distribución:
   - Ubuntu, Debian: `sudo setcap 'cap_ipc_owner=-ep' /usr/lib/xorg/Xorg`
   - RHEL, Rocky: `sudo setcap 'cap_ipc_owner=-ep' /usr/libexec/Xorg`
   - SUSE: `sudo setcap 'cap_ipc_owner=-ep' /usr/libexec/Xorg /usr/bin/Xorg`

Marca de agua de sesión

La marca de agua de sesión ayuda a disuadir y permitir el seguimiento del robo de datos. La información rastreable aparece en los escritorios de la sesión como un elemento disuasorio para los usuarios que emplean fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua como una capa de texto o una imagen PNG con canal alfa. La marca de agua se muestra en toda la pantalla de la sesión sin cambiar el contenido del documento original.

Importante:

La marca de agua de sesión no es una función de seguridad. No evita por completo el robo de datos, pero proporciona cierto nivel de disuasión y trazabilidad. No garantizamos la trazabilidad completa de la información al utilizar esta función. En su lugar, le recomendamos que combine esta función con otras soluciones de seguridad, según corresponda.

La marca de agua de sesión contiene información para rastrear el robo de datos. Los datos más importantes son la identidad del usuario, tal como se rastrea por sus credenciales de

> inicio de sesión, de la sesión donde se tomó la imagen de la pantalla. Para rastrear la fuga de datos de manera más efectiva, incluya otra información como la dirección IP del servidor o del cliente y la hora de conexión.

Para ajustar la experiencia del usuario, utilice las siguientes configuraciones de directiva de marca de agua de sesión para configurar la ubicación y la apariencia de la marca de agua en la pantalla:

Configuración de directivas de marca de agua de sesión

Habilitar marca de agua de sesión

Cuando habilita esta configuración, la pantalla de la sesión tiene una marca de agua opaca que muestra información específica de la sesión. Las demás configuraciones de marca de agua dependen de que esta esté habilitada.

De forma predeterminada, la marca de agua de sesión está inhabilitada.

Incluir dirección IP del cliente

Cuando habilita esta configuración, la sesión muestra la dirección IP del cliente actual como marca de agua.

De forma predeterminada, **Incluir dirección IP del cliente** está inhabilitado.

Incluir hora de conexión

Cuando habilita esta configuración, la marca de agua de sesión muestra una hora de conexión. El formato es aaaa/mm/dd hh:mm. La hora mostrada se basa en el reloj del sistema y la zona horaria.

De forma predeterminada, **Incluir hora de conexión** está inhabilitado.

Incluir nombre de usuario de inicio de sesión

Cuando habilita esta configuración, la sesión muestra el nombre de usuario de inicio de sesión actual como marca de agua. El formato de visualización es NOMBREDEUSUARIO@NOMBREDEDOMINIO. Recomendamos que el nombre de usuario tenga un máximo de 20 caracteres. Cuando un nombre de usuario tiene más de 20 caracteres, pueden producirse tamaños de fuente más pequeños o truncamiento, lo que disminuye la eficacia de la marca de agua.

De forma predeterminada, **Incluir nombre de usuario de inicio de sesión** está habilitado.

Incluir nombre de host de VDA

Cuando habilita esta configuración, la sesión muestra el nombre de host de VDA de la sesión ICA® actual como marca de agua.

De forma predeterminada, **Incluir nombre de host de VDA** está habilitado.

Incluir dirección IP de VDA

Cuando habilita esta configuración, la sesión muestra la dirección IP de VDA de la sesión ICA actual como marca de agua.

De forma predeterminada, **Incluir dirección IP de VDA** está inhabilitado.

Estilo de marca de agua de sesión

Esta configuración controla si se muestra una única etiqueta de texto de marca de agua o varias etiquetas. Elija **Múltiple** o **Única** en el menú desplegable **Valor**. Para obtener opciones de estilo adicionales, consulte la sección **Texto personalizado de marca de agua** de este artículo.

Múltiple muestra cinco etiquetas de marca de agua en la sesión. Una en el centro y cuatro en las esquinas.

Única muestra una única etiqueta de marca de agua en el centro de la sesión.

De forma predeterminada, el **Estilo de marca de agua de sesión** es **Múltiple**.

Transparencia de marca de agua

Puede especificar la opacidad de la marca de agua de 0 a 100. Cuanto mayor sea el valor especificado, más opaca será la marca de agua.

De forma predeterminada, el valor es 17.

Texto personalizado de la marca de agua

El valor está vacío de forma predeterminada. Puede escribir una cadena no vacía, establecer una sintaxis para formar una cadena o usar la combinación para mostrarla en la marca de agua de la sesión. Las cadenas no vacías admiten hasta 25 caracteres Unicode por línea. Las cadenas más largas se truncan a 25 caracteres.

Por ejemplo, puede establecer la directiva con el siguiente valor:

```
<date>
<time><newline><username><style=single><fontsize=40><font=Ubuntu><position=center><rotation
Linux VDA<newline>Version 2207
```

Para obtener una descripción de todas las opciones de sintaxis, consulte la siguiente tabla:

OPCIÓN DE SINTAXIS	DESCRIPCIÓN	CONFIGURACIÓN VÁLIDA (DISTINGUE MAYÚSCULAS DE MINÚSCULAS)	VALOR PREDETERMINADO	OBSERVACIONES
`<style>`	Estilo de diseño de la marca de agua	`xstyle`, `single`, `tile`, `horizontal`	`xstyle`	-
`<position>`	Posición de la marca de agua	`center`, `topleft`, `topright`, `bottomleft`, `bottomright`	`center`	Válido solo cuando el estilo de diseño está establecido en **single**.
`<rotation>`	Rotación de la marca de agua a un ángulo determinado	-180–180	0	-
`<transparency>`	Opacidad de la marca de agua	0–100	17	-
`<font>`	-	Una fuente compatible con el sistema	Sans	-
`<fontsize>`	-	20–50	0 (calculado automáticamente)	-
`<fontzoom>`	Porcentaje de los tamaños de fuente e imagen que establece a través de	0 –	100	-

OPCIÓN DE SINTAXIS	DESCRIPCIÓN	CONFIGURACIÓN VÁLIDA (DISTINGUE MAYÚSCULAS DE MINÚSCULAS)	VALOR PREDETERMINADO	OBSERVACIONES
	`<fontsize>` y `<image>`			
`<image>`	Marca de agua PNG	Ruta a una imagen PNG en el VDA	N/D	Esta sintaxis configura una marca de agua PNG. Solo se admite PNG con canal alfa. Cuando se utiliza una marca de agua PNG, solo las opciones de sintaxis `<style>`, `<position>`, `<rotation>`, `<transparency>` y `<fontzoom>` pueden ser efectivas.
`<date>`	Marcador de posición para la fecha de conexión de la sesión (AAAA/MM/DD)	N/D	N/D	-
`<time>`	Marcador de posición para la hora de conexión de la	N/D	N/D	-

OPCIÓN DE SINTAXIS	DESCRIPCIÓN	CONFIGURACIÓN VÁLIDA (DISTINGUE MAYÚSCULAS DE MINÚSCULAS)	VALOR PREDETERMINADO	OBSERVACIONES
	sesión (HH:MM)			
`<domain>`	Marcador de posición para el dominio de la cuenta de usuario	N/D	N/D	-
`<username>`	Marcador de posición para el nombre de usuario de inicio de sesión actual (excluyendo el dominio de la cuenta de usuario)	N/D	N/D	-
`<hostname>`	Marcador de posición para el nombre de host del VDA	N/D	N/D	-
`<clientip>`	Marcador de posición para la dirección IP del cliente	N/D	N/D	-
`<serverip>`	Marcador de posición para la dirección IP del VDA	N/D	N/D	-

Nota:

> Si se especifica **Texto personalizado de marca de agua** con al menos una opción de sintaxis válida, se ignoran todas las demás directivas de marca de agua de sesión, excepto **Habilitar marca de agua de sesión**.

> Si deja una opción de sintaxis sin especificar o la establece en un valor no admitido, se utiliza su valor predeterminado.

Limitaciones

- La marca de agua de sesión se admite en cualquiera de los siguientes casos:
  - Cuando **Usar códec de vídeo para la compresión** está establecido en **Para toda la pantalla**.
  - Cuando **Usar códec de vídeo para la compresión** está establecido en **Usar cuando se prefiera** y Optimizar para cargas de trabajo de gráficos 3D está habilitado.
- La marca de agua de sesión no se admite en sesiones donde se utiliza la redirección de contenido del explorador. Para usar la función de marca de agua de sesión, asegúrese de que la redirección de contenido del explorador esté inhabilitada.
- La marca de agua de sesión no se admite y no aparece si la sesión se ejecuta en modo de codificación H.264 o H.265 acelerado por hardware a pantalla completa con controladores NVIDIA heredados. (En este caso, NvCaptureType se establece en 2 en el Registro).
- La marca de agua no es visible para el sombreado de sesión.
- Si pulsa la tecla Impr Pant para capturar una pantalla, la pantalla capturada en el lado del VDA no incluye la marca de agua. Le recomendamos que tome medidas para evitar que se copien las capturas de pantalla.

Aceleración de GPU compartida en un VDA de Linux multisesión

HDX™ 3D PRO solo admite los VDA de Linux configurados para escritorios VDI (modo de sesión única). Para un VDA de Linux multisesión, puede habilitar la aceleración de GPU compartida para acelerar las aplicaciones 3D de OpenGL.

> **Nota:**

> El servidor de visualización Wayland no es compatible con la aceleración de GPU compartida.

Configuración

Para habilitar la aceleración de GPU compartida en un VDA de Linux multisesión y acelerar las aplicaciones 3D de OpenGL, complete los siguientes pasos de configuración:

Paso 1: Instalar VirtualGL

Descargue e instale **VirtualGL** desde `<https://sourceforge.net/projects/virtualgl/files>`. Descargue los paquetes **.deb** para distribuciones de Linux basadas en Debian y los paquetes **.rpm** para distribuciones de Linux basadas en RHEL.

Paso 2: Configurar VirtualGL

1. Detenga el administrador de visualización de Linux, por ejemplo, LightDM o GNOME Display Manager (GDM).
2. Ejecute el script de configuración de VirtualGL ejecutando:

   ```
   #/opt/VirtualGL/bin/vglserver_config
   ```

   Le recomendamos que realice las siguientes selecciones durante la ejecución del script:

   - Seleccione "1" para "Configurar el servidor para usar con VirtualGL (back-ends GLX + EGL)"
   - Seleccione "n" para "Restringir el acceso al servidor 3D X al grupo **vglusers**"
   - Seleccione "n" para "Restringir el acceso a los dispositivos de búfer de fotogramas al grupo **vglusers**"
   - Seleccione "n" para "Deshabilitar la extensión XTEST"
3. Salga del script de configuración y reinicie el administrador de visualización de Linux.

Paso 3: Ejecutar aplicaciones 3D OpenGL con aceleración de GPU

Hay dos métodos para ejecutar aplicaciones 3D OpenGL con aceleración de GPU en una sesión de Linux VDA:

- **Método 1:** Habilitar la aceleración de GPU compartida para todas las aplicaciones 3D OpenGL

Para ello, abra un terminal bash en el Linux VDA, ejecute el siguiente comando y, a continuación, reinicie el terminal bash. Este enfoque habilita la aceleración de GPU compartida para todas las aplicaciones 3D OpenGL iniciadas desde el terminal bash.

```
#/opt/Citrix/VDA/sbin/ctxgpushare.sh enable
```

- **Método 2:** Habilitar la aceleración de GPU compartida para una aplicación 3D OpenGL específica:

  Para ello, abra un terminal en el Linux VDA y ejecute el siguiente comando con el nombre de la aplicación especificado:

```
#vglrun <AppName>
```

Limitaciones

- La aceleración de GPU compartida funciona en estrecha colaboración con el administrador de pantalla en el Linux VDA. Se recomienda utilizar LightDM como administrador de pantalla para la aceleración de GPU compartida a fin de lograr la funcionalidad y el rendimiento esperados.
- La aceleración de hardware WebGL solo es compatible con Firefox en Ubuntu y Debian.

Escalabilidad

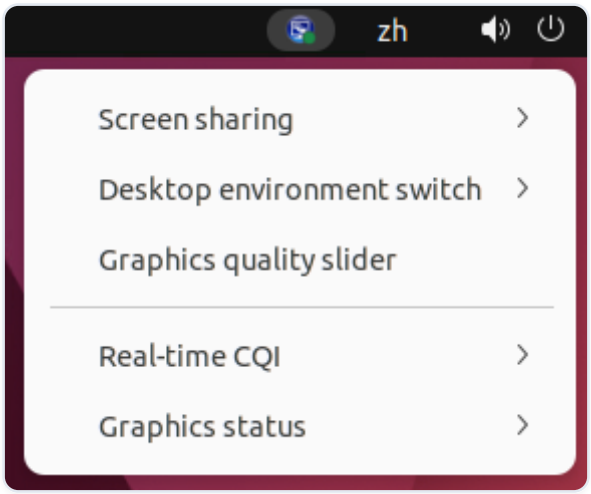
El número máximo admitido de sesiones simultáneas que pueden compartir una GPU depende de la CPU y la memoria del sistema. También depende en gran medida de la memoria de vídeo máxima de la GPU.

Por ejemplo:

SI	ENTONCES
la vGPU NVIDIA **M10-2B** tiene 2048 MB de memoria de vídeo y una aplicación OpenGL como VariCAD Viewer utiliza 100 MB de memoria de vídeo para su carga de trabajo en cada sesión,	en teoría, el número máximo admitido de sesiones simultáneas no puede superar las 20.

Bandeja del sistema

Los usuarios de la sesión pueden hacer clic en el siguiente icono de la bandeja del sistema para realizar las acciones o ver los indicadores:



Introducción a los elementos de la bandeja del sistema

Cada elemento corresponde a una función con un conmutador. Cuando la función correspondiente a un elemento está deshabilitada, el elemento se oculta y no se muestra.

- **Uso compartido de pantalla**

  Para obtener más información sobre esta función, consulte Uso compartido de pantalla de HDX.

- **Conmutador de entorno de escritorio**

  Este elemento es una GUI para **ctxdesktopswitch.sh**. Para obtener más información, consulte Entornos de escritorio personalizados por usuarios de sesión.

  La personalización del entorno de escritorio por parte de los usuarios de la sesión está habilitada de forma predeterminada. Para deshabilitarla, ejecute el siguiente comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg create -k
  "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
  -v "EnableDesktopSwitch" -d "0x00000000" --force
  ```

- **Control deslizante de calidad gráfica**

  Para obtener más información, consulte la sección Control deslizante de calidad gráfica del artículo de configuración de gráficos.

- **CQI en tiempo real**

  Actualmente, se muestran los datos de tiempo de ida y vuelta (RTT) de ICA y la latencia. Para obtener más información, consulte las Utilidades de consulta de métricas de sesión.

El icono de la bandeja del sistema se muestra de forma diferente según la latencia en el CQI en tiempo real:



Hay umbrales que controlan cuándo cambia la visualización del icono. De forma predeterminada, se configuran de la siguiente manera:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "HighLatencyThreshold" -d "0x000000dc" --force
```

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "LowLatencyThreshold" -d "0x00000078" --force
```

Cuando la latencia real es menor o igual que **LowLatencyThreshold**, el icono se marca en verde. Cuando la latencia real es mayor que **HighLatencyThreshold**, el icono se marca en rojo. En otras circunstancias, el icono se marca en amarillo. Si el CQI en tiempo real está inhabilitado, el icono no tiene una marca de color.

El CQI en tiempo real está habilitado y se muestra de forma predeterminada. Para inhabilitarlo y ocultarlo, y para que el icono de la bandeja no tenga una marca de color, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "EnableCqiShow" -d "0x00000000" --force
```

- **Estado de los gráficos**

Este indicador muestra la configuración de gráficos de la sesión actual. Está habilitado de forma predeterminada. Para inhabilitarlo, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "EnableGfxInfo" -d "0x00000000" --force
```

Habilitar la bandeja del sistema

La bandeja del sistema, así como la visualización del estado de la batería del cliente, están habilitadas de forma predeterminada. Sin embargo, bajo ciertas condiciones, debe realizar una configuración adicional para habilitar la bandeja del sistema y la visualización del estado de la batería del cliente. Los detalles son los siguientes:

1. Habilite la directiva del indicador de estado de los gráficos en Citrix Studio.
2. (**Este paso solo es necesario si utiliza RHEL 8.x/9.x, Rocky Linux 8.x/9.x, Debian 11 o SUSE 15.x con GNOME instalado.**) Instale una extensión compatible para su shell de GNOME para habilitar la compatibilidad con AppIndicator.

   a. Ejecute el comando `gnome-shell --version` para comprobar la versión de su shell de GNOME.

   b. Descargue una extensión compatible para su shell de GNOME desde `<https://extensions.gnome.org/extension/615/appindicator-support>`. Por ejemplo, si la versión de su shell es 3.28, puede seleccionar 24 o 26 para la versión de la extensión.

   c. Descomprima el paquete descargado y cambie el nombre del directorio descomprimido a `appindicatorsupport@rgcjonas.gmail.com`. verificar que el valor de **"uuid"** en el archivo **metadata.json** del paquete esté establecido en `appindicatorsupport@rgcjonas.gmail.com`.

   d. Ejecute el comando `mv` para mover el directorio `appindicatorsupport@rgcjonas.gmail.com` a la ubicación en `/usr/share/gnome-shell/extensions/`.

   e. Ejecute el comando `chmod a+r metadata.json` para que el archivo **metadata.json** sea legible para otros usuarios.

   > **Sugerencia:**
   >
   > De forma predeterminada, el archivo **metadata.json** del directorio `appindicatorsupport@rgcjonas.gmail.com` solo es legible para el usuario root. Para admitir el uso compartido de pantalla, haga que el archivo **metadata.json** también sea legible para otros usuarios.

   f. Instale GNOME Tweaks.

g. En el entorno de escritorio, recargue su shell de GNOME pulsando las teclas `Alt+F2`, `r` y `Enter` en secuencia o ejecutando el comando `killall -SIGQUIT gnome-shell`.

h. En el entorno de escritorio, ejecute GNOME Tweaks y, a continuación, habilite **KStatusNotifierItem/AppIndicator Support** en la herramienta Tweaks o Extensions.

> **Nota:**
>
> Para RHEL 9.x, Rocky Linux 9.x y SUSE 15.x instalados con GNOME, la administración de extensiones se ha trasladado fuera de Tweaks. Le recomendamos que descargue las extensiones de GNOME de la tienda de aplicaciones de software de GNOME y, a continuación, habilite la compatibilidad con AppIndicator en las extensiones de GNOME.

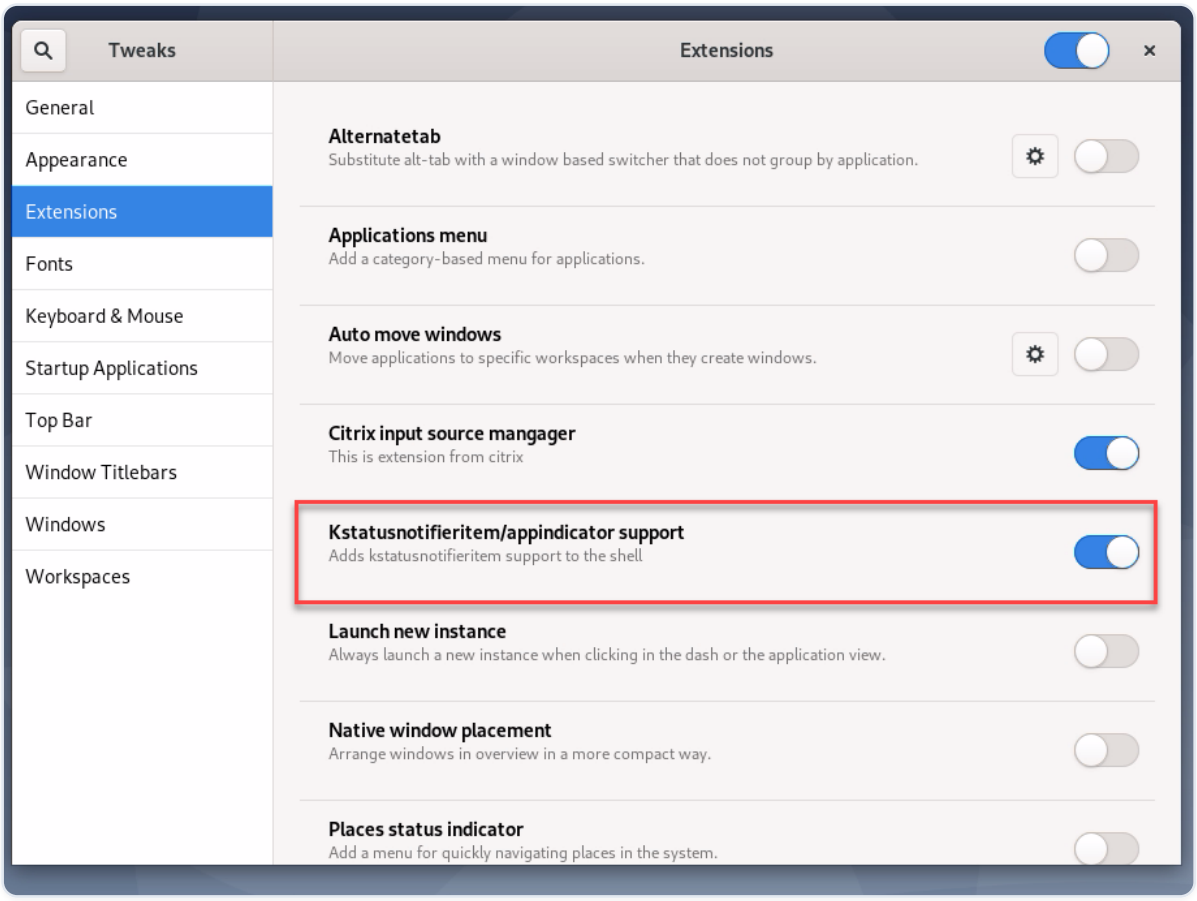
3. (**Este paso solo es necesario si utiliza Debian 11 instalado con GNOME.**) Complete los siguientes pasos para instalar y habilitar los iconos de la bandeja del sistema de GNOME.

a. Ejecute el comando `sudo apt install gnome-shell-extension-appindicator`. Es posible que tenga que cerrar la sesión y volver a iniciarla para que GNOME vea la extensión.

b. Busque Tweaks en su pantalla de **Actividades**.

c. Seleccione **Extensiones** en la herramienta Tweaks.

d. Habilite **Kstatusnotifieritem/appindicator support**.

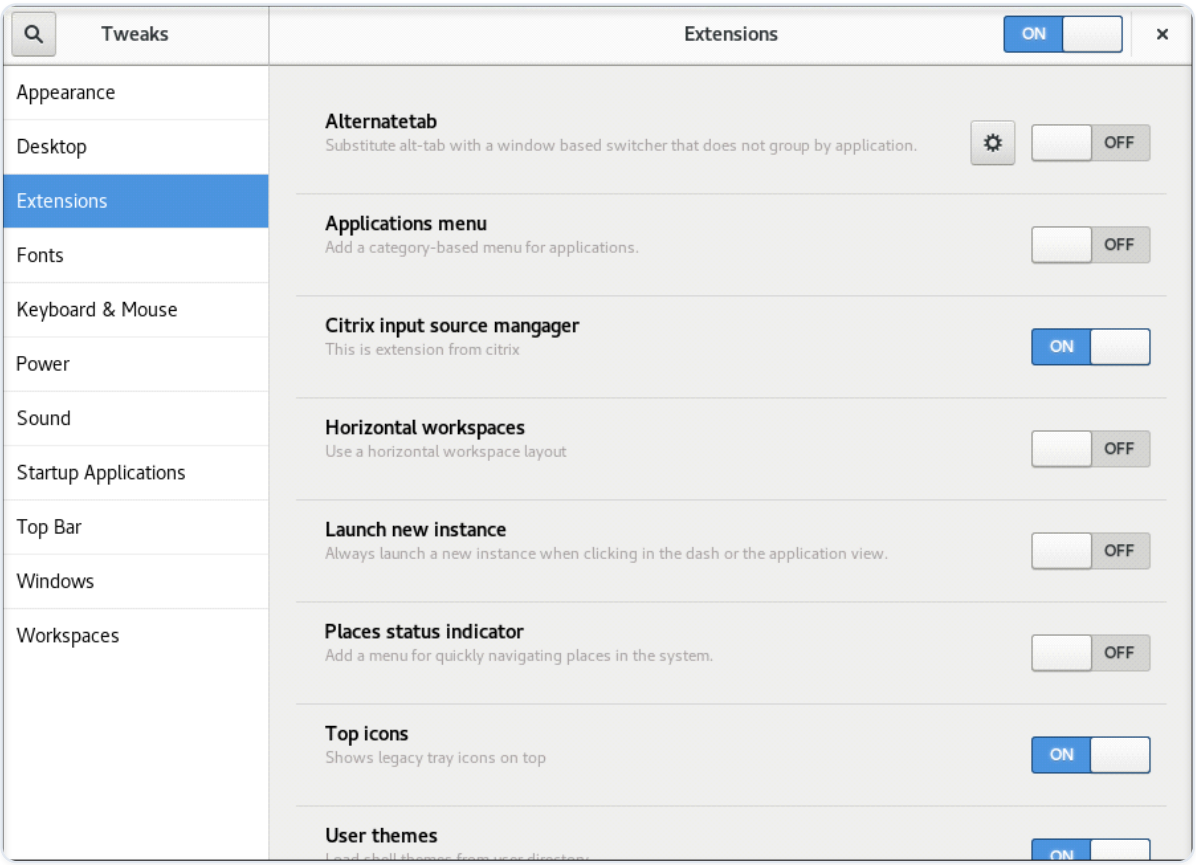


4. (**Este paso es necesario si utiliza RHEL 7.9 instalado con GNOME.**) Complete los siguientes pasos para instalar y habilitar los iconos de la bandeja del sistema de GNOME.

   a. Busque Tweaks en su pantalla de **Actividades**.

   b. Seleccione **Extensiones** en la herramienta Tweaks.

   c. Habilitar **Iconos superiores**.



d. Cierre la sesión y vuelva a iniciarla.

Visualización progresiva de Thinwire

La interactividad de la sesión puede degradarse en conexiones de bajo ancho de banda o alta latencia. Por ejemplo, el desplazamiento en una página web puede volverse lento, no responder o ser entrecortado. Las operaciones de teclado y ratón pueden ir por detrás de las actualizaciones gráficas.

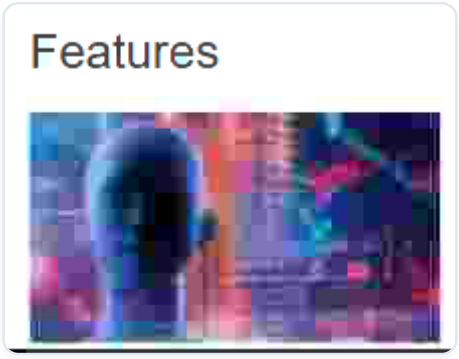
Hasta la versión 7.17, podía usar la configuración de directiva para reducir el consumo de ancho de banda configurando la sesión a una calidad visual **Baja** o estableciendo una profundidad de color inferior (gráficos de 16 o 8 bits). Sin embargo, tenía que saber que un usuario estaba en una conexión débil. HDX Thinwire no ajustaba dinámicamente la calidad de la imagen estática según las condiciones de la red.

A partir de la versión 7.18, HDX Thinwire cambia a un modo de actualización progresiva de forma predeterminada en cualquiera de los siguientes casos:

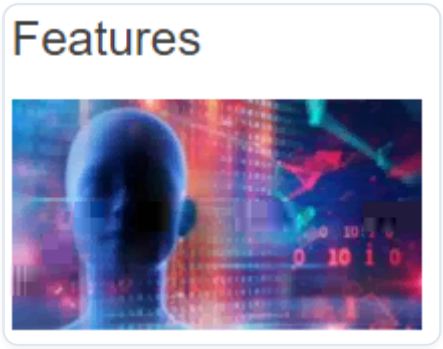
- El ancho de banda disponible cae por debajo de 2 Mbps.
- La latencia de red supera los 200 ms.

En este modo:

Por ejemplo, en el siguiente gráfico donde el modo de actualización progresiva está activo, las letras **F** y **e** tienen artefactos azules y la imagen está muy comprimida. Este enfoque reduce significativamente el consumo de ancho de banda, lo que permite que las imágenes y el texto se reciban más rápidamente y mejora la interactividad de la sesión.



Cuando deja de interactuar con la sesión, las imágenes y el texto degradados se mejoran progresivamente hasta ser sin pérdidas. Por ejemplo, en el siguiente gráfico, las letras ya no contienen artefactos azules y la imagen aparece con la calidad original.



Para las imágenes, el enfoque utiliza un método aleatorio similar a bloques. Para el texto, se enfocan letras individuales o partes de palabras. El proceso de enfoque ocurre a lo largo de varios fotogramas. Este enfoque evita introducir un retraso con un único fotograma de enfoque grande.

Las imágenes transitorias (vídeo) se siguen gestionando con la visualización adaptativa o H.264 selectivo.

Cómo se utiliza el modo progresivo

De forma predeterminada, el modo progresivo está en espera para la configuración de directiva de **Calidad visual**: **Alta**, **Media** (predeterminada) y **Baja**.

El modo progresivo se desactiva (no se usa) cuando:

- **Calidad visual** = **Siempre sin pérdidas** o **Compilación sin pérdidas**
- **Profundidad de color preferida para gráficos simples** = 8 bits

- **Usar códec de vídeo para la compresión** = **Para toda la pantalla** (cuando se desea H.264 a pantalla completa)

Cuando el modo progresivo está en espera, por defecto se habilita cuando se produce alguna de las siguientes condiciones:

- El ancho de banda disponible cae por debajo de 2 Mbps
- La latencia de red aumenta por encima de 200 ms

Después de un cambio de modo, se pasa un mínimo de 10 s en ese modo, incluso si las condiciones de red adversas son momentáneas.

Cambiar el comportamiento del modo progresivo

Puede cambiar el comportamiento del modo progresivo ejecutando el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplay" -d "<value>" --force
```

Donde \<valor\>:

0 = Siempre desactivado (no usar bajo ninguna circunstancia)

1 = Automático (alterna según las condiciones de red, valor predeterminado)

2 = Siempre activado

Cuando está en modo automático (1), puede ejecutar cualquiera de los siguientes comandos para cambiar los umbrales en los que se alterna el modo progresivo:

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
```

Donde \<valor\> es \<umbral en Kbps\> (predeterminado = 2.048)

Ejemplo: 4096 = activar el modo progresivo si el ancho de banda cae por debajo de 4 Mbps

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayLatencyThreshold" -d "<value>" --force
```

Donde \<valor\> es \<umbral en ms\> (predeterminado = 200)

Ejemplo: 100 = activar el modo progresivo si la latencia de red cae por debajo de 100 ms.

Redirección general de contenido

Asignación de unidades de cliente y redirección de carpetas de cliente

SI	ENTONCES
habilita solo la asignación de unidades de cliente en el host (VDA),	los volúmenes completos del lado del cliente se asignan automáticamente a las sesiones en el subdirectorio **ctxmnt/drivers** del directorio de inicio.
habilita la redirección de carpetas de cliente en el host (VDA) y el usuario la configura en el dispositivo de usuario (cliente),	la parte del volumen local especificada por el usuario se redirige.

Redirección de dispositivos USB

Los dispositivos USB se comparten entre la aplicación Citrix Workspace™ y el escritorio de Linux VDA. Cuando un dispositivo USB se redirige al escritorio, puede usar el dispositivo USB como si estuviera conectado localmente.

Asignación de unidades de cliente

Puede usar la asignación de unidades de cliente y la redirección de carpetas de cliente para que los archivos del lado del cliente sean accesibles en la sesión del lado del host. La comparación entre la asignación de unidades de cliente y la redirección de carpetas de cliente es la siguiente:

SI	ENTONCES
habilita solo la asignación de unidades de cliente en el host (VDA),	los volúmenes completos del lado del cliente se asignan automáticamente a las sesiones en el subdirectorio **ctxmnt** del directorio de inicio.
habilita la redirección de carpetas de cliente en el host (VDA) y el usuario la configura en el dispositivo de usuario (cliente),	se redirige la parte del volumen local especificada por el usuario.

Habilitar la asignación de unidades de cliente

Para habilitar la asignación de unidades de cliente, establezca la directiva **Redirección de unidades de cliente** en **Permitido** en Citrix Studio. Para obtener más información sobre la directiva, consulte Configuración de directiva de redirección de archivos.

Habilitar la redirección de carpetas de cliente y especificar las carpetas que se van a redirigir

Para habilitar la redirección de carpetas de cliente, ejecute el siguiente comando en el VDA:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\Client Folder Redirection" -t "REG_DWORD" -v "CFROnlyModeAvailable" -d "0x00000001" --force
```

Para especificar qué carpetas redirigir del cliente a la sesión del lado del host, siga estos pasos en el dispositivo de usuario:

1. Asegúrese de que la última versión de la aplicación Citrix Workspace™ esté instalada.
2. Desde el directorio de instalación de la aplicación Citrix Workspace, inicie **CtxCFRUI.exe**.
3. Elija el botón de opción **Custom** y agregue, edite o elimine carpetas.
4. desconectar y vuelva a conectar sus sesiones para que la configuración surta efecto.

Redirección de dispositivos USB

Los dispositivos USB se comparten entre la aplicación Citrix Workspace™ y el escritorio de Linux VDA. Cuando un dispositivo USB se redirige al escritorio, puede utilizarlo como si estuviera conectado localmente.

> **Sugerencia:**
>
> Recomendamos utilizar la redirección de dispositivos USB cuando la latencia de la red sea inferior a 100 milisegundos. No utilice la redirección de dispositivos USB cuando la latencia de la red sea superior a 200 milisegundos.

La redirección de dispositivos USB incluye tres áreas principales de funcionalidad:

- Proyecto USB/IP de código abierto
- Módulo de sesión USB de Citrix

- Módulo de servicio USB de Citrix

Proyecto USB/IP de código abierto:

El proyecto USB/IP consta de un controlador de kernel de Linux y algunas bibliotecas de modo de usuario que le permiten comunicarse con el controlador de kernel para obtener todos los datos USB.

El Linux VDA implementa la redirección de dispositivos USB basándose en el proyecto USB/IP de código abierto y reutiliza el controlador de kernel y las bibliotecas de modo de usuario de USB/IP. Sin embargo, todas las transferencias de datos USB entre el Linux VDA y la aplicación Citrix Workspace están encapsuladas por el protocolo USB de Citrix ICA.

Módulo de sesión USB de Citrix:

El módulo de sesión USB de Citrix actúa como un puente de comunicación entre el módulo de kernel USB/IP y la aplicación Citrix Workspace.

Módulo de servicio USB de Citrix:

El módulo de servicio USB de Citrix gestiona todas las operaciones en dispositivos USB, por ejemplo, conectar o desconectar dispositivos USB.

Cómo funciona la redirección de dispositivos USB

Normalmente, si un dispositivo USB se redirige correctamente al Linux VDA, se crea uno o más nodos de dispositivo en la ruta /dev del sistema. Sin embargo, a veces el dispositivo redirigido no es utilizable para una sesión activa de Linux VDA. Los dispositivos USB dependen de los controladores para funcionar correctamente y algunos dispositivos requieren controladores especiales. Si no se proporcionan los controladores, los dispositivos USB redirigidos son inaccesibles para la sesión activa de Linux VDA. Para garantizar la conectividad de los dispositivos USB, instale los controladores y configure el sistema correctamente.

El VDA de Linux admite una lista de dispositivos USB que se redirigen correctamente desde el cliente.

Dispositivos USB compatibles

> **Sugerencia:**

Hemos añadido compatibilidad con puertos USB 3.0. Puede insertar dispositivos USB 3.0 en puertos USB 3.0 de un dispositivo cliente.

Se ha comprobado que los siguientes dispositivos son compatibles con esta versión del VDA de Linux. Otros dispositivos se pueden usar libremente, pero con resultados inesperados:

DISPOSITIVO DE ALMACENAMIENTO MASIVO USB	VID:PID	SISTEMA DE ARCHIVOS
`Netac Technology Co., Ltd`	0dd8:173c	FAT32, NTFS
`Kingston Datatraveler 101 II`	0951:1625	FAT32, NTFS
`Kingston Datatraveler GT101 G2`	1567:8902	FAT32, NTFS
`SanDisk SDCZ80 flash drive`	0781:5580	FAT32, NTFS
`WD HDD`	1058:10B8	FAT32, NTFS
`Toshiba Kingston DataTraveler 3.0 USB device`	0930:6545	FAT32, NTFS
`Taiwan OEM – OBSOLETE VendorCo ProductCode Disk 2.0`	FFFF:5678	FAT32, NTFS
`TD-RDF5A Transcend USB device`	8564:4000	FAT32, NTFS

Nota:

Para usar NTFS en RHEL, Rocky Linux y SUSE, habilite primero la compatibilidad con NTFS en estas distribuciones.

RATÓN USB 3D	VID:PID
`3DConnexion SpaceMouse Pro`	046d: c62b

ESCÁNER USB	VID:PID
`Epson Perfection V330 photo`	04B8: 0142

YUBICO USB	VID:PID
`Yubico YubiKey OTP+FIDO+CCID -Keyboard, HID`	1050:0407

CÁMARA WEB USB	VID:PID
`Logitech composite USB device – WebCam, Audio`	0460:0825

Configurar la redirección de dispositivos USB

(Solo para RHEL y Rocky Linux) Instale o compile el módulo del kernel USB/IP

El VDA de Linux utiliza USB/IP como controlador de host virtual para la redirección de dispositivos USB. Dado que en la mayoría de los casos el módulo del kernel USB/IP se lanza con la versión 3.17 o posterior del kernel de Linux, no es necesario compilar el módulo del kernel de forma predeterminada. Sin embargo, el módulo del kernel USB/IP no está disponible para RHEL y Rocky Linux. Para usar la redirección de dispositivos USB con estas distribuciones de Linux, debe instalar o compilar el módulo del kernel USB/IP. Descargue e instale USB/IP desde `<https://pkgs.org/download/kmod-usbip>` según su distribución de Linux.

Establecer políticas de redirección de dispositivos USB

Una política de Citrix controla si la redirección de dispositivos USB está habilitada o deshabilitada. El tipo de dispositivo también se puede especificar mediante una política de Delivery Controller™. Al configurar la redirección de dispositivos USB para el VDA de Linux, configure las siguientes políticas:

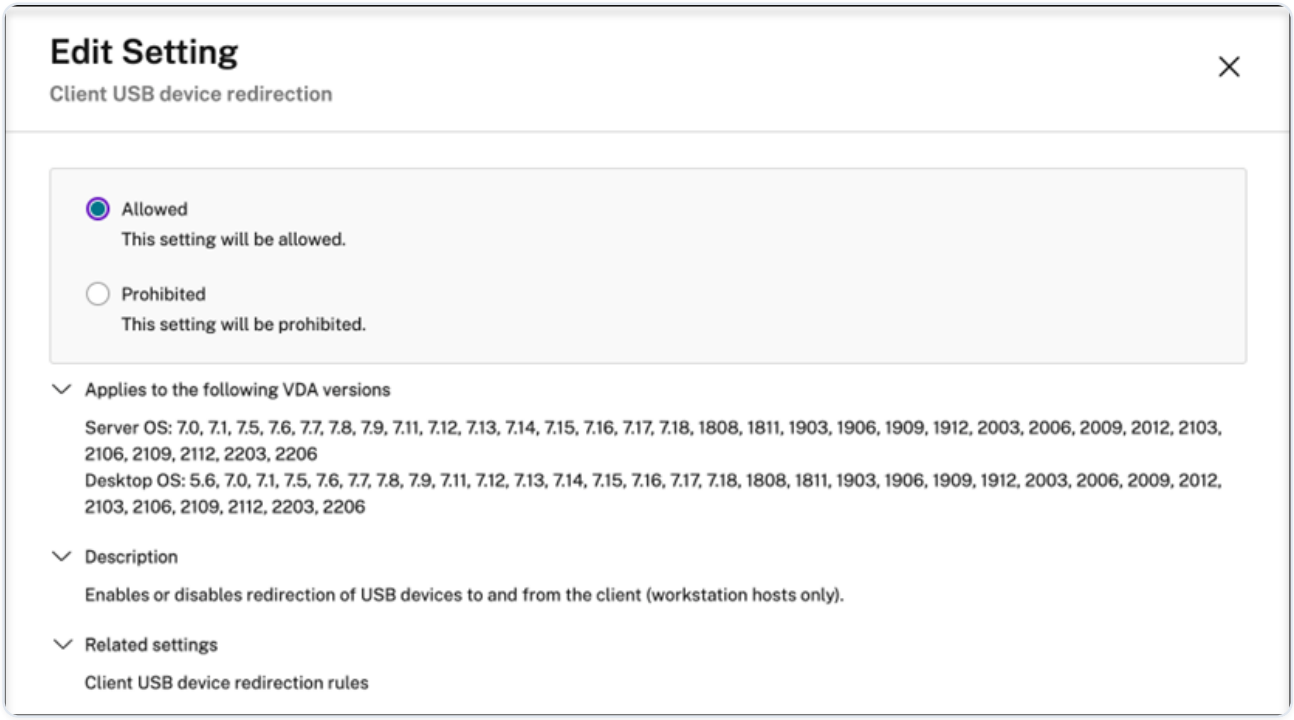
- Política de redirección de dispositivos USB del cliente
- Reglas de redirección de dispositivos USB de cliente

HABILITAR LA REDIRECCIÓN DE DISPOSITIVOS USB

En Citrix Studio, habilite (o deshabilite) la redirección de dispositivos USB desde el cliente (solo para hosts de estación de trabajo).

En el cuadro de diálogo **Editar configuración**:

1. Seleccione **Permitido**.
2. Haga clic en **Aceptar**.



ESTABLECER REGLAS DE REDIRECCIÓN DE DISPOSITIVOS USB

Después de habilitar la directiva de redirección USB, establezca las reglas de redirección mediante Citrix Studio especificando qué dispositivos están permitidos (o denegados) en el VDA de Linux.

En el cuadro de diálogo **Reglas de redirección de dispositivos USB del cliente**:

1. Haga clic en **Nuevo** para agregar una regla de redirección, o haga clic en **Editar** para revisar una regla existente.
2. Después de crear (o editar) una regla, haga clic en **Aceptar**.



Nota:

Al configurar la redirección de dispositivos USB, asegúrese de establecer la opción **Redirección de dispositivos USB del cliente** en **Permitido** y configure las **Reglas de redirección de dispositivos USB del cliente** como **Permitir:#todo correcto**. Si no se configuran ambas opciones, el ratón externo puede desaparecer al hacer clic en una sesión.

Compatibilidad con la redirección USB para Ubuntu en Azure

De forma predeterminada, Ubuntu en Azure puede no incluir ciertos controladores de kernel USB. Puede habilitar la redirección USB para dispositivos genéricos y específicos siguiendo las instrucciones a continuación.

Habilitar la redirección USB para dispositivos genéricos

Para dispositivos USB genéricos, como dispositivos de almacenamiento USB estándar, dispositivos USB HID YubiKey y adaptadores de red ASIX, puede simplemente ejecutar el siguiente script de configuración:

```
sudo /opt/Citrix/VDA/sbin/usbazure/ctxusbcfg.sh
```

Después de ejecutar el script, reinicie el servicio USB de Citrix para activar la compatibilidad:

`sudo service ctxusbsd restart`

Creación de módulos de controlador de kernel USB para dispositivos específicos

Para los dispositivos no compatibles de forma predeterminada, puede utilizar el siguiente flujo de trabajo genérico para compilar e instalar los módulos de controlador de kernel necesarios. El siguiente ejemplo utiliza un `Kingston DataTraveler 2.0 Stick (VID=0930, PID=6544)` a modo de ilustración.

Requisito previo:

- Una máquina VDA con el paquete Linux VDA instalado.
- Una máquina física Linux que ejecute un kernel de Linux genérico.

Identificar los controladores de kernel necesarios en la máquina física Linux

PASO 1: CONECTAR EL DISPOSITIVO

Conecte el dispositivo USB a una máquina física que ejecute un kernel de Linux genérico.

PASO 2: PREPARAR EL SCRIPT DE IDENTIFICACIÓN DEL CONTROLADOR DE KERNEL USB

Copie `/opt/Citrix/VDA/sbin/usbazure/ctxusbkodriver.sh` a la máquina física y hágalo ejecutable.

PASO 3: OBTENER EL VID Y PID DEL DISPOSITIVO

Utilice **lsusb** para identificar el dispositivo USB conectado.

```
lsusb

Example output:

Bus 001 Device 040: ID 0930:6544 Toshiba Corp. TransMemory-Mini / Kingston
DataTraveler 2.0 Stick
```

PASO 4: IDENTIFICAR LOS CONTROLADORES DE KERNEL NECESARIOS

Ejecute el script auxiliar con el `VID:PID` del dispositivo:

```
./ctxusbkodriver.sh 0930:6544

Example output:

All USB Kernel drivers for 0930:6544:
```

```
usb-storage
```

Compilar e instalar los controladores de kernel en la máquina VDA

PASO 1: CONFIGURAR EL ENTORNO DE COMPILACIÓN

Ejecute el script de configuración para configurar el entorno de compilación y descargar el código fuente del kernel necesario en `/root/.ctxusb`:

`sudo /opt/Citrix/VDA/sbin/usbazure/ctxusbcfg.sh`

PASO 2: DETERMINAR LA CONFIGURACIÓN DE COMPILACIÓN DEL KERNEL

Utilice el script de configuración para recuperar las opciones de compilación del módulo del kernel adecuadas:

```
sudo /opt/Citrix/VDA/sbin/usbazure/ctxusbkoconfig.sh /root/.ctxusb/linux
usb-storage

Example output:

Config option: CONFIG_USB_STORAGE

Folder: /root/.ctxusb/linux/drivers/usb/storage
```

PASO 3: INSPECCIONAR Y REGISTRAR LAS OPCIONES DE CONFIGURACIÓN DEL KERNEL

```
cd /root/.ctxusb/linux

make menuconfig
```

- Utilice la función de búsqueda (pulse /) para localizar opciones (por ejemplo, CONFIG_USB_STORAGE).
- Registre la configuración relevante (por ejemplo, CONFIG_USB_SUPPORT=y, CONFIG_USB_STORAGE=m).
- Salir sin guardar los cambios.

PASO 4: COMPILAR E INSTALAR LOS CONTROLADORES DEL KERNEL

Compile e instale el módulo del kernel:

`sudo /opt/Citrix/VDA/sbin/usbazure/ctxusbkobuild.sh /root/.ctxusb/linux/drivers/usb/storage "CONFIG_USB_SUPPORT=y CONFIG_USB_STORAGE=m"`

PASO 5 - VERIFICAR LOS CONTROLADORES DEL KERNEL

```
modinfo usb-storage
```

Una vez completado correctamente, el controlador del kernel para el dispositivo USB especificado se habrá compilado e instalado.

Solucionar problemas de redirección de dispositivos USB

Utilice la información de esta sección para solucionar varios problemas que pueden surgir al usar el VDA de Linux.

No se puede desmontar el disco USB redirigido

El VDA de Linux administra todos los discos USB redirigidos desde la aplicación Citrix Workspace bajo el privilegio administrativo para asegurarse de que solo el propietario pueda acceder al dispositivo redirigido. Como resultado, solo puede desmontar el dispositivo con el privilegio administrativo.



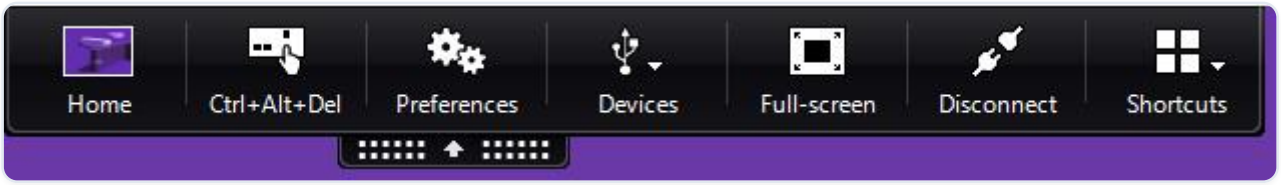
Archivo perdido al dejar de redirigir un disco USB

Si deja de redirigir un disco USB inmediatamente usando la barra de herramientas de la aplicación Citrix Workspace, los archivos que modificó o creó en el disco pueden perderse. Este problema ocurre porque cuando escribe datos en un sistema de archivos, el sistema monta la caché de memoria en el sistema de archivos. Los datos no se escriben en el propio disco. Si deja de redirigir usando la barra de herramientas de la aplicación Citrix Workspace, no queda tiempo para que los datos se vacíen en el disco, lo que resulta en la pérdida de datos.

Para resolver este problema, use el comando **sync** en un terminal para vaciar los datos en el disco antes de detener la redirección USB.

No hay dispositivos en la barra de herramientas de la aplicación Citrix Workspace

A veces, es posible que no pueda ver los dispositivos enumerados en la barra de herramientas de la aplicación Citrix Workspace, lo que indica que no se está realizando ninguna redirección USB.



Si se encuentra con el problema, verificar lo siguiente:

- La directiva está configurada para permitir la redirección de dispositivos USB.
- El módulo de servicio USB de Citrix está en ejecución.

Si la directiva no está configurada correctamente, corríjala consultando la sección Configurar directivas de redirección de dispositivos USB de este artículo.

Si el módulo de servicio USB de Citrix no está en ejecución, complete los siguientes pasos:

1. Compruebe si hay un módulo de kernel USB/IP disponible en su distribución de Linux usando el siguiente comando:

   ```
   modinfo usbip-core
   ```

2. Si la salida se muestra como sigue, instale o compile el módulo de kernel USB/IP según su distribución de Linux:

   ```
   modinfo: ERROR: Module usbip-core not found.
   ```

   - Para RHEL y Rocky Linux, consulte la sección Instalar o compilar el módulo de kernel USB/IP de este artículo.
   - Para SUSE, descargue e instale el paquete USB/IP desde `<https://software.opensuse.org/package/usbip>`.
   - Para Ubuntu/Debian, complete los siguientes pasos para compilar e instalar el módulo de kernel USB/IP:

     a. Descargue el código fuente del módulo del kernel USB/IP.

        Vaya al repositorio del kernel de Linux en `<https://github.com/torvalds/linux/tree/master/drivers/usb/usbip>`, seleccione la etiqueta de la versión del kernel de

Linux de destino (v4.15 o posterior) y obtenga el enlace como `<https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip>`.

Vaya a DownGit e introduzca el enlace anterior para crear un enlace de descarga para el código fuente de USB/IP.

b. Descomprima el archivo fuente utilizando los siguientes comandos:

```
unzip ${USBIP_SRC}.zip



cd usbip
```

c. Modifique el archivo **Makefile** de la siguiente manera:

```
# SPDX-License-Identifier: GPL-2.0



ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG



obj-$(CONFIG_USBIP_CORE) += usbip-core.o



usbip-core-y := usbip_common.o usbip_event.o



obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o



vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o



#obj-$(CONFIG_USBIP_HOST) += usbip-host.o
```

```
#usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o



#obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o



#usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.o
vudc_transfer.o vudc_main.o
```

d. Compile el código fuente:

```
apt-get install linux-headers-`uname -r`



make -C /lib/modules/`uname -r`/build M=$PWD
```

e. Instale el módulo del kernel USB/IP:

```
cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
```

f. Reinicie el servicio **ctxusbsd** para cargar el módulo del kernel USB/IP:

```
systemctl restart ctxusbsd
```

Fallo de redirección cuando los dispositivos USB son visibles en la barra de herramientas de la aplicación Citrix Workspace, pero están etiquetados como "restringidos por política"

Cuando se produzca el problema, haga lo siguiente:

- Configure la política de Linux VDA para habilitar la redirección.
- Compruebe si hay restricciones de política adicionales configuradas en el registro de la aplicación Citrix Workspace. Compruebe **DeviceRules** en la ruta del registro para asegurarse de que el acceso al dispositivo no esté denegado por esta configuración:

  HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\ICA Client\\GenericUSB

Un dispositivo USB se redirige correctamente, pero no puedo usarlo en mi sesión

Normalmente, solo se pueden redirigir dispositivos USB compatibles. Otros dispositivos también pueden redirigirse a una sesión activa de Linux VDA. Para cada dispositivo redirigido, se crea un nodo propiedad del usuario en la ruta **/dev** del sistema. Sin embargo, son los controladores y la configuración los que determinan si el usuario puede utilizar el dispositivo correctamente. Si encuentra un dispositivo que es propiedad (conectado) pero inaccesible, añada el dispositivo a una política sin restricciones.

> **Nota:**
>
> Para las unidades USB, el VDA de Linux configura y monta el disco. El usuario (y solo el propietario que lo instaló) puede acceder al disco sin ninguna configuración adicional. Puede que no sea el caso para los dispositivos que no están en la lista de dispositivos compatibles.

Redirección del Portapapeles

La redirección del Portapapeles le permite copiar y pegar datos entre aplicaciones que se ejecutan en la sesión de VDA y aplicaciones que se ejecutan en el dispositivo cliente.

Este artículo describe las directivas de Citrix® disponibles que le permiten lograr la redirección del Portapapeles.

Directivas de Citrix para la redirección del Portapapeles

Redirección del Portapapeles del cliente

Esta configuración permite o impide que el Portapapeles del dispositivo cliente se asigne al Portapapeles del VDA.

De forma predeterminada, la redirección del Portapapeles está establecida en **Permitida**.

Para evitar la transferencia de datos de copiar y pegar entre una sesión y el Portapapeles local, seleccione **Prohibida**. Los usuarios pueden seguir copiando y pegando datos entre aplicaciones que se ejecutan en las sesiones.

Límite de ancho de banda de redirección del Portapapeles

Esta configuración especifica el ancho de banda máximo permitido (kbps) para la transferencia de datos entre la sesión y los Portapapeles locales.

Porcentaje de límite de ancho de banda de redirección del Portapapeles

Esta configuración especifica el ancho de banda máximo permitido para la transferencia de datos entre la sesión y los Portapapeles locales, como porcentaje del ancho de banda total de la sesión.

Limitar el tamaño de transferencia del Portapapeles de cliente a sesión

Esta configuración especifica el tamaño máximo de los datos del Portapapeles que una única operación de copiar y pegar puede transferir de un dispositivo cliente a una sesión virtual.

Para limitar el tamaño de la transferencia del Portapapeles, habilite la configuración **Limit clipboard client to session transfer size**. A continuación, en el campo **Size Limit**, introduzca un valor en kilobytes para definir el tamaño de la transferencia de datos entre el Portapapeles local y una sesión.

De forma predeterminada, esta configuración está inhabilitada.

Limitar el tamaño de transferencia del portapapeles de sesión a cliente

Esta configuración especifica el tamaño máximo de los datos del Portapapeles que una única operación de copiar y pegar puede transferir de una sesión virtual a un dispositivo cliente.

Para limitar el tamaño de la transferencia del Portapapeles, habilite la configuración **Limit clipboard session to client transfer size**. A continuación, en el campo **Size Limit**, introduzca un valor en kilobytes para definir el tamaño de la transferencia de datos entre una sesión y el Portapapeles local.

De forma predeterminada, esta configuración está inhabilitada.

Restringir la escritura del Portapapeles del cliente Y Formatos permitidos para la escritura del Portapapeles del cliente

Al habilitar estas dos configuraciones, puede permitir que se copien y peguen formatos de datos específicos de la sesión al cliente (escritura en el cliente).

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB

- CF_PALETTE
- CF_UNICODETEXT
- CF_LOCALE
- CF_DIBV5
- CF_HDROP

Restringir la escritura del portapapeles de la sesión Y Formatos permitidos para la escritura del portapapeles de la sesión

Al habilitar las dos configuraciones, puede permitir que se copien y peguen formatos de datos específicos del cliente a la sesión (escribiendo en la sesión).

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_LOCALE
- CF_DIBV5
- CF_HDROP

Teclado

Esta sección contiene los siguientes temas:

- IME de cliente
- Sincronización de la interfaz de usuario del IME de cliente
- Sincronización dinámica de la distribución del teclado
- Teclado virtual
- Compatibilidad con varias entradas de idioma

Configuración de la extensión de teclado X (XKB)

A partir de la versión 2407, el VDA de Linux especifica evdev como la regla XKB predeterminada para la configuración del teclado. Esta decisión se puede justificar por varias razones:

- La mayoría de las distribuciones modernas de Linux utilizan la regla XKB de evdev de forma predeterminada.
- Casi todas las aplicaciones siguen el patrón de código de tecla de la regla XKB de evdev.
- La regla XKB de evdev proporciona soporte extendido para una amplia gama de símbolos de teclas más allá de los caracteres alfanuméricos básicos y las teclas de función típicas, como 'Cancel', 'Redo', 'Undo', 'XF86Copy', 'XF86Open' y 'XF86Paste'.
- La regla XKB de evdev en Linux aborda varios problemas relacionados con el teclado, en particular los relacionados con respuestas incorrectas a las entradas de teclas.

Si desea volver a la regla XFree86, puede realizar la siguiente configuración de registro:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar"
-v "XkbRuleName" -d "xorg"
```

En este comando, solo el texto exacto que distingue entre mayúsculas y minúsculas 'xorg' se reconoce como el conjunto de reglas 'xfree86'; cualquier otro valor de entrada es ineficaz.

Editor de métodos de entrada (IME) del cliente

Información general

Los caracteres de doble byte, como los caracteres chinos, japoneses y coreanos, deben escribirse a través de un IME. Escriba estos caracteres con cualquier IME que sea compatible con la aplicación Citrix Workspace™ en el lado del cliente, como el IME CJK nativo de Windows.

Instalación

Esta función se instala automáticamente al instalar el VDA de Linux.

Uso

Abra una sesión de Citrix Virtual Apps o Citrix Virtual Desktops™ como de costumbre.

Cambie su método de entrada según sea necesario en el lado del cliente para empezar a usar la función IME del cliente.

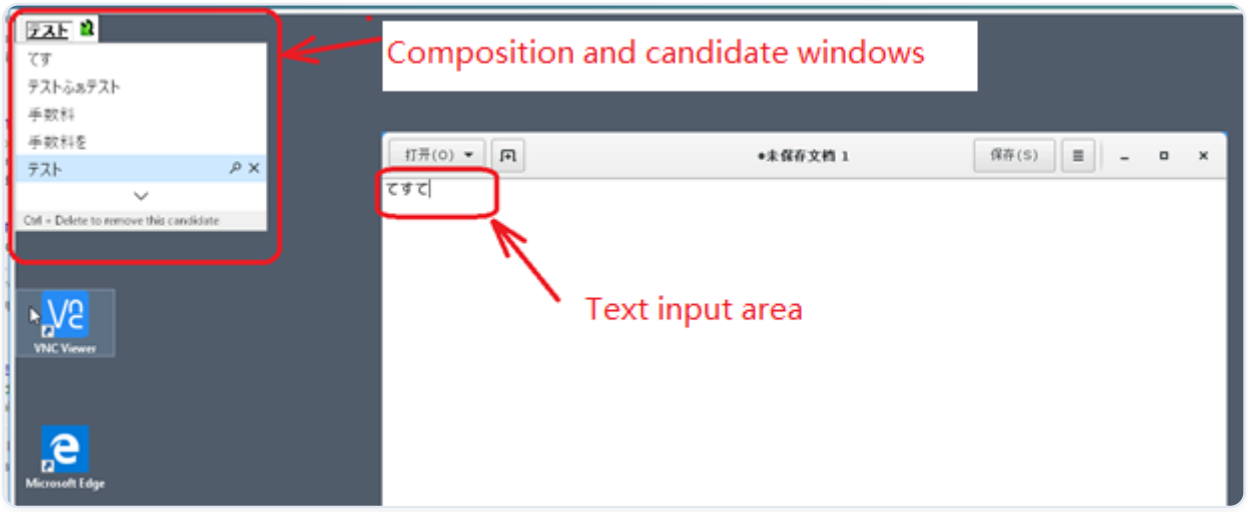
Problemas conocidos

- Hacer doble clic en una celda de una hoja de cálculo de Google es imprescindible antes de poder usar la función IME del cliente para escribir caracteres en la celda.
- La función IME del cliente no se deshabilita automáticamente en los campos de contraseña.
- La interfaz de usuario del IME no sigue el cursor en el área de entrada.

Sincronización de la interfaz de usuario del IME del cliente

Información general

Hasta la fecha, la interfaz de usuario del IME del cliente (incluidas la ventana de composición y la ventana de candidatos) se colocaba en la esquina superior izquierda de la pantalla. No seguía el cursor y, a veces, se encontraba lejos del cursor en el área de entrada de texto:



Citrix® mejora la facilidad de uso y la experiencia del usuario con el IME del cliente de la siguiente manera:



Requisitos previos para usar la función

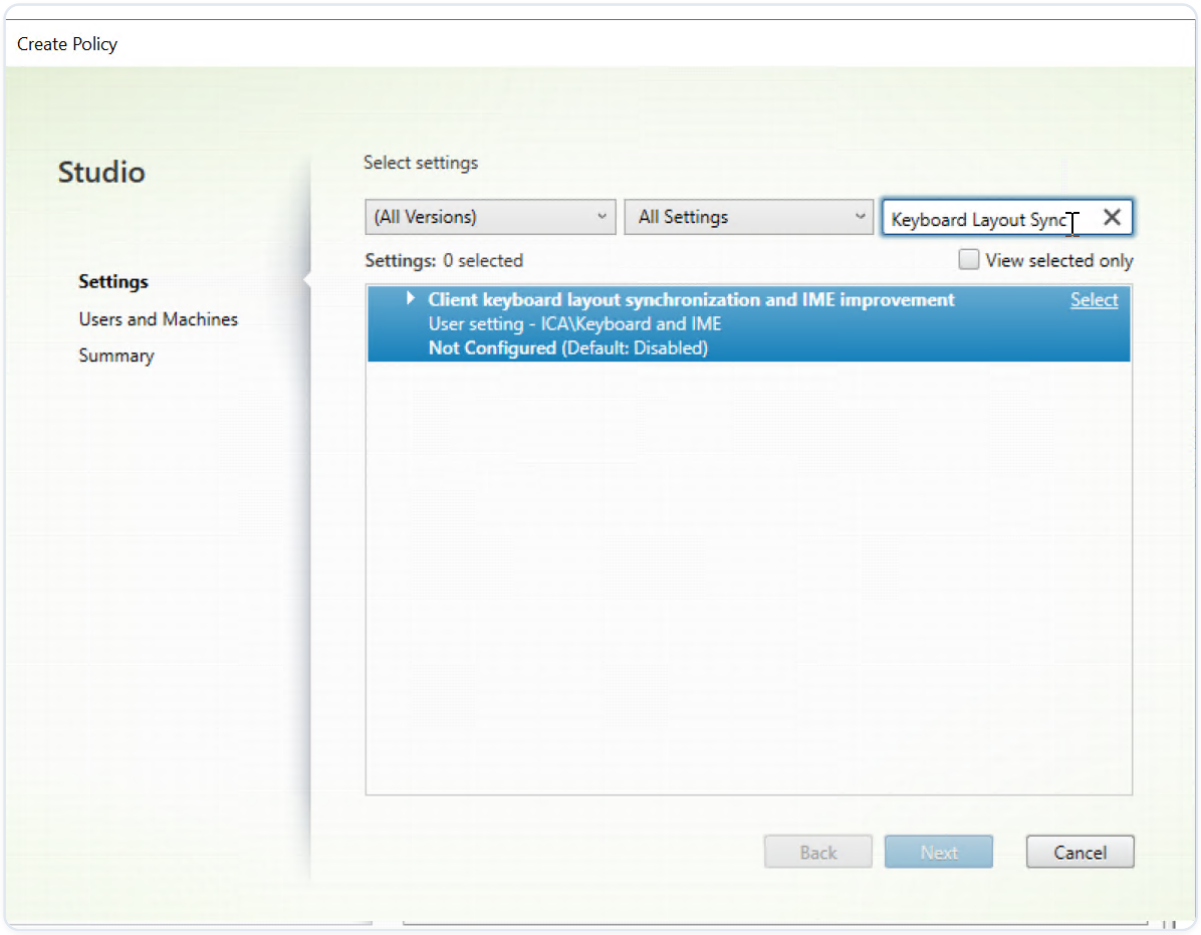
1. Habilite Intelligent Input Bus (`IBus`) en su Linux VDA. Para obtener información sobre cómo habilitar `IBus` en un sistema operativo Linux, consulte la documentación del proveedor del sistema operativo. Por ejemplo:
   - Ubuntu: `<https://help.ubuntu.com/community/ibus>`
   - CentOS, RHEL: `<https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods>`
   - Debian: `<https://wiki.debian.org/I18n/ibus>`
   - SUSE: `<https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang>`
2. La función se instala automáticamente, pero debe habilitarla antes de poder usarla.

Habilitar y deshabilitar la función

La función de sincronización de la interfaz de usuario del IME del cliente está inhabilitada de forma predeterminada. Para habilitar o inhabilitar la función, configure la directiva **Client Keyboard Layout Sync and IME Improvement** o edite el registro mediante la utilidad `ctxreg`.

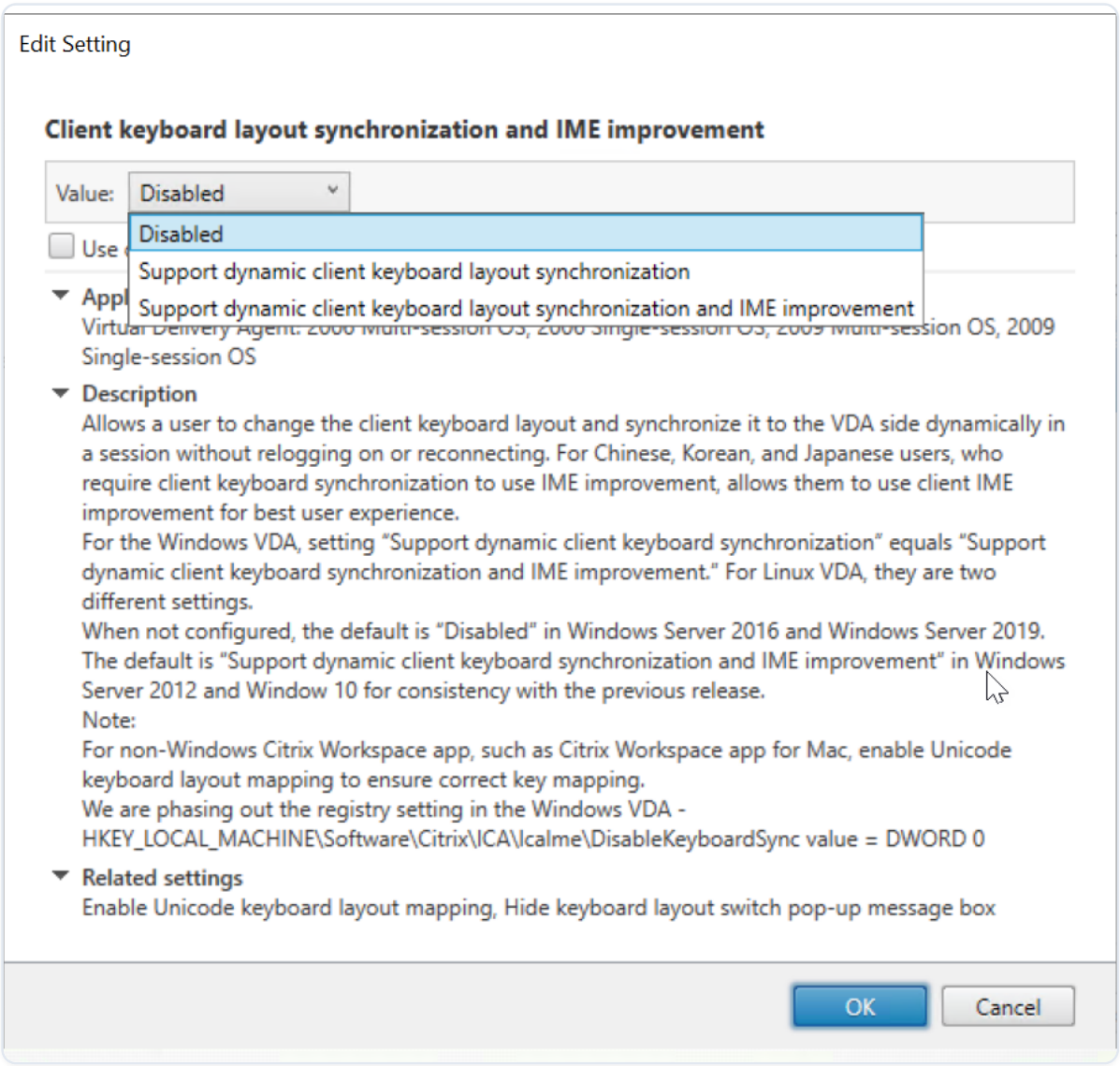
> **Nota:**
>
> La directiva **Client Keyboard Layout Sync and IME Improvement** tiene prioridad sobre la configuración del registro y se puede aplicar a los objetos de usuario y máquina que especifique o a todos los objetos de su sitio. La configuración del registro en un Linux VDA determinado se aplica a todas las sesiones de ese VDA.

- Establezca la directiva **Client Keyboard Layout Sync and IME Improvement** para habilitar o deshabilitar la sincronización de la interfaz de usuario de IME del cliente:
  a. En Studio, haga clic con el botón derecho en **Policies** y seleccione **Create Policy**.
  b. Busque la directiva **Client Keyboard Layout Sync and IME Improvement**.



c. Haga clic en **Select** junto al nombre de la directiva.

d. Establezca la directiva.



Hay tres opciones disponibles:

- **Disabled**: deshabilita la sincronización dinámica del diseño del teclado y la sincronización de la interfaz de usuario de IME del cliente.
- **Support dynamic client keyboard layout synchronization**: habilita la sincronización dinámica del diseño del teclado, independientemente del valor DWORD de la clave de registro **SyncKeyboardLayout** en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- **Support dynamic client keyboard layout synchronization and IME improvement**: habilita tanto la sincronización dinámica del diseño del teclado como la sincronización de la interfaz de usuario de IME del cliente, independientemente de los valores DWORD de las claves de registro **SyncKeyboardLayout** y **SyncClientIME** en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.

- Edite el registro mediante la utilidad `ctxreg` para habilitar o deshabilitar la sincronización de la interfaz de usuario de IME del cliente:

  Para habilitar la función, ejecute el comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v  "SyncClientIME" -d "0x00000001"
  ```

  Para deshabilitar la función, ejecute el comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncClientIME" -d "0x00000000"
  ```

Sincronización dinámica de la distribución del teclado

Anteriormente, la distribución del teclado en el VDA de Linux y en el dispositivo cliente tenía que ser la misma. Podrían producirse problemas de asignación de teclas, por ejemplo, cuando la distribución del teclado cambiaba de inglés a francés en el dispositivo cliente, pero no en el VDA.

Citrix® resuelve el problema sincronizando automáticamente la distribución del teclado del VDA con la distribución del teclado del dispositivo cliente. Cada vez que la distribución del teclado cambia en el dispositivo cliente, la distribución en el VDA hace lo mismo.

Nota:

La aplicación Citrix Workspace™ para HTML5 no admite la función de sincronización dinámica de la distribución del teclado.

Configuración

La función de sincronización dinámica de la distribución del teclado está inhabilitada de forma predeterminada. Para habilitar o inhabilitar la función, configure la directiva **Sincronización de la distribución del teclado del cliente y mejora del IME** o modifique el Registro mediante la utilidad `ctxreg`.

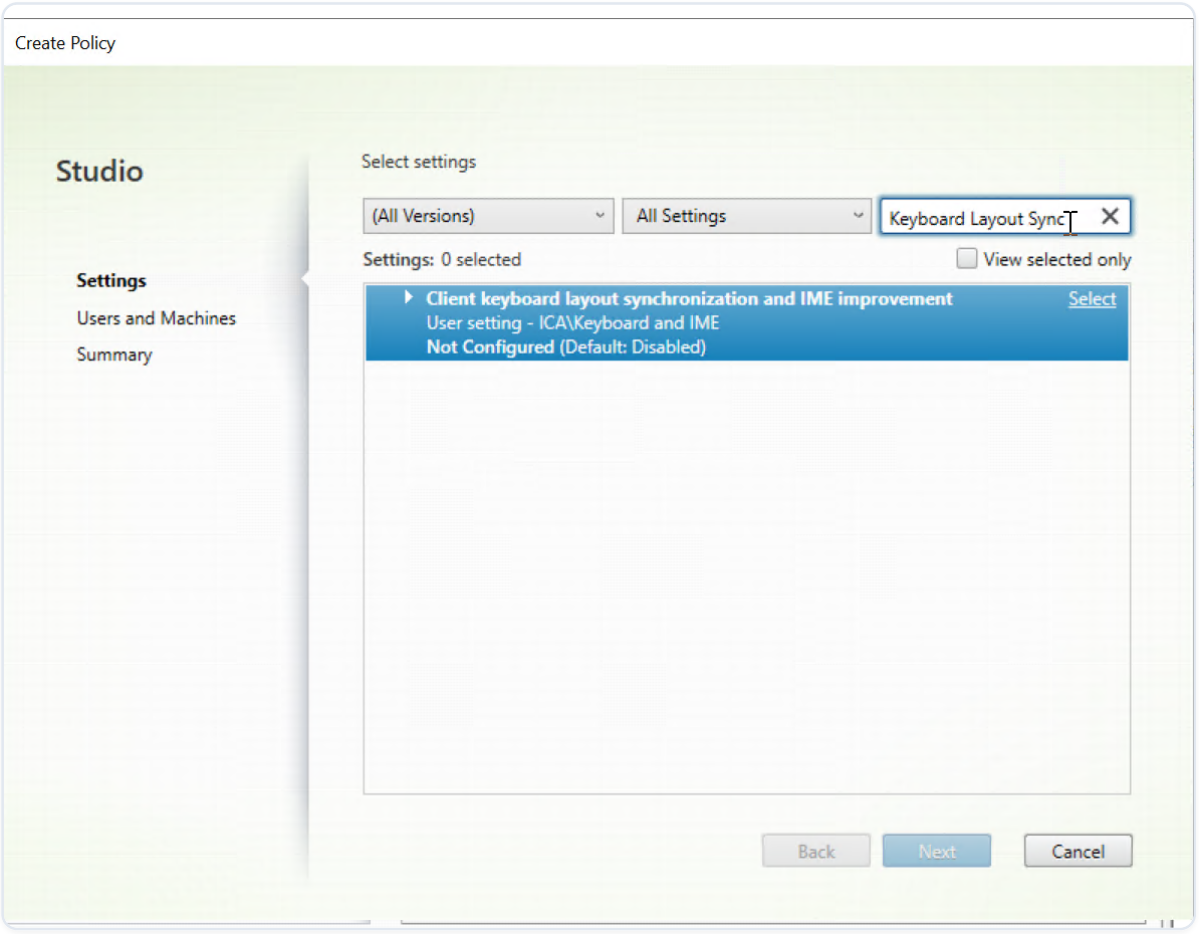
Nota:

> La directiva **Sincronización de la distribución del teclado del cliente y mejora del IME** tiene prioridad sobre la configuración del Registro y se puede aplicar a los objetos de usuario y máquina que especifique o a todos los objetos de su sitio. La configuración del Registro en un VDA de Linux determinado se aplica a todas las sesiones de ese VDA.

- Configure la directiva **Sincronización de la distribución del teclado del cliente y mejora del IME** para habilitar o inhabilitar la función de sincronización dinámica de la distribución del teclado:

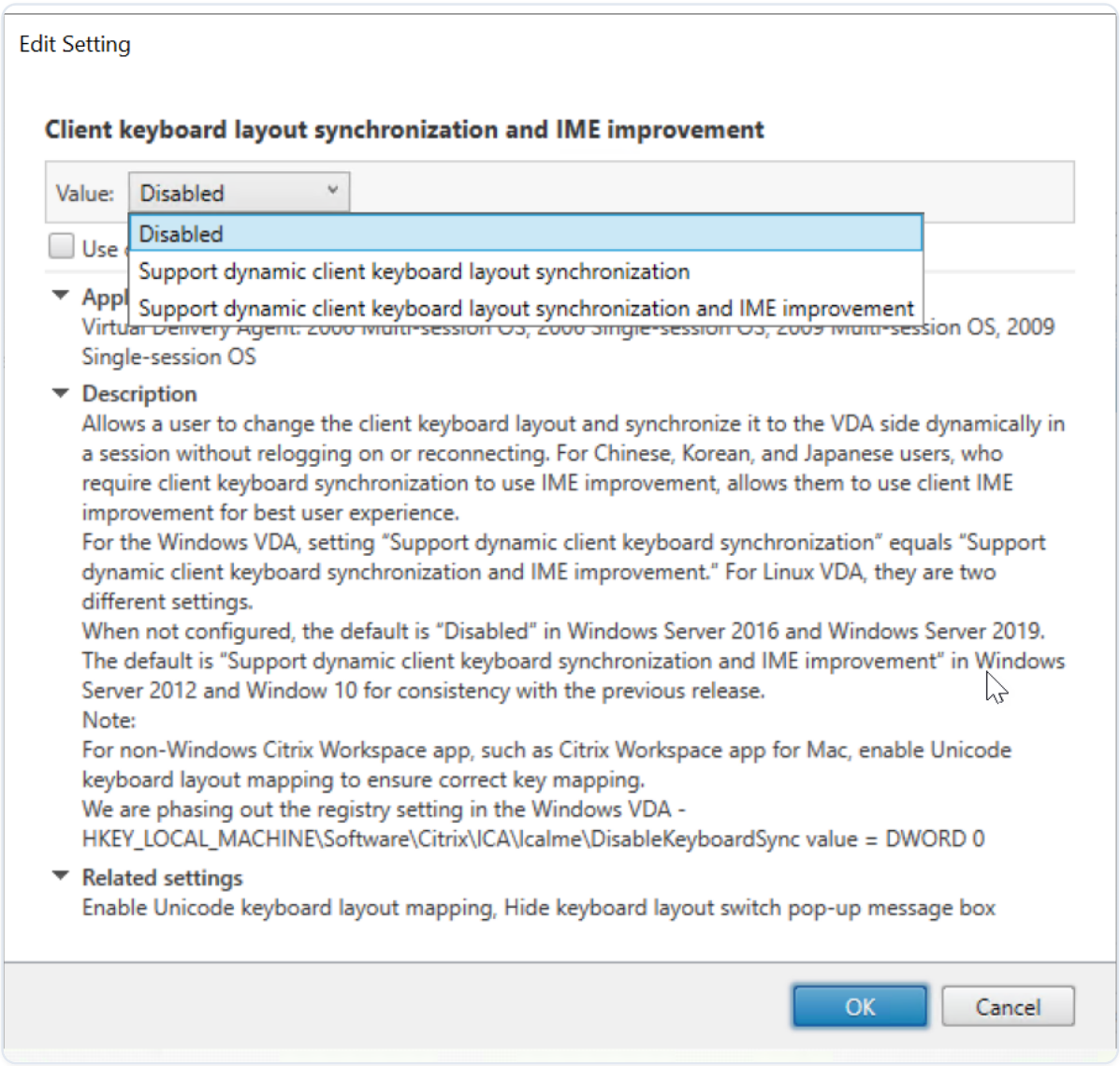
  a. En Studio, haga clic con el botón secundario en **Directivas** y seleccione **Crear directiva**.

  b. Busque la directiva **Sincronización de la distribución del teclado del cliente y mejora del IME**.



  c. Haga clic en **Seleccionar** junto al nombre de la directiva.

  d. Configure la directiva.



Hay tres opciones disponibles:

- **Inhabilitada**: inhabilita la sincronización dinámica de la distribución del teclado y la sincronización de la interfaz de usuario del IME del cliente.
- **Admitir la sincronización dinámica de la distribución del teclado del cliente**: habilita la sincronización dinámica de la distribución del teclado, independientemente del valor DWORD de la clave del Registro **SyncKeyboardLayout** en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- **Admitir la sincronización dinámica del diseño del teclado del cliente y la mejora del IME**: habilita la sincronización dinámica del diseño del teclado y la sincronización de la interfaz de usuario del IME del cliente, independientemente de los valores DWORD de las claves de registro **SyncKeyboardLayout** y **SyncClientIME** en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.

- Edite el registro mediante la utilidad `ctxreg` para habilitar o deshabilitar la función de sincronización dinámica del diseño del teclado:

  Para habilitar esta función, ejecute el comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000001"
  ```

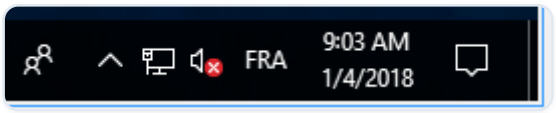
  Para deshabilitar esta función, ejecute el comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000000"
  ```

Uso

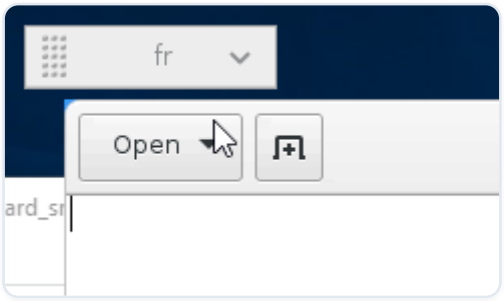
Con esta función habilitada, cuando el diseño del teclado cambia en el dispositivo cliente durante una sesión, el diseño del teclado de la sesión cambia en consecuencia.

Por ejemplo, si cambia el diseño del teclado en un dispositivo cliente a francés (FR):



Entonces, el diseño del teclado de la sesión de Linux VDA también cambia a "fr".

En una sesión de aplicación, puede ver este cambio automático si ha habilitado la barra de idioma:

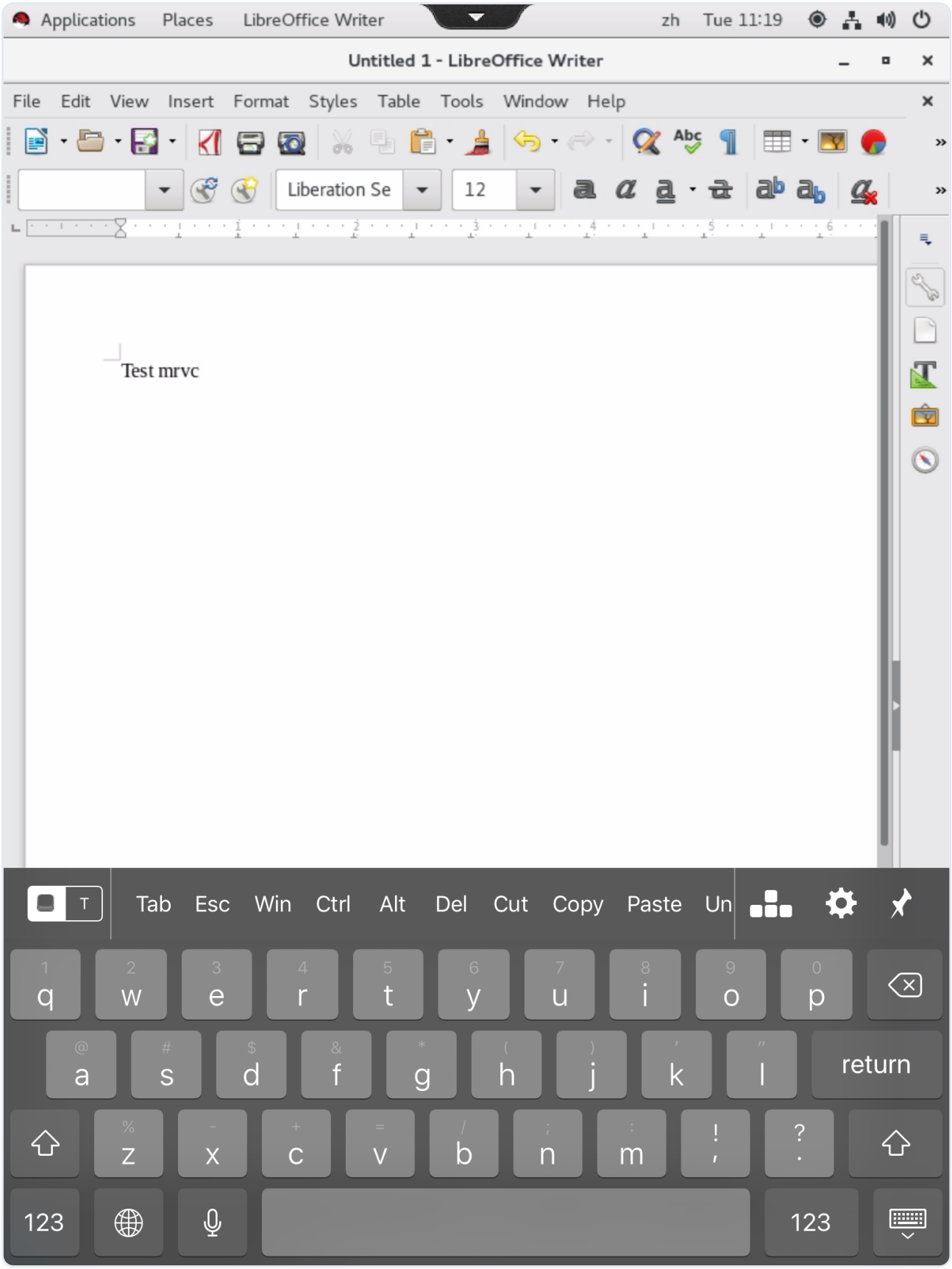


En una sesión de escritorio, puede ver este cambio automático en la barra de tareas:



Teclado en pantalla

La función de teclado en pantalla está disponible en una sesión de aplicación o escritorio virtual de Linux. El teclado en pantalla se muestra u oculta automáticamente al entrar o salir de un campo de entrada.


Applications
Places
LibreOffice Writer
zh
Tue 11:19
Untitled 1 - LibreOffice Writer
File
Edit
View
Insert
Format
Styles
Table
Tools
Window
Help
Liberation Se
12
Test mrvc
Tab
Esc
Win
Ctrl
Alt
Del
Cut
Copy
Paste
Un
return
123
123

Nota:

> La función es compatible con Citrix Workspace™ app para iOS y para Android.

Habilitar y deshabilitar la función

La función está inhabilitada de forma predeterminada. Utilice la utilidad **ctxreg** para habilitar o inhabilitar la función. La configuración de la función en un Linux VDA determinado se aplica a todas las sesiones de ese VDA.

Para habilitar la función:

1. Ejecute el comando:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
   "Enabled" -d "0x00000001"
   ```

2. En Citrix Studio, establezca la directiva **Visualización automática del teclado** en **Permitido**.
3. (Opcional) Para RHEL 7 y CentOS 7, ejecute el siguiente comando para configurar Intelligent Input Bus (`IBus`) como el servicio de MI predeterminado:

   ```
   echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
   ```

Para inhabilitar la función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

Nota:

> La configuración anterior surte efecto al iniciar una nueva sesión o al cerrar la sesión actual y volver a iniciarla.

Limitaciones

- Es posible que la función no funcione como se espera con Google Chrome, LibreOffice y otras aplicaciones.

- Para volver a mostrar el teclado en pantalla después de ocultarlo manualmente, haga clic en un campo que no sea de entrada y, a continuación, en el campo de entrada actual de nuevo.
- Es posible que el teclado en pantalla no aparezca al hacer clic de un campo de entrada a otro en un explorador web. Para solucionar este problema, haga clic en un campo que no sea de entrada y, a continuación, en el campo de entrada de destino.
- La función no admite caracteres Unicode ni caracteres de doble byte (como los caracteres chinos, japoneses y coreanos).
- El teclado en pantalla no está disponible para los campos de entrada de contraseña.
- El teclado en pantalla puede superponerse al campo de entrada actual. En este caso, mueva la ventana de la aplicación o desplace la pantalla hacia arriba para mover el campo de entrada a una posición accesible.
- Debido a problemas de compatibilidad entre la aplicación Citrix Workspace y las tabletas Huawei, el teclado en pantalla aparece en las tabletas Huawei incluso con un teclado físico conectado.

Compatibilidad con varias entradas de idioma

A partir de la versión 1.4 de Linux VDA, Citrix ha añadido compatibilidad con aplicaciones publicadas. Los usuarios pueden acceder a la aplicación Linux deseada sin el entorno de escritorio Linux.

Sin embargo, la barra de idioma nativa en Linux VDA no estaba disponible para la aplicación publicada porque la barra de idioma está muy integrada con el entorno de escritorio Linux. Como resultado, los usuarios no podían introducir texto en un idioma que requiriera IME, como chino, japonés o coreano. Tampoco era posible para los usuarios cambiar entre diseños de teclado durante una sesión de aplicación.

Para solucionar esos problemas, esta función proporciona una barra de idioma para las aplicaciones publicadas que aceptan la entrada de texto. La barra de idioma permite a los usuarios seleccionar un IME del lado del servidor y cambiar entre diseños de teclado durante una sesión de aplicación.

Configuración

Puede usar la utilidad **ctxreg** para habilitar o inhabilitar esta función (inhabilitada de forma predeterminada). La configuración de la función en un servidor Linux VDA determinado se aplica a todas las aplicaciones publicadas en ese VDA.

La clave de configuración es "HKEY_LOCAL_MACHINE \\SYSTEM\\CurrentControlSet\\Control\\Citrix\\LanguageBar" y el tipo es DWORD.

Para habilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000001"
```

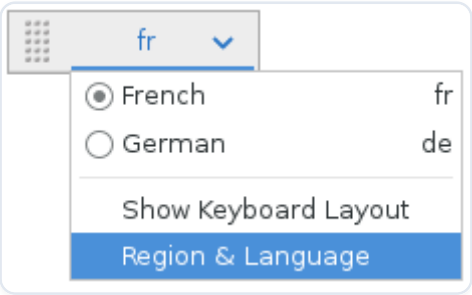
Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000000"
```

Uso

El uso es sencillo.

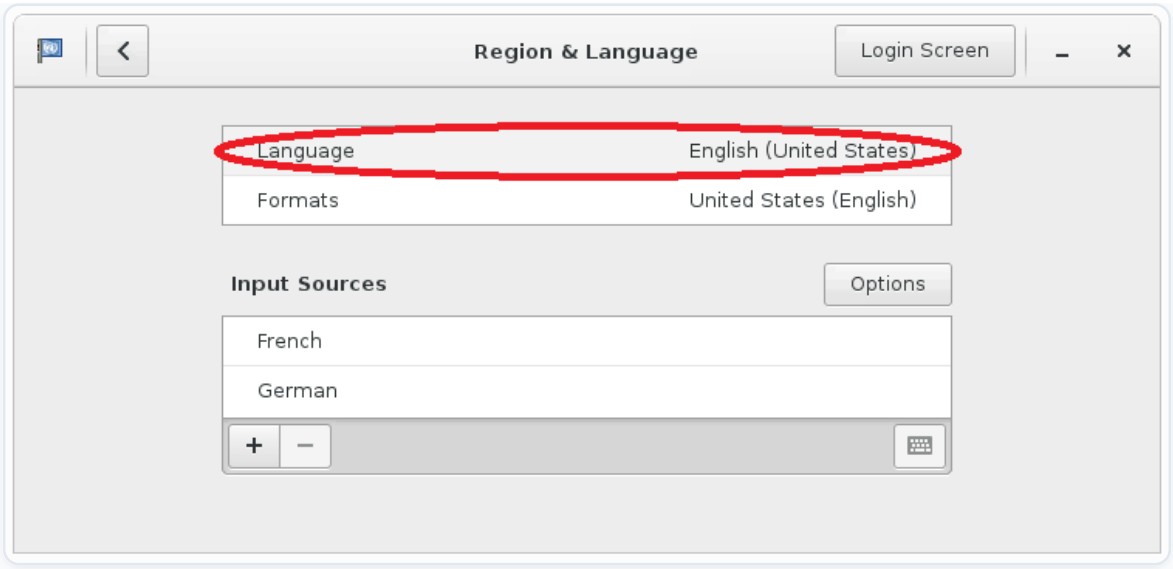
1. Habilite la función.
2. Acceda a una aplicación publicada que pueda aceptar la entrada de texto. Aparecerá una barra de idioma en la sesión, junto a la aplicación.
3. En el menú desplegable, seleccione **Región e idioma** para agregar el idioma deseado (origen de entrada).



4. Seleccione el IME o el diseño de teclado en el menú desplegable.
5. Escriba un idioma usando el IME o el diseño de teclado seleccionados.

> **Nota:**

- Cuando cambie la distribución del teclado en la barra de idioma del lado del VDA, asegúrese de que se utilice la misma distribución del teclado en el lado del cliente (que ejecuta la aplicación Citrix Workspace™).
- El paquete **accountsservice** debe actualizarse a la versión 0.6.37 o posterior antes de poder realizar ajustes en el cuadro de diálogo **Región e idioma**.



Multimedia

Esta sección contiene los siguientes temas:

- Funciones de audio
- Redirección de contenido del explorador
- Compresión de vídeo de cámara web HDX

Funciones de audio

Audio adaptable

Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en el VDA. El audio adaptable optimiza la configuración para su entorno y reemplaza los formatos de compresión de audio obsoletos para proporcionar una excelente experiencia de usuario.

El audio adaptable está habilitado de forma predeterminada. Es compatible con los siguientes clientes de la aplicación Citrix Workspace™:

- Aplicación Citrix Workspace para Windows – versiones 2109 y posteriores
- Aplicación Citrix Workspace para Linux – versiones 2109 y posteriores
- Aplicación Citrix Workspace para Mac – versiones 2109 y posteriores

El audio adaptable recurre al audio heredado cuando se utiliza un cliente no incluido en la lista.

Consideraciones sobre el servicio de audio

El VDA de Linux es compatible con PipeWire en Debian 12.x, RHEL 9.x, Rocky Linux 9.x y Ubuntu 24.04, donde es el servicio de audio predeterminado. Para las demás distribuciones, siga utilizando PulseAudio.

PulseAudio

- Utilice PulseAudio 13.99 o posterior en RHEL 8.x y Rocky Linux 8.x.

PipeWire

El VDA de Linux solo es compatible con PipeWire en Debian 12.x, RHEL 9.x, Rocky Linux 9.x y Ubuntu 24.04. A continuación, se presentan algunas consideraciones:

- Si tiene instalada la versión 2407 o posterior del VDA de Linux en Debian 12.x, RHEL 9.x o Rocky Linux 9.x, está utilizando PipeWire.
- Si tiene instalada la versión 2411 o posterior del VDA de Linux en Ubuntu 24.04, está utilizando PipeWire.
- Si tiene instalada una versión del VDA de Linux anterior a la 2407 en RHEL 9.x o Rocky Linux 9.x, está utilizando PulseAudio. Para seguir utilizando PulseAudio, no haga nada. Para cambiar a PipeWire, siga estos pasos:

  a. Sustituya el paquete de PulseAudio por pipewire-pulseaudio:

  ```
  dnf swap --allowerasing pulseaudio pipewire-pulseaudio
  ```

  b. Habilitar los servicios relacionados con PipeWire globalmente:

  ```
  systemctl --global --now enable pipewire pipewire-pulse pipewire-pulse.socket wireplumber
  ```

  c. Reinicie el VDA de Linux.

- Si el idioma del sistema de su máquina Linux no es inglés y el servicio de audio es PipeWire, siga estos pasos para garantizar la funcionalidad del audio:

  a. Abra el archivo ubicado en: /etc/xdg/autostart/ctxaudio.desktop

  b. Localice la siguiente línea: Exec=/opt/Citrix/VDA/bin/ctxaudio

  c. Reemplácela por: Exec=env LC_ALL=C /opt/Citrix/VDA/bin/ctxaudio

  Este cambio fuerza a ctxaudio a usar la configuración regional `C`, lo que garantiza la compatibilidad con PipeWire en entornos que no son en inglés.

Modo tolerante a pérdidas para audio

El modo tolerante a pérdidas admite audio. Esta función mejora la experiencia del usuario para la transmisión en tiempo real y mejora la calidad del audio a través de EDT cuando los usuarios se conectan a través de redes con alta latencia y pérdida de paquetes.

Para obtener más información sobre el modo tolerante a pérdidas y EDT, consulte Información adicional en la documentación de Citrix Virtual Apps and Desktops.

Habilitar la función de modo tolerante a pérdidas para audio

El modo tolerante a pérdidas para audio está habilitado de forma predeterminada. Si está deshabilitado, siga estos pasos para volver a habilitarlo:

1. Habilite el transporte adaptativo configurando la directiva transporte adaptativo HDX. El transporte adaptativo está habilitado de forma predeterminada.
2. Habilite el audio adaptativo configurando la directiva audio adaptativo. El audio adaptativo está habilitado de forma predeterminada.
3. Habilite el modo tolerante a pérdidas (transporte no fiable de EDT) configurando la directiva modo tolerante a pérdidas para audio.
4. Para conexiones directas, se requiere habilitar DTLS en los VDA.
5. Para conexiones remotas, el modo tolerante a pérdidas de EDT también debe ser compatible con Citrix Gateway Service o NetScaler Gateway.

Requisitos y configuración del cliente

Para usar el modo tolerante a pérdidas para el audio, asegúrese de que su aplicación Citrix Workspace lo admita y esté configurada para habilitar esta función; de lo contrario, el audio recurrirá al transporte fiable de EDT.

Las siguientes son las versiones mínimas de la aplicación Citrix Workspace que admiten el modo tolerante a pérdidas:

- Citrix Workspace app para Windows, versión mínima 2309
- Citrix Workspace app para Linux, versión mínima 2311
- Citrix Workspace app para Mac, versión mínima 2311

Herramienta de línea de comandos de diagnóstico de audio

La herramienta de línea de comandos de diagnóstico de audio en el VDA se puede utilizar para consultar datos de sesión relacionados con las directivas de audio, la configuración y el transporte de datos.

Uso

Abra un símbolo del sistema y ejecute `ctxaudiosession` desde la carpeta `/opt/Citrix/VDA/bin`.

La ejecución de la herramienta mostrará toda la información de audio de las sesiones ICA® activas y el estado de redirección de dispositivos para el usuario actual.

Salida

La herramienta muestra varias configuraciones que pueden ayudar a diagnosticar problemas relacionados con el audio dentro de una sesión.

SECCIÓN	DESCRIPCIÓN
Advertencia	Mensajes de advertencia del servicio de audio para estados de dispositivos, tipo de transporte, códec de audio, etc.
Información de estado	Estado de audio, versión, códecs, transporte aplicado a la(s) sesión(es) actual(es), etc.
Configuración de directivas	Directivas de audio aplicadas a la sesión o sesiones actuales.
Configuración local	Configuración relacionada con el audio almacenada en el registro o en la configuración local.

SECCIÓN	DESCRIPCIÓN
Capacidades	Resultados de las capacidades de audio entre CWA y VDA.
Dispositivos de sonido	Nombres de dispositivos, sus funciones y sus estados de ejecución en la(s) sesión(es).

Mejorador de calidad de audio para el modo tolerante a pérdidas de EDT

A partir de la versión 2507, el mejorador de calidad de audio está habilitado de forma predeterminada para audio adaptable a través de EDT modo tolerante a pérdidas para audio.

El mejorador de calidad de audio mantiene un audio claro durante interrupciones breves de la red. Esta función se adapta a las condiciones de la red para garantizar un rendimiento de audio constante durante la reproducción y la grabación.

> **Nota:**
>
> Para que esta función funcione, debe estar habilitado el Audio adaptativo.

Compatibilidad con varios dispositivos de audio

Información general

A partir de la versión 2311, Linux VDA introduce una función de redirección de audio. Esta función permite redirigir varios dispositivos de audio de la máquina cliente donde está instalada la aplicación Citrix Workspace a la sesión remota de Linux VDA.

Con la función habilitada:

- Todos los dispositivos de audio locales de la máquina cliente se muestran en una sesión. En lugar de CitrixAudioSink (salida de audio) o CitrixAudioSource (entrada de audio), los dispositivos de audio aparecen con sus respectivos nombres de dispositivo.
- Los dispositivos de audio dentro de las sesiones se actualizan dinámicamente al conectar o desconectar uno.

Configuración

Para usar la función, habilítela en Linux VDA y elija una aplicación Citrix Workspace compatible.

HABILITAR LA FUNCIÓN EN LINUX VDA

La compatibilidad con varios dispositivos de audio está habilitada de forma predeterminada. Para inhabilitar o volver a habilitar la función, ejecute los siguientes comandos, respectivamente:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\\System\
\CurrentControlSet\\Control\\Citrix\\VirtualChannels\\Audio" -v
"fEnableAudioRedirectionV4" -d "0"
```

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\\System\
\CurrentControlSet\\Control\\Citrix\\VirtualChannels\\Audio" -v
"fEnableAudioRedirectionV4" -d "1"
```

REQUISITOS Y CONFIGURACIÓN DEL CLIENTE

La función solo es compatible con los siguientes clientes:

- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para Linux, versión mínima 2212
- Aplicación Citrix Workspace para HTML5, versión mínima 2306
- Aplicación Citrix Workspace para Chrome, versión mínima 2306
- Aplicación Citrix Workspace para Mac, versión mínima 2311
- Aplicación Citrix Workspace para Android, versión mínima 2405

Se requieren los ajustes adecuados en la aplicación Citrix Workspace para que la función funcione como se espera. Para obtener más información, consulte la documentación de Citrix Workspace app.

Problemas conocidos

Debido a un problema con PulseAudio, los intentos de cambiar entre dispositivos de audio pueden fallar en una sesión de Ubuntu 22.04. Para solucionar el problema, elimine la configuración de PulseAudio para el usuario de la sesión actual del VDA y, a continuación, vuelva a abrir la sesión. Para eliminar la configuración de PulseAudio, ejecute el comando `$ rm -r ~/.config/pulse`.

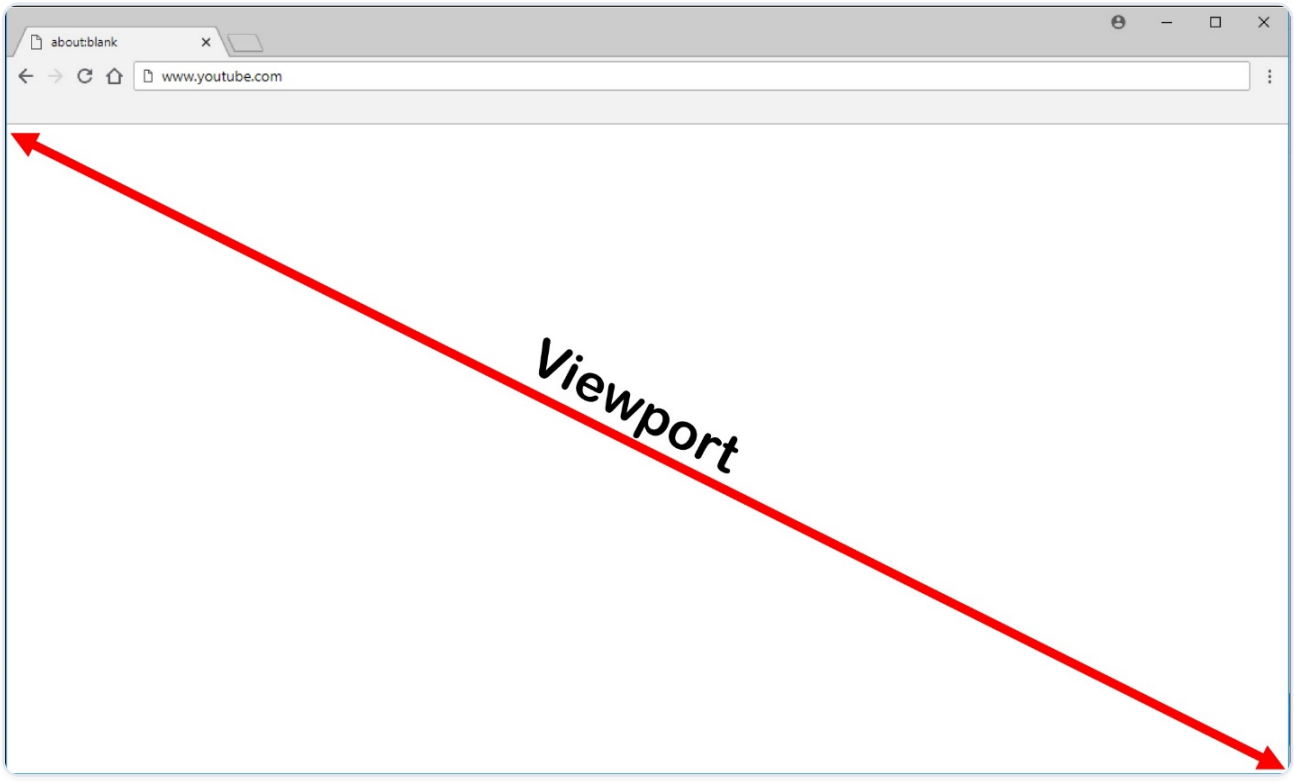
Redirección de contenido del navegador

Información general

La redirección de contenido del navegador proporciona la capacidad de renderizar páginas web en la lista de permitidos en el lado del cliente. Esta función utiliza la aplicación Citrix Workspace™ para instanciar un motor de renderizado correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS de la URL.

> **Nota:**
>
> El VDA de Linux admite la redirección de contenido del navegador en Google Chrome.
>
> Este motor de diseño web superpuesto se ejecuta en el cliente en lugar de en el VDA y utiliza la CPU, GPU, RAM y red del cliente.

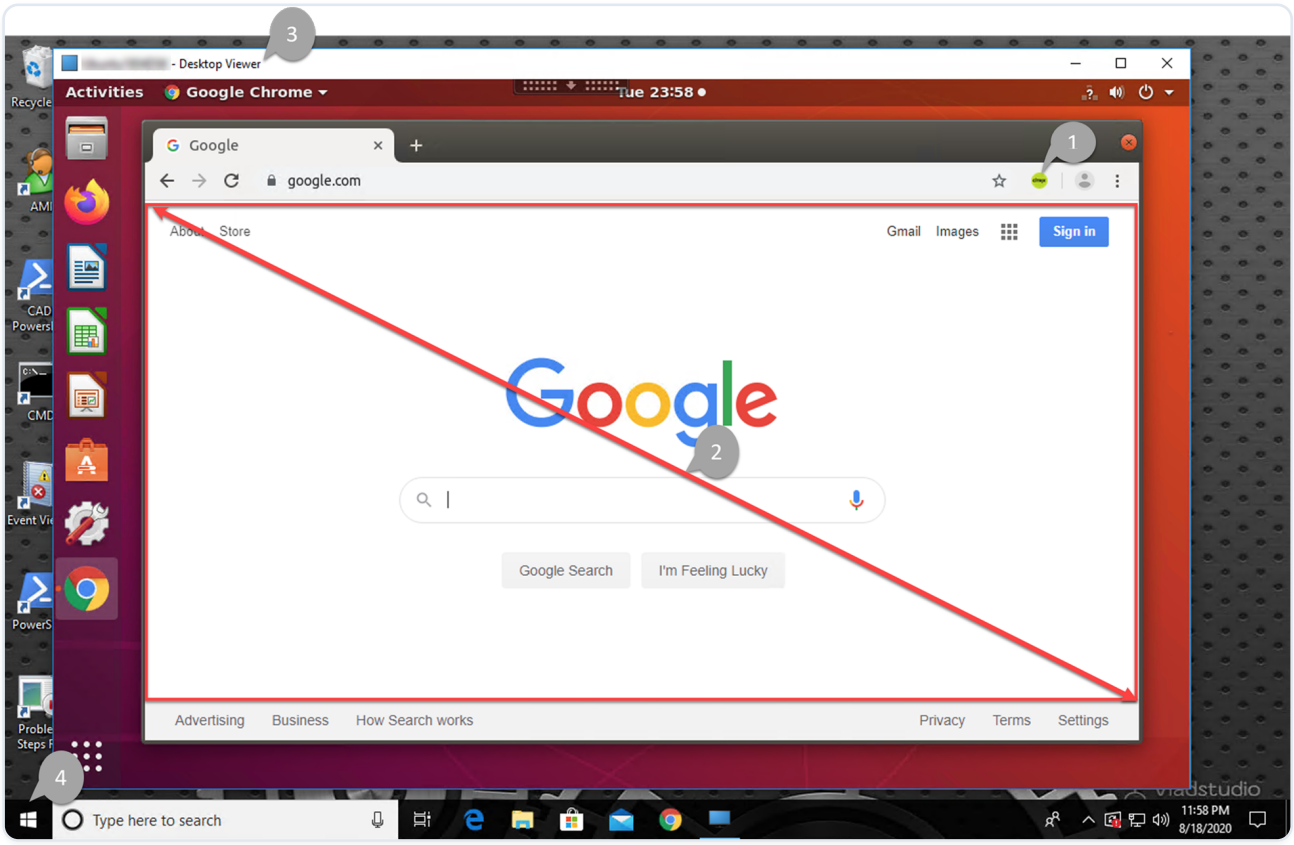
Solo se redirige la ventana gráfica del navegador. La ventana gráfica es el área rectangular de su navegador donde se muestra el contenido. La ventana gráfica no incluye elementos como la barra de direcciones, la barra de favoritos y la barra de estado. Esos elementos siguen ejecutándose en el navegador del VDA.



Configure una política de Studio que especifique una lista de control de acceso que contenga las URL de la lista de permitidos para la redirección. Configure una lista de bloqueo que deshabilite la redirección para URL específicas.

Si se encuentra una coincidencia con una URL en una lista de permitidos, pero no en ninguna lista de bloqueo, un canal virtual (CTXCSB) indica a la aplicación Citrix Workspace que se requiere una redirección y retransmite la URL. La aplicación Citrix Workspace instancia entonces un motor de renderizado local y muestra el sitio web.

A continuación, la aplicación Citrix Workspace integra el sitio web en el área de contenido del navegador del escritorio virtual sin problemas.



1. Icono de la extensión de redirección de contenido del navegador de Citrix®

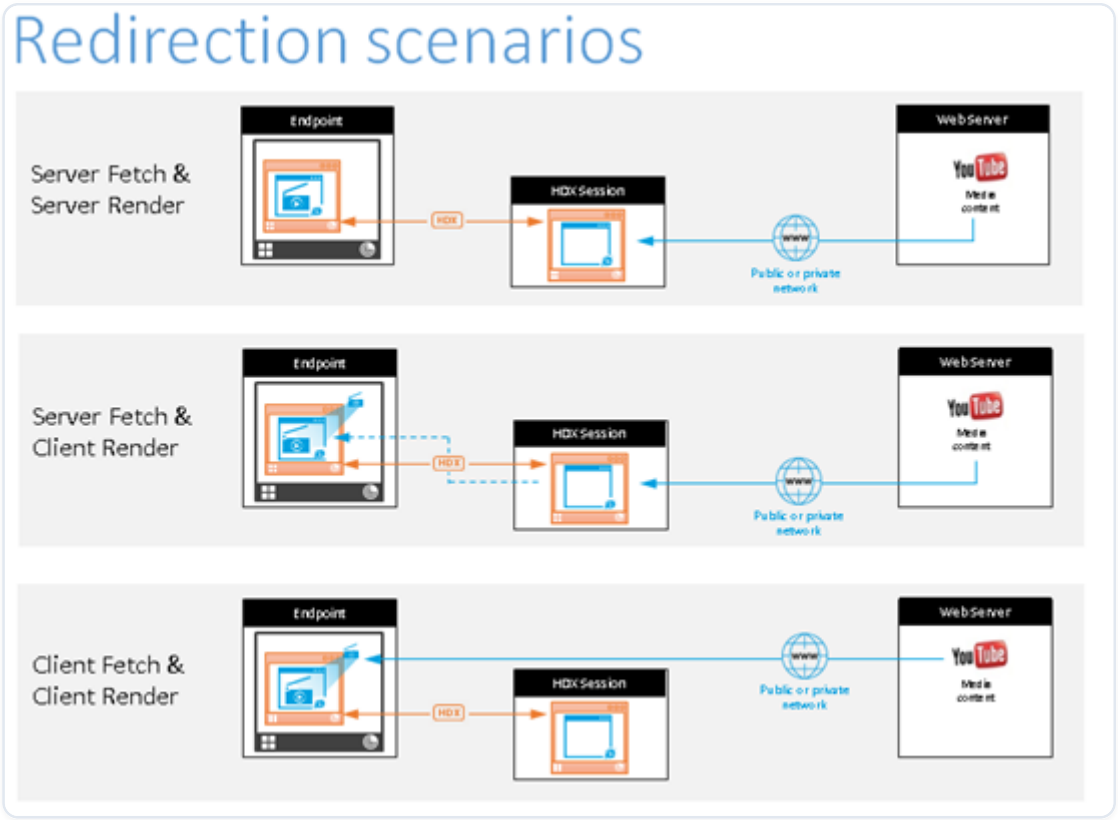
   El color del icono de la extensión especifica el estado de la extensión de Chrome. Es uno de los tres colores:

   - Verde: Activo y conectado
   - Gris: No activo/inactivo en la pestaña actual
   - Rojo: Roto/No funciona

2. Ventana gráfica renderizada en el cliente o mezclada de nuevo en el escritorio virtual
3. Linux VDA

4. Cliente Windows

Aquí hay escenarios de cómo la aplicación Citrix Workspace obtiene contenido:



- **Obtención por el servidor y renderizado por el servidor:** No hay redirección porque no ha agregado el sitio a la lista de permitidos o la redirección ha fallado. Recurrimos a renderizar la página web en el VDA y usamos Thinwire para remotizar los gráficos. Utilice directivas para controlar el comportamiento de reserva. Este escenario provoca un alto consumo de CPU, RAM y ancho de banda en el VDA.
- **Obtención por el servidor y renderizado por el cliente**: La aplicación Citrix Workspace contacta y obtiene contenido del servidor web a través del VDA mediante un canal virtual (CTXPFWD). Esta opción es útil cuando el cliente no tiene acceso al servidor web (por ejemplo, clientes ligeros). Reduce el consumo de CPU y RAM en el VDA, pero se consume ancho de banda en el canal virtual ICA®.

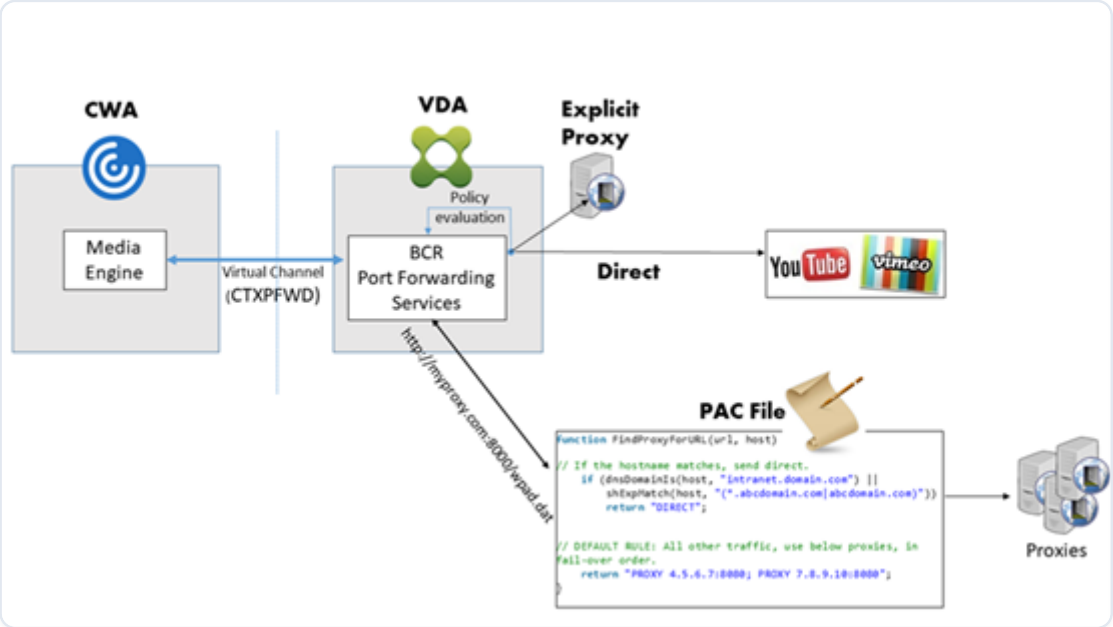
  Hay tres modos de funcionamiento para este escenario. CTXPFWD reenvía datos a un dispositivo proxy al que el VDA accede para obtener acceso al servidor web.

  Qué opción de política elegir:

  - Proxy explícito: si tiene un único proxy explícito en su centro de datos.
  - Directo o transparente: si no tiene proxies o si utiliza proxies transparentes.

- Archivos PAC: si depende de archivos PAC para que los navegadores del VDA puedan elegir automáticamente el servidor proxy adecuado para obtener una URL específica.

Para obtener más información, consulte la configuración **Browser Content Redirection Proxy Configuration** más adelante en este artículo.



- **Obtención por el cliente y renderizado por el cliente:** Como la aplicación Citrix Workspace contacta directamente con el servidor web, requiere acceso a Internet. Este escenario descarga todo el uso de red, CPU y RAM de su sitio de Citrix Virtual Apps and Desktops™.

  Ventajas:

  - Mejor experiencia de usuario final (tasa de bits adaptativa (ABR))
  - Uso reducido de recursos del VDA (CPU/RAM/E/S)
  - Consumo de ancho de banda reducido

Requisitos del sistema

Cliente Windows:

- Citrix Workspace app 1809 para Windows o posterior

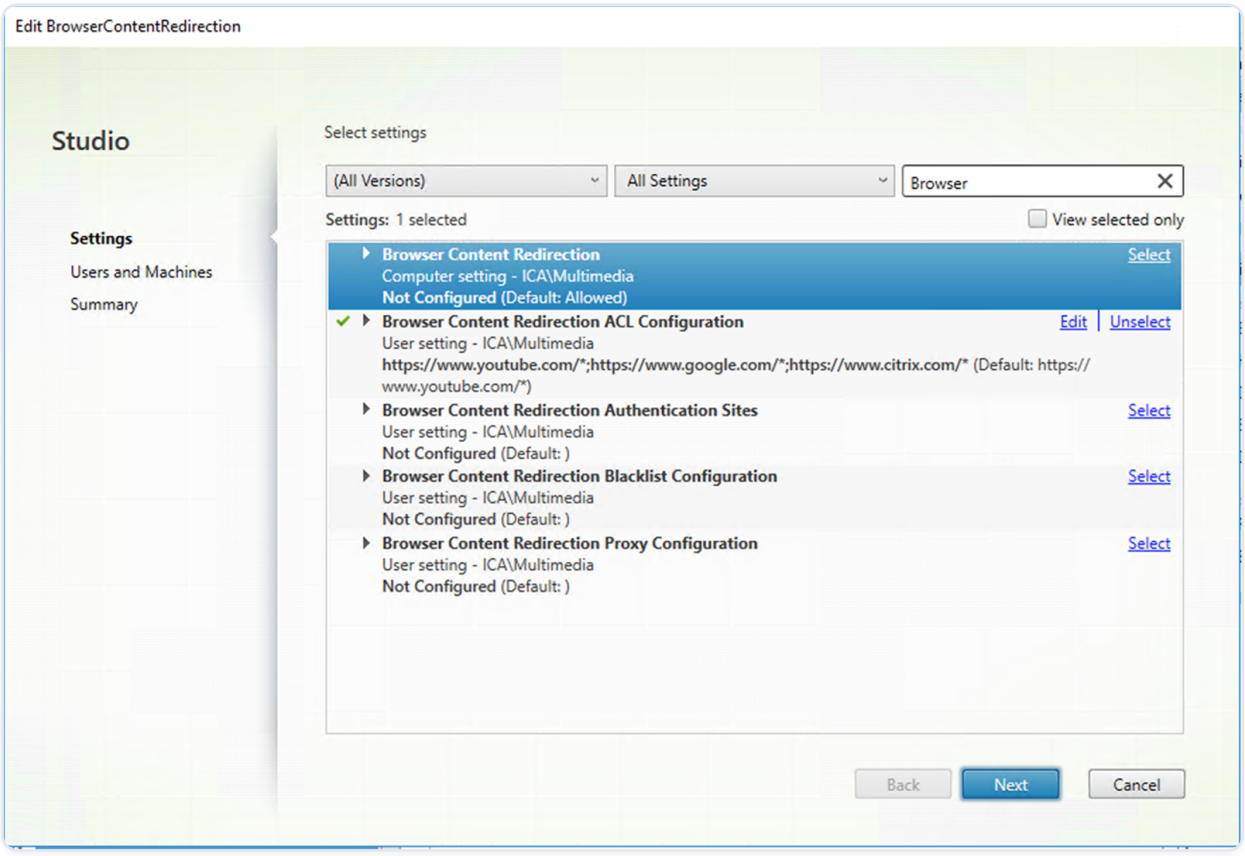
VDA de Linux:

- Navegador en el VDA: Google Chrome v66 o posterior con la extensión de redirección de contenido del explorador de Citrix agregada

Configurar la redirección de contenido del explorador

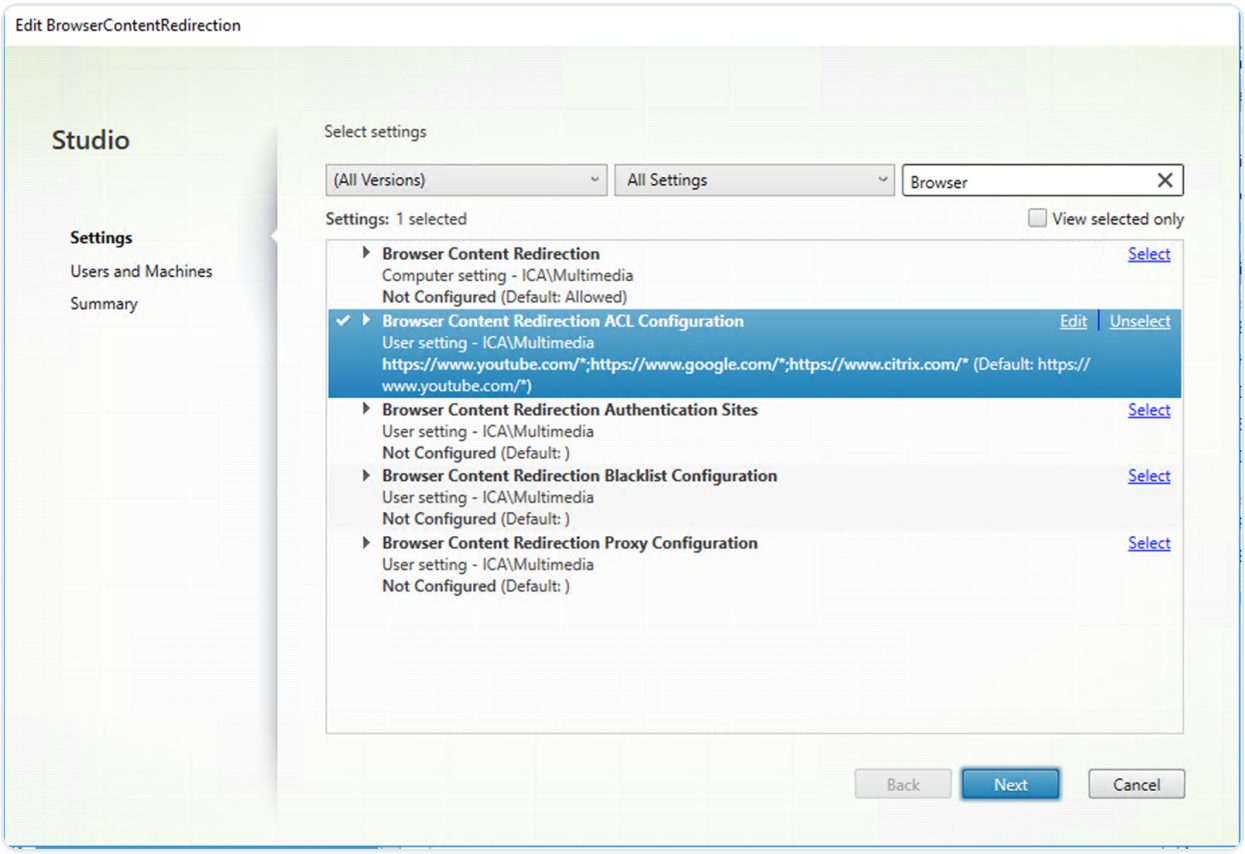
Para usar la redirección de contenido del explorador, configure las directivas pertinentes e instale la extensión de redirección de contenido del explorador en Google Chrome. Para ello, siga estos pasos:

1. En Citrix Studio, establezca **Browser Content Redirection** en **Allowed** para habilitar la redirección de contenido del explorador.



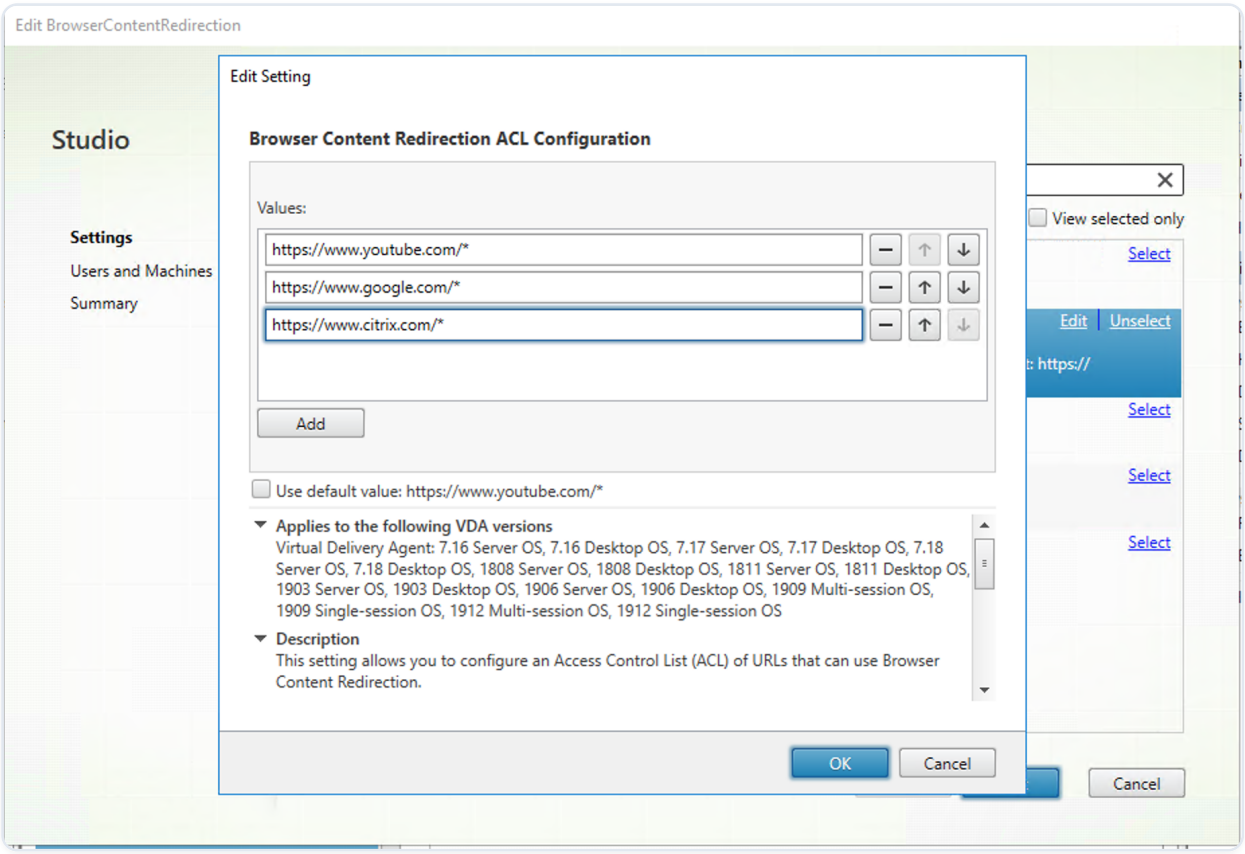
2. Especifique una lista de permitidos de URL cuyo contenido se puede redirigir al cliente y una lista de bloqueados que inhabilita la redirección para URL específicas. Configurar una lista de bloqueados es opcional.

   La configuración **Browser Content Redirection ACL Configuration** especifica una lista de permitidos de URL cuyo contenido se puede redirigir al cliente. Al especificar URL, puede usar el comodín `*` para representar todos los componentes de la URL excepto el protocolo.

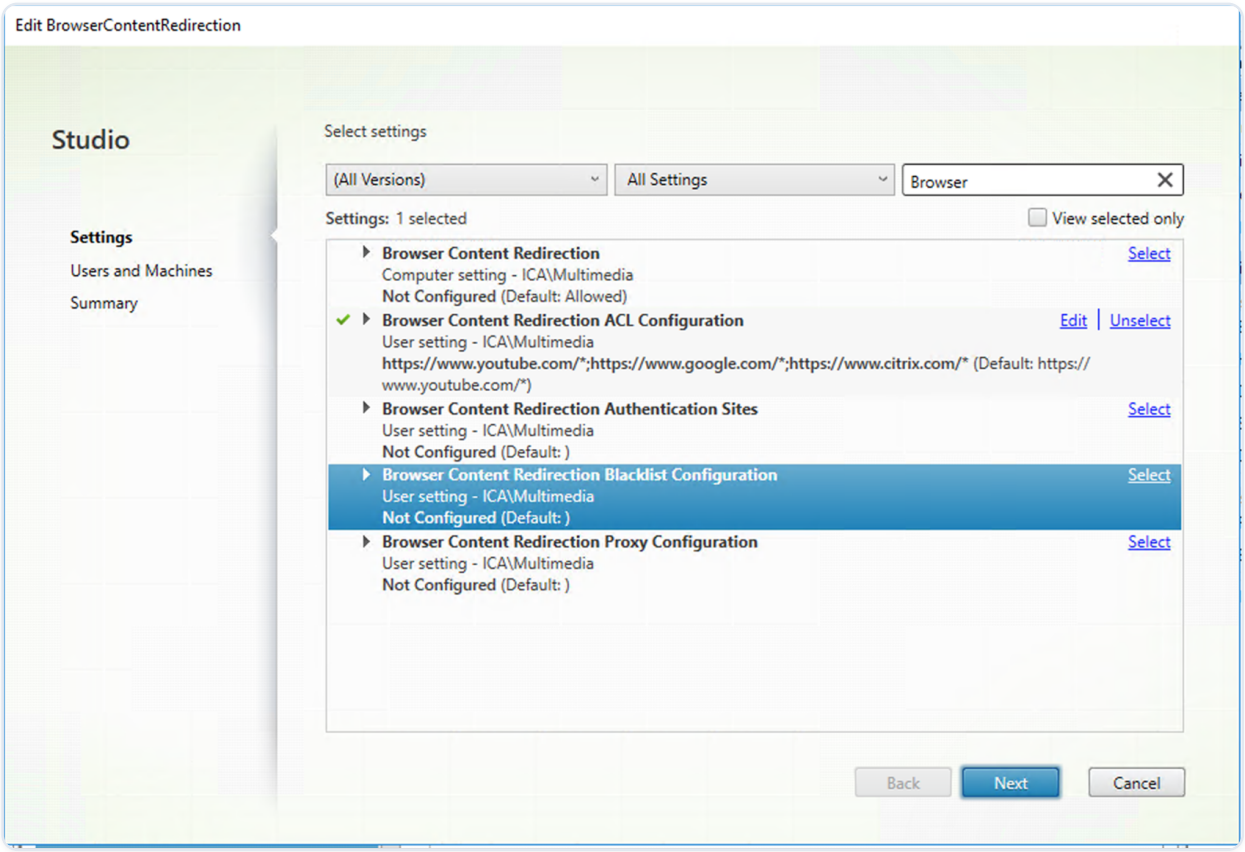


Los siguientes son ejemplos permitidos:

- `http://www.xyz.com/index.html` (Puede lograr una mayor granularidad especificando rutas en la URL. Por ejemplo, si especifica `https://www.xyz.com/sports/index.html`, solo se redirige la página `index.html`.)
- `https://www.xyz.com/*`
- `http://www.xyz.com/*videos*`
- `http://*.xyz.com/`
- `http://*.*.com/`



La configuración **Browser Content Redirection Blacklist Configuration** especifica una lista de bloqueados que inhabilita la redirección para URL específicas.



3. Para habilitar la obtención por parte del servidor y la representación por parte del cliente, configure la opción **Browser Content Redirection Proxy Configuration**.

   Esta configuración proporciona opciones de configuración para los parámetros de proxy en el VDA para la redirección de contenido del explorador. Si está habilitada con una dirección de proxy y un número de puerto válidos, una URL de PAC/WPAD o una configuración Directa/ Transparente, la aplicación Citrix Workspace siempre intenta primero la obtención por parte del servidor y la representación por parte del cliente. Para obtener más información, consulte el Mecanismo de reserva.

   Si está inhabilitada o no configurada y se utiliza un valor predeterminado, la aplicación Citrix Workspace intenta la obtención por parte del cliente y la representación por parte del cliente.

   De forma predeterminada, esta configuración está **Prohibida**.

   Patrón permitido para un proxy explícito:

   `http://<hostname/ip address\>:\<port\>`

   Ejemplo:

   `http://proxy.example.citrix.com:80 http://10.10.10.10:8080`

   Patrones permitidos para archivos PAC/WPAD:

   `http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

   Ejemplo: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

   `https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

   Ejemplo: `http://10.10.10.10/configuration/pac/wpad.dat`

   Patrones permitidos para proxies directos o transparentes:

   Escriba la palabra **DIRECT** en el cuadro de texto de la directiva.

   > **Nota:**
   >
   > También puede establecer un proxy editando el valor del Registro `HKLM\Software\Citrix\HdxMediastream\WebBrowserRedirectionProxyAddress.`. Además, el valor del Registro `HKLM\Software\Citrix\HdxMediastream\AllowNonTlsPacUri` le permite decidir si

> permite las descargas de archivos PAC a través de HTTP. El valor predeterminado es 0, lo que significa que HTTP no está permitido.

> Los Registros anulan las opciones de configuración de directivas. Para obtener una lista de las claves de Registro relevantes, consulte Anulaciones de claves de Registro de redirección de contenido del explorador.

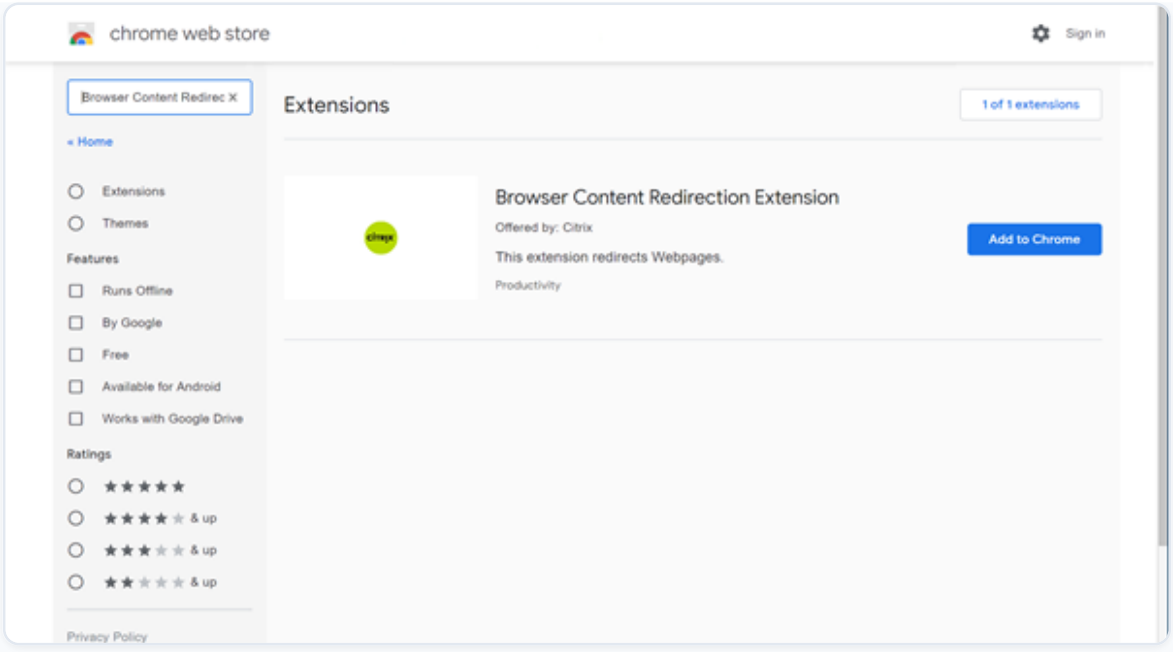
4. Haga clic en **Añadir a Chrome** en el VDA para añadir la extensión de redirección de contenido del explorador de Citrix desde Chrome Web Store. Esto ayuda al explorador del VDA a detectar si una URL (a la que se navega) coincide con una lista de permitidos o una lista de bloqueados.

> **Importante:**

> La extensión no es necesaria en el cliente. Agréguela solo en el VDA.

> \>

> Las extensiones de Chrome se instalan por usuario. No es necesario actualizar una imagen dorada para añadir o eliminar una extensión.



Mecanismo de reserva

Si habilita la directiva **Browser Content Redirection Proxy Configuration**, la aplicación Citrix Workspace intenta la obtención del servidor y la representación del cliente. Si la obtención del servidor y la representación del cliente fallan, se recurre a la obtención del cliente y la representación del cliente. Si la máquina cliente no tiene acceso al servidor web, el explorador del VDA puede volver a cargar y representar la página en el servidor (obtención del servidor y representación del servidor).

Sustituciones de clave de registro de redirección de contenido del explorador

> **Advertencia:**
>
> La edición incorrecta del registro puede causar problemas graves que podrían requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas resultantes del uso incorrecto del Editor del Registro puedan resolverse. Utilice el Editor del Registro bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de editarlo.

`HKLM\Software\Citrix\HdxMediastream`

NOMBRE	TIPO	VALOR
WebBrowserRedirection	DWORD	1=Permitido, 0=Prohibido
WebBrowserRedirectionAcl	REG_MULTI_SZ	/
WebBrowserRedirectionProxyAddress	REG_SZ	Si lo establece en cualquiera de los siguientes modos, se habilita la obtención del servidor y la representación del cliente: **Proxy explícito**: si tiene un único proxy explícito en su centro de datos. **Directo o transparente**: si no tiene proxies o si utiliza proxies transparentes. **Archivos PAC**: si utiliza archivos PAC para que los exploradores del

NOMBRE	TIPO	VALOR
		VDA puedan elegir automáticamente el servidor proxy adecuado para obtener una URL específica.
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	/
AllowNonTlsPacUri	DWORD	Determina si se permiten las descargas de archivos PAC a través de HTTP. El valor predeterminado es 0, lo que significa que HTTP no está permitido. Si lo establece en 1, **HDXWebProxy.exe** puede descargar archivos PAC a través de HTTP (no estrictamente a través de HTTPS).

Compresión de vídeo de cámara web HDX™

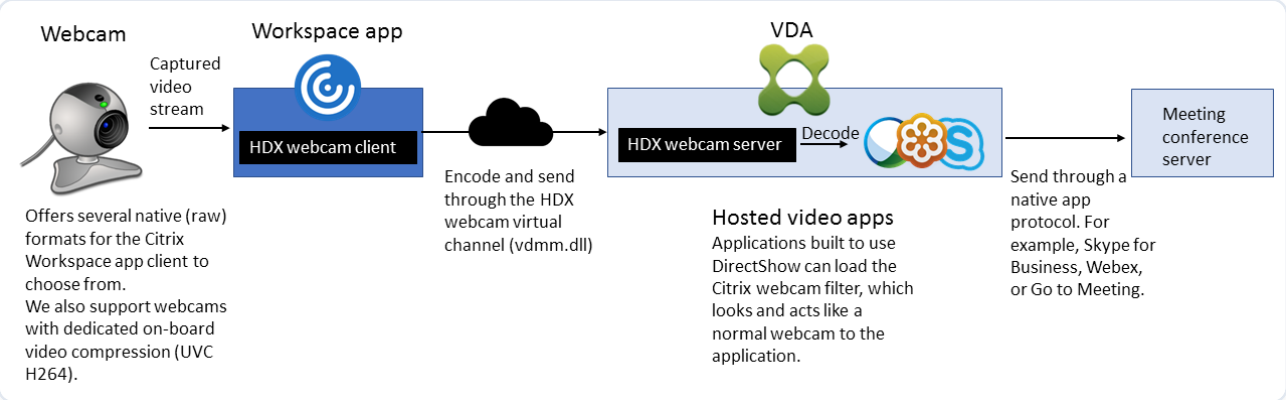
Información general

Los usuarios de aplicaciones de videoconferencia que se ejecutan en sesiones de VDA de Linux ahora pueden usar sus cámaras web con la compresión de vídeo de cámara web HDX. La función está habilitada de forma predeterminada. Le recomendamos que utilice siempre la compresión de vídeo de cámara web HDX si es posible.

La compresión de vídeo de cámara web HDX también se denomina modo de cámara web **optimizado**. Este tipo de compresión de vídeo de cámara web envía el vídeo H.264 directamente a la aplicación de videoconferencia que se ejecuta en la sesión virtual. La compresión de vídeo de cámara web HDX utiliza la tecnología de marco multimedia que forma parte del sistema operativo cliente para interceptar el vídeo de los dispositivos de captura, transcodificarlo y comprimirlo. Los fabricantes de dispositivos de captura suministran los controladores que se conectan a la arquitectura de transmisión del kernel del sistema operativo.

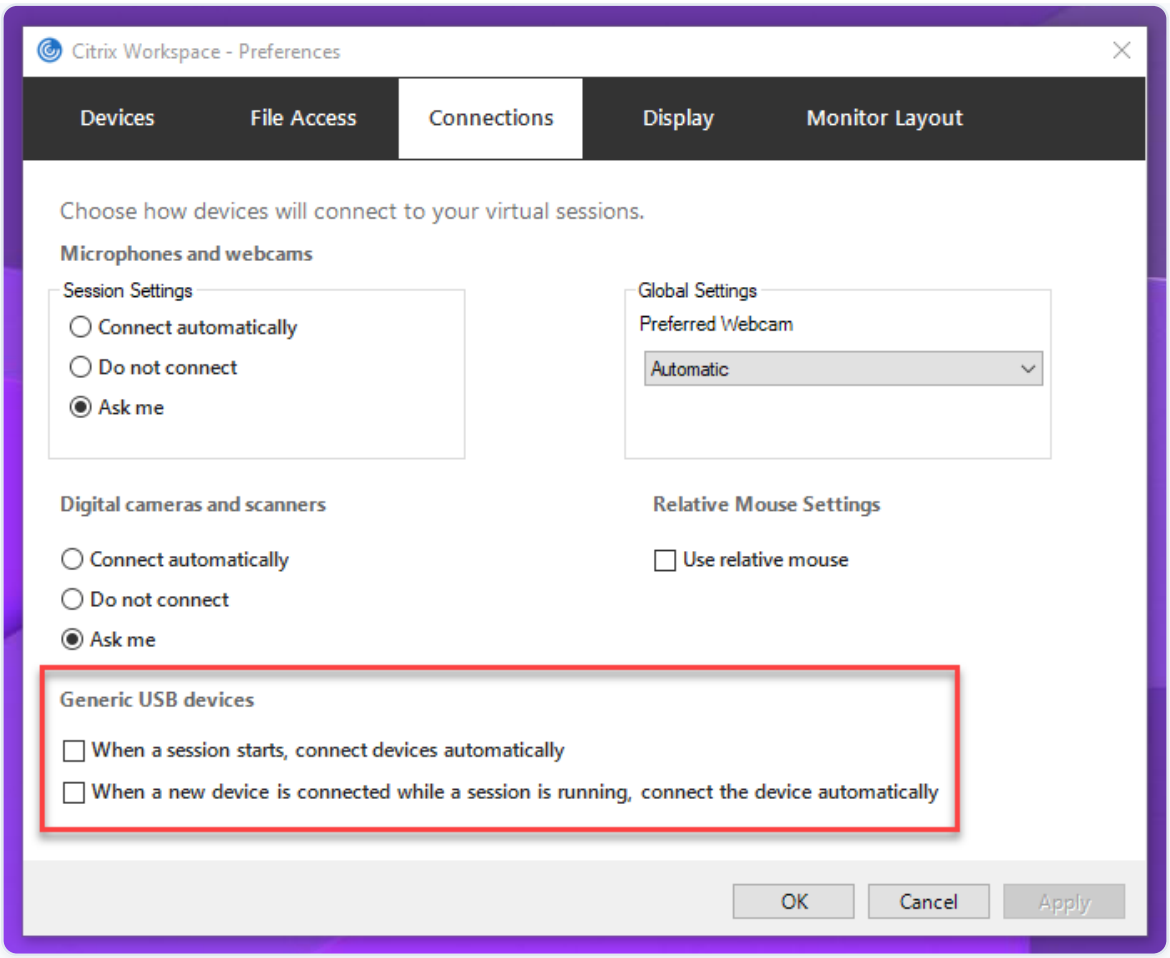
El cliente gestiona la comunicación con la cámara web. A continuación, el cliente envía el vídeo solo al servidor que puede mostrarlo correctamente. El servidor no trata directamente con la cámara web, pero su integración le proporciona la misma experiencia en su escritorio. La

aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mayor resiliencia en escenarios WAN.



Nota:

- La función no está disponible para máquinas de Azure porque falta el módulo del kernel **videodev** del que depende la función en las máquinas de Azure.
- La función solo admite vídeos H.264 de su cliente de la aplicación Citrix Workspace.
- La resolución de cámara web admitida oscila entre 48x32 y 1920x1080.
- No elija **Dispositivos USB genéricos** en la barra de herramientas de su aplicación Citrix Workspace™ cuando utilice una cámara web. De lo contrario, podrían producirse problemas inesperados.



Aplicación Citrix Workspace compatible

La compresión de vídeo de cámara web HDX admite las siguientes versiones de la aplicación Citrix Workspace:

PLATAFORMA	PROCESADOR
Aplicación Citrix Workspace para Windows	La aplicación Citrix Workspace para Windows admite la compresión de vídeo de la cámara web para aplicaciones de 32 y 64 bits en XenApp y XenDesktop 7.17 y versiones posteriores. En versiones anteriores, la aplicación Citrix Workspace para Windows solo admite aplicaciones de 32 bits.
Aplicación Citrix Workspace para Chrome	Dado que algunos Chromebooks ARM no admiten la codificación H.264, solo las aplicaciones de 32 bits pueden usar la

PLATAFORMA	PROCESADOR
	compresión de vídeo de cámara web HDX optimizada.

Cámaras web totalmente probadas

Las diferentes cámaras web ofrecen distintas velocidades de fotogramas y tienen diferentes niveles de brillo y contraste. Citrix® utiliza las siguientes cámaras web para la validación inicial de la función:

- Logitech HD Webcam C270
- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

Configuración

Esta función está habilitada de forma predeterminada. Para usarla, complete la siguiente verificación y configuración:

> **Sugerencia:**

> Los usuarios de la aplicación Citrix Workspace pueden anular la configuración predeterminada eligiendo **No conectar** para la configuración de **Micrófonos y cámaras web** del Visor de escritorio.

1. Una vez completada la instalación del VDA, verificar que el VDA puede registrarse en Delivery Controller™ y que las sesiones de escritorio Linux publicadas se pueden iniciar correctamente mediante credenciales de Windows.
2. Asegúrese de que su VDA tenga acceso a Internet y, a continuación, ejecute el comando `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` para completar las configuraciones de la cámara web. Si su VDA no tiene acceso a Internet, vaya al paso 3.

   > **Nota:**

   > Puede haber una falta de coincidencia del kernel entre `uname -r` y los encabezados del kernel. Esta falta de coincidencia hace que el script ctxwcamcfg.sh falle. Para usar la

> compresión de vídeo de la cámara web HDX correctamente, ejecute **sudo apt-get dist-upgrade**, reinicie el VDA y, a continuación, vuelva a ejecutar el script ctxwcamcfg.sh.

> Si su VDA está implementado en Debian, asegúrese de que se esté ejecutando en la versión más reciente del kernel. De lo contrario, ejecute los siguientes comandos para actualizar a la versión más reciente del kernel:

```
sudo apt-get update

sudo apt-get dist-upgrade

sudo reboot
```

Si su VDA está implementado en SUSE 15, ejecute los siguientes comandos para actualizar a la versión más reciente del kernel y para reiniciar:

```
zypper up kernel-default

reboot
```

El script ctxwcamcfg.sh ayuda a:

a. Instalar los programas `kernel-devel` y Dynamic Kernel Module Support (DKMS) en su VDA.

   - `kernel-devel` se utiliza para crear un módulo de kernel de cámara web virtual de la versión correspondiente.
   - DKMS se utiliza para administrar dinámicamente el módulo de kernel de la cámara web virtual.

   > **Nota:**
   >
   > Al instalar los programas anteriores en RHEL, Rocky Linux y CentOS, el script `ctxwcamcfg.sh` instala y habilita los siguientes repositorios en su VDA:
   >
   > - Paquetes adicionales para Enterprise Linux (EPEL)

> - RPM Fusion

b. Descargue el código abierto `v4l2loopback` de `<https://github.com/umlaeute/v4l2loopback>` y use DKMS para administrar `v4l2loopback`.

   `v4l2loopback` es un módulo de kernel que le permite crear dispositivos de bucle invertido V4L2.

c. Ejecute el comando `sudo systemctl restart ctxwcamsd`. El servicio de cámara web del VDA de Linux, `ctxwcamsd`, se reinicia y carga el módulo de kernel `v4l2loopback` para la función de compresión de vídeo de la cámara web HDX.

3. Si su VDA no tiene acceso a Internet, compile el módulo del kernel v4l2loopback en otra máquina y, a continuación, cópielo en su VDA.

   a. Prepare una máquina que tenga acceso a Internet y la misma versión del kernel que su VDA. El comando `uname -r` ayuda a encontrar las versiones del kernel.

   b. En la máquina, ejecute el comando `sudo mkdir -p /var/xdl`.

   c. Copie `/var/xdl/configure_*` de su VDA a la máquina en `/var/xdl/`.

   d. En la máquina, ejecute el comando `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` para compilar el módulo del kernel. Si el comando se ejecuta correctamente, crea un archivo v4l2loopback.ko en la ruta `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/`. Ignore los errores que puedan producirse al ejecutar el script ctxwcamcfg.sh.

   e. Copie v4l2loopback.ko de la máquina a su VDA y colóquelo en `/opt/Citrix/VDA/lib64/`.

   f. En su VDA, ejecute el comando `sudo systemctl restart ctxwcamsd` para reiniciar el servicio de la cámara web y cargar el módulo del kernel v4l2loopback.

VDA de Linux no unidos a un dominio

Información general

Los VDA no unidos a un dominio eliminan la necesidad de unir los VDA a dominios de Active Directory para la autenticación de VDA y de usuario. Al crear un VDA no unido a un dominio, se genera un par de claves pública-privada para registrar el VDA en el plano de control de la nube. Por lo tanto, ya no es necesario unirse a un dominio de Active Directory. Cuando un usuario inicia

una sesión desde el VDA no unido a un dominio, el VDA crea una cuenta de asignación local utilizando el nombre de usuario que el usuario utiliza para iniciar sesión en la aplicación Citrix Workspace. El VDA asigna una contraseña aleatoria que la cuenta de asignación local utiliza para el inicio de sesión único (SSO) y la reconexión de la sesión. Si cambia la contraseña aleatoria, el SSO y la reconexión de la sesión fallarán. Para inhabilitar el SSO, consulte Autenticación sin SSO.

Importante:

- Para clientes de Citrix DaaS™:
  - Puede implementar VDA no unidos a un dominio en una nube pública o en el centro de datos local. Los VDA no unidos a un dominio son administrados por el plano de control en Citrix DaaS.
  - Para crear VDA no unidos a un dominio, los clientes que utilizan el servicio Citrix Gateway deben asegurarse de que Rendezvous V2 esté habilitado. Los Cloud Connectors solo son necesarios si planea aprovisionar máquinas en hipervisores locales o si desea utilizar Active Directory como proveedor de identidades en Workspace.
- Para clientes de CVAD:
  - Habilite la función WebSocket en DDC siguiendo las instrucciones a continuación: `"HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force`

    Abra una powershell y ejecute el siguiente comando, luego reinicie el DDC New-ItemProperty
- Para crear VDA no unidos a un dominio, puede usar tanto MCS como la instalación sencilla. Para obtener más información, consulte Crear VDA de Linux no unidos a un dominio mediante MCS y Crear un VDA de Linux no unido a un dominio mediante la instalación sencilla.
- MCS no admite servidores bare metal.
- Las siguientes funciones están disponibles para VDA de Linux no unidos a un dominio:
  - Crear usuarios locales con atributos especificados en VDA no unidos a un dominio
  - Autenticación sin SSO

- Autenticación con Azure Active Directory
- Rendezvous V2

Funciones disponibles para VDA Linux no unidos a un dominio

Crear usuarios locales con atributos específicos en VDA no unidos a un dominio

Cuando abre una sesión alojada en un VDA no unido a un dominio, el VDA crea automáticamente un usuario local con atributos predeterminados. El VDA crea el usuario local basándose en el nombre de usuario que utilizó para iniciar sesión en la aplicación Citrix Workspace™. También puede especificar atributos de usuario, como el identificador de usuario (UID), el identificador de grupo (GID), el directorio principal y el shell de inicio de sesión del usuario. Para usar esta función, siga estos pasos:

1. Ejecute el siguiente comando para habilitar la función:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\LocalMappedAccount" -t
"REG_DWORD" -v "CreateWithUidGid" -d "0x00000001" --force
```

2. Especifique los siguientes atributos en el script `/var/xdl/getuidgid.sh` en la ruta de instalación del VDA:

ATRIBUTO	OBLIGATORIO U OPCIONAL	DESCRIPCIÓN
`uid`	Obligatorio	Un identificador de usuario (UID) es un número asignado por Linux a cada usuario del sistema. Determina a qué recursos del sistema puede acceder el usuario.
`gid`	Obligatorio	Un identificador de grupo (GID) es un número que se utiliza para representar un grupo específico.

ATRIBUTO	OBLIGATORIO U OPCIONAL	DESCRIPCIÓN
`homedir`	Opcional	El directorio principal de Linux es un directorio para un usuario en particular.
`shell`	Opcional	Un shell de inicio de sesión es un shell que se asigna a un usuario al iniciar sesión en su cuenta de usuario.

A continuación, se muestra un ejemplo del script `getuidgid.sh`:

> **Nota:**
>
> Asegúrese de que los atributos especificados en el script sean válidos.

```
#!/bin/bash



################################################################################
########

#

# Citrix Virtual Apps™ & Desktops For Linux Script: Get uid and gid for
the user

#

# Copyright (c) Citrix Systems, Inc. All Rights Reserved.

#



export LC_ALL="en_US.UTF-8"
```

```
function get_uid_gid_for_user()
{
echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
echo "shell:/bin/sh"
}

get_uid_gid_for_user $1
```

Autenticación sin SSO

De forma predeterminada, el VDA de Linux tiene habilitado el inicio de sesión único (SSO). Los usuarios inician sesión en la aplicación Citrix Workspace y en las sesiones de VDA con un único conjunto de credenciales. Para que los usuarios inicien sesión en las sesiones de VDA con un conjunto de credenciales diferente, inhabilite el SSO en el VDA de Linux. Para obtener más información, consulte Autenticación sin SSO.

Autenticación con Azure Active Directory

Los VDA no unidos a un dominio que implementa en Azure se integran con el servicio de identidad de AAD para proporcionar autenticación de usuario. Para obtener más información, consulte Autenticación con Azure Active Directory.

Rendezvous V2

Los VDA no unidos a un dominio son compatibles con el uso de Rendezvous V2 para omitir los Citrix Cloud Connectors. Para obtener más información, consulte Rendezvous V2.

Lista de compatibilidad de directivas

Lista de compatibilidad de directivas de Linux VDA

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Usar la hora local del cliente	UseLocalTimeOfClient	Usuario	ICA\Control de zona horaria	**Usar la zona horaria del servidor**
Cálculo de ida y vuelta de ICA	IcaRoundTripCheckEnabled	Equipo	ICA\Supervisión de usuarios finales	Habilitado (1)
Intervalo de cálculo de ida y vuelta de ICA	IcaRoundTripCheckPeriod	Equipo	ICA\Supervisión de usuarios finales	15
Cálculos de ida y vuelta de ICA para conexiones inactivas	IcaRoundTripCheckWhenIdle	Equipo	ICA\Supervisión de usuarios finales	Deshabilitado (0)
Límite de ancho de banda general de la sesión	LimitOverallBw	Usuario	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de audio	LimitAudioBw	Usuario	ICA\Ancho de banda	0
Porcentaje del límite de ancho de banda de	LimitAudioBwPercent	Usuario	ICA\Ancho de banda	0

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
redirección de audio				
Límite de ancho de banda de redirección de dispositivos USB de cliente	LimitUSBBw	Usuario	ICA\Bandwidth	0
Porcentaje de ancho de banda de redirección de dispositivos USB de cliente	LimitUSBBwPercent	Usuario	ICA\Bandwidth	0
Límite de ancho de banda de redirección de archivos	LimitCdmBw	Usuario	ICA\Bandwidth	0
Porcentaje de límite de ancho de banda de redirección de archivos	LimitCdmBwPercent	Usuario	ICA\Bandwidth	0
Límite de ancho de banda de redirección de impresora	LimitPrinterBw	Usuario	ICA\Bandwidth	0
Porcentaje de límite de ancho de banda de	LimitPrinterBwPercent	Usuario	ICA\Bandwidth	0

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
redirección de impresora				
Conexiones de WebSockets	AcceptWebSocketsConnections	Equipo	ICA\WebSockets	Prohibido
Número de puerto de WebSockets	WebSocketsPort	Equipo	ICA\WebSockets	8008
Lista de servidores de origen de confianza de WebSockets	WSTrustedOriginServerList	Equipo	ICA\WebSockets	*
Latidos de ICA®	SendICAKeepAlives	Equipo	**Latido de ICA**	No enviar mensajes de latido ICA (0)
Tiempo de espera de latido de ICA	ICAKeepAliveTimeout	Equipo	**Latido de ICA**	60 segundos
Número de puerto del oyente de ICA	IcaListenerPortNumber	Equipo	ICA	1494
Transporte adaptativo HDX™	HDXoverUDP	Equipo	ICA	Preferido(2)
Protocolo Rendezvous	RendezvousProtocol	Equipo	ICA	Prohibido
Conexiones de fiabilidad de sesión	AcceptSessionReliabilityConnections	Equipo	ICA\Fiabilidad de sesión	Permitido(1)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Nivel de transparencia de la interfaz de usuario de reconexión	ReconnectionUiTransparencyLevel	Equipo	ICA\Reconexión automática de cliente	80%
Número de puerto de fiabilidad de sesión	SessionReliabilityPort	Equipo	ICA\Fiabilidad de sesión	2598
Tiempo de espera de fiabilidad de sesión	SessionReliabilityTimeout	Equipo	ICA\Fiabilidad de sesión	180 s
Reconexión automática de cliente	AllowAutoClientReconnect	Usuario	ICA\Reconexión automática del cliente	Permitido (1)
Autenticación de reconexión automática del cliente	AllowAutoClientReconnectAuthentication	Equipo	ICA\Reconexión automática del cliente	Deshabilitado (0)
Registro de reconexión automática del cliente	AllowAutoClientReconnectLogging	Equipo	ICA\Reconexión automática del cliente	Deshabilitado (0)
Tiempo de espera de reconexión automática del cliente	AllowAutoClientReconnectTimeout	Equipo	ICA\Reconexión automática del cliente	120 segundos
Redirección de audio del cliente	AllowAudioRedirection	Usuario	Audio	Permitido (1)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Redirección de impresora de cliente	AllowPrinterRedir	Usuario	Impresión	Permitido (1)
Crear automáticamente impresora universal PDF	AutoCreatePDFPrinter	Usuario	Impresión	Deshabilitado (0)
Asignación y compatibilidad de controladores de impresora	DriverMappingList	Usuario	Impresión	`"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"`
Redirección del Portapapeles del cliente	AllowClipboardRedir	Usuario	Portapapeles	Permitido (1)
Limitar el tamaño de transferencia del Portapapeles de cliente a sesión	LimitClipboardTransferC2H	Usuario	ICA	Deshabilitado (0)
Limitar el tamaño de la transferencia del portapapeles de la sesión al cliente	LimitClipboardTransferH2C	Usuario	ICA	Deshabilitado (0)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Límite de ancho de banda de redirección del portapapeles	LimitClipbdBW	Usuario	ICA\Bandwidth	0
Porcentaje de límite de ancho de banda de redirección del portapapeles	LimitClipbdBWPercent	Usuario	ICA\Bandwidth	0
Restringir la escritura del portapapeles del cliente	RestrictClientClipboardWrite	Usuario	Portapapeles	Deshabilitado (0)
Formatos permitidos para la escritura del portapapeles del cliente	ClientClipboardWriteAllowedFormats	Usuario	Portapapeles	N/D
Restringir la escritura del portapapeles de la sesión	RestrictSessionClipboardWrite	Usuario	Portapapeles	Deshabilitado (0)
Formatos permitidos para la escritura del portapapeles de la sesión	SessionClipboardWriteAllowedFormats	Usuario	Portapapeles	N/D
Redirección de	AllowUSBRedir	Usuario	USB	Prohibido (0)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
dispositivos USB de cliente				
Reglas de redirección de dispositivos USB de cliente	USBDeviceRules	Usuario	USB	"\0"
Compresión de imágenes en movimiento	MovingImageCompressionConfiguration	Usuario	Thinwire	Habilitado (1)
Compresión de color adicional	ExtraColorCompression	Usuario	Thinwire	Deshabilitado (0)
Velocidad de fotogramas mínima de destino	TargetedMinimumFramesPerSecond	Usuario	Thinwire	10 fotogramas por segundo
Velocidad de fotogramas de destino	FramesPerSecond	Usuario	Thinwire	30 fotogramas por segundo
Calidad visual	VisualQuality	Usuario	Thinwire	Medio (3)
Usar códec de vídeo para la compresión	VideoCodec	Usuario	Thinwire	Usar cuando se prefiera (3)
Usar codificación de hardware para el códec de vídeo	UseHardwareEncodingForVideoCodec	Usuario	Thinwire	Habilitado (1)
Permitir compresión	AllowVisuallyLosslessCompression	Usuario	Thinwire	Deshabilitado (0)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
visualmente sin pérdidas				
Optimizar para cargas de trabajo de gráficos 3D	OptimizeFor3dWorkload	Usuario	Thinwire	Deshabilitado (0)
Profundidad de color preferida para gráficos simples	PreferredColorDepth	Usuario	Thinwire	24 bits por píxel (1)
Indicador de estado gráfico	DisplayLosslessIndicator	Usuario	Thinwire	Deshabilitado (0)
Calidad de audio	SoundQuality	Usuario	Audio	Alta – audio de alta definición (2)
Redirección de micrófono de cliente	AllowMicrophoneRedir	Usuario	Audio	Permitido (1)
Número máximo de sesiones	MaximumNumberOfSessions	Equipo	Administración de carga	250
Tolerancia de inicios de sesión simultáneos	ConcurrentLogonsTolerance	Equipo	Administración de carga	2
Habilitar actualización automática de Controllers	EnableAutoUpdateOfControllers	Equipo	Configuración de Virtual Delivery Agent	Permitido (1)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Modo de actualización de selección del portapapeles	ClipboardSelectionUpdateMode	Usuario	Portapapeles	3
Modo de actualización de selección principal	PrimarySelectionUpdateMode	Usuario	Portapapeles	3
Calidad máxima de Speex	MaxSpeexQuality	Usuario	Audio	5
Conectar automáticamente unidades de cliente	AutoConnectDrives	Usuario	Redirección de archivos\CDM	Habilitado (1)
Unidades ópticas de cliente	AllowCdromDrives	Usuario	Redirección de archivos\CDM	Permitido (1)
Unidades fijas de cliente	AllowFixedDrives	Usuario	Redirección de archivos\CDM	Permitido (1)
Unidades de disquete de cliente	AllowFloppyDrives	Usuario	Redirección de archivos\CDM	Permitido (1)
Unidades de red de cliente	AllowNetworkDrives	Usuario	Redirección de archivos\CDM	Permitido (1)
Unidades extraíbles de cliente	AllowRemoveableDrives	Usuario	Redirección de archivos\CDM	Permitido (1)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Redirección de unidades de cliente	AllowDriveRedir	Usuario	Redirección de archivos\CDM	Permitido (1)
Acceso de solo lectura a unidades de cliente	ReadOnlyMappedDrive	Usuario	Redirección de archivos\CDM	Deshabilitado (0)
Visualización automática del teclado	AllowAutoKeyboardPopUp	Usuario	MRVC	Deshabilitado (0)
Permitir la transferencia de archivos entre el escritorio y el cliente	AllowFileTransfer	Usuario	Transferencia de archivos	Permitido
Descargar archivo del escritorio	AllowFileDownload	Usuario	Transferencia de archivos	Permitido
Cargar archivo al escritorio	AllowFileUpload	Usuario	Transferencia de archivos	Permitido
Temporizador de inactividad de la sesión	EnableSessionIdleTimer	Usuario	Temporizadores de sesión	Habilitado (1)
Intervalo del temporizador de inactividad de la sesión	SessionIdleTimerInterval	Usuario	Temporizadores de sesión	1440 minutos
Temporizador de sesión desconectada	EnableSessionDisconnectTimer	Usuario	Temporizadores de sesión	Deshabilitado (0)

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Intervalo del temporizador de sesión desconectada	SessionDisconnectTimerPeriod	Usuario	Temporizadores de sesión	1440 minutos
Redirección de contenido del navegador	WebBrowserRedirection	Equipo	ICA\Multimedia	Permitido
Configuración de ACL de redirección de contenido del navegador	WebBrowserRedirectionAcl	Usuario	ICA\Multimedia	`https://www.youtube.com/*`
Sitios de autenticación de redirección de contenido del navegador	WebBrowserRedirectionAuthenticationSites	Usuario	ICA\Multimedia	Nulo
Configuración de la lista negra de redirección de contenido del explorador	WebBrowserRedirectionBlacklist	Usuario	ICA\Multimedia	Nulo
Configuración del proxy de redirección de contenido del explorador	WebBrowserRedirectionProxy	Usuario	ICA\Multimedia	Nulo
Habilitar marca de agua de sesión	EnableSessionWatermark	Usuario	ICA\Marca de agua de sesión\Contenido de la marca de agua	Deshabilitado

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Incluir dirección IP del cliente	IncludeClientIPAddress	Usuario	ICA\Marca de agua de sesión\Contenido de la marca de agua	Deshabilitado
Incluir hora de conexión	IncludeConnectTime	Usuario	ICA\Session Watermark\Watermark Content	Deshabilitado
Incluir nombre de usuario de inicio de sesión	IncludeLogonUsername	Usuario	ICA\Session Watermark\Watermark Content	Habilitado
Incluir nombre de host de VDA	IncludeVDAHostname	Usuario	ICA\Session Watermark\Watermark Content	Habilitado
Incluir dirección IP de VDA	IncludeVDAIPAddress	Usuario	ICA\Session Watermark\Watermark Content	Deshabilitado
Estilo de marca de agua de sesión	WatermarkStyle	Usuario	ICA\Session Watermark\Watermark Style	Múltiple
Transparencia de marca de agua	WatermarkTransparency	Usuario	ICA\Session Watermark\Watermark Style	17
Texto personalizado de marca de agua	WatermarkCustomText	Usuario	ICA\Session Watermark\Watermark Content	Una configuración de texto personalizado válida puede ser similar a: `<font=Arial Unicode`

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
				`MS><domain><newline><fontsize=47><username><newline><fontzoom=120>Citrix<newline><style=tile>Najing <clientip><newline><rotation=45><serverip><position=bottomleft>`. Para obtener más información, consulte Marca de agua de sesión.
Recopilación de métricas de sesión	UsageDataCollectionThroughClient	Equipo	ICA	Habilitado (1)
Vista previa dinámica de ventanas	EnableDynamicPreview	Equipo	ICA\Graphics	Esta configuración habilita o deshabilita la visualización de ventanas transparentes. Con esta configuración habilitada, puede previsualizar el contenido en pantalla en las ventanas de las

DIRECTIVA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
				aplicaciones publicadas. Por ejemplo, puede abrir varias ventanas de sesiones de Google Chrome mediante la aplicación Citrix Workspace para Windows y, a continuación, pasar el ratón por el icono de Chrome en la barra de tareas para previsualizar el contenido. Para obtener más información, consulte Vista previa dinámica de ventanas. De forma predeterminada, esta configuración está **Habilitada (1)**.

Nota:

Solo el Virtual Delivery Agent (VDA) de Windows admite audio a través del Protocolo de datagramas de usuario (UDP). El VDA de Linux no lo admite. Para obtener más información,

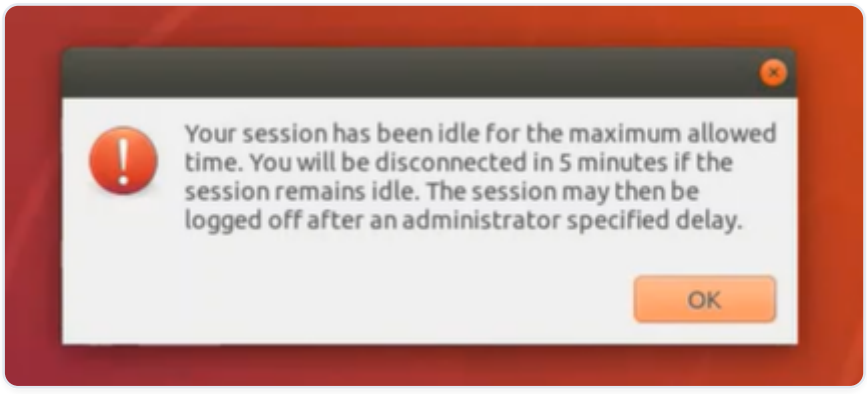
> consulte Audio a través del Protocolo de datagramas de usuario (UDP) de transporte en tiempo real.

> Puede usar las siguientes configuraciones de directiva de Citrix para configurar los temporizadores de conexión de sesión en Citrix Studio:

- **Temporizador de inactividad de sesión**: Determina si se aplica un límite de tiempo para las sesiones inactivas.
- **Intervalo del temporizador de inactividad de sesión**: Establece un límite de tiempo para las sesiones inactivas. Si **Temporizador de inactividad de sesión** está establecido en **Habilitado** y una sesión activa no ha recibido ninguna entrada de usuario durante el tiempo establecido, la sesión se desconecta.
- **Temporizador de sesión desconectada**: Determina si se aplica un límite de tiempo para las sesiones desconectadas.
- **Intervalo del temporizador de sesión desconectada**: Establece un intervalo antes de que se cierre la sesión desconectada.

Cuando actualice cualquiera de las configuraciones de directiva, asegúrese de que sean coherentes en toda la implementación.

Aparece un mensaje de advertencia cuando expira el límite de tiempo para las sesiones inactivas. Consulte la siguiente captura de pantalla para ver un ejemplo. Al pulsar **Aceptar**, se cierra el mensaje de advertencia, pero no se puede mantener la sesión activa. Para mantener la sesión activa, proporcione una entrada de usuario para restablecer el temporizador de inactividad.



Las siguientes directivas se pueden configurar en Citrix Studio versión 7.12 y posteriores.

- MaxSpeexQuality

  Valor (entero):

  Valor predeterminado: 5

Detalles:

La redirección de audio codifica los datos de audio con el códec Speex cuando la calidad de audio es media o baja (consulte la directiva Calidad de audio). Speex es un códec con pérdida, lo que significa que logra la compresión a expensas de la fidelidad de la señal de voz de entrada. A diferencia de otros códecs de voz, es posible controlar el equilibrio entre la calidad y la velocidad de bits. El proceso de codificación Speex se controla la mayor parte del tiempo mediante un parámetro de calidad que oscila entre 0 y 10. Cuanto mayor sea la calidad, mayor será la velocidad de bits.

La calidad máxima de Speex elige la mejor calidad de Speex para codificar datos de audio según la calidad de audio y el límite de ancho de banda (consulte la directiva Límite de ancho de banda de redirección de audio). Si la calidad de audio es media, el codificador está en modo de banda ancha, lo que significa una mayor frecuencia de muestreo. Si la calidad de audio es baja, el codificador está en modo de banda estrecha, lo que significa una menor frecuencia de muestreo. La misma calidad de Speex tiene diferentes tasas de bits en diferentes modos. La mejor calidad de Speex se da cuando el valor más grande cumple las siguientes condiciones:

- Es igual o inferior a la calidad máxima de Speex.
- Su tasa de bits es igual o inferior al límite de ancho de banda.

Configuración relacionada: Calidad de audio, Límite de ancho de banda de redirección de audio

- PrimarySelectionUpdateMode

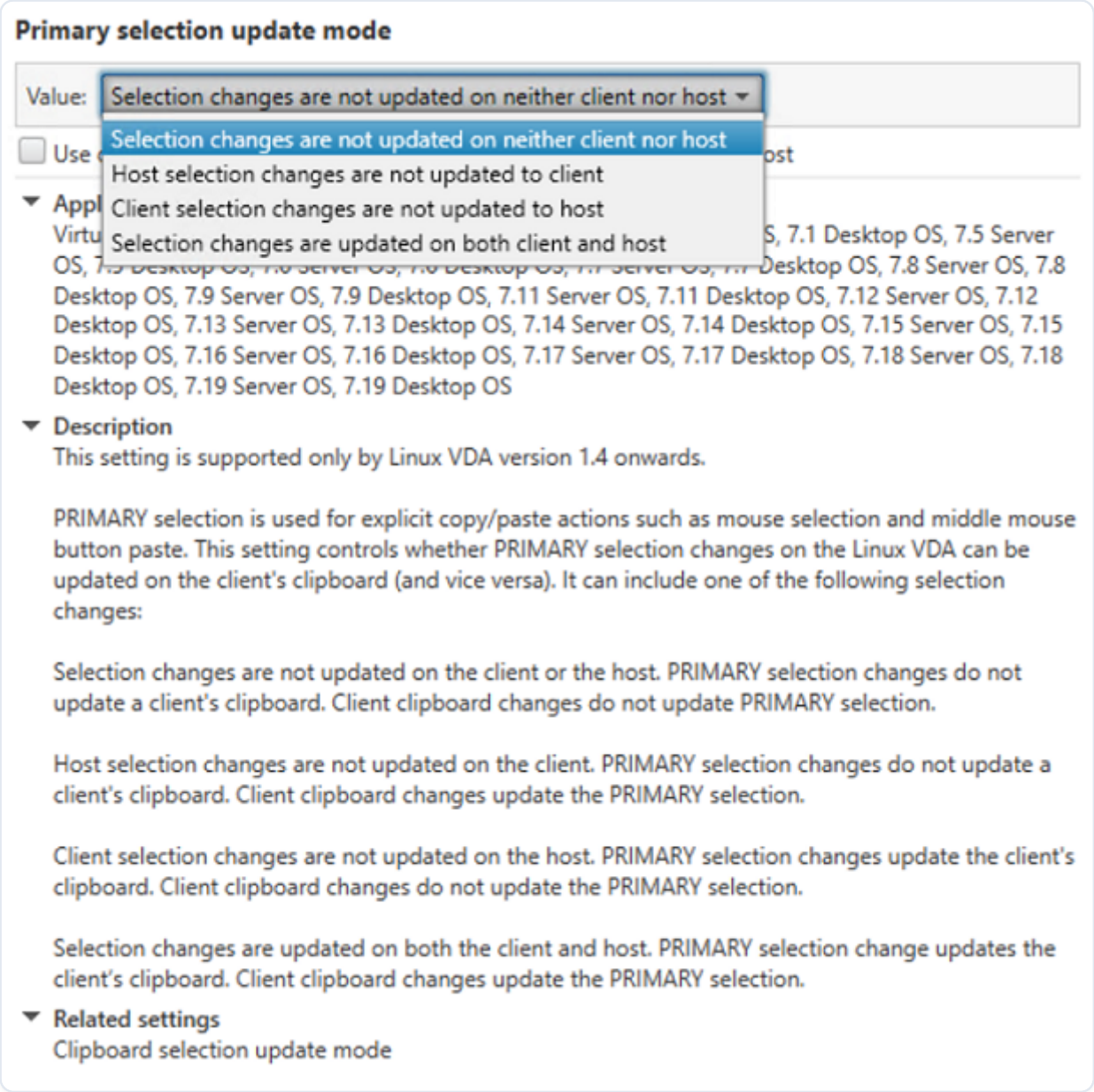
Valor (enumeración):

Valor predeterminado: 3

Detalles:

La selección principal se utiliza cuando se seleccionan datos y se pegan pulsando el botón central del ratón.

Esta directiva controla si los cambios de selección principal en el VDA de Linux y el cliente pueden actualizar el portapapeles entre sí. Hay cuatro opciones de valor:



- **Los cambios de selección no se actualizan ni en el cliente ni en el host**

  Los cambios de selección principal en el VDA de Linux no actualizan el portapapeles del cliente. Los cambios de selección principal en el cliente no actualizan el portapapeles del VDA de Linux.

- **Los cambios de selección del host no se actualizan en el cliente**

  Los cambios de selección principal en el VDA de Linux no actualizan el portapapeles del cliente. Los cambios de selección principal en el cliente actualizan el portapapeles del VDA de Linux.

- **Los cambios de selección del cliente no se actualizan en el host**

Los cambios de selección principal en el VDA de Linux actualizan el portapapeles del cliente. Los cambios de selección principal en el cliente no actualizan el portapapeles del VDA de Linux.

- **Los cambios de selección se actualizan tanto en el cliente como en el host**

  Los cambios de selección principal en el VDA de Linux actualizan el portapapeles del cliente. Los cambios de selección principal en el cliente actualizan el portapapeles del VDA de Linux. Esta opción es el valor predeterminado.

Configuración relacionada: Modo de actualización de la selección del portapapeles

- ClipboardSelectionUpdateMode

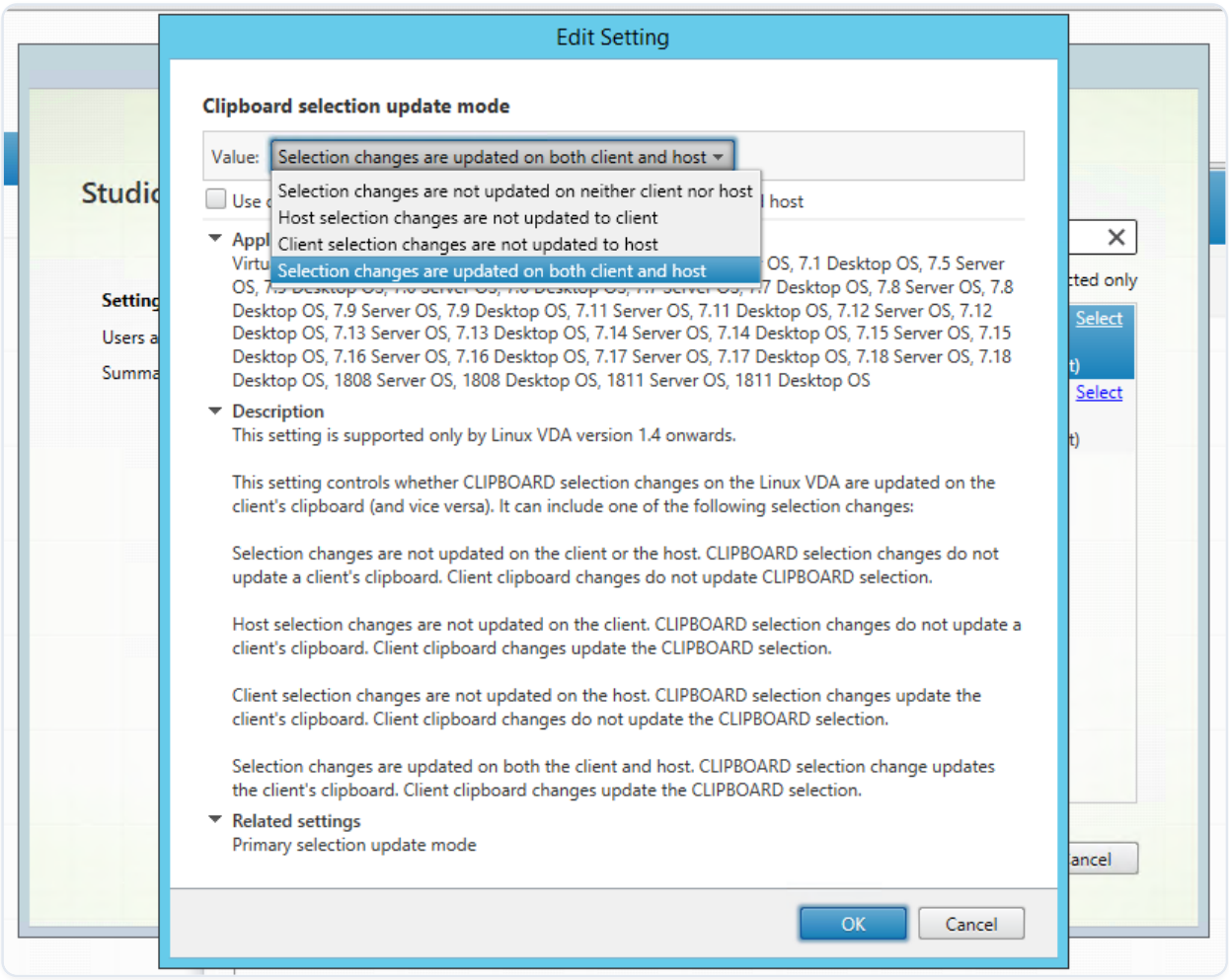
Valor (enumeración):

Valor predeterminado: 3

Detalles:

La selección del portapapeles se utiliza cuando se seleccionan algunos datos y se solicita explícitamente que se copien al portapapeles, por ejemplo, eligiendo 'Copiar' en el menú contextual. La selección del portapapeles se asocia principalmente con las operaciones del portapapeles de Microsoft Windows, mientras que la selección principal es exclusiva de Linux.

Esta directiva controla si los cambios en la selección del portapapeles en el VDA de Linux y en el cliente pueden actualizar el portapapeles entre sí. Hay cuatro opciones de valor:



- **Los cambios de selección no se actualizan ni en el cliente ni en el host**

  Los cambios en la selección del portapapeles en el VDA de Linux no actualizan el portapapeles en el cliente. Los cambios en la selección del portapapeles en el cliente no actualizan el portapapeles en el VDA de Linux.

- **Los cambios de selección del host no se actualizan en el cliente**

  Los cambios en la selección del portapapeles en el VDA de Linux no actualizan el portapapeles en el cliente. Los cambios en la selección del portapapeles en el cliente actualizan el portapapeles en el VDA de Linux.

- **Los cambios de selección del cliente no se actualizan en el host**

  Los cambios en la selección del portapapeles en el VDA de Linux actualizan el portapapeles en el cliente. Los cambios en la selección del portapapeles en el cliente no actualizan el portapapeles en el VDA de Linux.

- **Los cambios de selección se actualizan tanto en el cliente como en el host**

Los cambios en la selección del portapapeles en el VDA de Linux actualizan el portapapeles en el cliente. Los cambios en la selección del portapapeles en el cliente actualizan el portapapeles en el VDA de Linux. Esta opción es el valor predeterminado.

Configuración relacionada: Modo de actualización de la selección principal

Nota:

El VDA de Linux admite tanto la selección del portapapeles como la selección principal. Para controlar los comportamientos de copiar y pegar entre el VDA de Linux y el cliente, le recomendamos que establezca el mismo valor para el modo de actualización de la selección del portapapeles y el modo de actualización de la selección principal.

Impresión

Esta sección contiene los siguientes temas:

- Prácticas recomendadas de impresión
- Impresión de PDF

Prácticas recomendadas de impresión

Este artículo proporciona información sobre las prácticas recomendadas de impresión.

Instalación

El VDA de Linux requiere los filtros **cups** y **foomatic**. Los filtros se instalan al instalar el VDA. También puede instalar los filtros manualmente según la distribución.

Configuración de directivas de impresión

Redirección de impresora de cliente

Esta configuración le permite determinar si las impresoras cliente se asignan a una sesión de VDA. De forma predeterminada, la asignación de impresoras cliente está permitida.

Crear automáticamente impresoras de cliente

Esta configuración especifica las impresoras cliente que se pueden asignar a las sesiones de VDA. De forma predeterminada, está establecida en **Crear automáticamente todas las impresoras cliente**, lo que significa que todas las impresoras cliente se asignan a las sesiones de

VDA. Para obtener más información sobre esta configuración, consulte Crear automáticamente impresoras cliente en la documentación de Citrix Virtual Apps and Desktops.

Crear automáticamente impresora universal PDF

Para usar la función de impresión PDF, establezca esta directiva en **Habilitado**.

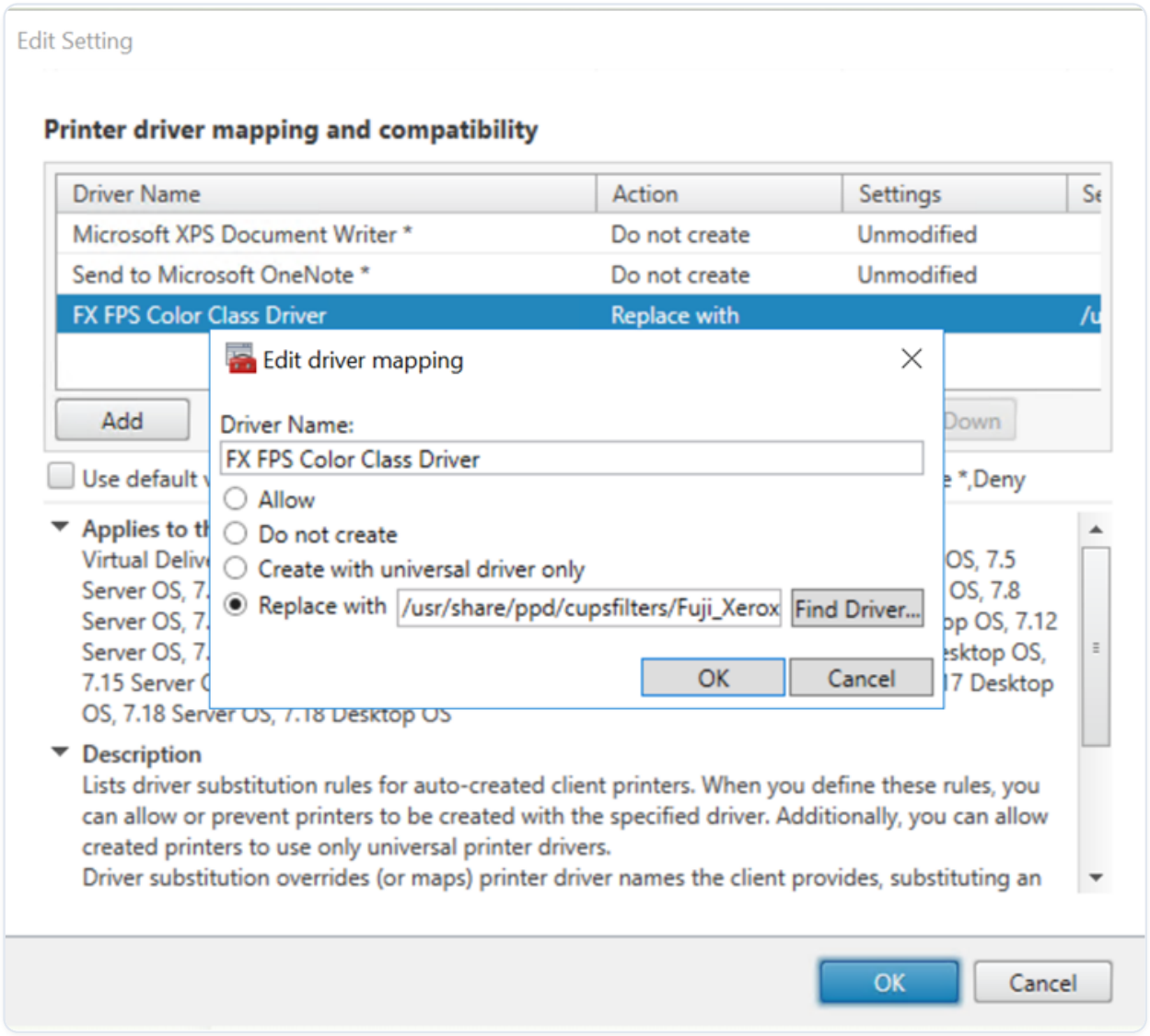
Asignación y compatibilidad de controladores de impresora

Citrix suministra tres tipos de controladores de impresora universales (postscript, pcl5 y pcl6). Sin embargo, es posible que el controlador de impresora universal no sea compatible con su impresora cliente. En este caso, su única opción en versiones anteriores era editar el archivo de configuración ~/.CtxlpProfile$CLIENT_NAME. A partir de la versión 1906, puede optar por configurar la directiva **Asignación y compatibilidad de controladores de impresora** en Citrix Studio.

Para configurar la directiva **Asignación y compatibilidad de controladores de impresora** en Citrix Studio:

1. Seleccione la directiva **Asignación y compatibilidad de controladores de impresora**.
2. Haga clic en **Agregar**.
3. Rellene **Nombre del controlador** con el nombre del controlador de la impresora cliente. Si utiliza la aplicación Citrix Workspace™ para Linux, rellene el nombre de la impresora en su lugar.
4. Realice las siguientes acciones según sea necesario:

    - Para permitir que la impresora cliente se redirija a la sesión de VDA y use solo controladores de impresión universales, seleccione **Permitir** o **Crear solo con controlador universal**.
    - Para evitar que la impresora cliente con el nombre de controlador especificado se redirija a la sesión de VDA, seleccione **No crear**.
    - Para dar a las aplicaciones de servidor acceso a la impresora cliente que tiene el mismo controlador que el servidor pero con un nombre de controlador diferente, seleccione **Reemplazar con** e introduzca la ruta absoluta del archivo del controlador en el VDA.



Nota:

Solo se admiten archivos de controlador PPD.

Uso

Puede imprimir tanto desde escritorios publicados como desde aplicaciones publicadas. Todas las impresoras cliente se pueden asignar a una sesión de VDA. Los nombres de las impresoras son diferentes para escritorios y aplicaciones:

- Para escritorios publicados:

  ```
  <client printer name>:$CLIENT_NAME:dsk$SESSION_ID
  ```

- Para aplicaciones publicadas:

`<client printer name>:$CLIENT_NAME:app$SESSION_ID`

Nota:

Si el mismo usuario abre un escritorio publicado y una aplicación publicada, ambas impresoras estarán disponibles para la sesión. La impresión en una impresora de escritorio en una sesión de aplicación publicada, o la impresión en una impresora de aplicación en un escritorio publicado, fallará.

Solución de problemas

No se puede imprimir

Cuando la impresión no funciona correctamente, compruebe el demonio de impresión **ctxlpmngt** y el **marco de trabajo de CUPS**.

El demonio de impresión **ctxlpmngt** es un proceso por sesión y debe estar en ejecución durante toda la sesión. Ejecute el siguiente comando para verificar que el demonio de impresión está en ejecución. Si **ctxlpmngt** no está en ejecución, inicie **ctxlpmngt** manualmente desde la línea de comandos.

```
ps –ef | grep ctxlpmngt
```

Si la impresión sigue sin funcionar, compruebe el marco de trabajo de **CUPS**. El servicio **ctxcups** se utiliza para la gestión de impresoras y se comunica con el marco de trabajo de CUPS de Linux. Es un único proceso por máquina y se puede comprobar ejecutando el siguiente comando:

```
systemctl status ctxcups
```

Pasos adicionales para recopilar registros de CUPS

Para recopilar registros de CUPS, ejecute los siguientes comandos para configurar el archivo de servicio de CUPS. De lo contrario, los registros de CUPS no se podrán grabar en **hdx.log**:

```
sudo systemctl stop cups



sudo vi /etc/systemd/system/printer.target.wants/cups.service
```

```
PrivateTmp=false
```

```
sudo systemctl start cups
```

```
sudo systemctl daemon-reload
```

Nota:

Esta configuración se realiza únicamente para recopilar el registro de impresión completo cuando surge un problema. En circunstancias normales, esta configuración no se recomienda porque rompe la seguridad de CUPS.

La salida de impresión está distorsionada

Un controlador de impresora incompatible puede causar una salida ilegible. Hay disponible una configuración de controlador por usuario que se puede configurar editando el archivo de configuración **~/.CtxlpProfile$CLIENT_NAME**:

```
[DEFAULT_PRINTER]
```

```
printername=
```

```
model=
```

```
ppdpath=
```

```
drivertype=
```

Importante:

El campo **printername** contiene el nombre de la impresora predeterminada actual del lado del cliente. Es un valor de solo lectura. No lo edite.

Los campos **ppdpath**, **model** y **drivertype** no se pueden configurar al mismo tiempo porque solo uno de ellos surte efecto para la **impresora asignada**.

- Si el controlador de impresora universal no es compatible con la impresora cliente, configure el modelo del controlador de impresora nativo mediante la opción **model**=. Puede encontrar el nombre del modelo actual de la impresora utilizando el comando **lpinfo**:

```
lpinfo –m

…

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

A continuación, puede configurar el modelo para que coincida con la impresora:

```
model=xerox/ph3115.ppd.gz
```

- Si el controlador de impresora universal no es compatible con la impresora cliente, configure la ruta del archivo PPD del controlador de impresora nativo. El valor de **ppdpath** es la ruta absoluta del archivo del controlador de impresora nativo.

  Por ejemplo, hay un **controlador ppd** en /home/tester/NATIVE_PRINTER_DRIVER.ppd:

  ```
  ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
  ```

- Citrix suministra tres tipos de controlador de impresora universal (postscript, pcl5 y pcl6). Puede configurar el tipo de controlador según las propiedades de su impresora.

  Por ejemplo, si el tipo de controlador de impresora predeterminado del cliente es PCL5, establezca **drivertype** en:

  ```
  drivertype=pcl5
  ```

El tamaño de salida es cero

Pruebe diferentes tipos de impresoras. Y pruebe una impresora virtual como CutePDF y PDFCreator para averiguar si este problema está relacionado con el controlador de la impresora.

El trabajo de impresión depende del controlador de la impresora predeterminada del cliente. Es importante identificar el tipo de controlador activo actual. Si la impresora cliente utiliza un controlador PCL5 pero el VDA de Linux elige un controlador Postscript, puede producirse un problema.

Si el tipo de controlador de impresora es correcto, puede identificar el problema realizando los siguientes pasos:

1. Inicie sesión en una sesión de escritorio publicada.
2. Ejecute el comando **vi ~/.CtxlpProfile$CLIENT_NAME**.
3. Añada el siguiente campo para guardar el archivo de cola en el VDA de Linux:

   ```
   deletespoolfile=no
   ```

4. Cierre la sesión y vuelva a iniciarla para cargar los cambios de configuración.
5. Imprima el documento para reproducir el problema. Después de imprimir, se guarda un archivo de cola en `/var/spool/cups-ctx/$logon_user/$spool_file`.

6. Compruebe si la cola está vacía. Si el archivo de cola es cero, representa un problema. Póngase en contacto con el Soporte de Citrix (y proporcione el registro de impresión) para obtener más orientación.
7. Si el tamaño de la cola no es cero, copie el archivo en el cliente. El contenido del archivo de cola depende del tipo de controlador de impresora de la impresora predeterminada del cliente. Si el controlador de la impresora asignada (nativa) es PostScript, el archivo de cola se puede abrir directamente en el sistema operativo Linux. Compruebe si el contenido es correcto.

   Si el archivo de cola es PCL, o si el sistema operativo cliente es Windows, copie el archivo de cola en el cliente e imprímalo en la impresora del lado del cliente utilizando un controlador de impresora diferente.
8. Cambie la **impresora asignada** para usar un controlador de impresora diferente. El siguiente ejemplo utiliza la impresora cliente PostScript como ejemplo:

   a. Inicie sesión en una sesión activa y abra un explorador en el escritorio del cliente.
   b. Abra el portal de administración de impresión:

      ```
      localhost:631
      ```

   c. Elija la **impresora asignada** `CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID` y **Modificar impresora**. Esta operación requiere privilegios de administrador.
   d. Mantenga la conexión **cups-ctx** y, a continuación, haga clic en **Continuar** para cambiar el controlador de impresora.
   e. En los campos **Fabricante** y **Modelo**, elija un controlador de impresora diferente del controlador UPD de Citrix. Por ejemplo, si la impresora virtual CUPS-PDF está instalada, seleccione el controlador de impresora genérico CUPS-PDF. Guarde el cambio.
   f. Si este proceso se realiza correctamente, configure la ruta del archivo PPD del controlador en `.CtxlpProfile$CLIENT_NAME` para permitir que la impresora asignada utilice el controlador recién seleccionado.

Problemas conocidos

Se han identificado los siguientes problemas durante la impresión en el VDA de Linux:

El controlador CTXPS no es compatible con algunas impresoras PLC

Si encuentra corrupción en la salida de impresión, configure el controlador de impresora al nativo proporcionado por el fabricante.

Rendimiento de impresión lento para documentos grandes

Cuando imprime un documento grande en una impresora cliente local, el documento se transfiere a través de la conexión del servidor. En conexiones lentas, la transferencia puede tardar mucho tiempo.

Notificaciones de impresora y trabajos de impresión vistas desde otras sesiones

Linux no tiene el mismo concepto de sesión que el sistema operativo Windows. Por lo tanto, todos los usuarios reciben notificaciones en todo el sistema. Puede deshabilitar estas notificaciones cambiando el archivo de configuración de CUPS: **/etc/cups/cupsd.conf**.

Localice el nombre de la política actual configurado en el archivo:

`DefaultPolicy default`

Si el nombre de la política es *default*, añada las siguientes líneas al bloque XML de la política predeterminada:

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default

     … …
```

```
    <Limit Create-Printer-Subscription>

        Require user @OWNER

        Order deny,allow

    </Limit>

    <Limit All>

        Order deny,allow

    </Limit>

</Policy>
```

Impresión PDF

Al usar una versión de la aplicación Citrix Workspace™ que admita la impresión de PDF, puede imprimir archivos PDF convertidos desde las sesiones de Linux VDA. Los trabajos de impresión de la sesión se envían a la máquina local donde está instalada la aplicación Citrix Workspace. En la máquina local, puede abrir archivos PDF con el visor de PDF que prefiera e imprimirlos en la impresora que elija.

El VDA de Linux admite la impresión de PDF en las siguientes versiones de la aplicación Citrix Workspace:

- Citrix Receiver para HTML5 versiones 2.4 a 2.6.9, aplicación Citrix Workspace 1808 para HTML5 y posteriores
- Citrix Receiver para Chrome versiones 2.4 a 2.6.9, aplicación Citrix Workspace 1808 para Chrome y posteriores
- Aplicación Citrix Workspace 1905 para Windows y posteriores

Configuración

Además de usar una versión de la aplicación Citrix Workspace que admita la impresión de PDF, configure las siguientes directivas en Citrix Studio:

- Establezca **Redirección de impresora cliente** en **Permitido** (**Permitido** de forma predeterminada)
- Establezca **Crear automáticamente impresora universal PDF** en **Habilitado** (**Deshabilitado** de forma predeterminada)
- Establezca **Crear automáticamente impresoras cliente** en **Crear automáticamente todas las impresoras cliente**.

Con estas directivas habilitadas, aparece una vista previa de impresión en la máquina local para que seleccione una impresora al hacer clic en **Imprimir** dentro de la sesión iniciada. Consulte la documentación de la aplicación Citrix Workspace para obtener información sobre cómo configurar las impresoras predeterminadas.

Acceso con PC remoto

Información general

Acceso remoto a PC es una extensión de Citrix Virtual Apps and Desktops. Permite a las organizaciones que los empleados accedan fácilmente a sus equipos físicos de oficina de forma remota y segura. Si los usuarios pueden acceder a sus equipos de oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para realizar su trabajo.

Acceso remoto a PC utiliza los mismos componentes de Citrix Virtual Apps™ y Desktops que ofrecen escritorios y aplicaciones virtuales. Los requisitos y el proceso de implementación y configuración de Acceso remoto a PC son los mismos que los requisitos y el proceso necesarios para implementar Citrix Virtual Apps and Desktops. Esta uniformidad proporciona una experiencia administrativa coherente y unificada. Los usuarios obtienen la mejor experiencia de usuario al utilizar Citrix HDX para ofrecer sus sesiones remotas de PC de oficina.

Para obtener más información, consulte Acceso remoto a PC en la documentación de Citrix Virtual Apps and Desktops.

Consideraciones

Estas consideraciones son específicas de Linux VDA:

- En máquinas físicas, utilice el VDA de Linux solo en modo no 3D. Debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no se puede apagar cuando el modo HDX™ 3D está habilitado. Mostrar esta pantalla es un riesgo potencial de seguridad.
- Utilice catálogos de máquinas de tipo SO de sesión única para máquinas físicas Linux.
- La asignación automática de usuarios no está disponible para máquinas Linux. Con la asignación automática de usuarios, los usuarios se asignan a sus máquinas automáticamente cuando inician sesión localmente en los PC. Este inicio de sesión se produce sin la intervención del administrador. La aplicación Citrix Workspace™ en el cliente ayuda a los usuarios a acceder a las aplicaciones y los datos del PC de oficina dentro de la sesión de escritorio de Acceso remoto a PC.
- Si los usuarios ya han iniciado sesión en sus PC localmente, los intentos de iniciar los PC desde StoreFront™ fallarán.
- Las opciones de ahorro de energía no están disponibles para máquinas Linux.

Configuración

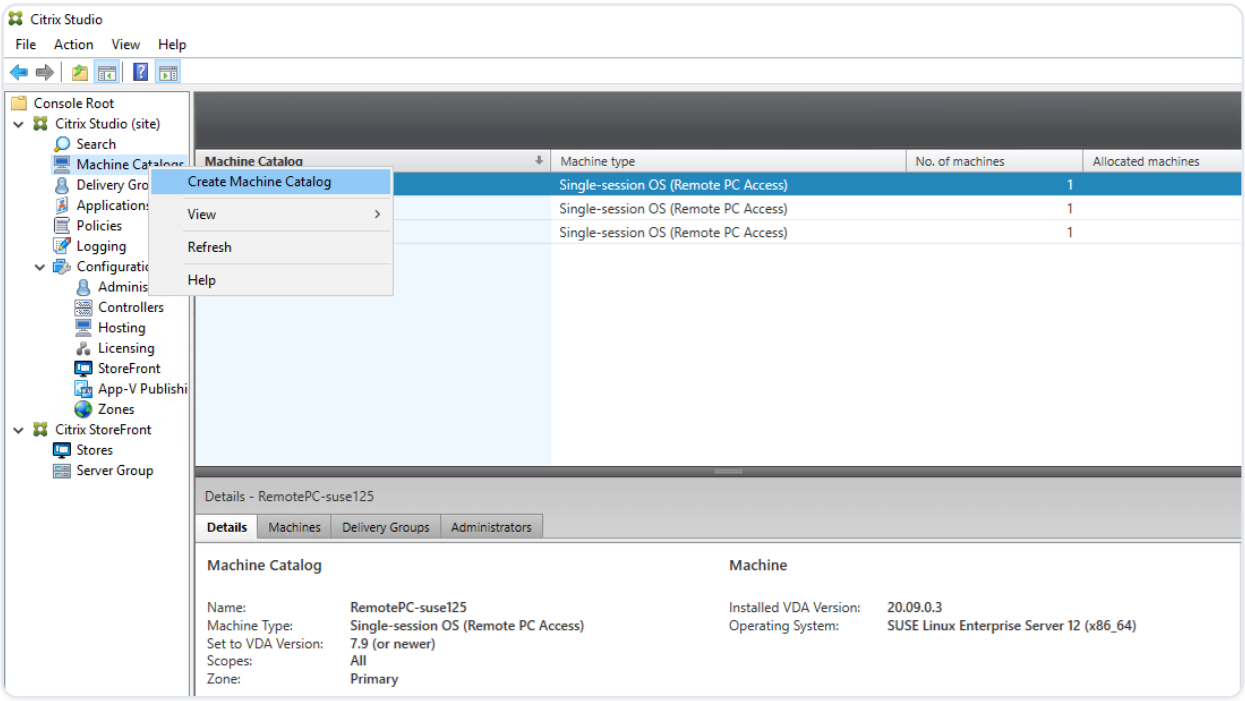
Para ofrecer sesiones de PC Linux, instale el VDA de Linux en los PC de destino, cree un catálogo de máquinas del tipo **Acceso remoto a PC** y cree un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso. La siguiente sección detalla el procedimiento:

Paso 1: Instale el VDA de Linux en los PC de destino

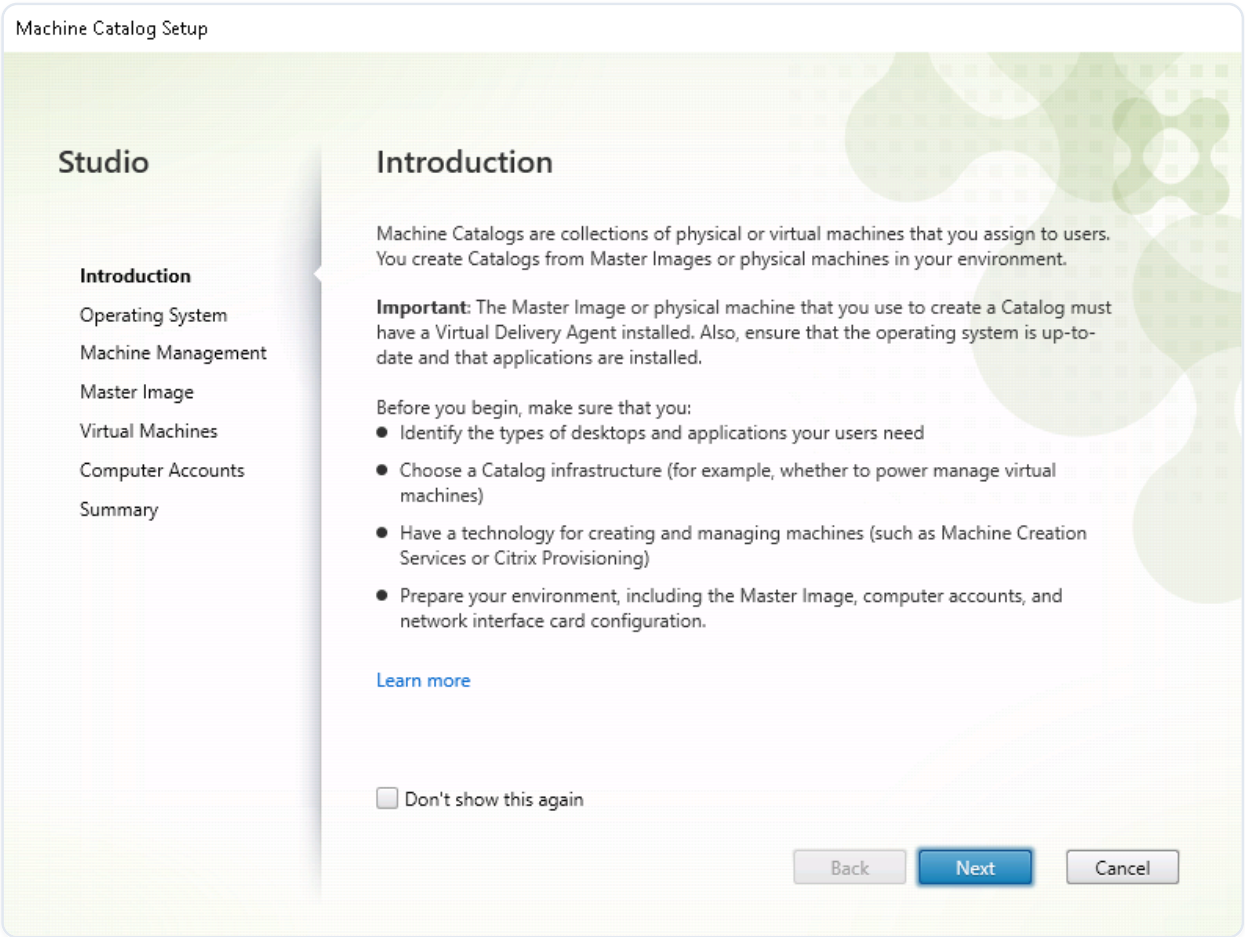
Le recomendamos que utilice instalación sencilla para instalar el VDA de Linux. Durante la instalación, establezca el valor de la variable `CTX_XDL_VDI_MODE` en `Y`.

Paso 2: Cree un catálogo de máquinas del tipo Acceso remoto a PC

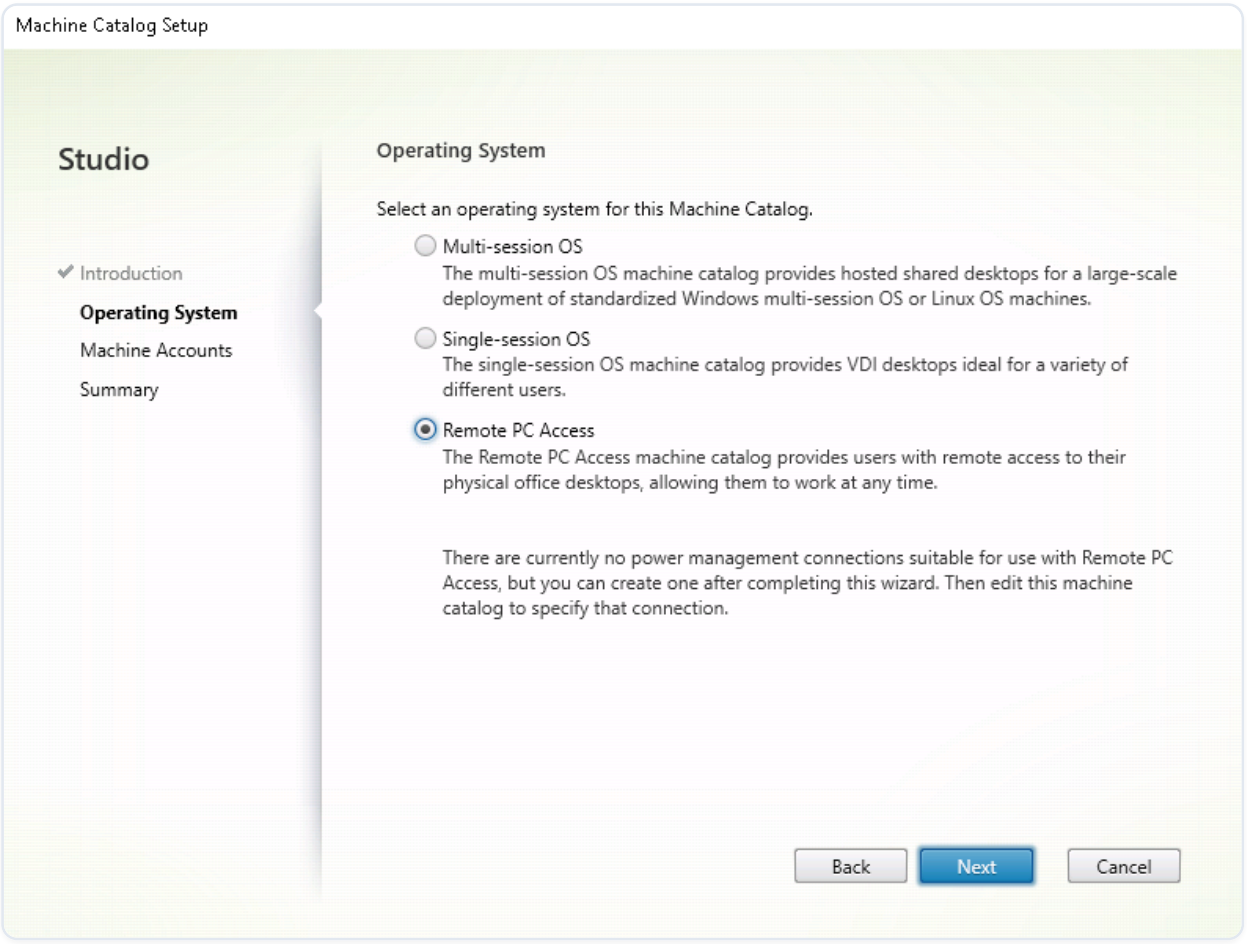
1. En Citrix Studio, haga clic con el botón derecho en **Catálogos de máquinas** y seleccione **Crear catálogo de máquinas** en el menú contextual.



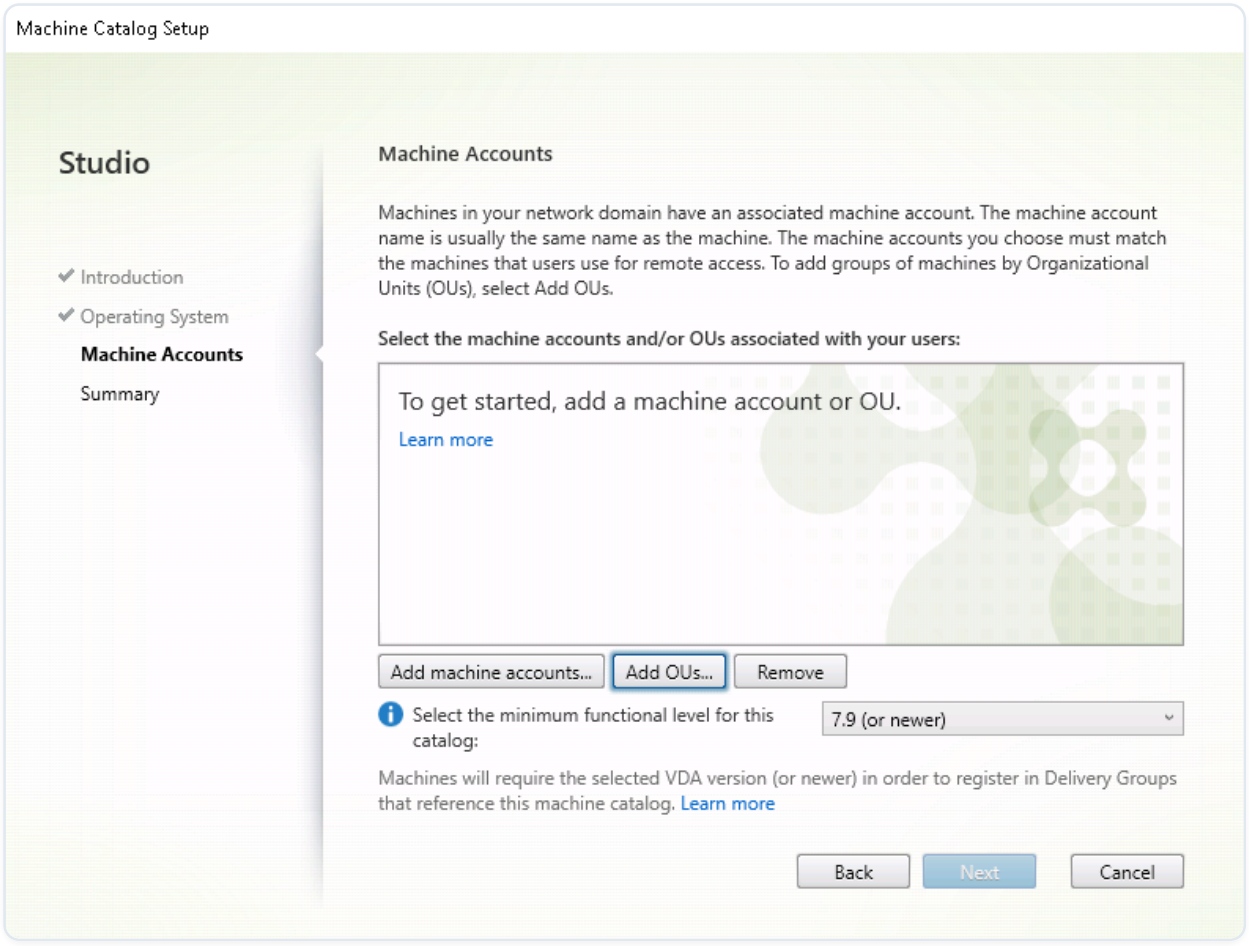
2. Haga clic en **Siguiente** en la página **Introducción**.



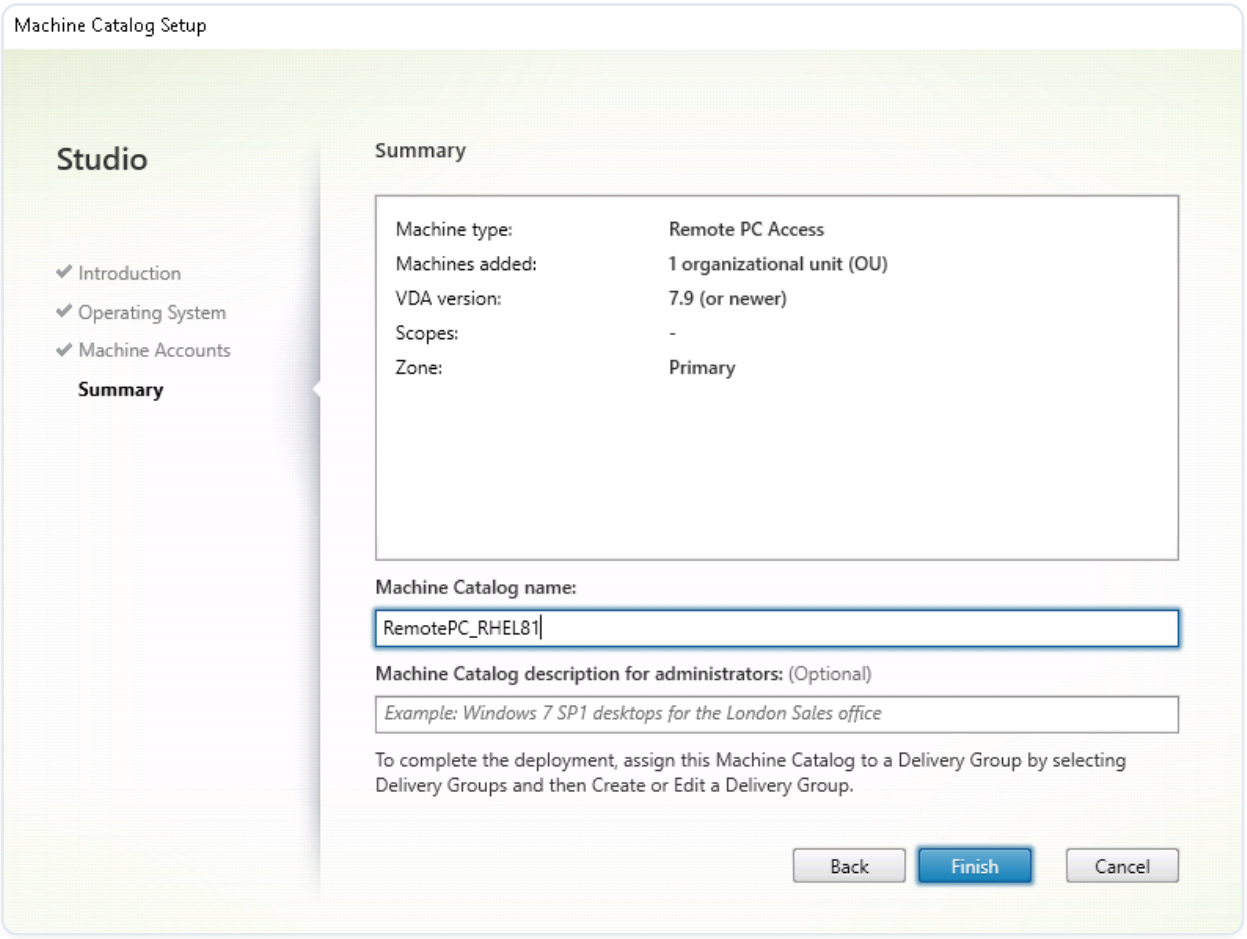
3. Seleccione **Acceso remoto a PC** en la página **Sistema operativo**.



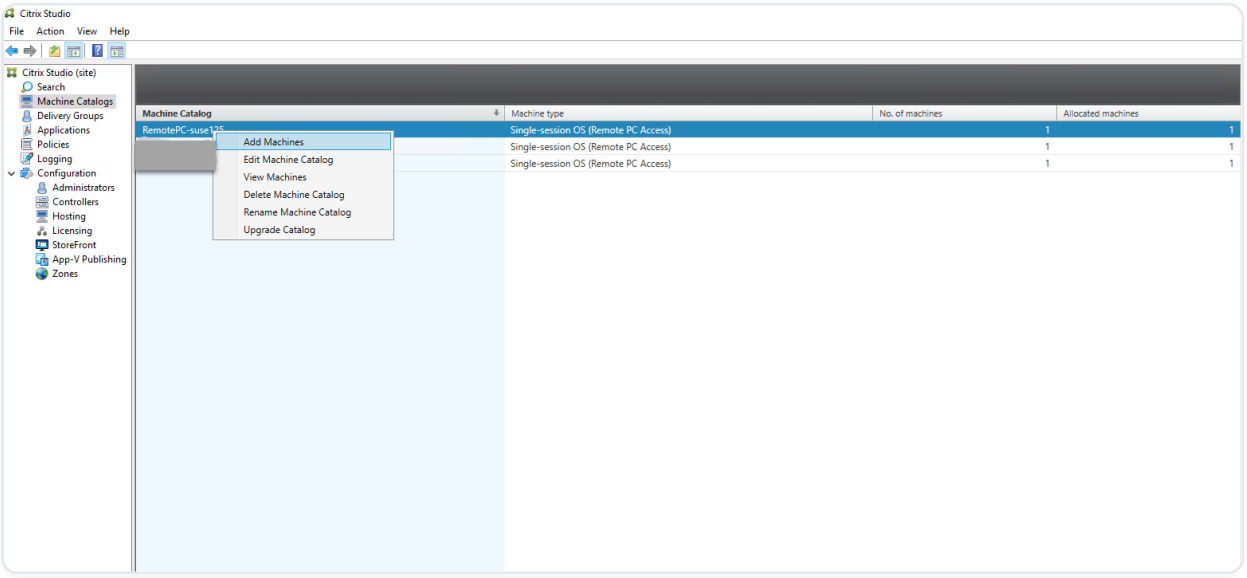
4. Haga clic en **Agregar UO** para seleccionar las UO que contienen los PC de destino, o haga clic en **Agregar cuentas de máquina** para agregar máquinas individuales al catálogo de máquinas.



5. Asigne un nombre al catálogo de máquinas.

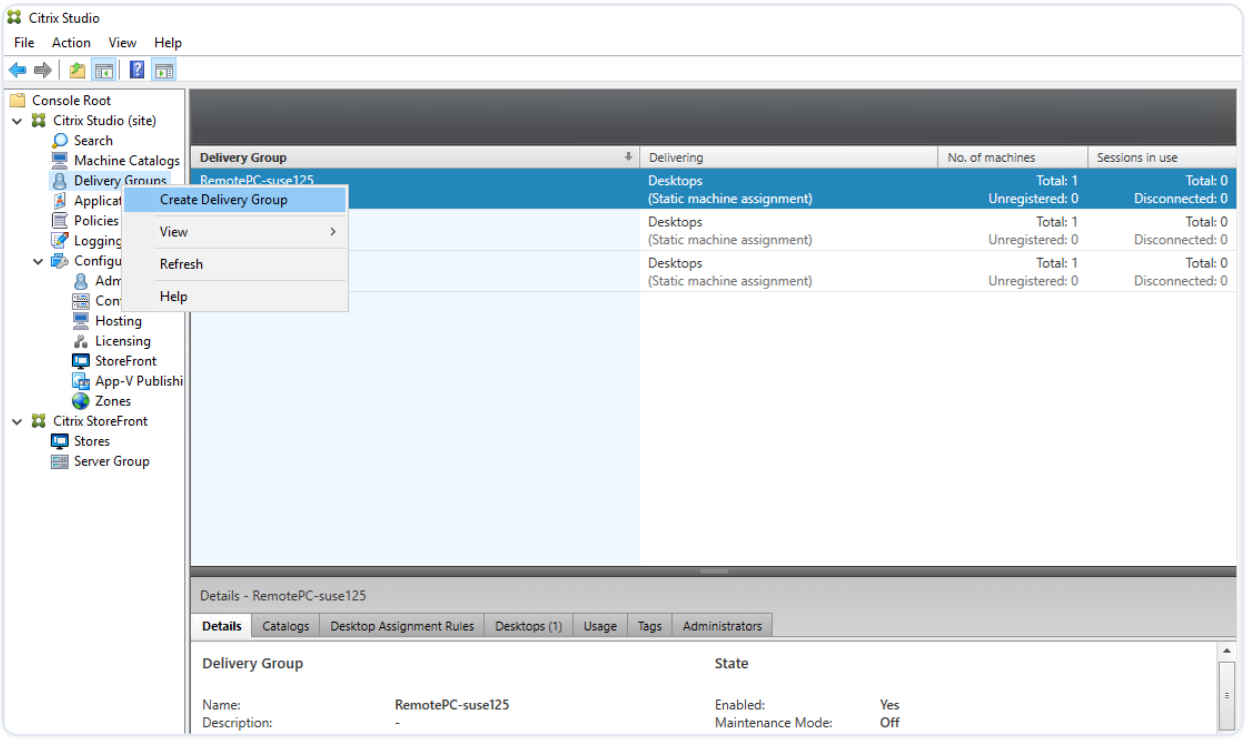


6. (Opcional) Haga clic con el botón derecho en el catálogo de máquinas para realizar las operaciones pertinentes.

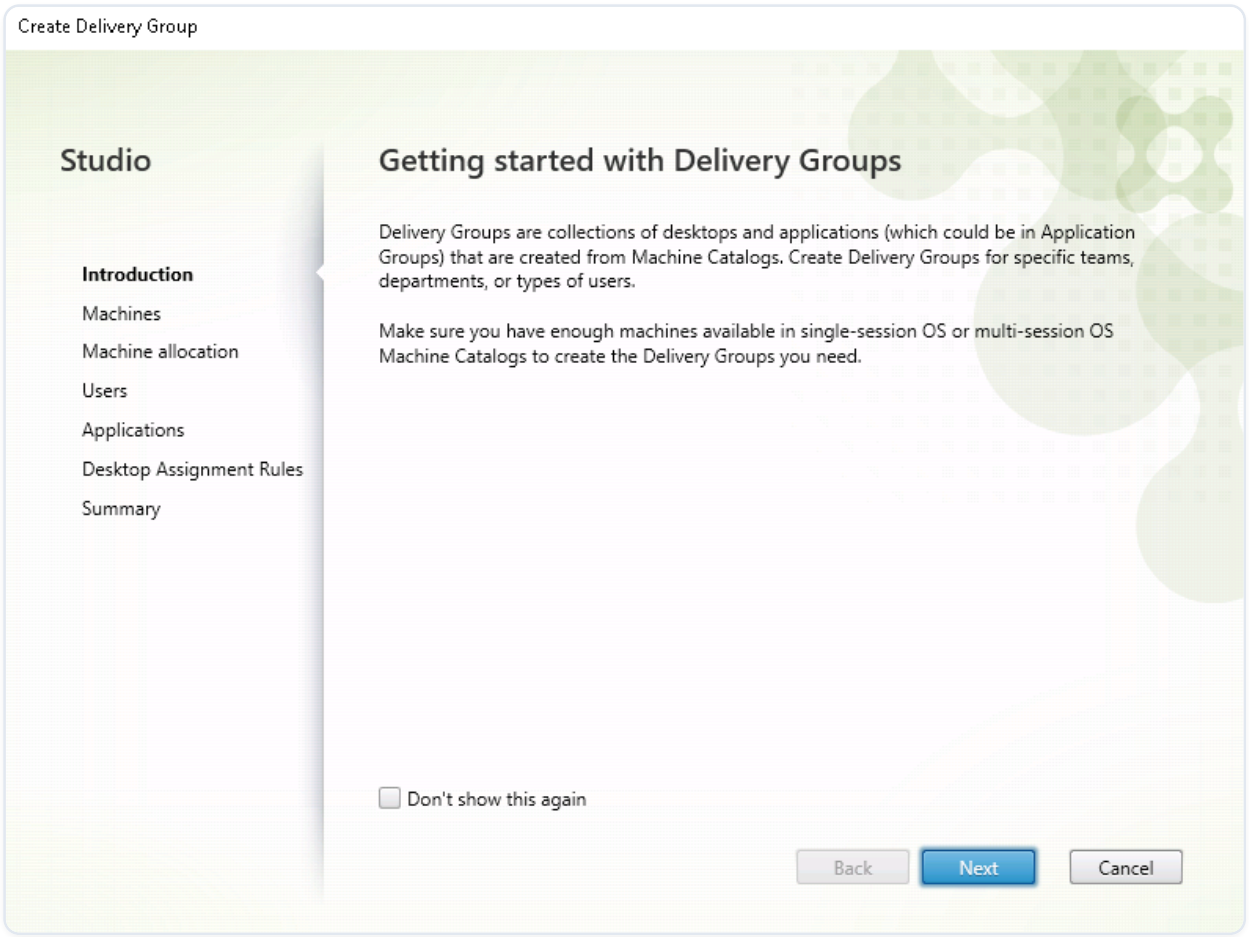


Paso 3: Cree un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso

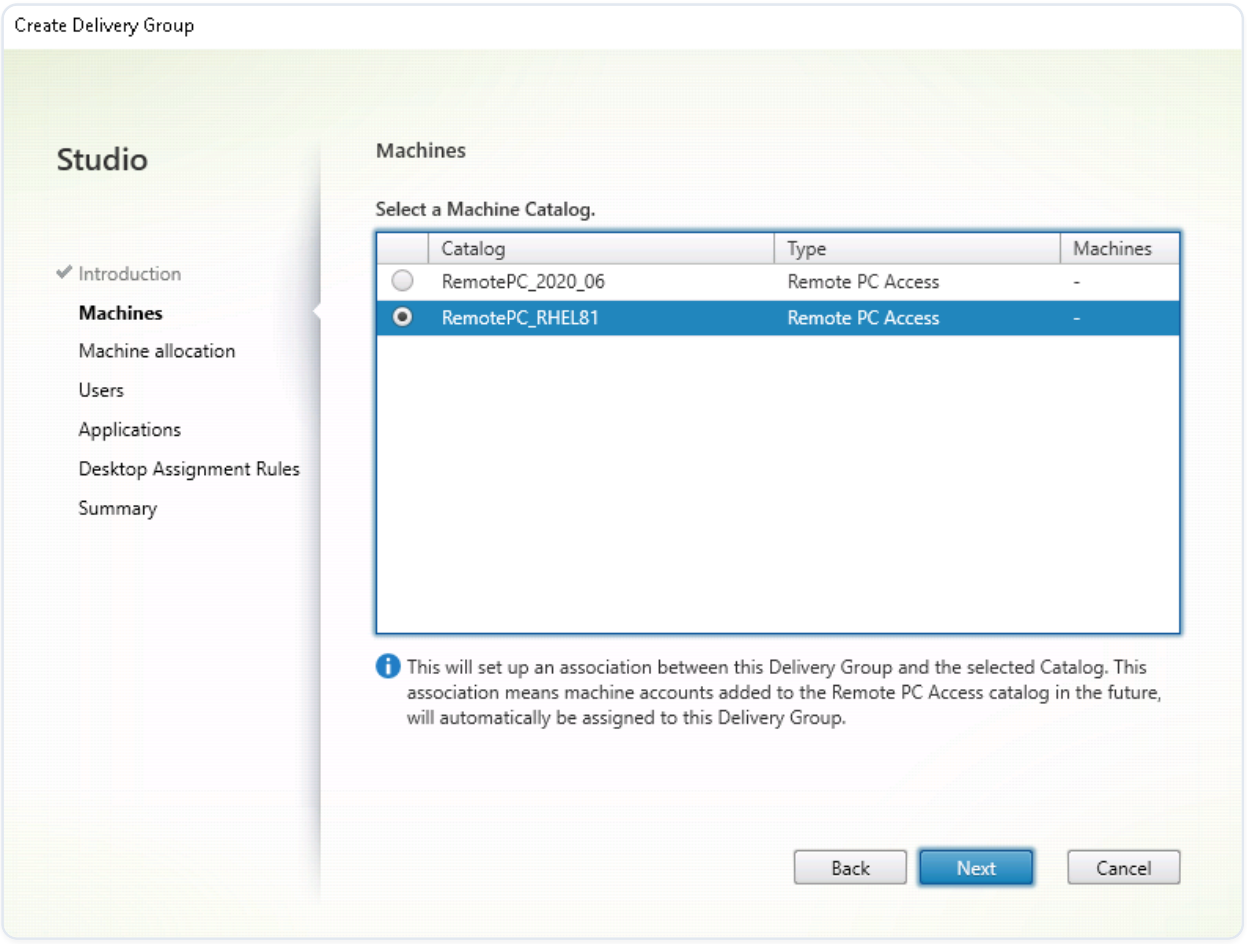
1. En Citrix Studio, haga clic con el botón derecho en **Grupos de entrega** y seleccione **Crear grupo de entrega** en el menú contextual.



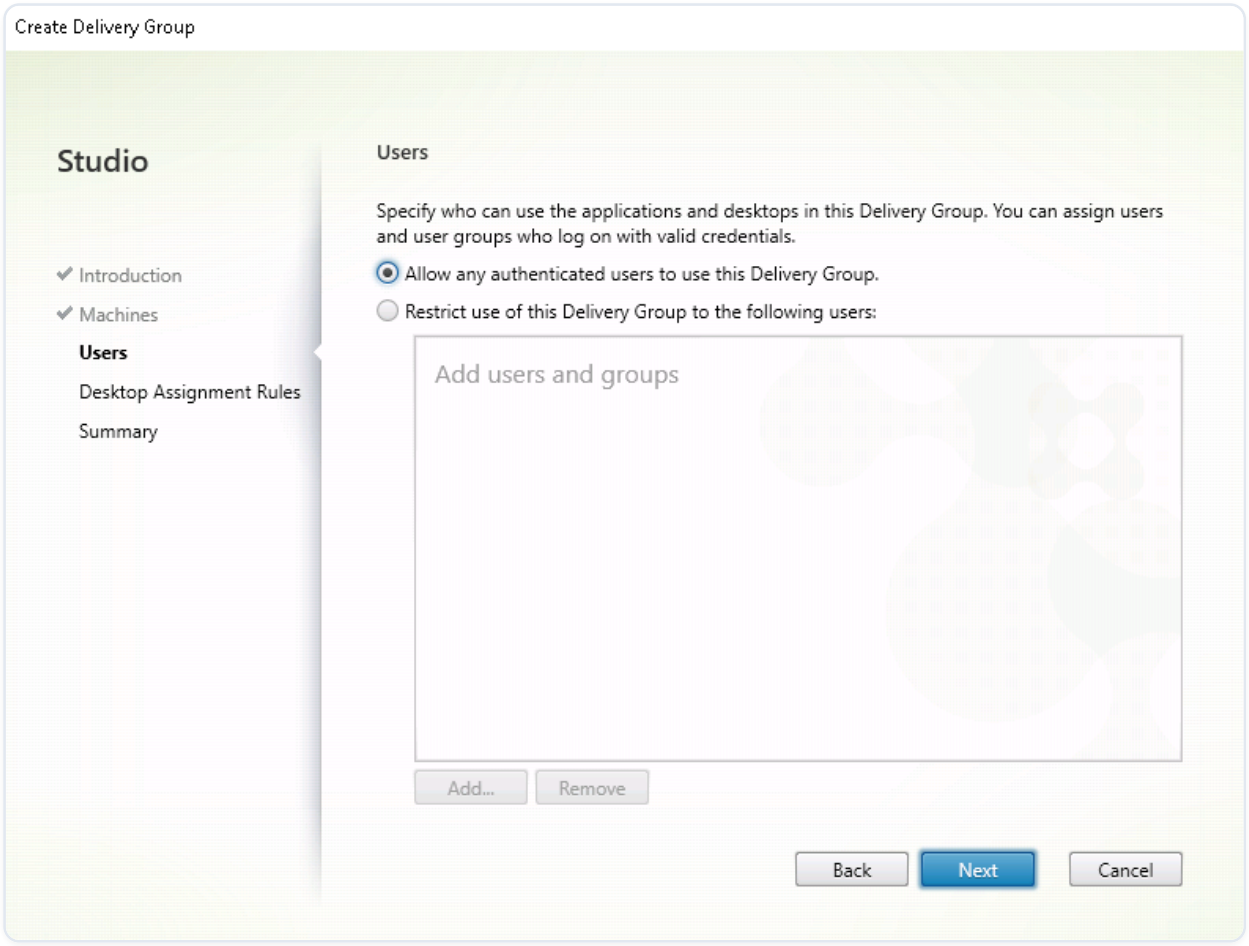
2. Haga clic en **Siguiente** en la página **Introducción a los grupos de entrega**.



3. Seleccione el catálogo de máquinas creado en el Paso 2 para asociarlo con el Grupo de entrega.



4. Agregue usuarios que puedan acceder a los PC del catálogo de máquinas. Los usuarios que agregue pueden usar la aplicación Citrix Workspace en un dispositivo cliente para acceder a los PC de forma remota.



Wake on LAN

Acceso con PC remoto admite Wake on LAN, lo que permite a los usuarios encender PC físicos de forma remota. Esta función permite a los usuarios mantener sus PC de oficina apagados cuando no están en uso para ahorrar costes de energía. También permite el acceso remoto cuando una máquina se ha apagado inadvertidamente.

Con la función Wake on LAN, los paquetes mágicos se envían directamente desde el VDA que se ejecuta en el PC a la subred en la que reside el PC cuando lo indica el controlador de entrega. Esto permite que la función funcione sin depender de componentes de infraestructura adicionales o soluciones de terceros para la entrega de paquetes mágicos.

La función Wake on LAN difiere de la función Wake on LAN heredada basada en SCCM. Para obtener información sobre Wake on LAN basado en SCCM, consulte Wake on LAN – Integrado con SCCM.

Requisitos del sistema

Los siguientes son los requisitos del sistema para usar la función Wake on LAN:

- Plano de control:

  - Citrix DaaS™ (anteriormente Citrix Virtual Apps and Desktops servicio)
  - Citrix Virtual Apps and Desktops 2012 o posterior

- PC físicos:
  - VDA versión 2012 o posterior
  - Wake on LAN habilitado en la BIOS y en la NIC

Configurar Wake on LAN

Actualmente, la configuración de Wake on LAN integrado solo se admite mediante PowerShell.

Para configurar Wake on LAN:

1. Cree el catálogo de máquinas de Acceso con PC remoto si aún no tiene uno.
2. Cree la conexión de host de Wake on LAN si aún no tiene una.

> **Nota:**
>
> Para usar la función Wake on LAN, si tiene una conexión de host del tipo "Microsoft Configuration Manager Wake on LAN", cree una conexión de host.

3. Recupere el identificador único de la conexión de host de Wake on LAN.
4. Asocie la conexión de host de Wake on LAN con un catálogo de máquinas.

   Para crear la conexión de host de Wake on LAN:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection
```

```
$hypHc = New-Item -Path xdhyp:\Connections `
             -Name $connectionName `
             -HypervisorAddress "N/A" `
             -UserName "woluser" `
             -Password "wolpwd" `
             -ConnectionType Custom `
             -PluginId VdaWOLMachineManagerFactory `
             -CustomProperties "<CustomProperties></CustomProperties>" `
             -Persist


$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid


# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{
    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
}
```

Cuando la conexión de host esté lista, ejecute los siguientes comandos para recuperar el identificador único de la conexión de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

Después de recuperar el identificador único de la conexión, ejecute los siguientes comandos para asociar la conexión con el catálogo de máquinas de Acceso con PC remoto:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

5. Habilite Wake on LAN en la BIOS y en la NIC en cada VM del catálogo de máquinas.

   Nota: El método para habilitar Wake on LAN varía según las diferentes configuraciones de la máquina.

   - Para habilitar Wake on LAN en la BIOS:

     a. Acceda a la BIOS y habilite la función Wake on LAN.

        El método para acceder a la BIOS depende del fabricante de su placa base y del proveedor de BIOS que haya seleccionado el fabricante.

     b. Guarde la configuración y reinicie la máquina.

   - Para habilitar Wake on LAN en la NIC:

     a. Ejecute el comando `sudo ethtool <NIC>` para comprobar si su NIC admite paquetes mágicos.

        `<NIC>` es el nombre de dispositivo de su NIC, por ejemplo, `eth0`. El comando `sudo ethtool <NIC>` proporciona una salida sobre las capacidades de su NIC:

        - Si la salida contiene una línea similar a `Supports Wake-on: <letters>` donde `<letters>` contiene la letra `g`, su NIC es compatible con el método de paquete mágico Wake on LAN.
        - Si la salida contiene una línea similar a `Wake-on: <letters>` donde `<letters>` contiene la letra `g` y no contiene la letra `d`, el método de paquete mágico Wake on LAN está habilitado. Sin embargo, si `<letters>` contiene la letra `d`, indica que la función Wake on LAN está inhabilitada. En este caso, habilite Wake on LAN ejecutando el comando `sudo ethtool -s <NIC> wol g`.

b. En la mayoría de las distribuciones, el comando `sudo ethtool -s <NIC> wol g` es necesario después de cada inicio. Para establecer esta opción de forma persistente, siga estos pasos según sus distribuciones:

   Ubuntu:

   Añada la línea `up ethtool -s <NIC> wol g` al archivo de configuración de la interfaz `/etc/network/interfaces`. Por ejemplo:

```
# ifupdown has been replaced by netplan(5) on this system. See

# /etc/netplan for current configuration.

# To re-enable ifupdown on this system, you can run:

# sudo apt install ifupdown

auto eth0

iface eth0 inet static

           address 10.0.0.1

           netmask 255.255.240.0

           gateway 10.0.0.1

           up ethtool -s eth0 wol g
```

   RHEL/SUSE:

   Añada el siguiente parámetro `ETHTOOL_OPTS` al archivo de configuración de la interfaz `/etc/sysconfig/network-scripts/ifcfg-<NIC>`:

```
ETHTOOL_OPTS="-s ${DEVICE} wol g"
```

Consideraciones de diseño

Cuando planifique usar Wake on LAN con Acceso con PC remoto, tenga en cuenta lo siguiente:

- Varios catálogos de máquinas pueden usar la misma conexión de host de Wake on LAN.

- Para que un PC active a otro PC, ambos PC deben estar en la misma subred y usar la misma conexión de host de Wake on LAN. No importa si los PC están en el mismo catálogo de máquinas o en catálogos diferentes.
- Las conexiones de host se asignan a zonas específicas. Si su implementación contiene más de una zona, necesita una conexión de host de Wake on LAN en cada zona. Lo mismo se aplica a los catálogos de máquinas.
- Los paquetes mágicos se transmiten utilizando la dirección de difusión global 255.255.255.255. Asegúrese de que la dirección no esté bloqueada.
- Debe haber al menos un PC encendido en la subred (para cada conexión de Wake on LAN) para poder activar las máquinas de esa subred.

Consideraciones operativas

A continuación, se presentan consideraciones para usar la función Wake on LAN:

- El VDA debe registrarse al menos una vez antes de que el PC pueda activarse mediante la función integrada Wake on LAN.
- Wake on LAN solo se puede usar para activar PC. No admite otras acciones de energía, como reiniciar o apagar.
- Una vez creada la conexión Wake on LAN, es visible en Studio. Sin embargo, no se admite la edición de sus propiedades en Studio.
- Los paquetes mágicos se envían de una de estas dos maneras:
  - Cuando un usuario intenta iniciar una sesión en su PC y el VDA no está registrado
  - Cuando un administrador envía un comando de encendido manualmente desde Studio o PowerShell
- Dado que el Delivery Controller no conoce el estado de energía de un PC, Studio muestra **No compatible** en el estado de energía. El Delivery Controller utiliza el estado de registro del VDA para determinar si un PC está encendido o apagado.

Más recursos

Los siguientes son otros recursos para Acceso con PC remoto:

- Guía de diseño de soluciones: Decisiones de diseño de Acceso con PC remoto.
- Ejemplos de arquitecturas de Acceso con PC remoto: Arquitectura de referencia para la solución de Acceso con PC remoto de Citrix.

Sesión

Esta sección contiene los siguientes temas:

- Transporte adaptable
- Inicio de sesión con un directorio principal temporal
- Publicar aplicaciones
- Fiabilidad de la sesión
- Rendezvous V1
- Rendezvous V2
- Proteger sesiones de usuario con TLS
- Proteger sesiones de usuario con DTLS

Transporte adaptable

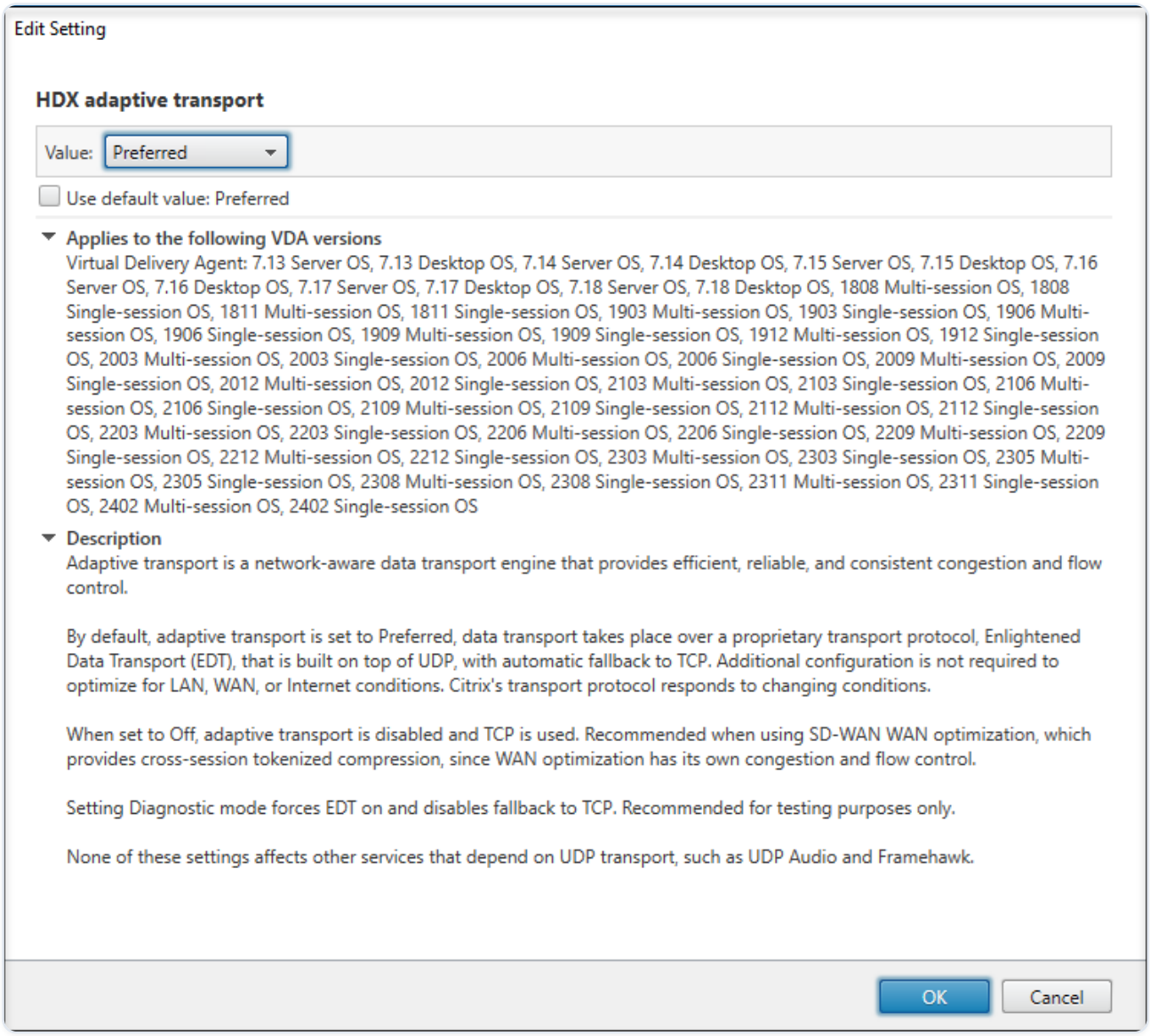
El transporte adaptativo es un mecanismo en Citrix Virtual Apps and Desktops™ que puede usar Enlightened Data Transport (EDT) como protocolo de transporte para las conexiones ICA. El transporte adaptativo cambia a TCP cuando EDT no está disponible.

EDT es un protocolo de transporte propietario de Citrix basado en el Protocolo de datagramas de usuario (UDP). Ofrece una experiencia de usuario superior en conexiones de larga distancia desafiantes, al tiempo que mantiene la escalabilidad del servidor. EDT mejora el rendimiento de los datos para todos los canales virtuales ICA® en redes poco fiables, lo que proporciona una experiencia de usuario mejor y más consistente.

Para obtener más información, consulte Transporte adaptativo en la documentación de Citrix Virtual Apps and Desktops.

Habilitar o deshabilitar el transporte adaptativo

El transporte adaptativo está habilitado de forma predeterminada. Puede configurar las siguientes opciones mediante la configuración de directiva **HDX™ Adaptive Transport**:



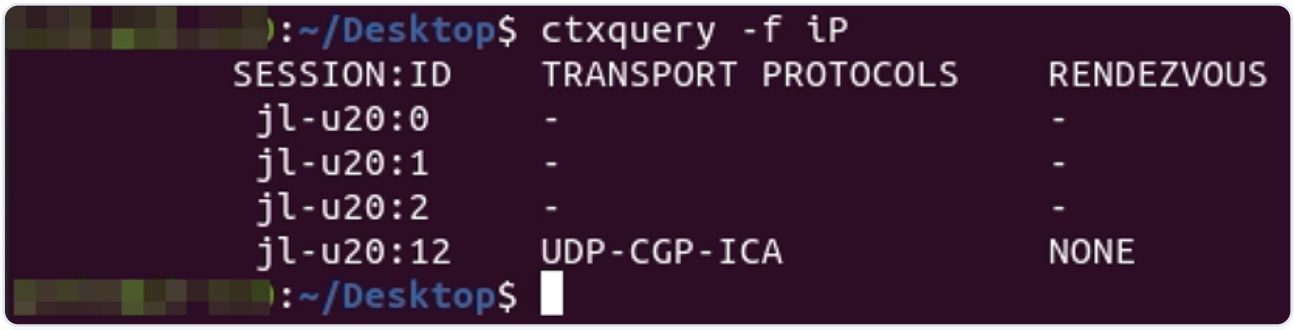
- **Preferido**: El transporte adaptativo está habilitado y utiliza Enlightened Data Transport (EDT) como protocolo de transporte preferido, con reserva a TCP.
- **Modo de diagnóstico**: El transporte adaptativo está habilitado y fuerza el uso de EDT. La reserva a TCP está deshabilitada. Esta configuración se recomienda solo para pruebas y solución de problemas.
- **Desactivado**. El transporte adaptativo está deshabilitado y solo se utiliza TCP para el transporte.

Comprobar si se está utilizando el transporte adaptativo

Para comprobar si se está utilizando EDT como protocolo de transporte para la sesión actual, ejecute el siguiente comando.

```
/opt/Citrix/VDA/bin/ctxquery -f iP
```

Si se está utilizando EDT, los protocolos de transporte mostrados incluyen UDP, por ejemplo:



Detección de MTU de EDT

La detección de MTU permite a EDT determinar automáticamente la Unidad de transmisión máxima (MTU) al establecer una sesión. Esto evita la fragmentación de paquetes EDT que podría provocar una degradación del rendimiento o un fallo al establecer una sesión.

Requisitos del sistema:

- Linux VDA versión mínima 2012
- Aplicación Citrix Workspace™:
  - Windows: 1911 o posterior
- Citrix ADC:
  - 13.0.52.24 o posterior
  - 12.1.56.22 o posterior
- La fiabilidad de la sesión debe estar habilitada

Si utiliza plataformas o versiones de cliente que no admiten esta función, consulte CTX231821 para obtener detalles sobre cómo configurar una MTU de EDT personalizada que sea adecuada para su entorno.

Controlar la detección de MTU de EDT en el VDA

La detección de MTU de EDT está habilitada en el VDA de forma predeterminada. Puede habilitarla o deshabilitarla configurando la clave del Registro `MtuDiscovery` de la siguiente manera:

- Para habilitar la detección de MTU de EDT, configure la clave del Registro `MtuDiscovery` con el siguiente comando, reinicie el VDA y espere a que el VDA se registre:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd" -t
"REG_DWORD" -v "MtuDiscovery" -d "0x00000001" --force
```

- Para inhabilitar la detección de MTU de EDT, elimine el valor del Registro `MtuDiscovery`.

Advertencia:

La modificación incorrecta del Registro puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas resultantes del uso incorrecto del **Editor del Registro** puedan resolverse. Utilice el **Editor del Registro** bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de modificarlo.

Controlar la detección de MTU de EDT en el cliente

Puede controlar la detección de MTU de EDT de forma selectiva en el cliente agregando el parámetro `MtuDiscovery` en el archivo ICA. Para inhabilitar la función, configure lo siguiente en la sección `Application`:

`MtuDiscovery=Off`

Para volver a habilitar la función, elimine el parámetro `MtuDiscovery` del archivo ICA.

Importante:

Para que este parámetro del archivo ICA funcione, habilite la detección de MTU de EDT en el VDA. Si la detección de MTU de EDT no está habilitada en el VDA, el parámetro del archivo ICA no tiene ningún efecto.

Control de congestión de EDT mejorado

Se introduce un algoritmo de control de congestión para optimizar el protocolo EDT. Esta implementación permite a EDT lograr un mayor rendimiento y reducir la latencia para una experiencia de usuario mejorada.

Esta función está habilitada de forma predeterminada. Para deshabilitarla y volver a habilitarla, ejecute los siguientes comandos, respectivamente, y luego reinicie el servicio `ctxhdx`:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Terminal
Server\Wds\icawd\Tds\udp\UDPStackParameters" -t "REG_DWORD" -v "edtBBR" -d
"0x00000000" --force
```

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Terminal
Server\Wds\icawd\Tds\udp\UDPStackParameters" -t "REG_DWORD" -v "edtBBR" -d
"0x00000001" --force
```

Rendimiento adaptativo de HDX™

El rendimiento adaptativo de HDX ajusta de forma inteligente el rendimiento máximo de las sesiones ICA® mediante la adaptación de los búferes de salida. El número de búferes de salida se establece inicialmente en un valor alto. Este valor alto permite que los datos se transmitan al cliente de forma más rápida y eficiente, especialmente en redes de alta latencia. Esta función mejora la experiencia del usuario. Ofrece una mejor interactividad, transferencias de archivos más rápidas, una reproducción de vídeo más fluida y una mayor velocidad de fotogramas y resolución. La interactividad de la sesión se mide constantemente para determinar si algún flujo de datos dentro de una sesión ICA afecta negativamente a la interactividad. Si esto ocurre, el rendimiento se reduce para disminuir el impacto del gran flujo de datos en la sesión y permitir que la interactividad se recupere.

Importante:

El rendimiento adaptativo de HDX cambia la forma de configurar los búferes de salida al mover el mecanismo del cliente al VDA. No es necesaria ninguna configuración manual.

La función requiere la versión mínima 2311 del VDA. Está habilitada de forma predeterminada. Si está deshabilitada, puede habilitarla ejecutando el siguiente comando en el VDA:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd" -t
"REG_DWORD" -v "AdaptiveScalingEnabled" -d "0x00000001" --force
```

> La función se aplica solo a las sesiones que se inician después de habilitar la función.

HDX™ Direct para Linux

Al acceder a los recursos proporcionados por Citrix, HDX Direct permite que tanto los dispositivos cliente internos como los externos establezcan una conexión directa segura con el host de sesión si la comunicación directa es posible.

Requisitos del sistema

Los siguientes son los requisitos del sistema para usar HDX Direct:

- Plano de control
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 o posterior
- Virtual Delivery Agent (VDA)
  - Linux: Versión 2503 o posterior
- Aplicación Workspace
  - Windows: versión 2503 o posterior
  - Linux: versión 2411 o posterior
  - Mac: versión 2411 o posterior
- Nivel de acceso
  - Citrix Workspace™
  - Citrix StoreFront™ 2503 o posterior
  - Citrix Gateway Service
  - Citrix NetScaler® Gateway

Requisitos de red

Los siguientes son los requisitos de red para usar HDX Direct.

Hosts de sesión

Si sus hosts de sesión tienen un firewall, debe permitir el siguiente tráfico entrante para las conexiones internas.

DESCRIPCIÓN	ORIGEN	PROTOCOLO	PUERTO
Conexión interna directa	Cliente	TCP	443
Conexión interna directa	Cliente	UDP	443

Red del cliente

La siguiente tabla describe la red del cliente para usuarios internos y externos.

USUARIOS INTERNOS

DESCRIPCIÓN	PROTOCOLO	ORIGEN	PUERTO DE ORIGEN	DESTINO	PUERTO DE DESTINO
Conexión interna directa	TCP	Red del cliente	1024–65535	Red VDA	443
Conexión interna directa	UDP	Red del cliente	1024–65535	Red VDA	443

USUARIOS EXTERNOS

DESCRIPCIÓN	PROTOCOLO	ORIGEN	PUERTO DE ORIGEN	DESTINO	PUERTO DE DESTINO
STUN (solo usuarios externos)	UDP	Red del cliente	1024–65535	Internet (consulte la nota a continuación)	3478, 19302
Conexión de usuario externo	UDP	Red del cliente	1024–65535	Dirección IP pública del centro de datos	1024–65535

Red del centro de datos

La siguiente tabla describe la red del centro de datos para usuarios internos y externos.

USUARIOS INTERNOS

DESCRIPCIÓN	PROTOCOLO	ORIGEN	PUERTO DE ORIGEN	DESTINO	PUERTO DE DESTINO
Conexión interna directa	TCP	Red del cliente	1024–65535	Red VDA	443
Conexión interna directa	UDP	Red del cliente	1024–65535	Red VDA	443

USUARIOS EXTERNOS

DESCRIPCIÓN	PROTOCOLO	ORIGEN	PUERTO DE ORIGEN	DESTINO	PUERTO DE DESTINO
STUN (solo usuarios externos)	UDP	Red VDA	1024–65535	Internet (consulte la nota a continuación)	3478, 19302
Conexión de usuario externo	UDP	DMZ / Red interna	1024–65535	Red VDA	55000–55250
Conexión de usuario externo	UDP	Red VDA	55000–55250	IP pública del cliente	1024–65535

Nota:

Tanto el VDA como la aplicación Workspace intentan enviar solicitudes STUN a los siguientes servidores en el mismo orden:

- stun.cloud.com:3478
- stun.cloudflare.com:3478

- stun.l.google.com:19302

> Si cambia el rango de puertos predeterminado para las conexiones de usuarios externos mediante la configuración de directiva **Rango de puertos de HDX Direct**, las reglas de firewall correspondientes deben coincidir con su rango de puertos personalizado.

Configuración

HDX Direct está deshabilitado de forma predeterminada. Puede configurar esta función mediante la configuración **HDX Direct** en la directiva de Citrix.

- **HDX Direct**: Para habilitar o deshabilitar una función.
- **Modo HDX Direct**: Determina si **HDX Direct** está disponible solo para clientes internos o para clientes internos y externos.
- **Rango de puertos de HDX Direct**: Define el rango de puertos que utiliza el VDA para las conexiones de clientes externos.

Consideraciones

Las siguientes son consideraciones para usar HDX Direct:

- HDX Direct para usuarios externos solo está disponible con EDT (UDP) como protocolo de transporte. Por lo tanto, **Transporte adaptable** debe estar habilitado.
- Si utiliza **HDX Insight**, tenga en cuenta que el uso de **HDX Direct** impide la recopilación de datos de HDX Insight, ya que la sesión ya no se enviaría a través de NetScaler Gateway.
- El uso de sus propios certificados con HDX Direct no es compatible actualmente.

Cómo funciona

HDX Direct permite a los clientes establecer una conexión directa con el host de sesión cuando la comunicación directa está disponible. Cuando se realizan conexiones directas mediante HDX Direct, se utilizan certificados autofirmados para proteger la conexión directa con cifrado a nivel de red (TLS/DTLS).

Usuarios internos

El siguiente diagrama muestra la descripción general del proceso de conexión directa de HDX para usuarios internos.



1. El cliente establece una sesión HDX a través del Servicio Gateway.
2. Tras una conexión correcta, el VDA envía al cliente el FQDN de la máquina VDA, una lista de sus direcciones IP y el certificado de la máquina VDA a través de la conexión HDX.
3. El cliente sondea las direcciones IP para ver si puede llegar al VDA directamente.
4. Si el cliente puede llegar al VDA directamente con cualquiera de las direcciones IP compartidas, el cliente establece una conexión directa con el VDA, protegida con (D)TLS mediante un certificado que coincide con el intercambiado en el paso (2).
5. Una vez establecida correctamente la conexión directa, la sesión se transfiere a la nueva conexión y la conexión al Servicio Gateway finaliza.

> **Nota:**
>
> Después de establecer la conexión en el paso 2 anterior, la sesión está activa. Los pasos posteriores no retrasan ni interfieren con la capacidad del usuario para usar la aplicación o el escritorio virtual. Si alguno de los pasos posteriores falla, la conexión a través de Gateway se mantiene sin interrumpir la sesión del usuario.

Usuarios externos

El siguiente diagrama muestra la descripción general del proceso de conexión directa de HDX para usuarios externos:



1. El cliente establece una sesión HDX a través del Servicio Gateway.
2. Tras una conexión exitosa, tanto el cliente como el VDA envían una solicitud STUN para descubrir sus direcciones IP públicas y puertos.
3. El servidor STUN responde al cliente y al VDA con sus correspondientes direcciones IP públicas y puertos.
4. A través de la conexión HDX, el cliente y el VDA intercambian sus direcciones IP públicas y puertos UDP, y el VDA envía su certificado al cliente.
5. El VDA envía paquetes UDP a la dirección IP pública y al puerto UDP del cliente. El cliente envía paquetes UDP a la dirección IP pública y al puerto UDP del VDA.
6. Al recibir un mensaje del VDA, el cliente responde con una solicitud de conexión segura.

7. Durante el protocolo de enlace DTLS, el cliente verifica que el certificado coincide con el certificado intercambiado en el paso 4. Después de la validación, el cliente envía su token de autorización. Ahora se establece una conexión directa segura.
8. Una vez establecida correctamente la conexión directa, la sesión se transfiere a la nueva conexión y la conexión al Servicio Gateway finaliza.

> **Nota:**
>
> Después de establecer la conexión en el paso 2 anterior, la sesión está activa. Los pasos posteriores no retrasan ni interfieren con la capacidad del usuario para usar la aplicación o el escritorio virtual. Si alguno de los pasos posteriores falla, la conexión a través de Gateway se mantiene sin interrumpir la sesión del usuario.

Compatibilidad con NAT

Para establecer una conexión directa entre un dispositivo de usuario externo y el host de sesión, HDX Direct aprovecha el hole punching para el recorrido NAT y STUN para facilitar el intercambio de la dirección IP pública y las asignaciones de puertos para el dispositivo cliente y el host de sesión. Esto es similar a cómo funcionan las soluciones de VoIP, comunicaciones unificadas y P2P.

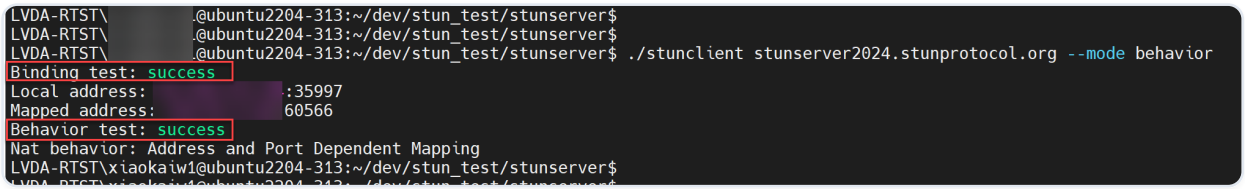
Siempre que los firewalls y otros componentes de red estén configurados para permitir el tráfico UDP para las solicitudes STUN y las sesiones HDX, se espera que HDX Direct funcione para usuarios externos. Sin embargo, hay ciertos escenarios en los que los tipos de NAT de las redes del usuario y del host de sesión conducen a una combinación incompatible, lo que provoca que HDX Direct falle.

Validaciones

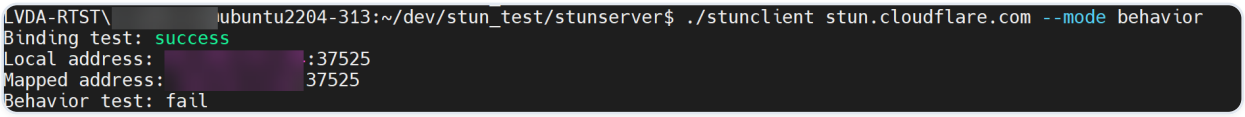
Puede validar el tipo y el filtrado de NAT en el cliente y el host de sesión utilizando la utilidad de cliente STUN de STUNTMAN:

1. Descargue el paquete adecuado para la plataforma de destino desde stunprotocol.org, y extraiga el contenido.
2. Abra una ventana de terminal y navegue hasta el directorio donde se extrajo el contenido.
3. Ejecute el siguiente comando: `./stunclient stunserver2024.stunprotocol.org --mode behavior`
4. Tome nota de la salida.

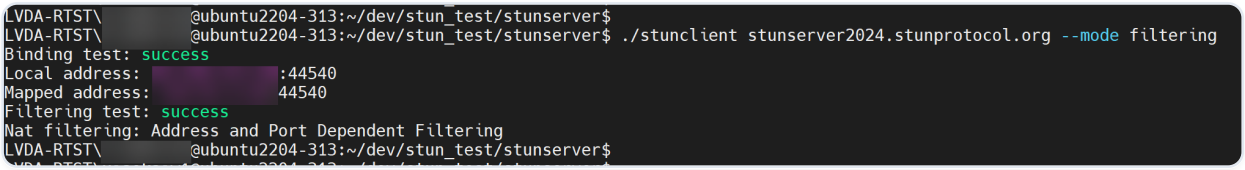
Si las pruebas de enlace y comportamiento son correctas, tanto la **prueba de enlace** como la **prueba de comportamiento** informan del éxito y se especifica un comportamiento NAT:



Si las pruebas fallan, la **prueba de enlace** y/o la **prueba de comportamiento** informan del fallo.



5. Ejecute el siguiente comando: `./stunclient stunserver2024.stunprotocol.org --mode filtering`
6. Tome nota de la salida.



Consulte la siguiente tabla para determinar si se espera que HDX Direct para usuarios externos funcione según los resultados de las pruebas tanto del cliente como del host de sesión:

COMPORTAMIENTO NAT DEL CLIENTE	FILTRADO NAT DEL CLIENTE	COMPORTAMIENTO NAT DEL HOST DE SESIÓN	FILTRADO NAT DEL HOST DE SESIÓN	¿SE ESPERA QUE FUNCIONE?
Asignación independiente de punto final	Cualquiera	Asignación independiente de punto final	Cualquiera	Sí
Asignación independiente de punto final	Filtrado independiente de punto final	Asignación dependiente de la dirección	Cualquiera	Sí
Asignación independiente de punto final	Filtrado dependiente de la dirección	Asignación dependiente de la dirección	Cualquiera	No

COMPORTAMIENTO NAT DEL CLIENTE	FILTRADO NAT DEL CLIENTE	COMPORTAMIENTO NAT DEL HOST DE SESIÓN	FILTRADO NAT DEL HOST DE SESIÓN	¿SE ESPERA QUE FUNCIONE?
Asignación independiente de punto final	Filtrado dependiente de la dirección y el puerto	Asignación dependiente de la dirección	Cualquiera	No
Asignación independiente de punto final	Filtrado independiente de punto final	Asignación dependiente de la dirección y el puerto	Filtrado independiente de punto final	Sí
Asignación independiente de punto final	Filtrado dependiente de la dirección	Asignación dependiente de la dirección	Cualquiera	No
Asignación independiente de punto final	Filtrado dependiente de la dirección y el puerto	Asignación dependiente de la dirección	Cualquiera	No
Asignación dependiente de la dirección	Cualquiera	Asignación independiente de punto final	Filtrado independiente de punto final	Sí
Asignación dependiente de la dirección	Cualquiera	Asignación independiente de punto final	Filtrado dependiente de la dirección	No
Asignación dependiente de la dirección	Cualquiera	Asignación independiente de punto final	Filtrado dependiente de la dirección y el puerto	No
Asignación dependiente de la dirección	Cualquiera	Asignación dependiente de la dirección	Cualquiera	No

COMPORTAMIENTO NAT DEL CLIENTE	FILTRADO NAT DEL CLIENTE	COMPORTAMIENTO NAT DEL HOST DE SESIÓN	FILTRADO NAT DEL HOST DE SESIÓN	¿SE ESPERA QUE FUNCIONE?
Asignación dependiente de la dirección	Cualquiera	Asignación dependiente de la dirección y el puerto	Cualquiera	No
Asignación dependiente de la dirección y el puerto	Cualquiera	Asignación independiente de punto final	Filtrado independiente de punto final	Sí
Asignación dependiente de la dirección y el puerto	Cualquiera	Asignación independiente de punto final	Filtrado dependiente de la dirección	No
Asignación dependiente de la dirección y el puerto	Cualquiera	Asignación independiente de punto final	Filtrado dependiente de la dirección y el puerto	No
Asignación dependiente de la dirección y el puerto	Cualquiera	Asignación dependiente de la dirección	Cualquiera	No
Asignación dependiente de la dirección y el puerto	Cualquiera	Asignación dependiente de la dirección y el puerto	Cualquiera	No
Fallo	Cualquiera	Cualquiera	Cualquiera	No
Cualquiera	Cualquiera	Fallo	Cualquiera	No
Fallo	Cualquiera	Fallo	Cualquiera	No

Fondos personalizados y mensajes de banner en las pantallas de inicio de sesión de la sesión

Añadir un fondo personalizado o un mensaje de banner a las pantallas de inicio de sesión de la sesión

> **Sugerencia:**

> Para usar la función en SUSE 15.6, instale `imlib2` desde `<http://download.opensuse.org/distribution/leap/15.3/repo/oss/>`.

> Puede usar los siguientes comandos para añadir un fondo personalizado o un mensaje de banner a las pantallas de **inicio de sesión** de la sesión. Para añadir un fondo y un mensaje de banner a las pantallas de **inicio de sesión** de la sesión, puede incrustar el mensaje de banner en la imagen de fondo. Después de abrir una sesión, primero se muestra la página del mensaje de banner y luego aparece el cuadro de diálogo de autenticación.

Para establecer el título de un mensaje de banner personalizado, ejecute:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
"LogonDisplayStringTitle" -d "<Banner message title>" --force
```

La longitud máxima del título de un mensaje de banner es de 64 bytes.

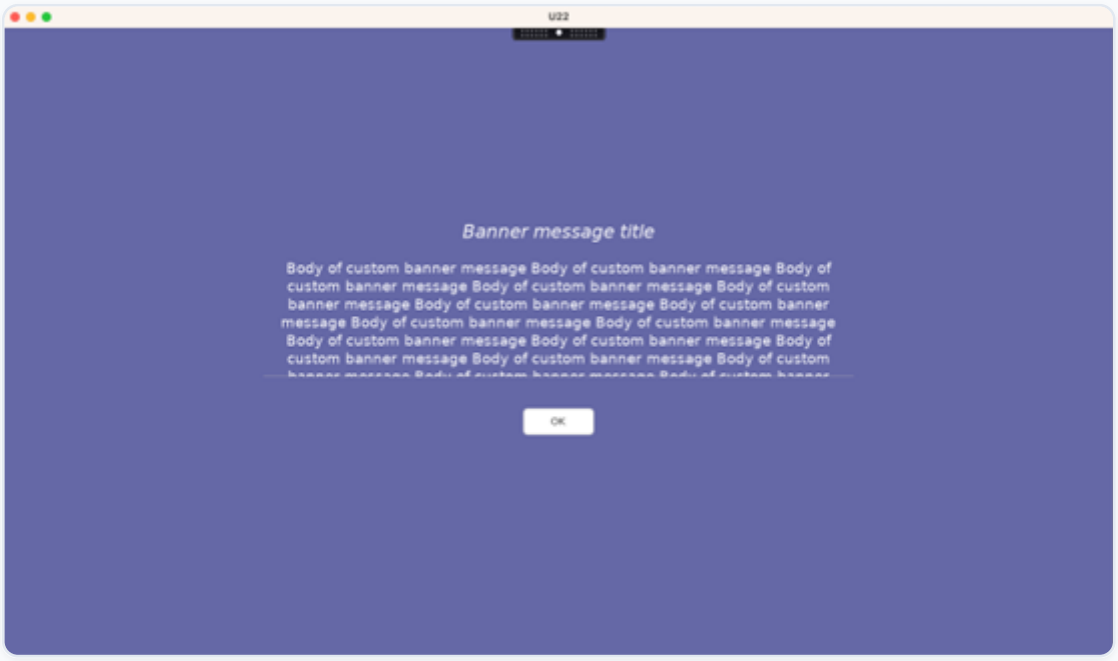
Para establecer el texto del cuerpo de un mensaje de banner personalizado, ejecute:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
"LogonDisplayString" -d "Body of custom banner message\nBody of custom
banner message\nBody of custom banner message\n" --force
```

La longitud máxima del cuerpo de un mensaje de banner es de 1024 bytes.

> **Sugerencia:**

El elemento `\n` crea un salto de línea. En este ejemplo, la pantalla del mensaje de banner tiene este aspecto:



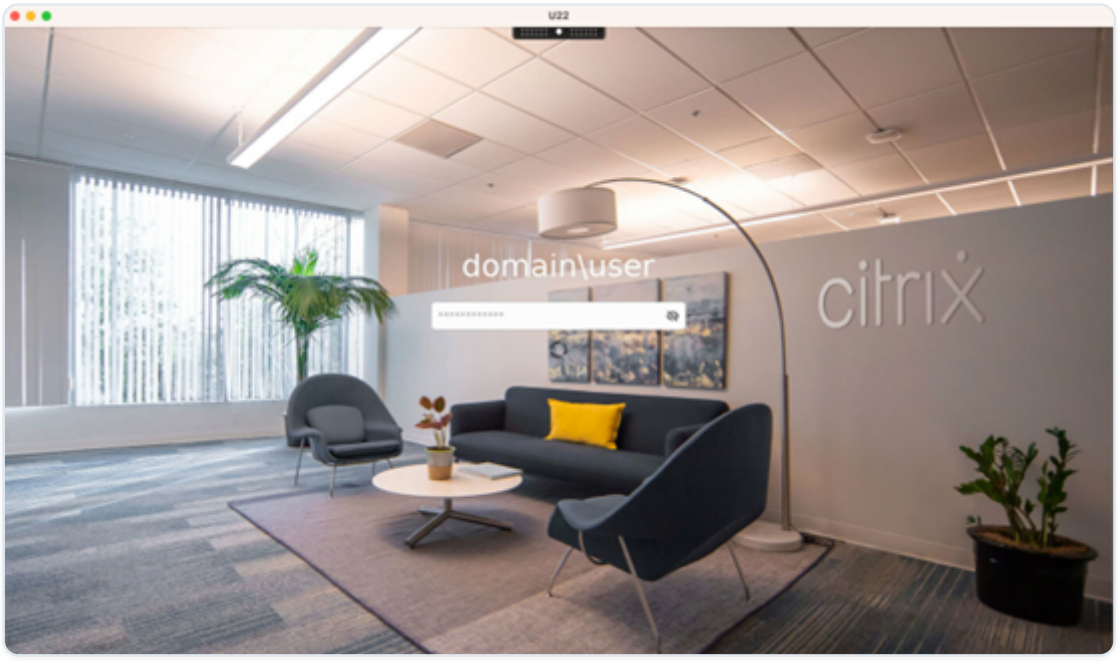
Para asegurarse de que el mensaje de banner personalizado se muestre como se espera, es posible que deba usar caracteres de escape. Por ejemplo, use **&amp\;** para representar **&** en HTML y coloque una barra invertida (****) antes del carácter **\!** para escaparlo en los comandos de Bash.

Para añadir un fondo personalizado a las pantallas de **inicio de sesión** de la sesión, ejecute:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
"BackgroundImagePath" -d "<path to the background image>" --force
```

Para ver el fondo personalizado, los usuarios de la sesión deben tener acceso a la ruta de la imagen de fondo.

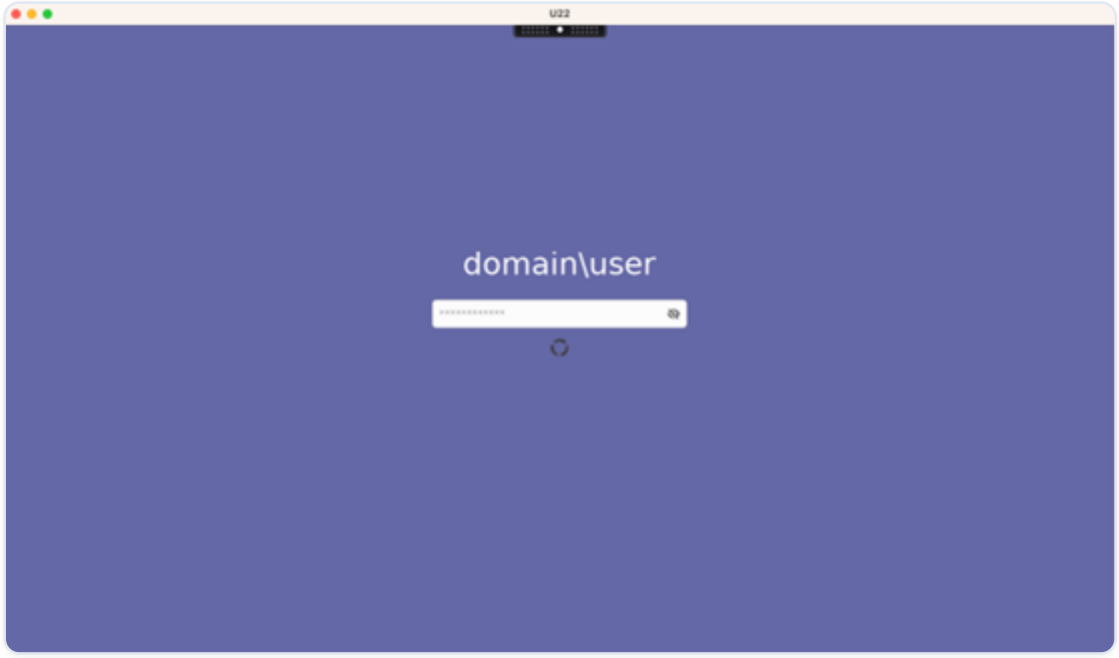
Por ejemplo:



Ejemplo de pantallas de inicio de sesión de la sesión

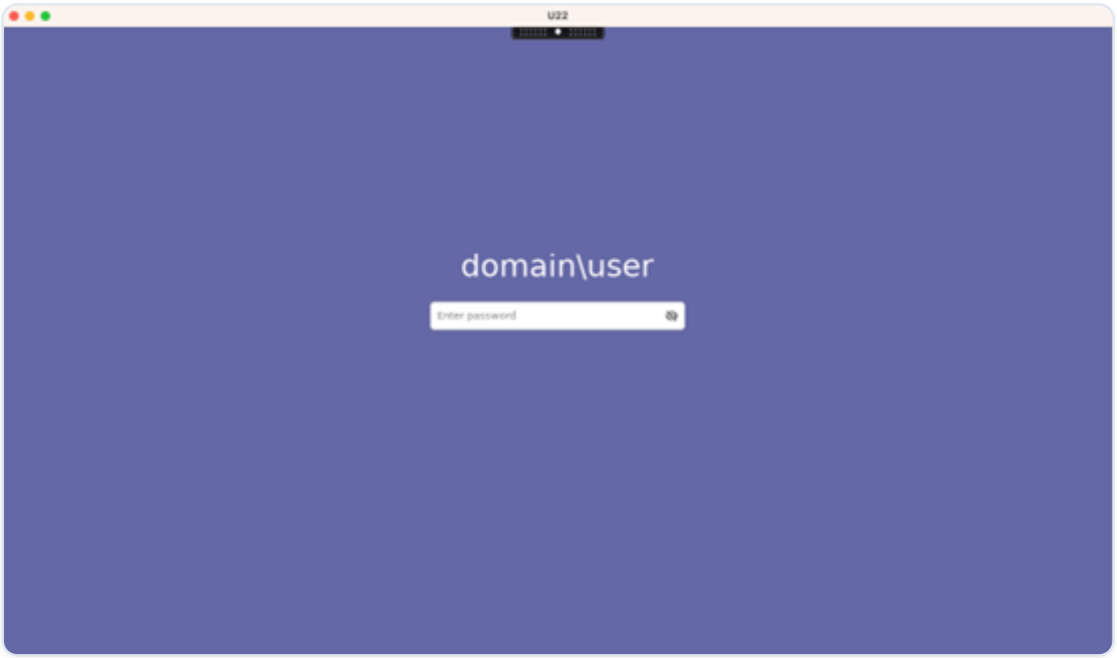
A continuación se muestran ejemplos de pantallas de inicio de sesión en diferentes escenarios:

- Inicio de **sesión** en escenarios de inicio de sesión único (SSO):

  Se muestra el proceso de **inicio de sesión**.

- Inicio de **sesión** en escenarios típicos sin SSO:



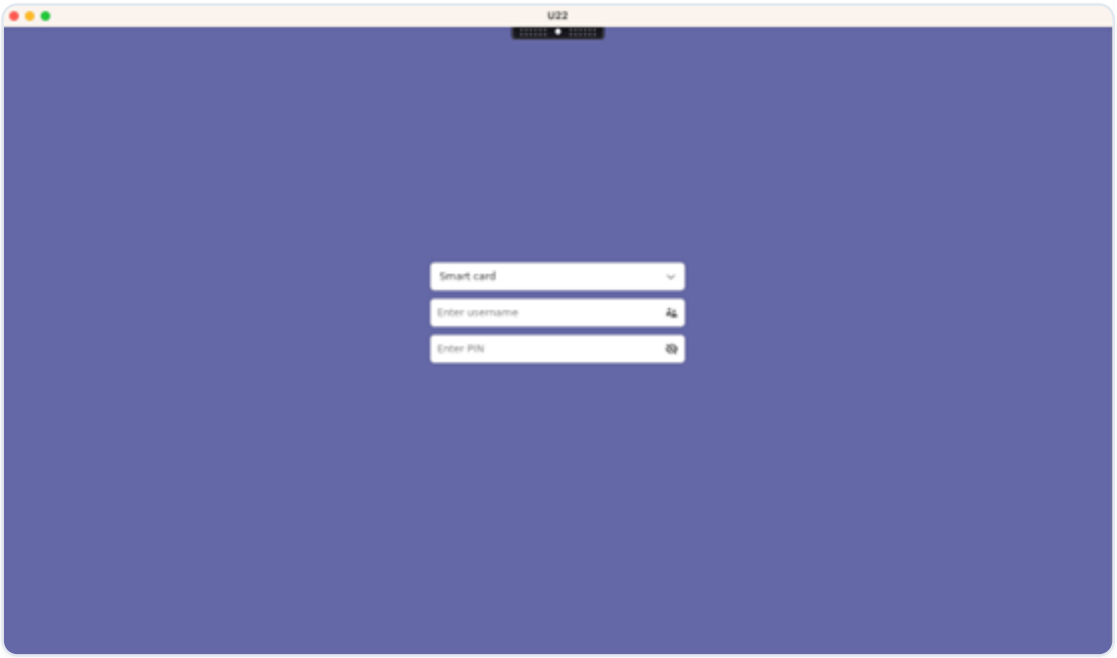
  - Se requiere una contraseña o un código PIN en escenarios sin SSO.
  - Los usuarios pueden alternar la visibilidad de las contraseñas y los códigos PIN, lo que facilita la detección de entradas incorrectas.

- Inicio de sesión en escenarios sin SSO cuando los usuarios inician sesión en sesiones VDA con credenciales diferentes a las utilizadas para iniciar sesión en la aplicación Citrix Workspace™:

  Nombre de usuario y contraseña utilizados para el inicio de sesión:



  Tarjeta inteligente utilizada para el inicio de sesión:



Para conocer las combinaciones de métodos de autenticación de usuario compatibles en escenarios sin SSO, consulte Autenticación sin SSO.

Tiempo de espera configurable para la visualización del banner de inicio de sesión

Para establecer un valor de tiempo de espera personalizado (en segundos), utilice el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v
"LogonDisplayTimeoutS" -d "<timeout_value>" --force
```

Parámetros

- Un valor de 0 deshabilita el tiempo de espera, lo que requiere la interacción del usuario para continuar.
- Cualquier valor distinto de cero especifica la duración del tiempo de espera en segundos. Rango válido: **1–1800 segundos**.
- El valor predeterminado es **60 segundos**.

Entornos de escritorio personalizados por usuarios de sesión

Puede especificar un entorno de escritorio para los usuarios de sesión mediante la variable **CTX_XDL_DESKTOP_ENVIRONMENT**. A partir de la versión 2209, los usuarios de sesión

pueden personalizar sus propios entornos de escritorio. Para permitir que los usuarios de sesión utilicen esta función, debe instalar los entornos de escritorio en el VDA con antelación.

La siguiente tabla muestra una matriz de las distribuciones de Linux y los entornos de escritorio que admiten entornos de escritorio personalizados por usuarios de sesión.

DISTRIBUCIÓN DE LINUX	ESCRITORIO COMPATIBLE
Debian 12.15	MATE, GNOME, GNOME-Classic, KDE, Xfce
Debian 11.11	MATE, GNOME, GNOME-Classic, KDE
RHEL 9.8/9.6/9.4	MATE, GNOME, Xfce
RHEL 8.10	MATE, GNOME, GNOME-Classic, Xfce
Rocky Linux 9.8/9.6/9.4	MATE, GNOME, Xfce
Rocky Linux 8.10	MATE, GNOME, GNOME-Classic, KDE, Xfce
SUSE 15.6	MATE, GNOME, GNOME-Classic
Ubuntu 22.04	MATE, GNOME, GNOME-Classic, KDE, Xfce
Ubuntu 24.04	MATE, KDE, Xfce

Comandos para cambiar de escritorio

> **Nota:**

> Puede cambiar entre entornos de escritorio tanto desde el Terminal como desde la bandeja del sistema.

> Para cambiar a un entorno de escritorio de destino desde el Terminal, ejecute el comando correspondiente dentro de la sesión:

SI EL ENTORNO DE ESCRITORIO DE DESTINO ES	EJECUTE EL COMANDO
GNOME	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME`
GNOME Classic	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC`
MATE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE`
KDE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE`

Consejos de KDE

- Magnus podría cargarse al inicio en KDE. Como solución alternativa, puede eliminar el paquete Magnus ejecutando `sudo apt remove magnus`.
- Para deshabilitar las advertencias de QT que aparecen durante el inicio de KDE, edite `/usr/share/qt5/qtlogging.ini` como usuario root añadiendo las siguientes entradas:

```
qt.qpa.xcb.xcberror.error=false

qt.qpa.xcb.warning=false

qt.qpa.xcb.error=false
```

- El desbloqueo de pantalla podría fallar en KDE. Como solución alternativa, le recomendamos que deshabilite la función de bloqueo automático de su escritorio.

Inicio de sesión con un directorio personal temporal

Puede especificar un directorio personal temporal para los casos en que el punto de montaje en el VDA de Linux falle. Si se especifica un directorio personal temporal, aparece un mensaje durante el inicio de sesión cuando el punto de montaje falla. Los datos del usuario se almacenan entonces en el directorio personal temporal.

La siguiente tabla describe las claves del Registro que le ayudan con la configuración de su directorio personal.

CLAVE DEL REGISTRO	DESCRIPCIÓN	COMANDO
`LogNoHome`	Controla si los usuarios pueden iniciar sesión sin un directorio personal. El valor predeterminado es 1, lo que significa sí. Si el valor se establece en 0, los inicios de sesión sin un directorio personal están inhabilitados.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "LogNoHome" -d "0x00000001" --force`
`HomeMountPoint`	Establece un punto de montaje local en el VDA de Linux. Por ejemplo, si `/mnt/home` es el punto de montaje, el directorio personal de un usuario es `/mnt/home/domain/<user_name>`. Asegúrese de que el punto de montaje sea el mismo que el directorio personal del usuario en su entorno. Esta configuración solo surte efecto cuando `CheckUserHomeMountPoint` se establece en 0.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "HomeMountPoint" -d "<A directory where the NFS share is to be mounted>" --force`
`CheckUserHomeMountPoint`	Controla si se deben establecer directorios personales específicos del usuario como punto de montaje en el VDA de Linux. Si quiere establecer directorios personales específicos del usuario como punto de montaje, establezca el valor en **1**. El valor predeterminado es **0**.	`ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "CheckUserHomeMountPoint" -d "0x00000001" --force`
`TempHomeDirectoryPath`	Establece un directorio personal temporal en el VDA de Linux en caso de que el punto de montaje falle. El	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v`

CLAVE DEL REGISTRO	DESCRIPCIÓN	COMANDO
	valor predeterminado es `/tmp`. La configuración del directorio personal temporal solo surte efecto cuando el punto de montaje determinado por `HomeMountPoint` y `CheckUserHomeMountPoint` no está disponible. Un directorio personal temporal para un usuario es `/tmp/CTXSmf_user_id`.	`"TempHomeDirectoryPath" -d "</tmp by default>" --force`
`CheckMountPointRetryTime`	Establece el número de comprobaciones, con una frecuencia de una vez por segundo, sobre si el montaje se ha realizado correctamente. El valor predeterminado es 5.	`ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "CheckMountPointRetryTime" -d "0x000000010" --force`
`RemoveHomeOnLogoff`	Controla si se deben eliminar los directorios personales temporales al cerrar la sesión el usuario. 1 significa sí. 0 significa no.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "RemoveHomeOnLogoff" -d "0x00000000" --force`

Publicar aplicaciones

Con Linux VDA versión 7.13, Citrix añadió la función de aplicaciones fluidas a todas las plataformas Linux compatibles. No se requieren procedimientos de instalación específicos para usar esta función.

> **Sugerencia:**

> Con Linux VDA versión 1.4, Citrix añadió compatibilidad con aplicaciones publicadas no fluidas y uso compartido de sesiones.

Publicar aplicaciones con Citrix Studio

Puede publicar aplicaciones instaladas en un VDA de Linux al crear un grupo de entrega o al agregar aplicaciones a un grupo de entrega existente. El proceso es similar a la publicación de aplicaciones instaladas en un VDA de Windows. Para obtener más información, consulte la documentación de Citrix Virtual Apps and Desktops (según la versión de Citrix Virtual Apps and Desktops que se utilice).

Nota:

- Al configurar grupos de entrega, asegúrese de que el tipo de entrega esté establecido en **Escritorio y aplicaciones** o **Aplicaciones**.
- Recomendamos crear VDA y grupos de entrega separados para las entregas de aplicaciones y escritorios.
- Para usar aplicaciones fluidas, no inhabilite el modo fluido en StoreFront. El modo fluido está habilitado de forma predeterminada. Si ya lo ha inhabilitado configurando "TWIMode=Off", quite esta configuración en lugar de cambiarla a "TWIMode=On". De lo contrario, es posible que no pueda iniciar un escritorio publicado.

Limitación

El VDA de Linux no admite el inicio de varias instancias simultáneas de la misma aplicación por parte de un único usuario.

En una sesión de aplicación, solo los accesos directos específicos de la aplicación funcionan como se espera.

Problemas conocidos

Se han identificado los siguientes problemas conocidos al publicar aplicaciones:

- Las ventanas no rectangulares no son compatibles. Las esquinas de una ventana pueden mostrar el fondo del lado del servidor.
- La vista previa del contenido de una ventana de una aplicación publicada no es compatible.
- Cuando se ejecutan varias aplicaciones de LibreOffice, solo la que se inició primero se muestra en Citrix Studio porque estas aplicaciones comparten el proceso.

- Es posible que las aplicaciones publicadas basadas en Qt5, como "Dolphin", no muestren iconos. Para resolver el problema, consulte el artículo en `<https://wiki.archlinux.org/title/Qt>`.
- Las aplicaciones de Linux a menudo tienen una ventana Acerca de que contiene información sobre la aplicación en uso, y los enlaces web para obtener más información se encuentran comúnmente en esas ventanas. Al hacer clic en los enlaces web de la ventana Acerca de, se puede iniciar un navegador web desde dentro de aplicaciones publicadas como **calc**, **gedit**, **calendar** y **LibreOffice Suite**. El inicio involuntario de un navegador web omite el aislamiento de la aplicación y puede comprometer la seguridad. Para solucionar el problema, cambie el navegador web predeterminado siguiendo estos pasos:

  a. Cree un archivo none.sh en una ubicación personalizada, por ejemplo:

  ```
  sudo mkdir /home/none


  sudo touch /home/none/none.sh


  sudo chmod +x /home/none/none.sh
  ```

  b. Agregue las siguientes líneas al archivo none.sh:

  ```
  #!/bin/bash


  echo "NONE"
  ```

  c. Cree el archivo /etc/xdg/mimeapps.list con sudo y, a continuación, agregue las siguientes líneas al archivo mimeapps.list:

  ```
  [Default Applications]


  text/html=none.desktop
  ```

```
x-scheme-handler/http=none.desktop

x-scheme-handler/https=none.desktop

x-scheme-handler/about=none.desktop

x-scheme-handler/unknown=none.desktop
```

d. Cree el archivo /usr/share/applications/none.desktop con sudo y, a continuación, agregue las siguientes líneas al archivo none.desktop:

```
[Desktop Entry]

Encoding=UTF-8

Version=1.0

Type=Application

Terminal=false

Exec=/home/none/none.sh
```

```
Name=None


Icon=/home/none/none.sh
```

Dado que puede colocar el archivo none.sh en una ubicación personalizada, asegúrese de que none.desktop pueda hacer referencia al archivo none.sh correctamente.

Rendezvous V1

Cuando se utiliza el servicio Citrix Gateway, el protocolo Rendezvous permite que el tráfico omita los Citrix Cloud™ Connectors y se conecte de forma directa y segura con el plano de control de Citrix Cloud.

Hay dos tipos de tráfico a considerar: 1) tráfico de control para el registro de VDA y la intermediación de sesiones; 2) tráfico de sesión HDX™.

Rendezvous V1 permite que el tráfico de sesión HDX omita los Cloud Connectors, pero aún requiere que los Cloud Connectors actúen como proxy para todo el tráfico de control para el registro de VDA y la intermediación de sesiones.

Requisitos

- Acceso al entorno mediante Citrix Workspace™ y el servicio Citrix Gateway.
- Plano de control: Citrix DaaS (anteriormente servicio Citrix Virtual Apps and Desktops™).
- Linux VDA versión 2112 o posterior.
  - La versión 2112 es la mínima requerida para los proxies HTTP no transparentes.
  - La versión 2204 es la mínima requerida para los proxies transparentes y SOCKS5.
- Habilite el protocolo Rendezvous en la directiva de Citrix. Para obtener más información, consulte Configuración de directiva del protocolo Rendezvous.
- Los VDA deben tener acceso a `https://*.nssvc.net`, incluidos todos los subdominios. Si no puede agregar todos los subdominios a la lista de permitidos de esa manera, use `https://*.c.nssvc.net` y `https://*.g.nssvc.net` en su lugar. Para obtener más información, consulte la sección Requisitos de conectividad a Internet de la documentación de Citrix Cloud (en el servicio Virtual Apps and Desktop) y el artículo del Centro de conocimientos CTX270584.

- Los Cloud Connectors deben obtener los FQDN de los VDA al intermediar una sesión. Realice esta tarea de una de estas dos maneras:
  - **Habilitar la resolución DNS para el sitio.** Vaya a **Configuración completa > Parámetros** y active la opción **Habilitar la resolución DNS**. Alternativamente, use el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops y ejecute el comando `Set-BrokerSite -DnsResolutionEnabled $true`. Para obtener más información sobre el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops, consulte SDK y API.
  - **Zona de búsqueda inversa de DNS con registros PTR para los VDA.** Si elige esta opción, le recomendamos que configure los VDA para que siempre intenten registrar registros PTR. Para ello, use el Editor de directivas de grupo o el Objeto de directiva de grupo, vaya a **Configuración del equipo > Plantillas administrativas > Red > Cliente DNS** y establezca **Registrar registros PTR** en **Habilitado y registrar**. Si el sufijo DNS de la conexión no coincide con el sufijo DNS del dominio, también debe configurar la opción **Sufijo DNS específico de la conexión** para que las máquinas registren los registros PTR correctamente.

> **Nota:**
>
> Si se utiliza la opción de resolución DNS, los Cloud Connectors deben poder resolver los nombres de dominio completos (FQDN) de las máquinas VDA. En el caso de que los usuarios internos se conecten directamente a las máquinas VDA, los dispositivos cliente también deben poder resolver los FQDN de las máquinas VDA.

> Si se utiliza una zona de búsqueda inversa de DNS, los FQDN de los registros PTR deben coincidir con los FQDN de las máquinas VDA. Si el registro PTR contiene un FQDN diferente, la conexión Rendezvous falla. Por ejemplo, si el FQDN de la máquina es `vda01.domain.net`, el registro PTR debe contener `vda01.domain.net`. Un FQDN diferente, como `vda01.sub.domain.net`, no funciona.

Configuración del proxy

El VDA admite el establecimiento de conexiones Rendezvous a través de proxies HTTP y SOCKS5.

Consideraciones sobre el proxy

Tenga en cuenta lo siguiente al usar proxies con Rendezvous:

- Se admiten proxies HTTP no transparentes y proxies SOCKS5.
- No se admiten el descifrado ni la inspección de paquetes. Configure una excepción para que el tráfico ICA® entre el VDA y el servicio Gateway no se intercepte, descifre ni inspeccione. De lo contrario, la conexión se interrumpe.
- Los proxies HTTP admiten la autenticación basada en máquinas mediante los protocolos de autenticación Negotiate y Kerberos. Al conectarse al servidor proxy, el esquema de **autenticación Negotiate** selecciona automáticamente el protocolo Kerberos. Kerberos es el único esquema que admite el VDA de Linux.

  > **Nota:**
  >
  > Para usar Kerberos, debe crear el nombre principal de servicio (SPN) para el servidor proxy y asociarlo a la cuenta de Active Directory del proxy. El VDA genera el SPN en el formato `HTTP/<proxyURL>` al establecer una sesión, donde la URL del proxy se recupera de la configuración de la directiva **Proxy de Rendezvous**. Si no crea un SPN, la autenticación falla.

- Actualmente no se admite la autenticación con un proxy SOCKS5. Si utiliza un proxy SOCKS5, debe configurar una excepción para que el tráfico destinado a las direcciones del servicio Gateway (especificadas en los requisitos) pueda omitir la autenticación.
- Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como protocolo de transporte para ICA.

Proxy transparente

El proxy HTTP transparente es compatible con Rendezvous. Si utiliza un proxy transparente en su red, no se requiere ninguna configuración adicional en el VDA.

Proxy no transparente

Cuando utilice un proxy no transparente en su red, configure la opción Configuración del proxy de Rendezvous. Cuando la opción esté habilitada, especifique la dirección del proxy HTTP o SOCKS5 para que el VDA sepa qué proxy usar. Por ejemplo:

- Dirección del proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`

Validación de Rendezvous

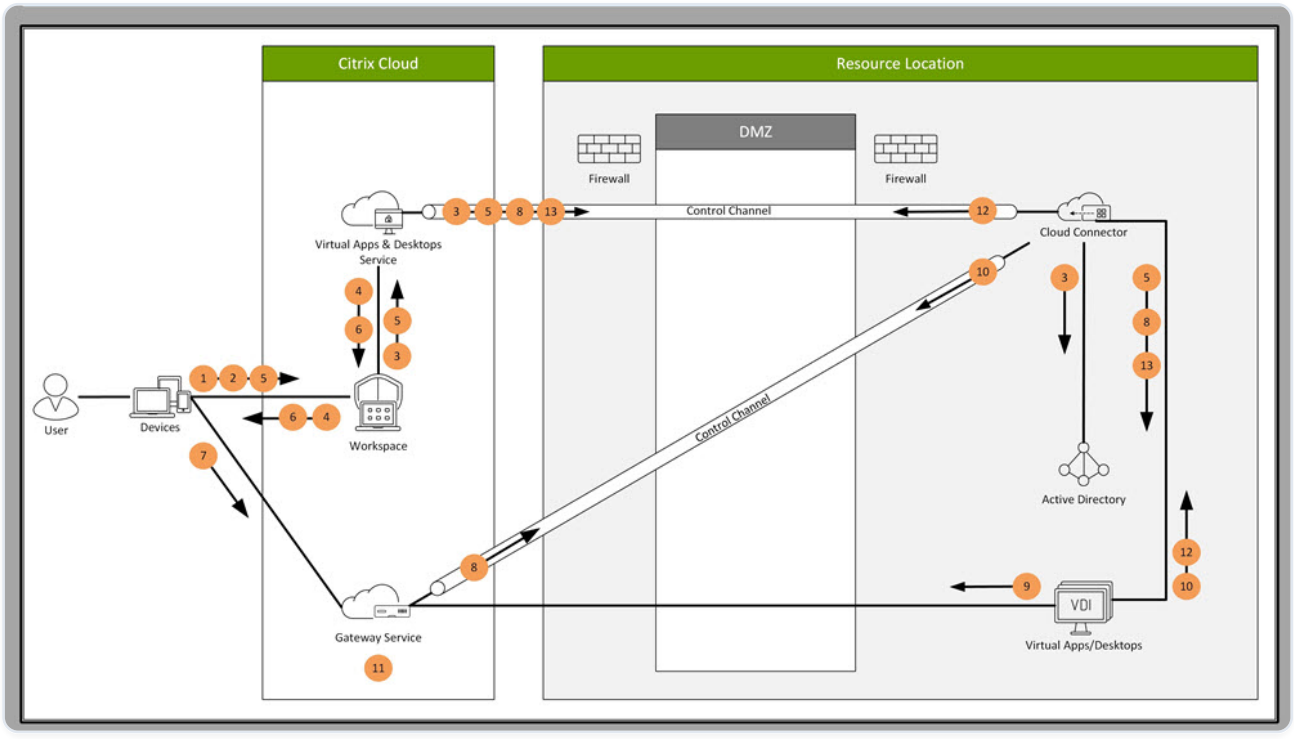
Si cumple todos los requisitos, siga estos pasos para validar si Rendezvous está en uso:

1. Inicie un terminal en el VDA.
2. Ejecute `/opt/Citrix/VDA/bin/ctxquery -f iP`.
3. Los PROTOCOLOS DE TRANSPORTE indican el tipo de conexión:
   - Rendezvous TCP: TCP - TLS - CGP - ICA
   - Rendezvous EDT: UDP - DTLS - CGP - ICA
   - Proxy a través de Cloud Connector: TCP - PROXY - SSL - CGP - ICA o UDP - PROXY - DTLS - CGP - ICA

> **Sugerencia:**
>
> Si el VDA no puede alcanzar el servicio Citrix Gateway directamente con Rendezvous habilitado, el VDA recurre a la intermediación de la sesión HDX a través de Cloud Connector.

Cómo funciona Rendezvous

Este diagrama es una descripción general del flujo de conexión de Rendezvous.



Siga los pasos para comprender el flujo.

1. Vaya a Citrix Workspace.
2. Introduzca las credenciales en Citrix Workspace.

3. Si utiliza Active Directory local, Citrix DaaS™ autentica las credenciales con Active Directory mediante el canal de Cloud Connector.
4. Citrix Workspace muestra los recursos enumerados de Citrix DaaS.
5. Seleccione los recursos de Citrix Workspace. Citrix DaaS envía un mensaje al VDA para prepararse para una sesión entrante.
6. Citrix Workspace envía un archivo ICA al punto final que contiene un ticket STA generado por Citrix Cloud.
7. El punto final se conecta al servicio Citrix Gateway, proporciona el ticket para conectarse al VDA y Citrix Cloud valida el ticket.
8. El servicio Citrix Gateway envía información de conexión al Cloud Connector. El Cloud Connector determina si la conexión es una conexión Rendezvous y envía la información al VDA.
9. El VDA establece una conexión directa con el servicio Citrix Gateway.
10. Si no es posible una conexión directa entre el VDA y el servicio Citrix Gateway, el VDA establece su conexión a través del Cloud Connector.
11. El servicio Citrix Gateway establece una conexión entre el dispositivo de punto final y el VDA.
12. El VDA verifica su licencia con Citrix DaaS a través del Cloud Connector.
13. Citrix DaaS envía las directivas de sesión al VDA a través del Cloud Connector. Esas directivas se aplican.

Rendezvous V2

Al utilizar el servicio Citrix Gateway, el protocolo Rendezvous permite que el tráfico omita los conectores de Citrix Cloud™ y se conecte de forma directa y segura con el plano de control de Citrix Cloud.

Hay dos tipos de tráfico a considerar: 1) tráfico de control para el registro de VDA y la intermediación de sesiones; 2) tráfico de sesión HDX™.

Rendezvous V1 permite que el tráfico de sesión HDX omita los Cloud Connectors, pero aún requiere que los Cloud Connectors actúen como proxy para todo el tráfico de control para el registro de VDA y la intermediación de sesiones.

Las máquinas unidas a un dominio de AD estándar y las máquinas no unidas a un dominio son compatibles con Rendezvous V2 con VDA de Linux de sesión única y de varias sesiones. Con las máquinas no unidas a un dominio, Rendezvous V2 permite que tanto el tráfico HDX como el tráfico de control omitan los Cloud Connectors.

Requisitos

Los requisitos para usar Rendezvous V2 son:

- Acceso al entorno mediante Citrix Workspace™ y el servicio Citrix Gateway.
- Plano de control: Citrix DaaS (anteriormente servicio Citrix Virtual Apps and Desktops™).
- VDA versión 2201 o posterior.
    - La versión 2204 es la mínima requerida para los proxies HTTP y SOCKS5.
- Habilite el protocolo Rendezvous en la directiva de Citrix. Para obtener más información, consulte Configuración de directiva del protocolo Rendezvous.
- Los VDA deben tener acceso a:
    - `https://*.xendesktop.net` en `TCP 443`. Si no puede permitir todos los subdominios de esa manera, puede usar `https://<customer_ID>.xendesktop.net`, donde `<customer_ID>` es su ID de cliente de Citrix Cloud, como se muestra en el portal de administración de Citrix Cloud.
    - `https://*.nssvc.net`, incluidos todos los subdominios. Si no puede incluir en la lista blanca todos los subdominios de esa manera, use `https://*.c.nssvc.net` y `https://*.g.nssvc.net` en su lugar. Para obtener más información, consulte la sección Requisitos de conectividad a Internet de la documentación de Citrix Cloud (en el servicio Virtual Apps and Desktop) y el artículo del Centro de conocimientos CTX270584.
- Los VDA deben poder conectarse a las direcciones mencionadas anteriormente:
    - En TCP 443, para Rendezvous TCP.
    - En UDP 443, para Rendezvous EDT.

Configuración del proxy

El VDA admite la conexión a través de proxies tanto para el tráfico de control como para el tráfico de sesión HDX al usar Rendezvous. Los requisitos y consideraciones para ambos tipos de tráfico son diferentes, así que revíselos con atención.

Consideraciones sobre el proxy para el tráfico de control

- Solo se admiten proxies HTTP.
- No se admite el descifrado ni la inspección de paquetes. Configure una excepción para que el tráfico de control entre el VDA y el plano de control de Citrix Cloud no se intercepte, descifre ni inspeccione. De lo contrario, la conexión fallará.

- No se admite la autenticación de proxy.
- Para configurar un proxy para el tráfico de control, modifique el registro de la siguiente manera:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ProxySettings" -d "http://<URL or IP>:<port>" --force
```

Consideraciones sobre el proxy para el tráfico HDX

- Se admiten proxies HTTP y SOCKS5.
- EDT solo se puede usar con proxies SOCKS5.
- Para configurar un proxy para el tráfico HDX, utilice la configuración de directiva Configuración del proxy de Rendezvous.
- No se admite el descifrado ni la inspección de paquetes. Configure una excepción para que el tráfico HDX entre el VDA y el plano de control de Citrix Cloud no se intercepte, descifre ni inspeccione. De lo contrario, la conexión fallará.
- Los proxies HTTP admiten la autenticación basada en máquinas mediante los protocolos de autenticación Negotiate y Kerberos. Al conectarse al servidor proxy, el **esquema de autenticación Negotiate** selecciona automáticamente el protocolo Kerberos. Kerberos es el único esquema que admite el VDA de Linux.

> **Nota:**
>
> Para usar Kerberos, debe crear el nombre principal de servicio (SPN) para el servidor proxy y asociarlo a la cuenta de Active Directory del proxy. El VDA genera el SPN en el formato `HTTP/<proxyURL>` al establecer una sesión, donde la URL del proxy se recupera de la configuración de la directiva **Proxy de Rendezvous**. Si no crea un SPN, la autenticación falla.

- Actualmente no se admite la autenticación con un proxy SOCKS5. Si utiliza un proxy SOCKS5, debe configurar una excepción para que el tráfico destinado a las direcciones del servicio Gateway (especificadas en los requisitos) pueda omitir la autenticación.
- Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como protocolo de transporte para ICA.

Proxy transparente

El proxy HTTP transparente es compatible con Rendezvous. Si utiliza un proxy transparente en su red, no se requiere ninguna configuración adicional en el VDA.

Cómo configurar Rendezvous V2

A continuación, se indican los pasos para configurar Rendezvous en su entorno:

1. Asegúrese de que se cumplen todos los requisitos.
2. Una vez instalado el VDA, ejecute el siguiente comando para establecer la clave de registro necesaria:

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k
   "HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
   "GctRegistration" -d "0x00000001" --force
   ```

3. Reinicie la máquina VDA.
4. Cree una directiva de Citrix o edite una existente:
   - Establezca la configuración del Protocolo Rendezvous en **Permitido**. El Protocolo Rendezvous está inhabilitado de forma predeterminada. Cuando el Protocolo Rendezvous está habilitado (**Permitido**), se aplica Rendezvous V2 en lugar de V1.
   - Asegúrese de que los filtros de la directiva de Citrix estén configurados correctamente. La directiva se aplica a las máquinas que necesitan tener Rendezvous habilitado.
   - Asegúrese de que la directiva de Citrix tenga la prioridad correcta para que no sobrescriba otra.

Validación de Rendezvous

Para comprobar si una sesión utiliza el protocolo Rendezvous, ejecute el comando `/opt/Citrix/VDA/bin/ctxquery -f iP` en el terminal.

Los protocolos de transporte mostrados indican el tipo de conexión:

- Rendezvous TCP: TCP - TLS - CGP - ICA
- Rendezvous EDT: UDP - DTLS - CGP - ICA
- Proxy a través de Cloud Connector: TCP - PROXY - SSL - CGP - ICA o UDP - PROXY - DTLS - CGP - ICA

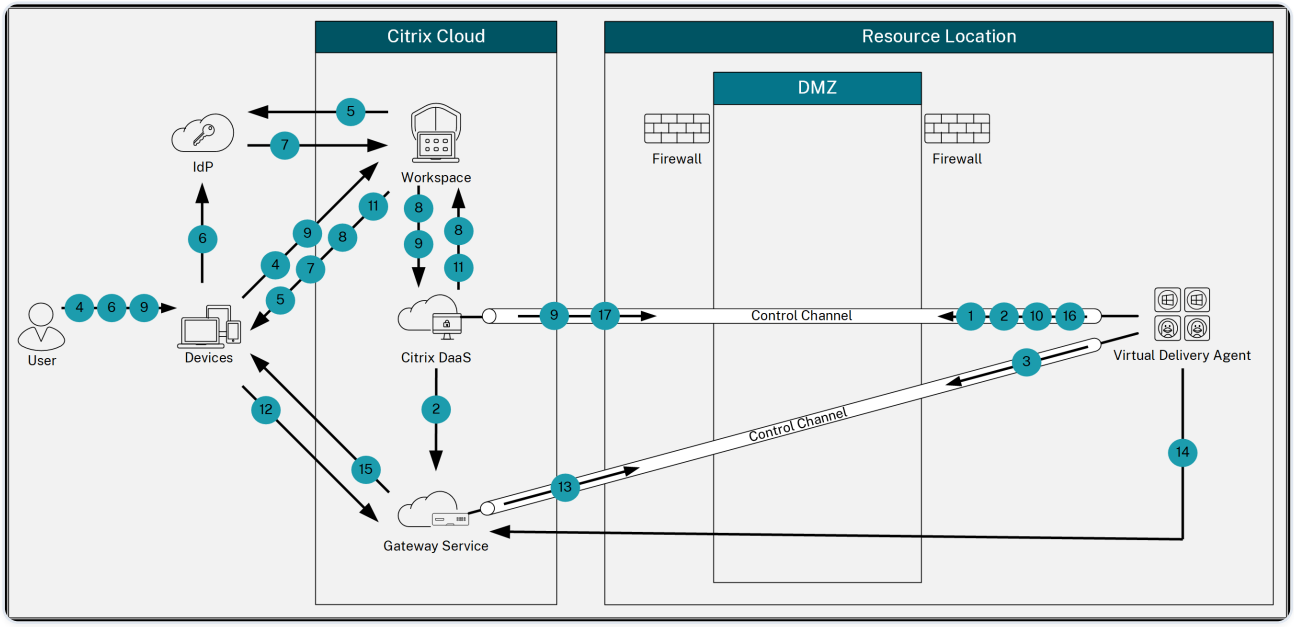
Si Rendezvous V2 está en uso, la versión del protocolo muestra 2.0.

Sugerencia:

Si el VDA no puede llegar al servicio Citrix Gateway directamente con Rendezvous habilitado, el VDA recurre a usar el proxy para la sesión HDX a través del Cloud Connector.

Flujo de tráfico de Rendezvous

El siguiente diagrama ilustra la secuencia de pasos del flujo de tráfico de Rendezvous.



1. El VDA establece una conexión WebSocket con Citrix Cloud y se registra.
2. El VDA se registra en el servicio Citrix Gateway y obtiene un token dedicado.
3. El VDA establece una conexión de control persistente con el servicio Gateway.
4. El usuario navega a Citrix Workspace.
5. Workspace evalúa la configuración de autenticación y redirige a los usuarios al IdP apropiado para la autenticación.
6. El usuario introduce sus credenciales.
7. Después de validar correctamente las credenciales del usuario, este es redirigido a Workspace.
8. Workspace cuenta los recursos para el usuario y los muestra.
9. El usuario selecciona un escritorio o una aplicación desde Workspace. Workspace envía la solicitud a Citrix DaaS™, que intermedia la conexión e indica al VDA que se prepare para la sesión.

10. El VDA responde con la capacidad Rendezvous y su identidad.
11. Citrix DaaS genera un ticket de inicio y lo envía al dispositivo del usuario a través de Workspace.
12. El endpoint del usuario se conecta al Gateway Service y proporciona el ticket de inicio para autenticar e identificar el recurso al que conectarse.
13. El Gateway Service envía la información de conexión al VDA.
14. El VDA establece una conexión directa para la sesión con el Gateway Service.
15. El Gateway Service completa la conexión entre el endpoint y el VDA.
16. El VDA verifica la licencia para la sesión.
17. Citrix DaaS envía las directivas aplicables al VDA.

HDX™ seguro

Puede cifrar sesiones ICA® de extremo a extremo entre la aplicación Citrix Workspace™ (cliente) y el VDA (host de sesión).

La función de cifrado de extremo a extremo (E2EE) no permite que ningún elemento de red intermedio, incluido Citrix Gateway, descifre el tráfico ICA. Mejora la postura de seguridad de su entorno y es fácil de configurar y administrar.

Requisitos del sistema

- Linux VDA versión mínima 2311
- Delivery Controller™ versión mínima 2308
- StoreFront™ versión mínima 2308
- Aplicación Citrix Workspace para Windows versión mínima 2308

Configuración

Habilitar el cifrado de extremo a extremo

La función de cifrado de extremo a extremo (E2EE) está inhabilitada de forma predeterminada. Para habilitarla, establezca la directiva **Secure HDX** en **Habilitado** en Citrix Studio.

Programar renovaciones de certificados

La función de cifrado de extremo a extremo (E2EE) requiere un certificado autofirmado y su clave privada que administra el servicio **ctxcertmgr** en el VDA de Linux.

Se crea un nuevo certificado autofirmado cuando el servicio **ctxcertmgr** se inicia o se reinicia. De forma predeterminada, el servicio **ctxcertmgr** renueva el certificado (incluida su clave privada) cada dos años a las 2:00 AM. También puede programar renovaciones de certificados con una configuración del Registro similar a la siguiente:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\SecureHDX" -t
"REG_SZ" -v "CaRotationStartDate" -d "2023-10-19" --force



/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\SecureHDX" -t
"REG_SZ" -v "CaRotationTime" -d "00:45:30" --force



/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\SecureHDX" -t
"REG_DWORD" -v "CaRotationPeriod" -d "0x00000005" --force
```

En el ejemplo anterior, la primera hora de renovación del certificado se establece a las 00:45:30 del 2023-10-19. Después de eso, el servicio **ctxcermgr** renueva el certificado cada 5 días a las 00:45:30. La fecha y hora programadas son la fecha y hora en el VDA de Linux.

Proteger las sesiones de usuario con DTLS

El cifrado DTLS es una función totalmente compatible a partir de la versión 7.18. De forma predeterminada, esta función está inhabilitada en Linux VDA. Para obtener más información, consulte Seguridad de la capa de transporte.

Habilitar el cifrado DTLS

verificar que el transporte adaptable está habilitado

En Citrix Studio, verificar que la directiva **HDX™ Adaptive Transport** está establecida en **Preferred** o **Diagnostic mode**.

Habilitar el cifrado SSL en Linux VDA

En Linux VDA, utilice la herramienta **enable_vdassl.sh** en **/opt/Citrix/VDA/sbin** para habilitar (o inhabilitar) el cifrado SSL. Para obtener información sobre las opciones disponibles en la herramienta, ejecute el comando `/opt/Citrix/VDA/sbin/enable_vdassl.sh –h`.

> **Nota:**

> Compruebe qué versión de DTLS se utiliza en su aplicación Citrix Workspace™. Asegúrese de que se utiliza la misma versión de DTLS tanto en Linux VDA como en su aplicación Citrix Workspace.

Proteger las sesiones de usuario con TLS

A partir de la versión 7.16, Linux VDA admite el cifrado TLS para proteger las sesiones de usuario. El cifrado TLS está inhabilitado de forma predeterminada.

Habilitar el cifrado TLS

Para habilitar el cifrado TLS para las sesiones de usuario seguras, instale certificados y habilite el cifrado TLS tanto en Linux VDA como en Delivery Controller™ (el Controller).

Instalar certificados en Linux VDA

Obtenga certificados de servidor en formato PEM y certificados raíz en formato CRT. Un certificado de servidor contiene las siguientes secciones:

- Certificado
- Clave privada sin cifrar
- Certificados intermedios (opcional)

Un ejemplo de certificado de servidor:

```
-----BEGIN CERTIFICATE-----

MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV

BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU

MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0

MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL

MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE

ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G

A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD

gY0AMIGJAoGBALCTTOdxcivbI0L0F66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9

t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEw13YxM6COyBf7L6psrsCDNnBP1q8TJH

4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+0FQ2Bq3NhwsRhnAgMBAAGj

gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8y0w

gZkGA1UdIwSBkTCBjoAU85kN1EPJ0cVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV

BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU

MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0

ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB

AD5axBYHwIxJCJzNt2zdXnbp2O0yUToWElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68

VelBu1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbu0IjOtr3pkxAe

b6CFJtNLudHUrwF6l0rB72zbyz3PiIx+HEwt1j0j8z4K

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q

fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy

R+MaDyF1HmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB

AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea

FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSx0Yb/lAdck/
```

Habilitar el cifrado TLS

HABILITAR EL CIFRADO TLS EN LINUX VDA

En Linux VDA, use el script `enable_vdassl.sh` en el directorio **/opt/Citrix/VDA/sbin** para habilitar (o inhabilitar) el cifrado TLS. Para obtener información sobre las opciones disponibles en el script, ejecute el comando `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help`.

```
root@lxu1804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used, If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
       -Certificate <CERT-FILE>
       Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
       is currently supported, that is PEM.

       -RootCertificate <ROOT-CERT-FILE>
       Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path, The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

       -SSLPort <SSL-PORT-NUMBER>
       Specify an SSL port number. Unless otherwise specified, the default port 443 used.

       -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
       Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

       -SSLCipherSuite <GOV|COM|ALL>
       Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem"
       Enable Linux VDA SSL using Certificate cert001.pem.

       enable-vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
       Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -SSLPort 445
       Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
       Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

Sugerencia: Se debe instalar un certificado de servidor en cada servidor Linux VDA y se deben instalar certificados raíz en cada servidor y cliente Linux VDA.

HABILITAR EL CIFRADO TLS EN EL CONTROLLER

> **Nota:**
>
> Solo puede habilitar el cifrado TLS para grupos de entrega completos. No puede habilitar el cifrado TLS para aplicaciones específicas.

> En una ventana de PowerShell del Controller, ejecute los siguientes comandos en secuencia para habilitar el cifrado TLS para el grupo de entrega de destino.

1. `Add-PSSnapin citrix.*`.

2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $true`

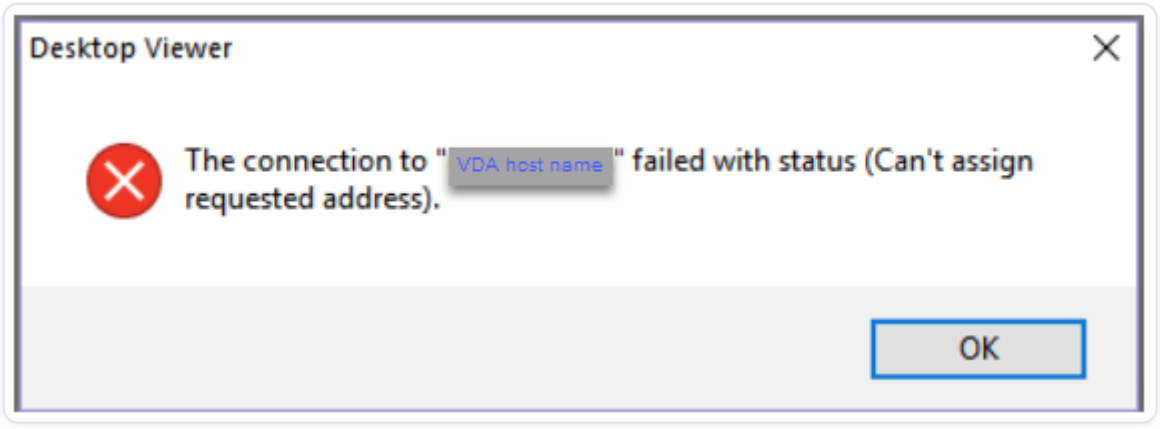
> **Nota:**
>
> Para asegurarse de que solo los FQDN de VDA estén contenidos en un archivo de sesión ICA®, también puede ejecutar el comando `Set-BrokerSite –DnsResolutionEnabled $true`. El comando habilita la resolución DNS. Si inhabilita la resolución DNS, un archivo de sesión ICA divulga las direcciones IP de VDA y proporciona FQDN solo para los elementos relacionados con TLS, como `SSLProxyHost` y `UDPDTLSPort`.

> Para inhabilitar el cifrado TLS en el Controller, ejecute los siguientes comandos en secuencia:

1. `Add-PSSnapin citrix.*`.
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $false`
3. `Set-BrokerSite –DnsResolutionEnabled $false`

Solución de problemas

El siguiente error "Can't assign requested address" puede ocurrir en la aplicación Citrix Workspace™ para Windows al intentar acceder a una sesión de escritorio publicada:



Como solución temporal, agregue una entrada al archivo **hosts**, similar a:

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

En las máquinas Windows, el archivo **hosts** se encuentra normalmente en `C:\Windows\System32\drivers\etc\hosts`.

Fiabilidad de la sesión

Citrix® introduce la función de fiabilidad de sesión en todas las plataformas Linux compatibles. La fiabilidad de sesión está habilitada de forma predeterminada.

La fiabilidad de sesión reconecta las sesiones ICA sin problemas a través de interrupciones de red. Para obtener más información sobre la fiabilidad de sesión, consulte Reconexión automática de clientes y fiabilidad de sesión.

> **Nota**:
>
> Los datos transmitidos a través de una conexión de fiabilidad de sesión están en texto sin formato de forma predeterminada. Por motivos de seguridad, le recomendamos que habilite el cifrado TLS. Para obtener más información sobre el cifrado TLS, consulte Proteger las sesiones de usuario mediante TLS.

Configuración

Configuración de directivas en Citrix Studio

Puede configurar las siguientes directivas para la fiabilidad de sesión en Citrix Studio:

- Conexiones de fiabilidad de la sesión
- Tiempo de espera de fiabilidad de la sesión
- Número de puerto de fiabilidad de la sesión
- Nivel de transparencia de la interfaz de usuario de reconexión

Para obtener más información, consulte Configuración de directivas de fiabilidad de sesión y Configuración de directivas de reconexión automática de clientes.

> **Nota:**
>
> Después de configurar la directiva **Conexiones de fiabilidad de sesión** o **Número de puerto de fiabilidad de sesión**, reinicie el servicio VDA y el servicio HDX™, en este orden, para que la configuración surta efecto.

Configuración en el VDA de Linux

- **Habilitar/deshabilitar el agente de escucha TCP de fiabilidad de sesión**

De forma predeterminada, el agente de escucha TCP de fiabilidad de sesión está habilitado y escucha en el puerto 2598. Para deshabilitar el agente de escucha, ejecute el siguiente comando.

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cgp" -v "fEnableWinStation" -d "0x00000000"
```

Nota:

Reinicie el servicio HDX para que la configuración surta efecto. Deshabilitar el agente de escucha TCP no deshabilita la fiabilidad de sesión. La fiabilidad de sesión sigue estando disponible a través de otros agentes de escucha (por ejemplo, SSL) si la función está habilitada a través de la directiva **Conexiones de fiabilidad de sesión**.

- **Número de puerto de fiabilidad de sesión**

También puede establecer el número de puerto de fiabilidad de sesión mediante el siguiente comando (usando el número de puerto 2599 como ejemplo).

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cgp" -v "PortNumber" -d "2599"
```

Nota:

Reinicie el servicio HDX para que la configuración surta efecto. Si el número de puerto se ha establecido a través de la configuración de directiva en **Citrix Studio**, la configuración en el VDA de Linux se ignora. Asegúrese de que el firewall del VDA esté configurado para no prohibir el tráfico de red a través del puerto establecido.

- **Intervalo de latido de servidor a cliente**

Los mensajes de latido se envían entre el VDA de Linux y el cliente cuando no hay actividad (por ejemplo, no hay movimiento del ratón ni actualización de la pantalla) en una sesión. Los mensajes de latido se utilizan para detectar si el cliente sigue respondiendo. Si no hay respuesta del cliente, la sesión se suspende hasta que el cliente se vuelva a conectar. Esta configuración especifica el

número de segundos entre mensajes de latido sucesivos. De forma predeterminada, esta configuración no está configurada. Para configurarla, ejecute el siguiente comando (usando 10 segundos como ejemplo).

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpServerToClientKeepAlive"  -d  "10"  --force
```

- **Intervalo de latido de cliente a servidor**

Esta configuración especifica el número de segundos entre mensajes de latido sucesivos enviados desde el cliente ICA® al VDA de Linux. De forma predeterminada, esta configuración no está configurada. Para configurarla, ejecute el siguiente comando (usando 10 segundos como ejemplo).

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpClientToServerKeepAlive"  -d  "10"  --force
```

Solución de problemas

No se pueden iniciar sesiones después de habilitar la fiabilidad de la sesión mediante la configuración de directiva.

Para solucionar este problema, haga lo siguiente:

1. Asegúrese de que el servicio VDA y el servicio HDX se reinicien, en este orden, después de habilitar la fiabilidad de la sesión mediante la configuración de directiva en Citrix Studio.
2. En el VDA, ejecute el siguiente comando para verificar que el agente de escucha TCP de fiabilidad de la sesión se está ejecutando (usando el puerto 2598 como ejemplo).

   ```
   netstat -an | grep 2598
   ```

   Si no hay ningún agente de escucha TCP en el puerto de fiabilidad de la sesión, habilite el agente de escucha ejecutando el siguiente comando.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations
   \cgp"   -v  "fEnableWinStation" -d "0x00000001"
   ```

Grabar sesión en almacenamiento local

Puede grabar y reproducir sesiones alojadas en un VDA de Linux.

Habilitar o deshabilitar la grabación de sesiones

Para habilitar o deshabilitar la grabación de sesiones para un VDA de Linux, establezca **SmAudAllowed** en **1** o **0**, respectivamente. Puede utilizar los siguientes comandos:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "SmAudAllowed" -d "0x00000001" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "SmAudAllowed" -d "0x00000000" --force
```

Nota:

Después de habilitar la grabación de sesiones en un VDA de Linux, los usuarios reciben una notificación de que sus sesiones se están grabando cuando inician sesión en ellas.

Especificar el tamaño de archivo para las grabaciones

A medida que las grabaciones aumentan de tamaño, los archivos de grabación tardan más en descargarse y responden más lentamente cuando se utiliza el control deslizante de búsqueda para navegar durante la reproducción. Para controlar el tamaño del archivo, especifique un límite de umbral para un archivo. Cuando la grabación alcanza este límite, el archivo actual se cierra y se crea un archivo adicional para continuar la grabación. Esta acción se denomina rotación.

Mediante los siguientes comandos, puede especificar dos umbrales para una rotación:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "RolloverFileSizeInMB" -d "0x00000032" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
```

```
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "RolloverTimeInHours" -d "0x0000000c" --force
```

- **RolloverFileSizeInMB**. El archivo actual se cierra cuando alcanza el tamaño y se abre un nuevo archivo. De forma predeterminada, la rotación se produce cuando el tamaño supera los 50 MB. Valores admitidos: 10–300.
- **RolloverTimeInHours**. Cuando se alcanza la duración, el archivo actual se cierra y se abre un nuevo archivo. De forma predeterminada, la rotación se produce cuando la sesión graba durante 12 horas. Valores admitidos: 1–24.

Las rotaciones se producen cuando se cumple la primera de las dos condiciones anteriores. Por ejemplo, si especifica 17 MB para el tamaño del archivo y 6 horas para la duración. Cuando la grabación alcanza los 17 MB en 3 horas, la grabación de sesiones cierra el archivo y abre uno nuevo.

Para evitar la creación de muchos archivos pequeños, la rotación no se produce hasta que transcurre al menos una hora, independientemente del valor especificado para el tamaño del archivo. La excepción a esta regla es si el tamaño del archivo supera los 300 MB.

Especificar dónde se almacenan las grabaciones

Los archivos de grabación se almacenan en `/var/xdl/session_recordings` de forma predeterminada. Para especificar una ruta diferente, ejecute el siguiente comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_SZ" -v
"Path" -d "<your custom storage path>" --force
```

Puede almacenar las grabaciones en una unidad local o en un punto de montaje que apunte a una ruta de red. Configure los permisos de acceso adecuados para la ruta de almacenamiento que establezca y conceda al usuario `ctxsrvr` permiso de escritura para la ruta.

Ver grabaciones

Para ver las grabaciones, siga estos pasos para instalar el reproductor de grabación de sesiones o el reproductor web de grabación de sesiones:

1. Utilice las credenciales de su cuenta de Citrix para acceder a la página de descarga de Citrix Virtual Apps and Desktops y descargar el archivo del producto. Descomprima el archivo.

2. Haga doble clic en SessionRecordingPlayer.msi y SessionRecordingWebPlayer.msi y siga las instrucciones para completar la instalación.

Sugerencia:

Para usar el reproductor web de grabación de sesiones, instálelo solo en el servidor de grabación de sesiones y asegúrese de que las grabaciones estén disponibles en el servidor de grabación de sesiones. Para obtener más información, consulte la documentación de Citrix Session Recording.

Limitaciones

- Para las sesiones de aplicaciones virtuales, es posible que las notificaciones de grabación no estén centradas.

Prácticas recomendadas

Esta sección le guía a través de los siguientes procedimientos:

- Configurar certificados autofirmados para WebSocket(/es-es/linux-virtual-delivery-agent/2507-ltsr/best-practices/configure-self-signed-certificates-for-websocket.html)
- Crear VDA de Linux en Google Cloud Platform (GCP) mediante Machine Creation Services (MCS)(/es-es/linux-virtual-delivery-agent/2507-ltsr/best-practices/create-linux-vda-on-gcp-using-mcs.html)
- Administrar la implementación con Ansible(/es-es/linux-virtual-delivery-agent/2507-ltsr/best-practices/manage-your-deployment-using-ansible.html)
- Integrar VDA de Linux no unido a un dominio con Red Hat IdM(/es-es/linux-virtual-delivery-agent/2507-ltsr/best-practices/non-domain-joined-linux-vda-red-hat-idm.html)

Configurar certificados autofirmados para WebSocket

A partir de la versión inicial de 2402 LTSR, Citrix Virtual Apps and Desktops le permite usar la tecnología WebSocket a través del Protocolo de intermediación de Citrix (CBP) para facilitar la comunicación entre los VDA y los Delivery Controllers. Esta función solo requiere el puerto TLS 443 para la comunicación del VDA al Delivery Controller. Para obtener más información, consulte Comunicación WebSocket entre VDA y Delivery Controller en la documentación de Citrix Virtual Apps and Desktops.

WebSocket es una tecnología potente que permite la comunicación bidireccional en tiempo real entre un cliente y un servidor. Sin embargo, para garantizar una conexión segura, especialmente al usar **wss://**, a menudo es necesario configurar un certificado autofirmado, sobre todo en entornos de desarrollo o prueba. Este artículo describe las prácticas recomendadas para configurar certificados autofirmados para WebSocket.

Paso 1: (Solo para VDA no unidos a un dominio) Configurar el servidor DNS

- **Para VDA de Ubuntu y Debian:**

1. Cambie la configuración de DNS editando **/etc/systemd/resolved.conf** de la siguiente manera:

```
[Resolve]

# Some examples of DNS servers which may be used for DNS= and
FallbackDNS=:

# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com
2606:4700:4700::1111#cloudflare-dns.com
2606:4700:4700::1001#cloudflare-dns.com

# Google:     8.8.8.8#dns.google 8.8.4.4#dns.google
2001:4860:4860::8888#dns.google 2001:4860:4860::8844#dns.google

# Quad9:      9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net
2620:fe::fe#dns.quad9.net 2620:fe::9#dns.quad9.net

DNS=<DNS IP address>

#FallbackDNS=

#Domains=

#DNSSEC=no

#DNSOverTLS=no

#MulticastDNS=no

#LLMNR=no

#Cache=no-negative

#CacheFromLocalhost=no

#DNSStubListener=yes

#DNSStubListenerExtra=

#ReadEtcHosts=yes

#ResolveUnicastSingleLabel=no
```

2. Reinicie el servicio systemd-resolved.

```
sudo service systemd-resolved restart
```

Para obtener más información, consulte `<https://notes.enovision.net/linux/changing-dns-with-resolve>`.

- **Para VDA de RHEL, Rocky Linux y SUSE:**

1. Ejecute el siguiente comando **nmcli** para obtener una lista de nombres de conexión:

```
sudo nmcli connection
```

2. Ejecute otro comando **nmcli** para configurar la dirección IP del DNS:

```
sudo nmcli con mod {connectionNameHere} ipv4.dns "<dns ip address>"
```

Por ejemplo, puede establecer la dirección IP del DNS en 192.168.2.254 mediante el siguiente comando:

```
sudo nmcli con mod eth0 ipv4.dns "192.168.2.254"
```

3. Vuelva a cargar la nueva configuración de DNS ejecutando cualquiera de los siguientes comandos:

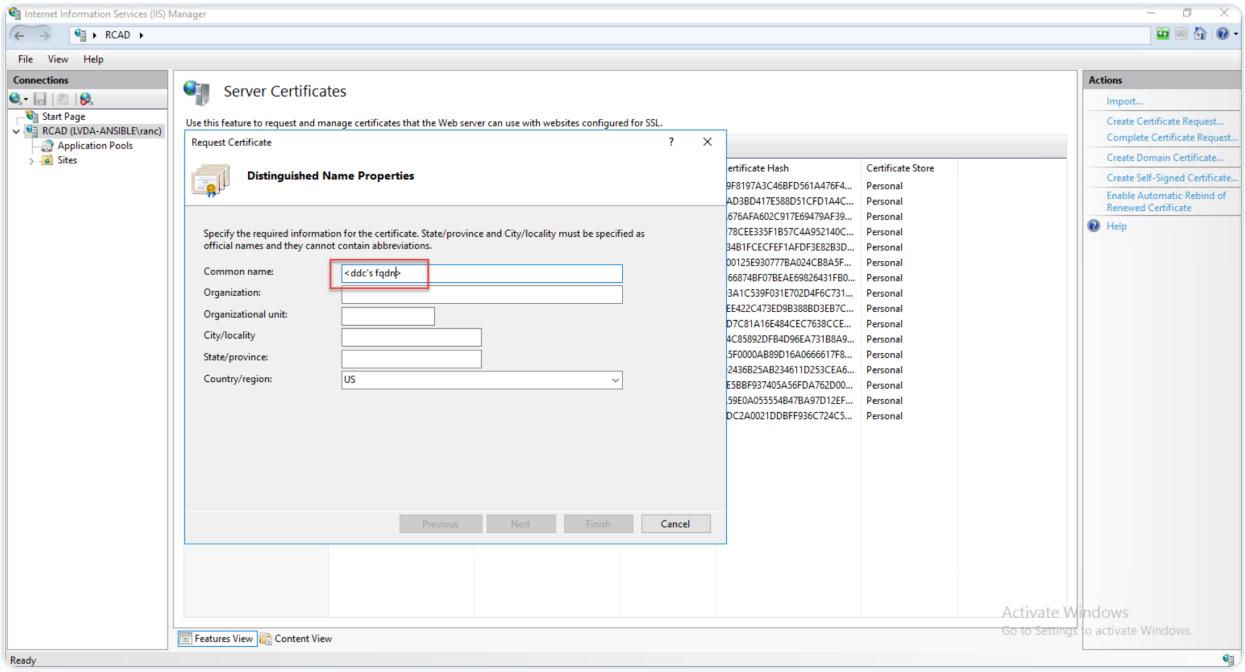
```
sudo systemctl restart NetworkManager.service
```

```
sudo nmcli connection reload
```

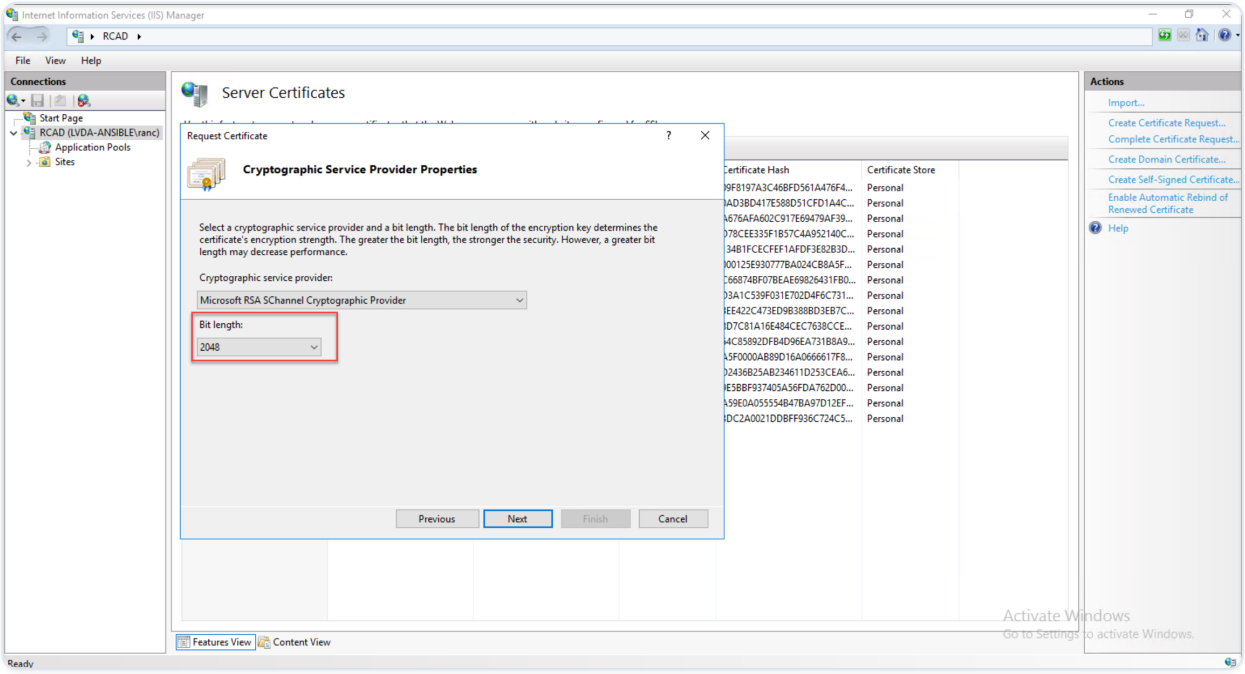
Para obtener más información, consulte `<https://www.cyberciti.biz/faq/change-dns-ip-address-rhel-redhat-linux/>`.

Paso 2: Solicitar un certificado a una autoridad de certificación (CA)

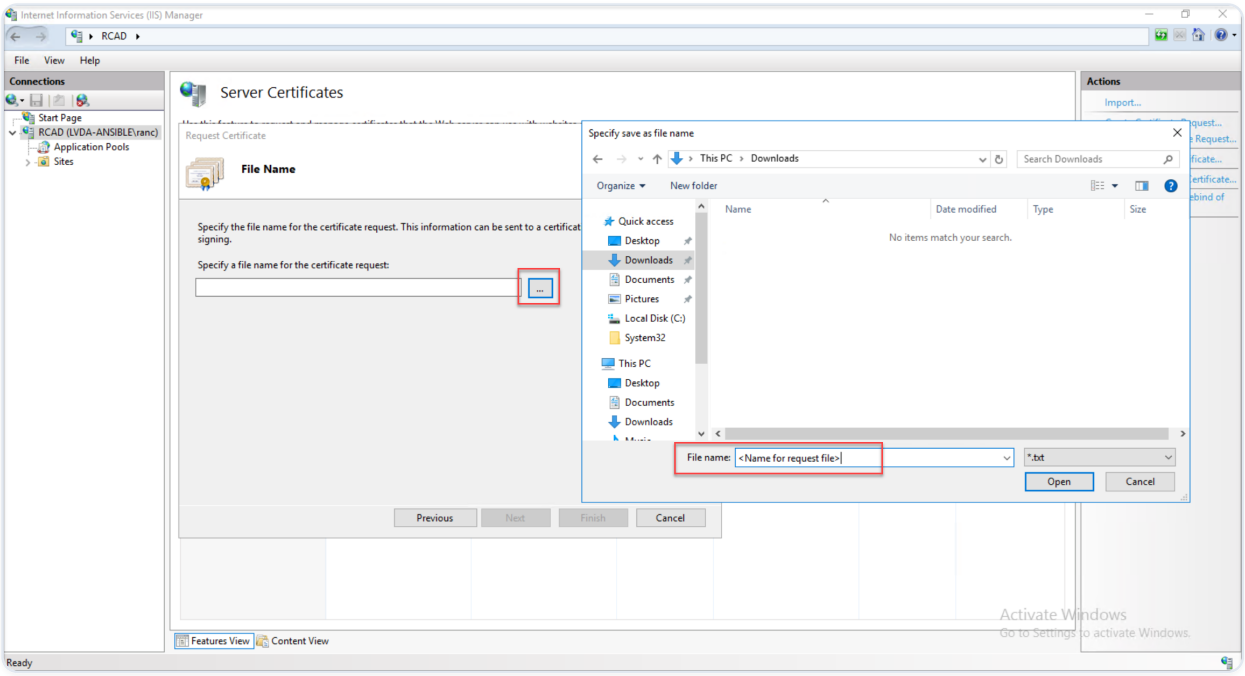
1. Inicie una solicitud de certificado. Cuando inicie una solicitud de certificado, rellene el nombre de dominio completo (FQDN) del Delivery Controller.



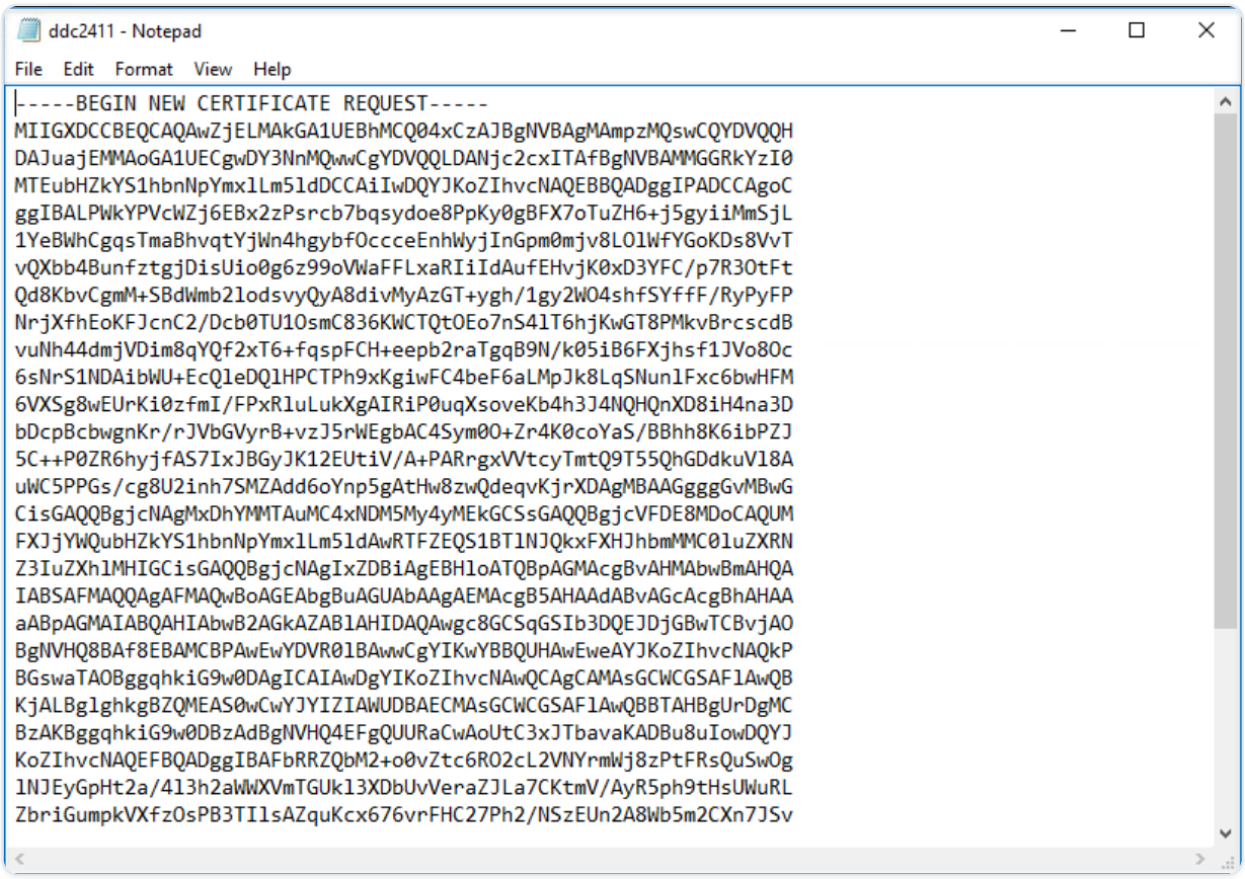
2. Seleccione una longitud de bits de 2048 o superior para garantizar una seguridad sólida para su certificado.



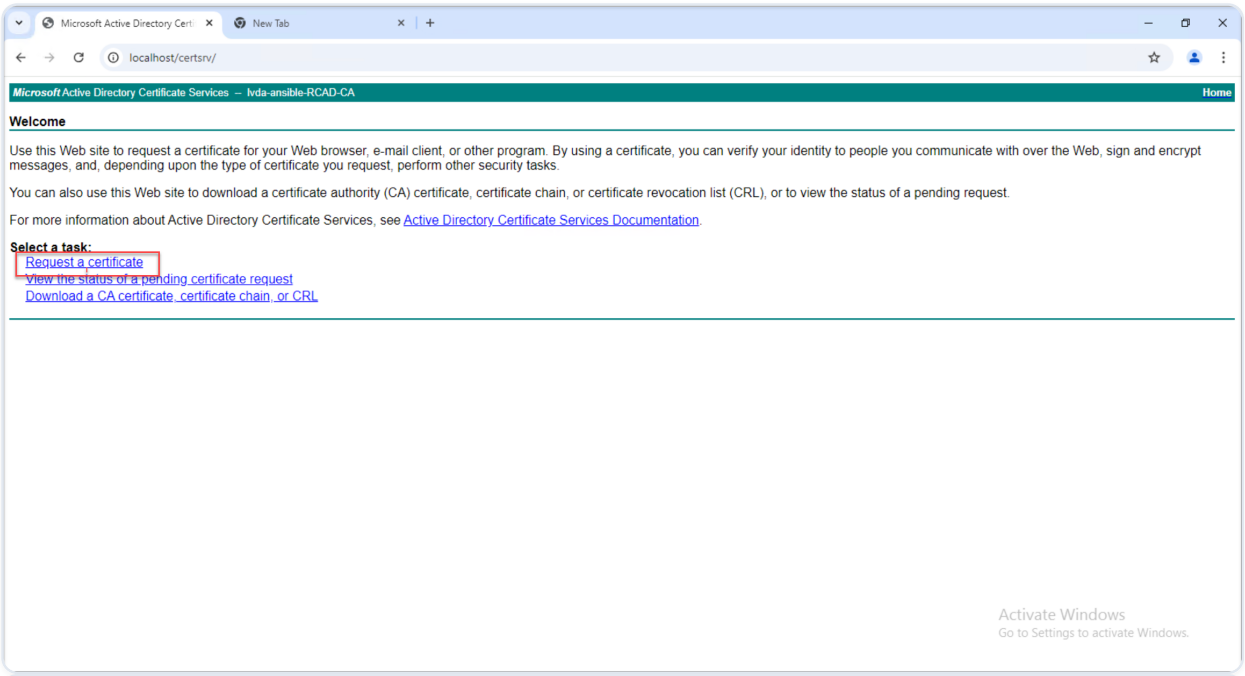
3. Asigne un nombre descriptivo a su archivo de solicitud de certificado para facilitar su identificación.

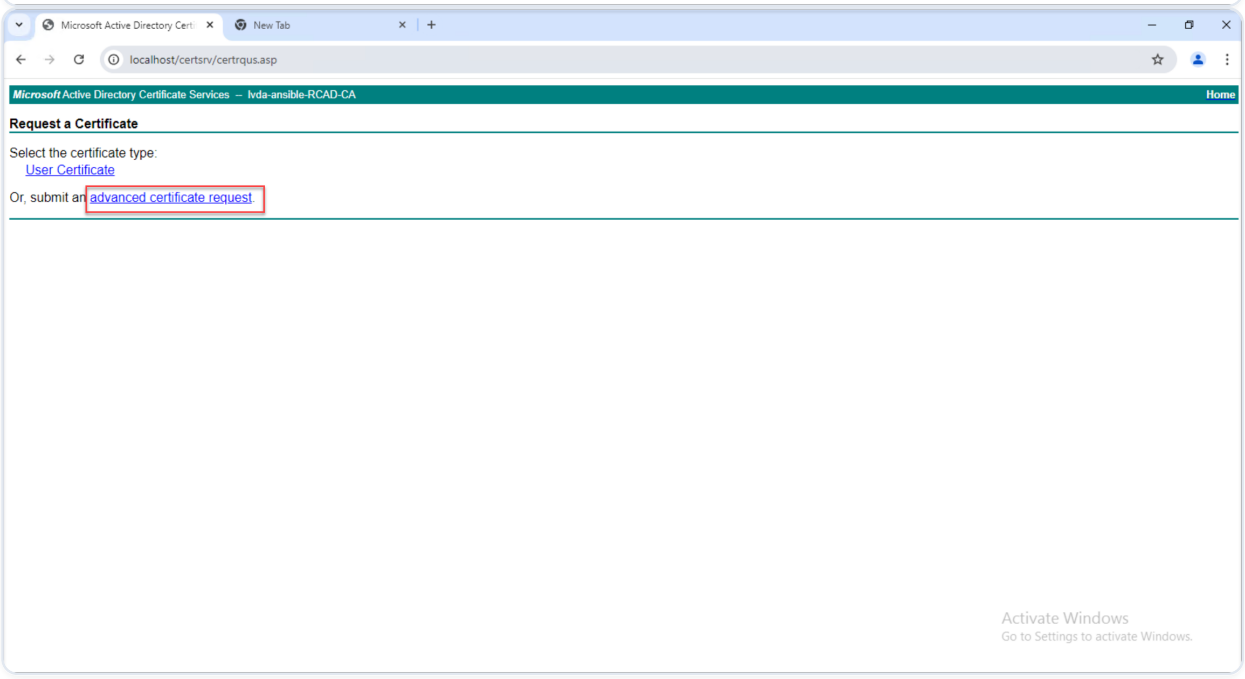


4. Abra el archivo de solicitud de certificado generado con un editor de texto como el Bloc de notas y seleccione todo el contenido.

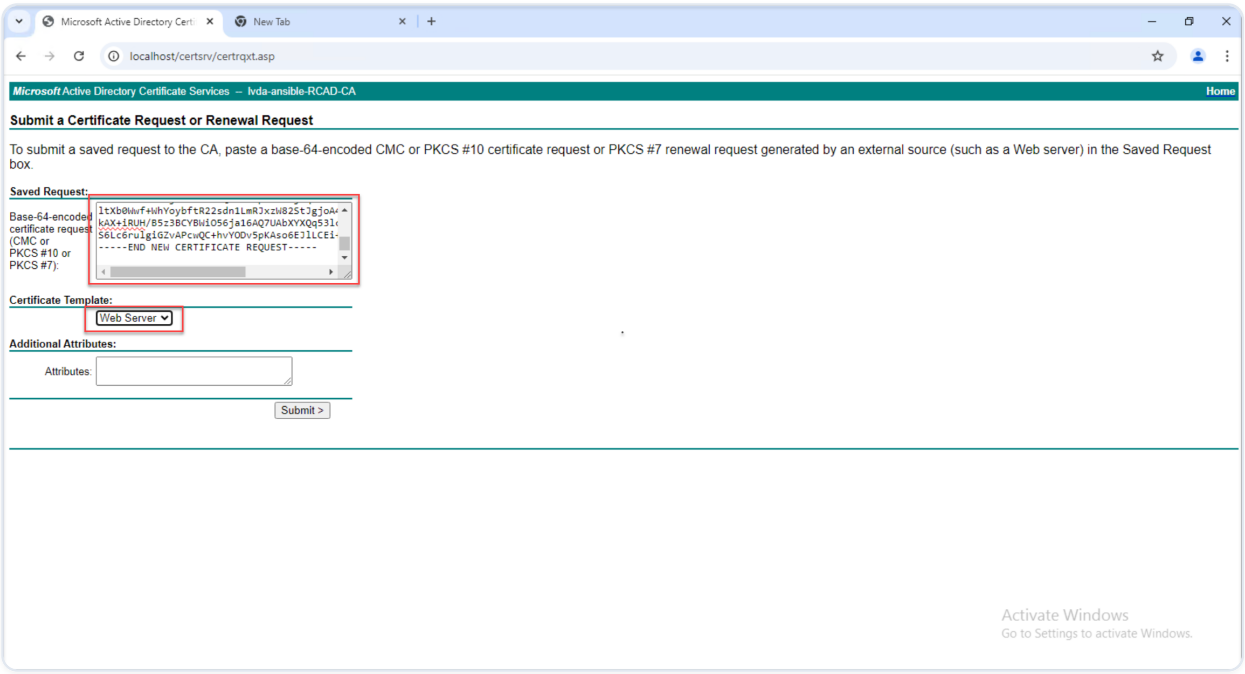


5. Inicie sesión en su servidor de certificados web y proceda a solicitar un certificado.

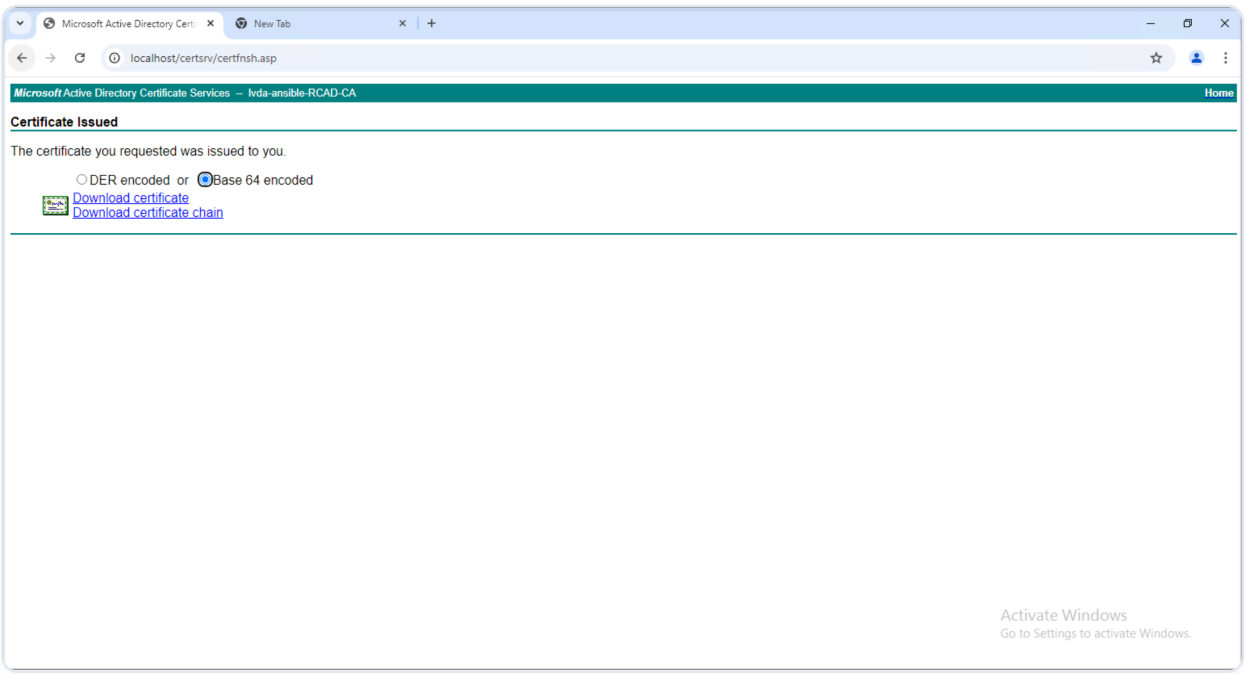




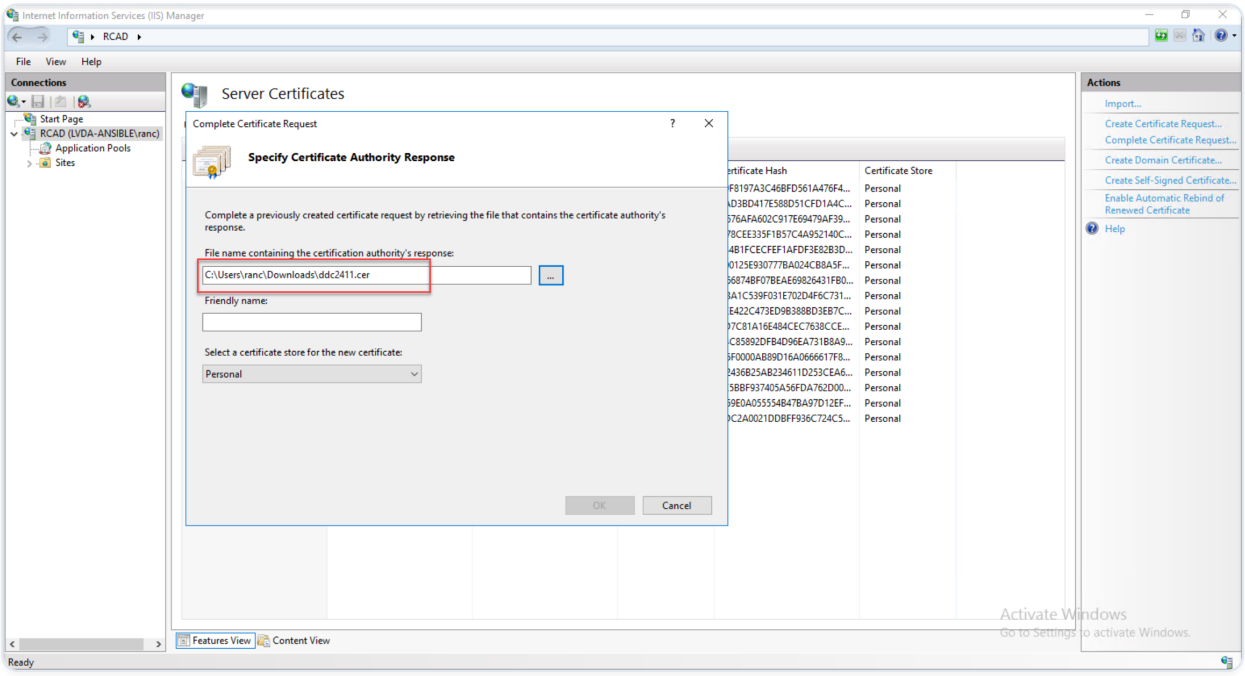
6. Pegue el contenido del archivo de solicitud copiado en el campo correspondiente del servidor web y seleccione la plantilla de certificado **Servidor web**.



7. Descargue el certificado en formato codificado Base 64.

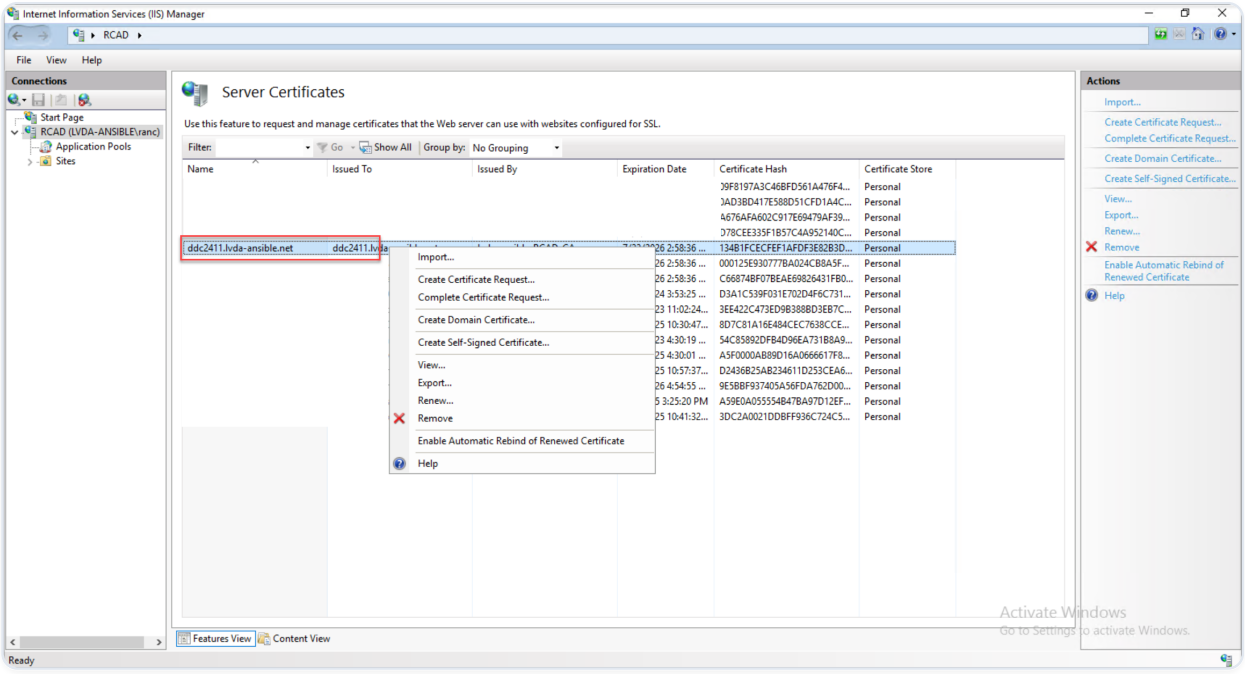


8. Complete la solicitud de certificado. Una vez descargado, el proceso de solicitud de certificado se habrá completado.

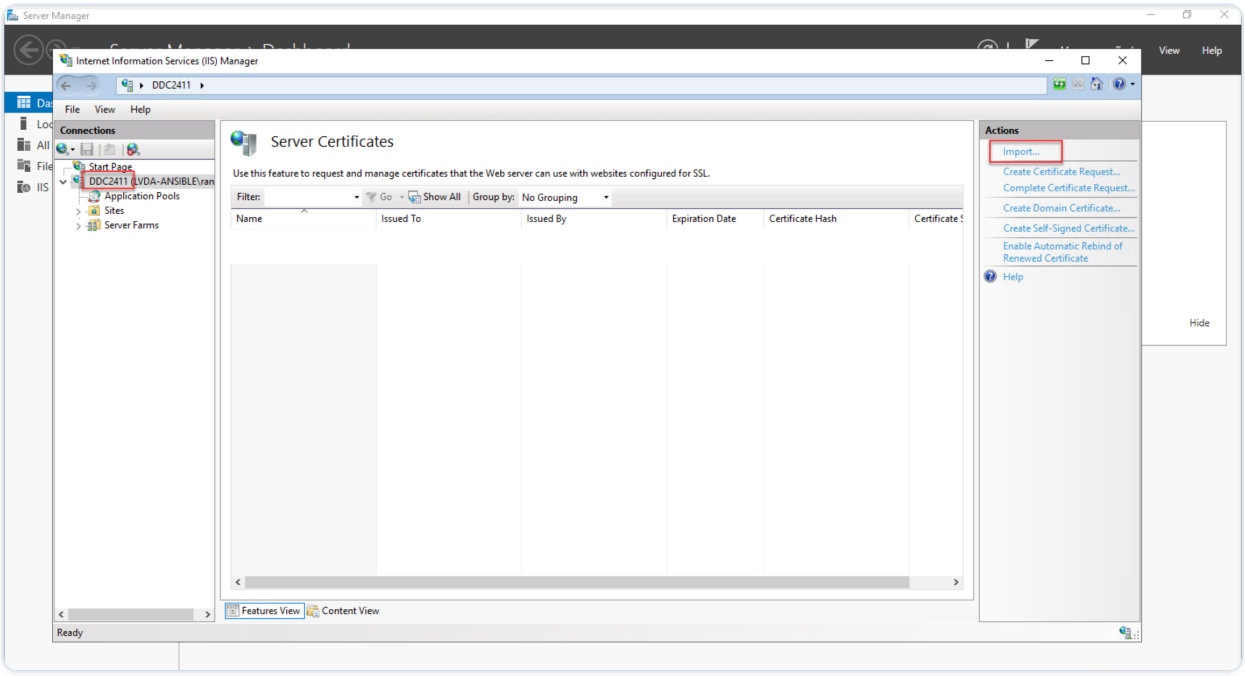


Paso 3: Vincular el certificado FQDN del Delivery Controller

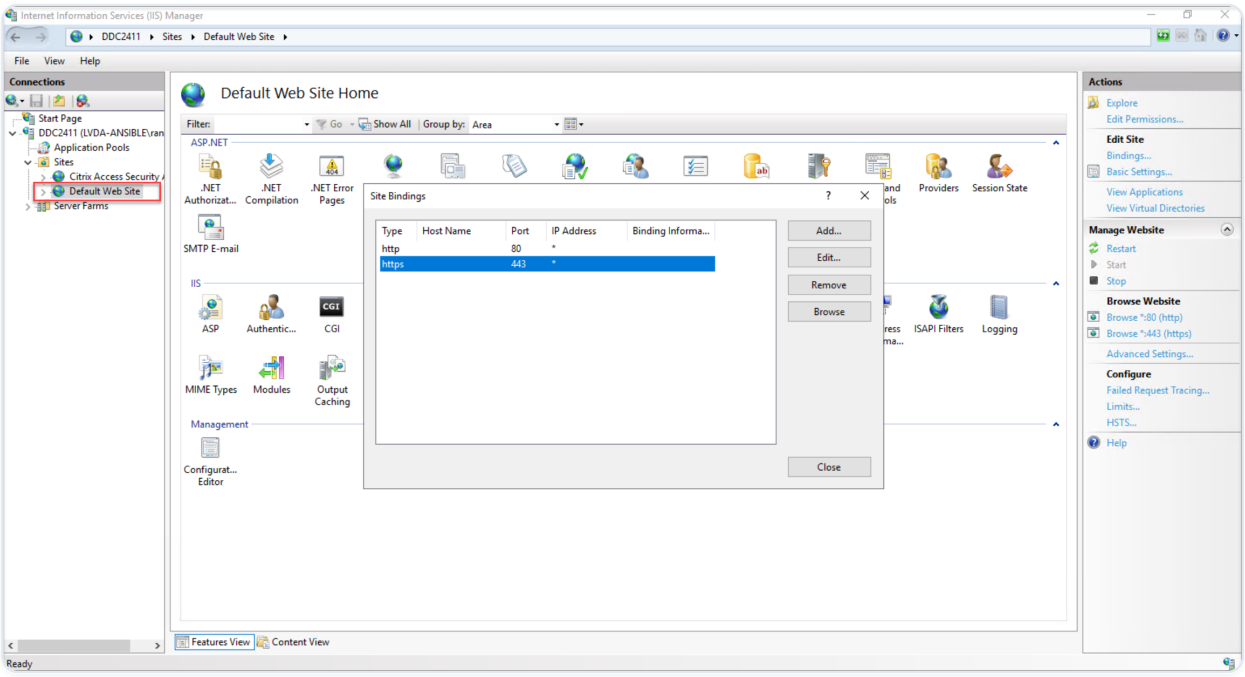
1. Exporte el certificado FQDN del Delivery Controller como un archivo PFX.



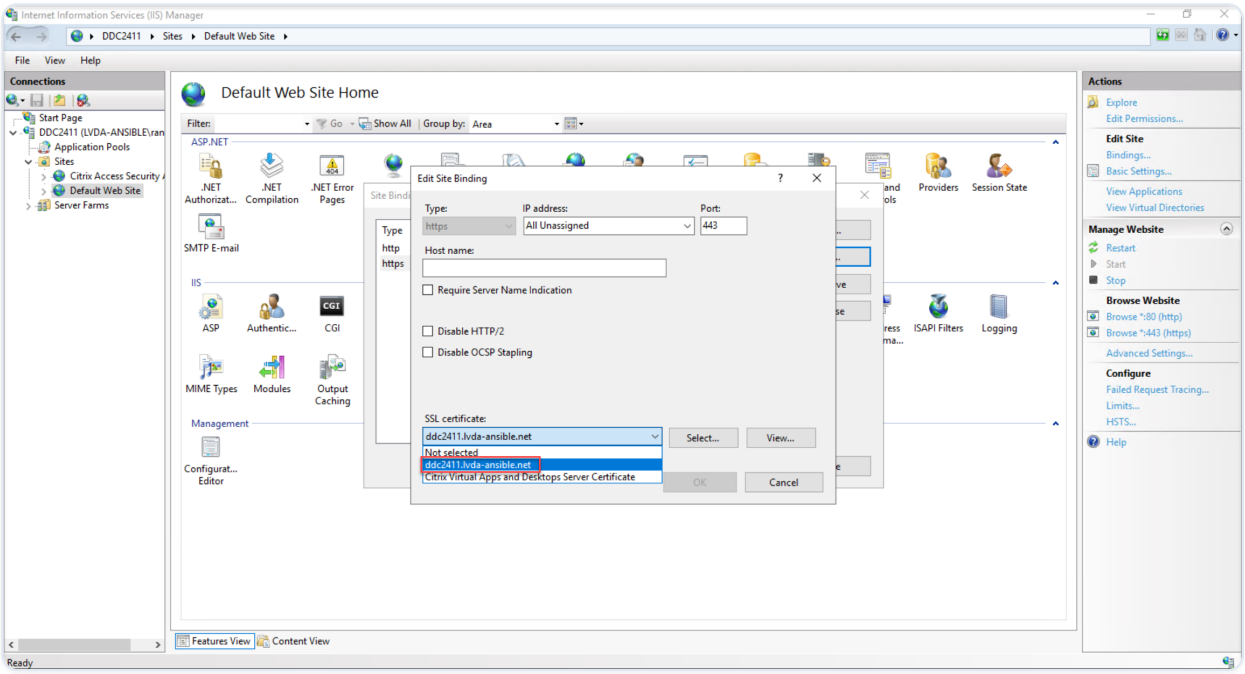
2. Importe el certificado PFX exportado en los Servicios de información de Internet (IIS) de su servidor Delivery Controller.



3. Vincule el certificado importado a su sitio web predeterminado dentro de IIS.

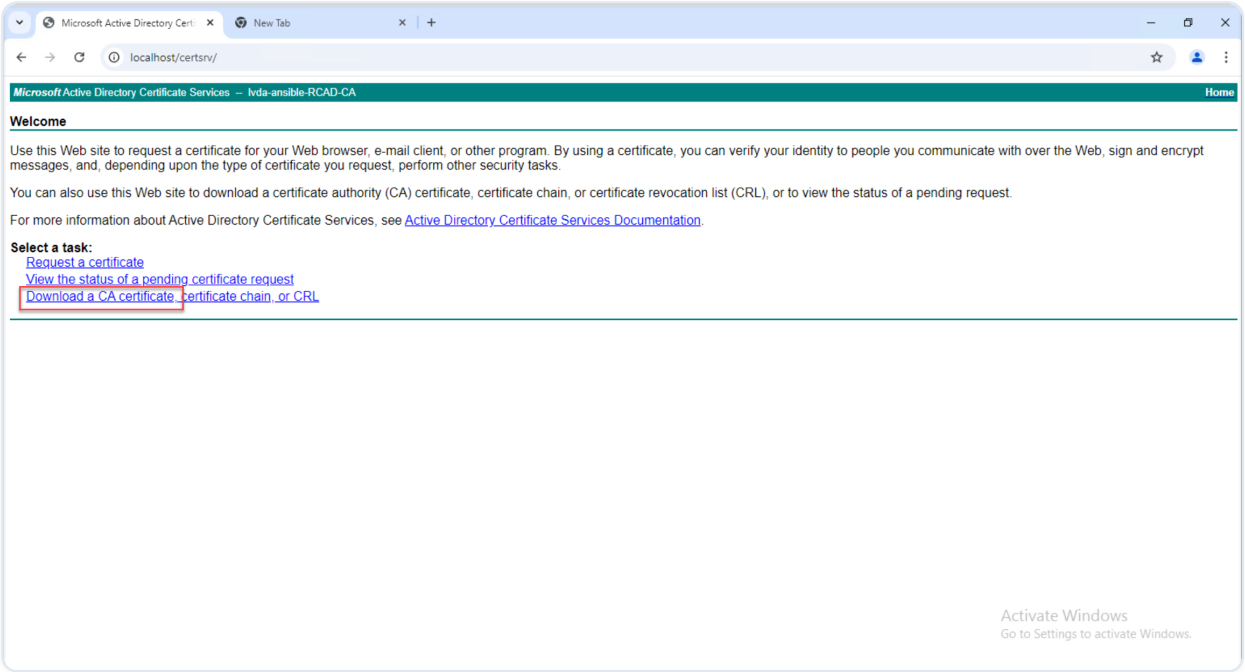


4. Durante el proceso de vinculación, asegúrese de seleccionar el certificado específico que importó.



Paso 4: Guardar y actualizar el certificado de CA en el VDA de Linux

1. Descargue el certificado de CA. Por ejemplo:



2. Coloque y actualice el certificado de CA.

   - **Para RHEL y Rocky Linux:**

     Utilice el comando **trust anchor <ruta/certificado de CA>** para añadir el certificado de CA. Asegúrese de que no se coloquen certificados manualmente en el directorio **/etc/pki/ca-trust/source/anchors**. Si encuentra errores relacionados con campos de solo lectura, elimine cualquier certificado presente en ese directorio.

- **Para SUSE, Ubuntu y Debian:**

  Coloque el certificado raíz de CA en el directorio **/usr/local/share/ca-certificates**. Si el certificado no tiene la extensión **.crt**, cámbiele el nombre según corresponda. A continuación, ejecute el comando **update-ca-certificate**.

Crear VDA de Linux en Google Cloud Platform (GCP) mediante Machine Creation Services™ (MCS)

Para crear VDA de Linux en GCP mediante MCS, complete los siguientes pasos:

Paso 1: Crear una máquina virtual (VM) Linux en GCP

Paso 2: Crear una cuenta de servicio de GCP

Paso 3: Crear una conexión de host a GCP en Citrix Studio

Paso 4: Preparar una imagen maestra de VDA de Linux

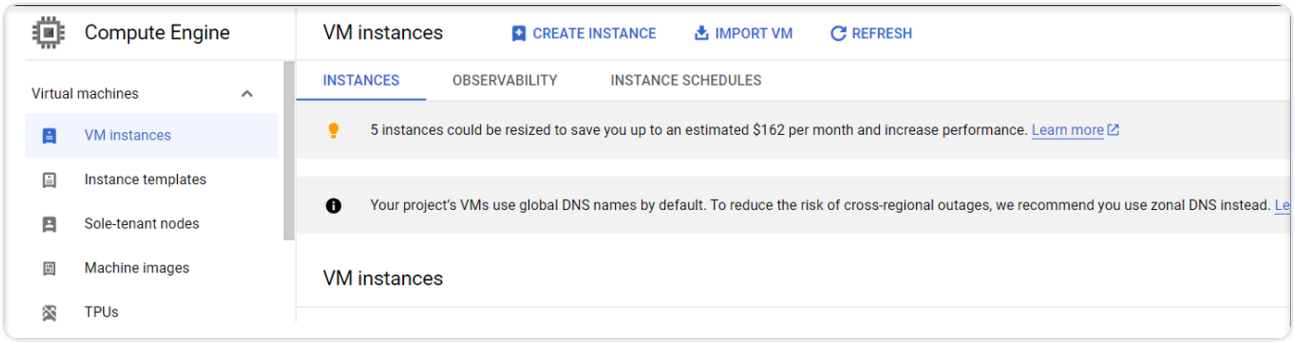
Paso 5: Crear un catálogo de máquinas

Paso 6: Crear un grupo de entrega

Paso 1: Crear una VM de Linux en GCP

Paso 1a: En la consola de Google Cloud, vaya a **Compute Engine > VM instances**.

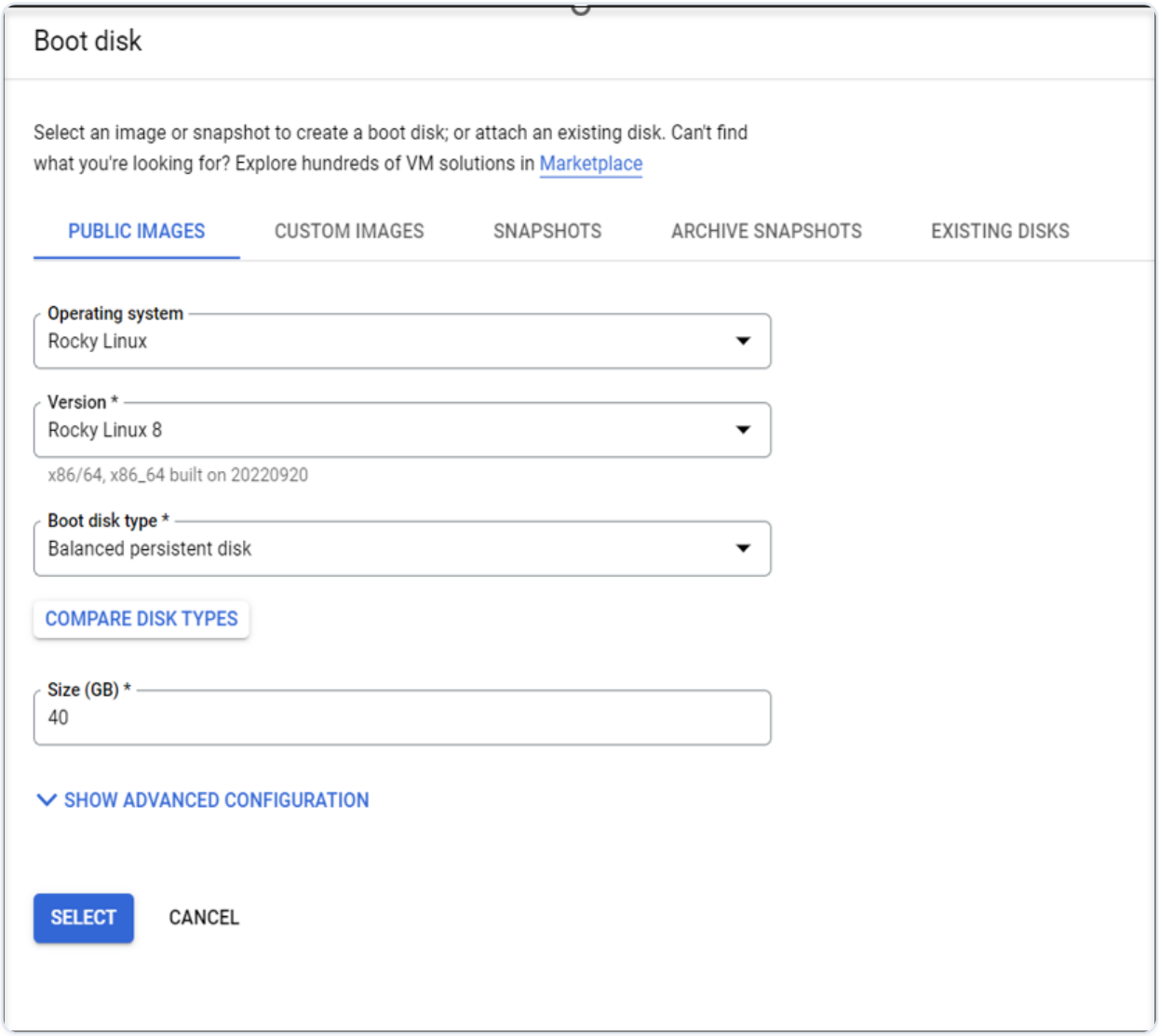
Paso 1b: En la página de instancias de VM, haga clic en **CREATE INSTANCE** para crear una instancia de VM.



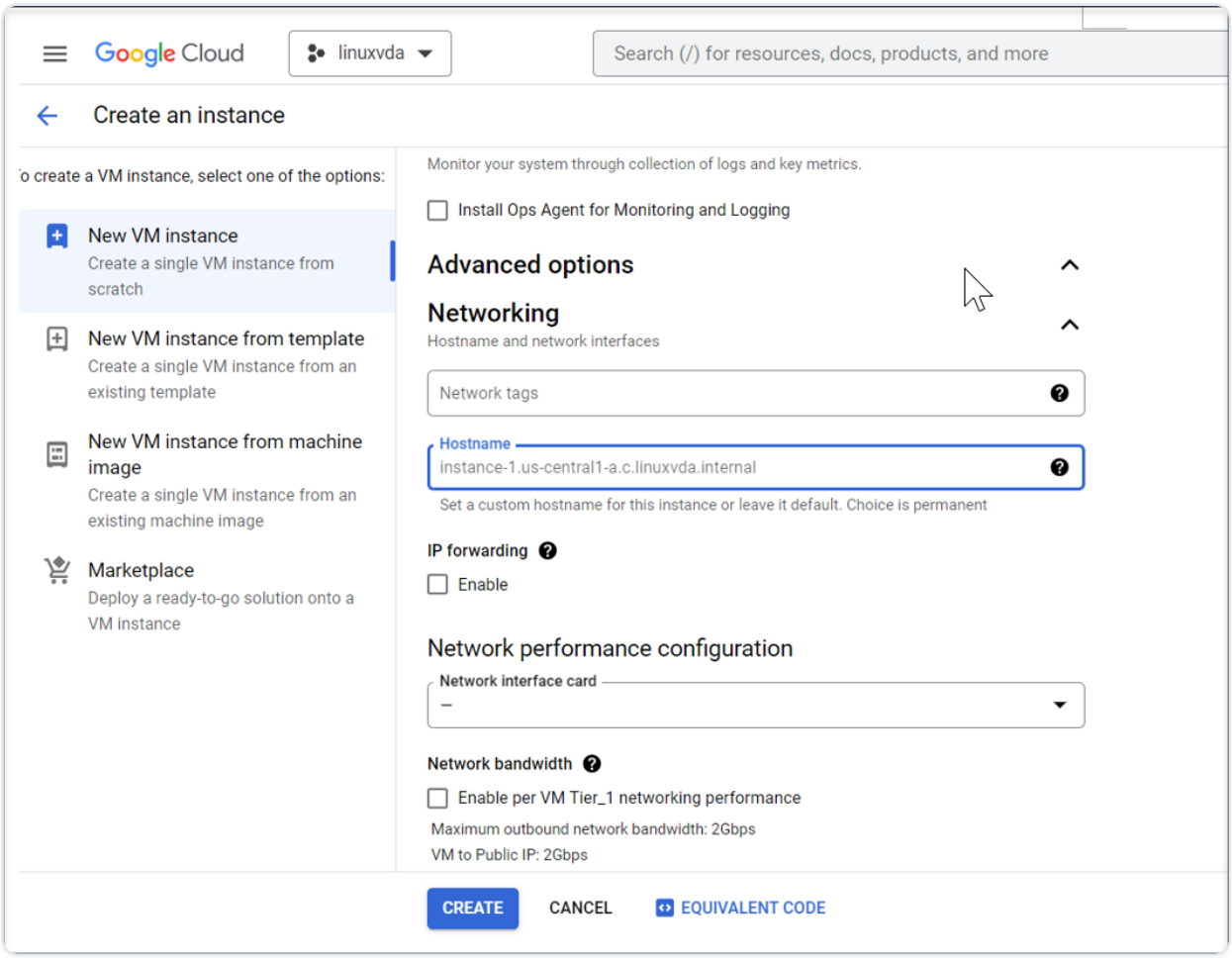
Paso 1c: Realice las siguientes configuraciones y mantenga las demás configuraciones predeterminadas:

- Introduzca un nombre para su instancia de VM.
- Seleccione una región y una zona para alojar su VM.

- (Opcional) Añada una GPU a su VM. Para obtener más información, consulte el **Paso 4c** más adelante en este artículo.
- En la sección **Disco de arranque**, seleccione el sistema operativo y el tamaño del disco para su VM. Por ejemplo:

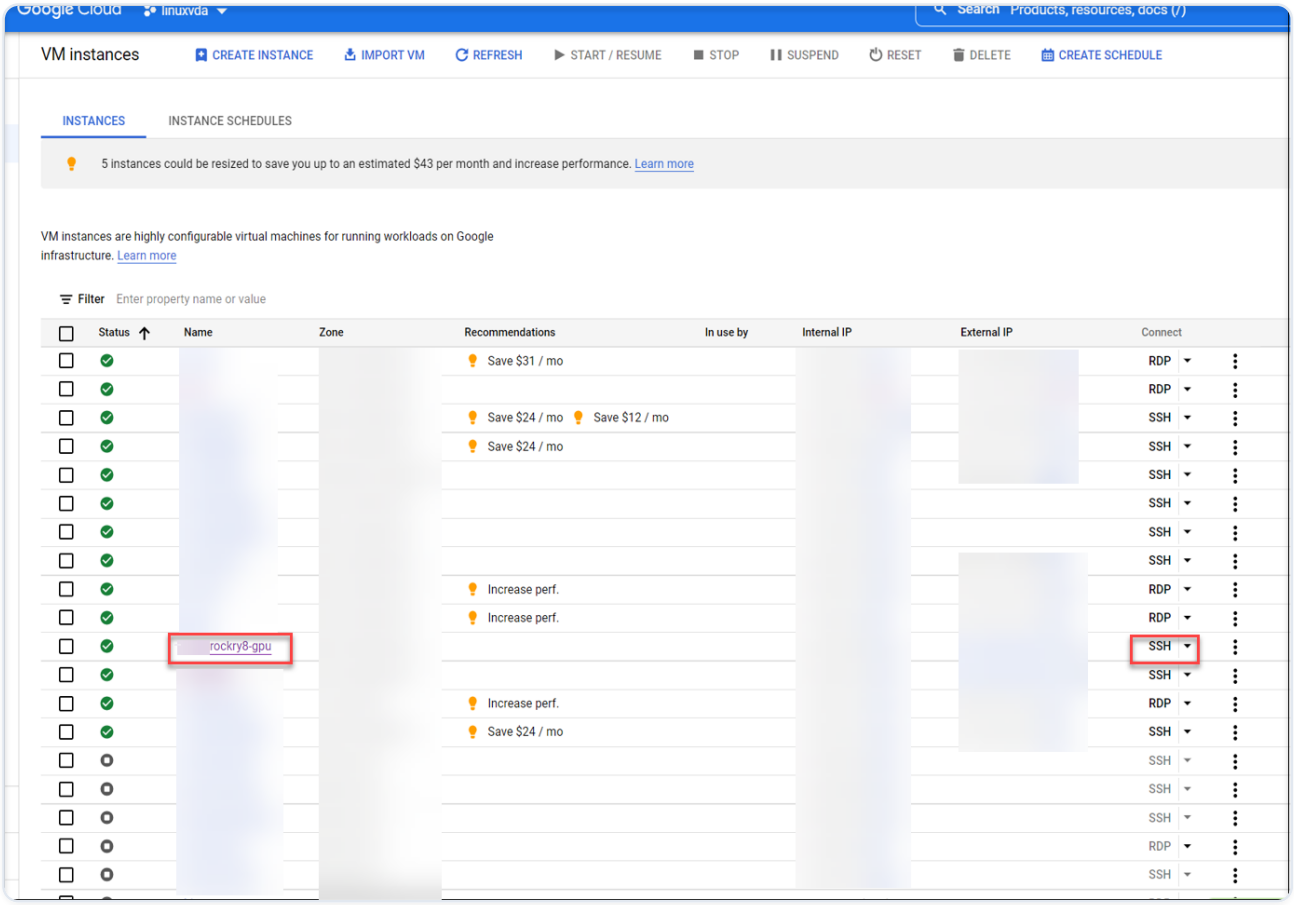


- Vaya a **Opciones avanzadas > Redes** y establezca el campo **Nombre de host** en un FQDN.

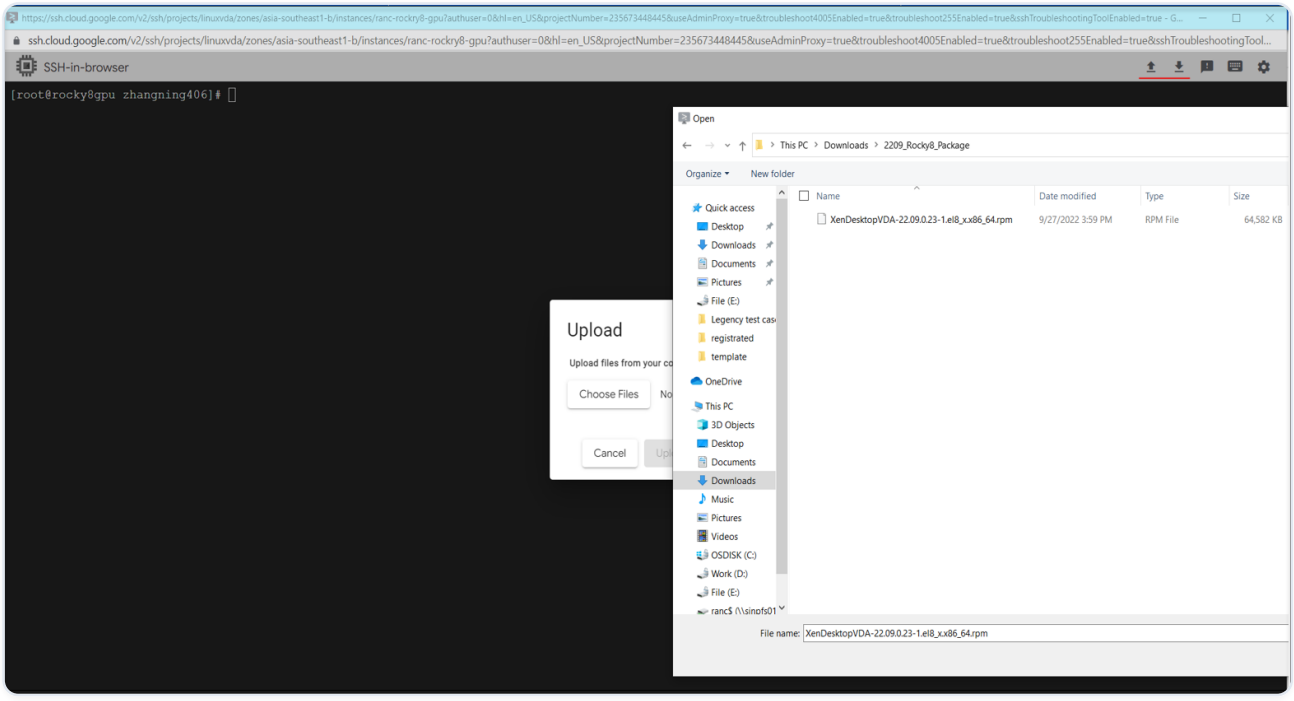


Paso 1d: Haga clic en **Crear** para crear la instancia de VM.

Paso 1e: Una vez creada la VM, vuelva al panel de control de **Compute Engine**, busque la instancia de VM en la lista y haga clic en el botón SSH para conectarse a la VM.



Paso 1f: Cargue el paquete de Linux VDA en su VM a través del cliente SSH basado en web.



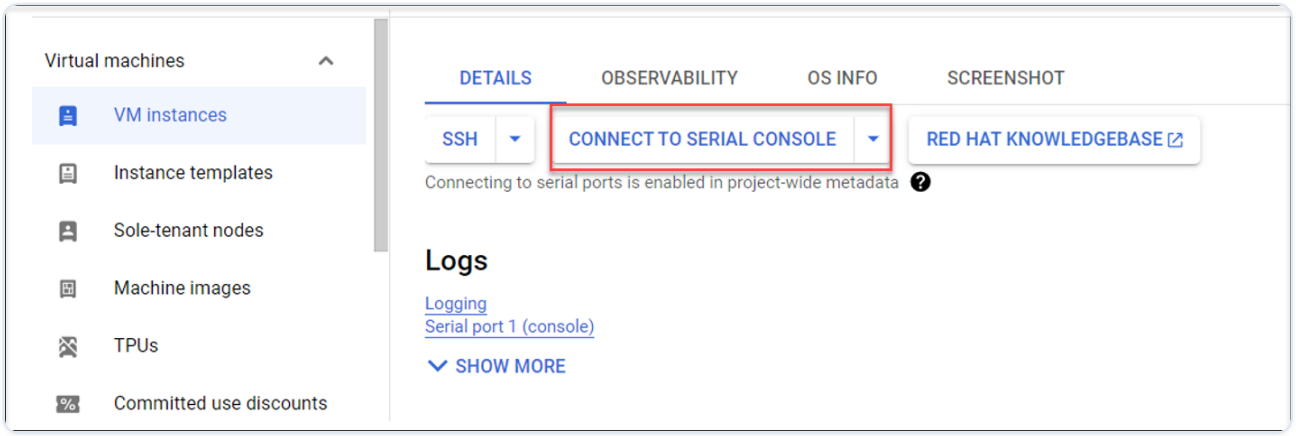
Paso 1g: Evite fallos al acceder a la VM mediante SSH.

La VM podría ser inaccesible después de un reinicio. Para solucionar el problema, establezca una contraseña de root al iniciar sesión en la VM por primera vez y asegúrese de que puede iniciar

sesión en la VM como root. Luego, ejecute los siguientes comandos en la consola después de reiniciar la VM:

```
nmcli dev connect eth0

systemctl restart NetworkManager
```

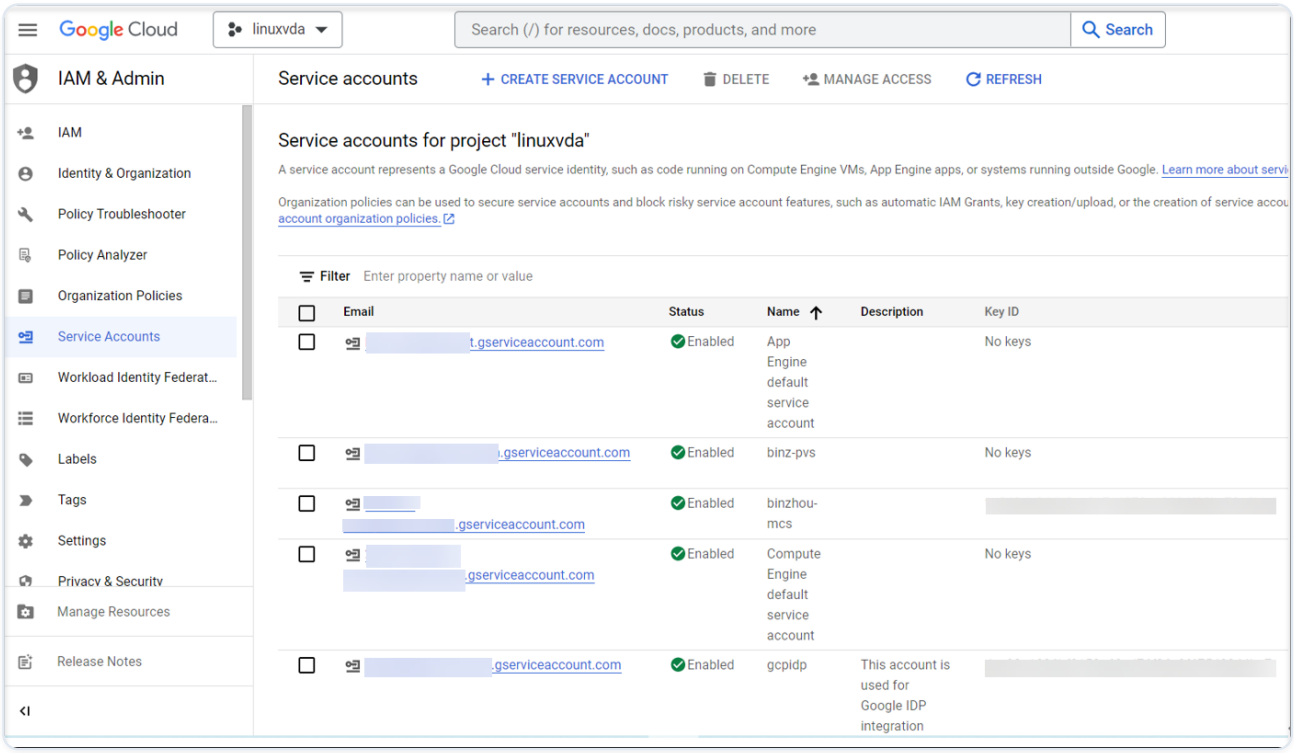


Paso 2: Crear una cuenta de servicio de GCP

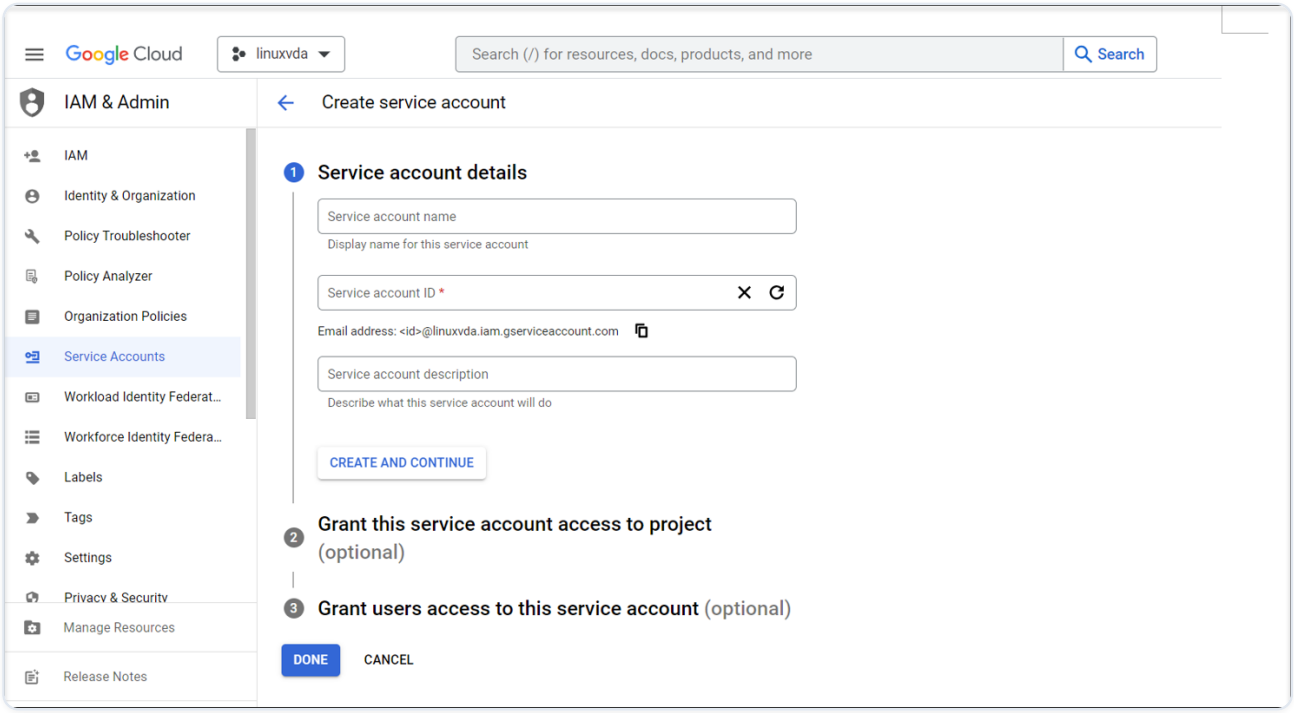
Esta sección le guía a través de la creación de una cuenta de servicio de GCP, lo que incluye la creación de una clave de cuenta de servicio y la concesión de los roles necesarios a la cuenta de servicio.

> **Nota:**
>
> Para crear una cuenta de servicio de GCP, asegúrese de que se le haya concedido el rol de IAM Administrador de cuentas de servicio (roles/iam.serviceAccountAdmin).

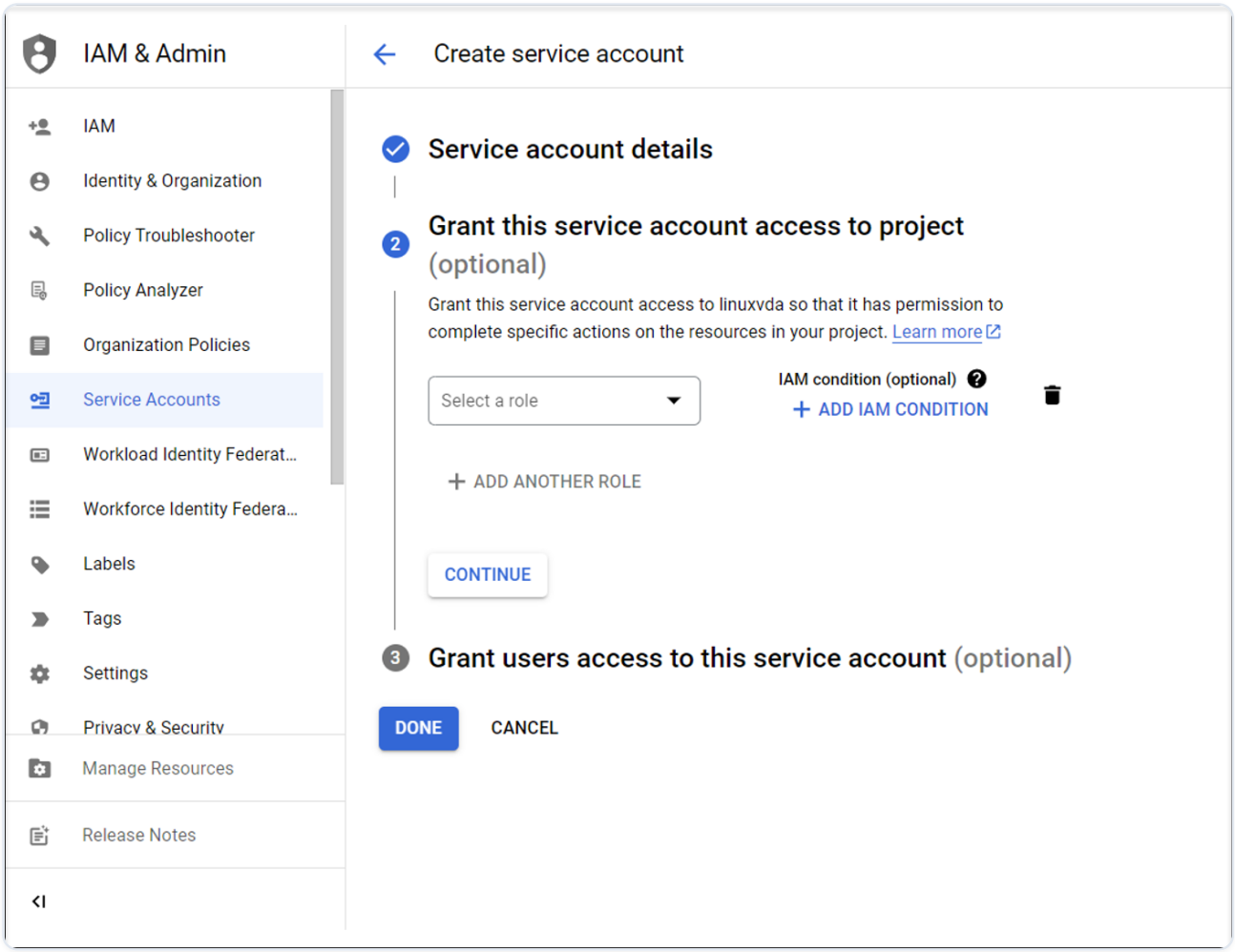
> **Paso 2a:** En la consola de Google Cloud, vaya a **IAM y administración > Cuentas de servicio** y, a continuación, haga clic en la pestaña **Crear cuenta de servicio**.



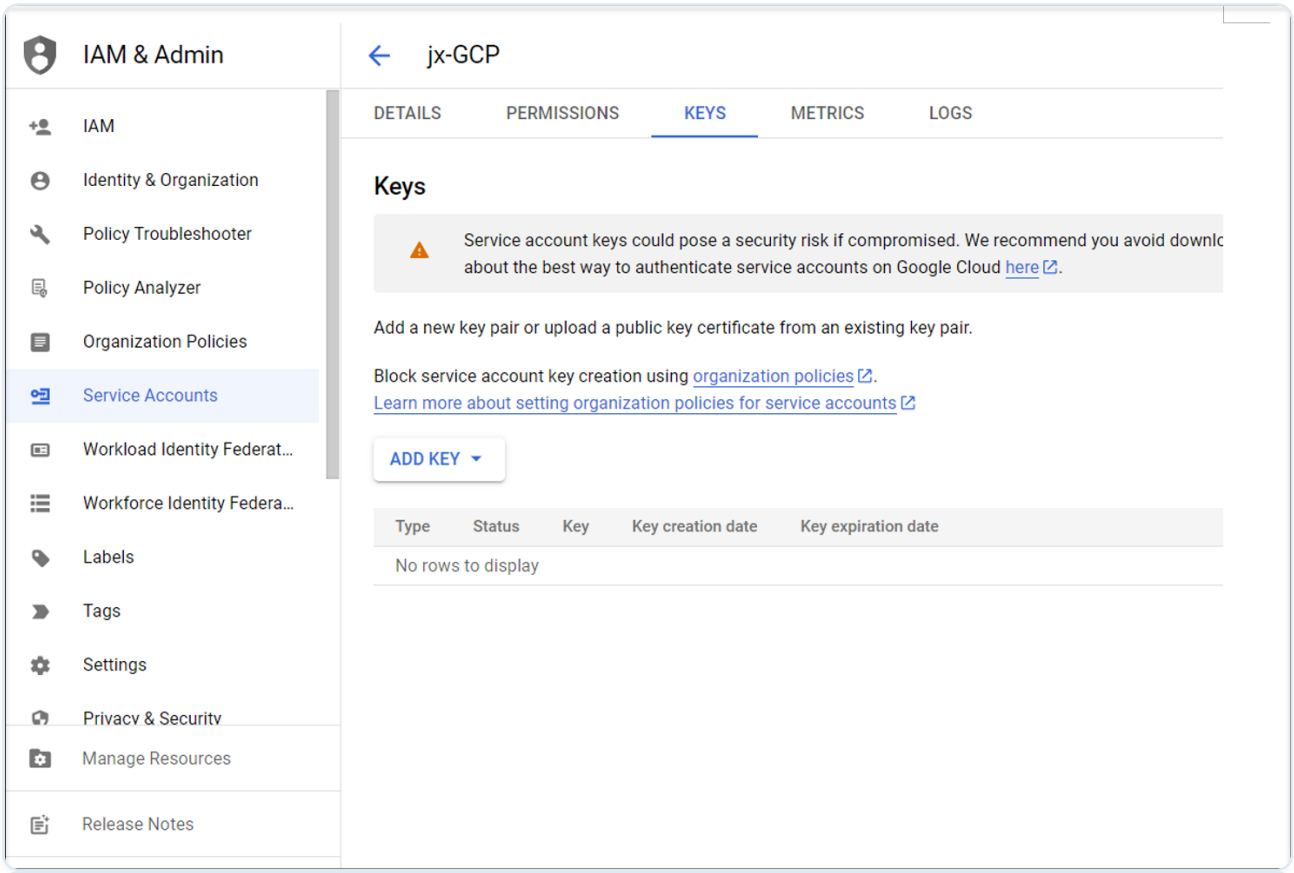
Paso 2b: En el paso **Detalles de la cuenta de servicio**, introduzca los valores en los campos y, a continuación, haga clic en **Crear y continuar**.

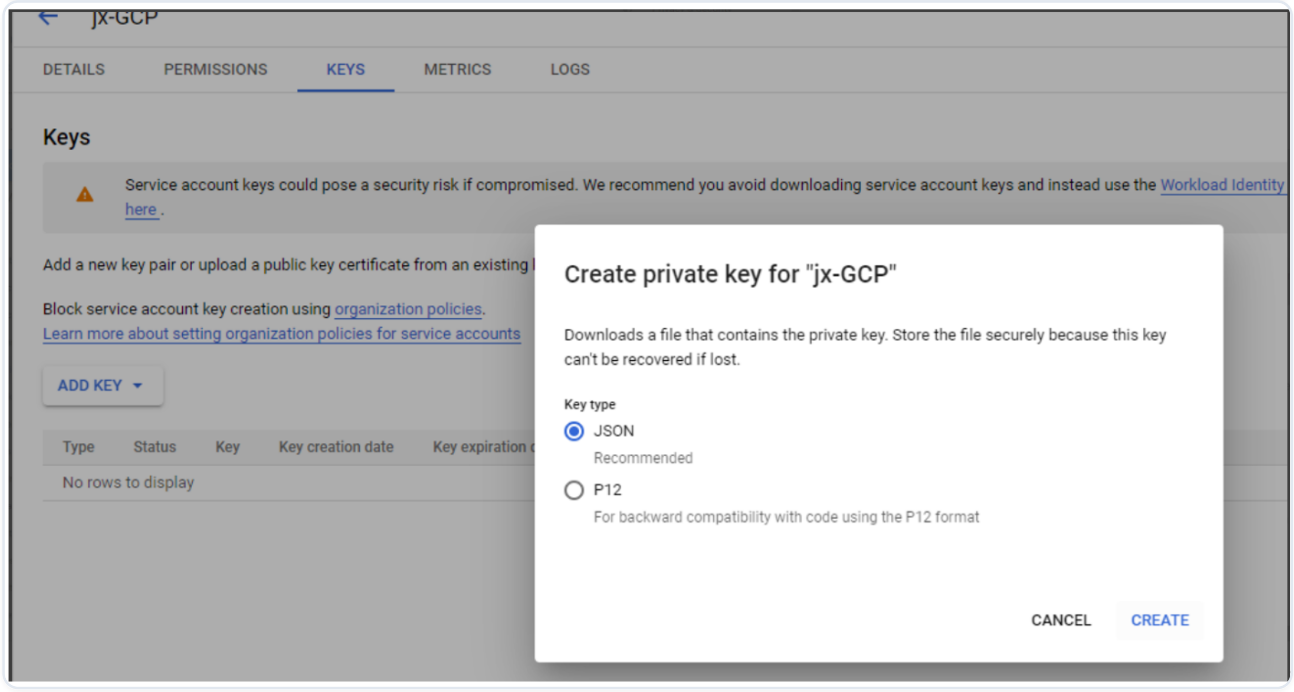


Paso 2c: Omita los pasos opcionales y haga clic en **Listo** en la parte inferior.



Paso 2d: Vaya de nuevo a **IAM y administración > Cuentas de servicio** y, a continuación, haga clic en la pestaña **Cuentas de servicio**. Busque la cuenta de servicio recién creada, vaya a la pestaña **Claves** y, a continuación, haga clic en **Añadir clave > Crear nueva clave > JSON > Crear**.





Nota:

Una vez que descargue el archivo de claves, no podrá volver a descargarlo.

> **Paso 2e:** En la consola de Google Cloud, vaya a **IAM y administración > IAM** y, a continuación, haga clic en **Añadir**. Busque y seleccione la cuenta de servicio recién creada en el campo **Nuevos miembros** y, a continuación, seleccione un rol para la cuenta de servicio para concederle acceso a sus recursos. Siga concediendo roles haciendo clic en **Añadir otro rol** para asegurarse de conceder todos los roles siguientes a la cuenta de servicio recién creada.

- **Administrador de Compute**
- **Administrador de Storage**
- **Editor de Cloud Build**
- **Usuario de cuenta de servicio**
- **Usuario de Cloud Datastore**
- **Administrador de instancias de Compute (beta)**
- **Propietario**

Por ejemplo:

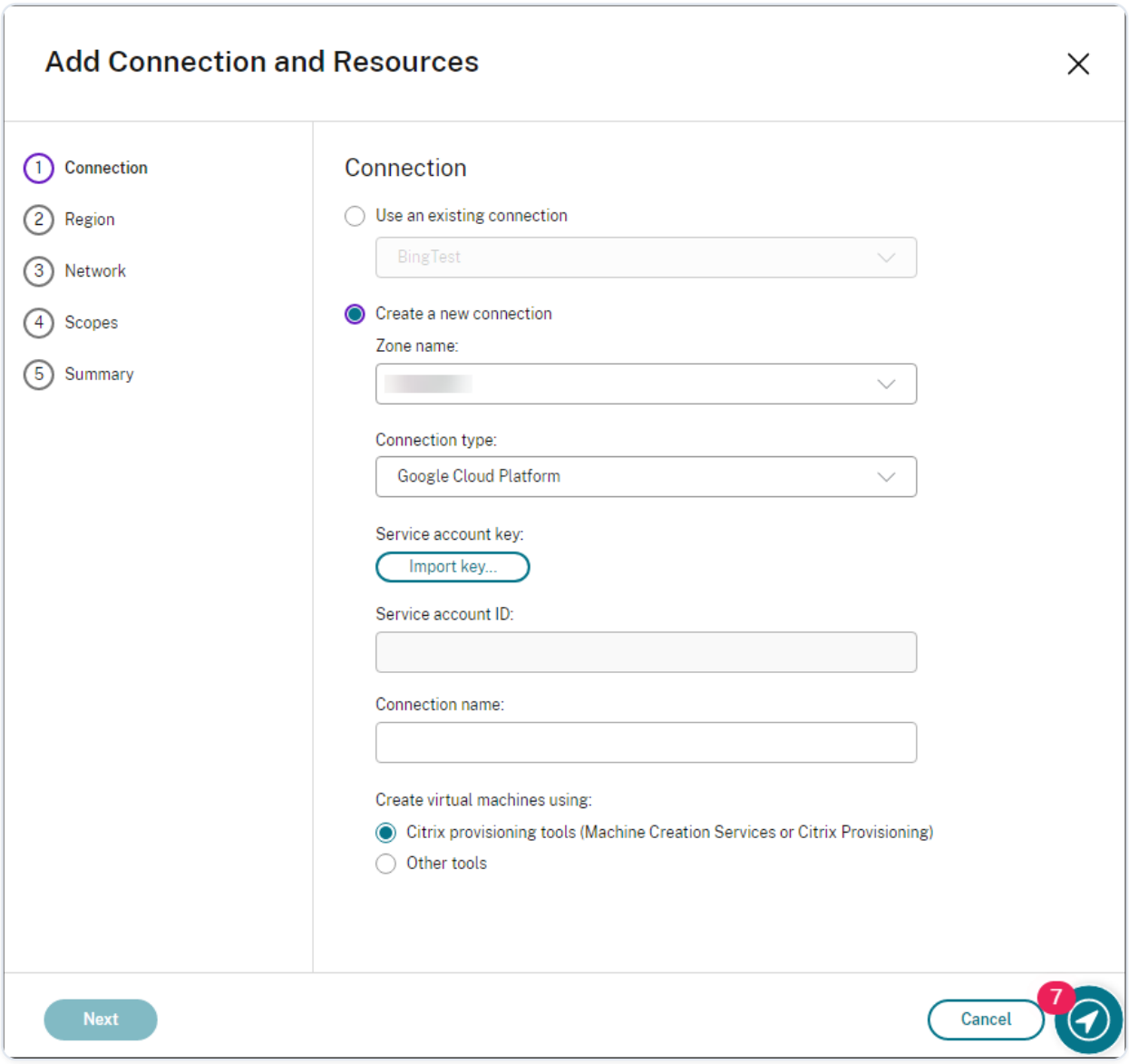


Paso 3: Crear una conexión de host a GCP en Citrix Studio

Configure su entorno de GCP según Google Cloud Platform virtualization environments y, a continuación, complete los siguientes pasos para crear una conexión de host a GCP.

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local para crear una conexión de host. Para los Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola de Studio basada en web en Citrix Cloud™ para crear una conexión de host.
2. En el asistente **Agregar conexión y recursos**, seleccione **Google Cloud Platform** como tipo de conexión.

   Por ejemplo, en la consola de Studio basada en web de Citrix Cloud:



3. Importe la clave de cuenta de servicio de su cuenta de GCP y escriba el nombre de la conexión.
4. El asistente le guiará por las páginas. El contenido específico de la página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte Paso 2: Crear una conexión de host en el artículo Crear VDA de Linux no unidos a un dominio mediante MCS.

Paso 4: Preparar una imagen maestra de VDA de Linux

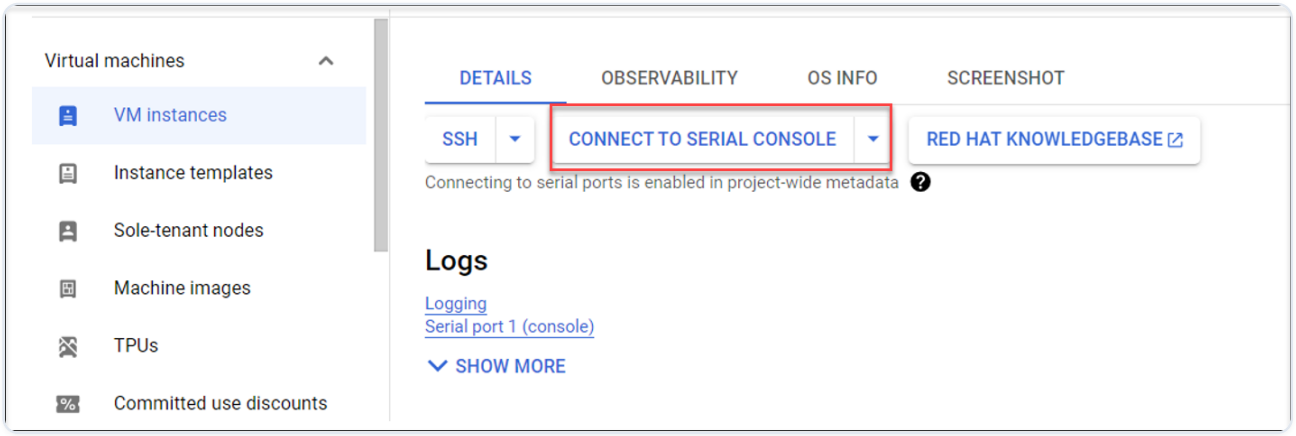
Paso 4a: (Para RHEL 8.x/9.x y Rocky Linux 8.x/9.x) Configurar la conexión Ethernet.

Después de instalar el VDA de Linux en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, la conexión Ethernet podría perderse y el VDA de Linux podría quedar inaccesible después de reiniciar una VM. Para solucionar el problema, establezca una contraseña de root al iniciar sesión

en la VM por primera vez y asegúrese de que puede iniciar sesión en la VM como root. A continuación, ejecute los siguientes comandos en la consola después de reiniciar la VM:

```
nmcli dev connect eth0

systemctl restart NetworkManager
```



Paso 4b: Instale el paquete de VDA de Linux en la VM de plantilla.

En la VM de plantilla, haga lo siguiente para instalar el paquete de VDA de Linux:

1. Instale .NET.

   Además de .NET Runtime, debe instalar .ASP.NET Core Runtime versión 8 en todas las distribuciones de Linux compatibles antes de instalar o actualizar el VDA de Linux.

   Si su distribución de Linux contiene la versión de .NET que necesita, instálela desde la fuente integrada. De lo contrario, instale .NET desde la fuente de paquetes de Microsoft. Para obtener más información, consulte `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

2. Instale el paquete de VDA de Linux:

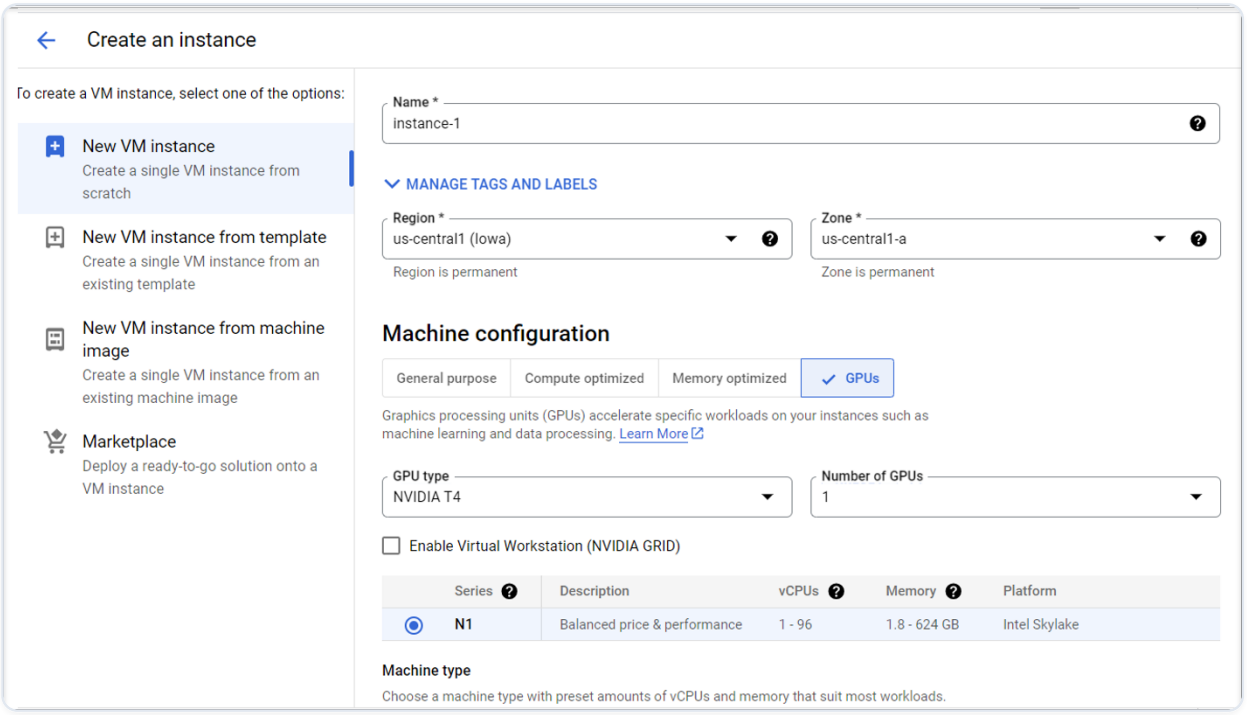
   ```
   sudo yum –y localinstall <PATH>/<Linux VDA RPM>
   ```

3. Habilite el repositorio EPEL:

   ```
   sudo rpm -ivh  https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

Paso 4c: Agregue una unidad de procesamiento gráfico (GPU) a la VM de plantilla en GCP (opcional).

1. En la consola de Google Cloud, agregue una o varias GPU a la VM de plantilla. Para obtener información sobre cómo agregar y quitar GPU en GCP, consulte `<https://cloud.google.com/compute/docs/gpus/add-remove-gpus>`.



2. Instale el controlador de GPU adecuado en la VM de plantilla. Para obtener más información, consulte `<https://cloud.google.com/compute/docs/gpus/install-drivers-gpu>`.

   Versiones de controlador NVIDIA requeridas:

   Las GPU NVIDIA que se ejecutan en Compute Engine deben usar las siguientes versiones de controlador NVIDIA:

   - Para GPU L4:
     - Linux : 525.60.13 o posterior
   - Para GPU A100:
     - Linux : 450.80.02 o posterior
   - Para GPU T4, P4, P100 y V100:
     - Linux : 410.79 o posterior
   - Para GPU K80 (Fin de vida útil):
     - Linux : 410.79 - última versión R470

Para las GPU K80, NVIDIA ha anunciado que la rama controlador R470 es la versión final del controlador que recibirá soporte de depuración. Para revisar esta actualización, consulte Matriz de soporte de software de NVIDIA.

Script de instalación:

Puede utilizar el siguiente script para automatizar el proceso de instalación:

```
https://raw.githubusercontent.com/GoogleCloudPlatform/compute-gpu-installation/main/linux/install_gpu_driver.py --output install_gpu_driver.py
```

Sistemas operativos compatibles:

El script de instalación se probó en las siguientes distribuciones de Linux:

- Debian 11
- Red Hat Enterprise Linux (RHEL) 8
- Rocky Linux 8
- Ubuntu 20/22

Si utiliza este script en otras distribuciones de Linux, la instalación fallará. Para las máquinas virtuales Linux, este script solo instala el controlador NVIDIA.

a. Descargue el script de instalación.

```
curl https://raw.githubusercontent.com/GoogleCloudPlatform/compute-gpu-installation/main/linux/install_gpu_driver.py --output install_gpu_driver.py
```

b. Conceda acceso completo al script.

```
chmod 777 install_gpu_driver.py
```

c. Ejecute el script de instalación.

```
python3 install_gpu_driver.py
```

d. Deshabilite Wayland en gdm3.

- Busque el archivo de configuración de Wayland de su distribución en una de las siguientes ubicaciones:
  - /etc/gdm3/custom.conf (Ubuntu)
  - /etc/gdm/custom.conf (CentOS, RHEL, Rocky Linux)
- Abra el archivo con privilegios de sudo/root.
- Quite el comentario de **WaylandEnable=false** eliminando el # al principio de la línea.
- Reinicie la máquina virtual.

e. Si instaló un controlador NVIDIA 510 o posterior, deshabilite el firmware GSP.

Si el firmware GSP está habilitado, desactívelo configurando el parámetro del módulo NVIDIA **NVreg_EnableGpuFirmware** en 0.

Establezca este parámetro añadiendo la siguiente entrada al archivo /etc/modprobe.d/nvidia.conf:

- opciones nvidia NVreg_EnableGpuFirmware=0
- Si el archivo /etc/modprobe.d/nvidia.conf no existe, créelo.

Al completar este paso, tenga en cuenta lo siguiente:

- Use sudo para ejecutar los comandos para crear y actualizar el archivo de configuración.
- Para reiniciar la VM, puede usar **sudo reboot** en el terminal de Linux o detener e iniciar la VM.

Paso 4d: Configure las variables de MCS.

Configure las variables de MCS editando el archivo /etc/xdl/mcs/mcs.conf. Las siguientes son variables de MCS que puede configurar para escenarios sin unión a dominio y con unión a dominio:

- **Para escenarios sin unión a dominio**

  Puede usar los valores predeterminados de las variables o personalizarlas según sea necesario (opcional):

  `DOTNET_RUNTIME_PATH` =*ruta-de-instalación-de-dotnet-runtime **

  `DESKTOP_ENVIRONMENT` = *gnome | mate ** `REGISTER_SERVICE` =**S | N**

`ADD_FIREWALL_RULES`=**S | N** `VDI_MODE`=**S | N**

`START_SERVICE`=**S | N**

```
#########################Linux VDA Configuration#################################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/usr/bin
DESKTOP_ENVIRONMENT=gnome
SUPPORT_DDC_AS_CNAME=N
VDA_PORT=80
REGISTER_SERVICE=Y
ADD_FIREWALL_RULES=Y
HDX_3D_PRO=N
VDI_MODE=N
SITE_NAME='<none>'
LDAP_LIST='<none>'
SEARCH_BASE='<none>'
START_SERVICE=Y
```

- **Para escenarios con unión a dominio**
  - `Use_AD_Configuration_Files_Of_Current_VDA`: Determina si se deben usar los archivos de configuración relacionados con AD existentes (/etc/krb5.conf, /etc/sssd.conf y /etc/samba/smb.conf) del VDA que se está ejecutando actualmente. Si se establece en Y, los archivos de configuración de las máquinas creadas por MCS son los mismos que los equivalentes en el VDA que se está ejecutando actualmente. Sin embargo, aún debe configurar las variables `dns` y `AD_INTEGRATION`. El valor predeterminado es N, lo que significa que las plantillas de configuración de la imagen maestra determinan los archivos de configuración de las máquinas creadas por MCS. Para usar un VDA que se está ejecutando actualmente como VM de plantilla, establezca el valor en Y. De lo contrario, establézcalo en N.
  - `dns`: Establece la dirección IP de cada servidor DNS. Puede configurar hasta cuatro servidores DNS.
  - `NTP_SERVER`: Establece la dirección IP de su servidor NTP. A menos que se especifique lo contrario, es la dirección IP de su controlador de dominio.
  - `WORKGROUP`: Establece el nombre del grupo de trabajo como el nombre NetBIOS (distingue mayúsculas y minúsculas) que configuró en AD. De lo contrario, MCS utiliza la parte del nombre de dominio que sigue inmediatamente al nombre de host de la máquina como nombre del grupo de trabajo. Por ejemplo, si la cuenta de la máquina es **user1.lvda.citrix.com**, MCS utiliza **lvda** como nombre del grupo de trabajo, mientras que **citrix** es la opción correcta. Asegúrese de establecer el nombre del grupo de trabajo correctamente.

- `AD_INTEGRATION`: Establece Winbind, SSSD, PBIS o Centrify. Para ver una matriz de las distribuciones de Linux y los métodos de unión a dominios que admite MSC, consulte Distribuciones admitidas.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete Server Suite Free (anteriormente Centrify Express). El valor solo surte efecto cuando se establece la variable `AD_INTEGRATION` en Centrify.
- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete Centrify Samba. El valor solo surte efecto cuando se establece la variable `AD_INTEGRATION` en Centrify.
- `PBIS_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete PBIS. El valor solo surte efecto cuando se establece la variable `AD_INTEGRATION` en PBIS.
- `UPDATE_MACHINE_PW`: Habilita o deshabilita la automatización de las actualizaciones de contraseñas de las cuentas de máquina. Para obtener más información, consulte Automatizar las actualizaciones de contraseñas de las cuentas de máquina.
- Variables de configuración de Linux VDA:

  `DOTNET_RUNTIME_PATH`=*path-to-install-dotnet-runtime **

  `DESKTOP_ENVIRONMENT`= *gnome | mate ** `SUPPORT_DDC_AS_CNAME`=**S | N**

  `VDA_PORT`=**número-de-puerto** `REGISTER_SERVICE`=**S | N**

  `ADD_FIREWALL_RULES`=**S | N** `HDX_3D_PRO`=**S | N**

  `VDI_MODE`=**S | N** `SITE_NAME`=**dns-site-name | '<none\>'**

  `LDAP_LIST`=**'list-ldap-servers' | '<none\>'** `SEARCH_BASE`=**search-base-set | '<none\>'**

  `FAS_LIST`=**'list-fas-servers' | '<none\>'** `START_SERVICE`=**S | N**

  `TELEMETRY_SOCKET_PORT`=**número-de-puerto** `TELEMETRY_PORT`=**número-de-puerto**

Paso 4e: Crear una imagen maestra

1. (Solo para SSSD + RHEL 8.x/9.x o Rocky Linux 8.x/9.x) Ejecute el comando `update-crypto-policies --set DEFAULT:AD-SUPPORT` y, a continuación, reinicie la VM de plantilla.
2. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.

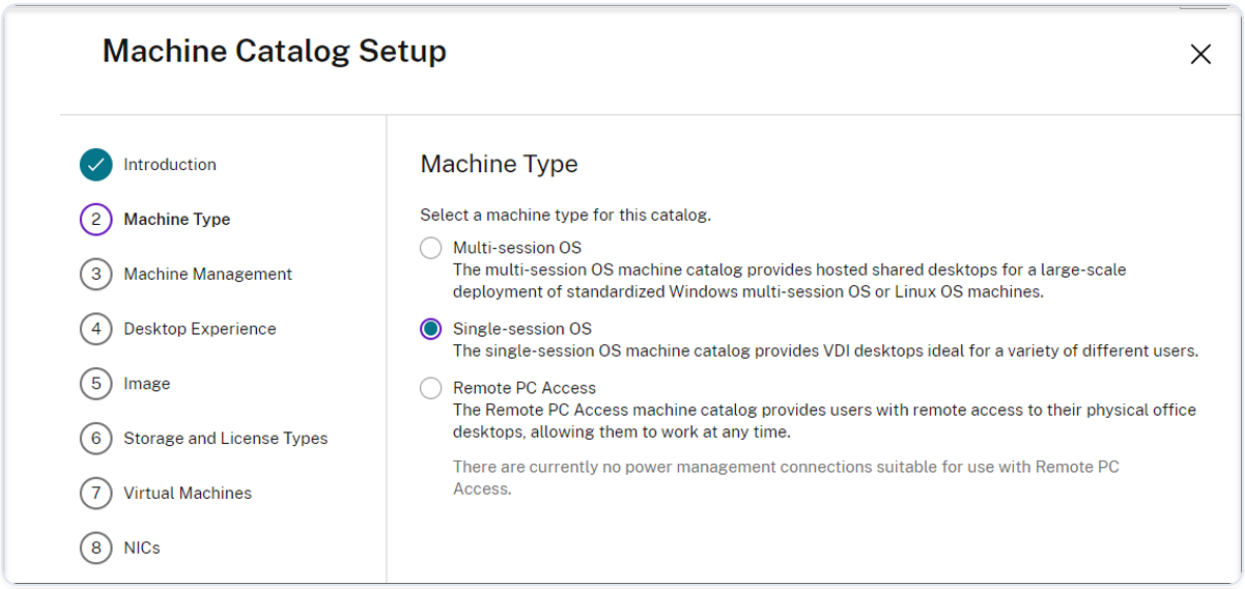
   Para escenarios sin unión a dominio, el siguiente error es normal y no impide continuar.

```
[root@localhost ~]#
[root@localhost ~]# /opt/Citrix/VDA/sbin/deploymcs.sh
Installing Linux VDA dependency packages ...
Installing package redhat-lsb-core
Installing package nautilus
Installing package totem-nautilus
Installing package brasero-nautilus
Installing package pulseaudio
Installing package pulseaudio-module-x11
Installing package pulseaudio-gdm-hooks
Installing package pulseaudio-module-bluetooth
Installing package alsa-plugins-pulseaudio
Installing package pciutils
Installing package openssh
Installing package openssh-clients
Installing package java-11-openjdk
Installing package chrony
Installing package krb5-workstation
Installing package oddjob-mkhomedir
Starting PostgreSQL database ...
Installing package tdb-tools
Installing package ntfs-3g
/opt/Citrix/VDA/lib64/mcs ~
installing mcs systemd unit file: ad_join.service ...
~
/opt/Citrix/VDA/lib64/mcs ~
~
Installing winbind dependency packages ...
Installing package samba-winbind
Installing package samba-winbind-clients
ERROR: Exit funtion conf_dns, dns not configured, please do it manually.
[root@localhost ~]#
```

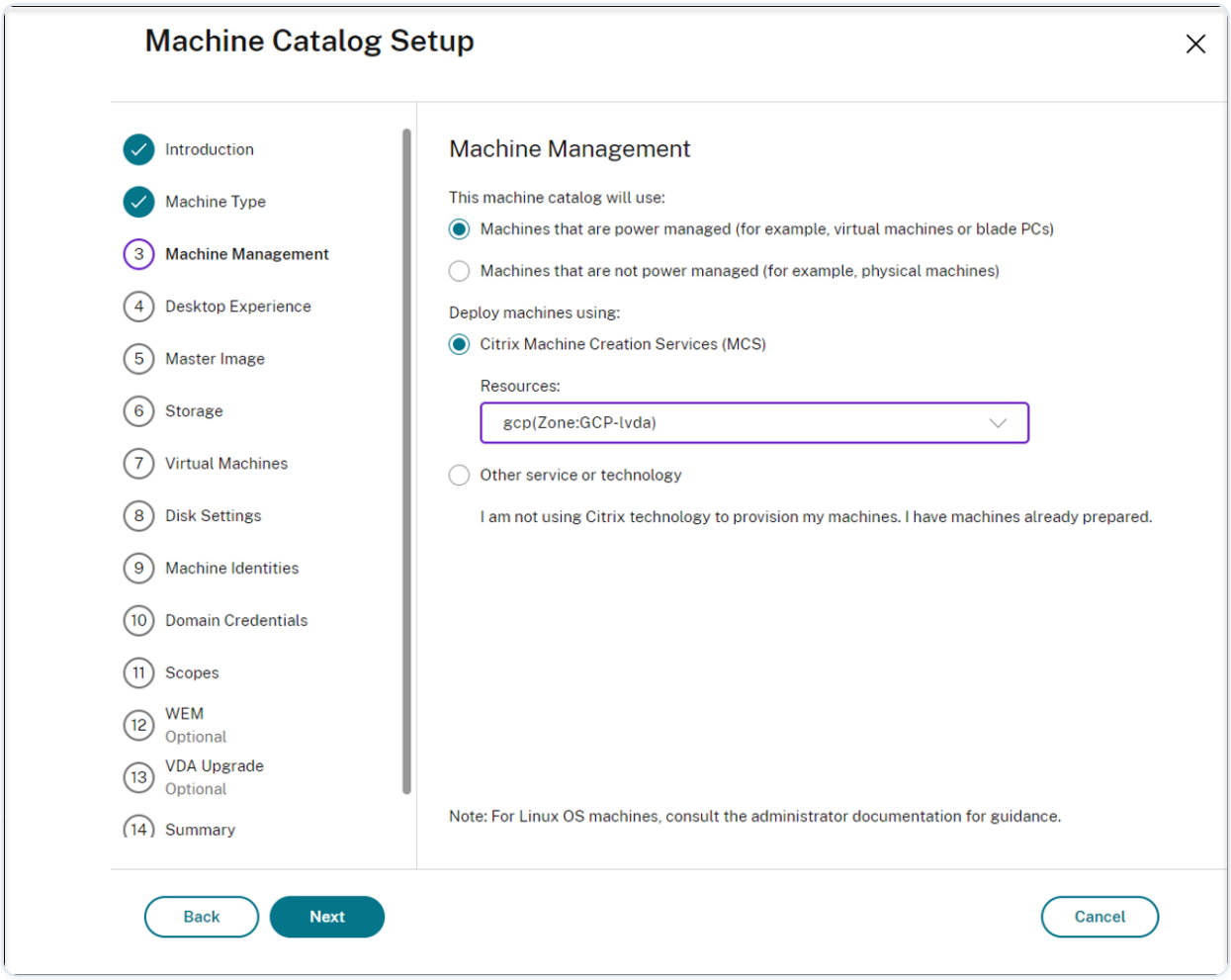
3. Instale las aplicaciones en la VM de plantilla y apáguela. Cree y asigne un nombre a una instantánea de su imagen maestra.

Paso 5: Crear un catálogo de máquinas

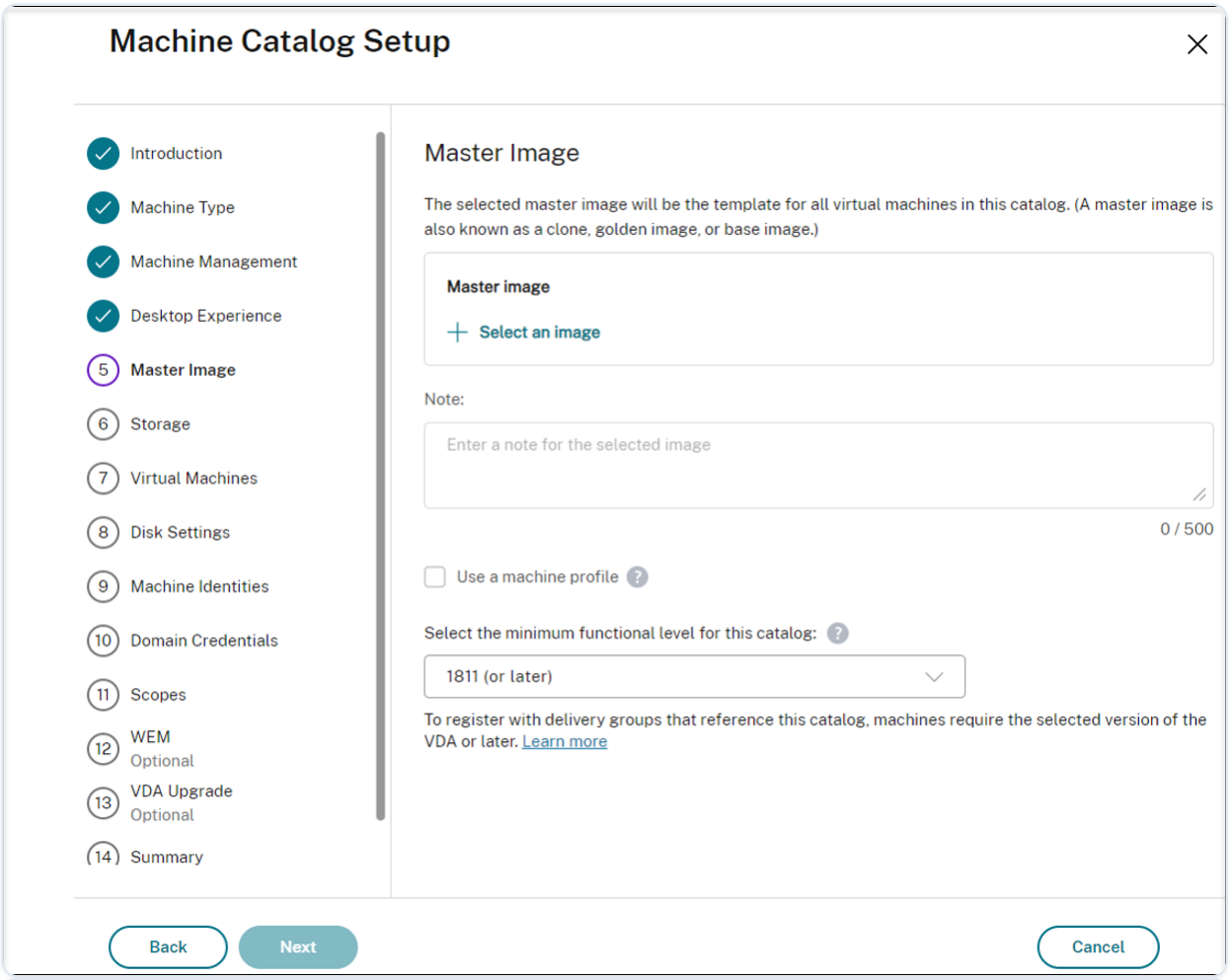
1. Inicie sesión en Citrix Cloud. En el menú superior izquierdo, seleccione **Mis servicios > DaaS**.
2. Desde **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel izquierdo.
3. Seleccione **Crear catálogo de máquinas** en la barra de acciones.
4. En la página **Tipo de máquina**, seleccione **SO multisesión** o **SO de sesión única** y, a continuación, seleccione **Siguiente**.

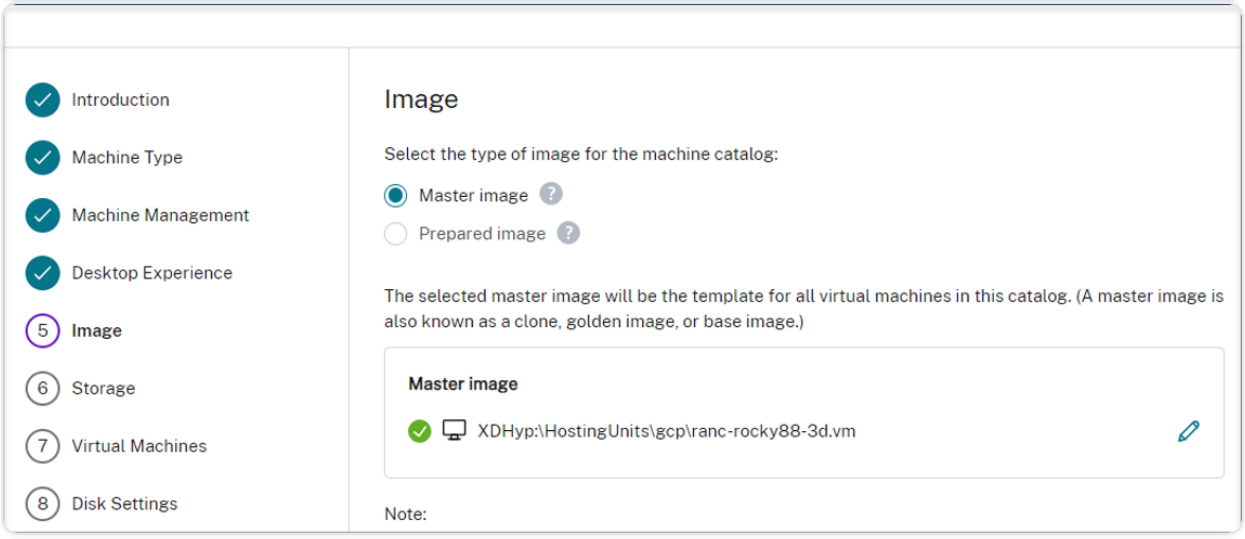


5. En la página **Administración de máquinas**, seleccione las opciones **Máquinas con administración de energía** y **Servicios de creación de máquinas de Citrix** y, a continuación, seleccione **Siguiente**. Si hay varios recursos, seleccione uno del menú.



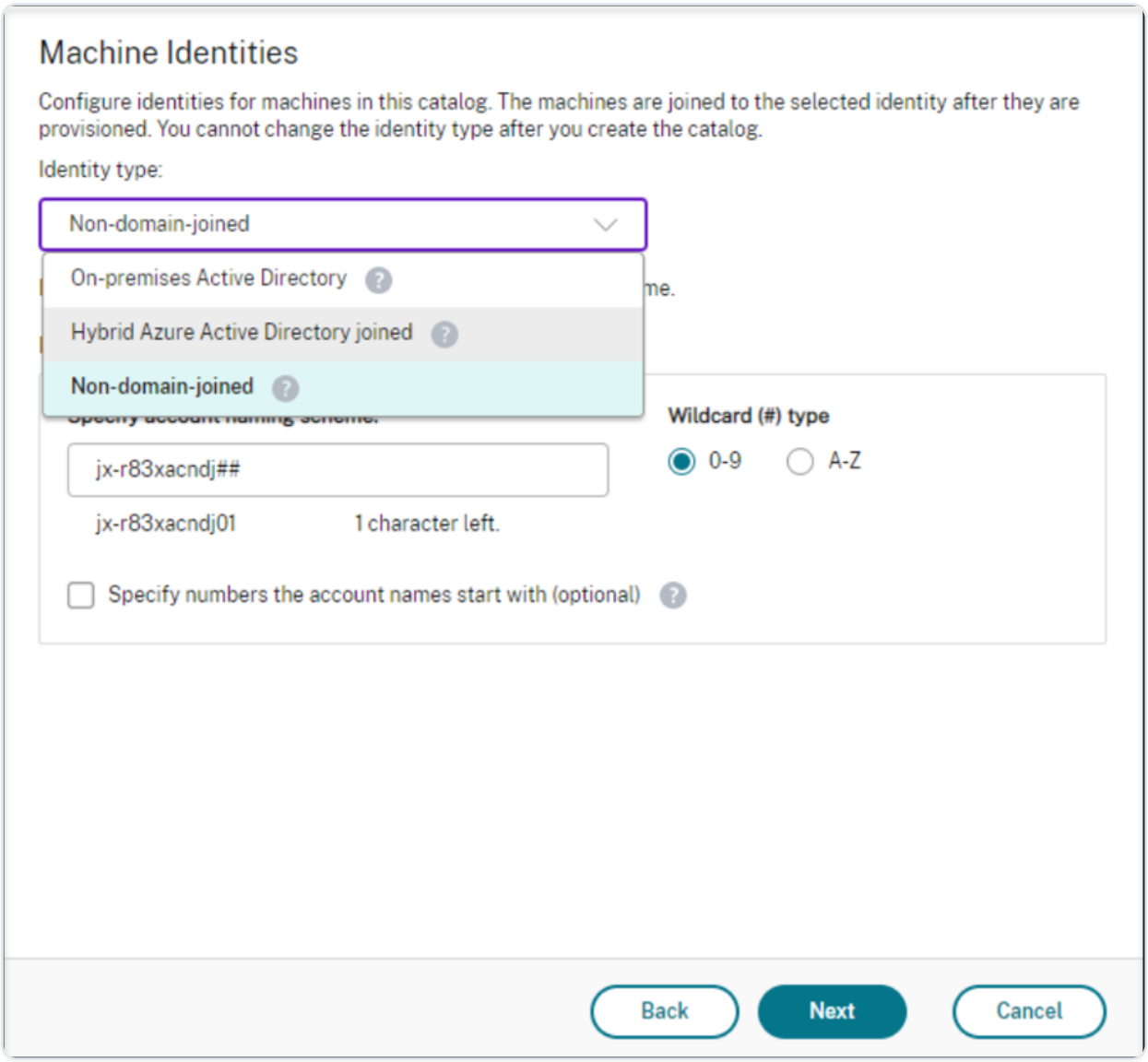
6. En la página **Imagen maestra**, seleccione la imagen maestra creada anteriormente.



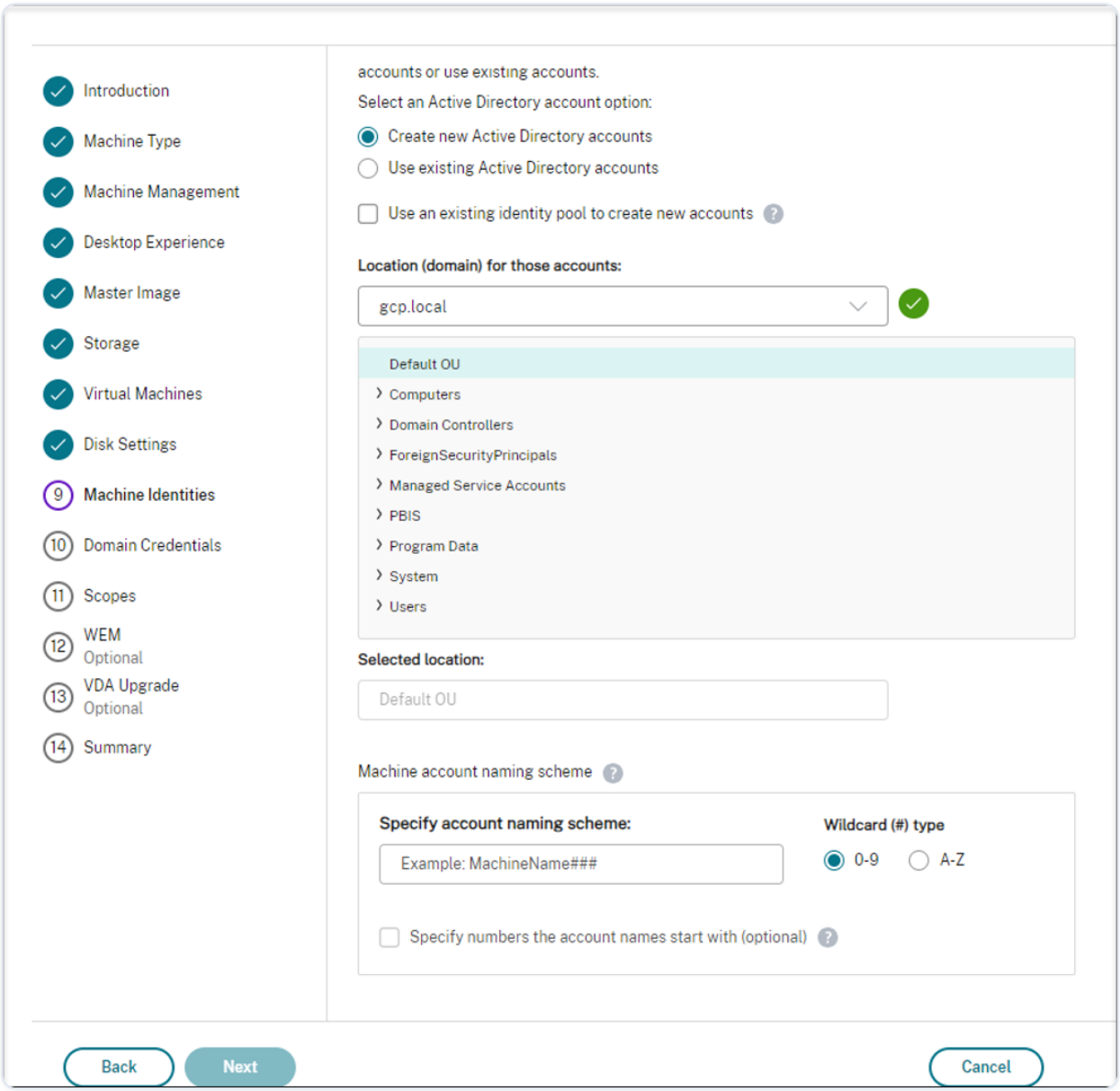


7. En la página **Identidades de máquina**, seleccione **No unido a un dominio** si la imagen maestra no estaba unida a ningún dominio o seleccione una cuenta de Active Directory si unió la imagen maestra a un dominio.

   Para escenarios no unidos a un dominio:

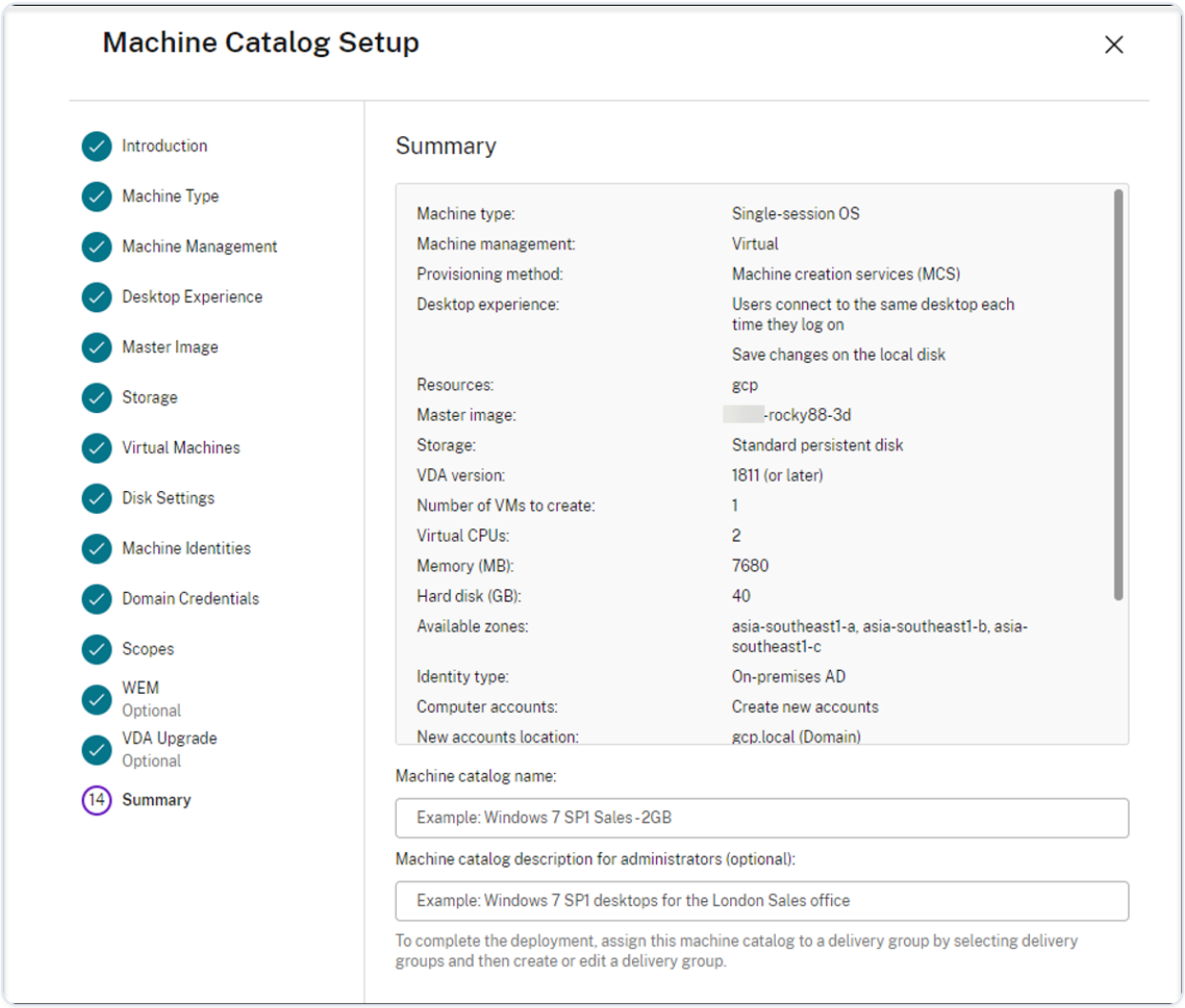


Para escenarios unidos a un dominio:



- Si selecciona **Crear nuevas cuentas de Active Directory**, seleccione un dominio y, a continuación, introduzca la secuencia de caracteres que representa el esquema de nombres para las cuentas de equipo de VM aprovisionadas creadas en Active Directory. El esquema de nombres de cuenta puede contener entre 1 y 64 caracteres, y no puede contener espacios en blanco, caracteres no ASCII o caracteres especiales.
- Si selecciona **Usar cuentas de Active Directory existentes**, seleccione **Examinar** para navegar a las cuentas de equipo de Active Directory existentes para las máquinas seleccionadas.
- En la página **Credenciales de dominio**, seleccione **Introducir credenciales**, escriba el nombre de usuario y la contraseña, seleccione **Guardar** y, a continuación, seleccione **Siguiente**. La credencial que escriba debe tener permiso para realizar operaciones de cuenta de Active Directory.

8. Configure ajustes adicionales en las demás páginas. Para obtener más información, consulte Crear un catálogo de Google Cloud Platform.
9. En la página **Resumen**, confirme la información, especifique un nombre para el catálogo y, a continuación, seleccione **Finalizar**.



La creación del catálogo de máquinas puede tardar mucho tiempo en completarse. Cuando se complete, el catálogo aparecerá en la lista. Puede verificar que las máquinas se crean en los grupos de nodos de destino en la consola de Google Cloud.

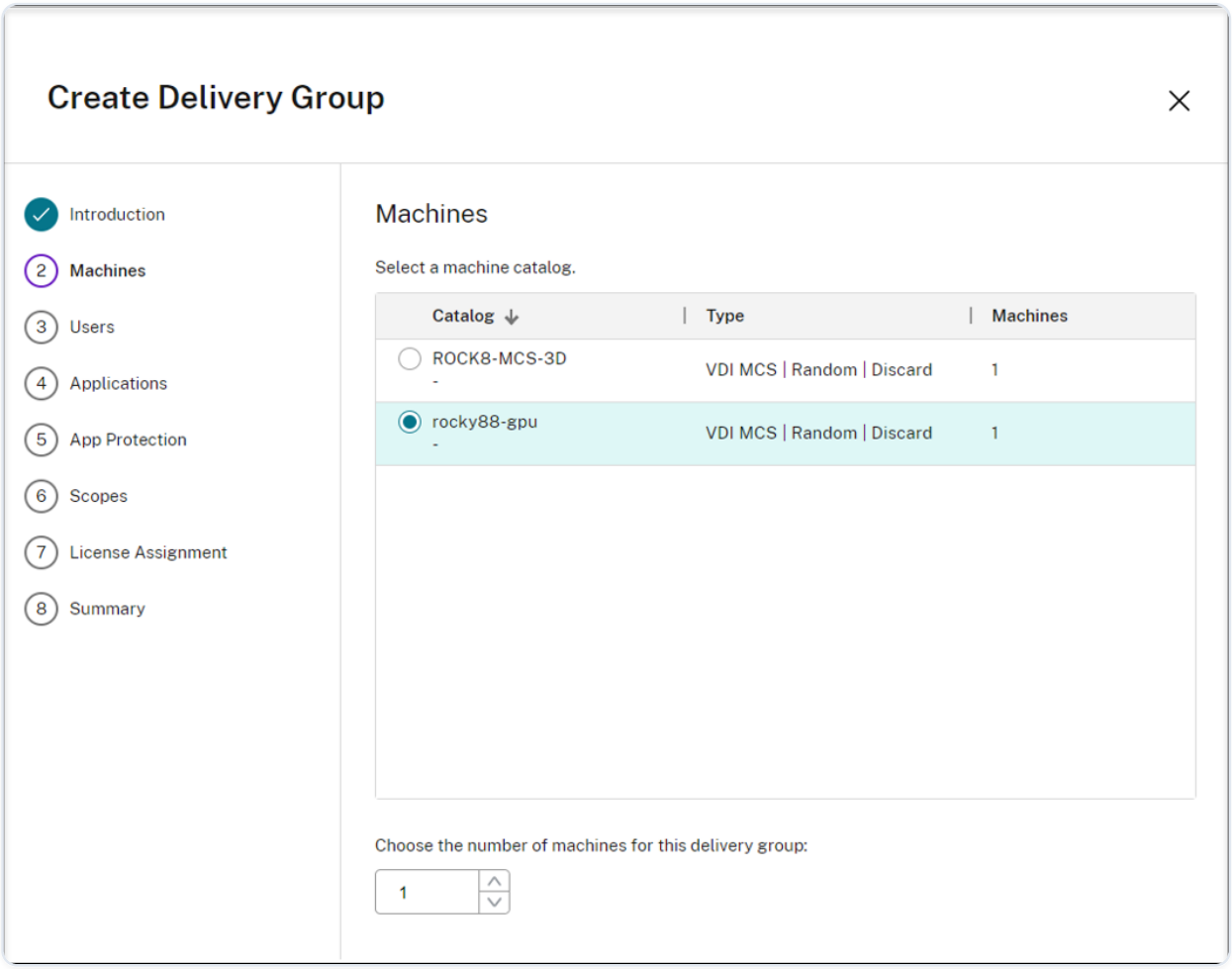
Paso 6: Crear un grupo de entrega

Un grupo de entrega es una colección de máquinas seleccionadas de uno o más catálogos de máquinas. Especifica qué usuarios pueden usar esas máquinas, y las aplicaciones y escritorios disponibles para esos usuarios.

Para obtener más información, consulte la creación de grupos de entrega en la documentación de Citrix DaaS.

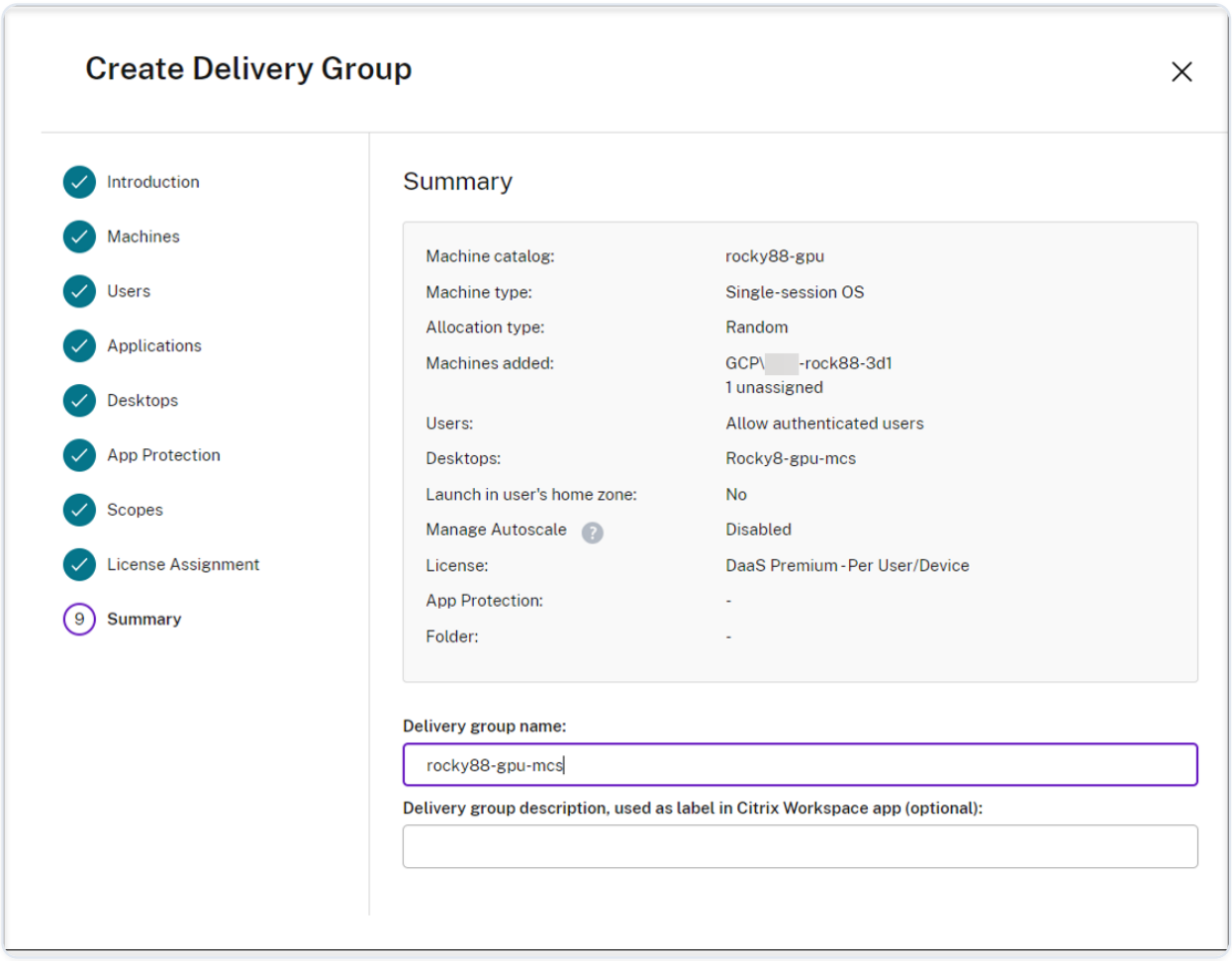
1. Inicie sesión en Citrix Cloud. En el menú superior izquierdo, seleccione **Mis servicios > DaaS**.
2. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel izquierdo.
3. Seleccione **Crear grupo de entrega** en la barra de acciones. Se abre el asistente para la creación de grupos de entrega.

   Las páginas del asistente que ve pueden ser diferentes, según las selecciones que realice.
4. En la página **Máquinas**, seleccione un catálogo de máquinas y seleccione el número de máquinas que desea usar de ese catálogo.

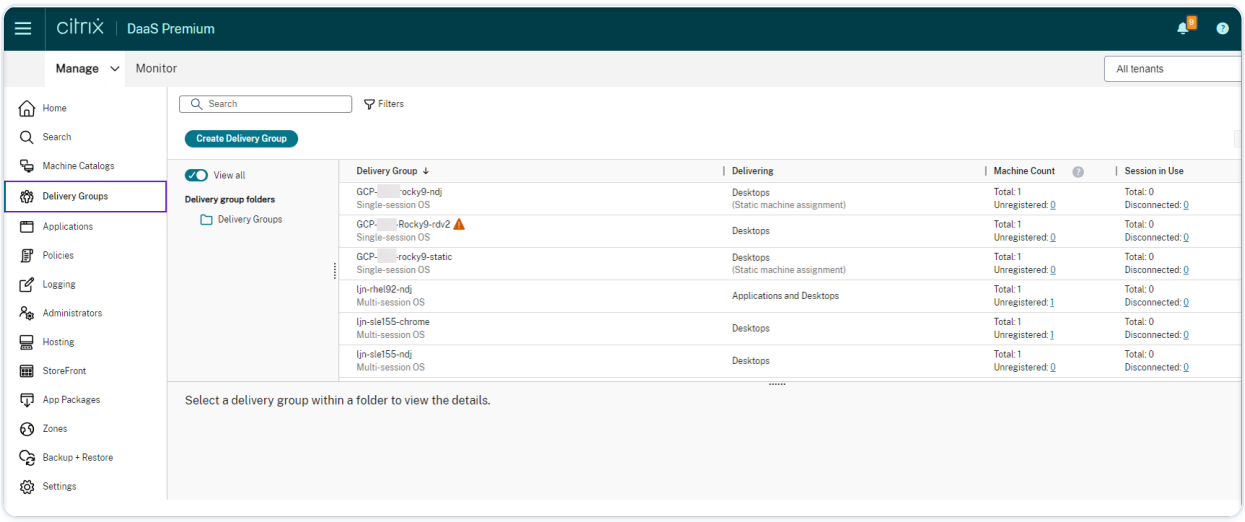


5. Configure ajustes adicionales en las demás páginas. Para obtener más información, consulte Crear grupos de entrega.
6. En la página **Resumen**, introduzca un nombre para el grupo de entrega. También puede (opcionalmente) introducir una descripción, que aparece en la aplicación Citrix Workspace™ y en la interfaz de administración de **Configuración completa**. Por ejemplo:

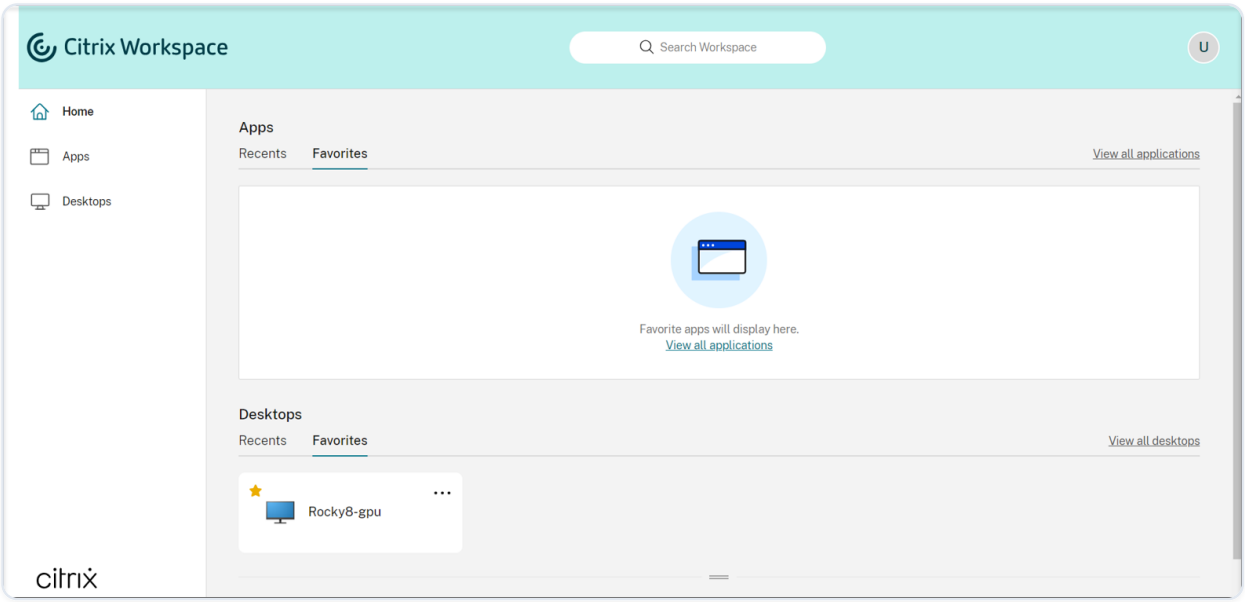
   Introduzca un nombre para el grupo de entrega:



Lista de grupos de entrega en la interfaz de administración de **Configuración completa**:



Máquina entregada en la aplicación Citrix Workspace



Administre su implementación con Ansible

Ansible ayuda a automatizar el proceso de implementación de aplicaciones, configuraciones y actualizaciones en toda su implementación. Este artículo ofrece instrucciones paso a paso sobre cómo usar Ansible para administrar su implementación de manera eficiente.

Paso 1: Determine qué implementar

Antes de empezar, identifique lo que necesita implementar, como aplicaciones, servicios, configuraciones y variables de entorno.

Paso 2: Configure su proyecto de Ansible

Cree una estructura de directorios para su proyecto de Ansible. Una forma crucial de organizar el contenido de su playbook es la función de "roles" de Ansible. Para obtener más información, consulte Roles en la documentación de Ansible.

A continuación, se muestran dos ejemplos de estructuras de directorios para su referencia:

Ejemplo de estructura de directorios n.º 1

```
production                # inventory file for production servers

staging                   # inventory file for staging environment



group_vars/
```

```
   group1.yml             # here we assign variables to particular groups
   group2.yml
host_vars/
   hostname1.yml          # here we assign variables to particular systems
   hostname2.yml


library/                  # if any custom modules, put them here
(optional)
module_utils/             # if any custom module_utils to support modules,
put them here (optional)
filter_plugins/           # if any custom filter plugins, put them here
(optional)


site.yml                  # master playbook
webservers.yml            # playbook for webserver tier
dbservers.yml             # playbook for dbserver tier


roles/
    common/               # this hierarchy represents a "role"
        tasks/            #
            main.yml      #  <-- tasks file can include smaller files if
warranted
        handlers/         #
            main.yml      #  <-- handlers file
```

```
        templates/        #  <-- files for use with the template resource
            ntp.conf.j2   #  <------- templates end in .j2
        files/            #
            bar.txt       #  <-- files for use with the copy resource
            foo.sh        #  <-- script files for use with the script
resource
        vars/             #
            main.yml      #  <-- variables associated with this role
        defaults/         #
            main.yml      #  <-- default lower priority variables for this
role
        meta/             #
            main.yml      #  <-- role dependencies
        library/          # roles can also include custom modules
        module_utils/     # roles can also include custom module_utils
        lookup_plugins/   # or other types of plugins, like lookup in this
case


    webtier/              # same kind of structure as "common" was above,
done for the webtier role
    monitoring/           # ""
    fooapp/               # ""
```

Ejemplo de estructura de directorios n.º 2

```
inventories/
   production/
      hosts               # inventory file for production servers
      group_vars/
         group1.yml       # here we assign variables to particular groups
         group2.yml
      host_vars/
         hostname1.yml    # here we assign variables to particular systems
         hostname2.yml

   staging/
      hosts               # inventory file for staging environment
      group_vars/
         group1.yml       # here we assign variables to particular groups
         group2.yml
      host_vars/
         stagehost1.yml   # here we assign variables to particular systems
         stagehost2.yml

library/
module_utils/
```

```
filter_plugins/



site.yml

webservers.yml

dbservers.yml



roles/

    common/

    webtier/

    monitoring/

    fooapp/
```

Paso 3: Configure su inventario

Defina su archivo de inventario (inventory.ini). Un archivo de inventario suele enumerar los hosts que desea administrar con Ansible, junto con los detalles necesarios, como nombres de host, direcciones IP y pertenencias a grupos. Por ejemplo:

```
# Hostname and ip address

[UBUNTU2004]

<ip address>

[UBUNTU2204]

<ip address>

[RHEL8]

<ip address>
```

```
[RHEL9]

<ip address>

[DEBIAN11]

<ip address>

[DEBIAN12]

<ip address>

[SUSE15]

<ip address>



[all:children]

UBUNTU2004

UBUNTU2204

RHEL8

RHEL9

DEBIAN11

DEBIAN12

SUSE15



[all:vars]

ansible_user=<ansible execute user e.g root>

ansible_password=<>
```

```
ansible_ssh_common_args='-o StrictHostKeyChecking=no'
```

Paso 4: Cree playbooks de Ansible

Cree playbooks (archivos .yml) para automatizar las tareas de implementación. La sección proporciona ejemplos de playbooks para automatizar diferentes tareas de implementación.

Ejemplo de playbook para aplicar parches a distribuciones de Linux

Para aplicar parches a varias distribuciones de Linux con Ansible, puede crear un archivo de playbook YAML llamado patch-for-different-distribution.yml y rellenar el archivo con tareas similares a las siguientes. La directiva hosts define los hosts de destino del inventario (inventory.ini en este contexto) a los que se dirigen las tareas del playbook.

```
- name: Upgrade and Reboot RHEL & Debian family Linux distros

  hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  vars:

    reboot_connect_timeout: 5

    reboot_post_reboot_delay: 15

    reboot_timeout: 600

  tasks:

    # Upgrade RHEL family OS packages

    - name: Upgrade RHEL Family OS packages

      ansible.builtin.yum:

        name: '*'

        state: latest

      when:

        - ansible_facts['distribution'] == "RedHat"
```

```
    - ansible_facts['distribution_major_version'] == "7"


# Upgrade RHEL family OS packages
- name: Upgrade RHEL Family OS packages
  ansible.builtin.yum:
    name: '*'
    state: latest
  when:
    - ansible_facts['distribution'] == "RedHat"
    - ansible_facts['distribution_major_version'] == "8"


# Upgrade RHEL family OS packages
- name: Upgrade RHEL Family OS packages
  ansible.builtin.yum:
    name: '*'
    state: latest
  when:
    - ansible_facts['distribution'] == "RedHat"
    - ansible_facts['distribution_major_version'] == "9"


# Ubuntu Family upgrade
- name: Update repositories cache
```

```
    apt:
      update_cache: yes
    when:
      - ansible_facts['distribution'] == "Ubuntu"
      - ansible_facts['distribution_major_version'] == "20"


  - name: Update all packages to their latest version
    apt:
      name: "*"
      state: latest
    when:
      - ansible_facts['distribution'] == "Ubuntu"
      - ansible_facts['distribution_major_version'] == "22"


  # Debian Family upgrade
  - name: Upgrade the OS (apt-get dist-upgrade)
    apt:
      upgrade: dist
    when:
      - ansible_facts['distribution'] == "Debian"
      - ansible_facts['distribution_major_version'] == "11"
```

```
    - name: Upgrade the OS (apt-get dist-upgrade)
      apt:
        upgrade: dist
      when:
        - ansible_facts['distribution'] == "Debian"
        - ansible_facts['distribution_major_version'] == "12"


    # Reboot after upgrade
    - name: Reboot host
      reboot:
        connect_timeout: "{{ reboot_connect_timeout }}"
        post_reboot_delay: "{{ reboot_post_reboot_delay }}"
        reboot_timeout: "{{ reboot_timeout }}"
```

Playbook de ejemplo para instalar entornos .Net

El siguiente playbook de ejemplo instala diferentes versiones de entornos .Net en las distribuciones de Linux específicas.

```
- name: Install dotnet runtime environment on Linux distros

  hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  tasks:

    # Install dotnet runtime environment on RHEL7

    - name: Enable the rhel-7-server-dotnet-rpms repository
```

```
      command: subscription-manager repos --enable=rhel-7-server-dotnet-
rpms

      when:

        - ansible_facts['distribution'] == "RedHat"

        - ansible_facts['distribution_major_version'] == "7"



    - name: Install dotnet runtime environment on RHEL7

      ansible.builtin.yum:

        name: rh-dotnet60-aspnetcore-runtime-6.0

        state: present

      when:

        - ansible_facts['distribution'] == "RedHat"

        - ansible_facts['distribution_major_version'] == "7"



    - name: Remove /usr/bin/dotnet if it exists

      file:

        path: /usr/bin/dotnet

        state: absent



    - name: Create a symbolic link

      file:

        src: /opt/rh/rh-dotnet60/root/usr/lib64/dotnet/dotnet
```

```
    dest: /usr/bin/dotnet
    state: link


# RHEL8 linux vda install dotnet runtime environment
- name: Install dotnet-runtime-8.0
  ansible.builtin.dnf:
    name: dotnet-runtime-8.0
    state: present
  when:
    - ansible_facts['distribution'] == "RedHat"
    - ansible_facts['distribution_major_version'] == "8"


- name: Install aspnetcore-runtime-8.0
  ansible.builtin.dnf:
    name: aspnetcore-runtime-8.0
    state: present
  when:
    - ansible_facts['distribution'] == "RedHat"
    - ansible_facts['distribution_major_version'] == "8"


# RHEL9 linux vda install dotnet runtime environment
- name: Install dotnet-runtime-8.0
```

```
      ansible.builtin.dnf:
        name: dotnet-runtime-8.0
        state: present
      when:
        - ansible_facts['distribution'] == "RedHat"
        - ansible_facts['distribution_major_version'] == "9"


    - name: Install aspnetcore-runtime-8.0
      ansible.builtin.dnf:
        name: aspnetcore-runtime-8.0
        state: present
      when:
        - ansible_facts['distribution'] == "RedHat"
        - ansible_facts['distribution_major_version'] == "9"


    # Ubuntu20.04 linux vda install dotnet runtime environment
    - name: Register Microsoft key and feed
      shell: |
        wget https://packages.microsoft.com/config/ubuntu/20.04/packages-
microsoft-prod.deb -O packages-microsoft-prod.deb
        dpkg -i packages-microsoft-prod.deb
        rm packages-microsoft-prod.deb
```

```
    when:
      - ansible_facts['distribution'] == "Ubuntu"
      - ansible_facts['distribution_major_version'] == "20"


- name: Install dotnet-runtime-8.0
  ansible.builtin.apt:
    name: dotnet-runtime-8.0
    state: present
    update_cache: yes
  when:
    - ansible_facts['distribution'] == "Ubuntu"
    - ansible_facts['distribution_major_version'] == "20"


- name: Install aspnetcore-runtime-8.0
  ansible.builtin.apt:
    name: aspnetcore-runtime-8.0
    state: present
    update_cache: yes
  when:
    - ansible_facts['distribution'] == "Ubuntu"
    - ansible_facts['distribution_major_version'] == "20"
```

```
# Ubuntu22.04 linux vda install dotnet runtime environment
- name: Install dotnet-runtime-8.0
  ansible.builtin.apt:
    name: dotnet-runtime-8.0
    state: present
    update_cache: yes
  when:
    - ansible_facts['distribution'] == "Ubuntu"
    - ansible_facts['distribution_major_version'] == "22"


- name: Install aspnetcore-runtime-8.0
  ansible.builtin.apt:
    name: aspnetcore-runtime-8.0
    state: present
    update_cache: yes
  when:
    - ansible_facts['distribution'] == "Ubuntu"
    - ansible_facts['distribution_major_version'] == "22"


# Debian11 linux vda install dotnet runtime environment
- name: Register Microsoft key and feed
  shell: |
```

```
        wget https://packages.microsoft.com/config/debian/11/packages-
microsoft-prod.deb -O packages-microsoft-prod.deb

        dpkg -i packages-microsoft-prod.deb

        rm packages-microsoft-prod.deb

      when:

        - ansible_facts['distribution'] == "Debian"

        - ansible_facts['distribution_major_version'] == "11"



    - name: Install dotnet-runtime-8.0

      ansible.builtin.apt:

        name: dotnet-runtime-8.0

        state: present

        update_cache: yes

      when:

        - ansible_facts['distribution'] == "Debian"

        - ansible_facts['distribution_major_version'] == "11"



    - name: Install aspnetcore-runtime-8.0

      ansible.builtin.apt:

        name: aspnetcore-runtime-8.0

        state: present

        update_cache: yes
```

```
      when:
        - ansible_facts['distribution'] == "Debian"
        - ansible_facts['distribution_major_version'] == "11"


    # Debian12 linux vda install dotnet runtime environment
    - name: Register Microsoft key and feed
      shell: |
        wget https://packages.microsoft.com/config/debian/12/packages-
microsoft-prod.deb -O packages-microsoft-prod.deb
        dpkg -i packages-microsoft-prod.deb
        rm packages-microsoft-prod.deb
      when:
        - ansible_facts['distribution'] == "Debian"
        - ansible_facts['distribution_major_version'] == "12"


    - name: Install dotnet-runtime-8.0
      ansible.builtin.apt:
        name: dotnet-runtime-8.0
        state: present
        update_cache: yes
      when:
        - ansible_facts['distribution'] == "Debian"
```

```
        - ansible_facts['distribution_major_version'] == "12"


    - name: Install aspnetcore-runtime-8.0
      ansible.builtin.apt:
        name: aspnetcore-runtime-8.0
        state: present
        update_cache: yes
      when:
        - ansible_facts['distribution'] == "Debian"
        - ansible_facts['distribution_major_version'] == "12"


    # Sles15 linux vda install dotnet runtime environment
    - name: Register Microsoft key and feed
      shell: |
        sudo rpm -Uvh https://packages.microsoft.com/config/sles/15/
packages-microsoft-prod.rpm
        sudo ln -s /etc/yum.repos.d/microsoft-prod.repo /etc/zypp/repos.d/
microsoft-prod.repo
      when:
        - ansible_facts['distribution'] == "SLES"
        - ansible_facts['distribution_major_version'] == "15"


    - name: Install dotnet-runtime-8.0
```

```
    community.general.zypper:
      name: dotnet-runtime-8.0
      state: present
      update_cache: yes
    when:
      - ansible_facts['distribution'] == "SLES"
      - ansible_facts['distribution_major_version'] == "15"


- name: Install aspnetcore-runtime-8.0
  community.general.zypper:
    name: aspnetcore-runtime-8.0
    state: present
    update_cache: yes
  when:
    - ansible_facts['distribution'] == "SLES"
    - ansible_facts['distribution_major_version'] == "15"


# Amazon2 linux vda install dotnet runtime environment
- name: Install dotnet-runtime-8.0
  ansible.builtin.yum:
    name: dotnet-runtime-8.0
    state: present
```

```
      when:
        - ansible_facts['distribution'] == "Amazon"
        - ansible_facts['distribution_major_version'] == "2"


    - name: Install aspnetcore-runtime-8.0
      ansible.builtin.yum:
        name: aspnetcore-runtime-8.0
        state: present
      when:
        - ansible_facts['distribution'] == "Amazon"
        - ansible_facts['distribution_major_version'] == "2"
```

Playbooks de ejemplo para actualizar el VDA de Linux

Para automatizar las actualizaciones del VDA de Linux con Ansible, puede crear dos playbooks separados. Un playbook, como get_the_build.yml, se dedica a descargar y transferir el paquete del VDA de Linux a las máquinas de destino (hosts). El otro playbook, por ejemplo linux_upgrade.yml, contiene tareas diseñadas para actualizar el VDA de Linux en las máquinas de destino utilizando el paquete descargado previamente.

Playbook de ejemplo get_the_build.yml

```
- hosts: localhost
  name: Get the latest release build to local
  vars:
    build_url: <linux vda download link>  # replace with your actual
value.
    local_tmp: "/tmp/"  # replace with your actual value.
```

```
    remote_tmp: "/tmp/"  # replace with your actual value.

    linuxvda_file_name : "linux vda rpm/deb file name" # replace with your
actual value.

  tasks:

  - name: Download the file

    get_url:

      url: "{{ build_url }}"

      dest: "{{ local_tmp }}"

    tags:

      - get




- hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  name: Copy a file to remote location

  tasks:

  - name: Copy vda to the remote machine

    ansible.builtin.copy:

      src: "{{ local_tmp }}{{ linuxvda_file_name }}"

      dest: "{{ remote_tmp }}"

      remote_src: no

    tags:
```

```
      - copy
```

Playbook de ejemplo linux_upgrade.yml

```
- name: Upgrade Linux VDA and Reboot RHEL & Debian Linux distros

  hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  vars:

    remote_tmp: "/path/to/remote/tmp"  # replace with your actual path

    rhel7_file_name: "rhel7_file.rpm"  # replace with your actual file
name

    rhel8_file_name: "rhel8_file.rpm"  # replace with your actual file
name

    rhel9_file_name: "rhel9_file.rpm"  # replace with your actual file
name

    ubuntu2004_file_name: "ubuntu2004_file.deb"  # replace with your
actual file name

    ubuntu2204_file_name: "ubuntu2204_file.deb"  # replace with your
actual file name

    debian11_file_name: "debian11_file.deb" # replace with your actual
file name

    debian12_file_name: "debian12_file.deb" # replace with your actual
file name

    suse15_file_name: "suse15_file.deb" # replace with your actual file
name

    amazon2_file_name: "amazon2_file.rpm" # replace with your actual file
name

  tasks:
```

```
# Upgrade RHEL linux vda packages
- name: Upgrade RHEL7 linux vda packages
  ansible.builtin.yum:
    name: "{{ remote_tmp }}{{ rhel7_file_name }}"
    state: present
  when:
    - ansible_facts['distribution'] == "RedHat"
    - ansible_facts['distribution_major_version'] == "7"


# Upgrade RHEL linux vda packages
- name: Upgrade RHEL8 linux vda packages
  ansible.builtin.yum:
    name: "{{ remote_tmp }}{{ rhel8_file_name }}"
    state: present
  when:
    - ansible_facts['distribution'] == "RedHat"
    - ansible_facts['distribution_major_version'] == "8"


# Upgrade RHEL linux vda packages
- name: Upgrade RHEL9 linux vda packages
  ansible.builtin.yum:
    name: "{{ remote_tmp }}{{ rhel9_file_name }}"
```

```
      state: present
    when:
      - ansible_facts['distribution'] == "RedHat"
      - ansible_facts['distribution_major_version'] == "9"


  # Ubuntu20.04 linux vda upgrade
  - name: Ubuntu20.04 linux vda upgrade
    ansible.builtin.apt:
      deb: "{{ remote_tmp }}{{ ubuntu2004_file_name }}"
    when:
      - ansible_facts['distribution'] == "Ubuntu"
      - ansible_facts['distribution_major_version'] == "20"


  - name: Ubuntu22.04 linux vda upgrade
    ansible.builtin.apt:
      deb: "{{ remote_tmp }}{{ ubuntu2204_file_name }}"
    when:
      - ansible_facts['distribution'] == "Ubuntu"
      - ansible_facts['distribution_major_version'] == "22"


  # Debian Linux VDA upgrade
  - name: Debian11 Linux VDA upgrade
```

```
    ansible.builtin.apt:
      deb: "{{ remote_tmp }}{{ debian11_file_name }}"
    when:
      - ansible_facts['distribution'] == "Debian"
      - ansible_facts['distribution_major_version'] == "11"


- name: Debian12 Linux VDA upgrade
    ansible.builtin.apt:
      deb: "{{ remote_tmp }}{{ debian12_file_name }}"
    when:
      - ansible_facts['distribution'] == "Debian"
      - ansible_facts['distribution_major_version'] == "12"


# Sles15 Linux VDA upgrade
- name: Sles15 Linux VDA upgrade
    community.general.zypper:
      name: "{{ remote_tmp }}{{ suse15_file_name }}"
      state: present
    when:
      - ansible_facts['distribution'] == "SLES"
      - ansible_facts['distribution_major_version'] == "15"
```

```
    # Amazon2 Linux VDA upgrade

    - name: Amazon2 Linux VDA upgrade

      ansible.builtin.yum:

        name: "{{ remote_tmp }}{{ amazon2_file_name }}"

      when:

        - ansible_facts['distribution'] == "Amazon"

        - ansible_facts['distribution_major_version'] == "2"

    # Reboot after upgrade

    - name: Reboot host

      reboot:

        connect_timeout: "{{ reboot_connect_timeout }}"

        post_reboot_delay: "{{ reboot_post_reboot_delay }}"

        reboot_timeout: "{{ reboot_timeout }}"
```

Playbook de ejemplo para montar un servidor de sistema de archivos de red (NFS) como directorio de inicio

El siguiente playbook de ejemplo monta un servidor NFS como directorio de inicio en los hosts de destino:

```
- hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  vars:

    nfs_server = <nfsserver ip address> # replace with your actual values

    mount_points = /home/<domain realm>/user1,/home/<domain realm>user2  #
replace with your actual values
```

```
    nfs_shares = user1,user2  # replace with your actual values

    owners = user1,user2   # replace with your actual values

    groups = group1,group2  # replace with your actual values

  tasks:

    - name: Enable NFS as home directory

      ansible.builtin.command:

        cmd: "/opt/Citrix/VDA/bin/ctxreg create -k 'HKLM\\System\
\CurrentControlSet\\Control\\Citrix' -t 'REG_DWORD' -v
'CheckUserHomeMountPoint' -d '0x00000001' --force"

      register: result

      failed_when: result.rc != 0

      check_mode: no



    - name: Mount NFS shares

      ansible.builtin.mount:

        path: "{{ item.0 }}"

        src: "{{ nfs_server }}:{{ item.1 }}"

        fstype: nfs

        opts: rw,nolock

        state: mounted

      loop: "{{ mount_points | zip(nfs_shares) | list }}"



    - name: Set owner, group and mode for NFS client paths
```

```
      ansible.builtin.file:

        path: "{{ item.0 }}"

        owner: "{{ item.1 }}"

        group: "{{ item.2 }}"

        mode: "{{ mode }}"

      loop: "{{ mount_points | zip(owners, groups) | list }}"
```

Playbooks de ejemplo para la ejecución remota de comandos

Playbook de ejemplo para modificar la configuración del registro

```
- hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  vars:

    registry_key: "your_registry_key"      #  E.g. registry_key =
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd

    registry_type: "your_registry_type"    #  E.g. registry_type =
REG_DWORD

    registry_value: "your_registry_value"  #  E.g. registry_value =
AdaptiveScalingEnabled

    registry_data: "your_registry_data"    #  E.g. registry_data =
0x00000000

  tasks:

  - name: Execute AdaptiveScaling redirection script

    ansible.builtin.command:

      cmd: "/opt/Citrix/VDA/bin/ctxreg create -k \"{{ registry_key }}\" -t
\"{{ registry_type }}\" -v \"{{ registry_value }}\" -d
\"{{ registry_data }}\" --force"
```

```
    register: result

    failed_when: result.rc != 0

    check_mode: no
```

Playbook de ejemplo para bloquear la versión secundaria de RHEL

```
- hosts: <host1,host2,host3>  # replace with your actual hosts in the
inventory file.

  vars:

    rhel_minor_version: "9.3"  # replace with your actual minor version
such as 9.3, 8.8

  tasks:

    - name: Lock system to a specific minor version

      ansible.builtin.command:

        cmd: "subscription-manager release --set={{ rhel_minor_version }}"

      register: result

      failed_when: "'Error' in result.stderr"
```

Integrar VDA de Linux no unido a un dominio con Red Hat IdM

Red Hat Identity Management (IdM) es una solución ampliamente adoptada para gestionar identidades en entornos Linux. En comparación con la unión directa de sistemas Linux a Active Directory (AD), IdM ofrece importantes ventajas estratégicas y operativas, especialmente en infraestructuras con una presencia sustancial de Linux.

Dado que **Citrix Linux VDA** admite implementaciones **no unidas a un dominio (NDJ)**, las organizaciones pueden considerar la integración de VDA de Linux NDJ con IdM. Este enfoque amplía la gama de métodos de autenticación disponibles y mejora la flexibilidad en la gestión de identidades. Los usuarios deben autenticarse en su espacio de trabajo utilizando credenciales de dominio de AD o credenciales de un dominio IdM que haya establecido confianza con AD. Una vez

autenticados, pueden acceder sin problemas a los escritorios Linux unidos a IdM a través de **Single Sign-On (SSO)**.

A continuación, se describen los pasos verificados de integración y prueba para configurar un VDA de Linux con IdM.

1. **Requisitos previos y configuración del entorno**

- **Integración de Identity Management (IdM):**
  - **Instalación del servidor IdM:** El servidor IdM debe estar correctamente instalado y su servicio operativo. Consulte el documento de Red Hat
- **Integración de IdM y AD:**
  - **Confianza bidireccional:** Se debe establecer una relación de confianza bidireccional entre IdM y AD para permitir que los usuarios de ambos dominios accedan a los servicios del otro. Consulte el documento de Red Hat
- **Validar la relación de confianza en el servidor IdM:**
  - **Comprobar el permiso de usuario de IdM:** `getentpasswd idmuser1@idm.example.com`
  - **Comprobar el permiso de usuario de AD:** `getentpasswd aduser1@domain`

1. **Crear una máquina VDA de Linux no unida a un dominio**

Para crear un VDA de Linux no unido a un dominio, consulte Crear VDA de Linux no unidos a un dominio mediante MCS

1. **Cambiar el tipo de inicio de sesión predeterminado en DDC**

El `MachineLogOnType` predeterminado de un grupo de entrega creado por MCS es `LocalMappedAccount`. Esto debe establecerse en `ActiveDirectory` ejecutando el siguiente comando de PowerShell en el DDC:

```
Set-BrokerDesktopGroup -Name "<your delivery group name>" -MachineLogOnType ActiveDirectory
```

1. **Instalar el cliente de IdM y unir el VDA a IdM**

- **Instalar y configurar el cliente de IdM en el VDA de Linux:**

  - **Configurar el cliente de IdM:** El cliente de IdM debe instalarse en el VDA de Linux para permitir que la máquina sea administrada por el servidor de IdM. Consulte el documento de Red Hat
  - Se recomienda utilizar el modo de instalación no interactivo

- **verificar la autenticación de usuario de AD/IDM:**
  - **Comprobar el permiso de usuario de IdM:** `ssh localhost -l idmuser1@idm.example.com`
  - **Comprobar el permiso de usuario de AD:** `ssh localhost -l admuser1@domain`

1. **Iniciar sesión para verificar la integración**

- **Para el escenario local:** Tanto los usuarios de AD como los de IdM pueden iniciar sesiones con VDA de Linux integrados con IdM.
- **Para el escenario de DaaS:** Debido a que los usuarios de IdM no pueden utilizar los servicios que pertenecen al dominio de AD, solo los usuarios de AD pueden iniciar sesiones con VDA de Linux integrados con IdM en un entorno de DaaS.

1. **Aprovisionar máquinas VDA de Linux por lotes**

- Consulte el paso 2, Aprovisionar más VDA de Linux a través de MCS
- Consulte el paso 4, Aprovechar la automatización de terceros para unir cada VDA a IdM