Novedades

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 sombreado de sesiones ampliada a todas las distribuciones compatibles

La función de sombreado 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 Sombreado de 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 de inicio 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

Linux VDA 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 Linux VDA.

Problemas resueltos

Los siguientes problemas se han solucionado desde Linux Virtual Delivery Agent 2112:

- El lanzamiento inicial de una sesión de VDA de Linux que admite tarjetas NVIDIA GRID 3D podría resultar en una resolución de escritorio anormal.
- Con el registro detallado de SCARD_LIBPCSC deshabilitado, una sesión de VDA de Linux configurada con una tarjeta inteligente podría quedarse atascada en una pantalla gris durante el lanzamiento.

Problemas conocidos

Se han identificado los siguientes problemas en esta versión:

- Cambiar de un idioma europeo a japonés en una sesión no produce la salida escrita esperada después de la reconexión de la sesión. En su lugar, el japonés se muestra como la nueva distribución del teclado, pero la salida escrita sigue estando en el idioma europeo original. El problema ocurre incluso si **KeyboardLayout** está configurado como **Server Default** en el archivo WFCLIENT.ini con la intención de usar la distribución del teclado del VDA, independientemente de la configuración de la distribución del teclado del cliente.
- Es posible que las aplicaciones publicadas no integradas se cierren poco después de iniciarse. El problema ocurre después de una actualización de Mutter a una versión posterior a mutter-3.28.3-4. Para solucionar el problema, use mutter-3.28.3-4 o una versión anterior.
- El VDA de Linux no funciona como se espera cuando se utilizan tarjetas NVIDIA GRID 3D sin habilitar HDX 3D Pro. El problema ocurre en RHEL 7.7 y versiones anteriores, SUSE 12.5 y versiones anteriores, y Ubuntu 16.04. La razón es que varias bibliotecas OpenGL no pueden coexistir en los sistemas gráficos de estas distribuciones de Linux.
- Aparece una ventana inesperada durante la descarga de archivos. La ventana no afecta a la funcionalidad de descarga de archivos y desaparece automáticamente al cabo de un tiempo.
- La configuración predeterminada de PulseAudio hace que el programa del servidor de sonido se cierre después de 20 segundos de inactividad. Cuando PulseAudio se cierra, el audio no

funciona. Para solucionar este problema, establezca exit-idle-time=-1 en el archivo /etc/pulse/daemon.conf.

- `libtcmalloc 4.3.0` en SUSE 12.5 puede hacer que los procesos se cierren inesperadamente.
- El servicio `ctxhdx` puede cerrarse inesperadamente en los VDA de Ubuntu 16.04 y SUSE 12.5. El problema ocurre con las versiones 2.22 a 2.24 de GNU C Library (`glibc`). El problema se ha corregido en `glibc 2.25`. Si utiliza la distribución SUSE 12.5, puede instalar el parche que SUSE proporciona para solucionar el problema. No hay ninguna corrección disponible para Ubuntu 16.04 en el momento en que se lanza el VDA de Linux.
- No se pueden iniciar sesiones en la aplicación Citrix Workspace™ para Linux cuando el cifrado SSL está habilitado y la fiabilidad de la sesión está inhabilitada.
- El proceso `indicator-datetime-service` no consume la variable de entorno $TZ. Cuando el cliente y la sesión se encuentran en zonas horarias diferentes, el panel de unidad en Ubuntu 16.04 Unity Desktop no muestra la hora del cliente.
- Gráficos de Ubuntu: En HDX™ 3D Pro, puede aparecer un marco negro alrededor de las aplicaciones después de cambiar el tamaño del Visor de escritorio o, a veces, el fondo puede aparecer en negro.
- Es posible que las impresoras creadas por la redirección de impresión del VDA de Linux no se eliminen después de cerrar una sesión.
- Faltan archivos CDM cuando un directorio contiene numerosos archivos y subdirectorios. Este problema puede ocurrir si el lado del cliente tiene demasiados archivos o directorios.
- Solo se admite la codificación UTF-8 para idiomas no ingleses.
- El estado de BLOQ MAYÚS de la aplicación Citrix Workspace para Android puede invertirse durante la itinerancia de la sesión. El estado de BLOQ MAYÚS puede perderse al itinerar una conexión existente a la aplicación Citrix Workspace para Android. Como solución alternativa, use la tecla Mayús del teclado extendido para alternar entre mayúsculas y minúsculas.
- Las teclas de acceso directo con ALT no siempre funcionan cuando se conecta al VDA de Linux mediante la aplicación Citrix Workspace para Mac. La aplicación Citrix Workspace para Mac envía AltGr para las teclas de opción/Alt izquierda y derecha de forma predeterminada. Puede modificar este comportamiento en la configuración de la aplicación Citrix Workspace, pero los resultados varían según las aplicaciones.
- El registro falla cuando el VDA de Linux se vuelve a unir al dominio. La nueva unión genera un nuevo conjunto de claves Kerberos. Sin embargo, el Broker podría usar un ticket de servicio de VDA obsoleto en caché basado en el conjunto anterior de claves Kerberos. Cuando el VDA

intenta conectarse al Broker, es posible que el Broker no pueda establecer un contexto de seguridad de retorno al VDA. El síntoma habitual es que el registro del VDA falla.

Este problema puede resolverse por sí solo cuando el ticket de servicio del VDA caduca y se renueva. Pero como los tickets de servicio tienen una larga vida útil, puede llevar mucho tiempo.

Como solución alternativa, borre la caché de tickets del Broker. Reinicie el Broker o ejecute el siguiente comando en el Broker desde un símbolo del sistema como administrador:

```
klist -li 0x3e4 purge
```

Este comando purga todos los tickets de servicio de la caché LSA que posee la entidad de seguridad del servicio de red bajo la cual se ejecuta el servicio Citrix Broker. Elimina los tickets de servicio para otros VDA y, potencialmente, para otros servicios. Sin embargo, es inofensivo: estos tickets de servicio se pueden volver a adquirir del KDC cuando sea necesario.

- No se admite la función Plug-n-play de audio. Puede conectar un dispositivo de captura de audio a la máquina cliente antes de empezar a grabar audio en la sesión ICA®. Si se conecta un dispositivo de captura después de que se haya iniciado la aplicación de grabación de audio, la aplicación podría dejar de responder y deberá reiniciarla. Si se desconecta un dispositivo de captura durante la grabación, podría producirse un problema similar.
- La aplicación Citrix Workspace para Windows podría experimentar distorsión de audio durante la grabación de audio.

Avisos de terceros

Linux Virtual Delivery Agent Version 2201 (Descarga de PDF)

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

Obsoleto

Los anuncios de este artículo tienen como objetivo avisarle con antelación sobre las plataformas, los productos Citrix® y las funciones que se están retirando 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 funcionalidades obsoletas. Para obtener más información sobre el

soporte del ciclo de vida del producto, consulte el artículo Directiva 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 obsoletos o se han quitado. Los elementos **obsoletos** no se quitan de inmediato. Citrix sigue ofreciéndoles soporte en esta versión, pero se quitarán en una futura versión Current Release. Los elementos **quitados** se han quitado o ya no se admiten en el VDA de Linux.

ELEMENTO	ANUNCIO DE OBSOLESCENCIA EN	ELIMINADO EN
Compatibilidad con CentOS 8.x	2110	2201
Compatibilidad con SUSE 12.5	2109	2204
Compatibilidad con Ubuntu 16.04	2109	2203
Compatibilidad con RHEL 7.7, CentOS 7.7	2006	2009
Compatibilidad con SUSE 12.3	2006	2006
Compatibilidad con RHEL 6.10, CentOS 6.10	2003	2003
Compatibilidad con RHEL 6.9, CentOS 6.9	1909	1909
Compatibilidad con RHEL 7.5, CentOS 7.5	1903	1903
Compatibilidad con RHEL 7.4, CentOS 7.4	1811	1811
Compatibilidad con RHEL 6.8, CentOS 6.8	1811	1811

ELEMENTO	ANUNCIO DE OBSOLESCENCIA EN	ELIMINADO EN
Compatibilidad con RHEL 7.3, CentOS 7.3	7.18	7.18
Compatibilidad con RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

Requisitos del sistema

Distribuciones de Linux

Nota:

Los requisitos del sistema para los componentes no cubiertos aquí (como la aplicación Citrix Workspace™) se describen en sus respectivas documentaciones.

Antes de instalar Linux VDA, instale .NET Runtime 6.0 según las instrucciones de `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

Linux VDA no admite SecureICA para el cifrado. Habilitar SecureICA en Linux VDA provoca un error al iniciar la sesión.

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

Linux VDA admite las siguientes distribuciones de Linux:

Importante:

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.

- Amazon Linux
  - Amazon Linux 2
- CentOS Linux
  - CentOS 7.9
  - CentOS 7.8
- Debian Linux
  - Debian 10.9
- Red Hat Enterprise Linux
  - Workstation 8.4
  - Workstation 8.3
  - Workstation 8.2
  - Workstation 8.1
  - Workstation 7.9
  - Workstation 7.8
  - Server 8.4
  - Server 8.3
  - Server 8.2
  - Server 8.1
  - Server 7.9
  - Server 7.8
- SUSE Linux Enterprise:
  - Server 15 Service Pack 3
  - Server 15 Service Pack 2
  - Server 12 Service Pack 5 + SUSE Linux Enterprise Extensión de estación de trabajo 12 SP5
  - Server 12 Service Pack 5
- Ubuntu Linux

- Ubuntu Desktop 20.04
- Ubuntu Server 20.04
- Ubuntu Desktop 18.04
- Ubuntu Server 18.04
- Ubuntu Live Server 18.04
- Ubuntu Desktop 16.04
- Ubuntu Server 16.04

Nota:

- El proyecto CentOS cambia su enfoque a CentOS Stream. CentOS Linux 8, como una reconstrucción de RHEL 8, finaliza a finales de 2021. CentOS Stream continúa después de esa fecha, sirviendo como la rama ascendente (de desarrollo) de Red Hat Enterprise Linux. Para obtener más información, consulte `<https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux>`.
- Cuando utilice Citrix Provisioning™ para transmitir dispositivos de destino Linux, cree una partición de arranque separada en la única imagen de disco compartido 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 una matriz de las distribuciones de Linux y las versiones de Xorg que admite esta versión del VDA de Linux, consulte la siguiente tabla. Para obtener más información, consulte XorgModuleABIVersions.

DISTRIBUCIÓN DE LINUX	VERSIÓN DE XORG
Amazon Linux 2	1.20
Debian 10.9	1.20
RHEL 8.4	1.20.10
RHEL 8.3	1.20.8

DISTRIBUCIÓN DE LINUX	VERSIÓN DE XORG
RHEL 8.2	1.20.8
RHEL 8.1	1.20.8
RHEL 7.9, CentOS 7.9	1.20
RHEL 7.8, CentOS 7.8	1.20
SUSE 15.3	1.20
SUSE 15.2	1.20
SUSE 12.5	1.19
Ubuntu 20.04	1.20
Ubuntu 18.04	1.19
Ubuntu 16.04	1.18

No utilice `HWE kernel` o `HWE Xorg` en Ubuntu.

Utilice PulseAudio 13.99 en RHEL 8.x.

Utilice PulseAudio 14.2 en SUSE 15.3 y PulseAudio 13.0 en SUSE 15.2.

En todos los casos, la arquitectura de procesador compatible es x86-64.

> **Nota:**

> Los escritorios GNOME y KDE son compatibles con CentOS 7, RHEL 7, RHEL 8 y SUSE 12. El escritorio Unity es compatible con Ubuntu 16.04. El escritorio GNOME es compatible con Amazon Linux 2, Debian 10.9, SUSE 15, Ubuntu 20.04 y Ubuntu 18.04. El escritorio MATE es compatible con todas las distribuciones de Linux que admite Linux VDA, excepto SUSE 12.5. Se debe instalar al menos un escritorio.

Citrix Virtual Desktops™

El Linux VDA es compatible con todas las versiones actualmente admitidas de Citrix Virtual Apps and Desktops. Para obtener información sobre el ciclo de vida de los productos Citrix y para saber cuándo Citrix deja de admitir versiones específicas de productos, consulte la Matriz del ciclo de vida de los productos Citrix.

El proceso de configuración para los VDA de Linux difiere ligeramente de los VDA de Windows. Sin embargo, cualquier conjunto de Delivery Controller™ puede intermediar escritorios Windows y Linux.

Plataformas de host y entornos de virtualización compatibles

- Servidores bare metal
- Citrix Hypervisor™
- VMware vSphere Hypervisor
- Microsoft Hyper-V
- Nutanix AHV
- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

> **Sugerencia:**
>
> Consulte la documentación del proveedor para ver la lista de plataformas compatibles.

> **Nota:**
>
> Azure, AWS y GCP son compatibles solo con el servicio Citrix Virtual Apps and Desktops™. Los servidores bare metal no son compatibles cuando se utiliza MCS para crear máquinas virtuales.

Paquetes de integración de Active Directory

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

- Samba Winbind
- Quest Authentication Services v4.1 o posterior
- Centrify DirectControl
- SSSD
- PBIS (compatible con RHEL 7, Ubuntu y Debian)

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
Amazon Linux 2	Sí	Sí	Sí	Sí	No
Debian 10.9	Sí	Sí	Sí	Sí	No
RHEL 8.4	Sí	Sí	Sí	Sí	No
RHEL 8.3	Sí	Sí	Sí	Sí	No
RHEL 8.2	Sí	Sí	Sí	Sí	No
RHEL 8.1	Sí	Sí	Sí	Sí	No
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí	Sí	Sí
RHEL 7.8, CentOS 7.8	Sí	Sí	Sí	Sí	Sí
SUSE 15.3	Sí	Sí	Sí	Sí	No
SUSE 15.2	Sí	Sí	Sí	Sí	No
SUSE 12.5	Sí	Sí	Sí	Sí	Sí
Ubuntu 20.04	Sí	Sí	Sí	Sí	Sí
Ubuntu 18.04	Sí	Sí	Sí	Sí	Sí
Ubuntu 16.04	Sí	Sí	Sí	Sí	Sí

HDX™ 3D Pro

Las capacidades HDX 3D Pro de Citrix Virtual Apps™ y Desktops le permiten ofrecer escritorios y aplicaciones que ofrecen el mejor rendimiento utilizando una Unidad de Procesamiento Gráfico (GPU) para la aceleración de hardware.

Hipervisores

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

- 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 saber qué tarjetas GPU NVIDIA admite su distribución de Linux, vaya a la matriz de compatibilidad de productos de NVIDIA y compruebe las columnas **SO de hipervisor o sin sistema operativo**, **Implementación de productos de software**, **Hardware compatible** y **Compatibilidad con SO invitado**.

Asegúrese de instalar el controlador vGPU más reciente para su tarjeta GPU. Actualmente, el VDA de Linux admite hasta vGPU 13. Para obtener más información, consulte GPU compatibles con el software NVIDIA Virtual GPU.

Información general de la instalación

Esta sección le guía a través de los siguientes procedimientos:

- Instalación rápida mediante la instalación sencilla (recomendado para instalaciones nuevas)
- Instalación manual basada en varias distribuciones de Linux
- Usar MCS para crear máquinas virtuales Linux
- Crear VDA de Linux unidos a un dominio y no unidos a un dominio en Citrix Virtual Apps and Desktops™ Standard para Azure
- Usar Citrix Provisioning™ para crear máquinas virtuales Linux
- Configurar Delivery Controllers para XenDesktop 7.6 y versiones anteriores

Instalación rápida mediante la instalación sencilla (Recomendado)

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, debe usar Machine Creation Services (MCS). Para obtener más información, consulte Usar Machine Creation Services (MCS) para crear máquinas virtuales Linux.
- 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 dominio Kerberos: el nombre de dominio Kerberos
- Nombre de dominio completo (FQDN) del dominio

> **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.

Consideraciones

- El nombre del grupo de trabajo, de forma predeterminada, es el nombre de dominio. Para personalizar el grupo de trabajo en su entorno, haga lo siguiente:

  a. Cree el archivo /tmp/ctxinstall.conf en la máquina VDA de Linux.

  b. Agregue la línea workgroup=\<your workgroup\> al archivo y guarde los cambios.

- Centrify no admite la configuración DNS IPv6 pura. Se requiere al menos un servidor DNS que use 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:

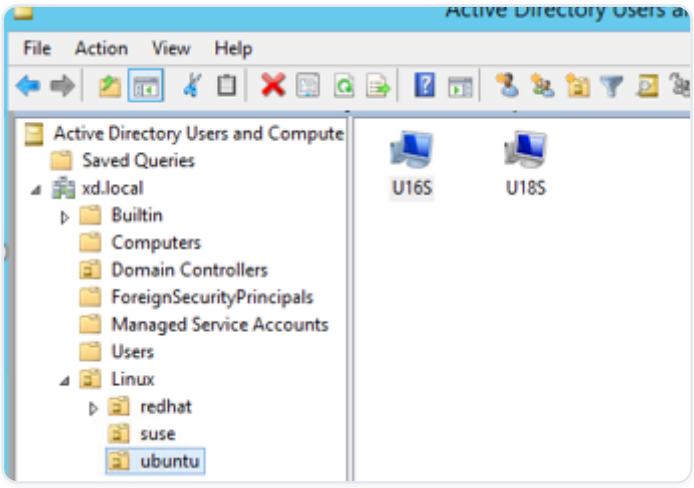
a. Abra **Herramientas administrativas** en el controlador de dominio.

b. Seleccione **Sitios y servicios de Active Directory**. c. Agregue una dirección de subred adecuada para **Subredes**.

- 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. Cree el archivo /tmp/ctxinstall.conf en el VDA.

  c. Agregue la línea ou=\<your ou\> al archivo /tmp/ctxinstall.conf.

  Los valores de OU varían según los diferentes métodos de AD. Consulte la siguiente tabla.

OS	WINBIND	SSSD	CENTRIFY	PBIS
Amazon Linux 2	`ou="Linux/amazon"`	`ou="Linux/amazon"`	`ou="XD.LOCAL/Linux/amazon"`	`ou="Linux/amazon"`
Debian	`ou="Linux/debian"`	`ou="Linux/debian"`	`ou="XD.LOCAL/Linux/debian"`	`ou="Linux/debian"`

OS	WINBIND	SSSD	CENTRIFY	PBIS
RHEL 8	`ou="OU=redhat,OU=Linux"`	`ou="OU=redhat,OU=Linux"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
RHEL 7	`ou="Linux/redhat"`	`ou="Linux/redhat"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
SUSE	`ou="Linux/suse"`	`ou="Linux/suse"`	`ou="XD.LOCAL/Linux/suse"`	`ou="Linux/suse"`
Ubuntu	`ou="Linux/ubuntu"`	`ou="Linux/ubuntu"`	`ou="XD.LOCAL/Linux/ubuntu"`	`ou="Linux/ubuntu"`

- La instalación fácil es compatible con 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 el 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.

- Si elige Centrify como método para unirse a un dominio, el script ctxinstall.sh requiere el paquete de Centrify. Hay dos formas en que ctxinstall.sh puede obtener el paquete de Centrify:
  - La instalación fácil ayuda a descargar el paquete de Centrify de Internet automáticamente. A continuación se muestran las URL para cada distribución:

Para RHEL: wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956>`

Para CentOS: wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.186648044.558673738.1478847956>`

Para SUSE: wget `<http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-suse10-x86_64.tgz?_ga=1.10831088.558673738.1478847956>`

Para Ubuntu/Debian: wget `<https://downloads.centrify.com/products/infrastructure-services/19.9/centrify-infrastructure-services-19.9-deb8-x86_64.tgz?_ga=2.151462329.1042350071.1592881996-604509155.1572850145>`

- Obtenga el paquete de Centrify de un directorio local. Para designar el directorio del paquete de Centrify, haga lo siguiente:

  a. Cree el archivo /tmp/ctxinstall.conf en el servidor Linux VDA si no existe.

  b. Agregue la línea "centrifypkgpath=\<path name\>" al archivo.

  Por ejemplo:

```
cat /tmp/ctxinstall.conf

set "centrifypkgpath=/home/mydir"

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 PBIS. Hay dos formas para que ctxinstall.sh obtenga el paquete PBIS:
    - La instalación fácil ayuda a descargar el paquete PBIS de Internet automáticamente. A continuación, se muestran las URL para cada distribución:

      CentOS 7, RHEL 7, SUSE 12.5: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh`

      Amazon Linux 2, RHEL 8, SUSE 15.3, SUSE 15.2: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh`

Debian, Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh`

- Obtenga una versión específica del paquete PBIS de Internet. Para ello, cambie la línea "pbisDownloadPath" en el archivo /opt/Citrix/VDA/sbin/ctxinstall.sh para designar la URL del paquete PBIS.

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



Paso 2: Preparar el hipervisor

Se requieren algunos cambios al ejecutar el Linux VDA 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 horaria en Citrix Hypervisor™

Cuando la función de sincronización horaria de Citrix Hypervisor está habilitada, dentro de cada máquina virtual Linux paravirtualizada, experimentará problemas con NTP y Citrix Hypervisor. 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 horaria del host. No se requieren cambios en el modo HVM.

Si está ejecutando un kernel de Linux paravirtualizado con Citrix VM Tools instalado, puede comprobar si la función de sincronización horaria de Citrix Hypervisor 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, no es necesario realizar los siguientes pasos.

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 añada 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 VM de 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 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 VM de Linux, seleccione **Servicios de integración**.
3. Asegúrese de que **Sincronización de hora** esté seleccionada.

> **Nota:**

> Este enfoque es diferente al de VMware y Citrix Hypervisor, donde la sincronización de la hora del host está deshabilitada 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 la 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 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 **Propiedades de la máquina virtual**, abra la pestaña **Opciones**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Avanzado**, desactive **Sincronizar la hora del invitado con el host**.

Paso 3: (Solo para Ubuntu 16.04) Instalar OpenJDK 11

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la última versión de OpenJDK 11 desde `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.
4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

Paso 4: Descargar 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.

Paso 5: Instalar el paquete de Linux VDA

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

Para distribuciones RHEL y CentOS:

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

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, añada la línea `deb http://deb.debian.org/debian/ oldstable main` al archivo /etc/apt/sources.list.

Para distribuciones SUSE:

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

Paso 6: Instalar controladores NVIDIA GRID

La habilitación de HDX™ 3D Pro requiere que instale 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:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Para instalar y configurar los controladores de VM invitados 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 en la VM.

Paso 7: Configure el entorno de ejecución para completar la instalación

> **Nota:**

> Antes de configurar el entorno de ejecución, asegúrese de que la configuración regional `en_US.UTF-8` se haya instalado 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 de Linux VDA, configure el entorno de ejecución mediante el script ctxinstall.sh. Puede ejecutar el script en modo interactivo o en modo silencioso.

> **Nota:**

> La instalación fácil puede parecer que no responde mientras descarga el tiempo de ejecución de .NET, que tiene un tamaño superior a 27 MB. Para ver el progreso de la descarga, consulte /var/log/ctxinstall.log.

> **Modo interactivo:**

Para realizar una configuración manual, ejecute el siguiente comando y escriba el parámetro correspondiente en cada solicitud.

```
sudo /opt/Citrix/VDA/sbin/ctxinstall.sh
```

Modo silencioso:

Para usar la instalación fácil en modo silencioso, establezca las siguientes variables de entorno antes de ejecutar ctxinstall.sh.

- **CTX_EASYINSTALL_HOSTNAME=host-name** – Indica el nombre de host del servidor Linux VDA.
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** – Dirección IP de DNS.

- **CTX_EASYINSTALL_NTPS=address-of-ntps** – Dirección IP o nombre de cadena del servidor NTP.
- **CTX_EASYINSTALL_DOMAIN=domain-name** – El nombre NetBIOS del dominio.
- **CTX_EASYINSTALL_REALM=realm-name** – El nombre del ámbito de Kerberos.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind \| sssd \| centrify \| pbis** – Indica el método de integración de Active Directory.
- **CTX_EASYINSTALL_USERNAME=domain-user-name** – Indica el nombre del usuario de dominio; se utiliza para unirse al dominio.
- **CTX_EASYINSTALL_PASSWORD=password** – Especifica la contraseña del usuario de dominio; se utiliza para unirse al dominio.

El script ctxsetup.sh utiliza las siguientes variables:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – El VDA de Linux admite especificar un nombre de Delivery Controller mediante un registro CNAME de DNS.
- **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_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Los servicios de escritorio virtual de Linux se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Los servicios de escritorio virtual 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 el escritorio virtual de Linux.
- **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_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_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 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. Si no es necesario, establézcalo en **\<none\>**.
- **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_FAS_LIST='list-fas-servers'** – Los servidores de Federated Authentication Service (FAS) se configuran a través de la directiva de grupo de AD. El VDA de Linux no admite la directiva de grupo de AD, pero puede proporcionar una lista de servidores FAS separados 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.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET Runtime 6.0 para admitir el nuevo servicio de agente de intermediación (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/mate** – Especifica el entorno de escritorio GNOME o MATE que se utilizará en las sesiones. 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 la variable en **mate**.

> **Nota:**
>
> También puede cambiar el entorno de escritorio para un usuario de sesión de destino siguiendo estos pasos:
>
> 1\. Cree un archivo `.xsession` o `.Xclients` en el directorio **$HOME/<username\>** del VDA. Si utiliza Amazon Linux 2, cree un archivo `.Xclients`. Si utiliza otras distribuciones, cree un archivo `.xsession`.

\>2\. Edite el archivo `.xsession` o `.Xclients` para especificar un entorno de escritorio según las distribuciones.

- **Para el escritorio MATE en Amazon Linux 2, CentOS, Debian, RHEL, SUSE 15 y Ubuntu**

```
MSESSION="$(type -p mate-session)"
```

\> if ; then

```
    exec mate-session
```

\> fi

- **Para el escritorio GNOME en CentOS, RHEL, SUSE 15 y SUSE 12.5**

```
GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi
```

\>- **Para el escritorio GNOME en Amazon Linux 2, Ubuntu y Debian**

```
    GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    exec gnome-session
```

\> fi

3\. Comparta el permiso de archivo 700 con el usuario de sesión de destino.

- **CTX_XDL_START_SERVICE=Y \| N** – Si los servicios del VDA de Linux se inician o no cuando se completa la configuración.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT** – El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Si no se establece ningún parámetro, la instalación revierte al modo interactivo, con una solicitud de entrada del usuario. Cuando todos los parámetros ya están establecidos a través de las variables de entorno, el script ctxinstall.sh sigue solicitando la entrada del usuario para la ruta de instalación de .NET Runtime 6.0.

En modo silencioso, debe ejecutar los siguientes comandos para establecer las variables de entorno y, a continuación, ejecutar el script ctxinstall.sh.

```
export CTX_EASYINSTALL_HOSTNAME=host-name


export CTX_EASYINSTALL_DNS=ip-address-of-dns


export CTX_EASYINSTALL_NTPS=address-of-ntps
```

```
export CTX_EASYINSTALL_DOMAIN=domain-name

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis

export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

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_VDI_MODE=Y | N

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_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y | N
```

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

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_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \
```

```
CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Paso 8: 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 9: Ejecutar el Linux VDA

Iniciar el Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Detener el Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **Nota:**
>
> Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando `service ctxmonitorservice stop` 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 /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart
```

```
sudo /sbin/service ctxvda start
```

Comprobar el estado del Linux VDA:

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

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

Paso 10: Crear catálogos de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops™

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 combine máquinas VDA de Linux y Windows en el mismo catálogo de máquinas.

Nota:

Las versiones anteriores de Citrix Studio no admitían el concepto de "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 una máquina del dominio de Active Directory y la vuelve a unir, debe quitar y agregar la máquina al catálogo de máquinas de nuevo.

Paso 11: Crear grupos de entrega en Citrix Virtual Apps™ o Citrix Virtual Desktops

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 combine 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 2112.

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 logs for screen printing):

`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. Elimine 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 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.



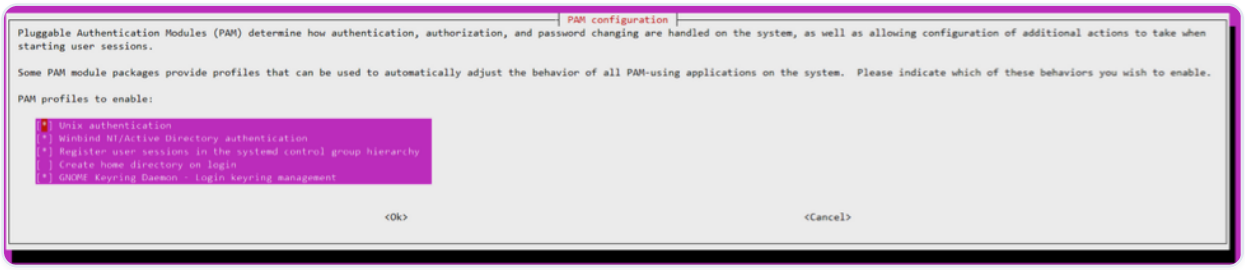
2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting normally.
```

Sugerencia:

La causa principal de este problema es que el directorio de inicio no se crea para el administrador de 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** está 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, use 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/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.

Instalar Linux Virtual Delivery Agent para Amazon Linux 2, CentOS y RHEL 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 distribución de Linux para la instalación del VDA

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 VDA de Linux como una máquina virtual 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 8/RHEL 7 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 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 /sbin/service chronyd restart
```

Paso 1g: Instalar OpenJDK 11

El VDA de Linux requiere la presencia de OpenJDK 11.

- Si utiliza CentOS o RHEL, OpenJDK 11 se instala automáticamente como dependencia al instalar el VDA de Linux.
- Si utiliza Amazon Linux 2, ejecute el siguiente comando para habilitar e instalar OpenJDK 11:

```
amazon-linux-extras install java-openjdk11
```

Confirme la versión correcta:

```
sudo yum info java-11-openjdk
```

Es posible que el OpenJDK preempaquetado sea una versión anterior. Actualice a OpenJDK 11:

```
sudo yum -y update java-11-openjdk
```

Paso 1h: Instalar PostgreSQL

El VDA de Linux requiere PostgreSQL 10.5 o posterior en RHEL 8, o PostgreSQL 9.2 o posterior en RHEL 7.

Instale los siguientes paquetes:

```
sudo yum -y install postgresql-server



sudo yum -y install postgresql-jdbc
```

El siguiente paso posterior a la instalación es necesario para inicializar la base de datos y para asegurarse de que el servicio se inicie al arrancar la máquina. Esta acción crea archivos de base de datos en **/var/lib/pgsql/data**. El comando difiere entre PostgreSQL 10 y 9:

```
sudo postgresql-setup initdb
```

Paso 1i: Iniciar PostgreSQL

Inicie el servicio al arrancar la máquina e inicie el servicio inmediatamente:

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

Compruebe la versión de PostgreSQL mediante:

```
psql --version
```

(Solo RHEL 7) verificar que el directorio de datos está configurado mediante la utilidad de línea de comandos **psql**:

```
sudo -u postgres psql -c 'show data_directory'
```

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 Citrix Hypervisor™

Cuando la función de sincronización horaria de Citrix Hypervisor está habilitada, dentro de cada máquina virtual Linux paravirtualizada, experimentará problemas con NTP y Citrix Hypervisor. 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 horaria del host. No se requieren cambios en el modo HVM.

Si está ejecutando un kernel Linux paravirtualizado con Citrix VM Tools instalado, puede verificar si la función de sincronización horaria de Citrix Hypervisor 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 horaria está habilitada y debe deshabilitarse.
- 1 - La función de sincronización horaria 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 horaria escribiendo 1 en el archivo:

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

Para que este cambio sea permanente y persista después de un reinicio, 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 garantizar 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 la **Sincronización de hora** esté seleccionada.

> **Nota:**
>
> Este enfoque es diferente al de VMware y 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 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 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 **Propiedades de la máquina virtual**, abra la ficha **Opciones**.
4. Seleccione **VMware Tools**.
5. En el cuadro **Avanzado**, desactive **Sincronizar hora del invitado con el host**.

Paso 3: Agregar la máquina virtual (VM) Linux al dominio de Windows

El VDA de Linux admite varios métodos para agregar 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 podrían 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

Instale o actualice los paquetes necesarios:

Para RHEL 8:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
oddjob-mkhomedir realmd authselect
```

Para Amazon Linux 2, CentOS 7 y RHEL 7:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
authconfig oddjob-mkhomedir
```

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 /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 8:

   ```
   sudo authselect select winbind with-mkhomedir --force
   ```

   Para Amazon Linux 2 y RHEL 7:

```
sudo authconfig --disablecache --disablesssd --disablesssdauth --
enablewinbind --enablewinbindauth --disablewinbindoffline --
smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM --
krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --
winbindtemplateshell=/bin/bash --enablemkhomedir --updateall
```

Donde **REALM** es el nombre del ámbito 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`

Ignore cualquier error devuelto por el comando `authconfig` sobre el fallo al iniciar el servicio `winbind`. Los errores pueden ocurrir cuando `authconfig` intenta iniciar el servicio `winbind` sin que la máquina se haya unido aún al dominio.

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 RHEL 8) 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 con 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 RHEL 8:

```
sudo realm join -U user --client-software=winbind REALM
```

Para Amazon Linux 2 y RHEL 7:

```
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 añadir equipos al dominio.

Configurar PAM para Winbind

De forma predeterminada, 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 Winbind:

```
sudo /sbin/service winbind restart
```

> **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}`

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 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 del shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre del 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 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 del 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 sean válidos y no hayan 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.

Servicios de autenticación de Quest

Configurar Quest en el controlador de dominio

Suponga que ha instalado y configurado el software de 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 VDA de Linux

Para permitir que los usuarios de 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 **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 VDA de Linux

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=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 mediante 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.

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 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
```

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.

Centrify DirectControl

Unirse a un dominio de Windows

Con el agente de 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 Unido al dominio es válido y que el modo CentrifyDC devuelve conectado. Si el modo permanece atascado en el estado inicial, el cliente de Centrify está experimentando problemas de conexión o autenticación del 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 y CentOS, haga lo siguiente:

1. Unir el dominio y crear el keytab del host
2. Configurar SSSD
3. Habilitar SSSD
4. verificar la configuración de Kerberos
5. verificar la autenticación de usuario

Unir el dominio y crear el keytab del host

SSSD no proporciona funciones de cliente de Active Directory para unir el dominio y administrar el archivo keytab del sistema. En su lugar, puede utilizar `adcli`, `realmd` o `Samba`.

Esta sección describe el enfoque `Samba` para Amazon Linux 2 y RHEL 7, y el enfoque `adcli` para RHEL 8. Para `realmd`, consulte la documentación de RHEL o CentOS. Estos pasos deben seguirse antes de configurar SSSD.

- **Samba (Amazon Linux 2 y RHEL 7):**

  Instale o actualice los paquetes necesarios:

  ```
  sudo yum -y install krb5-workstation authconfig oddjob-mkhomedir samba-common-tools
  ```

  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 Kerberos en mayúsculas y **domain** es el nombre corto de NetBIOS del dominio de Active Directory.

> **Nota:**
>
> La configuración de este artículo está pensada para el modelo de dominio único y bosque único. Configure Kerberos según su infraestructura de AD.
>
> Si se requiere la búsqueda basada en DNS del servidor KDC y el nombre del reino, agregue las dos opciones siguientes al comando anterior:

`--enablekrb5kdcdns --enablekrb5realmdns`

Abra **/etc/samba/smb.conf** y agregue 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`

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 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.

- **Adcli (RHEL 8):**

  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**.

Un ejemplo de configuración de **sssd.conf** para RHEL 7 (se pueden agregar opciones adicionales según sea necesario):

```
[sssd]
config_file_version = 2
domains = ad.example.com
services = nss, pam

[domain/ad.example.com]
# Uncomment if you need offline logins
# cache_credentials = true

id_provider = ad
auth_provider = ad
access_provider = ad
ldap_id_mapping = true
ldap_schema = ad

# Should be specified as the lower-case version of the long version of the Active Directory domain.
ad_domain = ad.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.example.com**, **server.ad.example.com** por los valores correspondientes. Para obtener más información, consulte sssd-ad(5) - página man de Linux.

(Solo RHEL 8) Abra **/etc/sssd/sssd.conf** y agregue 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`

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`

Habilitar SSSD

Para RHEL 8:

Ejecute los siguientes comandos para habilitar SSSD:

```
sudo systemctl restart sssd

sudo systemctl enable sssd.service

sudo chkconfig sssd on
```

Para Amazon Linux 2, CentOS 7 y RHEL 7:

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 service sssd start



sudo chkconfig sssd on
```

verificar 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 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
```

verificar 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 utilizando primero 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

Descargue el paquete PBIS necesario

Para CentOS 7 y RHEL 7, por ejemplo:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/
pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Para Amazon Linux 2 y RHEL 8, 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
```

Haga que el script de instalación de PBIS sea ejecutable

Para CentOS 7 y RHEL 7, por ejemplo:

```
chmod +x pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Para Amazon Linux 2 y RHEL 8, por ejemplo:

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

Ejecute el script de instalación de PBIS

Para CentOS 7 y RHEL 7, por ejemplo:

```
sh pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Por ejemplo, para Amazon Linux 2 y RHEL 8:

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

Unirse al dominio de Windows

El 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
```

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 Runtime 6.0 como requisito previo

Antes de instalar el VDA de Linux, instale .NET Runtime 6.0 según las instrucciones de `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

Después de instalar .NET Runtime 6.0, 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 5: Descargar 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 **Componentes** para descargar el paquete de Linux VDA que coincida con su distribución de Linux.

Paso 6: Instalar el Linux VDA

Puede realizar una instalación nueva o actualizar una instalación existente desde las dos versiones anteriores y desde una versión LTSR.

Para realizar una instalación nueva

1. (Opcional) Desinstalar la versión anterior

   Si instaló una versión anterior que no sea una de las dos anteriores ni una versión LTSR, desinstálela antes de instalar la nueva versión.

   a. Detenga los servicios de Linux VDA:

   ```
   sudo /sbin/service ctxvda stop



   sudo /sbin/service ctxhdx stop
   ```

   Nota:

> Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando **service ctxmonitorservice stop** 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. Descargar 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 **Componentes** para descargar el paquete de Linux VDA que coincida con su distribución de Linux.

3. Instalar el VDA de Linux

   - Instale el software VDA de Linux mediante `Yum`:

     Para Amazon Linux 2:

     ```
     sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
     ```

     Para RHEL 8:

     ```
     sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
     ```

     Para CentOS 7 y RHEL 7:

     ```
     sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
     ```

   - Instale el software VDA de Linux mediante el administrador de paquetes RPM. Antes de hacerlo, debe resolver las siguientes dependencias:

Para Amazon Linux 2:

```
sudo rpm -i XenDesktopVDA-<version>.amzn2.x86_64.rpm
```

Para RHEL 8:

```
sudo rpm -i XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

Para CentOS 7 y RHEL 7:

```
sudo rpm -i XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

Lista de dependencias RPM para RHEL 8:

```
qt5-qtbase >= 5.5~


ibus >= 1.5


nss-tools >= 3.44.0


gperftools-libs >= 2.4


cyrus-sasl-gssapi >= 2.1


python2 >= 2.7~


postgresql-jdbc >= 42.2.3
```

```
postgresql-server >= 10.6


java-11-openjdk >= 11


icoutils >= 0.32


firewalld >= 0.8.0


policycoreutils-python-utils >= 2.9


python3-policycoreutils >= 2.9


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

motif >= 2.3.4

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.4
```

```
findutils >= 4.6


gawk >= 4.2


sed >= 4.5


cups >= 2.2


foomatic-filters >= 4.0.9


cups-filters >= 1.20.0


ghostscript >= 9.25


libxml2 >= 2.9


libmspack >= 0.7
```

Lista de dependencias RPM para Amazon Linux 2, CentOS 7 y RHEL 7:

```
qt5-qtbase >= 5.5~


libmspack >= 0.5
```

```
ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

gperftools-libs >= 2.4

nss-tools >= 3.44.0

postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12
```

```
dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

motif >= 2.3.4

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2
```

```
findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.6.0

gperftools-libs >= 2.4
```

```
rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

pmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
```

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.

Después de instalar el VDA de Linux en RHEL 7.x, ejecute el comando `sudo yum install -y python-websockify x11vnc`. El objetivo es instalar `python-websockify` y `x11vnc` manualmente para usar la función de proyección de sesiones. Para obtener más información, consulte Proyección de sesiones.

Para actualizar una instalación existente

Puede actualizar una instalación existente desde las dos versiones anteriores y desde una versión 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.

- Para actualizar el software mediante `Yum`:

  Para Amazon Linux 2:

  ```
  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
  ```

  Para RHEL 8:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
  ```

  Para CentOS 7 y RHEL 7:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
  ```

- Para actualizar el software mediante el administrador de paquetes RPM:

  Para Amazon Linux 2:

  ```
  sudo rpm -U XenDesktopVDA-<version>.amzn2.x86_64.rpm
  ```

  Para RHEL 8:

  ```
  sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
  ```

  Para CentOS 7 y RHEL 7:

  ```
  sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
  ```

Nota:

Si utiliza RHEL 7, asegúrese de completar los siguientes pasos después de ejecutar los comandos de actualización anteriores:

1. ejecute `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v`

> `"DotNetRuntimePath" -d "/opt/rh/rh-dotnet31/root/usr/bin/" --force` para establecer la ruta de tiempo de ejecución de .NET correcta.
>
> 2. Reinicie el servicio `ctxvda`.

> **Importante:**

> Reinicie la máquina Linux VDA después de actualizar el software.

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 el Administrador de GPU virtual NVIDIA GRID (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 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 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 resoluciones grandes y las capacidades de varios monitores, necesita una licencia NVIDIA válida. Para solicitar la licencia, consulte la documentación del producto en "GRID Licensing Guide.pdf - DU-07757-001 September 2015".

Paso 8: Configure el VDA de Linux

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_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. Establecido en N de forma predeterminada.
- **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 un alias CNAME.
- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP, que es el puerto 80 de forma predeterminada.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** - Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina. El valor se establece en Y de forma predeterminada.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Los servicios de Linux Virtual Desktop requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos necesarios (puertos 80 y 1494 de forma predeterminada)

automáticamente en el firewall del sistema para Linux Virtual Desktop. Establecido en Y de forma predeterminada.

- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4 \| 5** – 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. Especifique el método de integración de Active Directory compatible que desea utilizar:
  - 1 – Samba Winbind
  - 2 – Quest Authentication Services
  - 3 – Centrify DirectControl
  - 4 – SSSD
  - 5 – PBIS
- **CTX_XDL_HDX_3D_PRO=Y \| N** – El VDA de Linux 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_VDI_MODE=Y \| N** – Si se debe configurar la máquina como un modelo de entrega de escritorio dedicado (VDI) o como un modelo de entrega de escritorio compartido alojado. Para entornos HDX 3D Pro, establezca esta variable en Y. Esta variable está establecida en N de forma predeterminada.
- **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. Esta variable está establecida en **\<none\>** de forma predeterminada.
- **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. Esta variable está establecida 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). Esta variable está establecida en **\<none\>** de forma predeterminada.

- **CTX_XDL_FAS_LIST='list-fas-servers'** – Los servidores de Federated Authentication Service (FAS) se configuran a través de la directiva de grupo de AD. El VDA de Linux no es compatible con la directiva de grupo de AD, pero puede proporcionar una lista de servidores FAS separados 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.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET Runtime 6.0 para admitir el nuevo servicio de agente de intermediación (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Especifica el entorno de escritorio GNOME o MATE que se utilizará en las sesiones. Si deja la variable sin especificar, se utiliza el escritorio actualmente instalado en el VDA. Sin embargo, si el escritorio actualmente instalado es MATE, debe establecer el valor de la variable en **mate**.

> **Nota:**
>
> También puede cambiar el entorno de escritorio para un usuario de sesión de destino siguiendo estos pasos:
>
> 1\. Cree un archivo `.xsession` o `.Xclients` en el directorio **$HOME/<username\>** del VDA. Si utiliza Amazon Linux 2, cree un archivo `.Xclients`. Si utiliza otras distribuciones, cree un archivo `.xsession`.
>
> \>2\. Edite el archivo `.xsession` o `.Xclients` para especificar un entorno de escritorio según las distribuciones.
>
> - **Para el escritorio MATE en Amazon Linux 2, CentOS y RHEL**
>
>   ```
>   MSESSION="$(type -p mate-session)"
>   ```
>
> \> if ; then

```
    exec mate-session
```

\> fi

- **Para el escritorio GNOME en CentOS y RHEL**

```
GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi
```

\>- **Para el escritorio GNOME en Amazon Linux 2**

```
    GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    exec gnome-session
```

\> fi

3\. Comparta el permiso de archivo 700 con el usuario de la sesión de destino.

- **CTX_XDL_START_SERVICE=Y \| N** – Si los servicios del VDA de Linux se inician o no cuando se completa la configuración del VDA de Linux. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT** – El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N


export CTX_XDL_DDC_LIST='list-ddc-fqdns'


export CTX_XDL_VDA_PORT=port-number


export CTX_XDL_REGISTER_SERVICE=Y|N


export CTX_XDL_ADD_FIREWALL_RULES=Y|N


export CTX_XDL_AD_INTEGRATION=1|2|3|4|5


export CTX_XDL_HDX_3D_PRO=Y|N


export CTX_XDL_VDI_MODE=Y|N
```

```
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_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \
```

```
CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Eliminar cambios de configuración

En algunos escenarios, es posible que tenga que 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.

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

Después de configurar el VDA de Linux con 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 /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Detener el VDA de Linux:

Para detener los servicios del VDA de Linux:

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

Nota:

Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando `service ctxmonitorservice stop` 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 /sbin/service ctxvda stop


sudo /sbin/service ctxhdx restart


sudo /sbin/service ctxvda start
```

Comprobar el estado del VDA de Linux:

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

```
sudo /sbin/service ctxvda status


sudo /sbin/service ctxhdx status
```

Paso 11: Crear el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops™

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 **Sistema operativo 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 primeras versiones de Citrix Studio no admitían la noción de un "sistema operativo 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 el grupo de entrega en Citrix Virtual Apps™ o Citrix Virtual Desktops

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, 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 2112.

Instalar el Virtual Delivery Agent de Linux para SUSE manualmente

> **Importante:**
>
> Para instalaciones nuevas, le recomendamos que utilice la 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 instalación

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 cómo configurar los distintos ajustes y servicios de red utilizados por el VDA de Linux. La configuración de la 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. Solo SLED 12: En la ficha **Opciones globales**, cambie el **Método de configuración de red** a **Servicio Wicked**.
4. Abra la ficha **Nombre de host/DNS**.
5. Seleccione **Asignar nombre de host a IP de bucle invertido**.
6. Desactive **Cambiar nombre de host mediante DHCP**.
7. Seleccione **Asignar nombre de host a IP de bucle invertido**.
8. Seleccione la opción **Usar directiva personalizada** para **Modificar configuración de DNS**.
9. Edite lo siguiente para que refleje la configuración de su red:

    - **Nombre de host** – Agregue el nombre de host DNS de la máquina.
    - **Nombre de dominio** – Agregue el nombre de dominio 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.

> **Nota:**

> El VDA de Linux no admite actualmente 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.

Inhabilitar DNS de multidifusión

Solo en SLED, la configuración predeterminada tiene habilitado el DNS de multidifusión (mDNS), lo que puede provocar resultados de resolución de nombres incoherentes. mDNS no está habilitado en SLES de forma predeterminada, por lo que no se requiere ninguna acción.

Para inhabilitar mDNS, edite **/etc/nsswitch.conf** y cambie la línea que contiene:

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

A:

```
hosts: files dns
```

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 está 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 ninguna de estas máquinas, revise los pasos antes de continuar.

Paso 1c: Configurar el servicio NTP

Es fundamental 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 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 15.3 y SUSE 15.2:

1. Inicie la herramienta YaST basada en la interfaz de usuario.
2. Seleccione **Network Services** y, a continuación, **NTP Configuration**.
3. En la sección **Start NTP Daemon**, seleccione **Now and on Boot**.
4. Seleccione **Dynamic** para **Configuration Source**.
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 descomente 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
```

Para SUSE 12.5:

1. Abra la configuración NTP de YaST y seleccione la ficha **General Settings**.
2. En la sección Start NTP Daemon, marque **Now and on Boot**.
3. Si está presente, seleccione el elemento **Undisciplined Local Clock (LOCAL)** y haga clic en **Delete**.
4. Agregue una entrada para un servidor NTP haciendo clic en **Add**.
5. Seleccione el **Server Type** y haga clic en **Next**.
6. Escriba el nombre DNS del servidor NTP en el campo Address. Este servicio normalmente se aloja en el controlador de dominio de Active Directory.
7. Deje el campo Options sin cambios.
8. Haga clic en **Test** para verificar que el servicio NTP es accesible.
9. Haga clic en **OK** en todas las ventanas para guardar los cambios.

Nota:

Para implementaciones de SLES 12, es posible que el demonio NTP no se inicie debido a un problema conocido de SUSE con las directivas de AppArmor. Siga la resolución para obtener información adicional.

Paso 1d: Instalar los paquetes dependientes de Linux VDA

El software Linux VDA para SUSE Linux Enterprise depende de los siguientes paquetes:

- Postgresql10-server 10.12 o posterior
- OpenJDK 11
- Open Motif Runtime Environment 2.3.1 o posterior
- Cups 1.6.0 o posterior
- Filtros Foomatic 3.0.0 o posterior
- ImageMagick 6.8 o posterior

Añadir repositorios

Puede obtener algunos paquetes necesarios, como PostgreSQL e ImageMagick, del Kit de desarrollo de software (SDK) de SUSE Linux Enterprise. Para obtener los paquetes, añada el repositorio del SDK mediante YaST o descargue el archivo de imagen del SDK y luego móntelo localmente mediante los siguientes comandos:

```
sudo mkdir -p /mnt/sdk



sudo mount -t iso9660 path-to-iso/SLE-12-SP5-SDK-DVD-x86_64-GM-DVD1.iso /
mnt/sdk



sudo zypper ar -f /mnt/sdk sdk
```

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 de qué enfoque de integración de Active Directory se utilice. Consulte la siguiente descripción.

Instalar OpenJDK 11

El VDA de Linux requiere la presencia de OpenJDK 11.

Para instalar OpenJDK 11, ejecute el siguiente comando:

```
sudo zypper install java-11-openjdk
```

Instalar PostgreSQL

En SLED/SLES 12, instale los paquetes:

```
sudo zypper install postgresql-init
```

```
sudo zypper install postgresql10-server
```

```
sudo zypper install postgresql-jdbc
```

Se requieren pasos posteriores a la instalación para inicializar el servicio de base de datos y para asegurar que PostgreSQL se inicie al arrancar la máquina:

```
sudo systemctl enable postgresql
```

```
sudo systemctl restart postgresql
```

Los archivos de la base de datos se encuentran en /var/lib/pgsql/data.

Eliminar repositorios

Con los paquetes dependientes instalados, ejecute los siguientes comandos para eliminar el repositorio SDK que se configuró anteriormente y los medios montados:

```
sudo zypper rr sdk
```

```
sudo umount /mnt/sdk
```

```
sudo rmdir /mnt/sdk
```

Paso 2: Preparar la VM de Linux para 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 está ejecutando la máquina Linux en hardware físico.

Corregir la sincronización de la hora en Citrix Hypervisor™

Si la función de sincronización de la hora de Citrix Hypervisor está habilitada, dentro de cada VM de Linux paravirtualizada experimentará problemas con NTP y Citrix Hypervisor. Ambos intentan administrar el reloj del sistema. Para evitar que el reloj se desincronice con otros servidores, el reloj del sistema dentro de cada invitado Linux debe sincronizarse con NTP. Este caso requiere deshabilitar la sincronización de la hora del host. No se requieren cambios en el modo HVM.

Si está ejecutando un kernel de Linux paravirtualizado con Citrix VM Tools instaladas, puede comprobar si la función de sincronización de la hora de Citrix Hypervisor está presente y habilitada desde dentro de la VM de 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 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 la 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 sea correcta:

```
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 Hyper-V para Linux 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, 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 horaria** esté seleccionada.

> **Nota:**

> Este enfoque es diferente al de VMware y 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

Si la función de sincronización horaria 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 horaria del host.

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

1. Abra vSphere Client.
2. Editar la configuración de la VM 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 sistema operativo invitado con la del host**.

Paso 3: Agregar la máquina virtual (VM) Linux al dominio de Windows

El VDA de Linux admite varios métodos para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Quest Authentication Service
- 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

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 **También usar información de SMB para la autenticación de Linux**.

- Marque **Crear directorio de inicio 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 Linux VDA.

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 equipos al dominio y haga clic en **Aceptar**.
6. Se muestra un mensaje que indica que la operación se realizó correctamente.
7. Si se le pide que instale algunos paquetes de samba y krb5, haga clic en **Instalar**.

Es posible que YaST haya indicado que estos cambios requieren que se reinicien algunos servicios o la máquina. Le recomendamos que reinicie la máquina:

```
su -



reboot
```

Solo SUSE 12: Parchear el nombre de la caché de credenciales de Kerberos

SUSE 12 ha cambiado la especificación predeterminada del nombre de la caché de credenciales de Kerberos de la habitual **FILE:/tmp/krb5cc_%{uid}** a **DIR:/run/user/%{uid}/krb5cc**. Este nuevo método de almacenamiento en caché DIR no es compatible con Linux VDA y debe cambiarse manualmente. Como usuario root, edite **/etc/krb5.conf** y agregue la siguiente configuración en la sección **\[libdefaults\]** si no está establecida:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

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 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 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 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 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 Winbind PAM está configurado correctamente, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\\username

id -u
```

verificar que se haya 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 sean válidos y no hayan 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.

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 las 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 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 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 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 mediante el comando Quest `vastool`:

```
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.

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 de la caché de credenciales Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
```

Salir 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.

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 **usuario** es cualquier usuario del 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 va a unir 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** de **CentrifyDC** devuelve **connected**. Si el modo permanece atascado en el estado inicial, el cliente de Centrify está experimentando problemas de conexión o autenticación del 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, complete los siguientes pasos:

1. Unir el dominio y crear keytabs 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

Unir el dominio y crear 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 `Samba`. Complete los siguientes pasos antes de configurar SSSD.

1. Detenga y deshabilite el demonio del Name Service Cache Daemon (NSCD).

```
sudo systemctl stop nscd



sudo systemctl disable nscd
```

2. Instale o actualice los paquetes necesarios:

```
sudo zypper install krb5-client



sudo zypper install samba-client
```

3. 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 = 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. **fqdn-of-domain-controller** es el FQDN del controlador de dominio.

4. 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



    realm = REALM



    security = ADS



    kerberos method = secrets and keytab



    client signing = yes



    client use spnego = yes
```

domain es el nombre corto de NetBIOS de un dominio de Active Directory, como EXAMPLE.

5. 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
```

6. 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:

   - Para SUSE 15.3 y SUSE 15.2:

     ```
     sudo net ads join -U user
     ```

   - Para SUSE 12.5:

     ```
     sudo realm join REALM -U user
     ```

   user es un usuario de dominio que tiene permisos para agregar equipos al dominio.

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 agregar 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 arrancar el 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

Para verificar que Kerberos está configurado correctamente para su uso con 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 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 para 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 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 `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 Paso 6: Instalar el VDA de Linux después de la verificación de la 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
```

Haga que el script de instalación de PBIS sea ejecutable

Por ejemplo:

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

Ejecute 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 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 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\\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
```

Salir 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 Runtime 6.0 como requisito previo

Antes de instalar el VDA de Linux, instale .NET Runtime 6.0 según las instrucciones de `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar la ruta del 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, utilice /aa/bb como ruta binaria de .NET.

Paso 5: Descargar el paquete del VDA de Linux

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 del VDA de Linux que coincida con su distribución de Linux.

Paso 6: Instalar el VDA de Linux

Paso 6a: Desinstalar la versión anterior

Si instaló una versión anterior que no sea una de las dos anteriores ni una versión LTSR, desinstálela antes de instalar la nueva versión.

1. Detenga los servicios del VDA de Linux:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

Nota:

> Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando `service ctxmonitorservice stop` para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reinicia los servicios que detuvo.

2. Desinstale el paquete:

```
sudo rpm -e XenDesktopVDA
```

Importante:

Se admite la actualización desde las dos últimas versiones.

Nota:

Los componentes de instalación se encuentran 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 VDA de Linux

Instale el software del VDA de Linux mediante Zypper:

Para SUSE 15:

```
sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

Para SUSE 12:

```
sudo zypper install XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Instale el software del VDA de Linux mediante el administrador de paquetes RPM. Antes de hacerlo, resuelva las siguientes dependencias:

Para SUSE 15:

```
sudo rpm -i XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

Para SUSE 12:

```
sudo rpm -i XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Paso 6c: Actualizar el VDA de Linux (opcional)

Puede actualizar una instalación existente desde las dos versiones anteriores y desde una versión 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.

Para SUSE 15:

```
sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

Para SUSE 12:

```
sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Lista de dependencias RPM para SUSE 15:

```
postgresql >= 13


postgresql-server >= 13


postgresql-jdbc >= 9.4
```

```
java-11-openjdk >= 11

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

motif >= 2.3.4

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

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1
```

```
libpython2_7-1_0 >= 2.7
```

Lista de dependencias RPM para SUSE 12:

```
libQt5Core5 >= 5.5~

mozilla-nss-tools >= 3.47.1

postgresql-server >= 10.12

postgresql-jdbc >= 9.2

java-11-openjdk >= 11

ImageMagick >= 6.8

dbus-1 >= 1.8.8

dbus-1-x11 >= 1.8.8

libXpm4 >= 3.5.11

libXrandr2 >= 1.4.2
```

```
libXtst6 >= 1.2.2

motif >= 2.3

pam >= 1.1.8

bash >= 4.2

findutils >= 4.5

gawk >= 4.1

sed >= 4.2

cups >= 1.6.0

cups-filters-foomatic-rip >= 1.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1
```

```
cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

libmspack0 >= 0.4

python-requests >= 2.8.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1

libtcmalloc4 >= 2.5

libcap-progs >= 2.22

xorg-x11-server >= 7.6_1.18.3-76.15

ibus >= 1.5
```

```
xorg- x11-server = 7.6_1.19.6

xorg-x11 = 7.6_1

postgresql10-server >= 10.12

libgtk-2_0-0 >= 2.24

libgthread-2_0-0 >= 2.48

pulseaudio-utils >= 5.0

lsb-release >= 2.0
```

Importante:

Reinicie la máquina VDA de Linux 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:

- Citrix Hypervisor
- 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 en la VM.

Paso 8: Configurar el VDA de Linux

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, 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_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. Se establece en N de forma predeterminada.
- **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 un alias CNAME.
- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP, que es el puerto 80 de forma predeterminada.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** - Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina. El valor se establece en Y de forma predeterminada.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Los servicios de Linux Virtual Desktop requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos necesarios (puertos 80 y 1494 de forma predeterminada) automáticamente en el firewall del sistema para Linux Virtual Desktop. Se establece en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4** – 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. Especifique el método de integración de Active Directory compatible que desea utilizar:
  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD
- **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_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 esta variable en Y. Esta variable está establecida en N de forma predeterminada.

- **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 de DNS a un sitio local, especifique un nombre de sitio DNS. Esta variable está establecida en **\<none\>** de forma predeterminada.
- **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. Esta variable está establecida 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). Esta variable está establecida en **\<none\>** de forma predeterminada.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Los servidores de Federated Authentication Service (FAS) se configuran a través de la directiva de grupo de AD. El VDA de Linux no admite la directiva de grupo de AD, pero puede proporcionar una lista de servidores FAS separados 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 los servidores.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET Runtime 6.0 para admitir el nuevo servicio de agente de intermediación (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Especifica el entorno de escritorio GNOME o MATE que se utilizará en las sesiones. Si deja la variable sin especificar, se utiliza el escritorio actualmente instalado en el VDA. Sin embargo, si el escritorio actualmente instalado es MATE, debe establecer el valor de la variable en **mate**.

> **Nota:**
>
> También puede cambiar el entorno de escritorio para un usuario de sesión de destino siguiendo estos pasos:
>
> 1\. Cree un archivo `.xsession` en el directorio **$HOME/<username\>** del VDA.

\>2\. Edite el archivo `.xsession` para especificar un entorno de escritorio basado en las distribuciones.

- **Para el escritorio MATE en SUSE 15**

```
MSESSION="$(type -p mate-session)"
```

\> if ; then

```
    exec mate-session
```

\> fi

- **Para el escritorio GNOME en SUSE 15 y SUSE 12.5**

```
GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi
```

3\. Comparta el permiso de archivo 700 con el usuario de la sesión de destino.

- **CTX_XDL_START_SERVICE=Y \| N** – Si los servicios del VDA de Linux se inician o no cuando se completa la configuración del VDA de Linux. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT** – El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N



export CTX_XDL_DDC_LIST='list-ddc-fqdns'



export CTX_XDL_VDA_PORT=port-number



export CTX_XDL_REGISTER_SERVICE=Y|N



export CTX_XDL_ADD_FIREWALL_RULES=Y|N



export CTX_XDL_AD_INTEGRATION=1|2|3|4



export CTX_XDL_HDX_3D_PRO=Y|N



export CTX_XDL_VDI_MODE=Y|N
```

```
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_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \
```

```
CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

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 /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 Linux VDA 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: 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

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 /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Detener el Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

Nota:

Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando `service ctxmonitorservice stop` 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 /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Comprobar el estado del Linux VDA:

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

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

Paso 11: Crear el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops™

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 **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 VDA y Windows VDA en el mismo catálogo de máquinas.

> **Nota:**

> Las versiones anteriores de Citrix Studio no admitían el concepto de "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 el grupo de entrega en Citrix Virtual Apps™ o Citrix Virtual Desktops

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, 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 2112.

Instalar el agente de entrega virtual de Linux para Ubuntu manualmente

> **Importante:**
>
> Para instalaciones nuevas, le recomendamos que utilice la 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 Ubuntu para la instalación de VDA

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 servidor Ubuntu 18.04 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 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 en el archivo.

> **Nota:**

> Actualmente, el VDA de Linux no admite la truncación de nombres NetBIOS. Por lo tanto, el nombre de host no debe exceder los 15 caracteres.

> **Sugerencia:**

> Utilice solo los caracteres a–z, A–Z, 0–9 y 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 el DNS de multidifusión (**mDNS**) habilitado, lo que puede provocar resultados de resolución de nombres incoherentes.

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 puede causar problemas de desviación del reloj. Por esta razón, se prefiere sincronizar la hora con un servicio de hora remoto.

Instale 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 OpenJDK 11

El VDA de Linux requiere la presencia de OpenJDK 11.

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la última versión de OpenJDK 11 desde `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.

4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

En Ubuntu 20.04 y Ubuntu 18.04, instale OpenJDK 11 usando:

```
sudo apt-get install -y openjdk-11-jdk
```

Paso 1i: Instalar PostgreSQL

El VDA de Linux requiere PostgreSQL versión 9.x en Ubuntu:

```
sudo apt-get install -y postgresql



sudo apt-get install -y libpostgresql-jdbc-java
```

Paso 1j: Instalar Motif

```
sudo apt-get install -y libxm4
```

Paso 1k: Instalar otros paquetes

```
sudo apt-get install -y libsasl2-2



sudo apt-get install -y libsasl2-modules-gssapi-mit



sudo apt-get install -y libldap-2.4-2



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 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 horaria en Citrix Hypervisor™

Cuando la función de sincronización horaria de Citrix Hypervisor está habilitada, dentro de cada máquina virtual Linux paravirtualizada, experimentará problemas con NTP y Citrix Hypervisor. 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 Citrix VM instaladas, puede comprobar si la función de sincronización horaria de Citrix Hypervisor 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 horaria está habilitada y debe deshabilitarse.
- 1 - La función de sincronización horaria 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 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 añada 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 Hyper-V Linux instalados pueden usar 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, 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 de VMware y 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 **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: Agregar la máquina virtual (VM) Linux al dominio de Windows

El VDA de Linux admite varios métodos para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Quest Authentication Service
- 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

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 Kerberos en mayúsculas, como **EXAMPLE.COM**.

Configurar la 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** y realice las siguientes configuraciones:

`[global]`

`workgroup =` *`WORKGROUP`*

`security = ADS`

`realm =` *`REALM`*

`encrypt passwords = yes`

`idmap config *:range = 16777216-33554431`

`winbind trusted domains only = no`

`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 de 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 diversas 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 de shell. En algunos entornos, el nombre de dominio DNS es diferente del nombre del 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 haya almacenado en caché usando:

```
sudo klist
```

Examine los detalles de la cuenta de la máquina usando:

```
sudo net ads status
```

verificar autenticación de usuario

Utilice la herramienta **wbinfo** para verificar que los usuarios del dominio puedan 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 Winbind PAM esté 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 esté habilitado y funcione correctamente.

verificar que se haya 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 sean válidos y no hayan 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 es correcta pero no puede mostrar 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 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 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 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 de 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), 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 usuario 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.

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 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 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 son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
```

Salir de 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 va a unir 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 **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 del 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`

`[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 utiliza `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 SPN en el formato host/hostname-fqdn@REALM, que el VDA de Linux requiere.

3. verificar el keytab del sistema.

   Para una máquina Ubuntu 20.04, ejecute el comando `adcli testjoin` para comprobar si está unida al dominio.

   Para una máquina Ubuntu 18.04 o Ubuntu 16.04, ejecute el comando `sudo klist -ket` para asegurarse de que se ha creado el archivo keytab del sistema.

   verificar que la marca de tiempo de cada clave coincide con la hora en que la máquina se unió al dominio.

- **Si utiliza `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 de **REALM**, y **REALM** es el nombre del reino Kerberos en mayúsculas.

3. Únase al 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 reino 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 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 de 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 tenga solo 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 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 **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 distintas 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 para la cuenta de la máquina se ha almacenado en caché utilizando:

```
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 la unión al dominio.

PBIS

Descargue el paquete PBIS necesario

Por ejemplo:

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Haga que el script de instalación de PBIS sea ejecutable

Por ejemplo:

```
sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Ejecute el script de instalación de PBIS

Por ejemplo:

```
sudo sh pbis-open-8.8.0.506.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 actualmente unidos. 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
```

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 Runtime 6.0 como requisito previo

Antes de instalar el VDA de Linux, instale .NET Runtime 6.0 según las instrucciones de `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar la ruta de su 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, use /aa/bb como la ruta del binario de .NET.

Paso 5: Descargar el paquete del VDA de Linux

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 del VDA de Linux que coincida con su distribución de Linux.

Paso 6: Instalar el VDA de Linux

Paso 6a: Instalar el VDA de Linux

Instale el software del VDA de Linux utilizando el gestor de paquetes de Debian:

Para Ubuntu 20.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
```

Para Ubuntu 18.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
```

Para Ubuntu 16.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu16.04_amd64.deb
```

Lista de dependencias de Debian para Ubuntu 20.04:

```
libqt5widgets5 >= 5.7~
```

```
ibus >= 1.5

libsasl2-modules-gssapi-mit >= 2.1.~

postgresql >= 12

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8
```

```
util-linux >= 2.34

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

libgoogle-perftools4 >= 2.7~

libpython2.7 >= 2.7~
```

Lista de dependencias de Debian para Ubuntu 18.04:

```
libqt5widgets5 >= 5.7~

libmspack0 >= 0.6
```

```
ibus >= 1.5

libnss3-tools >= 2:3.35

postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

openjdk-11-jdk >= 11

gtk3-nocsd >=3

imagemagick >= 8:6.8.9.9

ufw >= 0.35

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2
```

```
libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

libsasl2-modules-gssapi-mit >= 2.1.~

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~

xserver-xorg-core >= 2:1.18
```

```
xserver-xorg-core << 2:1.19

x11vnc>=0.9.13

python-websockify >= 0.6.1
```

Lista de dependencias de Debian para Ubuntu 16.04:

```
libqt5widgets5 >= 5.5~

libmspack0 >= 0.5

python-pkg-resources >= 20.7.0

libnss3-tools >= 2:3.28

postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

imagemagick >= 8:6.8.9.9

ufw >= 0.35
```

```
ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

libsasl2-modules-gssapi-mit >= 2.1.~
```

```
python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~

xserver-xorg-core >= 2:1.18

xserver-xorg-core << 2:1.19

x11vnc>=0.9.13

python-websockify >= 0.6.1
```

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)

Puede actualizar una instalación existente desde las dos versiones anteriores y desde una versión LTSR.

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

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.

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:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

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

1. Asegúrese de que la máquina virtual 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 en la VM.

Paso 8: Configurar el VDA de Linux

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 con preguntas

Ejecute una configuración manual con preguntas:

```
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 al usuario ninguna información, lo que permite un proceso de instalación mediante script.

Las variables de entorno admitidas incluyen:

- **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. Se establece en N de forma predeterminada.
- **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 un alias CNAME.
- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP, que es el puerto 80 de forma predeterminada.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina. Se establece en Y de forma predeterminada.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Los servicios de Linux Virtual Desktop requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos necesarios (puertos 80 y 1494 de forma predeterminada) automáticamente en el firewall del sistema para Linux Virtual Desktop. Se establece en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4 \|5** – 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. Especifique el método de integración de Active Directory compatible que desea utilizar:
  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD

    - 5 – PBIS

- **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_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 esta variable en Y. Esta variable se establece en N de forma predeterminada.
- **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 de DNS a un sitio local, especifique un nombre de sitio DNS. Esta variable se establece en **\<none\>** de forma predeterminada.
- **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. 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). Sin embargo, para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Esta variable se establece en **\<none\>** de forma predeterminada.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Los servidores de Federated Authentication Service (FAS) se configuran a través de `AD Group Policy`. El VDA de Linux no admite la directiva de grupo de AD, pero puede proporcionar una lista de servidores FAS separados por punto y coma. La secuencia debe ser la misma que la configurada en `AD Group Policy`. 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 los servidores.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET Runtime 6.0 para admitir el nuevo servicio de agente de broker (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Especifica el entorno de escritorio GNOME o MATE que se utilizará en las sesiones. Si deja la variable sin especificar, se utilizará

el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de la variable en **mate**.

Nota:

También puede cambiar el entorno de escritorio para un usuario de sesión de destino siguiendo estos pasos:

1\. Cree un archivo `.xsession` en el directorio **$HOME/<username\>** del VDA.

\>2\. Edite el archivo `.xsession` para especificar un entorno de escritorio según las distribuciones.

- **Para el escritorio MATE**

```
MSESSION="$(type -p mate-session)"
```

\> if ; then

```
    exec mate-session
```

\> fi

- **Para el escritorio GNOME**

```
GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    exec gnome-session
```

\> fi

3\. Comparta el permiso de archivo 700 con el usuario de la sesión de destino.

- **CTX_XDL_START_SERVICE=Y \| N** – Indica si los servicios de Linux VDA se inician o no cuando se completa la configuración de Linux VDA. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – El puerto de socket para escuchar Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT** – El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N


export CTX_XDL_DDC_LIST='list-ddc-fqdns'


export CTX_XDL_VDA_PORT=port-number


export CTX_XDL_REGISTER_SERVICE=Y|N


export CTX_XDL_ADD_FIREWALL_RULES=Y|N


export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
```

```
export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N
```

```
sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \
```

```
CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

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:**

> 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: 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 Linux VDA

Una vez que haya configurado Linux VDA mediante el script **ctxsetup.sh**, use los siguientes comandos para controlar Linux VDA.

Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Detener 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 `service ctxmonitorservice stop` para detener el demonio del servicio de monitorización. De lo contrario, el demonio del servicio de monitorización 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 el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops™

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 el grupo de entrega en Citrix Virtual Apps™ o Citrix Virtual Desktops

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.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte Citrix Virtual Apps and Desktops 7 2112.

Instalar Linux Virtual Delivery Agent para 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 Debian para la instalación de VDA

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

Asegúrese de que el nombre de dominio DNS y el nombre de dominio completo (FQDN) de la máquina se informen correctamente. La forma 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 en el archivo.

> **Nota:**

> El VDA de Linux actualmente no admite el truncamiento 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 FQDN.

verificar que el FQDN esté configurado correctamente:

```
hostname -f
```

Este comando devuelve el FQDN de la máquina.

Paso 1e: Deshabilitar DNS de multidifusión

La configuración predeterminada tiene el DNS de multidifusión (**mDNS**) habilitado, lo que puede provocar resultados de resolución de nombres incoherentes.

Para deshabilitar **mDNS**, edite **/etc/nsswitch.conf** y cambie la línea:

`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 puede causar problemas de desviación del reloj. Por esta razón, se prefiere sincronizar la hora con un servicio de hora remoto.

Instale 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 NTP públicos. Agregue una entrada de servidor para cada controlador de dominio de Active Directory en el dominio.

Elimine cualquier otra entrada de **server** o **pool** que aparezca, 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 chrony
```

Paso 1h: Instalar paquetes

```
sudo apt-get install -y libsasl2-2



sudo apt-get install -y libgtk2.0-0
```

Paso 1i: Agregue el repositorio `oldstable`

Para instalar las dependencias necesarias para una distribución Debian, agregue la línea `deb http://deb.debian.org/debian/ oldstable main` al archivo `/etc/apt/sources.list`.

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 Citrix Hypervisor™

Cuando la función de sincronización de hora de Citrix Hypervisor está habilitada, dentro de cada VM Linux paravirtualizada, experimentará problemas con NTP y Citrix Hypervisor. 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 Citrix VM Tools instaladas, puede comprobar si la función de sincronización de hora de Citrix Hypervisor está presente y habilitada desde dentro de la VM 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 Hyper-V Linux instalados pueden usar la función de sincronización horaria de Hyper-V para usar la hora del sistema operativo host. Para asegurarse de que el reloj del sistema siga siendo 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 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**, desmarque **Sincronizar la hora del invitado con el host**.

Paso 3: Agregue la máquina virtual (VM) Linux al dominio de Windows

El VDA de Linux admite varios métodos para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- Quest Authentication Service
- 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

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 de Winbind para que se inicie al arrancar la máquina

El demonio de 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** y realice la siguiente configuración:

`[global]`

`workgroup =` *`WORKGROUP`*

`security = ADS`

`realm =` *`REALM`*

`encrypt passwords = yes`

`idmap config *:range = 16777216-33554431`

`winbind trusted domains only = no`

`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: systemd winbind`

`group: systemd winbind`

Unirse al dominio de Windows

El 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 REALM -U user
```

Donde **REALM** es el nombre del reino Kerberos en mayúsculas, y **user** es un usuario de dominio con permisos para añadir equipos al dominio.

Reiniciar Winbind

```
sudo systemctl restart winbind
```

Configurar PAM para Winbind

Ejecute el siguiente comando y asegúrese de que las opciones **Winbind NT/Active Directory authentication** y **Create home directory on login** 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 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 ámbito 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 ámbito de Kerberos. Asegúrese de que se utiliza el nombre de ámbito. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el tíquet 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 ámbito de Kerberos. Para el shell bash, el carácter de barra invertida (\\) debe escaparse con otra barra invertida. Este comando devuelve un mensaje que indica si la operación se realizó correctamente o no.

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 tíquets 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 mostrar su escritorio al iniciar sesión con una cuenta de dominio, reinicie la máquina e inténtelo de nuevo.

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 las 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 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), 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 usuario 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.

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 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 (/es-es/linux-virtual-delivery-agent/2201/installation-overview/ubuntu.html#step-6-install-the-linux-vda) 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 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 (/es-es/linux-virtual-delivery-agent/2201/installation-overview/ubuntu.html#step-6-install-the-linux-vda) 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
[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. Puede usar `adcli`, `realmd` o `Samba` en su lugar.

> **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. Unirse 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 añadir 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 el keytab del sistema.

   Ejecute el comando `sudo klist -ket` para asegurarse de que se ha creado el archivo keytab del sistema.

   verificar que la marca de tiempo de cada clave coincide con la hora en que la máquina se unió al dominio.

- **Si utiliza `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 Kerberos en mayúsculas.

3. Unirse al dominio con `Samba`.

   Su controlador de dominio debe ser accesible y debe tener una cuenta de Windows con permisos para añadir 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 añadir 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 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 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 tenga solo 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 **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 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 TGT para la cuenta de la máquina se ha almacenado en caché utilizando:

```
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 de 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 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 la unión al dominio.

PBIS

Descargue el paquete PBIS necesario

Por ejemplo:

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Haga que el script de instalación de PBIS sea ejecutable

Por ejemplo:

```
sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Ejecute el script de instalación de PBIS

Por ejemplo:

```
sudo sh pbis-open-8.8.0.506.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 **user** es un usuario de dominio que tiene permisos para agregar equipos al dominio de Active Directory. El **domain-name** 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 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.

```
sudo 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
```

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 Runtime 6.0 como requisito previo

Antes de instalar el VDA de Linux, instale .NET Runtime 6.0 según las instrucciones de `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

Después de instalar .NET Runtime 6.0, 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 5: Descargar el paquete del VDA de Linux

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 del VDA de Linux que coincida con su distribución de Linux.

Paso 6: Instalar el VDA de Linux

Paso 6a: Instalar el VDA de Linux

Instale el software del VDA de Linux mediante el administrador de paquetes de Debian:

```
sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
```

Lista de dependencias de Debian para Debian 10.9:

```
libqt5widgets5          >= 5.5~

ibus                    >= 1.5

postgresql              >= 11

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk           >= 11

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             >= 9.27~

libmspack0              >= 0.10

libgoogle-perftools4    >= 2.7~

libpython2.7            >= 2.7~

libsasl2-modules-gssapi-mit >= 2.1.~
```

Nota:

Para ver una matriz de las distribuciones de Linux y las versiones de Xorg compatibles con esta versión de Linux VDA, consulte Requisitos del sistema.

Paso 6b: Actualizar el VDA de Linux (opcional)

Puede actualizar una instalación existente desde las dos versiones anteriores y desde una versión LTSR.

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

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.

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:

- 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 VM invitada en la VM.

Paso 8: Configurar el VDA de Linux

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. Consulte 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_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. Establecido en N de forma predeterminada.
- **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 usar en el registro con un Delivery Controller. Se debe especificar al menos un FQDN o un alias CNAME.
- **CTX_XDL_VDA_PORT=port-number** – El VDA de Linux se comunica con los Delivery Controllers a través de un puerto TCP/IP, que es el puerto 80 de forma predeterminada.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina. Establecido en Y de forma predeterminada.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Los servicios de Linux Virtual Desktop requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir los puertos necesarios (puertos 80 y 1494 de forma predeterminada) automáticamente en el firewall del sistema para Linux Virtual Desktop. Establecido en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4 \|5** – 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. Especifique el método de integración de Active Directory compatible que desea usar:
  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD
  - 5 – PBIS
- **CTX_XDL_HDX_3D_PRO=Y \| N** – 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_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 esta variable en Y. Esta variable se establece en N de forma predeterminada.

- **CTX_XDL_SITE_NAME=dns-name** – El Linux VDA 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. Esta variable se establece en **\<none\>** de forma predeterminada.
- **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. 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). Sin embargo, para mejorar el rendimiento de la búsqueda, puede especificar una base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Esta variable se establece en **\<none\>** de forma predeterminada.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Los servidores de Federated Authentication Service (FAS) se configuran a través de la directiva de grupo de AD. El Linux VDA no admite la directiva de grupo de AD, pero puede proporcionar una lista de servidores FAS separados 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 los servidores.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – La ruta para instalar .NET Runtime 6.0 para admitir el nuevo servicio de agente de intermediación (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Especifica el entorno de escritorio GNOME o MATE que se utilizará en las sesiones. Si deja la variable sin especificar, se utiliza el escritorio actualmente instalado en el VDA. Sin embargo, si el escritorio actualmente instalado es MATE, debe establecer el valor de la variable en **mate**.

> **Nota:**
>
> También puede cambiar el entorno de escritorio para un usuario de sesión de destino siguiendo estos pasos:
>
> 1\. Cree un archivo `.xsession` en el directorio **$HOME/<username\>** del VDA.

\>2\. Edite el archivo `.xsession` para especificar un entorno de escritorio según las distribuciones.

```
>-  **For MATE desktop**

>

>        MSESSION="$(type -p mate-session)"
```

\> if ; then

```
      exec mate-session
```

\> fi

\>- **For GNOME desktop**

```
    GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    exec gnome-session
```

\> fi

3\. Comparta el permiso de archivo 700 con el usuario de la sesión de destino.

- **CTX_XDL_START_SERVICE=Y \| N** – Si los servicios de Linux VDA se inician o no cuando se completa la configuración de Linux VDA. Establecido en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.

- **CTX_XDL_TELEMETRY_PORT** – El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Establezca la variable de entorno y ejecute el script de configuración:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \
```

```
CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
```

```
CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
```

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 el VDA de Linux 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 VDA de Linux:

```
dpkg -r xendesktopvda
```

Nota:

Al desinstalar el software VDA de Linux, se eliminan los datos de configuración de PostgreSQL y otros datos de configuración asociados. Sin embargo, el paquete de PostgreSQL y otros paquetes dependientes que se configuraron antes de la instalación del VDA de Linux 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 VDA de Linux. Para obtener más información, consulte XDPing.

Paso 10: Ejecutar el VDA de Linux

Una vez que haya configurado el VDA de Linux mediante el script **ctxsetup.sh**, use los siguientes comandos para controlar el VDA de Linux.

Iniciar el VDA de Linux:

Para iniciar los servicios del VDA de Linux:

```
sudo systemctl start ctxhdx



sudo systemctl start 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 `service ctxmonitorservice stop` para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reinicia los servicios que detuvo.

> **Reiniciar el VDA de Linux:**

Para reiniciar los servicios de Linux VDA:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Comprobar el estado de 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 el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops™

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 **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 combine máquinas Linux 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 una máquina del dominio de Active Directory y la vuelve a unir, debe quitar y agregar la máquina al catálogo de máquinas de nuevo.

Paso 12: Crear el grupo de entrega en Citrix Virtual Apps™ o Citrix Virtual Desktops

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 VDA de Linux.
- No permita el inicio de sesión de usuarios no autenticados (anónimos).
- No combine 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 2112.

Crear VDA de Linux en Citrix Virtual Apps and Desktops™ Standard para Azure

Puede crear VDA de Linux unidos a un dominio y 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 Citrix Virtual Apps and Desktops Standard para Azure.

Distribuciones de Linux compatibles

Las siguientes distribuciones de Linux admiten esta función:

- RHEL 8.3
- RHEL 8.2
- RHEL 7.8
- Ubuntu 20.04
- Ubuntu 18.04
- Ubuntu 16.04

Pasos

Para crear VDA de Linux en Citrix Virtual Apps™ and Desktops Standard para Azure, siga estos pasos:

1. Prepare una imagen maestra en Azure:

> **Nota:**
>
> También puede usar la función de autoactualización de Linux VDA 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 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 "<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. En Azure, cree una VM de Linux de una distribución compatible.

b. Instale un entorno de escritorio en la VM de Linux si es necesario.

c. En la VM, instale .NET Runtime 6.0 según las instrucciones en `<https://docs.microsoft.com/es-es/dotnet/core/install/linux-package-managers>`.

d. (Solo para Ubuntu) Agregue la línea `source /etc/network/interfaces.d/*` al archivo `/etc/network/interfaces`.

e. (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
```

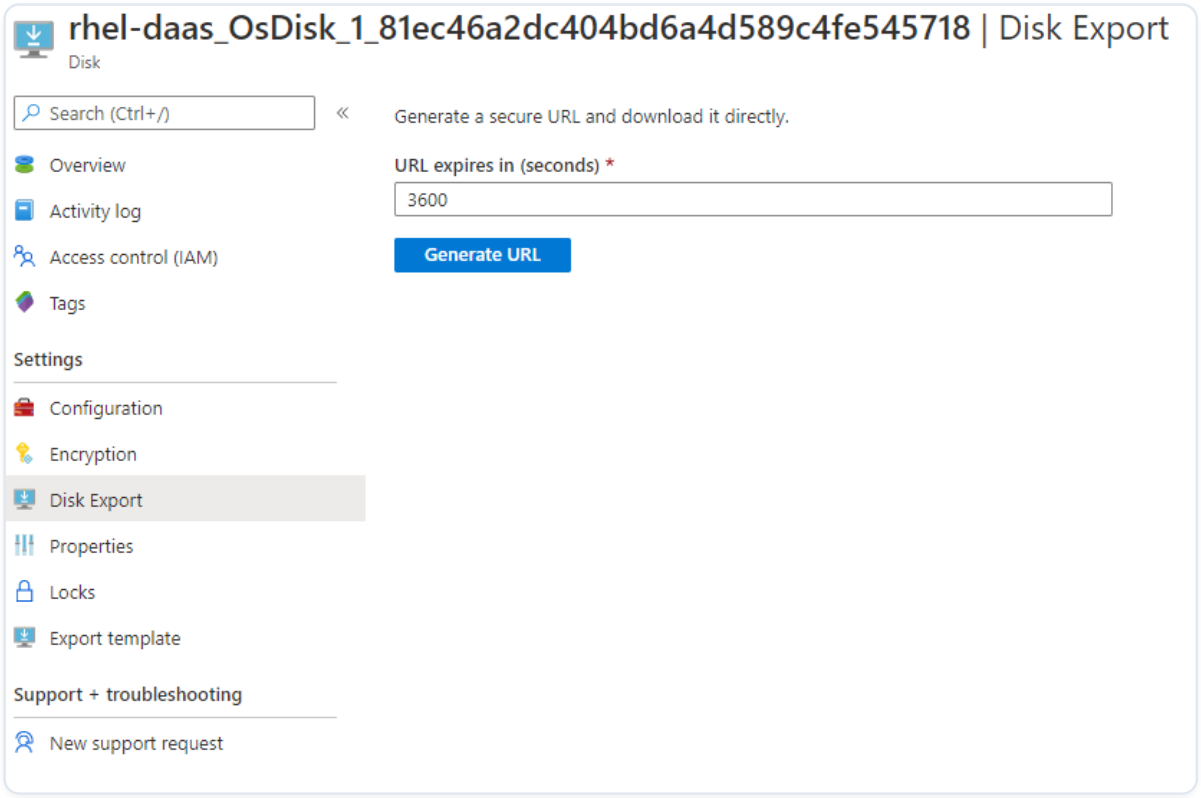
f. Instale el paquete de Linux VDA.

g. Cambie las variables en /etc/xdl/mcs/mcs.conf. El archivo de configuración `mcs.conf` contiene variables para configurar MCS y el Linux VDA.

> **Nota:**
>
> Deje la variable dns sin especificar. Si selecciona el tipo **Estático** o **Aleatorio** al crear un catálogo de máquinas, establezca `VDI_MODE=Y`.

h. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.

i. En Azure, detenga (o desasigne) la VM. Haga clic en **Exportar disco** para generar una URL SAS para el archivo de disco duro virtual (VHD) que puede usar como imagen maestra para crear otras VM.



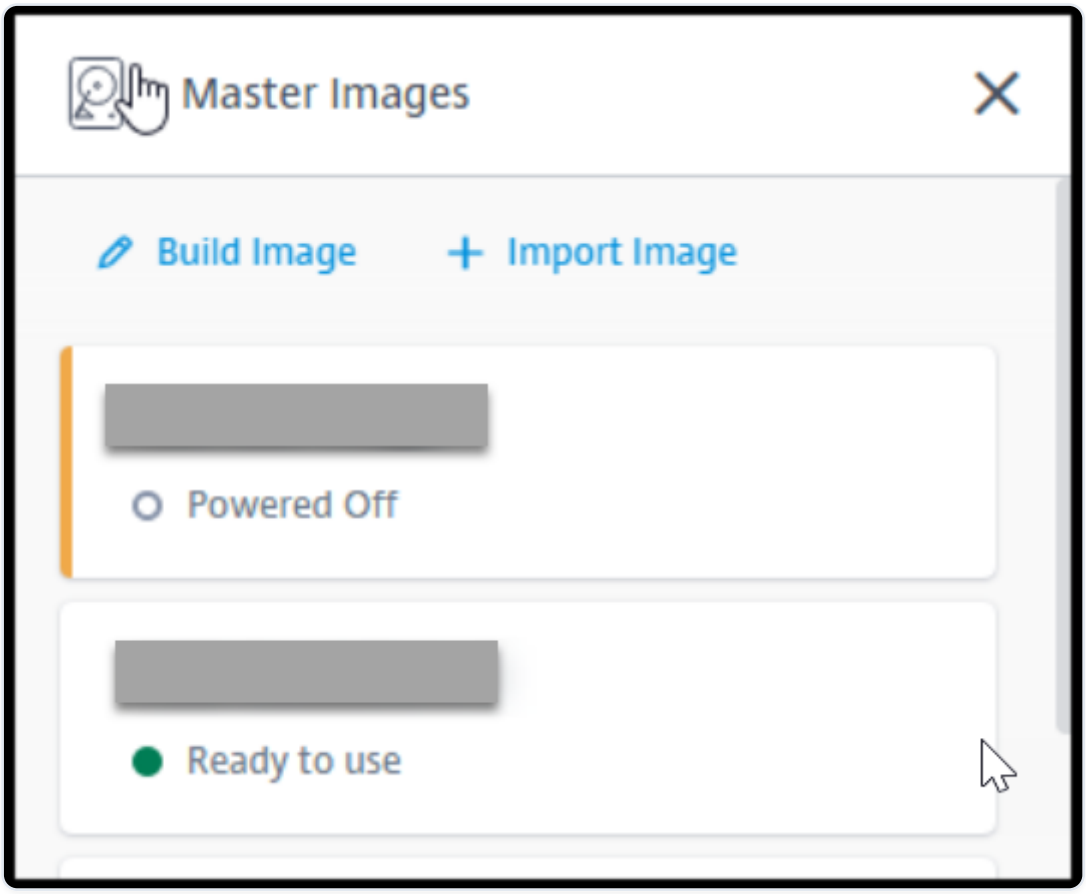
j. (Opcional) Realice la configuración de directivas de grupo en la imagen maestra. Puede usar la herramienta `ctxreg` para realizar la configuración de directivas de grupo. Por ejemplo, el siguiente comando habilita la directiva **Crear automáticamente impresora universal PDF** para la impresión de PDF.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\GroupPolicy\Defaults\PrintingPolicies" -t
"REG_DWORD" -v "AutoCreatePDFPrinter" -d "0x00000001" –force
```

2. Importe la imagen maestra desde Azure.

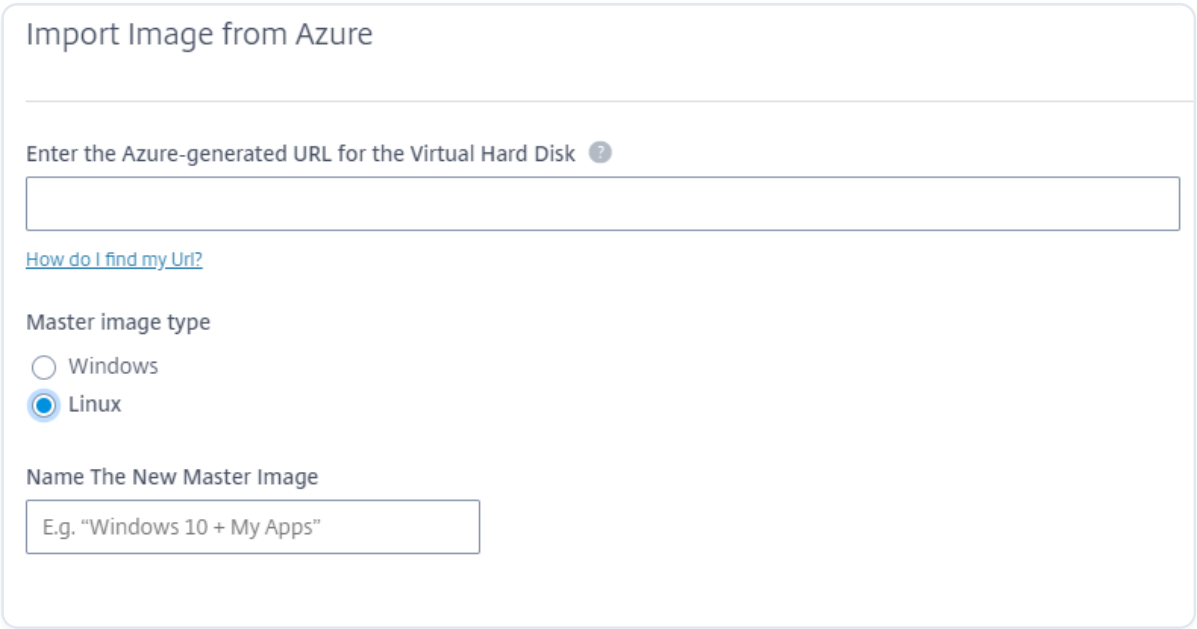
a. Desde el panel Administrar, expanda **Imágenes maestras** a la derecha. La pantalla muestra las imágenes maestras que proporciona Citrix y las imágenes que usted creó e importó.

Sugerencia: La mayoría de las actividades de administrador para este servicio se gestionan a través de los paneles **Administrar** y **Supervisar**. Después de crear su primer catálogo, el panel **Administrar** se inicia automáticamente después de iniciar sesión en Citrix Cloud™ y seleccionar el servicio **Managed Desktops**.



b. Haga clic en **Importar imagen**.

c. Introduzca la URL SAS del archivo VHD que generó en Azure. Seleccione **Linux** para el tipo de imagen maestra.



d. Siga las instrucciones del asistente para completar la importación de la imagen maestra.

3. Cree un Catálogo de máquinas.

Acceda al panel Administrar 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, use la Consola serie en el portal de Azure.

Usar Machine Creation Services™ (MCS) para crear máquinas virtuales Linux

El uso de MCS para crear máquinas virtuales Linux implica los siguientes pasos generales:

1. Prepare una imagen maestra en la máquina virtual de plantilla de su elección, que puede ser cualquier máquina virtual o un VDA en ejecución.
2. Cree un catálogo de máquinas en Citrix Studio.
3. Cree un grupo de entrega.

> **Nota:**
>
> Pueden producirse resultados inesperados si intenta preparar una imagen maestra en hipervisores que no sean Citrix Hypervisor™, Microsoft Azure, VMware vSphere, AWS, GCP o Nutanix AHV.

> Microsoft Azure, AWS y GCP no son compatibles a partir de Citrix Virtual Apps and Desktops™ 7 2003. Pero puede seguir utilizando los hosts en el servicio Citrix Virtual Apps and Desktops.

Distribuciones compatibles

	WINBIND	SSSD	CENTRIFY	PBIS
CentOS 7.9	Sí	Sí	Sí	Sí
CentOS 7.8	Sí	Sí	Sí	Sí

	WINBIND	SSSD	CENTRIFY	PBIS
Debian 10.9	Sí	Sí	No	Sí
RHEL 8.4	Sí	No	Sí	Sí
RHEL 8.3	Sí	No	Sí	Sí
RHEL 8.2	Sí	No	Sí	Sí
RHEL 8.1	Sí	No	Sí	Sí
RHEL 7.9	Sí	Sí	Sí	Sí
RHEL 7.8	Sí	Sí	Sí	Sí
SUSE 15.3	Sí	Sí	No	Sí
SUSE 15.2	Sí	Sí	No	Sí
SUSE 12.5	Sí	Sí	No	Sí
Ubuntu 20.04	Sí	Sí	No	Sí
Ubuntu 18.04	Sí	Sí	No	Sí
Ubuntu 16.04	Sí	Sí	No	Sí

Nota:

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 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.

Usar MCS para crear máquinas virtuales Linux en Citrix Hypervisor

Paso 1: Preparar una imagen maestra

Una imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software. Para preparar una imagen maestra, haga lo siguiente:

Paso 1a: Instalar Citrix VM Tools

Instale Citrix VM Tools en la máquina virtual de plantilla para que cada máquina virtual use la CLI 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. Ejecute el siguiente comando para montar Citrix VM Tools llamado guest-tools.iso.

   ```
   sudo mount /dev/cdrom /mnt
   ```

2. Ejecute el siguiente comando para instalar el paquete `xe-guest-utilities` según su distribución de Linux.

   Para RHEL/CentOS:

   ```
   sudo rpm -i /mnt/Linux/xe-guest-utilities_{package-version}_all.rpm
   ```

   Para Ubuntu/Debian:

   ```
   sudo dpkg -i /mnt/Linux/xe-guest-utilities_{package-version}_all.deb
   ```

Para SUSE:

```
sudo rpm -i /mnt/Linux/xe-guest-utilities_{package-version}_all.rpm
```

3. Compruebe el estado de virtualización de la VM de plantilla en la ficha **General** de XenCenter. Si Citrix VM Tools está instalado correctamente, el estado de virtualización es **Optimizado**:

   Estado de virtualización optimizado(/en-us/linux-virtual-delivery-agent/2201/media/optimized2.png)

Paso 1b: (Solo para Ubuntu 16.04) Instalar OpenJDK 11

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la versión más reciente de OpenJDK 11 de `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.
4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

Paso 1c: Instalar el paquete de Linux VDA en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso.

> Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Runtime 6.0.

> Según su distribución de Linux, ejecute el siguiente comando para configurar el entorno para el Linux VDA:

Para RHEL/CentOS:

```
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 1d: Habilitar repositorios para instalar el paquete `tdb-tools`

Para el servidor RHEL 7:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

Para la estación de trabajo RHEL 7:

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

Paso 1e: Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8, RHEL 7 y CentOS 7 para que, al ejecutar deploymcs.sh más tarde, se instale el paquete ntfs-3g disponible en el repositorio EPEL.

Paso 1f: Instale ntfs-3g manualmente en SUSE

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 1g: Configure el entorno de tiempo de ejecución

Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie las variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` proporciona variables para configurar MCS y el VDA de Linux. A continuación, se muestran las variables que puede configurar según sea necesario:
  - `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben usar las configuraciones existentes 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 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 con MCS.
  - `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, que es el nombre NetBIOS (distingue mayúsculas de minúsculas) si está configurado en AD. De lo contrario, es el nombre de dominio de forma predeterminada.
- `AD_INTEGRATION`: Configura 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 en este artículo.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete de Centrify. 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.
- Las siguientes variables de configuración del VDA de Linux:

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-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`=nombre-de-sitio-dns | '<none\>' `LDAP_LIST`='lista-de-servidores-ldap' | '<none\>'

  `SEARCH_BASE`=conjunto-de-base-de-búsqueda | '<none\>' `FAS_LIST`='lista-de-servidores-fas' | '<none\>'

  `START_SERVICE`=S | N `TELEMETRY_SOCKET_PORT`=número-de-puerto

  `TELEMETRY_PORT`=número-de-puerto

Para ver un ejemplo de `mcs.conf`, consulte la siguiente captura de pantalla:

```
#!/bin/bash

#############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.



##########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

##########################DNS Configuration#####################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

##########################NTP Configuration#####################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

##########################WORKGROUP Configuration###############################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

##########################Domain Join Configuration#############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

##########################Centrify download path Configuration##################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


##########################Centrify Samba download path Configuration#############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


##########################PBIS download path Configuration######################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


##########################Machine Password Automate Update######################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

##########################Linux VDA Configuration###############################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
```

- 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
  \ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
  ```

  ```
  update -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -v "Flags" -d "0x00000003"
  ```

Paso 1h: Crear una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Si utiliza un VDA en ejecución como VM de plantilla, 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/mcs/winbind_krb5.conf.tmpl` y `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

   Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` y `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/mcs/centrify_krb5.conf.tmpl` y `/etc/xdl/mcs/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.

3. En Citrix Hypervisor, apague la VM de plantilla. Cree y asigne un nombre a una instantánea de su imagen maestra.

Paso 2: Crear un catálogo de máquinas

En Citrix Studio, cree un catálogo de máquinas y especifique el número de VM que se crearán en el catálogo. Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear un catálogo de máquinas con Studio.

Paso 3: 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.

Usar MCS para crear VM Linux en Azure

Paso 1: Crear una conexión de alojamiento a Azure en Citrix Studio

1. En Citrix Studio en Citrix Cloud™, elija **Configuración > Alojamiento > Agregar conexión y recursos** para crear una conexión a Azure.

   Creando la conexión a Azure(/en-us/linux-virtual-delivery-agent/2201/media/create-connection-to-azure.png)

2. Elija Microsoft Azure como tipo de conexión.

   Eligiendo el tipo de conexión de Azure(/en-us/linux-virtual-delivery-agent/2201/media/choose-connection-type.png)

3. Escriba el ID de suscripción de su cuenta de Azure y el nombre de su conexión.

   Escribiendo un ID de suscripción de Azure(/en-us/linux-virtual-delivery-agent/2201/media/type-subscription-id.png)

   Aparece una nueva conexión en el panel de alojamiento.

   Una nueva conexión de Azure(/en-us/linux-virtual-delivery-agent/2201/media/new-connection-appears-in-hosting-pane.png)

Paso 2: Preparar una imagen maestra en la VM de plantilla

Una imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software. Para preparar una imagen maestra, haga lo siguiente:

Paso 2a: Configurar cloud-init para Ubuntu 18.04

Para asegurarse de que un nombre de host de VDA persista cuando una VM se reinicia o se detiene, ejecute el siguiente comando:

```
echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
```

verificar que las siguientes líneas estén presentes en la sección **system_info** del archivo /etc/cloud/cloud.cfg:

```
system_info:

   network:

       renderers: ['netplan', 'eni', 'sysconfig']
```

Paso 2b: (Solo para Ubuntu 16.04) Instalar OpenJDK 11

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la última versión de OpenJDK 11 desde `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.
4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

Paso 2c: Instale el paquete de Linux VDA en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso.

> Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Runtime 6.0.

> Según su distribución de Linux, ejecute el siguiente comando para configurar el entorno para el Linux VDA:

Para RHEL/CentOS:

```
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 2d: Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8/CentOS 8, RHEL 7/CentOS 7 para que la ejecución posterior de deploymcs.sh instale el paquete ntfs-3g disponible en el repositorio EPEL.

Paso 2e: Instale ntfs-3g manualmente en SUSE

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 2f: Configurar el entorno de ejecución

Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie las variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` proporciona variables para configurar MCS y el VDA de Linux. A continuación, se muestran algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben configurarse:

  Nota: Si una variable se puede configurar con varios valores, ponga los valores entre comillas simples y sepárelos con espacios. Por ejemplo, LDAP_LIST='aaa.lab:389 bbb.lab:389'.

  - `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben usar las configuraciones existentes 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 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 con MCS.
  - `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, que es el nombre de NetBIOS (distingue mayúsculas de minúsculas) si está configurado en AD. De lo contrario, es el nombre de dominio de forma predeterminada.

- `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 en este artículo.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete de Centrify. 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.
- Las siguientes variables de configuración de Linux VDA:

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-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`=nombre-de-sitio-dns | '<none\>' `LDAP_LIST`='lista-de-servidores-ldap' | '<none\>'

  `SEARCH_BASE`=conjunto-de-base-de-búsqueda | '<none\>' `FAS_LIST`='lista-de-servidores-fas' | '<none\>'

  `START_SERVICE`=S | N `TELEMETRY_SOCKET_PORT`=número-de-puerto

  `TELEMETRY_PORT`=número-de-puerto

Para ver un ejemplo de `mcs.conf`, consulte la siguiente captura de pantalla:

```
#!/bin/bash

#############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.



##########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

##########################DNS Configuration#####################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

##########################NTP Configuration#####################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

##########################WORKGROUP Configuration###############################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

##########################Domain Join Configuration#############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

##########################Centrify download path Configuration##################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


##########################Centrify Samba download path Configuration#############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


##########################PBIS download path Configuration######################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


##########################Machine Password Automate Update######################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

##########################Linux VDA Configuration###############################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
```

- 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
  \ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
  ```

  ```
  update -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -v "Flags" -d "0x00000003"
  ```

Paso 2g: Crear una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Si utiliza un VDA en ejecución como VM de plantilla, 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.

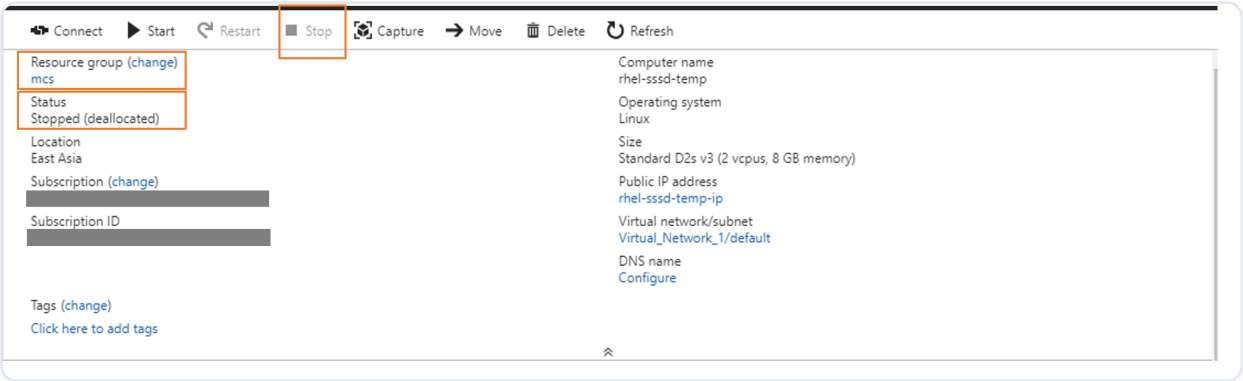
   Para los usuarios de Winbind, actualice las plantillas `/etc/xdl/mcs/winbind_krb5.conf.tmpl` y `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

   Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` y `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/mcs/centrify_krb5.conf.tmpl` y `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

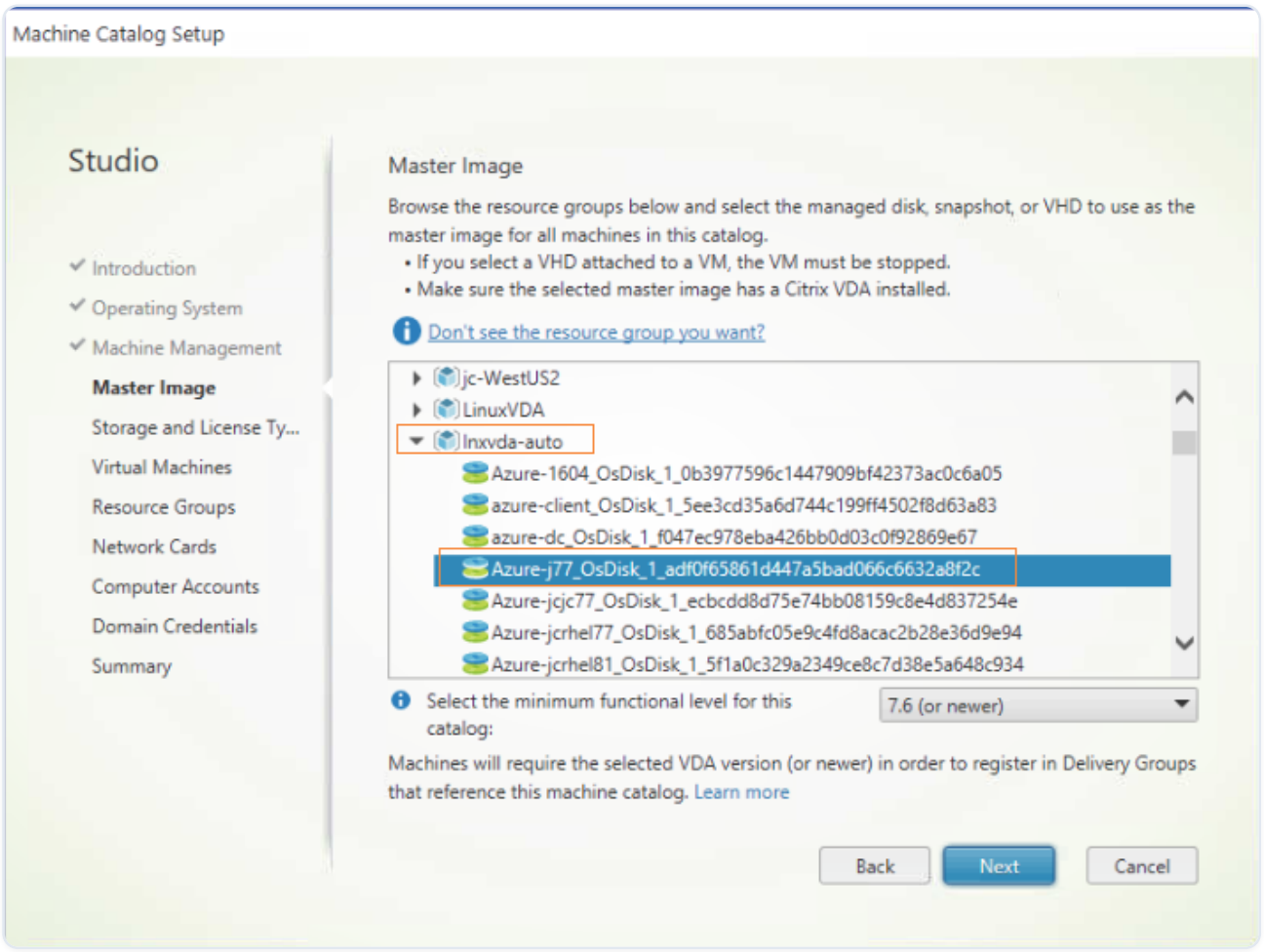
   Nota: Mantenga el formato existente utilizado en los archivos de plantilla y utilice variables como $WORKGROUP, $REALM, $realm, ${new_hostname} y $AD_FQDN.
3. Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de Azure. Asegúrese de que el estado de energía de 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.



Paso 3: Crear un catálogo de máquinas

En Citrix 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 del grupo de recursos al que pertenece la VM de plantilla y busque el VHD de la VM de plantilla.



Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear un catálogo de máquinas con Studio.

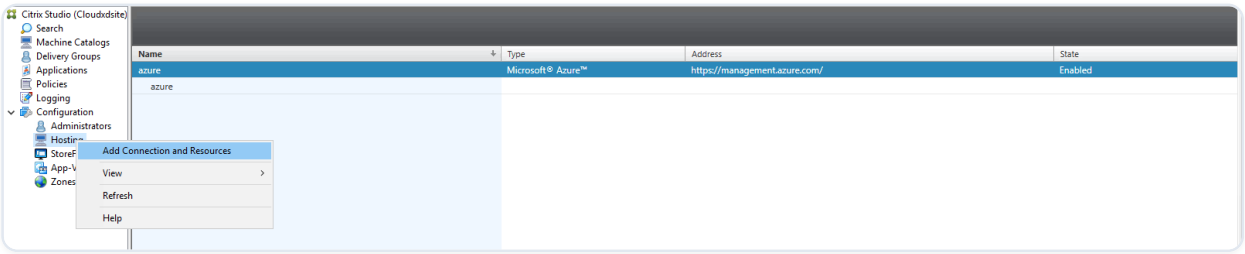
Paso 4: Crear un grupo de entrega

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 Crear grupos de entrega.

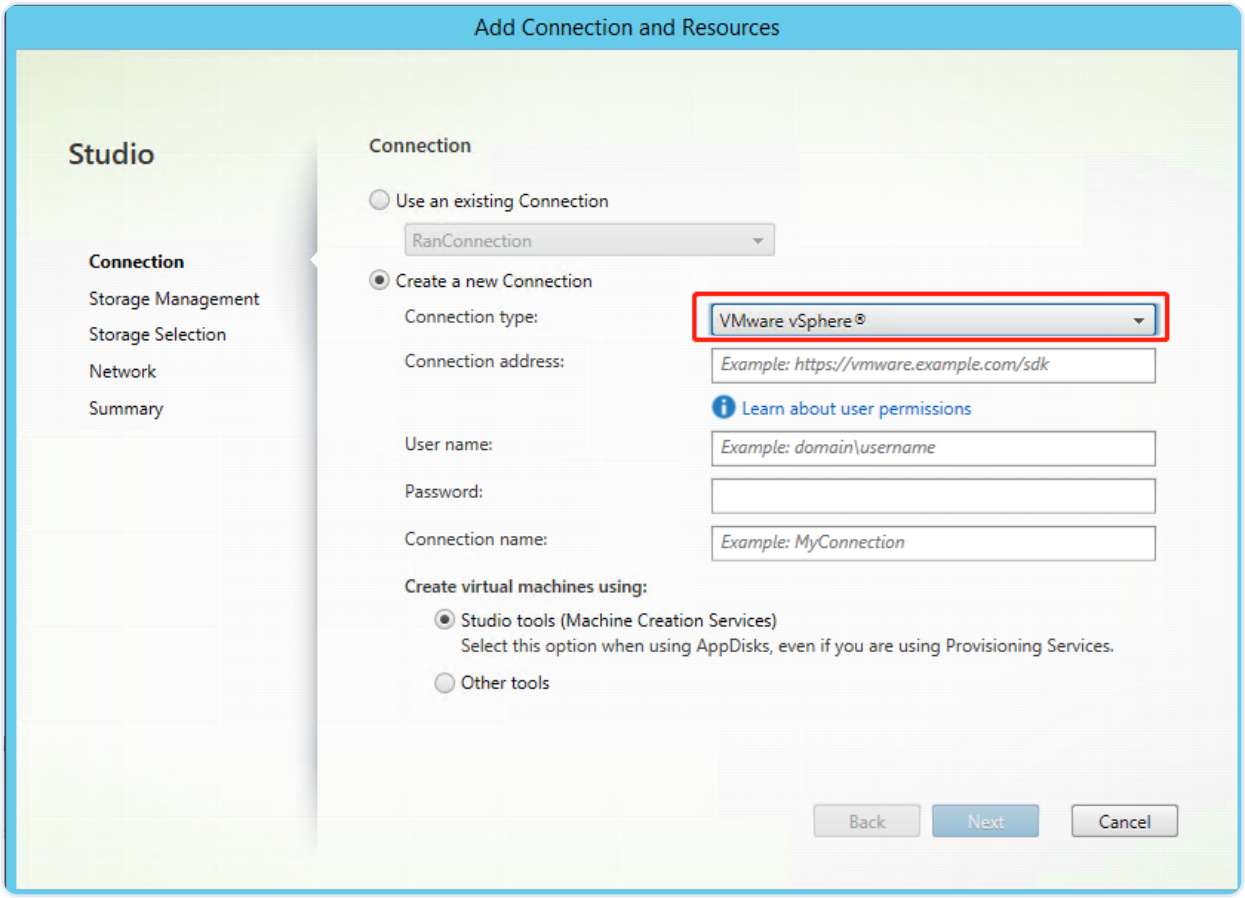
Usar MCS para crear VM Linux en VMware vSphere

Paso 1: Crear una conexión de alojamiento a VMware en Citrix Studio

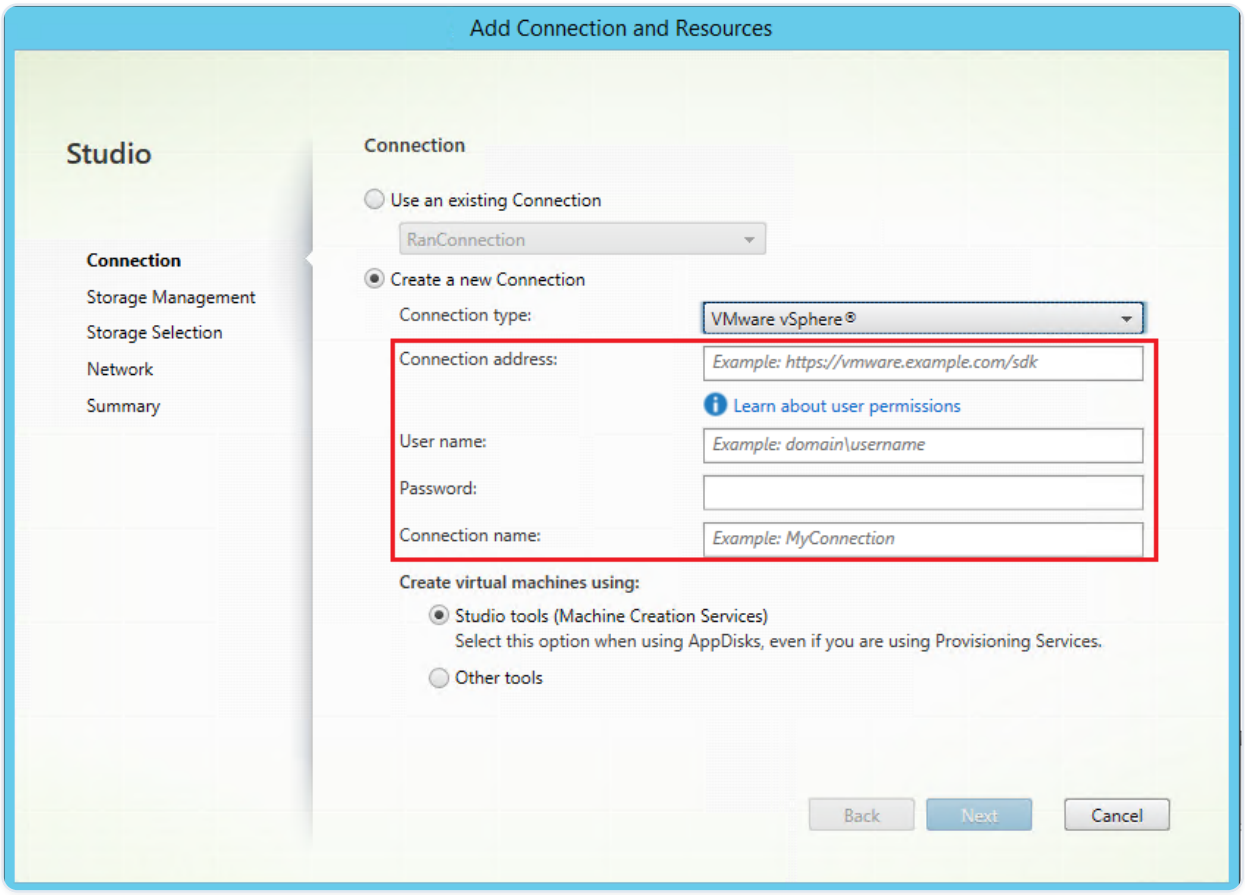
1. Instale vCenter Server en el entorno de vSphere. Para obtener más información, consulte VMware vSphere.
2. En Citrix Studio, elija **Configuración > Alojamiento > Agregar conexión y recursos** para crear una conexión a VMware vSphere.



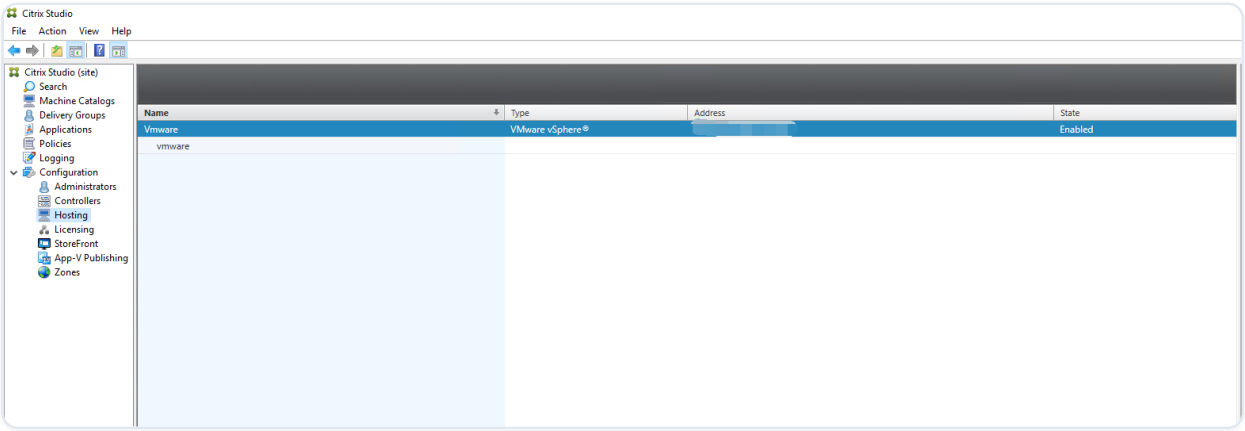
3. Elija VMware vSphere como tipo de conexión.



4. Escriba la dirección de conexión (la URL de vCenter Server) de su cuenta de VMware, su nombre de usuario y contraseña, y el nombre de su conexión.



Aparece una nueva conexión en el panel de alojamiento.



Paso 2: Preparar una imagen maestra

Una imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software. Para preparar una imagen maestra, haga lo siguiente:

Paso 2a: (Solo para Ubuntu 16.04) Instalar OpenJDK 11

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la última versión de OpenJDK 11 desde `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.
4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

Paso 2b: Instalar el paquete de Linux VDA en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso.

> Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Runtime 6.0.

> Según su distribución de Linux, ejecute el siguiente comando para configurar el entorno para el VDA de Linux:

Para RHEL/CentOS:

```
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 2c: Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8/CentOS 8, RHEL 7/CentOS 7 para que la ejecución posterior de deploymcs.sh instale el paquete ntfs-3g disponible en el repositorio EPEL.

Paso 2d: Instale ntfs-3g manualmente en SUSE

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 2e: Configure el entorno de tiempo de ejecución

Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie las variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` proporciona variables para configurar MCS y el VDA de Linux. A continuación, se muestran algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben configurarse:

Nota: Si una variable se puede configurar con varios valores, ponga los valores entre comillas simples y sepárelos con espacios. Por ejemplo, LDAP_LIST='aaa.lab:389 bbb.lab:389'.

- `Use_Existing_Configurations_Of_Current_VDA`: Determina si se utilizan las configuraciones existentes del VDA que se está ejecutando. Si se establece en Y, los archivos de configuración de las máquinas creadas con MCS son los mismos que los equivalentes en el VDA que se está ejecutando. 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.
- `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, que es el nombre NetBIOS (distingue mayúsculas de minúsculas) si está configurado en AD. De lo contrario, es el nombre de dominio de forma predeterminada.
- `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 en este artículo.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete de Centrify. 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.
- Las siguientes variables de configuración del VDA de Linux:

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-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`=nombre-de-sitio-dns | '<none\>' `LDAP_LIST`='lista-de-servidores-ldap' | '<none\>'

`SEARCH_BASE`=conjunto-de-base-de-búsqueda | '<none\>' `FAS_LIST`='lista-de-servidores-fas' | '<none\>'

`START_SERVICE`=S | N `TELEMETRY_SOCKET_PORT`=número-de-puerto

`TELEMETRY_PORT`=número-de-puerto

Para ver un ejemplo de `mcs.conf`, consulte la siguiente captura de pantalla:

```
#!/bin/bash

#############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.



##########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

##########################DNS Configuration#####################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

##########################NTP Configuration#####################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

##########################WORKGROUP Configuration###############################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

##########################Domain Join Configuration#############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

##########################Centrify download path Configuration##################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


##########################Centrify Samba download path Configuration#############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


##########################PBIS download path Configuration######################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


##########################Machine Password Automate Update######################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

##########################Linux VDA Configuration###############################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
```

- En la máquina de plantilla, añada 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 añadir 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
  \ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
  ```

  ```
  update -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -v "Flags" -d "0x00000003"
  ```

Paso 2f: Crear una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Si utiliza un VDA en ejecución como VM de plantilla, 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 pertinentes en todas las VM creadas.

   Para los usuarios de Winbind, actualice las plantillas `/etc/xdl/mcs/winbind_krb5.conf.tmpl` y `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

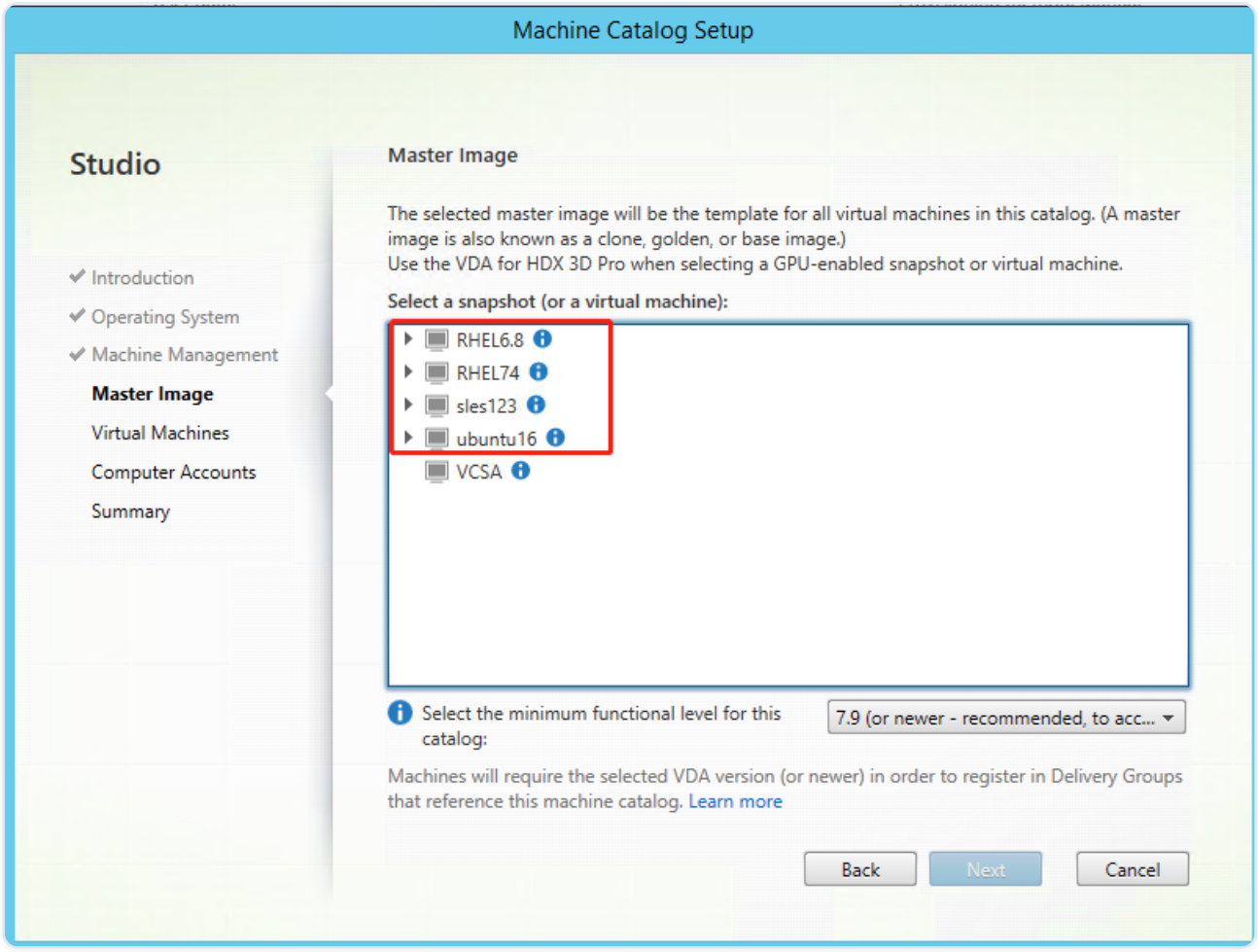
   Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` y `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/mcs/centrify_krb5.conf.tmpl` y `/etc/xdl/mcs/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.
3. Una vez que termine de instalar las aplicaciones en la VM de plantilla, apague la VM de plantilla desde VMware. Tome una instantánea de la VM de plantilla.

Paso 3: Crear un catálogo de máquinas

En Citrix 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 la imagen maestra de la lista de instantáneas.



Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear un catálogo de máquinas con Studio.

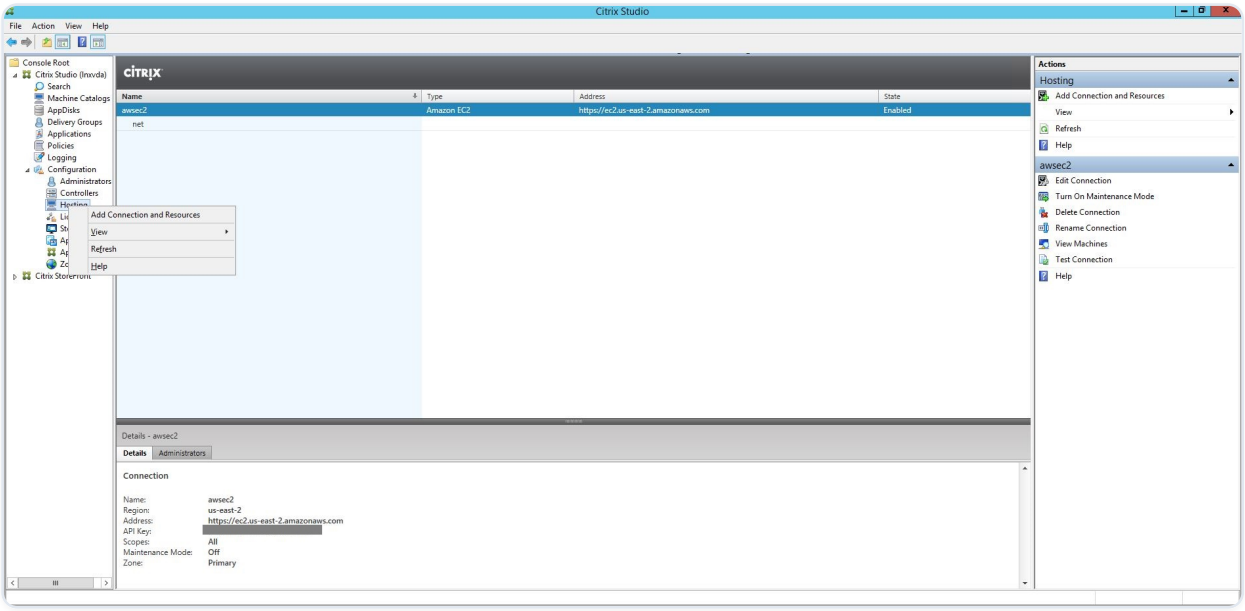
Paso 4: Crear un grupo de entrega

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.

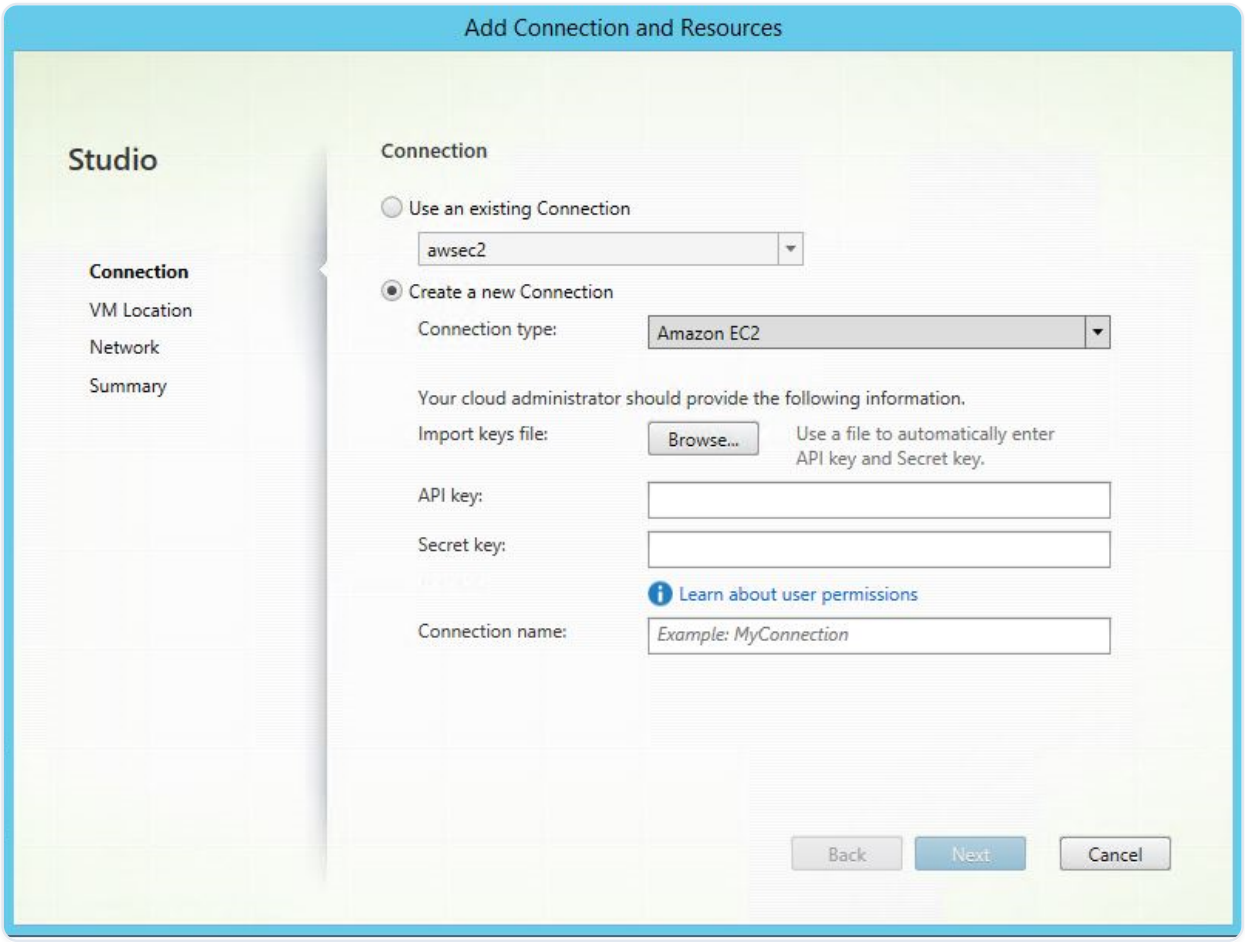
Usar MCS para crear VM Linux en AWS

Paso 1: Crear una conexión de alojamiento a AWS en Citrix Studio

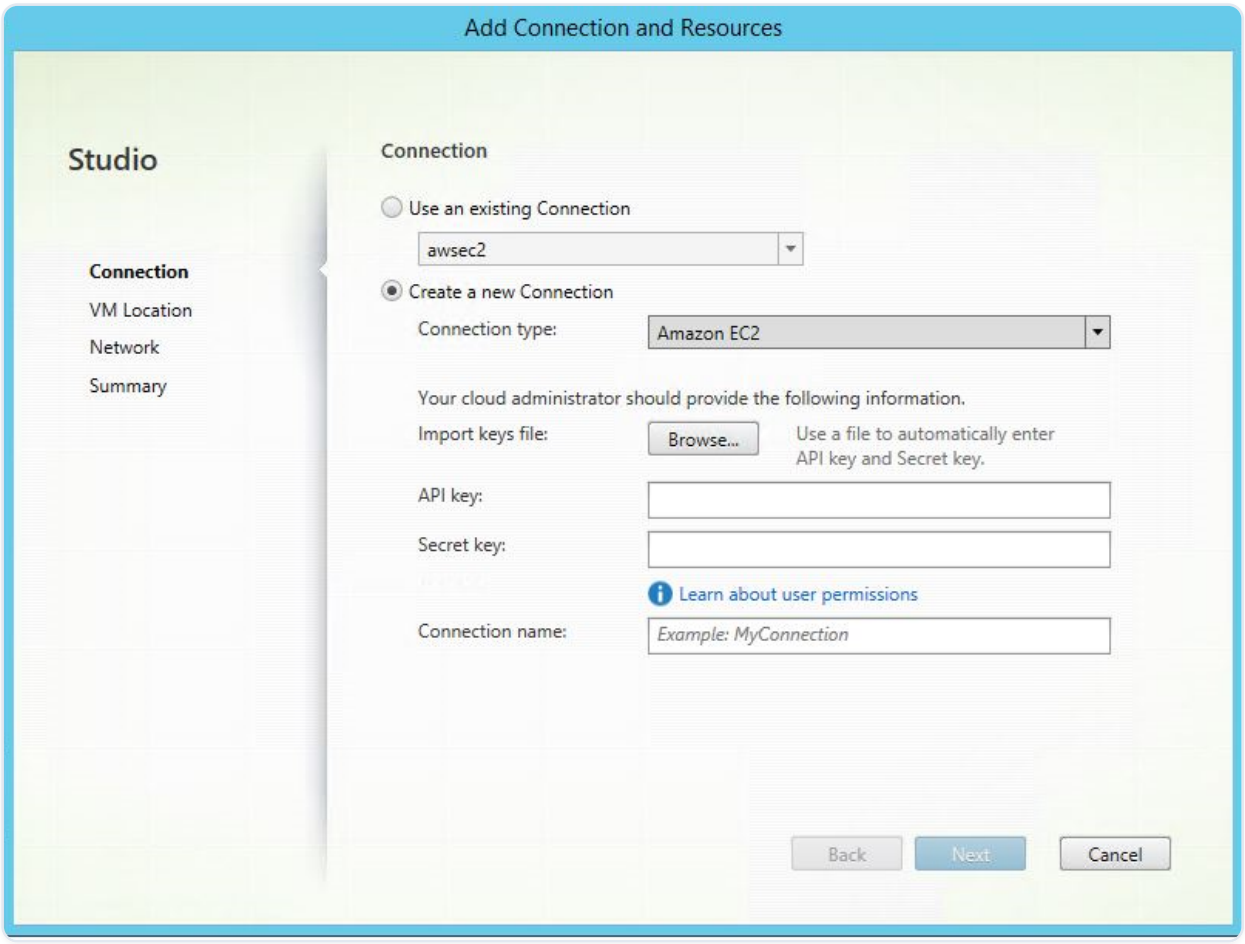
1. En Citrix Studio en Citrix Cloud, elija **Configuración** > **Alojamiento** > **Agregar conexión y recursos** para crear una conexión a AWS.



2. Elija **Amazon EC2** como tipo de conexión.



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).

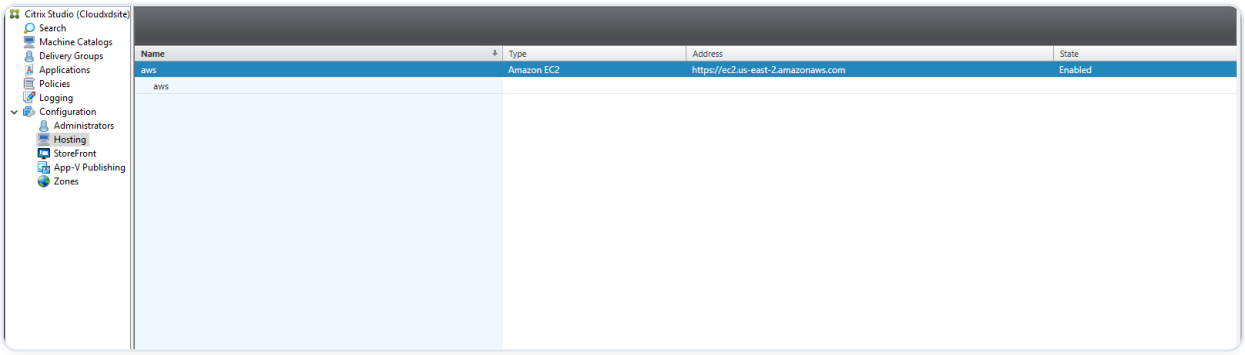
c. En el panel de navegación izquierdo, elija **Usuarios**.

d. Seleccione el usuario de destino y desplácese hacia abajo para seleccionar la ficha **Credenciales de seguridad**.

e. Desplácese hacia abajo y haga clic en **Crear clave de acceso**. Aparecerá una nueva ventana.

f. Haga clic en **Descargar archivo .csv** y guarde la clave de acceso en una ubicación segura.

Aparece una nueva conexión en el panel de alojamiento.



Paso 2: Preparar una imagen maestra

Una imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software. Para preparar una imagen maestra, haga lo siguiente:

Paso 2a: Configurar cloud-init

1. Para asegurarse de que un nombre de host de VDA persista cuando se reinicia o se detiene una instancia EC2, ejecute el siguiente comando para conservar el nombre de host de VDA.

   ```
   echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
   ```

   Para Ubuntu 18.04, asegúrese de que las siguientes líneas estén presentes en la sección system_info del archivo /etc/cloud/cloud.cfg:

   ```
   system_info:

       network:

           renderers: ['netplan', 'eni', 'sysconfig']
   ```

2. Para usar SSH para acceder de forma remota a las VM creadas con MCS en AWS, habilite la autenticación por contraseña, ya que no hay ningún nombre de clave asociado a esas VM. Haga lo siguiente según sea necesario.

   - Edite el archivo de configuración `cloud-init`, /etc/cloud/cloud.cfg. Asegúrese de que la línea **ssh_pwauth: true** esté presente. Elimine o comente la línea **set-password** y las siguientes líneas si existen.

     ```
     users:

     - default
     ```

- Si tiene previsto usar el usuario predeterminado `ec2-user` o `ubuntu` creado por `cloud-init`, puede cambiar la contraseña del usuario mediante el comando `passwd`. Tenga en cuenta la nueva contraseña para usarla más tarde al iniciar sesión en las VM creadas con MCS.
- Edite el archivo `/etc/ssh/sshd_config` para asegurarse de que la siguiente línea esté presente:

  ```
  PasswordAuthentication yes
  ```

  Guarde el archivo y ejecute el comando `sudo service sshd restart`.

Paso 2b: (Solo para Ubuntu 16.04) Instalar OpenJDK 11

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la última versión de OpenJDK 11 de `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.
4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

Paso 2c: Instalar el paquete Linux VDA en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso.

> Antes de instalar el paquete Linux VDA en la VM de plantilla, instale .NET Runtime 6.0.

> Según su distribución de Linux, ejecute el siguiente comando para configurar el entorno para Linux VDA:

Para RHEL/CentOS:

```
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 2d: Instalar el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8/CentOS 8, RHEL 7/CentOS 7 para que la ejecución posterior de deploymcs.sh instale el paquete ntfs-3g disponible en el repositorio EPEL.

Paso 2e: Instalar ntfs-3g manualmente en SUSE

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 2f: Configure el entorno de tiempo de ejecución

Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie las variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` proporciona variables para configurar MCS y el VDA de Linux. Las siguientes son algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben configurarse:

  Nota: Si una variable se puede configurar con varios valores, ponga los valores entre comillas simples y sepárelos con espacios. Por ejemplo, LDAP_LIST='aaa.lab:389 bbb.lab:389.'

  - `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben usar las configuraciones existentes 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 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 con MCS.
  - `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, que es el nombre NetBIOS (distingue entre mayúsculas y minúsculas) si está configurado en AD. De lo contrario, es el nombre de dominio de forma predeterminada.
  - `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 en este artículo.
  - `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete de Centrify. 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.
- Las siguientes variables de configuración de Linux VDA:

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-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`=nombre-de-sitio-dns | '<none\>' `LDAP_LIST`='lista-de-servidores-ldap' | '<none\>'

  `SEARCH_BASE`=conjunto-de-base-de-búsqueda | '<none\>' `FAS_LIST`='lista-de-servidores-fas' | '<none\>'

  `START_SERVICE`=S | N `TELEMETRY_SOCKET_PORT`=número-de-puerto

  `TELEMETRY_PORT`=número-de-puerto

Para ver un ejemplo de `mcs.conf`, consulte la siguiente captura de pantalla:

```
#!/bin/bash

#############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.



##########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

##########################DNS Configuration#####################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

##########################NTP Configuration#####################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

##########################WORKGROUP Configuration###############################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

##########################Domain Join Configuration#############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

##########################Centrify download path Configuration##################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


##########################Centrify Samba download path Configuration#############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


##########################PBIS download path Configuration######################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


##########################Machine Password Automate Update######################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

##########################Linux VDA Configuration###############################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
```

- 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
  \ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
  ```

  ```
  update -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -v "Flags" -d "0x00000003"
  ```

Paso 2g: Crear una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Si utiliza un VDA en ejecución como VM de plantilla, 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.

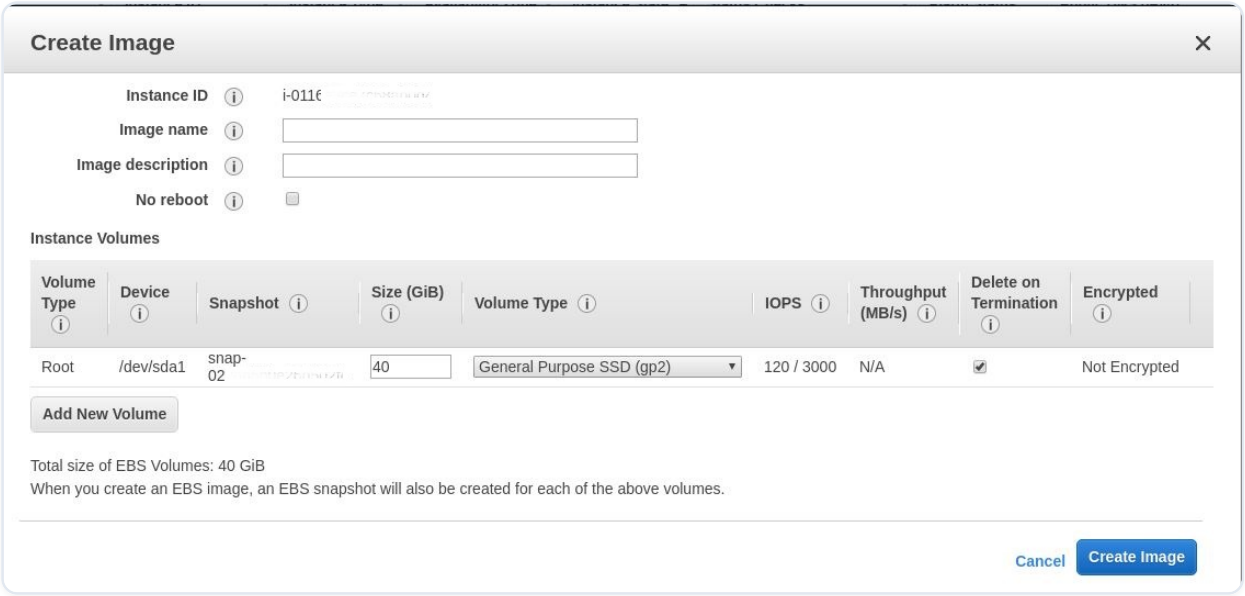
   Para los usuarios de Winbind, actualice las plantillas `/etc/xdl/mcs/winbind_krb5.conf.tmpl` y `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

   Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` y `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/mcs/centrify_krb5.conf.tmpl` y `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

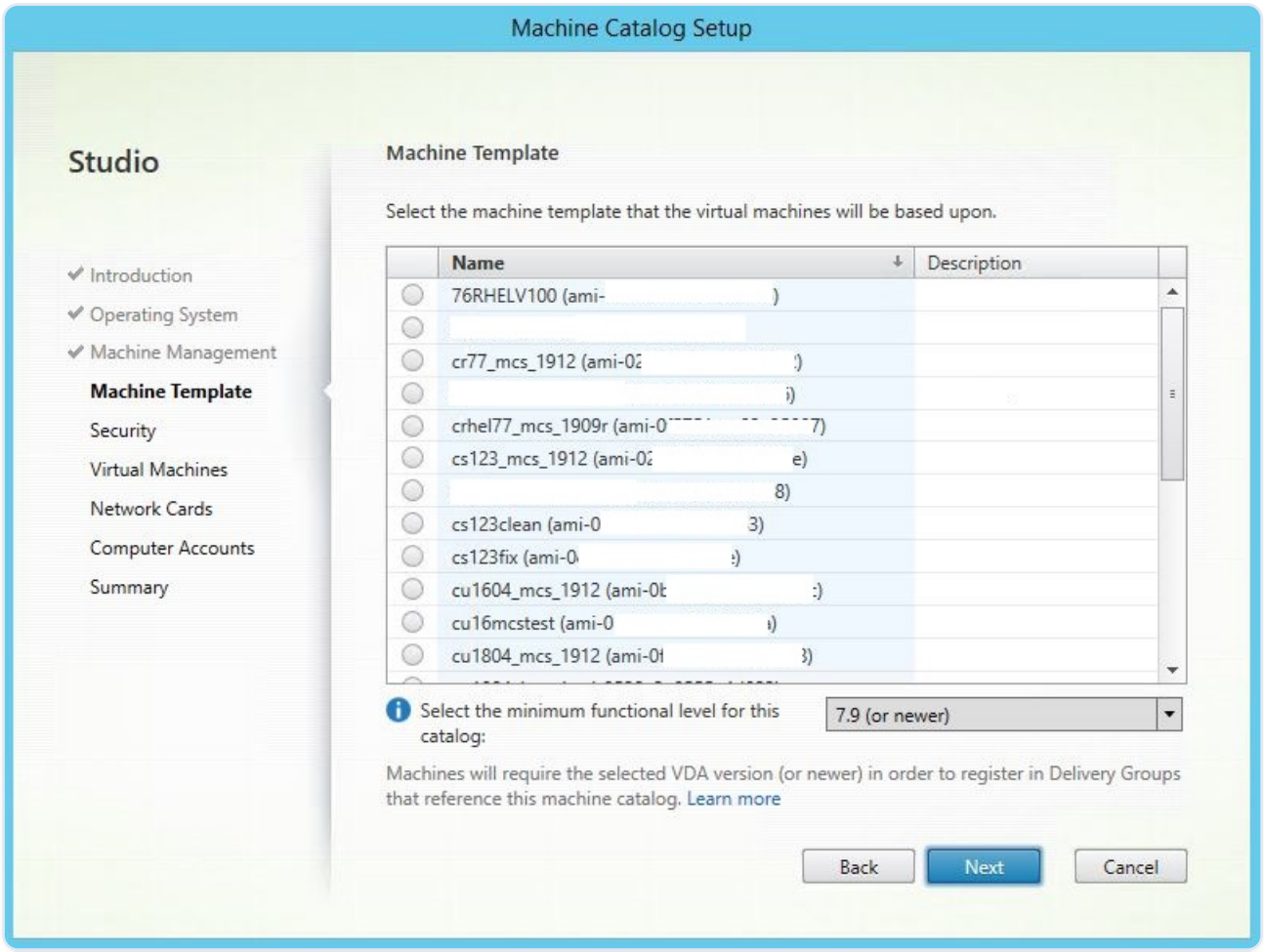
   Nota: Mantenga el formato existente utilizado en los archivos de plantilla y utilice variables como $WORKGROUP, $REALM, $realm, ${new_hostname} y $AD_FQDN.
3. Instale las aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de AWS EC2. Asegúrese de que el estado de la instancia de la VM de plantilla sea **Detenida**.

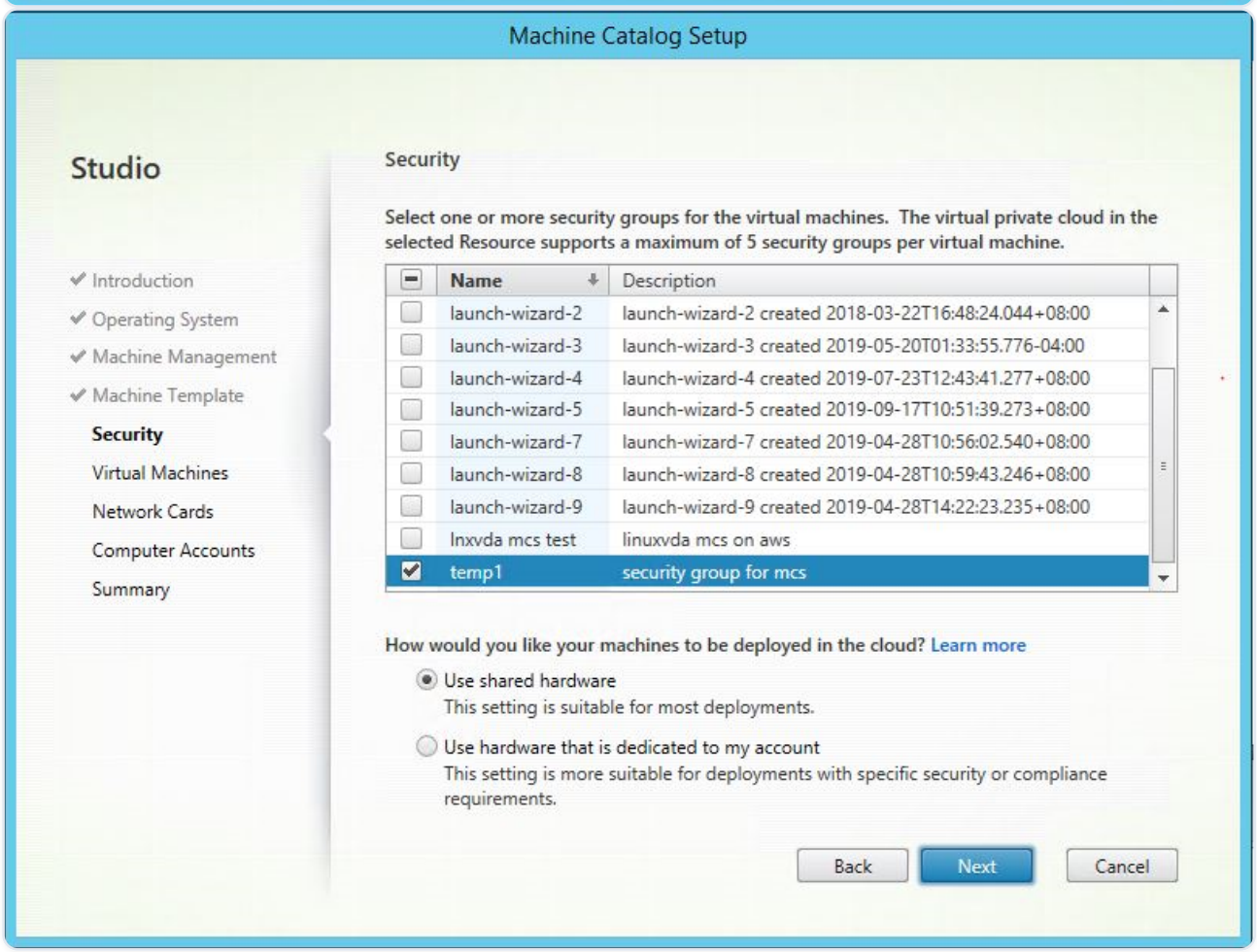
4. Haga clic con el botón secundario en la VM de plantilla y seleccione **Imagen > Crear imagen**. Escriba la información y realice los ajustes necesarios. Haga clic en **Crear imagen**.



Paso 3: Crear un catálogo de máquinas

En Citrix 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 la plantilla de máquina (la imagen maestra que creó anteriormente) y seleccione uno o varios grupos de seguridad.


Machine Catalog Setup
Studio
Introduction
Operating System
Machine Management
Machine Template
Security
Virtual Machines
Network Cards
Computer Accounts
Summary
Machine Template
Select the machine template that the virtual machines will be based upon.
Name
Description
76RHELV100 (ami-
cr77_mcs_1912 (ami-0
crhel77_mcs_1909r (ami-0
cs123_mcs_1912 (ami-0
cs123clean (ami-0
cs123fix (ami-0
cu1604_mcs_1912 (ami-0
cu16mcstest (ami-0
cu1804_mcs_1912 (ami-0
Select the minimum functional level for this catalog:
7.9 (or newer)
Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. Learn more
Back
Next
Cancel


Machine Catalog Setup
Studio
Introduction
Operating System
Machine Management
Machine Template
Security
Virtual Machines
Network Cards
Computer Accounts
Summary
Security
Select one or more security groups for the virtual machines. The virtual private cloud in the selected Resource supports a maximum of 5 security groups per virtual machine.
Name
Description
launch-wizard-2
launch-wizard-2 created 2018-03-22T16:48:24.044+08:00
launch-wizard-3
launch-wizard-3 created 2019-05-20T01:33:55.776-04:00
launch-wizard-4
launch-wizard-4 created 2019-07-23T12:43:41.277+08:00
launch-wizard-5
launch-wizard-5 created 2019-09-17T10:51:39.273+08:00
launch-wizard-7
launch-wizard-7 created 2019-04-28T10:56:02.540+08:00
launch-wizard-8
launch-wizard-8 created 2019-04-28T10:59:43.246+08:00
launch-wizard-9
launch-wizard-9 created 2019-04-28T14:22:23.235+08:00
lnxvda mcs test
linuxvda mcs on aws
temp1
security group for mcs
How would you like your machines to be deployed in the cloud? Learn more
Use shared hardware
This setting is suitable for most deployments.
Use hardware that is dedicated to my account
This setting is more suitable for deployments with specific security or compliance requirements.
Back
Next
Cancel

Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear un catálogo de máquinas con Studio.

Paso 4: 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.

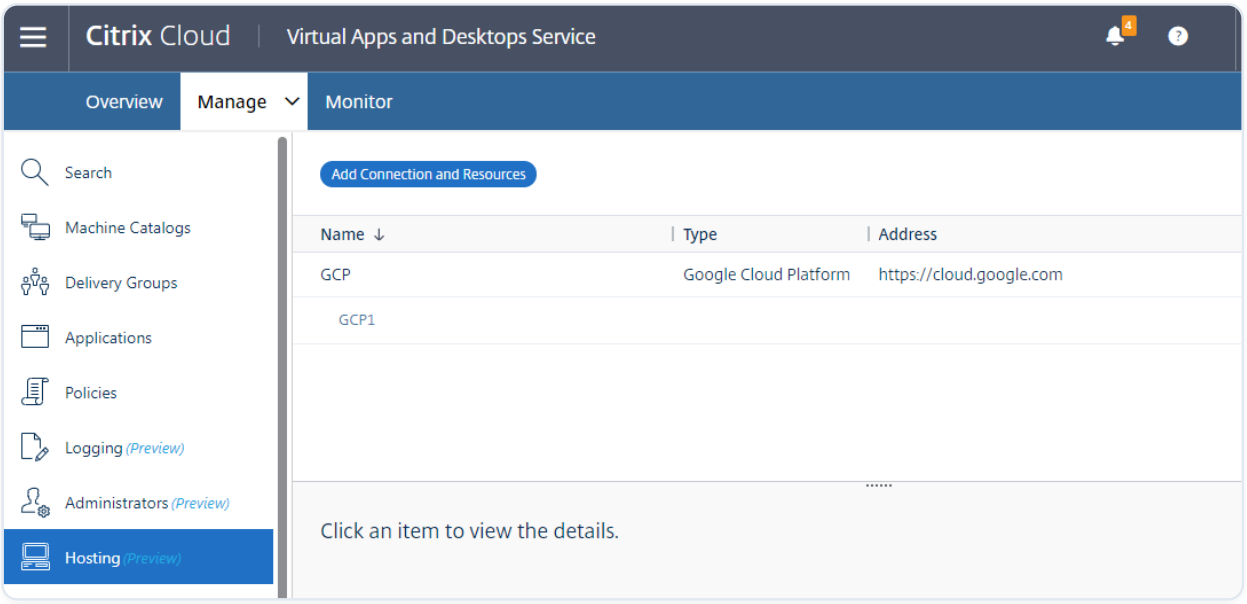
Usar MCS para crear VM Linux en GCP

Paso 1: Configure su entorno de GCP

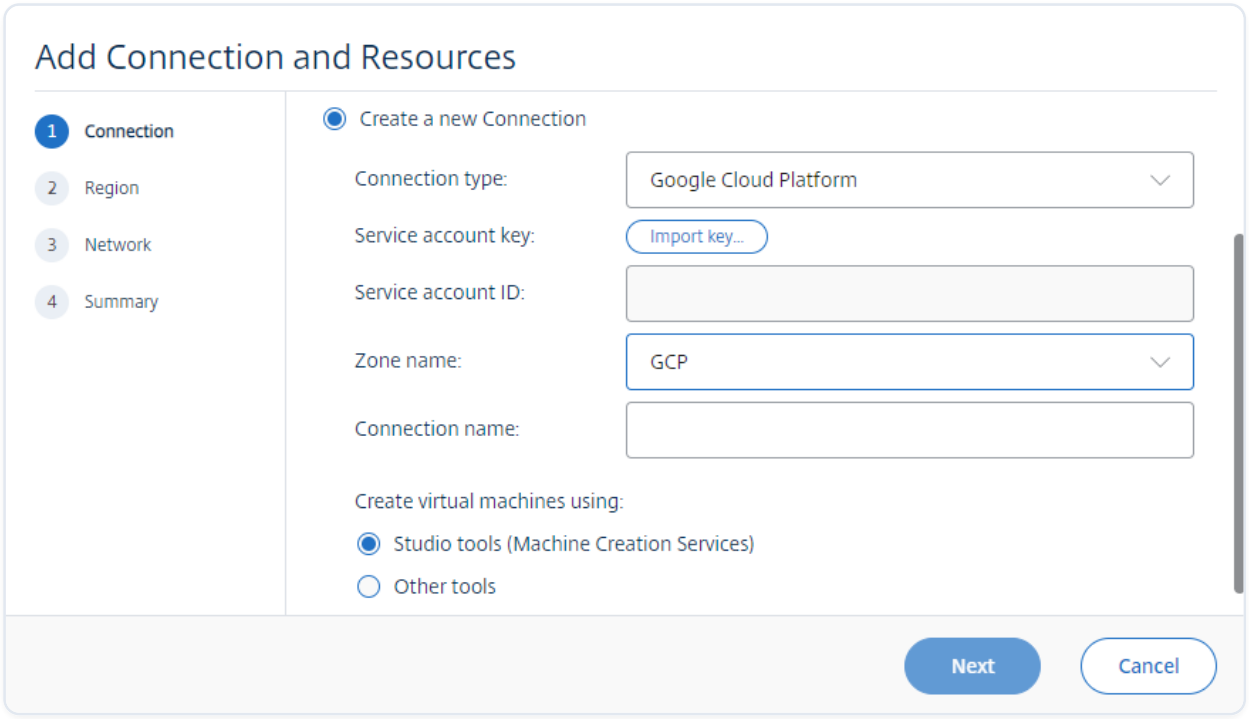
Para obtener más información, consulte Entornos de virtualización de Google Cloud Platform.

Paso 2: Cree una conexión de alojamiento a GCP en Citrix Studio

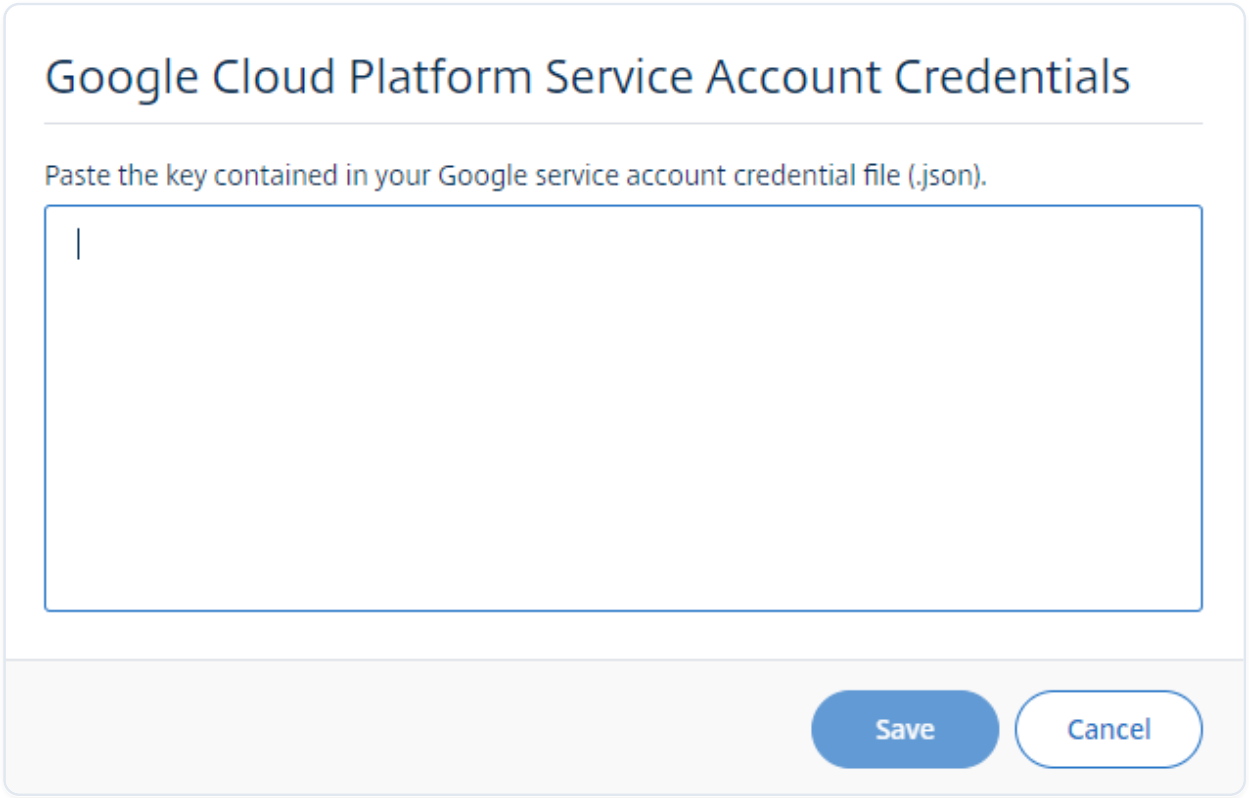
1. En Citrix Studio de Citrix Cloud, elija **Configuración** > **Alojamiento** > **Agregar conexión y recursos** para crear una conexión a GCP.



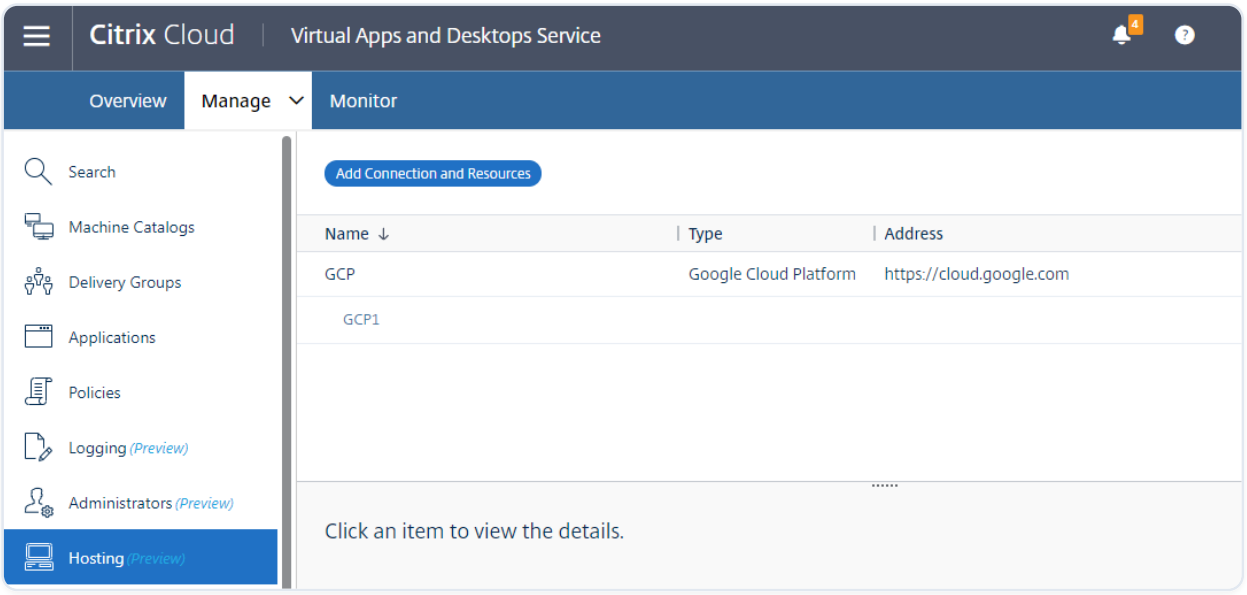
2. Elija **Google Cloud Platform** como tipo de conexión.



3. Importe la clave de cuenta de servicio de su cuenta de GCP y escriba el nombre de su conexión.



Aparece una nueva conexión en el panel de alojamiento.



Paso 3: Preparar una imagen maestra

Una imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software. Para preparar una imagen maestra, haga lo siguiente:

Paso 3a: (Solo para Ubuntu 16.04) Instalar OpenJDK 11

En Ubuntu 16.04, instale OpenJDK 11 siguiendo estos pasos:

1. Descargue la última versión de OpenJDK 11 desde `<https://jdk.java.net/archive/>`.
2. Ejecute el comando `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` para descomprimir el paquete descargado.
3. (Opcional) Ejecute el comando `mv jdk-11.0.2/ <target directory>` para guardar OpenJDK en un directorio de destino.
4. Ejecute el comando `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` para configurar el entorno de ejecución de Java.
5. Ejecute el comando `java -version` para verificar la versión de Java.

Paso 3b: Instalar el paquete Linux VDA en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso.

> Antes de instalar el paquete Linux VDA en la VM de plantilla, instale .NET Runtime 6.0.

> Según su distribución de Linux, ejecute el siguiente comando para configurar el entorno para Linux VDA:

Para RHEL/CentOS:

```
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 3c: Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8/CentOS 8, RHEL 7/CentOS 7 para que la ejecución posterior de deploymcs.sh instale el paquete ntfs-3g disponible en el repositorio EPEL.

Paso 3d: Instale ntfs-3g manualmente en SUSE

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 3e: Configurar el entorno de tiempo de ejecución

Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie las variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` proporciona variables para configurar MCS y el VDA de Linux. Las siguientes son algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben configurarse:

  Nota: Si una variable se puede establecer con varios valores, ponga los valores entre comillas simples y sepárelos con espacios. Por ejemplo, LDAP_LIST='aaa.lab:389 bbb.lab:389'.

  - `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben usar las configuraciones existentes 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 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 con MCS.
  - `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, que es el nombre NetBIOS (distingue entre mayúsculas y minúsculas) si está configurado en AD. De lo contrario, es el nombre de dominio de forma predeterminada.

- `AD_INTEGRATION`: Configura 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 en este artículo.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete de Centrify. 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.
- Las siguientes variables de configuración del VDA de Linux:

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-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`=nombre-de-sitio-dns | '<none\>' `LDAP_LIST`='lista-de-servidores-ldap' | '<none\>'

  `SEARCH_BASE`=conjunto-de-base-de-búsqueda | '<none\>' `FAS_LIST`='lista-de-servidores-fas' | '<none\>'

  `START_SERVICE`=S | N `TELEMETRY_SOCKET_PORT`=número-de-puerto

  `TELEMETRY_PORT`=número-de-puerto

Para ver un ejemplo de `mcs.conf`, consulte la siguiente captura de pantalla:

```
#!/bin/bash

#############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.



##########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

##########################DNS Configuration#####################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

##########################NTP Configuration#####################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

##########################WORKGROUP Configuration###############################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

##########################Domain Join Configuration#############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

##########################Centrify download path Configuration##################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


##########################Centrify Samba download path Configuration#############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


##########################PBIS download path Configuration######################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


##########################Machine Password Automate Update######################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

##########################Linux VDA Configuration###############################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
```

- 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
  \ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
  ```

  ```
  update -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -v "Flags" -d "0x00000003"
  ```

Paso 3f: Crear una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Si utiliza un VDA en ejecución como VM de plantilla, 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/mcs/winbind_krb5.conf.tmpl` y `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

   Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` y `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

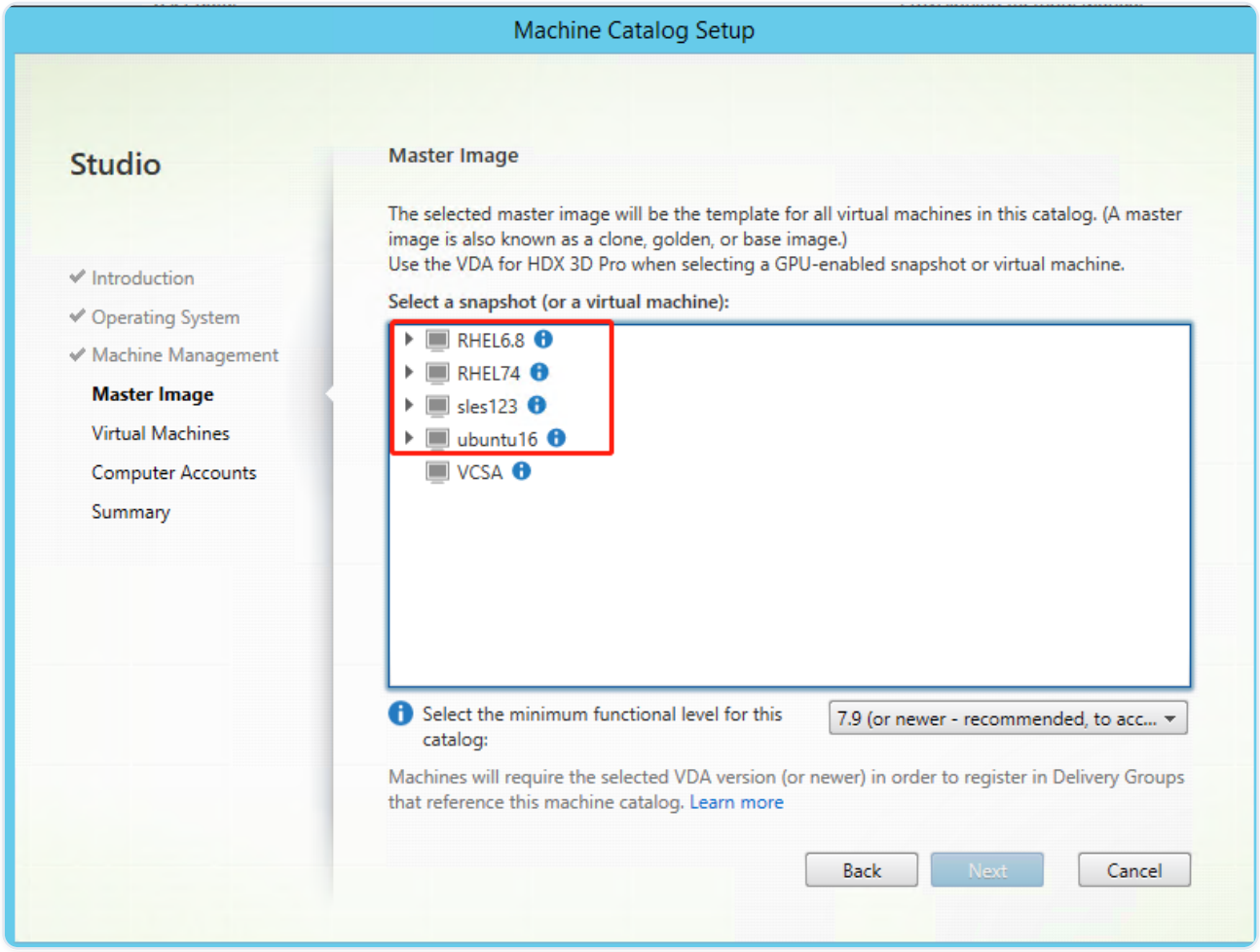
   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/mcs/centrify_krb5.conf.tmpl` y `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

   > **Nota:**
   >
   > Mantenga el formato existente utilizado en los archivos de plantilla y utilice variables como $WORKGROUP, $REALM, $realm, ${new_hostname} y $AD_FQDN.

3. Una vez que haya terminado de instalar las aplicaciones en la VM de plantilla, apague la VM de plantilla desde VMware. Tome una instantánea de la VM de plantilla.

Paso 4: Crear un catálogo de máquinas

En Citrix 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 de la lista de instantáneas.



Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear un catálogo de máquinas con Studio.

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.

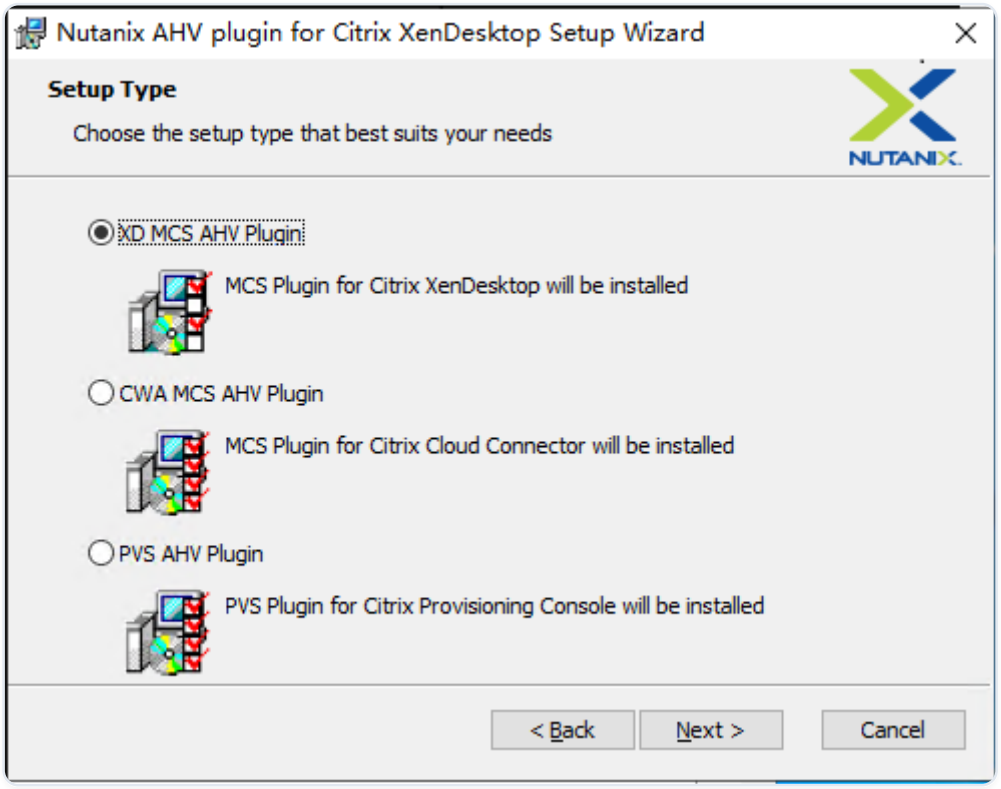
Usar MCS para crear máquinas virtuales Linux en Nutanix AHV

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 Nutanix Acropolis MCS, disponible en el Portal de asistencia 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: Instalar y registrar el plug-in de Nutanix AHV para Delivery Controllers en la nube

Después de instalar Citrix Virtual Apps and Desktops, seleccione e instale el **CWA MCS AHV Plugin** para Citrix Cloud Connectors. Instale el plug-in en todos los Citrix Cloud Connectors registrados con el arrendatario 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 plug-in

- verificar que se ha creado una carpeta de Nutanix Acropolis en `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.

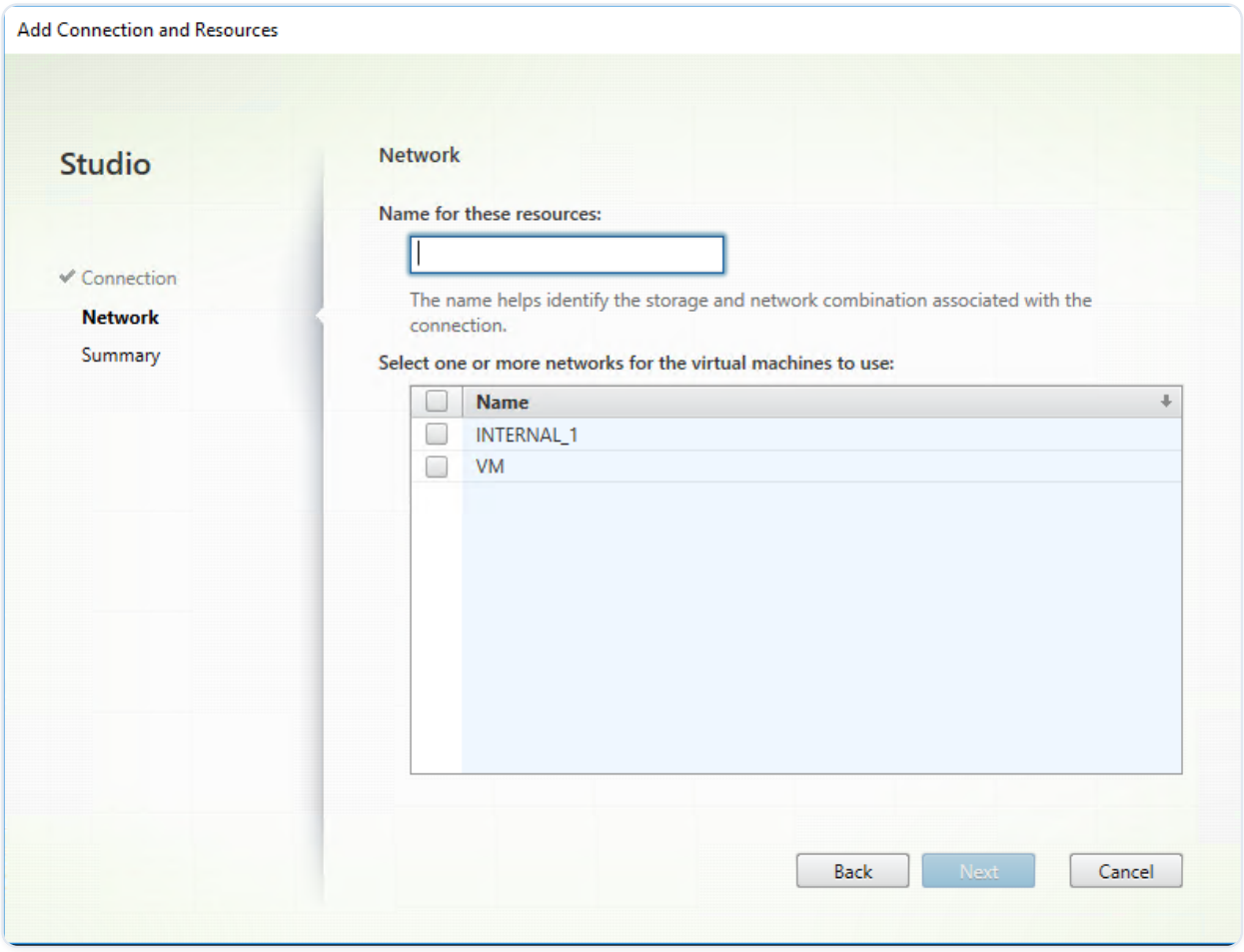
- Ejecute el comando `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`.
- Reinicie los servicios Citrix Host, Citrix Broker y Citrix Machine Creation Services en sus Delivery Controllers locales o reinicie el servicio Citrix RemoteHCLServer en los Citrix Cloud Connectors.

> **Sugerencia:**
>
> Recomendamos que detenga y luego reinicie Citrix Host, Citrix Broker y Machine Creation Services cuando instale o actualice el complemento de Nutanix AHV.

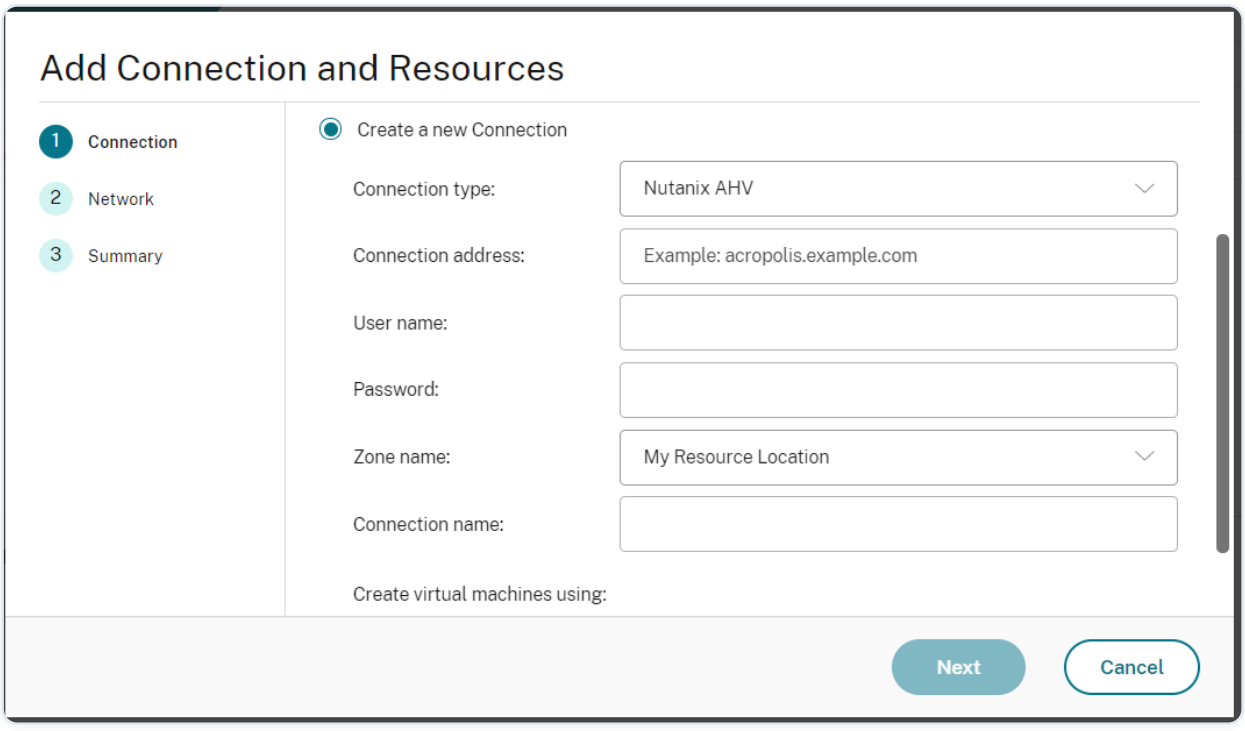
Paso 2: Crear una conexión de alojamiento a Nutanix en Citrix Studio

1. Para los Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en Citrix Studio local. 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 al hipervisor de Nutanix.
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 de alojamiento.

   Por ejemplo, en Citrix Studio local:



Por ejemplo, en la consola de Studio basada en web en Citrix Cloud:



3. En la página **Red**, seleccione una red para la unidad de alojamiento.

Paso 3: Preparar una imagen maestra en la VM de plantilla

Una imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software. Para preparar una imagen maestra, complete los siguientes pasos:

Paso 3a: Instalar el paquete de Linux VDA en la VM de plantilla

> **Nota:**

> Para usar un VDA en ejecución como VM de plantilla, omita este paso.

> Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Runtime 6.0.

> Según su distribución de Linux, ejecute el siguiente comando para configurar el entorno para el Linux VDA:

Para RHEL/CentOS:

```
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 3b: Instale el repositorio EPEL que puede ofrecer ntfs-3g

Instale el repositorio EPEL en RHEL 8/CentOS 8, RHEL 7/CentOS 7 para que la ejecución posterior de deploymcs.sh instale el paquete ntfs-3g disponible en el repositorio EPEL.

Paso 3c: Instale manualmente ntfs-3g en SUSE

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 3d: Configure el entorno de tiempo de ejecución

Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie las variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` proporciona variables para configurar MCS y el VDA de Linux. Las siguientes son algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben configurarse:

  Nota: Si una variable se puede establecer con varios valores, ponga los valores entre comillas simples y sepárelos con espacios. Por ejemplo, LDAP_LIST='aaa.lab:389 bbb.lab:389'.

  - `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben usar las configuraciones existentes 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 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 con MCS.

- `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, que es el nombre NetBIOS (distingue mayúsculas de minúsculas) si está configurado en AD. De lo contrario, es el nombre de dominio de forma predeterminada.
- `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 en este artículo.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete de Centrify. 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.
- Las siguientes variables de configuración de Linux VDA:

  `DOTNET_RUNTIME_PATH`=ruta-de-instalación-de-instalación-de-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`=nombre-de-sitio-dns | '<none\>' `LDAP_LIST`='lista-de-servidores-ldap' | '<none\>'

`SEARCH_BASE`=conjunto-de-base-de-búsqueda | '<none\>' `FAS_LIST`='lista-de-servidores-fas' | '<none\>'

`START_SERVICE`=S | N `TELEMETRY_SOCKET_PORT`=número-de-puerto

`TELEMETRY_PORT`=número-de-puerto

Para ver un ejemplo de `mcs.conf`, consulte la siguiente captura de pantalla:

```
#!/bin/bash

#############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.



##########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

##########################DNS Configuration#####################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

##########################NTP Configuration#####################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

##########################WORKGROUP Configuration###############################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

##########################Domain Join Configuration#############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

##########################Centrify download path Configuration##################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


##########################Centrify Samba download path Configuration#############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


##########################PBIS download path Configuration######################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


##########################Machine Password Automate Update######################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

##########################Linux VDA Configuration###############################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
```

- 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 de 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 de registro, respectivamente:

  ```
  create -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
  ```

  ```
  update -k
  "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard
  \ClipboardSelection" -v "Flags" -d "0x00000003"
  ```

Paso 3e: 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 las instantáneas cuando sea necesario. Después de cambiar el nombre de una instantánea, reinicie el asistente **Crear catálogo** para obtener una lista actualizada.

Paso 4: Crear un catálogo de máquinas

En Citrix Studio, cree un catálogo de máquinas y especifique el número de VM que se crearán en el catálogo. 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 CPU virtuales y el número de núcleos por vCPU.

Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear un catálogo de máquinas con Studio.

> **Nota:**
>
> Si el proceso de creación del catálogo de máquinas en 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. El grupo de entrega 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.

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 Runtime 6.0 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 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 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
```

Para RHEL 7 y CentOS 7:

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
```

Para RHEL 8 y CentOS 8:

```
sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
```

Para SUSE:

```
sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Para Ubuntu 16.04:

```
sudo dpkg -i xendesktopvda_20.12.0.20-1.ubuntu16.04_amd64.deb
```

Para Ubuntu 18.04:

```
sudo dpkg -i xendesktopvda_20.12.0.20-1.ubuntu18.04_amd64.deb
```

Para Ubuntu 20.04:

```
sudo dpkg -i xendesktopvda_20.12.0.20-1.ubuntu20.04_amd64.deb
```

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, de forma predeterminada, 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="enabled"
   ```

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 las VM creadas con MCS

Puede habilitar FAS en las VM creadas con MCS que se ejecutan en las siguientes distribuciones:

	WINBIND	SSSD	CENTRIFY	PBIS
RHEL 8, CentOS 8	Sí	No	No	Sí
RHEL 7, CentOS 7	Sí	Sí	No	Sí
Ubuntu 20.04	Sí	No	No	No

	WINBIND	SSSD	CENTRIFY	PBIS
Ubuntu 18.04	Sí	No	No	No
Ubuntu 16.04	Sí	No	No	No
Debian 10.9	Sí	No	No	No
SUSE 15.3	Sí	No	No	No
SUSE 15.2	Sí	No	No	No
SUSE 12.5	Sí	No	No	No

Habilitar FAS al preparar una imagen maestra en la VM de plantilla

1. Importe el certificado de CA raíz.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   ```

2. Ejecute ctxfascfg.sh. Para obtener más información, consulte Ejecutar ctxfascfg.sh.
3. Establezca las variables en `/etc/xdl/mcs/mcs.conf`.

   Nota:

   Debe establecer 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_Existing_Configurations_Of_Current_VDA` en Y.
   b. Establezca la variable `FAS_LIST` en la dirección de su servidor FAS o en varias direcciones de servidor FAS separadas por punto y coma y entre comillas dobles, por ejemplo, `FAS_LIST="<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>"`.
   c. Establezca las demás variables según sea necesario, como `VDI_MODE`.

4. Ejecute el script `/opt/Citrix/VDA/sbin/deploymcs.sh`.

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:**
   >
   > Debe establecer 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_Existing_Configurations_Of_Current_VDA` en Y.
   b. Establezca la variable `FAS_LIST` en la dirección de su servidor FAS.
   c. Establezca las demás variables según sea necesario, como `VDI_MODE`.

2. Importe el certificado de CA raíz.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   ```

3. Ejecute el script `/opt/Citrix/VDA/sbin/ctxfascfg.sh`. Para obtener más información, consulte Ejecutar ctxfascfg.sh.

Usar Citrix Provisioning™ para crear máquinas virtuales Linux

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 16.04
- Ubuntu 18.04
- Ubuntu 20.04
- RHEL 8.4
- RHEL 8.3

- RHEL 7.9
- SUSE 12.5
- SUSE 15.2
- SUSE 15.3

Importante:

- Recomendamos que utilice el paquete de instalación de la versión actual, disponible en el ejecutable de Citrix Provisioning, `Citrix_Provisioning_2112.iso`. Utilice el paquete según su distribución de Linux. Se requiere Citrix Provisioning Server 2109 o posterior para usar el agente de streaming de Linux 2109 y posterior.
- Cuando utilice 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.

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

Configurar Delivery Controllers para XenDesktop 7.6 y versiones anteriores

XenDesktop 7.6 y versiones anteriores requieren cambios para admitir el VDA de Linux. Para esas versiones, se requiere una revisión o un script de actualización. Las instrucciones de instalación y verificación se proporcionan en este artículo.

Actualizar la configuración de Delivery Controller™

Para XenDesktop 7.6 SP2, aplique la Actualización de revisión 2 para actualizar el Broker para escritorios virtuales Linux. La Actualización de revisión 2 está disponible aquí:

CTX142438: Actualización de revisión 2 - Para Delivery Controller 7.6 (32 bits) – Inglés

Para versiones anteriores a XenDesktop 7.6 SP2, puede usar el script de PowerShell denominado **Update-BrokerServiceConfig.ps1** para actualizar la configuración del servicio Broker. Este script está disponible en el siguiente paquete:

- citrix-linuxvda-scripts.zip

Repita los siguientes pasos en cada Delivery Controller de la granja:

1. Copie el script **Update-BrokerServiceConfig.ps1** en la máquina del Delivery Controller.
2. Abra una consola de Windows PowerShell en el contexto del administrador local.
3. Vaya a la carpeta que contiene el script **Update-BrokerServiceConfig.ps1**.
4. Ejecute el script **Update-BrokerServiceConfig.ps1**.

```
.\Update-BrokerServiceConfig.ps1
```

Sugerencia:

De forma predeterminada, PowerShell está configurado para evitar la ejecución de scripts de PowerShell. Si el script no se ejecuta, cambie la política de ejecución de PowerShell antes de volver a intentarlo:

```
Set-ExecutionPolicy Unrestricted
```

El script **Update-BrokerServiceConfig.ps1** actualiza el archivo de configuración del servicio Broker utilizando los nuevos puntos finales WCF requeridos por el VDA de Linux y reinicia el servicio Broker. El script determina automáticamente la ubicación del archivo de configuración del servicio Broker. Se crea una copia de seguridad del archivo de configuración original en el mismo directorio, con **.prelinux** añadido al nombre del archivo.

Estos cambios no afectan a la intermediación de los VDA de Windows configurados para usar la misma granja de Delivery Controller. Una única granja de Controller puede administrar e intermediar sesiones tanto para VDA de Windows como de Linux sin problemas.

verificar la configuración del Controlador de entrega

Cuando los cambios de configuración requeridos se hayan aplicado a un Delivery Controller, la cadena **EndpointLinux** aparece cinco veces en el archivo **%PROGRAMFILES%\\Citrix\\Broker\\Service\\BrokerService.exe.config**.

Desde el símbolo del sistema de Windows, inicie sesión como administrador local para comprobar:

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\

findstr EndpointLinux BrokerService.exe.config
```

Configurar el VDA de Linux

Esta sección detalla las funciones del VDA de Linux, incluida la descripción de las funciones, la configuración y la solución de problemas.

Sugerencia:

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 10.7
- SUSE 15.3
- SUSE 15.2

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 Windows AD.

Usar NIS como proveedor de UID y GID en lugar de usar AD requiere que la información de la cuenta (combinaciones de nombre de usuario y contraseña) sea la misma tanto en AD como en 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/CentOS, siga las instrucciones de Instalar Virtual Delivery Agent para Linux para RHEL/CentOS. Para una distribución Ubuntu, siga las instrucciones de Instalar Virtual Delivery Agent para Linux para Ubuntu.

> ¿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 mejor base de datos para almacenar cuentas de usuario locales y datos de usuario extendidos.

Integrar NIS con AD

Para integrar NIS con AD, haga lo siguiente:

1. Agregar el VDA de Linux como cliente NIS
2. Unirse al dominio y crear un keytab de host con Samba
3. Configurar SSSD
4. Configurar NSS/PAM
5. verificar la configuración de Kerberos

6. verificar la autenticación de usuario

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
```

Agregue 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 principal y el shell de inicio de sesión estén configurados correctamente.

Unirse al dominio y crear un keytab de host mediante Samba

SSSD no proporciona funciones de cliente de AD para unirse al dominio y administrar el archivo keytab del sistema. Existen algunos 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 mediante 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 ámbito 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 ámbito, agregue las dos opciones siguientes al comando anterior:

`--enablekrb5kdcdns --enablekrb5realmdns`

Abra **/etc/samba/smb.conf** y agregue 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`

Para unirse al dominio de Windows, su controlador de dominio debe ser accesible y debe tener 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 ámbito 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 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 agregar 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 información, consulte la página man de Linux 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`

Configurar NSS/PAM

RHEL/CentOS:

Use **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**, use el valor predeterminado.

verificar la configuración de Kerberos

Para asegurarse de que Kerberos esté configurado correctamente para su uso con Linux VDA, compruebe 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 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 utilice el nombre de dominio. Si este comando se ejecuta correctamente, no se muestra ninguna salida.

verificar que el ticket TGT para la cuenta de la máquina se haya almacenado en caché mediante:

```
sudo klist -ke
```

verificar la autenticación de usuario

Use el comando **getent** para verificar que el formato de inicio de sesión sea compatible y si el NSS funciona:

```
sudo getent passwd DOMAIN\\username
```

El parámetro **DOMAIN** indica el nombre de dominio de la 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, use una cuenta de usuario de dominio para iniciar sesión en el VDA de Linux. 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 de Kerberos del usuario son válidos y no han caducado:

```
klist
```

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**.
- 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 solucionar este problema, le recomendamos que cree 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.
- Actualmente, el modo de ventana transparente admite los siguientes administradores de ventanas: Mutter, Metacity y Compiz (Ubuntu 16.04). Kwin y otros administradores de ventanas no son compatibles. Asegúrese de que su administrador de ventanas esté configurado como uno 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>`.
- Todos los botones de la barra de tareas de las aplicaciones publicadas que se ejecutan en la misma sesión de ICA® se combinan en el mismo grupo. Para resolver este problema, configure la propiedad de la barra de tareas para que no combine los botones de la barra de tareas.

Actualización automática de Linux VDA

Esta función ayuda a actualizar automáticamente el software de su Linux VDA, de forma inmediata o a una hora programada. Es especialmente útil cuando se crean Linux VDA en Citrix Virtual Apps and Desktops Standard para Azure. No tiene privilegios de administrador de las máquinas virtuales en Azure. Para obtener más información, consulte Crear Linux VDA en Citrix Virtual Apps and Desktops Standard para Azure.

Configuración

Para usar esta función, siga estos pasos:

Paso 1: Cargue la información de actualización y los nuevos paquetes VDA en su contenedor de Azure

Paso 1a: Cree un contenedor en su cuenta de almacenamiento de Azure y establezca el nivel de acceso del contenedor en **Blob (acceso de lectura anónimo solo para blobs)**.

> **Nota:**

> Los contenedores y blobs de Azure son propiedad exclusiva de los clientes y son gestionados por ellos. Citrix® no se hace responsable de ningún problema de seguridad relacionado con ellos. Para garantizar la seguridad de los datos y la eficiencia de los costes, establezca el nivel de acceso de su contenedor en **Privado (sin acceso anónimo)** después de cada actualización automática.

> Paso 1b: Incorpore la información de actualización de su VDA a un archivo JSON llamado UpdateInfo.json. Para ver un ejemplo del formato del archivo, consulte el siguiente bloque:

```
{

 "Version": "21.04.200.4",

"Distributions":[

{

"TargetOS": "RHEL7_9",

"PackageName": "",

"PackageHash": ""

},

{

"TargetOS": "RHEL8_3",

"PackageName": "XenDesktopVDA-21.04.200.4-1.el8_x.x86_64.rpm",

"PackageHash":
"a6f2aba23b84bbc3a4640294a8bb92474e0cacbab1e5ae33416c0a4473a28d73"

},

{

"TargetOS": "UBUNTU16_04",

"PackageName": "",

"PackageHash": ""

},

{

"TargetOS": "UBUNTU18_04",

"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
```

```
"PackageHash":
"4148cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"

},

{

"TargetOS": "UBUNTU20_04",

"PackageName": "",

"PackageHash": ""

}

]

}
```

Donde, **"Version"** indica la nueva versión de VDA y **"Distributions"** es una matriz de objetos de actualización. Cada objeto contiene tres elementos:

- **"TargetOS"**: debe ser "RHEL7_9" (para RHEL 7, CentOS 7 y Amazon Linux 2), "RHEL8_3", "UBUNTU16_04", "UBUNTU18_04" o "UBUNTU20_04". El `ctxmonitorservice` no reconoce ninguna otra distribución.
- **"PackageName"**: Nombre completo del paquete VDA de la versión especificada.
- **"PackageHash"**: Un valor SHA-256 que se calcula utilizando el comando `shasum -a 256 <pkgname>`.

Paso 1c: Cargue el archivo JSON y la nueva versión de los paquetes de Linux VDA en su contenedor de Azure.

Paso 2: Habilite la función de actualización automática en la imagen maestra o en cada VDA

De forma predeterminada, la actualización automática está deshabilitada. Si crea Linux VDA en Citrix Virtual Apps and Desktops™ Standard para Azure, la habilitación de la función debe realizarse en la imagen maestra. De lo contrario, habilite la función directamente en cada VDA de destino.

Para habilitar la actualización automática, ejecute comandos similares a los siguientes para editar la clave de registro en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate.

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



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"ScheduledTime" -d "Immediately" --force



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"Url" -d "<Your-Azure-Container-Url>" --force



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
```

La siguiente tabla describe la configuración del registro.

CONFIGURACIÓN DEL REGISTRO	DESCRIPCIÓN
fEnabled	Esta configuración es obligatoria. De forma predeterminada, el valor es 0, lo que significa que la autoactualización está deshabilitada. Puede establecerlo en 1 para habilitar la autoactualización.
Url	Esta configuración es obligatoria. Establece la URL de su contenedor de Azure para obtener la información de actualización y los nuevos paquetes VDA.

CONFIGURACIÓN DEL REGISTRO	DESCRIPCIÓN
ScheduledTime	Esta configuración es obligatoria. Puede establecerla en **Immediately** o **NextStart**. **Immediately** significa ejecutar una actualización inmediatamente después de descargar los paquetes VDA. Esta opción es adecuada cuando la velocidad de descarga es alta y la actualización es urgente. Pero puede interrumpir la experiencia del usuario si hay sesiones activas al descargar el paquete. **NextStart** significa ejecutar una actualización al siguiente inicio de `ctxmonitorservice`. Esta opción es adecuada cuando la velocidad de descarga no es alta y la actualización no es urgente.
CaCertificate	Esta configuración es opcional. Establece la ruta completa de un certificado PEM para verificar la URL de su contenedor de Azure. Para los blobs de Azure, puede ser el certificado de portal.azure.com que se recupera del navegador y luego se convierte a PEM. Por seguridad, le recomendamos que añada esta configuración de registro, pero solo es compatible con Ubuntu. En RHEL, faltan algunas bibliotecas NSS para el comando `curl`. Asegúrese de establecer los privilegios mínimos del certificado.

Cuando `ctxmonitorservice` se reinicia, primero consulta **Url** para obtener el archivo UpdateInfo.json y recupera la versión de actualización del archivo JSON. Luego, `ctxmonitorservice` compara la versión de actualización con la versión actual. Si la versión actual es anterior, el servicio descarga la nueva versión del paquete VDA de Azure y la guarda localmente. Después de eso, ejecuta una actualización según la configuración de **ScheduledTime**. Para una implementación local, puede reiniciar `ctxmonitorservice` directamente para activar la actualización. Sin embargo, en Citrix Virtual Apps and Desktops Standard para Azure, donde no tiene privilegios de administrador para las máquinas virtuales, `ctxmonitorservice` solo se puede reiniciar después de que se reinicie la máquina VDA. Si una actualización falla, su VDA se revierte a la versión existente.

Nota:

- La configuración del registro que configuró en la imagen maestra no se puede cambiar.
- Si todas las máquinas virtuales de un entorno descargan un paquete al mismo tiempo, la red local puede congestionarse.
- Si tanto una actualización como la reversión fallan, se pierden los datos del usuario.
- Si una actualización falla pero la reversión tiene éxito, los usuarios de la misma red podrían tener diferentes versiones del VDA de Linux. Este caso es subóptimo.
- Una actualización suele tardar varios minutos en completarse. No hay ningún indicador de estado en Citrix Studio.

Acceso con PC remoto

Información general

El Acceso con PC remoto es una extensión de Citrix Virtual Apps and Desktops. Permite a las organizaciones que los empleados accedan fácilmente a los PC físicos de su oficina de forma remota y segura. Si los usuarios pueden acceder a los PC de su oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para realizar su trabajo.

El Acceso con PC remoto utiliza los mismos componentes de Citrix Virtual Apps™ and Desktops que ofrecen escritorios y aplicaciones virtuales. Los requisitos y el proceso de implementación y configuración del Acceso con PC remoto son los mismos que los requisitos y el proceso necesarios para implementar Citrix Virtual Apps and Desktops para la entrega de recursos virtuales. 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 de PC de oficina remotas.

Para obtener más información, consulte Acceso con PC remoto en la documentación de Citrix Virtual Apps and Desktops.

Consideraciones

Estas consideraciones son específicas de Linux VDA:

- En máquinas físicas, utilice el Linux VDA solo en modo no 3D. Debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no se puede apagar y muestra las actividades

de la sesión cuando el modo HDX™ 3D está habilitado. Mostrar esta pantalla es un riesgo potencial para la 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™ que se ejecuta en el dispositivo cliente proporciona a los usuarios acceso a las aplicaciones y los datos del PC de la oficina dentro de la sesión de escritorio de Acceso con PC remoto.
- 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

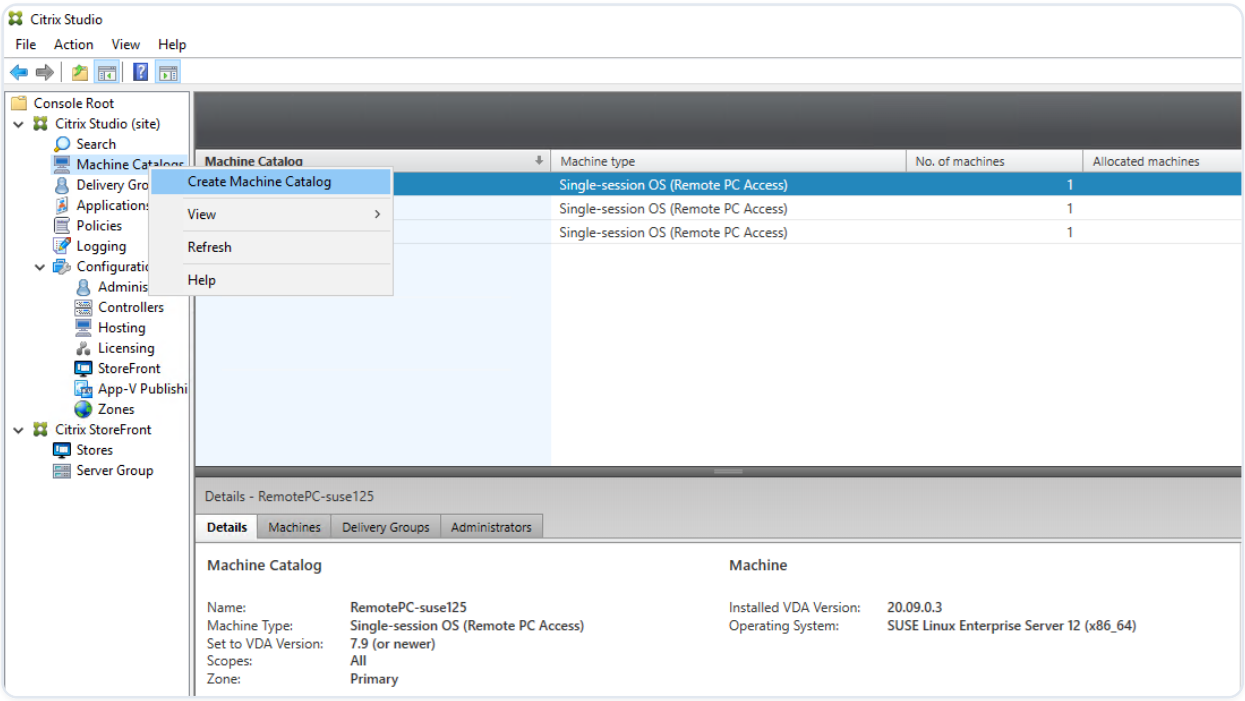
Para ofrecer sesiones de PC Linux, instale el Linux VDA en los PC de destino, cree un catálogo de máquinas de tipo **Acceso con PC remoto** y cree un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso. La siguiente sección detalla el procedimiento:

Paso 1: Instale el Linux VDA en los PC de destino

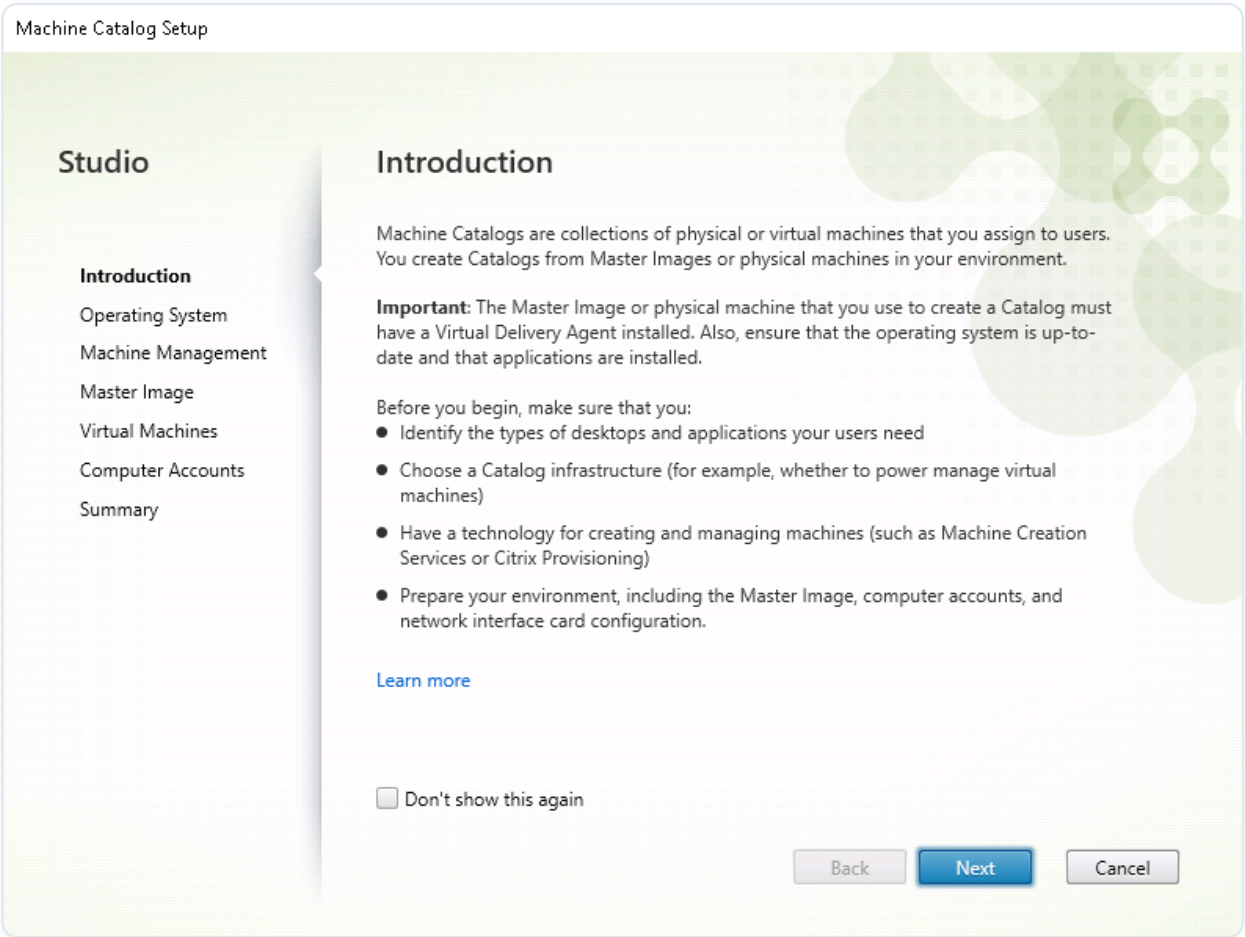
Le recomendamos que utilice easy install para instalar el Linux VDA. Durante la instalación, establezca el valor de la variable `CTX_XDL_VDI_MODE` en `Y`.

Paso 2: Cree un catálogo de máquinas de tipo Acceso con PC remoto

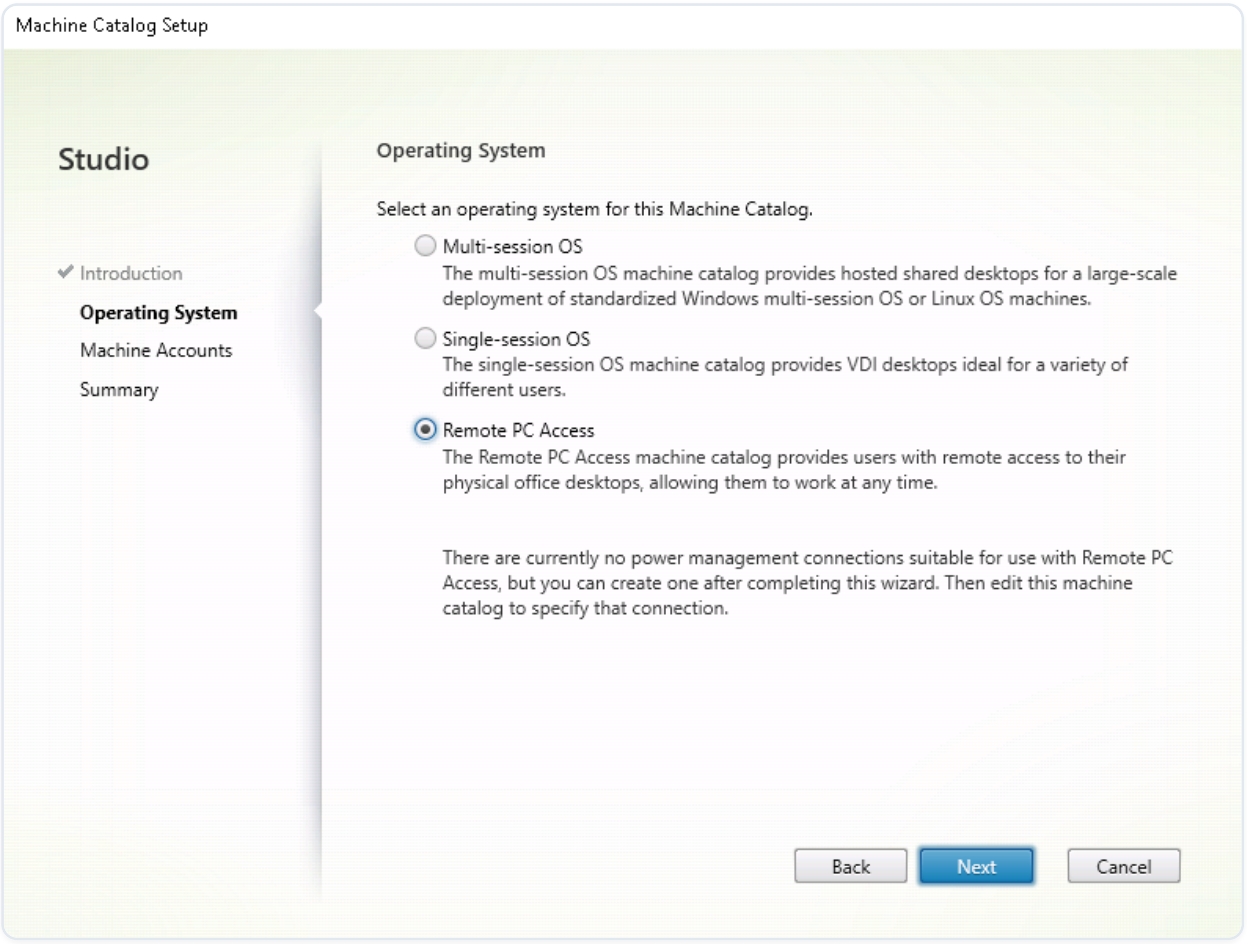
1. En Citrix Studio, haga clic con el botón secundario en **Machine Catalogs** y seleccione **Create Machine Catalog** en el menú contextual.



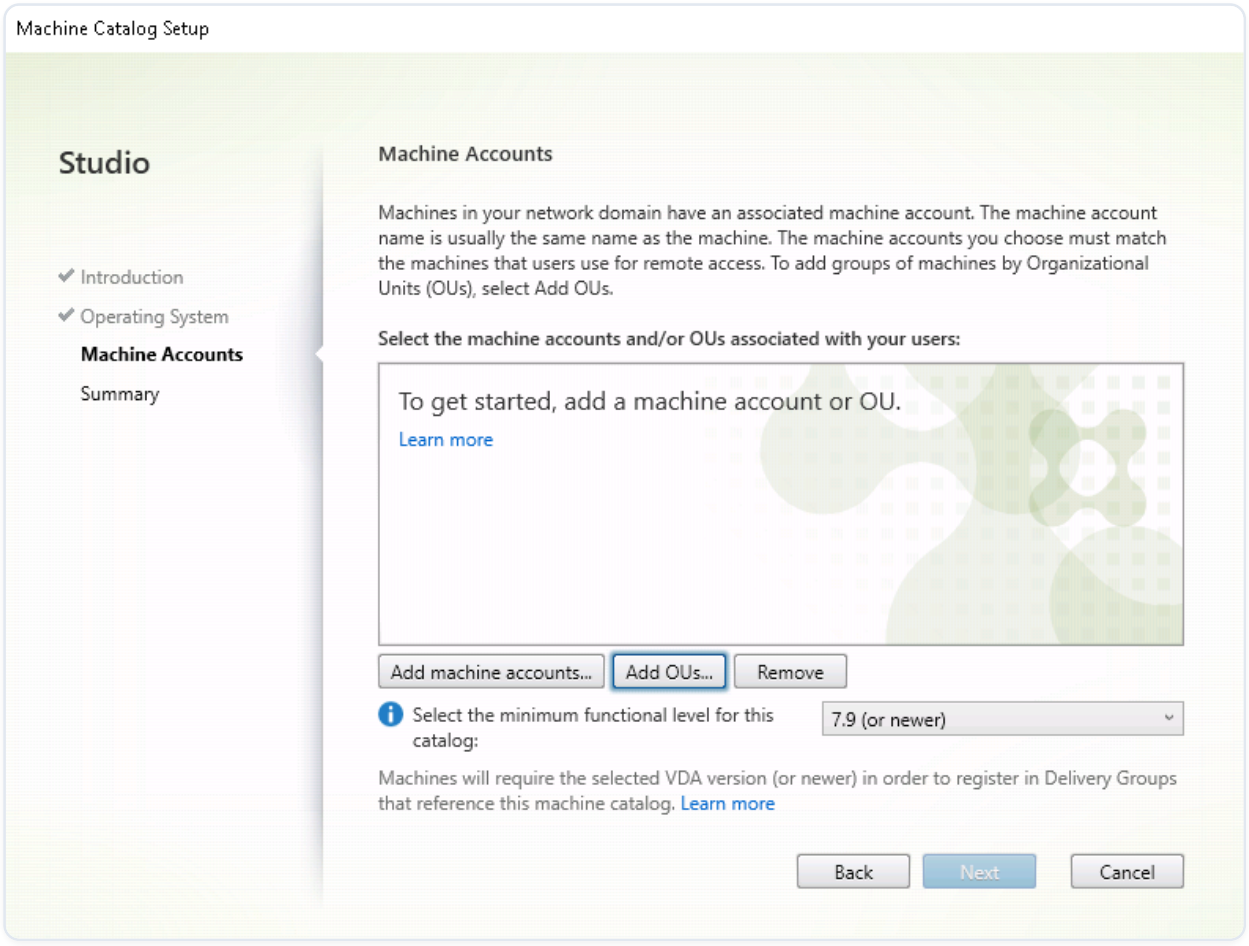
2. Haga clic en **Next** en la página **Introduction**.



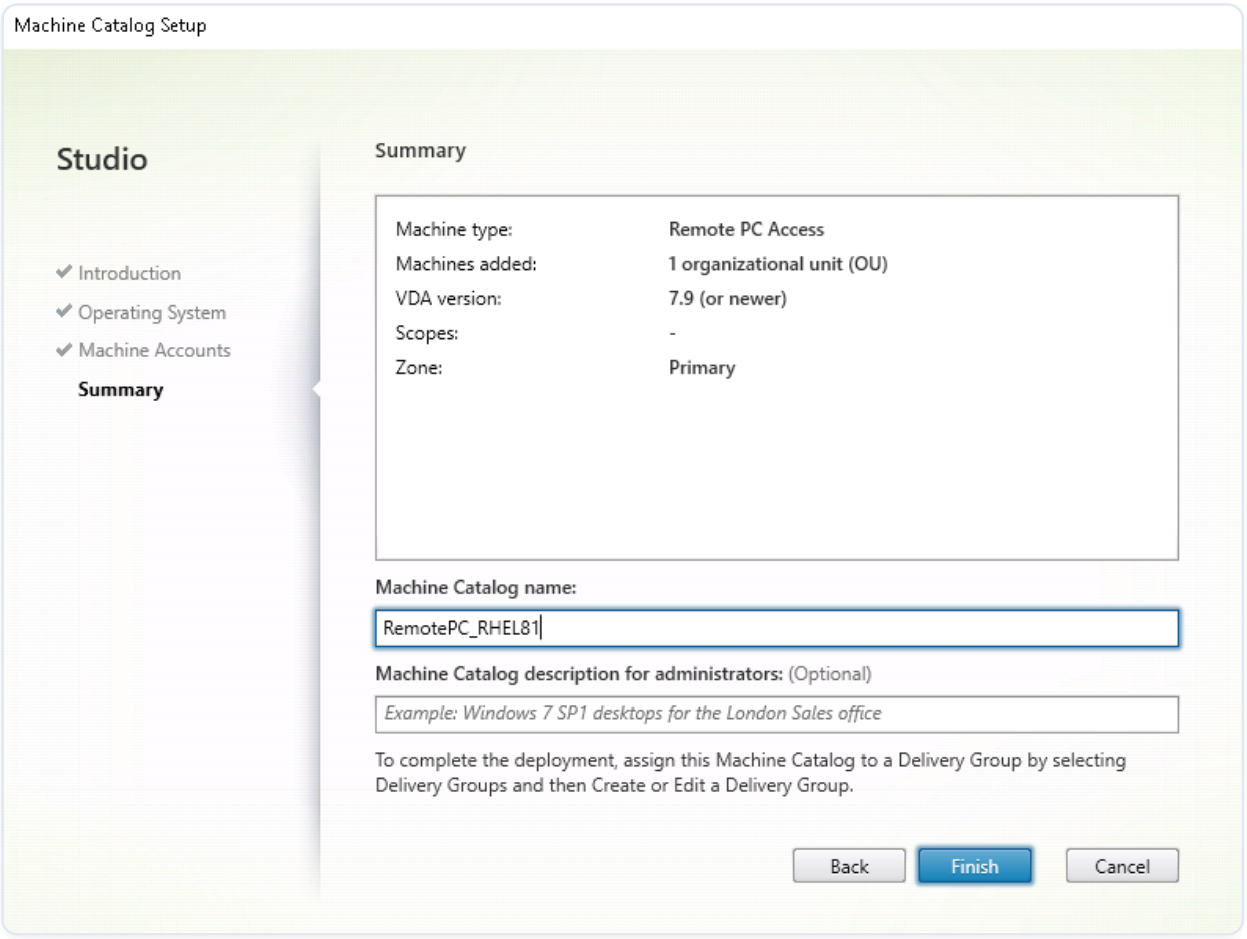
3. Seleccione **Remote PC Access** en la página **Operating System**.



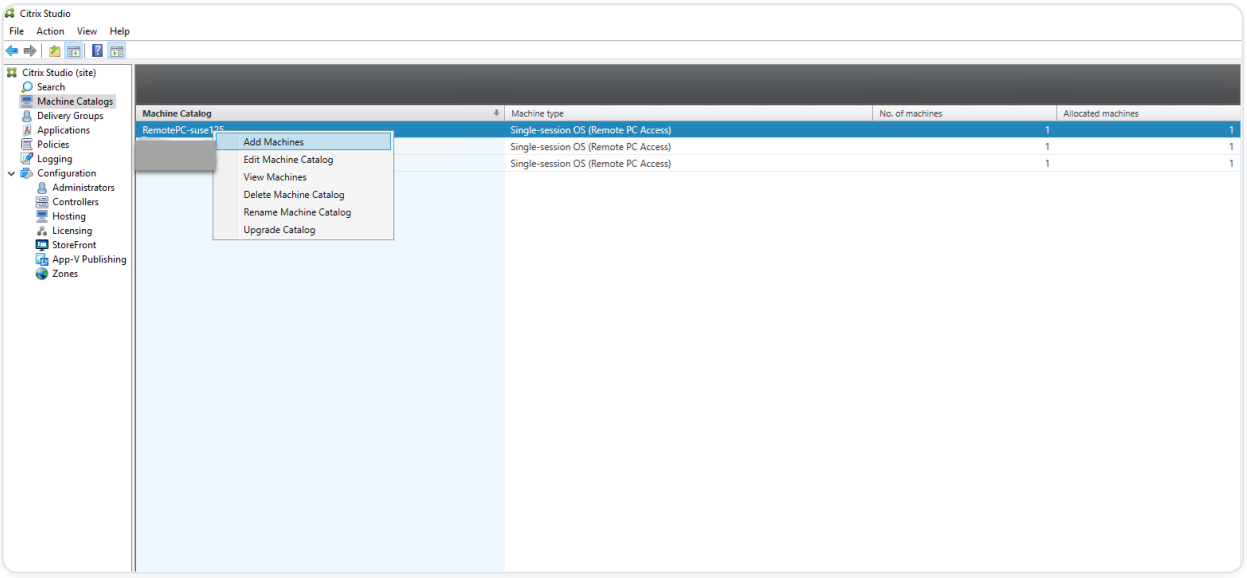
4. Haga clic en **Agregar UO** para seleccionar las UO que contienen los PC de destino, o haga clic en **Agregar cuentas de máquina** para agregar máquinas individuales al catálogo de máquinas.



5. Asigne un nombre al catálogo de máquinas.

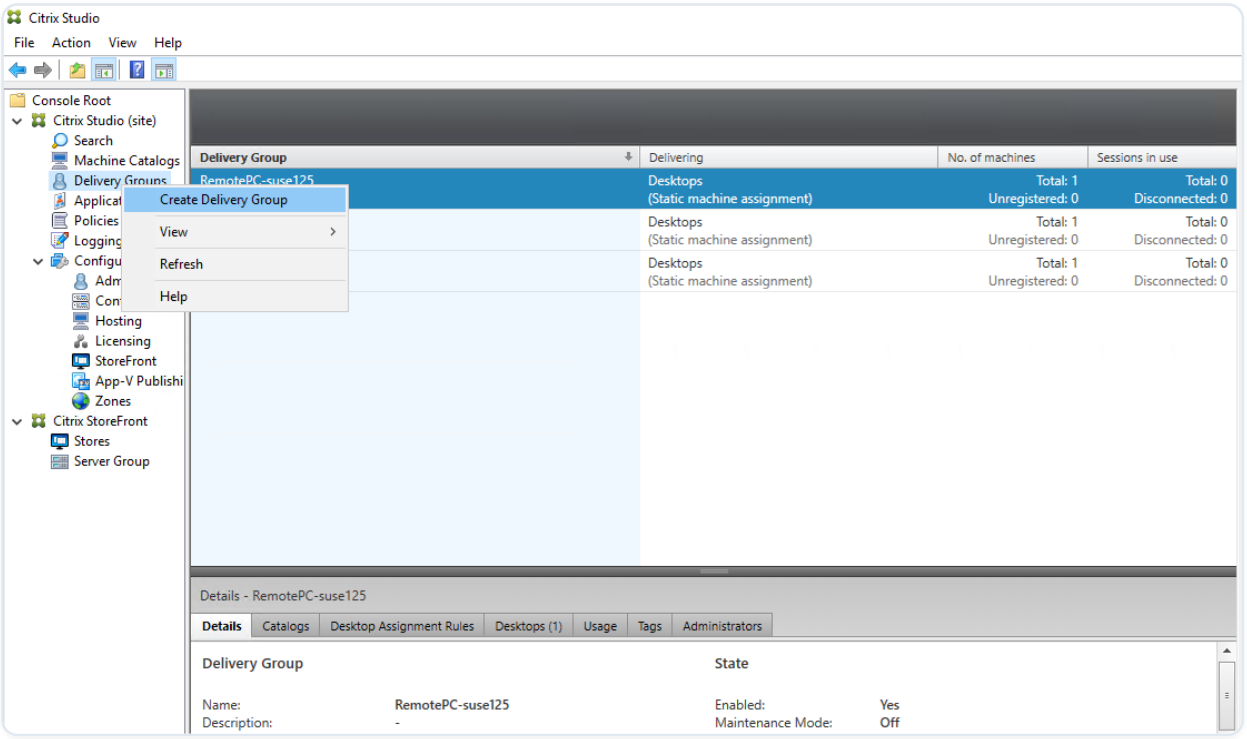


6. (Opcional) Haga clic con el botón derecho en el catálogo de máquinas para realizar las operaciones pertinentes.

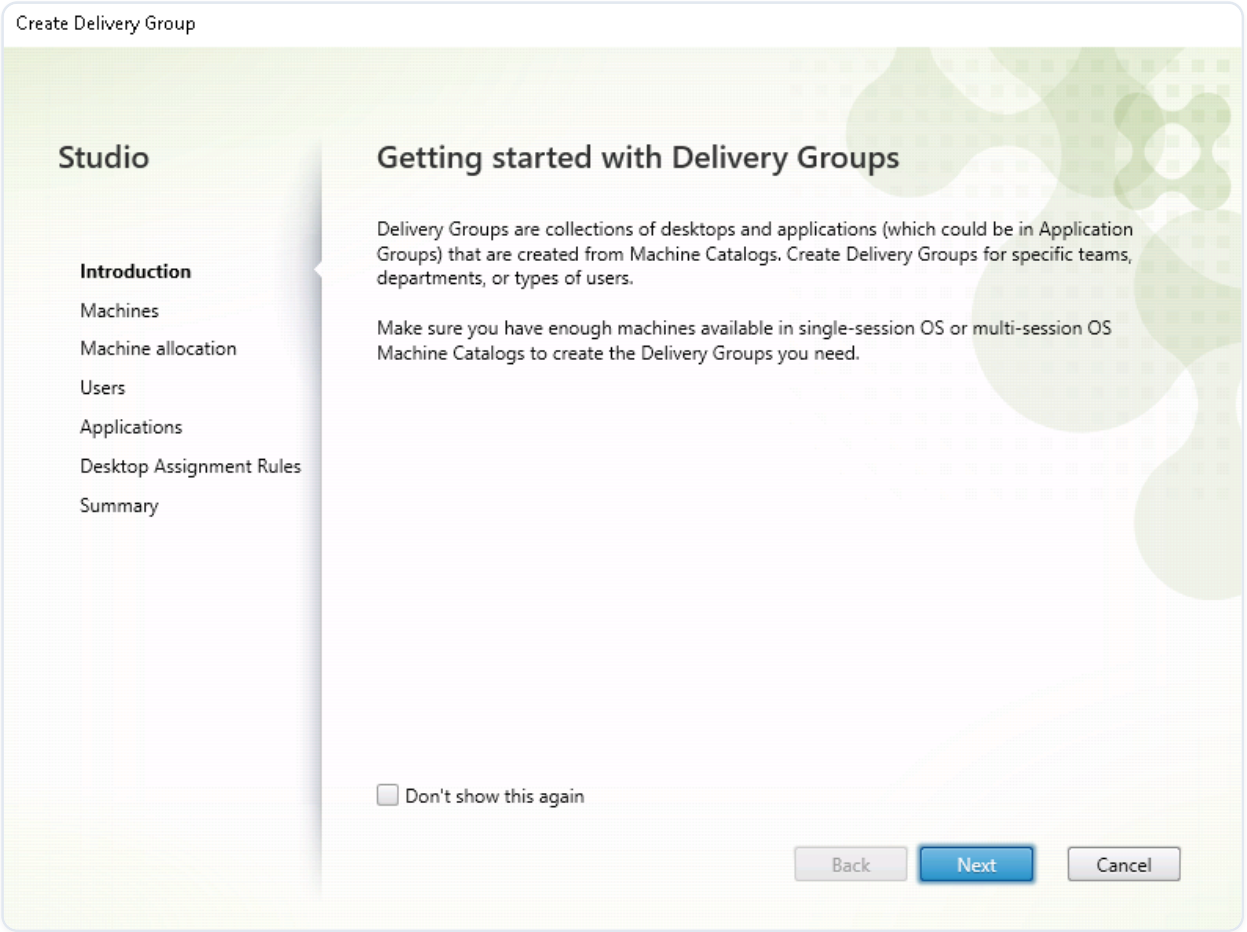


Paso 3 - Crear un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso

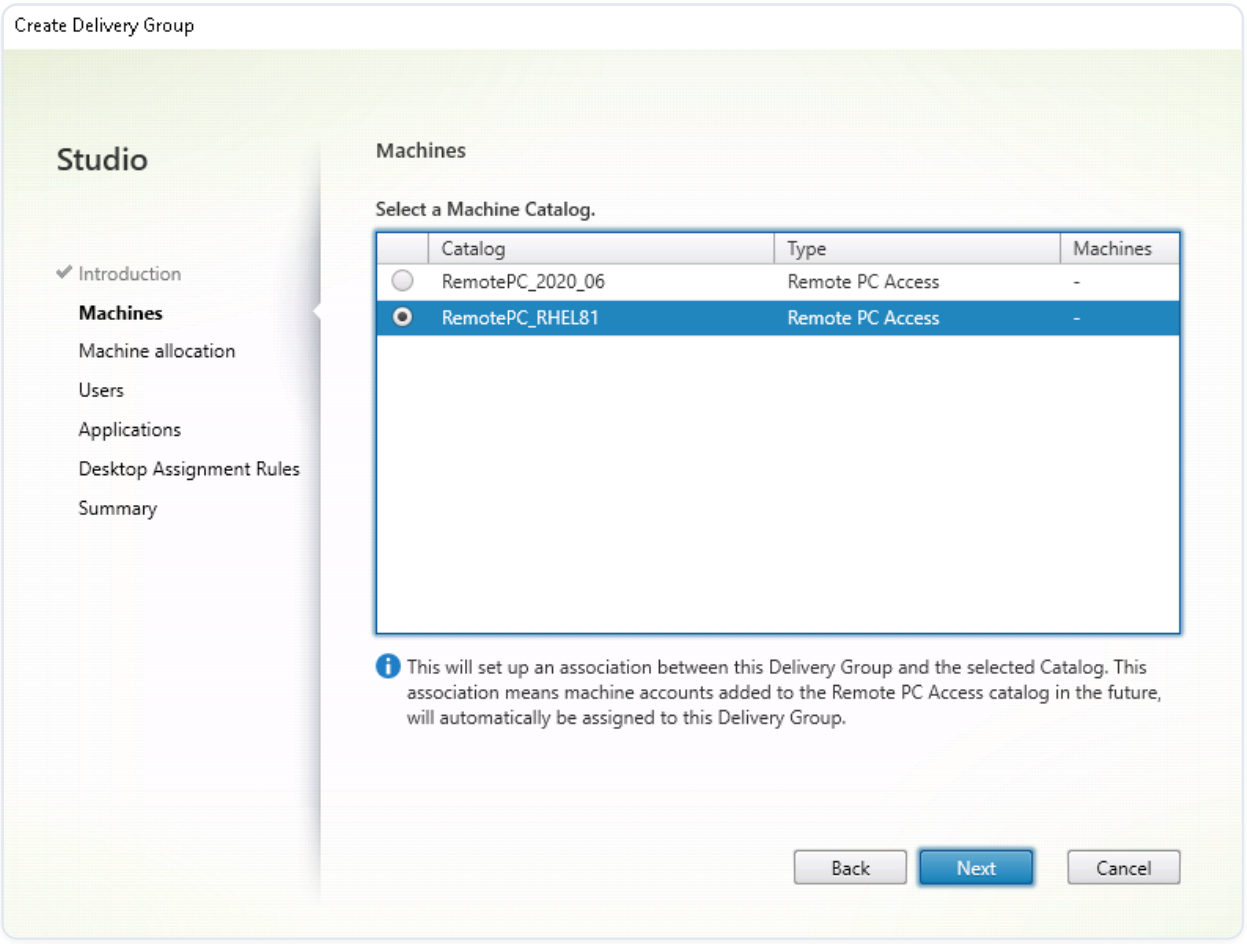
1. En Citrix Studio, haga clic con el botón derecho en **Grupos de entrega** y seleccione **Crear grupo de entrega** en el menú contextual.



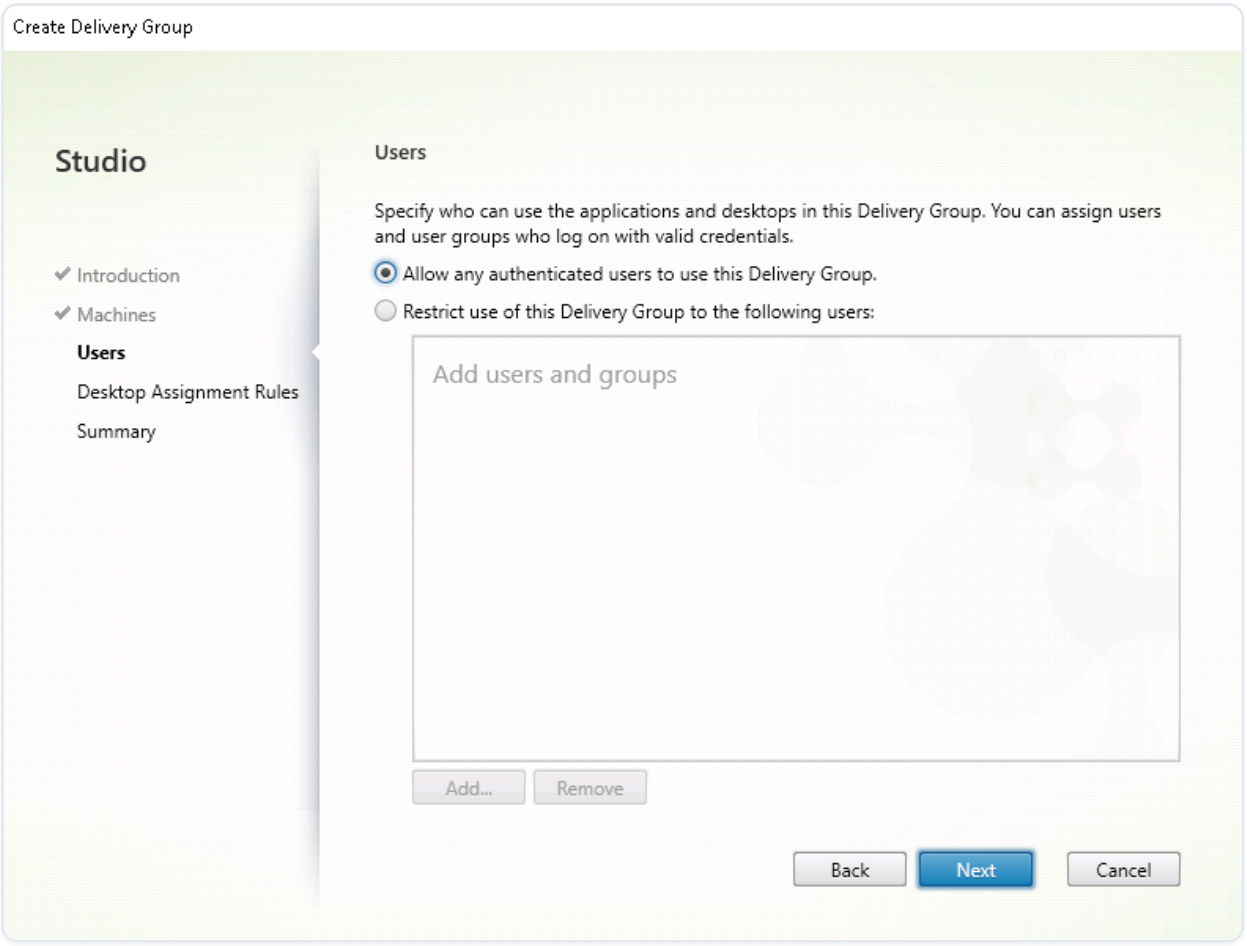
2. Haga clic en **Siguiente** en la página **Introducción a los grupos de entrega**.



3. Seleccione el catálogo de máquinas creado en el Paso 2 para asociarlo al grupo de entrega.



4. Agregue los usuarios que pueden 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:

- Servicio Citrix Virtual Apps and Desktops
- 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 remoto a PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

5. Habilite Wake on LAN en la BIOS y en la NIC de 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 la 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 del dispositivo de su NIC, por ejemplo, `eth0`. El comando `sudo ethtool <NIC>` proporciona información 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 deshabilitada. 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 configurar esta opción de forma persistente, siga los pasos siguientes según sus distribuciones:

Ubuntu:

Agregue 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:

Agregue 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.

Imprimir

Este artículo proporciona información sobre las mejores prácticas 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. Por ejemplo:

En RHEL 7:

```
sudo yum –y install cups



sudo yum -y install foomatic-filters
```

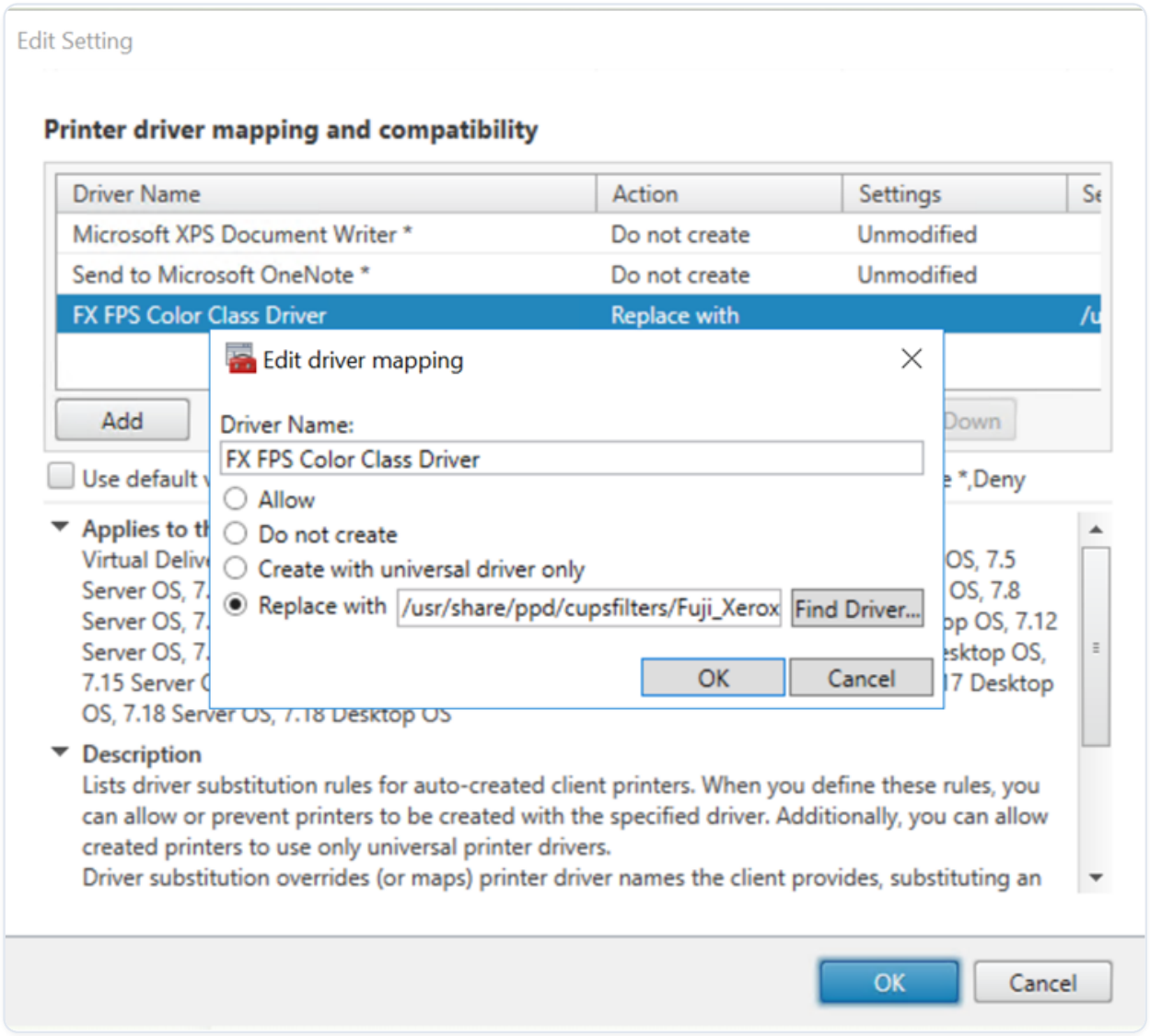
Configuración

Citrix suministra tres tipos de controlador de impresora universal (postscript, pcl5 y pcl6). Sin embargo, es posible que el controlador de impresora universal no sea compatible con la impresora del cliente. En este caso, su única opción en versiones anteriores era modificar 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\. Elija **Reemplazar con** e introduzca la ruta absoluta del archivo del controlador en el VDA.



Nota:

- Solo se admiten archivos de controlador PPD.
- No se admiten otras opciones de la directiva **Asignación y compatibilidad de controladores de impresora**. Solo **Reemplazar con** surte efecto.

Uso

Puede imprimir desde escritorios publicados y aplicaciones publicadas. Solo la impresora predeterminada del lado del cliente se asigna a una sesión de VDA de Linux. Los nombres de las impresoras son diferentes para escritorios y aplicaciones:

- Para escritorios publicados:

`CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`

- Para aplicaciones publicadas:

`CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

> **Nota:**
>
> Si el mismo usuario abre tanto un escritorio publicado como 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 administración 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:

```
service ctxcups status
```

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 service cups stop


sudo vi /etc/systemd/system/printer.target.wants/cups.service


PrivateTmp=false


sudo service cups start


sudo systemctl daemon-reload
```

Nota:

Esta configuración se realiza solo 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 ilegible

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 **printername** es un campo que 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 establecer 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 del 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 siguiendo estos pasos:

1. Inicie sesión en una sesión de escritorio publicada.
2. Ejecute el comando **vi ~/.CtxlpProfile$CLIENT_NAME**.
3. Agregue 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 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 del 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 daños en la salida de impresión, configure el controlador de impresora como el 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 inhabilitar estas notificaciones cambiando el archivo de configuración de CUPS: **/etc/cups/cupsd.conf**.

Localice el nombre de la directiva actual configurado en el archivo:

`DefaultPolicy default`

Si el nombre de la directiva es *default*, agregue las siguientes líneas al bloque XML de la directiva 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>
```

Copia y pegado de archivos

Los usuarios pueden copiar y pegar archivos entre una sesión y un cliente local. Esta función requiere Citrix Virtual Apps and Desktops™ 2006 o posterior y la aplicación Citrix Workspace™ 1903 o posterior para Windows. Las funciones de copiar y pegar se realizan mediante el menú contextual o los métodos abreviados de teclado.

Para copiar y pegar archivos correctamente, asegúrese de que:

- El número máximo de archivos no supera los 20.
- El tamaño máximo de los archivos no supera los 200 MB.

Plataformas admitidas

La función de copiar y pegar archivos está disponible para:

- RHEL 7.8
- SLES 12.5
- Ubuntu 16.04
- Ubuntu 18.04
- Debian 10

Directivas relevantes

Las siguientes directivas de portapapeles son relevantes para configurar la función. Para obtener más información sobre las directivas de portapapeles, consulte Lista de directivas admitidas.

- Redirección del Portapapeles del cliente
- Modo de actualización de la selección del portapapeles
- Modo de actualización de la selección principal

> **Nota:**
>
> Para deshabilitar la función de copiar y pegar archivos, establezca la directiva **Redirección del portapapeles del cliente** en **Prohibido** en Citrix Studio.

Limitaciones

- No se admite la función de cortar. Las solicitudes para cortar un archivo se tratan como copiar.

- No se admite la función de arrastrar y soltar.
- No se admite la copia de directorios.

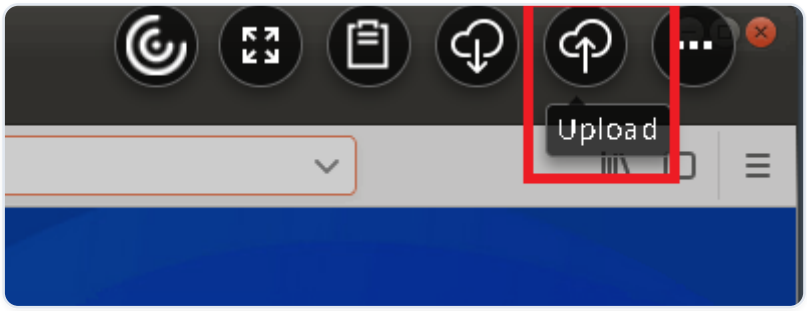
Transferencia de archivos

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 sandbox de HTML5. El atributo sandbox de HTML5 permite a los usuarios acceder a escritorios virtuales y aplicaciones 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 que desee 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 100 archivos a la vez.



> **Nota:**

> Para cargar y descargar archivos entre el VDA de Linux y el dispositivo cliente, asegúrese de que la barra de herramientas de la aplicación Citrix Workspace esté habilitada.

> 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 **Permitir la transferencia de archivos entre el escritorio y el cliente** y **Descargar archivo desde el escritorio** estén configuradas como **Permitido**.

> Estos son algunos casos de uso para la descarga automática:

- Descargar archivos en **Guardar en mi dispositivo**

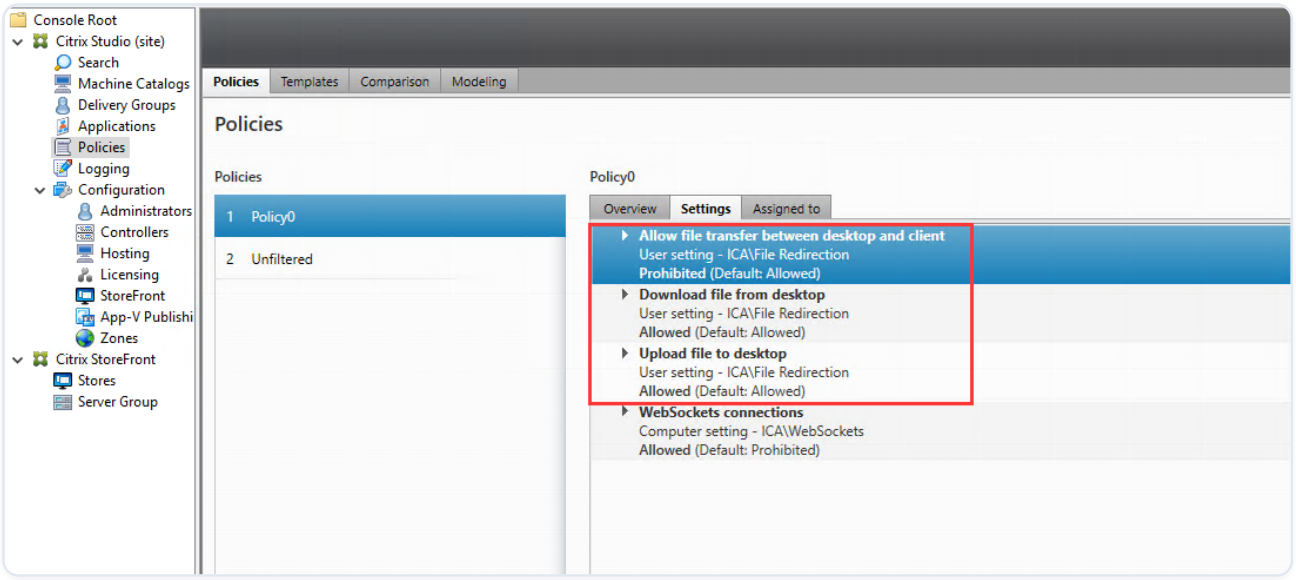
  En las sesiones de aplicaciones de escritorio y navegador web publicadas, los archivos que descargue de sitios web se pueden guardar en el directorio **Guardar en mi dispositivo** del VDA para su transferencia automática al dispositivo cliente. Para lograr la descarga automática, establezca el directorio 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 escritorio publicadas, 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

Puede usar Citrix Studio para configurar las directivas de transferencia de archivos. De forma predeterminada, la transferencia de archivos está habilitada.



Descripciones de las directivas:

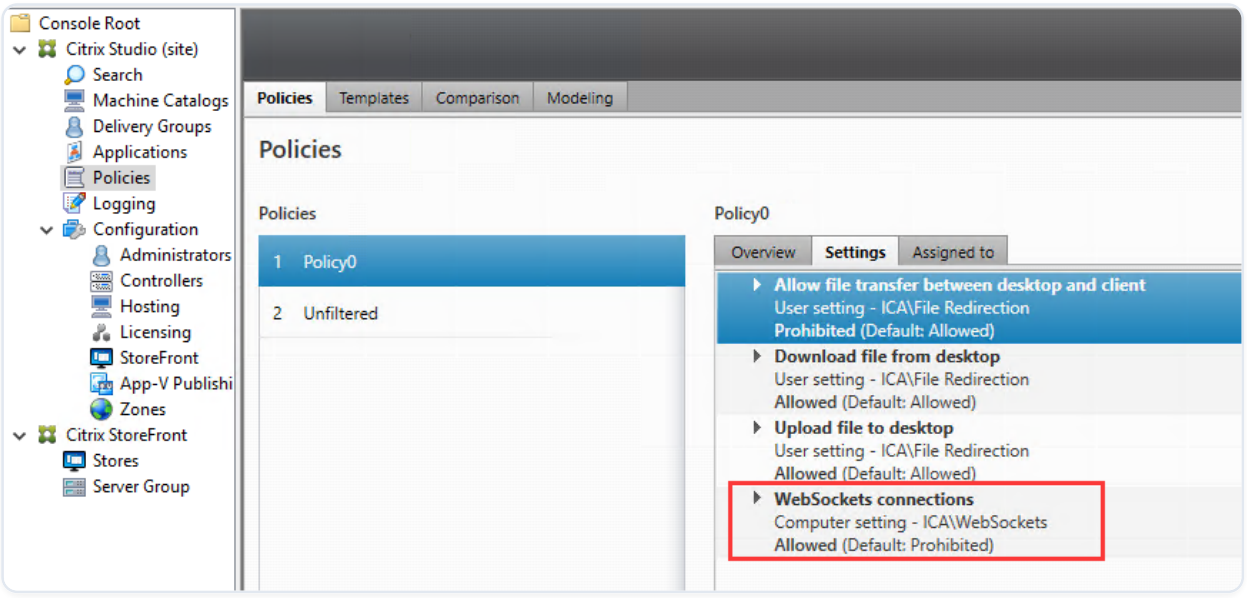
- **Permitir la transferencia de archivos entre el escritorio y el cliente.** Permite o impide que los usuarios transfieran archivos entre una sesión de Citrix Virtual Apps and Desktops™ y sus dispositivos.
- **Descargar archivo desde el escritorio.** Permite o impide que los usuarios descarguen archivos desde una sesión de Citrix Virtual Apps™ and Desktops a su dispositivo.
- **Cargar archivo al escritorio.** Permite o impide que los usuarios carguen archivos desde su dispositivo a una sesión de Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Para asegurarse de que las directivas **Descargar archivo desde el escritorio** y **Cargar archivo al escritorio** surtan efecto, establezca la directiva **Permitir la transferencia de archivos entre el escritorio y el cliente** en **Permitido**.

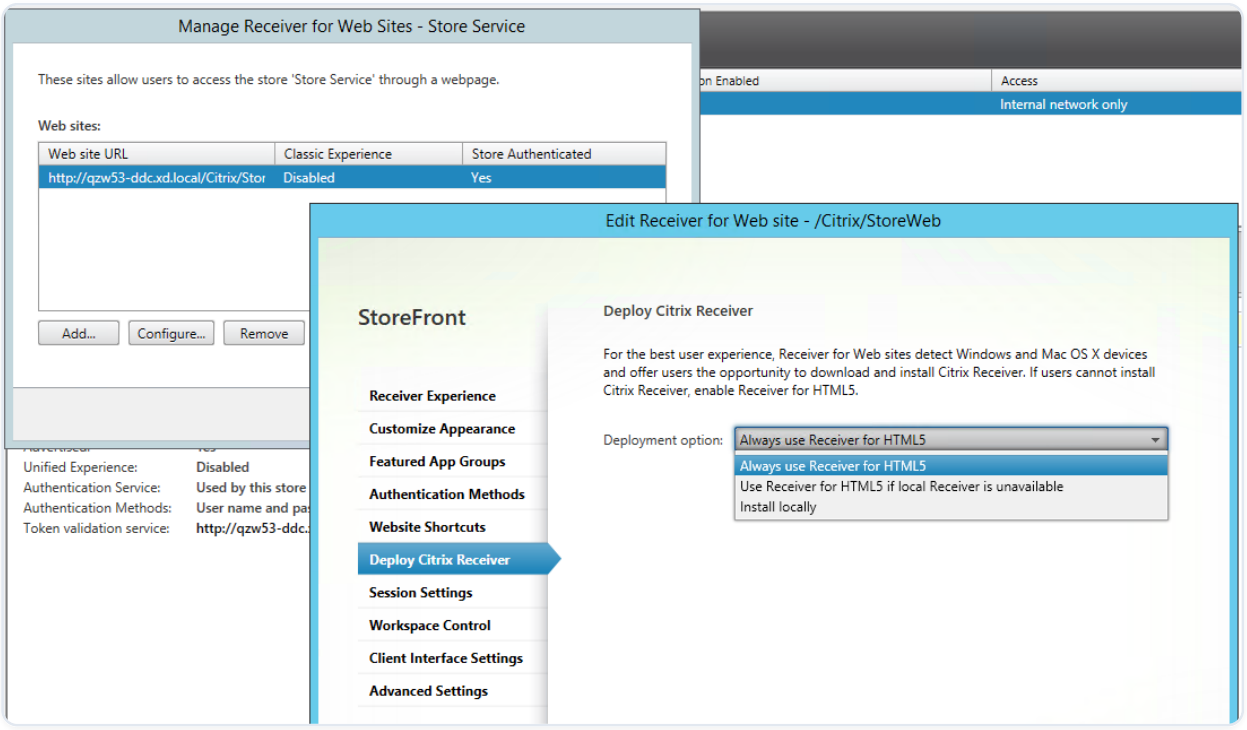
Uso

Para usar la función de transferencia de archivos a través de Citrix Workspace app para HTML5:

1. En Citrix Studio, establezca la directiva **Conexiones de WebSockets** en **Permitido**.



2. En Citrix Studio, habilite la transferencia de archivos mediante las directivas de transferencia de archivos descritas anteriormente.
3. En la consola de administración de Citrix StoreFront, haga clic en **Stores**, seleccione el nodo **Manage Receiver for Web Sites** y habilite Citrix Receiver™ para HTML5 seleccionando la opción **Always use Receiver for 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.

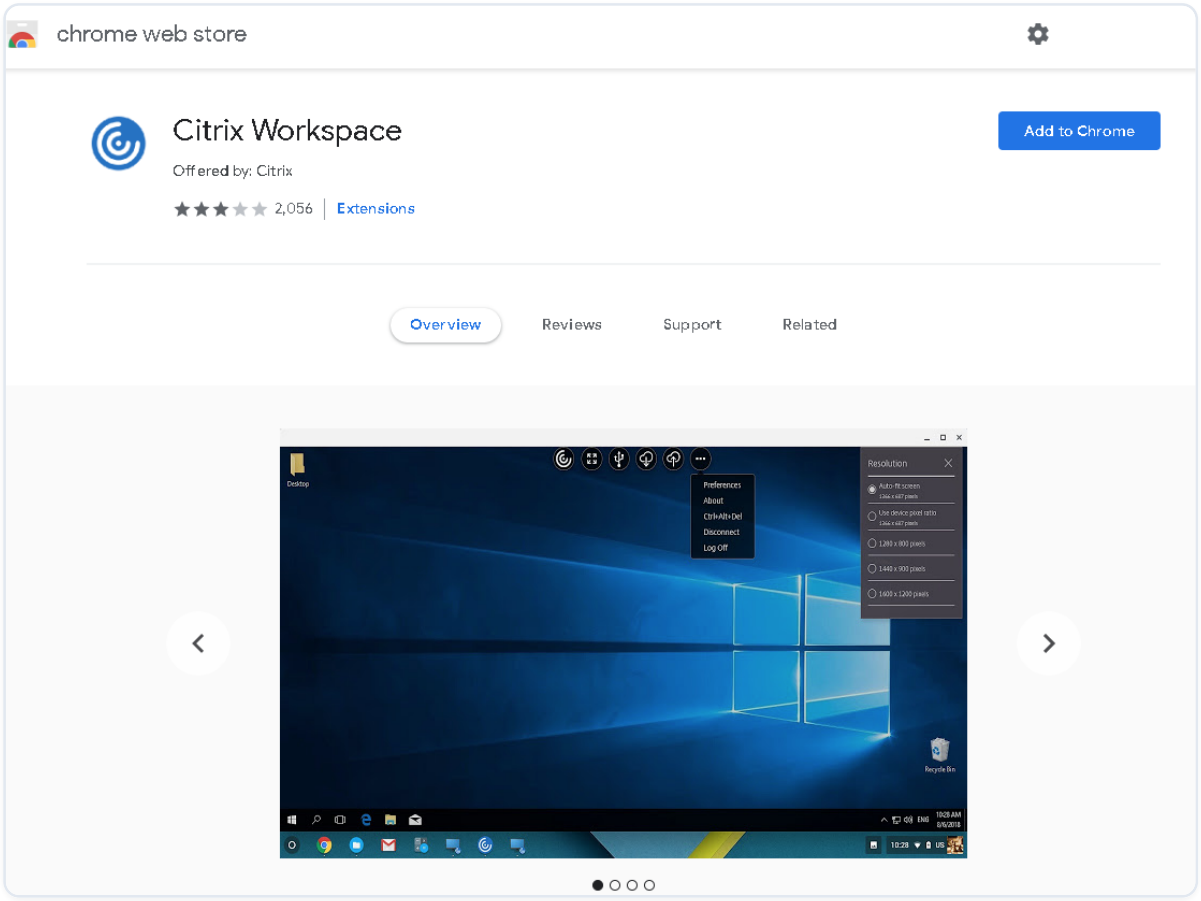
Para usar la función de transferencia de archivos a través de Citrix Workspace app para Chrome:

1. Habilite la transferencia de archivos mediante las directivas de transferencia de archivos descritas anteriormente.
2. Obtenga Citrix Workspace app de Chrome Web Store.

   Omita este paso si ya ha agregado Citrix Workspace app para Chrome a la página de 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 la 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 añadir la aplicación Citrix Workspace a Google Chrome.

3. Haga clic en la aplicación Citrix Workspace para Chrome en la página Aplicaciones de Chrome.
4. Escriba la URL de su almacén StoreFront™ para conectarse.

   Omita este paso si ya ha escrito la URL.

5. Inicie una sesión de aplicación o escritorio virtual. Realice una o varias transferencias de archivos entre el VDA de Linux y su dispositivo cliente.

Impresión PDF

Con 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.

Linux VDA 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, habilite las siguientes directivas en Citrix Studio:

- **Redirección de impresora de cliente** (habilitada de forma predeterminada)
- **Crear automáticamente impresora universal PDF** (inhabilitada de forma predeterminada)

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.

Configurar gráficos

Este artículo proporciona orientación para la configuración y el ajuste fino de los gráficos de Linux VDA.

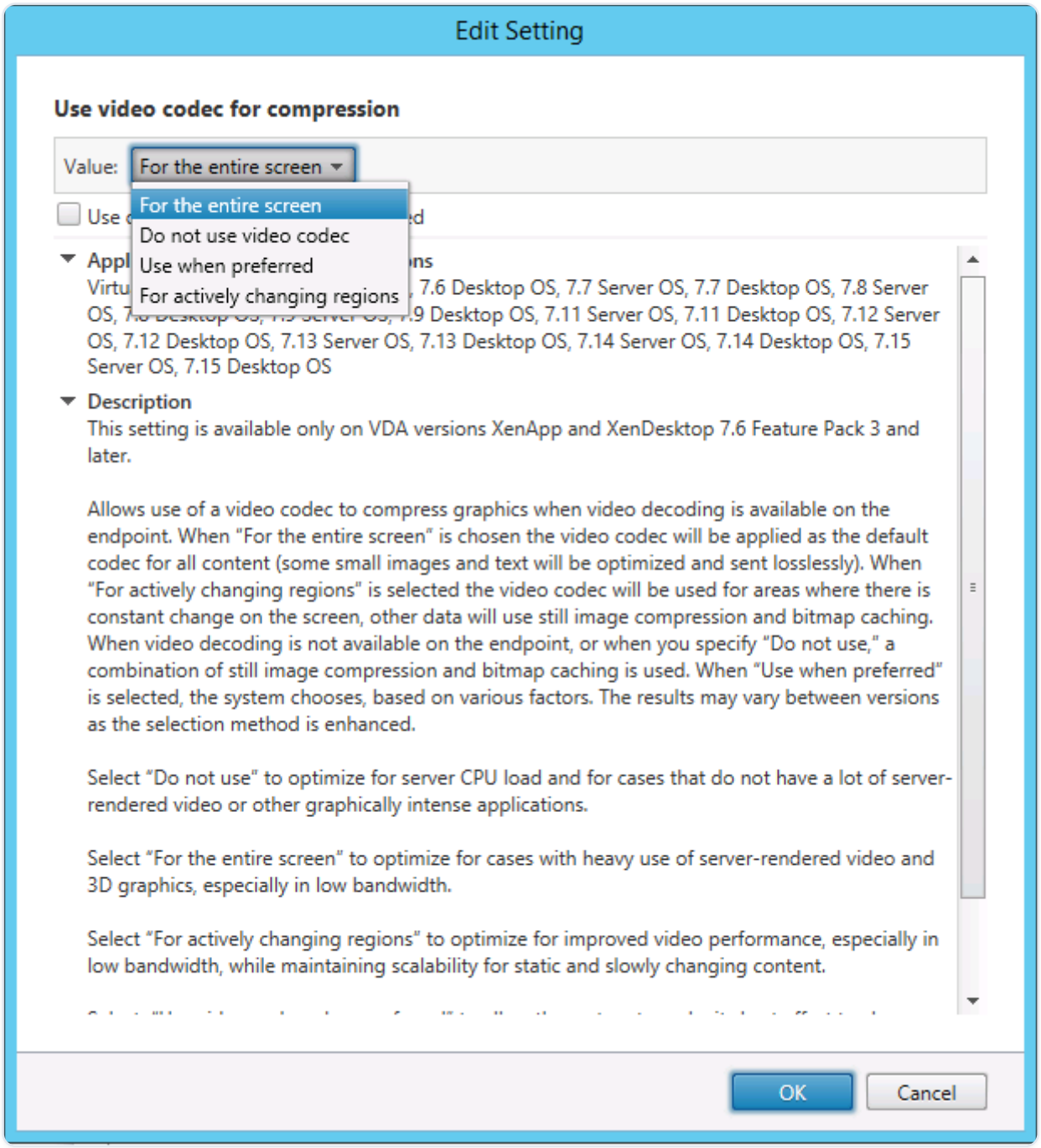
Para obtener más información, consulte Requisitos del sistema y la sección Información general de la instalación.

Configuración

Thinwire es la tecnología de acceso remoto a la pantalla 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. Mantener esta configuración garantiza que Thinwire se seleccione para todas las conexiones 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 a pantalla completa para optimizar la experiencia del usuario y el ancho de banda, especialmente en casos de uso intensivo de gráficos 3D.
- **Para regiones que cambian activamente**. La tecnología de visualización adaptativa de Thinwire identifica las imágenes en movimiento (vídeo, 3D en movimiento) y utiliza H.264 solo en la parte de la pantalla donde la imagen se mueve. El ***uso selectivo del códec de vídeo H.264*** permite a HDX Thinwire detectar y codificar las partes de la pantalla que se actualizan con frecuencia utilizando el códec de vídeo H.264, por ejemplo, contenido de vídeo. 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 ancho de banda y una mejor calidad para el contenido de vídeo, combinado con texto sin pérdidas o imágenes de alta calidad en otras partes. Para habilitar esta función, cambie la configuración de la directiva **Usar códec de vídeo para la compresión** a **Usar cuando se prefiera** (predeterminado) o **Para regiones que cambian activamente**. Para obtener más información, consulte Configuración de directivas de gráficos.



Algunas otras configuraciones de directiva, incluidas las siguientes configuraciones de directiva de visualización, se pueden utilizar para optimizar el rendimiento del acceso remoto a la pantalla:

- **Profundidad de color preferida para gráficos sencillos**
- **Velocidad de fotogramas objetivo**
- **Calidad visual**

Usar H.264 para Compilación a sin pérdidas en Thinwire

De forma predeterminada, la preferencia **Compilación a sin pérdidas** de la configuración de directiva **Calidad visual** es ahora H.264 en lugar de JPEG para las imágenes en movimiento.

La codificación H.264 ofrece una calidad de imagen superior. La directiva **Usar códec de vídeo para la compresión** controla esa preferencia, siendo el valor predeterminado **Usar cuando se prefiera**. Para forzar que **Compilación sin pérdidas** use JPEG, establezca la directiva **Usar códec de vídeo para la compresión** en **No usar códec de vídeo**. Si su cliente no admite H.264 selectivo, **Compilación sin pérdidas** recurre a JPEG independientemente de la configuración de la directiva. Citrix Receiver para Windows 4.9 a 4.12, Citrix Receiver para Linux 13.5 a 13.10, la aplicación Citrix Workspace 1808 para Windows y versiones posteriores, y la aplicación Citrix Workspace 1808 para Linux y versiones posteriores admiten H.264 selectivo. Para obtener más información sobre la configuración de las directivas **Calidad visual** y **Usar códec de vídeo para la compresión**, consulte Configuración de directivas de visualización y Configuración de directivas de gráficos.

Compatibilidad con el códec de vídeo H.265

A partir de la versión 7.18, el VDA de Linux admite el códec de vídeo H.265 para la aceleración de hardware de gráficos y vídeos remotos. Puede usar esta función en Citrix Receiver para Windows 4.10 a 4.12 y en la aplicación Citrix Workspace 1808 para Windows y versiones posteriores. Para beneficiarse de esta función, habilítela tanto en el VDA de Linux como en su cliente. Si la GPU de su cliente no admite la decodificación H.265 mediante la interfaz DXVA, la configuración de la directiva Decodificación H.265 para gráficos se ignora y la sesión vuelve a usar el códec de vídeo H.264. Para obtener más información, consulte Codificación de vídeo H.265.

Para habilitar la codificación de hardware H.265 en el VDA:

1. Habilite la directiva **Usar codificación de hardware para códec de vídeo**.
2. Habilite la directiva **Optimizar para cargas de trabajo de gráficos 3D**
3. Asegúrese de que la directiva **Usar códec de vídeo para la compresión** sea la predeterminada o esté establecida en **Para toda la pantalla**.
4. Asegúrese de que la directiva **Calidad visual NO** esté establecida en **Compilación sin pérdidas** o **Siempre sin pérdidas**.

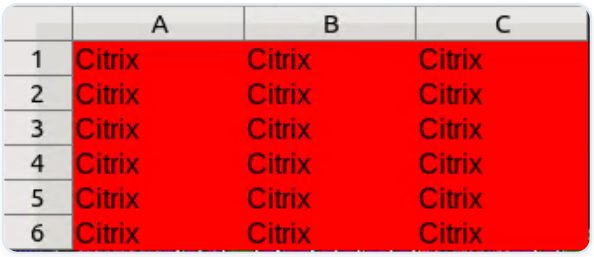
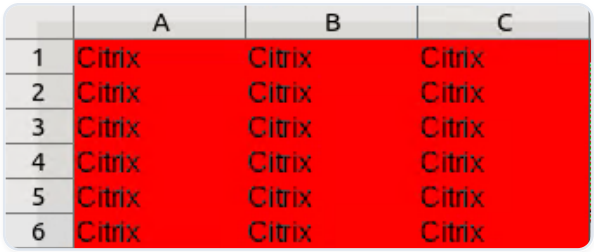
Para habilitar la codificación de hardware H.265 en su cliente, consulte Codificación de vídeo H.265.

Compatibilidad con la codificación de software YUV444

El VDA de Linux admite la codificación de software YUV444. El esquema de codificación YUV asigna valores de brillo y color a cada píxel. En YUV, '`Y`' representa el brillo o el valor '`luma`', y '`UV`' representa los valores de color o 'croma'. Puede usar esta función del VDA de Linux en Citrix

Receiver para Windows 4.10 a 4.12 y en la aplicación Citrix Workspace 1808 para Windows y versiones posteriores.

Cada valor único de Y, U y V comprende 8 bits, o un byte, de datos. El formato de datos YUV444 transmite 24 bits por píxel. El formato de datos YUV422 comparte los valores U y V entre dos píxeles, lo que resulta en una tasa de transmisión promedio de 16 bits por píxel. La siguiente tabla muestra una comparación intuitiva entre YUV444 y YUV420.

YUV444	YUV420
	

Para habilitar la codificación de software YUV444 en el VDA:

1. Asegúrese de que la directiva **Usar códec de vídeo para la compresión** esté establecida en **Para toda la pantalla**.
2. Asegúrese de que la directiva **Calidad visual** esté establecida en **Siempre sin pérdidas** o **Crear sin pérdidas**.

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 según las estimaciones de ancho de banda. 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, mayor será la nitidez de 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 directivas compatibles.

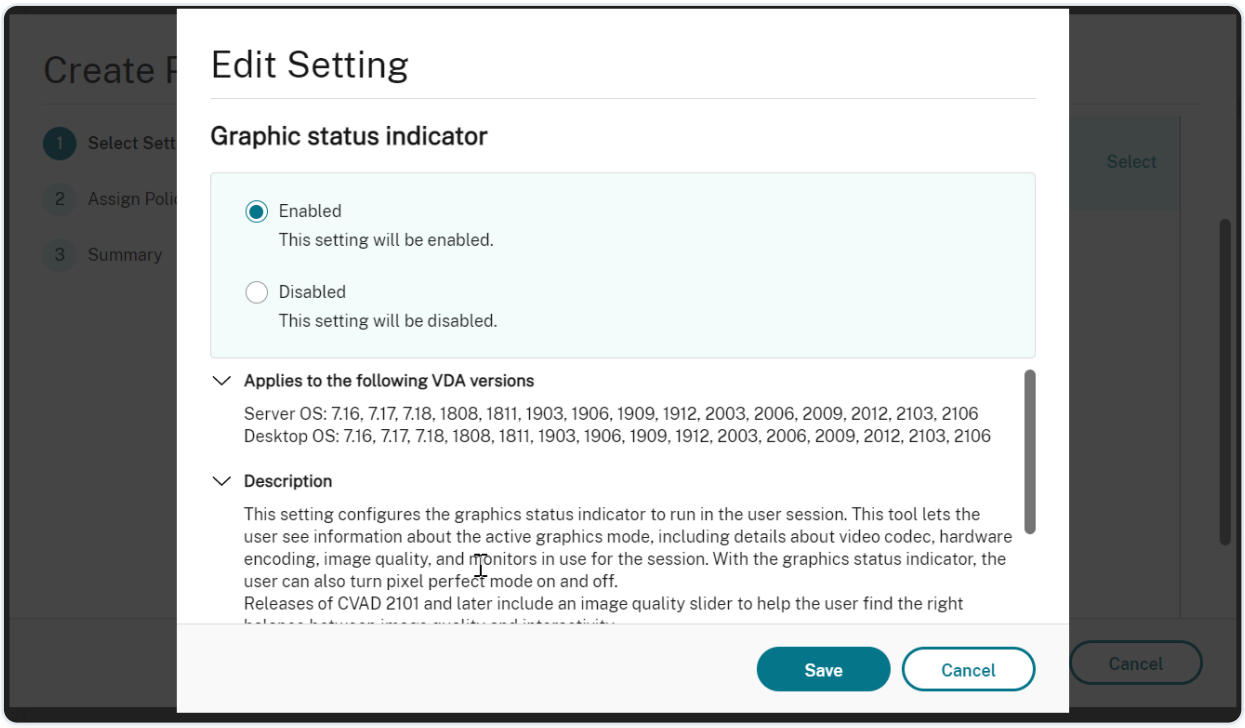
Para obtener información sobre la configuración de la compatibilidad con varios monitores en el Linux VDA, consulte CTX220128.

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 usar el control deslizante, siga estos pasos:

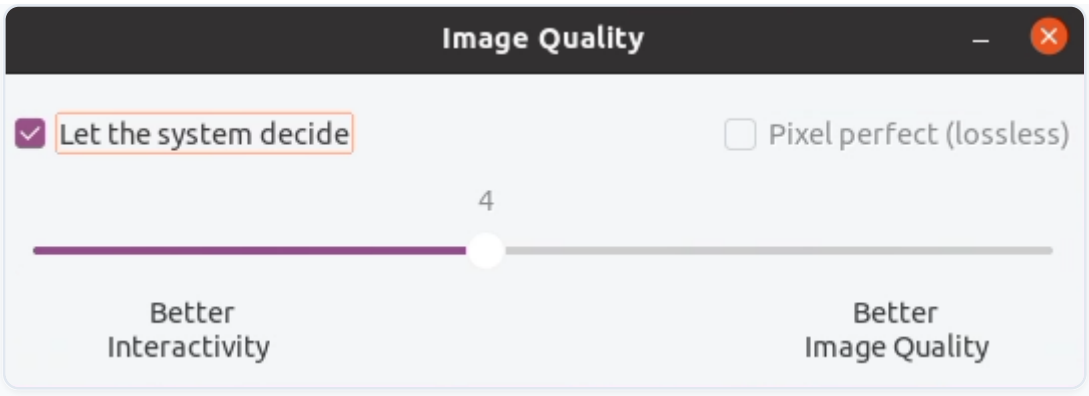
1. Habilite la política **Indicador de estado gráfico** en Citrix Studio.



2. Abra el Terminal y ejecute el comando `ctxslider`. Aparecerá la interfaz de usuario del control deslizante.

Nota:

Si ha establecido la directiva **Calidad visual** en **Siempre sin pérdidas** o **Compilación sin pérdidas**, la interfaz de usuario del control deslizante no se muestra.



Las siguientes opciones están ahora disponibles:

- Para cambiar la calidad de la 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**.

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 a pantalla completa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000000" --force
```

Comprobar si H.264 está en uso

Ejecute el siguiente comando para comprobar si H.264 está en uso (**0** significa no en uso; **1** significa en uso):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000000" --force
```

Comprobar si H.265 está en uso

Ejecute el siguiente comando para comprobar si 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
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H265" -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 es significativo cuando se utiliza un códec de vídeo.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000000" --force
```

Comprobar si la codificación por software YUV444 está en uso

Ejecute el siguiente comando para comprobar si la codificación por 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
```

Comprobar si la codificación por 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
```

Los resultados son similares a:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --force
```

Otra forma es usar el comando **nvidia-smi**. Los resultados son similares a los siguientes si la codificación por hardware está en uso:

```
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 el controlador de gráficos NVIDIA GRID esté instalado correctamente

Para verificar que el controlador de gráficos NVIDIA GRID esté instalado correctamente, ejecute **nvidia-smi**. Los resultados son similares 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 sean 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 tiene un nombre similar a **Xorg.{DISPLAY}.log** en la carpeta **/var/log/**.

Problemas conocidos y limitaciones

Para vGPU, la consola local de Citrix Hypervisor™ muestra la pantalla de la sesión de escritorio ICA

Solución alternativa: Deshabilite la consola VGA local de la VM ejecutando los siguientes comandos:

Para Citrix Hypervisor 8.1 y versiones posteriores:

```
[root@xenserver® ~]# xe vgpu-param-set uuid=vgpu-uuid
extra_args=disable_vnc=1
```

Para Citrix Hypervisor anterior a 8.1:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

Las tarjetas gráficas NVIDIA K2 no admiten la codificación de hardware YUV444 en modo de paso a través

Con **Build to Lossless** habilitado a través de la configuración de directiva, aparece una pantalla negra o gris cuando los usuarios inician una sesión de aplicación o escritorio con una tarjeta gráfica NVIDIA K2. El problema ocurre porque las tarjetas gráficas NVIDIA K2 no admiten la codificación de hardware YUV444 en modo de paso a través. Para obtener más información, consulte Video Encode and Decode GPU Support Matrix.

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 correctamente al cambiar el tamaño de la ventana de la aplicación Citrix Workspace

Al cambiar el tamaño de la ventana de la aplicación Citrix Workspace, la resolución de pantalla cambia. El controlador propietario de NVIDIA cambia algunos estados internos y podría 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)`'.

Visualización progresiva de Thinwire

La interactividad de la sesión puede degradarse en conexiones con ancho de banda bajo o latencia alta. Por ejemplo, en conexiones con menos de 2 Mbps de ancho de banda o una latencia superior a 200 ms, el desplazamiento en una página web puede volverse lento, sin respuesta o entrecortado. Las operaciones de teclado y ratón pueden retrasarse con respecto a las actualizaciones gráficas.

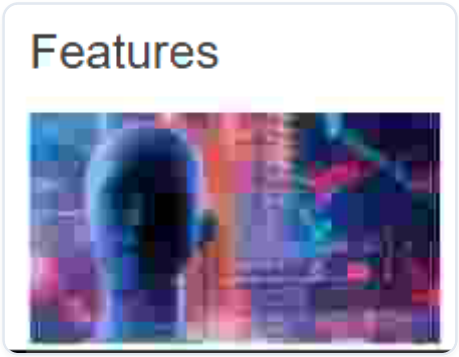
Hasta la versión 7.17, podía usar la configuración de directivas para reducir el consumo de ancho de banda configurando la sesión con una calidad visual **Baja** o estableciendo una menor profundidad de color (gráficos de 16 o 8 bits). Sin embargo, tenía que saber que un usuario estaba

en una conexión débil. HDX Thinwire no ajustaba dinámicamente la calidad de la imagen estática en función de las condiciones de la red.

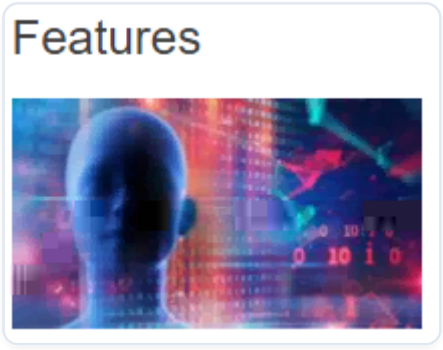
A partir de la versión 7.18, HDX Thinwire, de forma predeterminada, cambia a un modo de actualización progresiva cuando el ancho de banda disponible cae por debajo de 2 Mbps o la latencia de red supera los 200 ms. En este modo:

- Todas las imágenes estáticas están muy comprimidas.
- La calidad del texto se reduce.

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 agudizan 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 de origen.



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 se produce a lo largo de varios fotogramas. Este enfoque evita introducir un retraso con un único fotograma de enfoque grande.

Las imágenes transitorias (vídeo) todavía se gestionan con 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 directivas de **Calidad visual**: **Alta**, **Media** (predeterminada) y **Baja**.

El modo progresivo se desactiva forzosamente (no se utiliza) cuando:

- **Calidad visual** = **Siempre sin pérdidas** o **Compilación sin pérdidas**
- **Profundidad de color preferida para gráficos sencillos** = 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, se habilita de forma predeterminada 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 permanece en ese modo un mínimo de 10 s, 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 \<value\>:

0 = Siempre desactivado (no usar bajo ninguna circunstancia)

1 = Automático (alternar según las condiciones de red, valor predeterminado)

2 = Siempre activado

En el 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 \<value\> es \<threshold in 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 \<value\> es \<threshold in ms\> (predeterminado = 200)

Ejemplo: 100 = activar el modo progresivo si la latencia de red cae por debajo de 100 ms.

Gráficos 3D que no son GRID

Información general

Con esta mejora de funciones, el VDA de Linux es compatible no solo con las tarjetas 3D NVIDIA GRID, sino también con las tarjetas 3D que no son GRID.

Instalación

Para usar la función de gráficos 3D que no son GRID, debe:

- Instalar XDamage como requisito previo. Normalmente, XDamage existe como una extensión de XServer.
- Establecer `CTX_XDL_HDX_3D_PRO` en `Y` al instalar el VDA de Linux. Para obtener información sobre las variables de entorno, consulte Paso 7: Configurar el entorno de tiempo de ejecución para completar la instalación.

Configuración

Archivos de configuración de Xorg

Si el controlador de su tarjeta 3D es NVIDIA, los archivos de configuración se instalan y configuran automáticamente.

Otros tipos de tarjetas 3D

Si el controlador de su tarjeta 3D NO es NVIDIA, debe modificar los cuatro archivos de configuración de plantilla instalados en `/etc/X11/`:

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

Tomando como ejemplo **ctx-driver_name-1.conf**, 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 de la tarjeta 3D proporcionada por el fabricante para obtener información de configuración. Se puede generar un archivo de configuración nativo. verificar que su tarjeta 3D puede funcionar en un entorno local con el archivo de configuración nativo cuando no esté utilizando una sesión ICA® de Linux VDA.

   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 Linux VDA 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
   ```

Habilitar la función de gráficos 3D sin GRID

La función de gráficos 3D sin GRID está inhabilitada de forma predeterminada. Puede ejecutar el siguiente comando para habilitarla estableciendo XDamageEnabled en 1.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_DWORD" -v "XDamageEnabled" -d "0x00000001" --force
```

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 verbose para recopilar la información de seguimiento para la depuración.

La codificación de hardware no funciona

Esta función solo admite la codificación por software.

Configurar directivas

Instalación

Siga los artículos de instalación para preparar el VDA de Linux.

Dependencias

Asegúrese de instalar estas dependencias antes de instalar el paquete de VDA de Linux.

RHEL/CentOS:

```
sudo yum -y install openldap



sudo yum -y install libxml2



sudo yum -y install cyrus-sasl
```

```
sudo yum -y install cyrus-sasl-gssapi
```

SLES/SELD:

```
sudo zypper install openldap2


sudo zypper install libxml2


sudo zypper install cyrus-sasl


sudo zypper install cyrus-sasl-gssapi
```

Ubuntu:

```
sudo apt-get install -y libldap-2.4-2


sudo apt-get install -y libsasl2-2


sudo apt-get install -y libsasl2-modules-gssapi-mit
```

Configuración

Configuración de directivas en Citrix Studio

Para configurar directivas en Citrix Studio, haga lo siguiente:

1. Abra **Citrix Studio**.
2. Seleccione el panel **Directivas**.
3. Haga clic en **Crear directiva**.

4. Configure la directiva según la lista de compatibilidad de directivas.

Configuración del servidor LDAP en el VDA

La configuración del servidor LDAP en el VDA de Linux es opcional para entornos de dominio único, pero obligatoria para entornos de varios dominios y varios bosques. La configuración es necesaria para que el servicio de directivas realice una búsqueda LDAP en estos entornos.

Después de instalar el paquete de Linux VDA, ejecute el comando:

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Escriba todos los servidores LDAP en el formato sugerido: lista separada por espacios de Nombres de Dominio Completamente Cualificados (FQDN) de LDAP con el puerto LDAP (por ejemplo, ad1.mycompany.com:389 ad2.mycomany.com:389).

Imagen de la configuración del servidor LDAP en el VDA de Linux(/en-us/linux-virtual-delivery-agent/2201/media/ldap-server-setting-on-linux-vda-new.png)

También puede ejecutar el comando **ctxreg** para escribir esta configuración directamente en el registro:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ListOfLDAPServers" -d "ad1.mycompany.com:389 ad2.mycomany.com:389" --
force
```

Lista de soporte de políticas

Lista de soporte de políticas de Linux VDA

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Usar la hora local del cliente	UseLocalTimeOfClient	Usuario	ICA\Time Zone Control	Usar la zona horaria del servidor
Cálculo de ida y vuelta de ICA	IcaRoundTripCheckEnabled	Equipo	ICA\End User Monitoring	Habilitado (1)

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Intervalo de cálculo de ida y vuelta de ICA	IcaRoundTripCheckPeriod	Equipo	ICA\End User Monitoring	15
Cálculos de ida y vuelta de ICA para conexiones inactivas	IcaRoundTripCheckWhenIdle	Equipo	ICA\End User Monitoring	Deshabilitado (0)
Límite de ancho de banda general de la sesión	LimitOverallBw	Usuario	ICA\Bandwidth	0
Límite de ancho de banda de redirección de audio	LimitAudioBw	Usuario	ICA\Bandwidth	0
Porcentaje de límite de ancho de banda de redirección de audio	LimitAudioBwPercent	Usuario	ICA\Bandwidth	0
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

POLÍTICA 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
Límite de ancho de banda de redirección de archivos	LimitCdmBw	Usuario	ICA\Ancho de banda	0
Porcentaje de límite de ancho de banda de redirección de archivos	LimitCdmBwPercent	Usuario	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de impresora	LimitPrinterBw	Usuario	ICA\Ancho de banda	0
Porcentaje de límite de ancho de banda de redirección de impresora	LimitPrinterBwPercent	Usuario	ICA\Ancho de banda	0
Conexiones WebSockets	AcceptWebSocketsConnections	Equipo	ICA\WebSockets	Prohibido

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Número de puerto de WebSockets	WebSocketsPort	Equipo	ICA\WebSockets	8008
Lista de servidores de origen de confianza de WebSockets	WSTrustedOriginServerList	Equipo	ICA\WebSockets	*
Keep alives de ICA®	SendICAKeepAlives	Equipo	Keep alive de ICA	No enviar mensajes keep alive de ICA (0)
Tiempo de espera de mantenimiento de conexión de ICA	ICAKeepAliveTimeout	Equipo	Keep alive de ICA	60 segundos
Número de puerto del agente de escucha de ICA	IcaListenerPortNumber	Equipo	ICA	1494
Transporte adaptativo HDX™	HDXoverUDP	Equipo	ICA	Preferido(2)
Conexiones de fiabilidad de la sesión	AcceptSessionReliabilityConnections	Equipo	ICA\Fiabilidad de sesión	Permitido(1)
Nivel de transparencia de la interfaz de usuario de reconexión	ReconnectionUiTransparencyLevel	Equipo	ICA\Auto Client Reconnect	80%

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Número de puerto de fiabilidad de la sesión	SessionReliabilityPort	Equipo	ICA\Session Reliability	2598
Tiempo de espera de fiabilidad de la sesión	SessionReliabilityTimeout	Equipo	ICA\Session Reliability	180 s
Reconexión automática de clientes	AllowAutoClientReconnect	Usuario	ICA\Auto Client Reconnect	Permitido (1)
Redirección de audio del cliente	AllowAudioRedirection	Usuario	Audio	Permitido (1)
Redirección de impresoras 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)

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Redirección de dispositivos USB de cliente	AllowUSBRedir	Usuario	USB	Prohibido (0)
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 objetivo	TargetedMinimumFramesPerSecond	Usuario	Thinwire	10 fotogramas por segundo
Velocidad de fotogramas objetivo	FotogramasPorSegundo	Usuario	Thinwire	30 fotogramas por segundo
Calidad visual	CalidadVisual	Usuario	Thinwire	Medio (3)
Usar códec de vídeo para la compresión	CódecDeVídeo	Usuario	Thinwire	Usar cuando se prefiera (3)
Usar codificación de hardware para códec de vídeo	UsarCodificaciónPorHardwareParaCódecDeVídeo	Usuario	Thinwire	Habilitado (1)
Permitir compresión visualmente sin pérdidas	PermitirCompresiónVisualmenteSinPérdidas	Usuario	Thinwire	Deshabilitado (0)

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Optimizar para cargas de trabajo de gráficos 3D	OptimizarParaCargaDeTrabajo3D	Usuario	Thinwire	Deshabilitado (0)
Profundidad de color preferida para gráficos sencillos	ProfundidadDeColorPreferida	Usuario	Thinwire	24 bits por píxel (1)
Calidad de audio	CalidadDeSonido	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 la actualización automática de los Controllers	EnableAutoUpdateOfControllers	Equipo	Configuración del Virtual Delivery Agent	Permitido (1)
Modo de actualización de la selección del portapapeles	ClipboardSelectionUpdateMode	Usuario	Portapapeles	3

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Modo de actualización de la selección principal	PrimarySelectionUpdateMode	Usuario	Portapapeles	3
Calidad máxima de Speex	MaxSpeexQuality	Usuario	Audio	5
Conectar automáticamente las unidades cliente	AutoConnectDrives	Usuario	Redirección de archivos/CDM	Habilitado (1)
Unidades ópticas del 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)
Redirección de unidades cliente	Permitir redirección de unidades	Usuario	Redirección de archivos/CDM	Permitido (1)
Acceso de solo lectura a las unidades del cliente	Unidad asignada de solo lectura	Usuario	Redirección de archivos/CDM	Deshabilitado (0)

POLÍTICA DE STUDIO	NOMBRE DE CLAVE	TIPO	MÓDULO	VALOR PREDETERMINADO
Visualización automática del teclado	Permitir aparición automática del teclado	Usuario	MRVC	Deshabilitado (0)
Permitir la transferencia de archivos entre el escritorio y el cliente	Permitir transferencia de archivos	Usuario	Transferencia de archivos	Permitido
Descargar archivo del escritorio	Permitir descarga de archivos	Usuario	Transferencia de archivos	Permitido
Cargar archivo al escritorio	Permitir carga de archivos	Usuario	Transferencia de archivos	Permitido
Temporizador de inactividad de sesión	Habilitar temporizador de inactividad de sesión	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	Inhabilitado (0)
Intervalo del temporizador de sesión desconectada	SessionDisconnectTimerPeriod	Usuario	Temporizadores de sesión	1440 minutos

Nota:

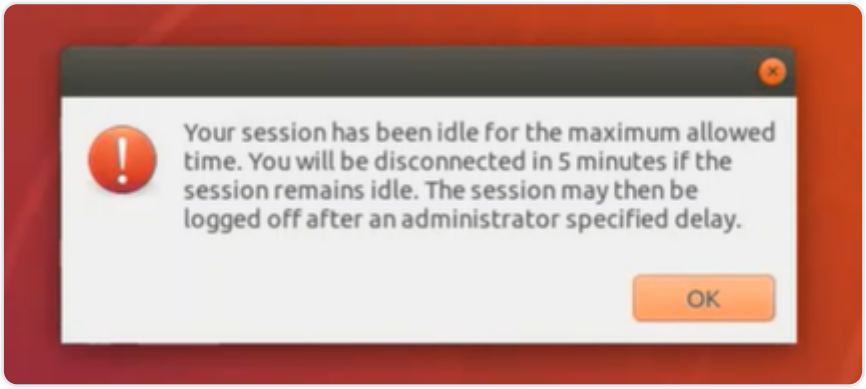
Solo el Virtual Delivery Agent (VDA) de Windows admite audio a través del Protocolo de datagramas de usuario (UDP). El VDA de Linux no lo admite. Para obtener más información, consulte Audio a través del transporte en tiempo real del Protocolo de datagramas de usuario (UDP).

Puede usar las siguientes configuraciones de directiva de Citrix para configurar los temporizadores de conexión de sesión en Citrix Studio:

- **Temporizador de inactividad de la sesión**: Determina si se debe aplicar un límite de tiempo para las sesiones inactivas.
- **Intervalo del temporizador de inactividad de la sesión**: Establece un límite de tiempo para las sesiones inactivas. Si el temporizador de inactividad de la sesión está **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 para las sesiones desconectadas.
- **Intervalo del temporizador de sesión desconectada**: Establece un intervalo antes de que se cierre la sesión de una 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 caduca 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 velocidades de bits en diferentes modos. La mejor calidad de Speex es cuando el valor más grande cumple las siguientes condiciones:

  - Es igual o inferior a la calidad máxima de Speex.
  - Su velocidad 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

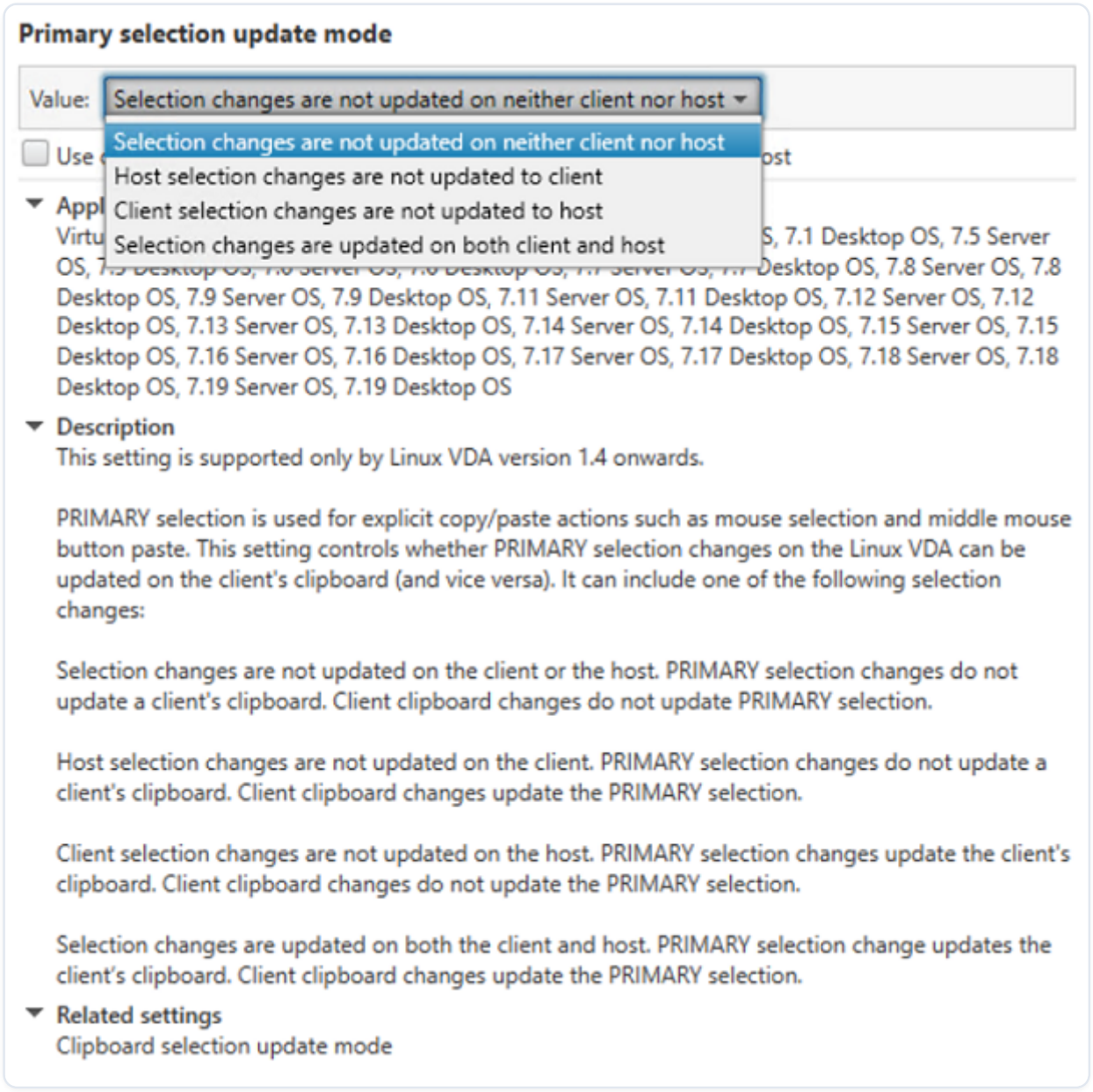
  Valor (enumeración):

  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 en el cliente. Los cambios de selección principal 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 de selección principal en el VDA de Linux no actualizan el portapapeles en el cliente. Los cambios de selección principal 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 de selección principal en el VDA de Linux actualizan el portapapeles en el cliente. Los cambios de selección principal 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 de selección principal en el VDA de Linux actualizan el portapapeles en el cliente. Los cambios de selección principal 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 del portapapeles

- ClipboardSelectionUpdateMode

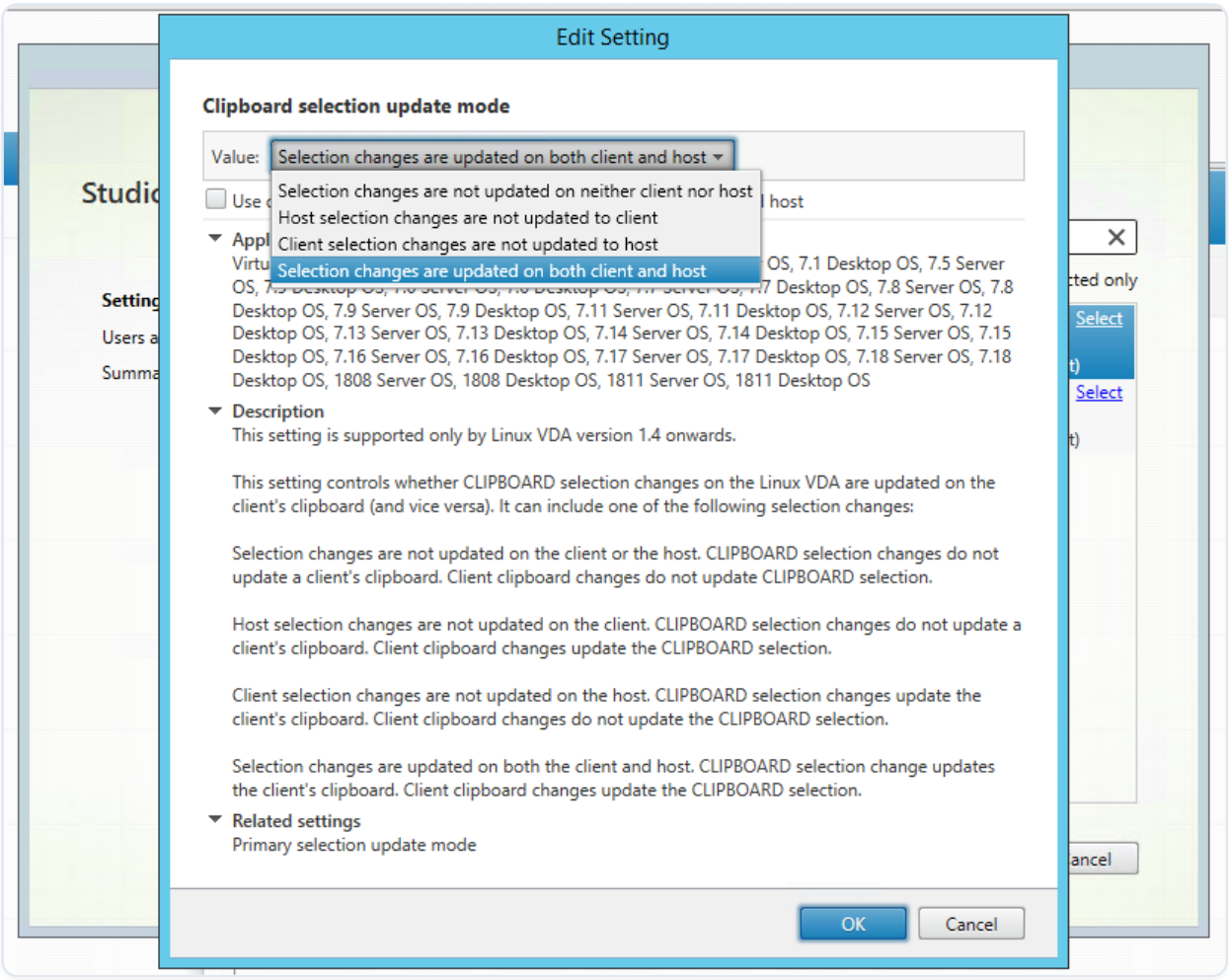
Valor (enumeración):

Valor predeterminado: 3

Detalles:

La selección del portapapeles se utiliza cuando se seleccionan algunos datos y se solicita explícitamente que se “copien” al portapapeles, como al seleccionar “Copiar” en el menú contextual. La selección del portapapeles se utiliza principalmente en relación con las operaciones del portapapeles de Microsoft Windows, mientras que la selección principal es exclusiva de Linux.

Esta directiva controla si los cambios de selección del portapapeles 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 del portapapeles en el VDA de Linux no actualizan el portapapeles en el cliente. Los cambios de 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 de selección del portapapeles en el VDA de Linux no actualizan el portapapeles en el cliente. Los cambios de 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 de selección del portapapeles en el VDA de Linux actualizan el portapapeles en el cliente. Los cambios de 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 de selección del portapapeles en el VDA de Linux actualizan el portapapeles en el cliente. Los cambios de 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.

Configurar IPv6

El VDA de Linux admite IPv6 para alinearse con Citrix Virtual Apps and Desktops. Al usar esta función, tenga en cuenta lo siguiente:

- En entornos de pila dual, se usa 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 admite 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, **ControllerRegistrationIPv6Netmask** se puede usar para especificar cuál se usa 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.

Configurar el Programa de mejora de la experiencia del cliente (CEIP) de Citrix

Cuando participa en el CEIP, se envían estadísticas anónimas e información de uso a Citrix para ayudar a mejorar la calidad y el rendimiento de los productos de Citrix. Además, se envía una copia de los datos anónimos a Google Analytics (GA) para un análisis rápido y eficiente.

Configuración del Registro

De forma predeterminada, participa automáticamente en el CEIP al instalar el VDA de Linux. La primera carga de datos se produce aproximadamente siete días después de instalar el VDA de Linux. Puede cambiar esta configuración predeterminada en el Registro.

- **CEIPSwitch**

Configuración del Registro que habilita o inhabilita el CEIP (predeterminado = 0):

Ubicación: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Nombre: CEIPSwitch

Valor: 1 = inhabilitado, 0 = habilitado

Cuando no se especifica, el CEIP está habilitado.

Puede ejecutar el siguiente comando en un cliente para inhabilitar el CEIP:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

- **GASwitch**

Configuración del Registro que habilita o inhabilita GA (predeterminado = 0):

Ubicación: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Nombre: GASwitch

Valor: 1 = deshabilitado, 0 = habilitado

Cuando no se especifica, GA está habilitado.

Puede ejecutar el siguiente comando en un cliente para deshabilitar GA:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "GASwitch" -d "1"
```

- **DataPersistPath**

Configuración del Registro que controla la ruta de persistencia de datos (predeterminada = /var/xdl/ceip):

Ubicación: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Nombre: DataPersistPath

Valor: Cadena

Puede ejecutar el siguiente comando para establecer esta ruta:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "DataPersistPath" -d
"your_path"
```

Si la ruta configurada no existe o no se puede acceder a ella, los datos se guardan en la ruta predeterminada.

Datos de CEIP recopilados del VDA de Linux

La siguiente tabla muestra un ejemplo de los tipos de información anónima recopilada. Los datos no contienen ningún detalle que lo identifique como cliente.

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
GUID de la máquina	machine_guid	Identificación de la máquina de origen de los datos
Solución de AD	ad_solution	Cadena de texto que indica el método de unión al dominio de la máquina
Versión del kernel de Linux	kernel_version	Cadena de texto que indica la versión del kernel de la máquina
Versión de LVDA	vda_version	Cadena de texto que indica la versión instalada del VDA de Linux.
Actualización o instalación nueva de LVDA	update_or_fresh_install	Cadena de texto que indica si el paquete actual del VDA de Linux se está instalando de nuevo o actualizando

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
Método de instalación de LVDA	install_method	Cadena de texto que indica que el paquete actual de Linux VDA está instalado mediante MCS, PVS, instalación sencilla o instalación manual.
HDX 3D Pro habilitado o no	hdx_3d_pro	Cadena de texto que indica si HDX 3D Pro está habilitado en la máquina
Modo VDI habilitado o no	vdi_mode	Cadena de texto que indica si el modo VDI está habilitado
Configuración regional	system_locale	Cadena de texto que indica la configuración regional de esta máquina
Última hora de reinicio de los servicios clave de LVDA	ctxhdx y ctxvda	La última hora de reinicio de los servicios `ctxhdx` y `ctxvda`, en el formato dd-hh:mm:ss, por ejemplo, 10-17:22:19
Tipo de GPU	gpu_type	Indica el tipo de GPU de la máquina
Núcleos de CPU	cpu_cores	Número entero que indica el número de núcleos de CPU de la máquina
Frecuencia de CPU	cpu_frequency	Número flotante que indica la frecuencia de la CPU en MHz
Tamaño de la memoria física	memory_size	Número entero que indica el tamaño de la memoria física en KB
Número de sesiones iniciadas	session_launch	Número entero que indica la cantidad de sesiones iniciadas (conectadas o reconectadas) en la máquina

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
		en el momento en que recopilamos este punto de datos
Nombre y versión del SO Linux	os_name_version	Cadena de texto que indica el nombre y la versión del sistema operativo Linux de la máquina
Clave de sesión	session_key	Identifica la sesión de donde provienen los datos
Tipo de recurso	resource_type	Cadena de texto que indica el tipo de recurso de la sesión iniciada: escritorio o `<appname>`
Tiempo de sesión activa	active_session_time	Se utiliza para guardar los tiempos activos de la sesión. Una sesión puede tener varios tiempos activos porque la sesión puede desconectar/reconnectarse
Tiempo de duración de la sesión	session_duration_time	Se utiliza para guardar la duración de la sesión desde el inicio de sesión hasta el cierre de sesión
Tipo de cliente de Receiver	receiver_type	Entero que indica el tipo de aplicación Citrix Workspace utilizada para iniciar la sesión
Versión del cliente de Receiver	receiver_version	Cadena de texto que indica la versión de la aplicación Citrix Workspace utilizada para iniciar la sesión
Recuento de impresiones	printing_count	Entero que indica el número de veces que la sesión utiliza la función de impresión

PUNTO DE DATOS	NOMBRE DE CLAVE	DESCRIPCIÓN
Recuento de redirecciones USB	usb_redirecting_count	Entero que indica el número de veces que la sesión utiliza un dispositivo USB
Tipo de proveedor de gráficos	gfx_provider_type	Cadena de texto que indica el tipo de proveedor de gráficos de la sesión
Recuento de shadowing	shadow_count	Número entero que indica el número de veces que la sesión ha sido supervisada
Idioma seleccionado por el usuario	ctxism_select	Cadena larga compuesta que contiene todos los idiomas que los usuarios han seleccionado
Recuento de redirección de tarjeta inteligente	scard_redirecting_count	Número entero que indica el número de veces que se utiliza la redirección de tarjeta inteligente para inicios de sesión y autenticación de usuario para aplicaciones en sesión

Configurar la redirección 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.

> **Sugerencia:**

> Recomendamos usar la redirección USB cuando la latencia de red sea inferior a 100 milisegundos. No use la redirección USB cuando la latencia de red sea superior a 200 milisegundos.

> La redirección USB incluye tres áreas principales de funcionalidad:

- Implementación de proyecto de código abierto (VHCI)
- Servicio VHCI
- Servicio USB

VHCI de código abierto:

Esta parte de la función de redirección USB desarrolla un sistema general de uso compartido de dispositivos USB a través de una red IP. Consiste en 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. En la implementación de Linux VDA, Citrix reutiliza el controlador de kernel de VHCI. Sin embargo, todas las transferencias de datos USB entre Linux VDA y la aplicación Citrix Workspace están encapsuladas en el paquete de protocolo Citrix ICA®.

Servicio VHCI:

El servicio VHCI es un servicio de código abierto proporcionado por Citrix para comunicarse con el módulo del kernel VHCI. Este servicio funciona como una puerta de enlace entre VHCI y el servicio USB de Citrix.

Servicio USB:

El servicio USB actúa como un módulo de Citrix que gestiona toda la virtualización y las transferencias de datos en el dispositivo USB.

Cómo funciona la redirección USB

Normalmente, si un dispositivo USB se redirige correctamente al Linux VDA, se crean uno o más nodos de dispositivo en la ruta /dev del sistema. Sin embargo, a veces el dispositivo redirigido no se puede usar 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 controladores, los dispositivos USB redirigidos son inaccesibles para la sesión activa de Linux VDA. Para garantizar la conectividad del dispositivo USB, instale los controladores y configure el sistema correctamente.

El VDA de Linux admite una lista de dispositivos USB que se redirigen correctamente hacia y desde el cliente.

Dispositivos USB compatibles

Se ha comprobado que los siguientes dispositivos son compatibles con esta versión del VDA de Linux. Otros dispositivos se pueden usar libremente, con resultados inesperados:

Nota:

El VDA de Linux solo admite protocolos USB 2.0.

DISPOSITIVO DE ALMACENAMIENTO MASIVO USB	VID:PID	SISTEMA DE ARCHIVOS
`Netac Technology Co., Ltd`	0dd8:173c	FAT32
`Kingston Datatraveler 101 II`	0951:1625	FAT32
`Kingston Datatraveler GT101 G2`	1567:8902	FAT32
`SanDisk SDCZ80 flash drive`	0781:5580	FAT32
`WD HDD`	1058:10B8	FAT32

RATÓN USB 3D	VID:PID
`3DConnexion SpaceMouse Pro`	046d: c62b

ESCÁNER USB	VID:PID
`Epson Perfection V330 photo`	04B8: 0142

Configurar la redirección 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 USB para el VDA de Linux, configure la siguiente política y reglas:

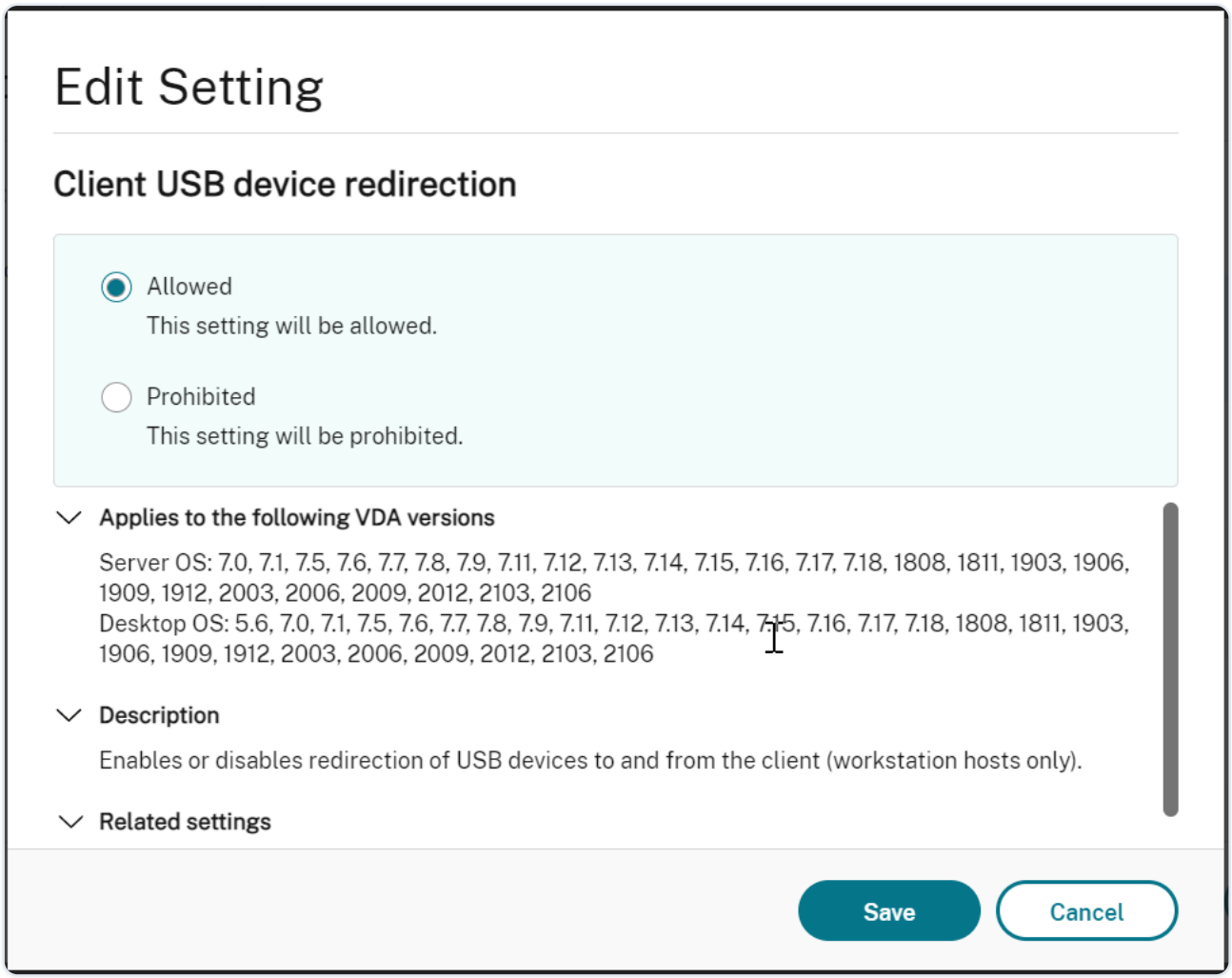
- Política de redirección de dispositivos USB de cliente
- Reglas de redirección de dispositivos USB de cliente

Habilitar la redirección USB

En Citrix Studio, habilite (o deshabilite) la redirección de dispositivos USB hacia y desde el cliente (solo para hosts de estación de trabajo).

En el cuadro de diálogo **Modificar configuración**:

1. Seleccione **Permitido**.
2. Haga clic en **Aceptar**.



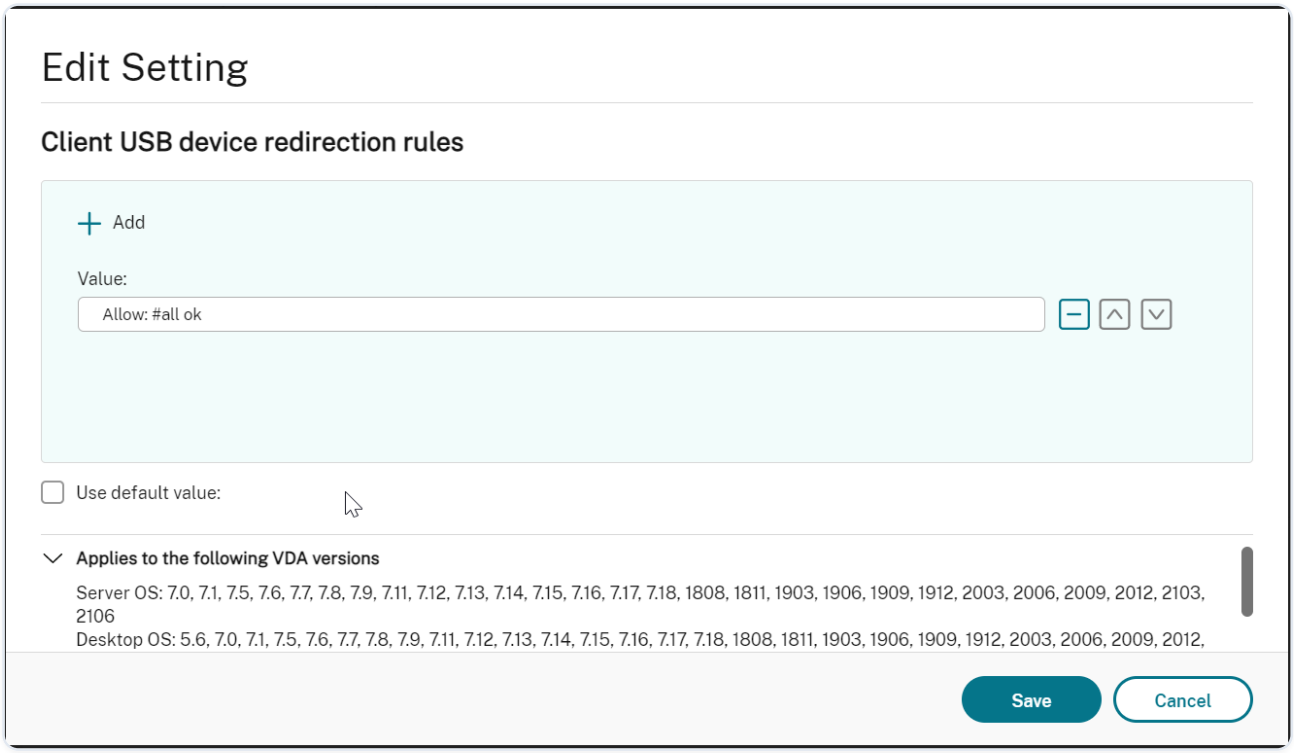
Establecer reglas de redirección USB

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 Linux VDA.

En el cuadro de diálogo Reglas de redirección de dispositivos USB de cliente:

1. Haga clic en **Nuevo** para agregar una regla de redirección, o haga clic en **Modificar** para revisar una regla existente.

2. Después de crear (o modificar) una regla, haga clic en **Aceptar**.



Crear el módulo del kernel VHCI

La redirección USB depende de los módulos del kernel VHCI (`usb-vhci-hcd.ko` y `usb-vhci-iocif.ko`). Estos módulos forman parte de la distribución de Linux VDA (como parte del paquete RPM). Se compilan basándose en los kernels oficiales de la distribución de Linux y se indican en la siguiente tabla:

DISTRIBUCIÓN DE LINUX COMPATIBLE	VERSIÓN DEL KERNEL
RHEL 8.3	4.18.0-240
RHEL 8.2	4.18.0-240
RHEL 8.1	4.18.0-240
RHEL 7.9, CentOS 7.9	3.10.0-1160
RHEL 7.8, CentOS 7.8	3.10.0-1160
SUSE 12.5	4.12.14
Ubuntu 20.04	5.4.0-81
Ubuntu 18.04	4.15.0-154

DISTRIBUCIÓN DE LINUX COMPATIBLE	VERSIÓN DEL KERNEL
Ubuntu 16.04	4.4.0-210
Debian 10	4.19.0-17

Importante:

Si el kernel de su máquina no es compatible con el controlador creado para Linux VDA, es posible que el servicio USB no se inicie. En este caso, solo puede usar la función de redirección USB si crea sus propios módulos del kernel VHCI.

verificar si su kernel es coherente con los módulos creados por Citrix

En la línea de comandos, ejecute el siguiente comando para verificar si el kernel es coherente:

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
```

Si el comando se ejecuta correctamente, el módulo del kernel se ha cargado correctamente y la versión es coherente con la instalada por Citrix.

Si el comando se ejecuta con errores, el kernel es incoherente con el módulo de Citrix y debe reconstruirse.

Reconstruir el módulo del kernel VHCI

Si el módulo del kernel no es coherente con la versión de Citrix, haga lo siguiente:

1. Descargue el código fuente de LVDA del sitio de descargas de Citrix. Seleccione el archivo en la sección "**Linux Virtual Delivery Agent (sources)**".
2. Extraiga el archivo **citrix-linux-vda-sources.zip**. Vaya a **linux-vda-sources/vhci-hcd-1.15.zip** y extraiga los archivos fuente de VHCI mediante el comando `unzip vhci-hcd-1.15.zip`.
3. Asegúrese de tener instalado el paquete de Linux VDA y, a continuación, ejecute uno de los siguientes comandos:
   - `sudo bash ctxusbcfg.sh dkms`

Este comando le permite usar el programa Dynamic Kernel Module Support (DKMS) para administrar sus módulos del kernel VHCI. DKMS no está disponible para SUSE.

> **Nota:**
>
> El comando `sudo bash ctxusbcfg.sh dkms` instala los programas `kernel-devel` y `DKMS` en su VDA. Al instalar los programas en RHEL y CentOS, el comando instala y habilita el repositorio Extra Packages for Enterprise Linux (EPEL) en su VDA.
>
> DKMS podría fallar al compilar los módulos del kernel VHCI (`usb-vhci-hcd.ko` y `usb-vhci-iocif.ko`) cuando realice una actualización importante del kernel, por ejemplo, de la versión 4.x.y a la versión 5.x.y. Si DKMS falla, ejecute `sudo bash ctxusbcfg.sh dkms` de nuevo.

- `sudo bash ctxusbcfg.sh build`

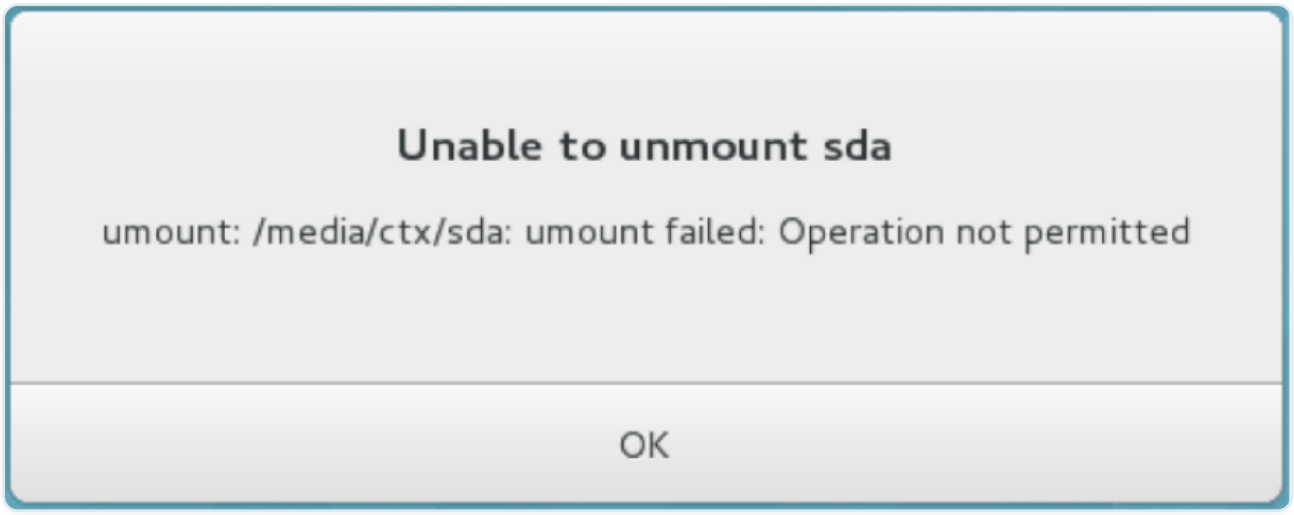
  Este comando compila e instala los módulos del kernel VHCI sin la opción DKMS.

Solucionar problemas de redirección USB

Utilice la información de esta sección para solucionar varios problemas que pueden surgir al usar el VDA de Linux.

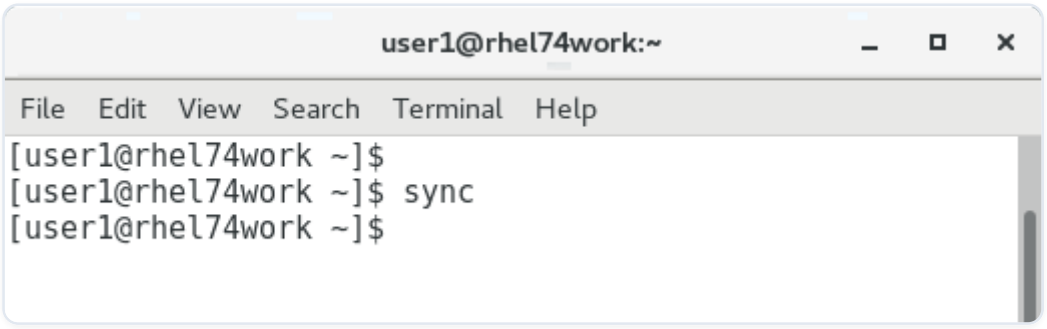
No se puede desmontar el disco USB redirigido

El VDA de Linux administra todos los discos USB redirigidos desde la aplicación Citrix Workspace con privilegios administrativos para garantizar que solo el propietario pueda acceder al dispositivo redirigido. Como resultado, solo puede desmontar el dispositivo con privilegios administrativos.



Archivo perdido al dejar de redirigir un disco USB

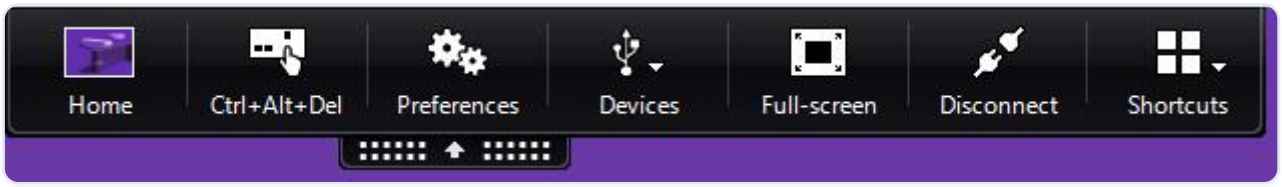
Si deja de redirigir un disco USB inmediatamente usando la barra de herramientas de la aplicación Citrix Workspace, los archivos que modificó o creó en el disco pueden perderse. Este problema ocurre porque cuando se escriben datos en un sistema de archivos, el sistema monta la caché de memoria en el sistema de archivos. Los datos no se escriben en el disco en sí. 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 vea dispositivos en la barra de herramientas de la aplicación Citrix Workspace, lo que indica que no se está produciendo ninguna redirección USB. Si se encuentra con este problema, verificar lo siguiente:

- La directiva está configurada para permitir la redirección USB
- El módulo del kernel es compatible con su kernel



Nota:

La ficha **Dispositivos** no está disponible en la aplicación Citrix Workspace para Linux.

Redirección fallida cuando los dispositivos USB se ven en la barra de herramientas de la aplicación Citrix Workspace, pero están etiquetados como *restringidos por directiva*

Cuando ocurra 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 este ajuste no deniega el acceso al dispositivo:

  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 usar el dispositivo correctamente. Si encuentra un dispositivo conectado (enchufado) pero inaccesible, añádalo a una política sin restricciones.

Nota:

Para las unidades USB, el Linux VDA configura y monta el disco. El usuario (y solo el propietario que lo instaló) puede acceder al disco sin ninguna configuración adicional. Este podría no ser el caso de los dispositivos que no están en la lista de dispositivos compatibles.

Audio adaptable

El audio adaptable está habilitado de forma predeterminada. Es compatible con los siguientes clientes de la aplicación Citrix Workspace™:

- Aplicación Citrix Workspace para Windows – 2109 y versiones posteriores
- Aplicación Citrix Workspace para Linux – 2109 y versiones posteriores
- Aplicación Citrix Workspace para Mac – 2109 y versiones posteriores

El audio adaptable recurre al audio heredado cuando se utiliza un cliente que no está en la lista.

Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en el VDA. El audio adaptable ajusta dinámicamente las velocidades de bits de muestreo de audio en función de las condiciones de la red para proporcionar una experiencia de audio de primera calidad.

La siguiente tabla muestra una comparación entre el audio adaptable y el audio heredado:

AUDIO ADAPTABLE	AUDIO HEREDADO
Velocidad de muestreo de audio máx.: 48 kHz	Velocidad de muestreo de audio máx.: 8 kHz
Canal estéreo	Canal mono

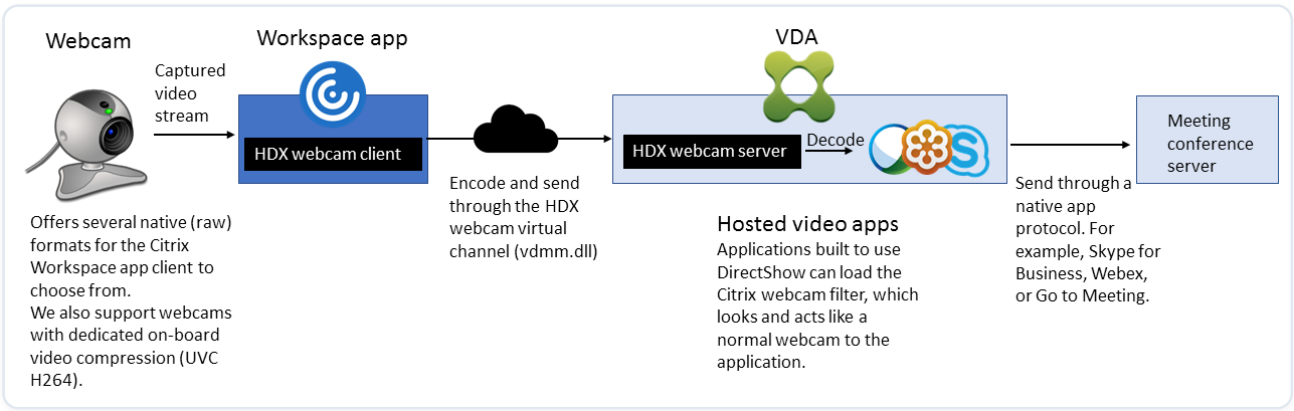
Compresión de vídeo de cámara web HDX™

Información general

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 cámara web HDX. Esta función está habilitada de forma predeterminada. Recomendamos utilizar siempre la compresión de vídeo de cámara web HDX si es posible.

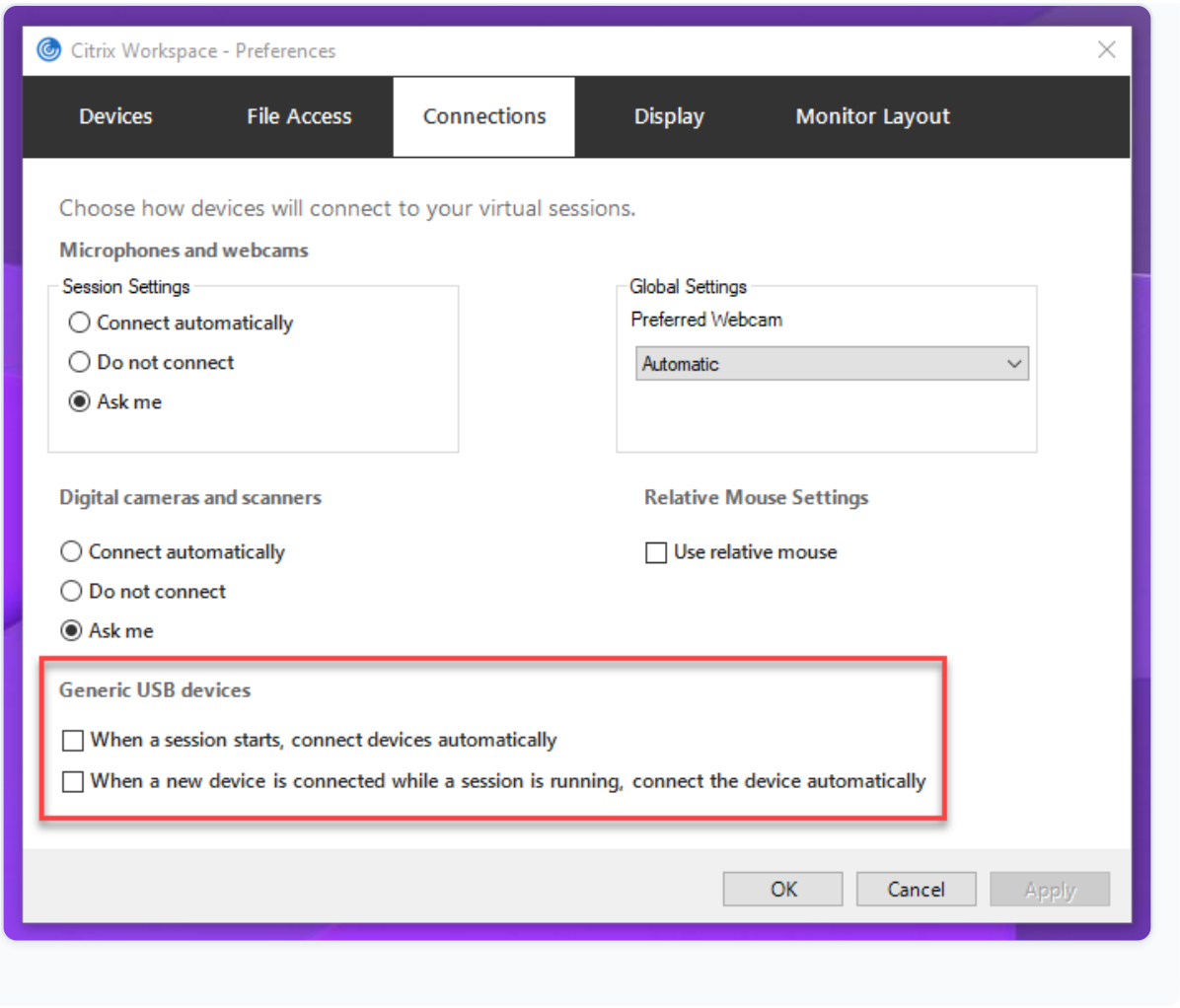
La compresión de vídeo de cámara web HDX también se denomina modo de cámara web **optimizado**. Este tipo de compresión de vídeo de cámara web envía el vídeo H.264 directamente a la aplicación de videoconferencia que se ejecuta en la sesión virtual. La compresión de vídeo de cámara web HDX utiliza la 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 streaming 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 ofrece la misma experiencia en su escritorio. La aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mejor resistencia en escenarios WAN.



Nota:

- Esta 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.



Distribuciones de Linux compatibles

- RHEL 8.4
- RHEL 8.3
- RHEL 7.9/CentOS 7.9
- Ubuntu 20.04
- Ubuntu 18.04
- Ubuntu 16.04
- Debian 10
- SUSE 15.3
- SUSE 15.2
- SUSE 12.5

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 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 las funciones:

- Logitech HD Webcam C270
- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

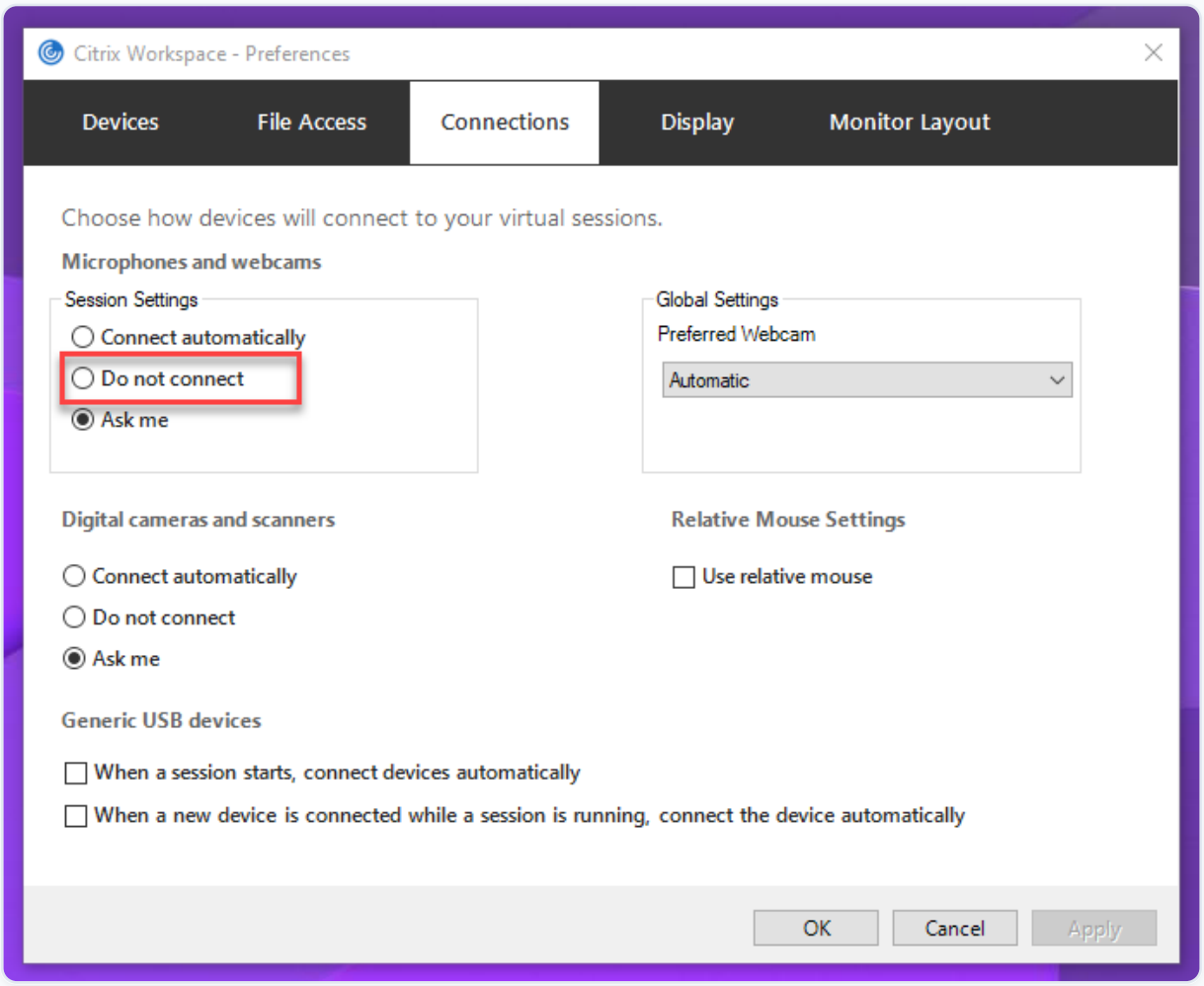
Configuración

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 la opción **Micrófonos y cámaras web** del Visor de escritorio, **No**

conectar.



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 con 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.

   Si su VDA está implementado en Debian 10, asegúrese de que se esté ejecutando en la última versión del kernel. De lo contrario, ejecute los siguientes comandos para actualizar a la última versión del kernel:

   ```
   sudo apt-get update

   sudo apt-get dist-upgrade
   ```

```
sudo reboot
```

Si su VDA está implementado en SUSE 15.3, SUSE 15.2 o SUSE 12.5, ejecute los siguientes comandos para actualizar a la última versión del kernel y 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 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 fuente abierto `v4l2loopback` de `<https://github.com/umlaeute/v4l2loopback>` y utilice DKMS para administrar `v4l2loopback`.

   `v4l2loopback` es un módulo de kernel que le permite crear dispositivos de bucle invertido V4L2.

c. Ejecute el comando `sudo service ctxwcamsd restart`. 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, cree el módulo de kernel v4l2loopback en otra máquina y luego cópielo a su VDA.

    a. Prepare una máquina de compilación que tenga acceso a Internet y la misma versión de kernel que su VDA. El comando `uname -r` ayuda a encontrar las versiones del kernel.

    b. En la máquina de compilación, ejecute el comando `sudo mkdir -p /var/xdl`.

    c. Copie `/var/xdl/configure_*` de su VDA a la máquina de compilación en `/var/xdl/`.

    d. En la máquina de compilación, 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 de compilación a su VDA y colóquelo en `/opt/Citrix/VDA/lib64/`.

    f. En su VDA, ejecute el comando `sudo service ctxwcamsd restart` para reiniciar el servicio de la cámara web y cargar el módulo del kernel v4l2loopback.

Uso compartido de pantalla de HDX™

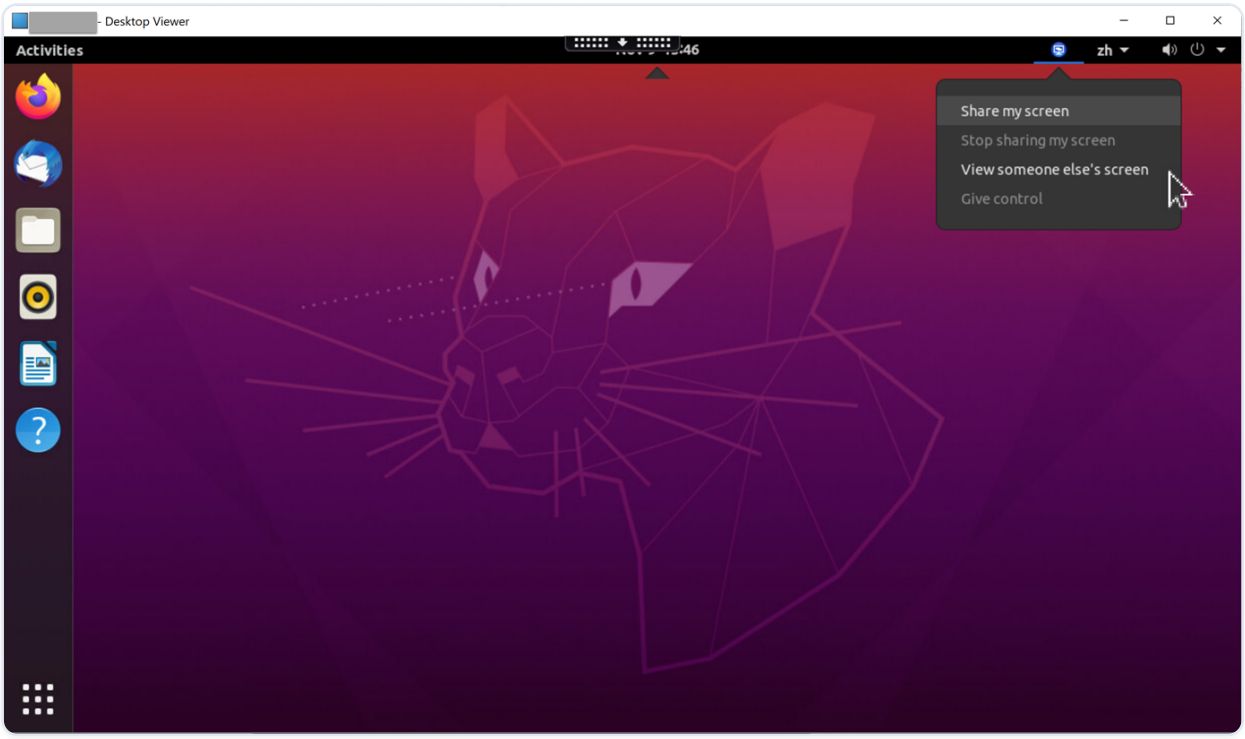
Información general

El VDA de Linux le permite compartir la pantalla de su escritorio virtual con usuarios de sesión en otros escritorios virtuales.

El siguiente ejemplo le guía a través del procedimiento para compartir una pantalla y ver la pantalla de otra persona.

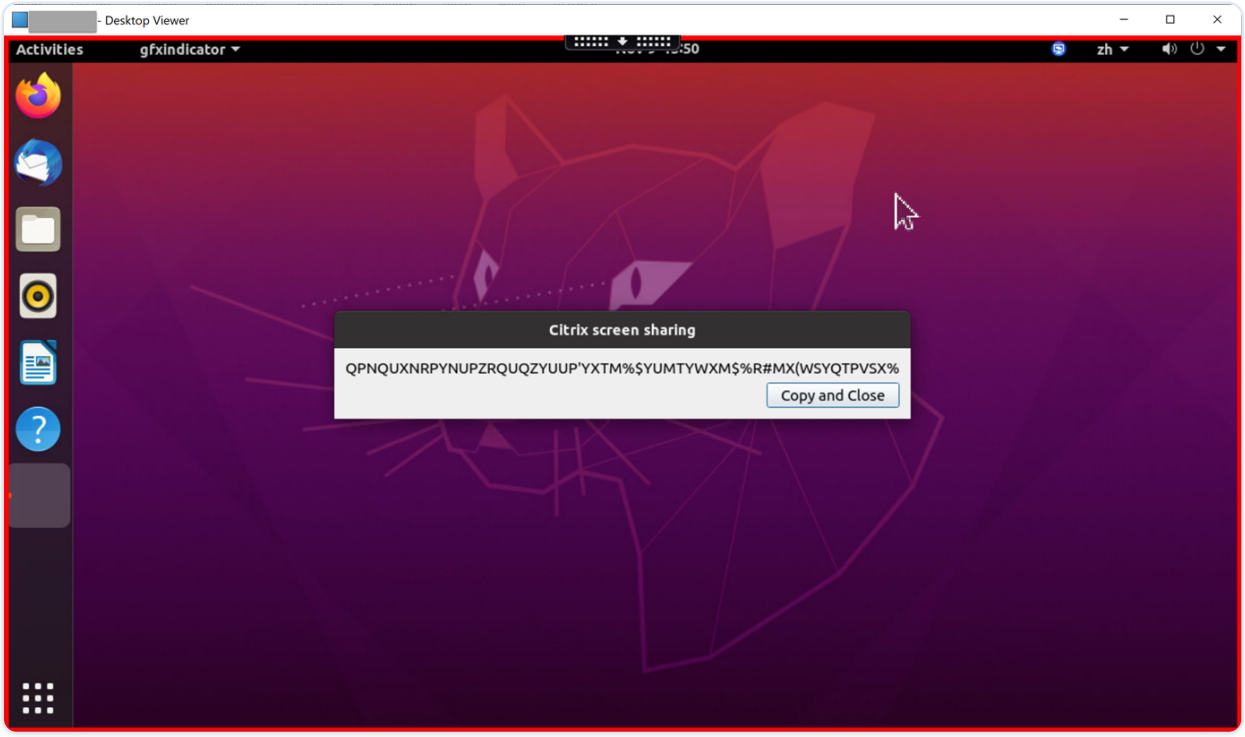
Para compartir una pantalla:

1. En el área de notificación de su escritorio virtual, haga clic en el icono de uso compartido de pantalla y seleccione **Compartir mi pantalla**.



2. Haga clic en **Copiar y cerrar**.

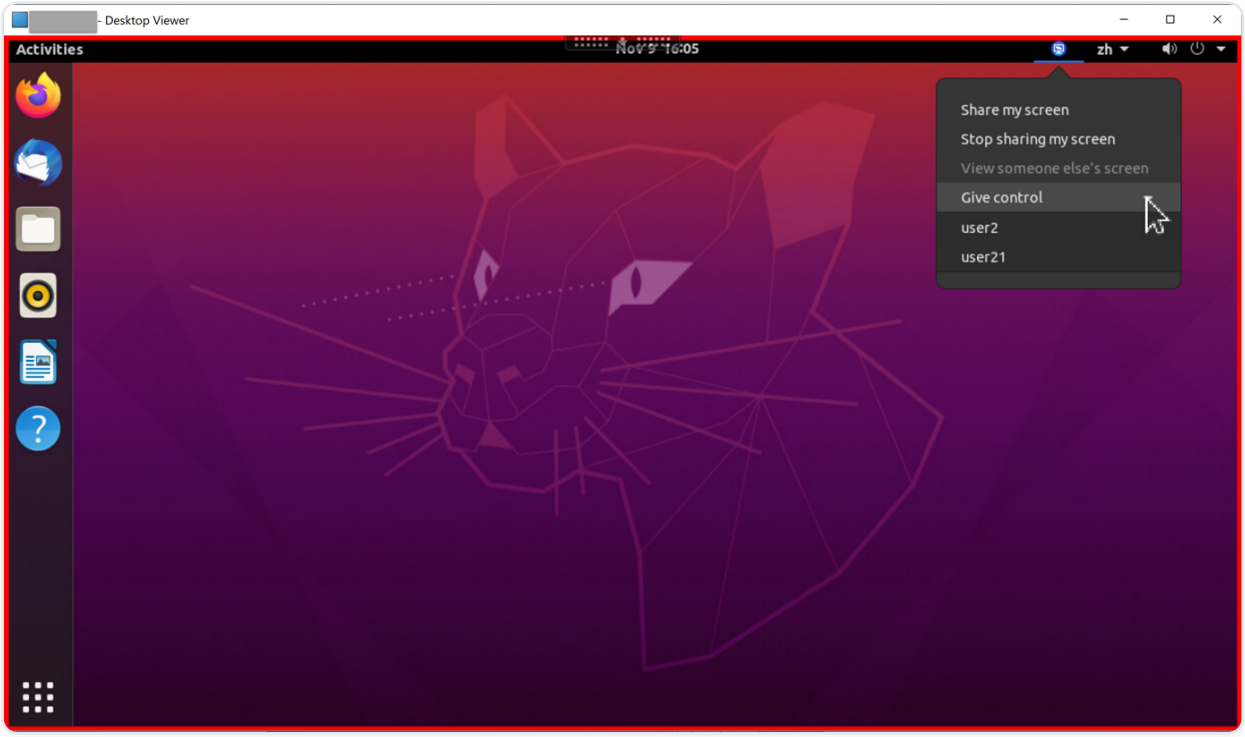
   El código actual para compartir pantalla persiste hasta que detenga y reinicie el uso compartido de su pantalla.



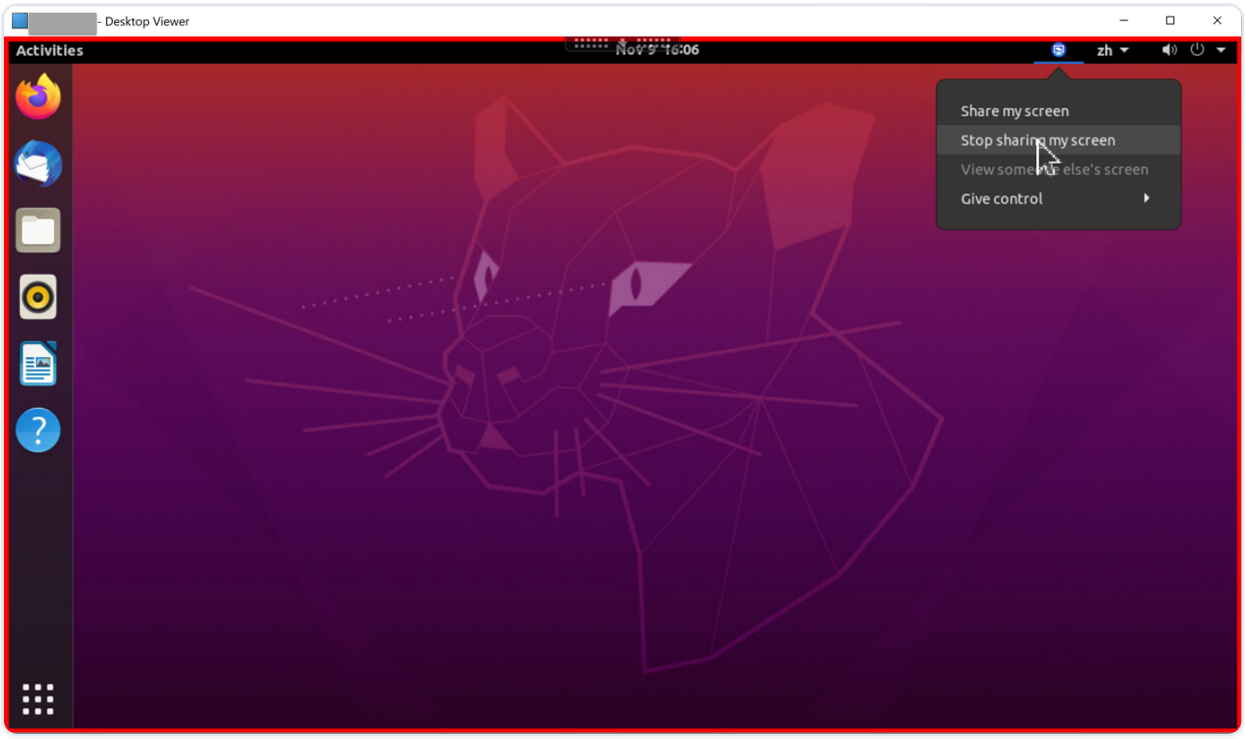
> **Sugerencia:**

> Mientras comparte su pantalla, aparece un borde rojo alrededor de ella, lo que indica que el uso compartido está en curso.

3. Comparta el código copiado con los usuarios de sesión en otros escritorios virtuales con los que desee compartir su pantalla.
4. Para permitir que un espectador controle su pantalla, seleccione **Dar control** y, a continuación, el nombre del espectador. Para dejar de dar el control, desactive el nombre del espectador.

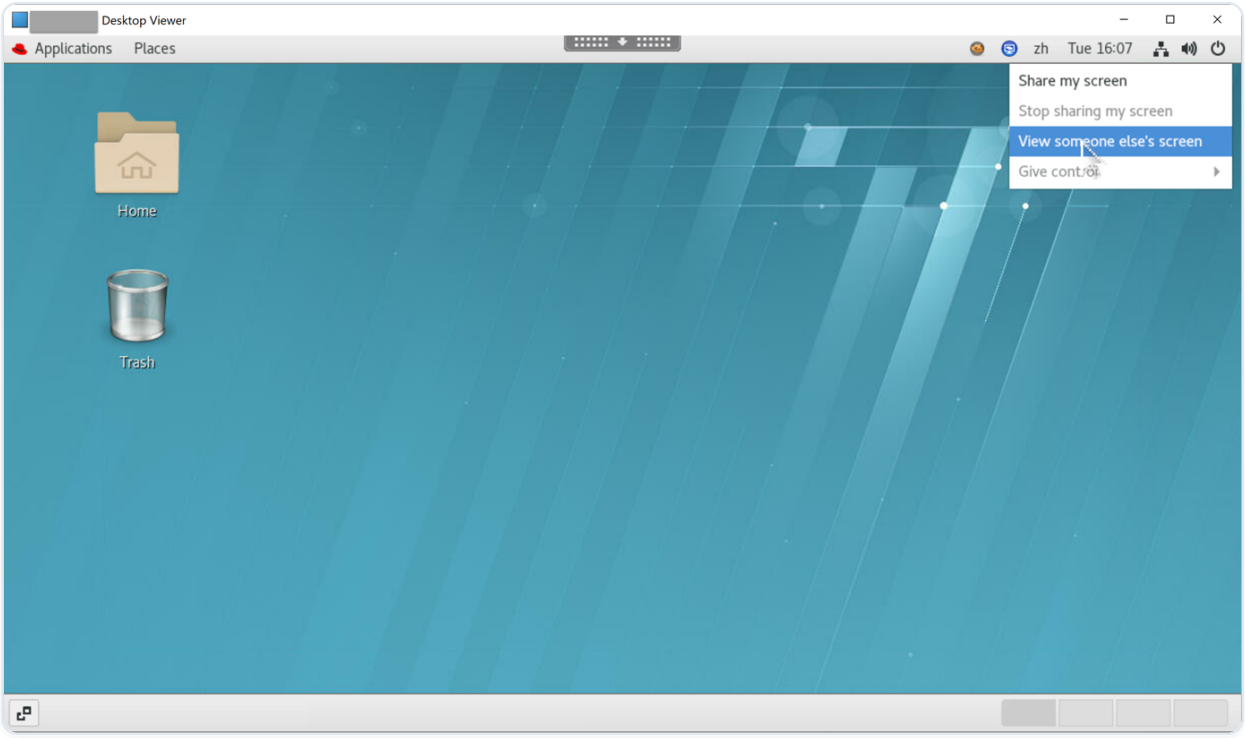


5. Para dejar de compartir su pantalla, seleccione **Dejar de compartir mi pantalla**.

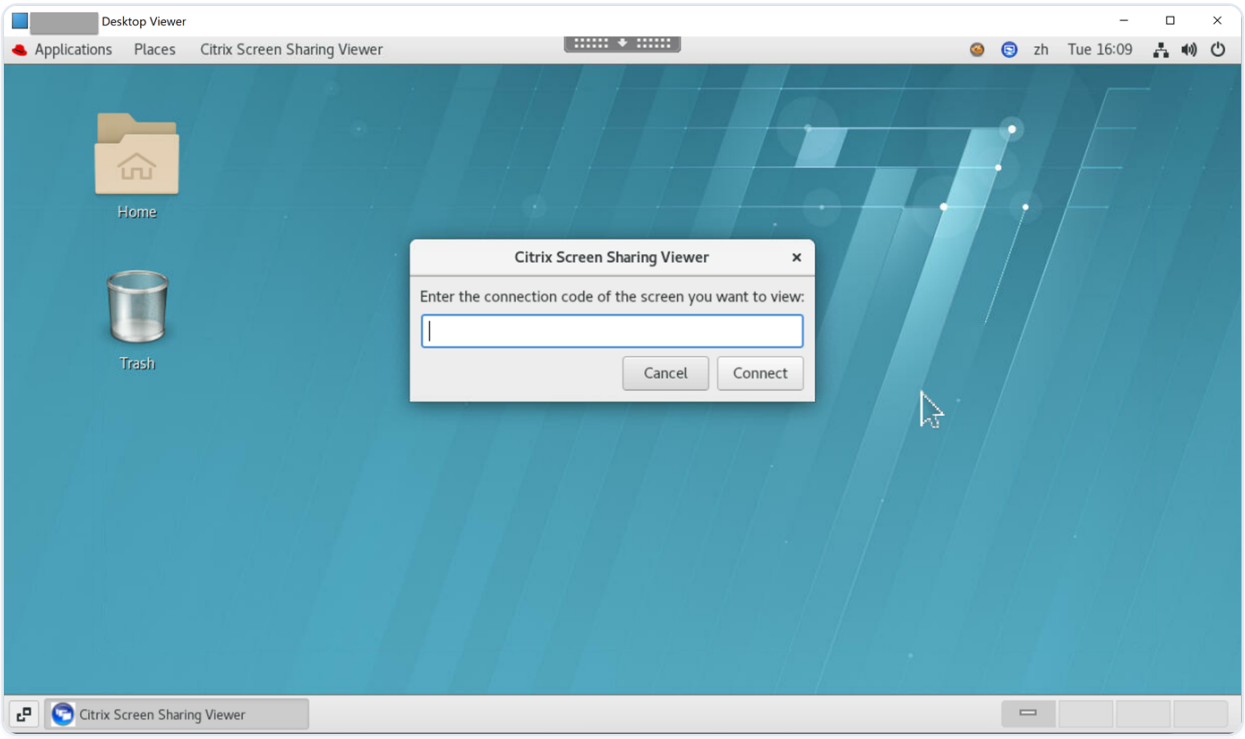


Para ver la pantalla de otra persona:

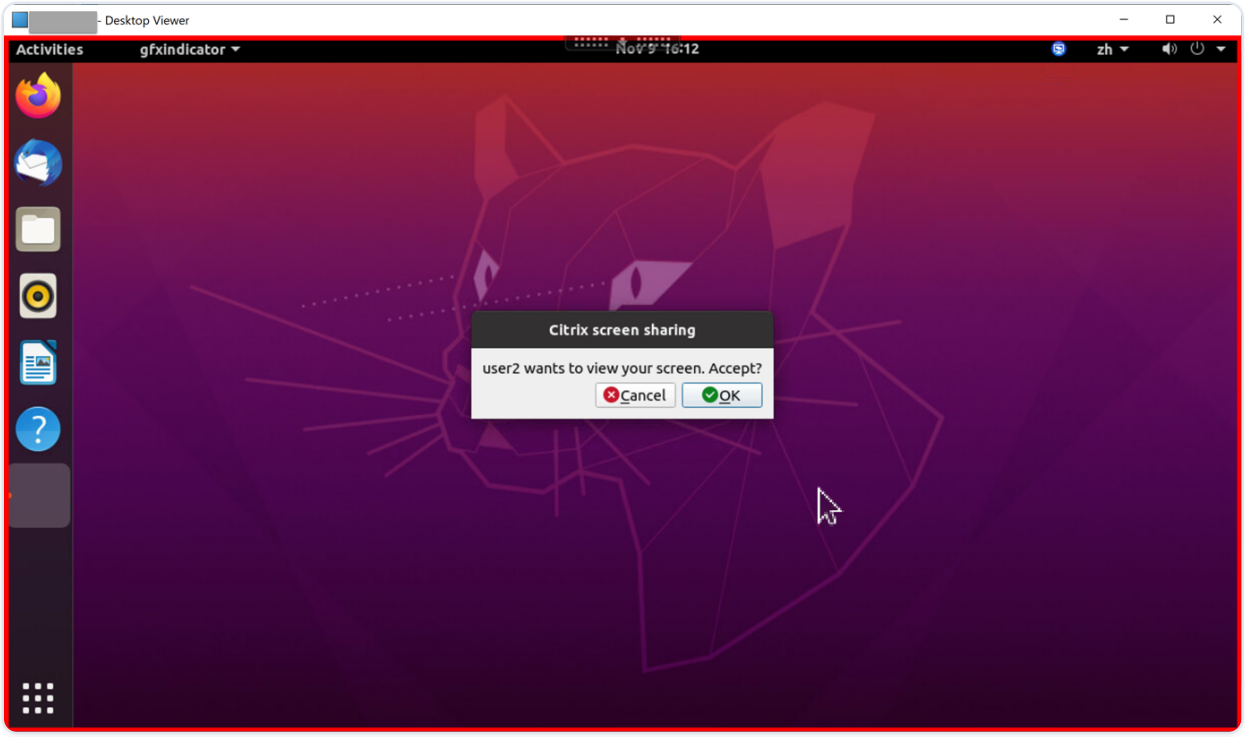
1. En el área de notificaciones de su escritorio virtual, haga clic en el icono de uso compartido de pantalla y seleccione **Ver la pantalla de otra persona**.



2. Introduzca el código de conexión de la pantalla que desea ver y, a continuación, haga clic en **Conectar**.



3. Espere a que el usuario que comparte la pantalla acepte su solicitud. Por ejemplo:

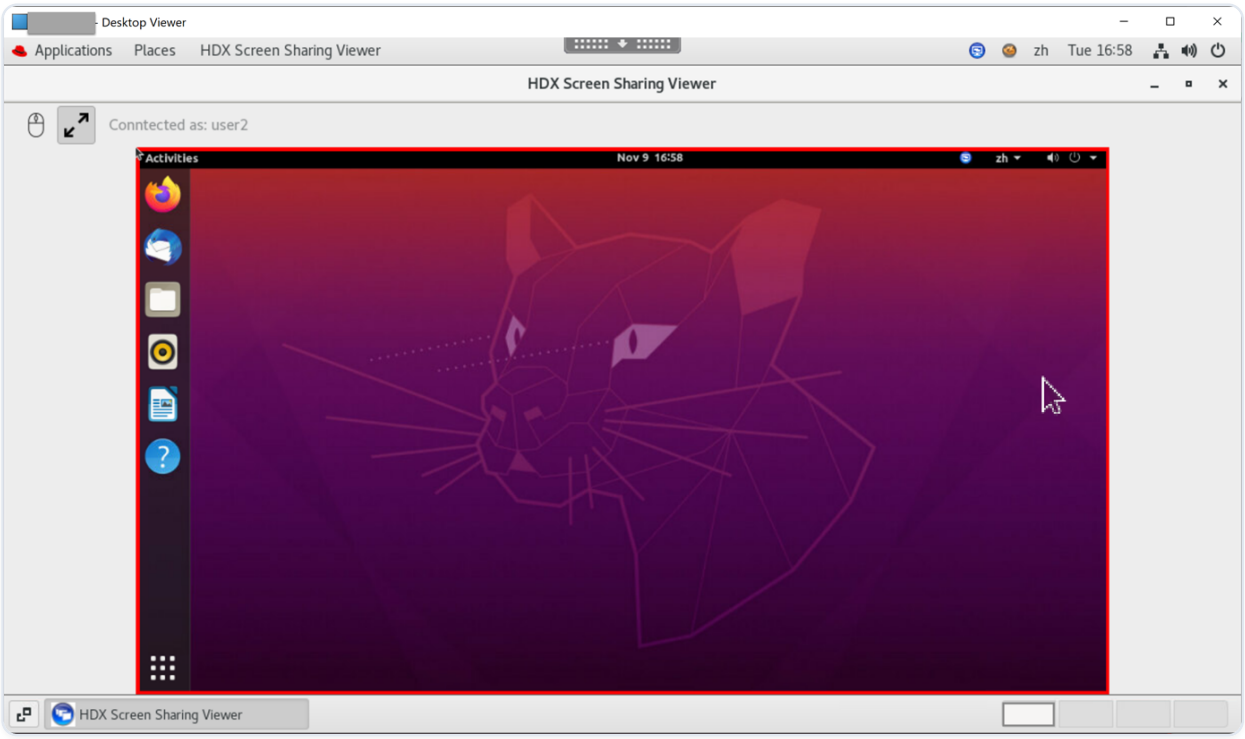


Sugerencia:

- Por parte del usuario que comparte la pantalla, el sistema Linux emite una notificación de su solicitud.

- Si el usuario que comparte la pantalla no acepta su solicitud en 30 segundos, la solicitud caduca y aparece un mensaje.

4. Una vez que el usuario que comparte la pantalla acepta su solicitud haciendo clic en **Aceptar**, la pantalla compartida aparece en su Desktop Viewer. Se conecta como espectador 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 usuario que comparte la pantalla no acepta su solicitud en 30 segundos, la solicitud caduca.
- Solo se permite que un espectador controle una pantalla compartida a la vez.

Vuelva a hacer clic en el icono del ratón para liberar el control de la pantalla compartida.

Soltar el control de una pantalla compartida(/en-us/linux-virtual-delivery-agent/2201/media/release-control-over-shared-screen.png)

6. Para deshabilitar el escalado de la pantalla o escalar al tamaño de la ventana, haga clic en el icono junto al icono del ratón.

   Escalado de ventana(/en-us/linux-virtual-delivery-agent/2201/media/window-scaling.png)

Configuración

La función de compartir pantalla está deshabilitada de forma predeterminada. Para habilitarla, complete la siguiente configuración:

1. Habilite la directiva del indicador de estado de gráficos en Citrix Studio.
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.
5. (Opcional) Si utiliza RHEL 8.x o SUSE 15.x instalado con GNOME, 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.

      Extensión de shell de GNOME(/en-us/linux-virtual-delivery-agent/2201/media/gnome-extension.png)

   c. Descomprima el paquete descargado. verificar que el valor **"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** sea legible también para otros usuarios.

f. Instale GNOME Tweaks.

g. En el entorno de escritorio, recargue su shell 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.

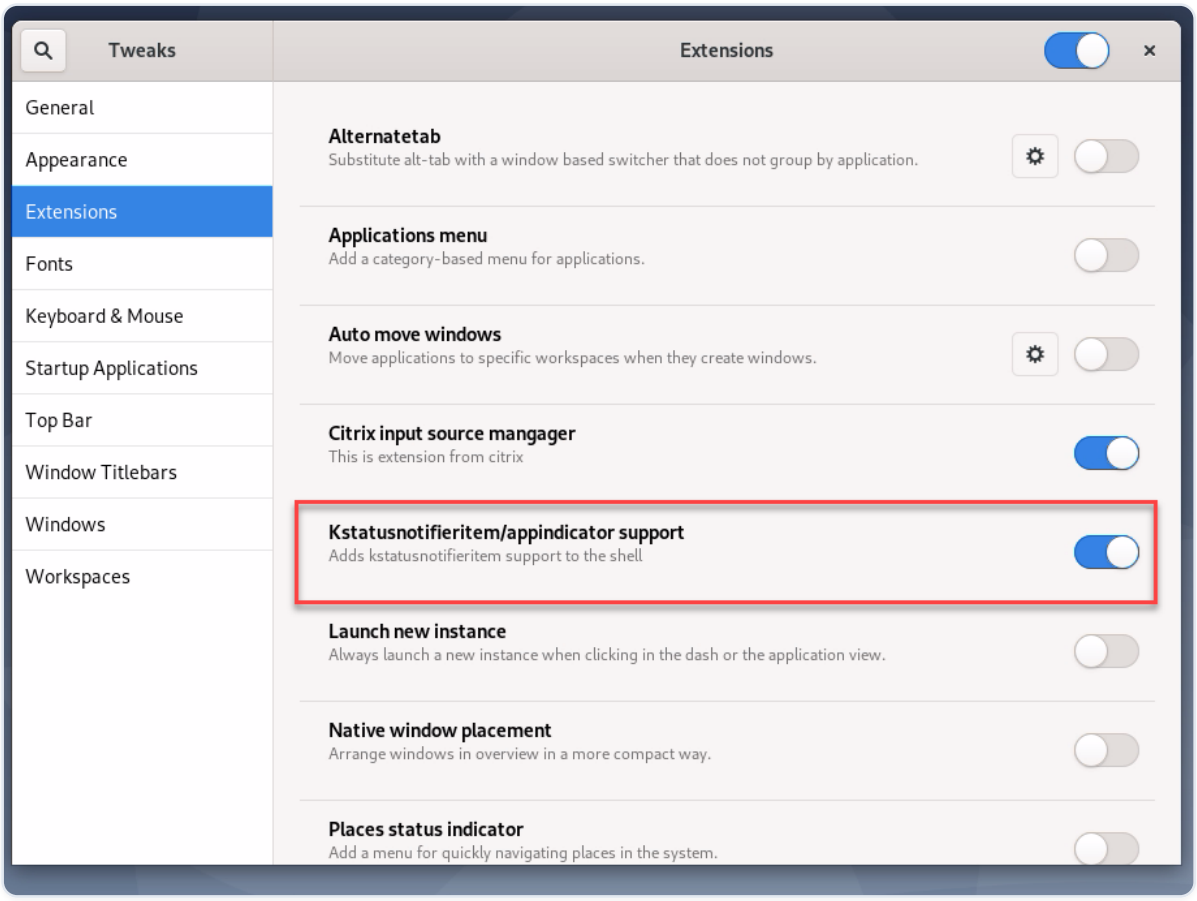
6. (Opcional) Si utiliza Debian 10 instalado con GNOME, complete los siguientes pasos para instalar y habilitar los iconos de la bandeja del sistema de GNOME:

a. Ejecute el comando `sudo apt install gnome-shell-extension-appindicator`. Es posible que deba cerrar la sesión y volver a iniciarla para que GNOME vea la extensión.

b. Busque Tweaks en la pantalla de **Actividades**.

c. Seleccione **Extensiones** en la herramienta Tweaks.

d. Habilite **Kstatusnotifieritem/appindicator support**.



Consideraciones

- La función de uso compartido de pantalla no es compatible con el códec de vídeo H.265.
- La función de uso compartido de 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 mediante `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.

Configurar la fiabilidad de la sesión

Citrix® introduce la función de fiabilidad de la sesión en todas las plataformas Linux compatibles. La fiabilidad de la sesión está habilitada de forma predeterminada.

La fiabilidad de la sesión reconecta las sesiones ICA sin interrupciones a través de interrupciones de red. Para obtener más información sobre la fiabilidad de la sesión, consulte Reconexión automática de clientes y fiabilidad de la sesión.

Nota: Los datos transmitidos a través de una conexión de fiabilidad de la 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 establecer las siguientes directivas para la fiabilidad de la 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 la sesión y Configuración de directivas de reconexión automática de clientes.

Nota: Después de establecer la directiva **Conexiones de fiabilidad de la sesión** o **Número de puerto de fiabilidad de la 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 la sesión**

De forma predeterminada, el agente de escucha TCP de fiabilidad de la sesión está habilitado y a la 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\cg
p"   -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 la sesión. La fiabilidad de la 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 la sesión**.

- **Número de puerto de fiabilidad de la sesión**

También puede establecer el número de puerto de fiabilidad de la 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\cg
p"   -v  "PortNumber" -d  "2599"
```

Nota: Reinicie el servicio HDX para que la configuración surta efecto. Si el número de puerto se ha configurado a través de la 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 de fiabilidad de sesión se envían entre el VDA de Linux y el cliente ICA® cuando no hay actividad en la sesión (por ejemplo, no hay movimiento del ratón ni actualización de la pantalla). 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 reconecta. 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 sesión a través de 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 sesión a través de 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 sesión se está ejecutando (usando el puerto 2598 como ejemplo).

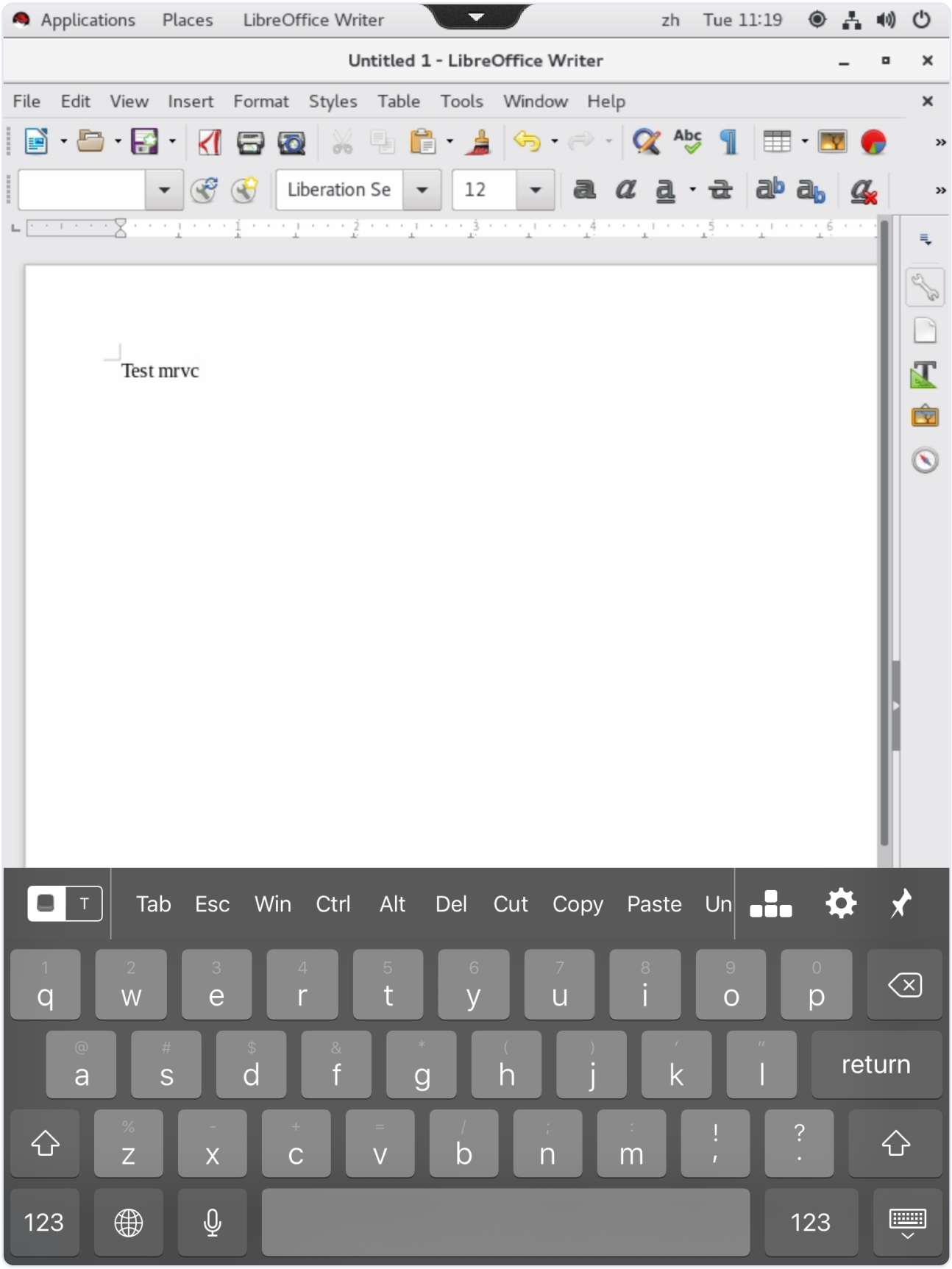
   ```
   netstat -an | grep 2598
   ```

   Si no hay ningún agente de escucha TCP en el puerto de fiabilidad de 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"
   ```

Teclado virtual

La función de teclado virtual está disponible en una sesión de escritorio virtual o aplicación de Linux. El teclado virtual se muestra u oculta automáticamente cuando entra o sale 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 está disponible para RHEL 7.8, RHEL 7.9, RHEL 8.1, RHEL 8.2, RHEL 8.3, SUSE 15.3, SUSE 15.2, SUSE 12.5, Ubuntu 16.04, Ubuntu 18.04 y Ubuntu 20.04. Es compatible con Citrix Workspace app para iOS y para Android.

Habilitar y deshabilitar la función

La función está deshabilitada de forma predeterminada. Utilice la utilidad **ctxreg** para habilitar o deshabilitar 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 deshabilitar 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 cuando inicia sesión en una nueva sesión o cierra sesión y vuelve a iniciarla en la sesión actual.

Limitaciones

- Es posible que la función no funcione como se espera con Google Chrome, LibreOffice y otras aplicaciones.
- Para volver a mostrar el teclado virtual después de ocultarlo manualmente, haga clic en un campo que no sea de entrada y, a continuación, de nuevo en el campo de entrada actual.
- Es posible que el teclado virtual no aparezca cuando hace clic de un campo de entrada a otro en un navegador 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 caracteres chinos, japoneses y coreanos).
- El teclado en pantalla no está disponible para campos de entrada de contraseña.
- El teclado en pantalla podría superponerse al campo de entrada actual. En este caso, mueva la ventana de la aplicación o desplácese hacia arriba en la pantalla 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.

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 esos 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 inhabilita automáticamente en los campos de contraseña.
- La interfaz de usuario del IME no sigue al cursor en el área de entrada.

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 de Linux.

Sin embargo, la barra de idioma nativa en el Linux VDA no estaba disponible para la aplicación publicada porque la barra de idioma está muy integrada con el entorno de escritorio de Linux. Como resultado, los usuarios no podían introducir texto en un idioma que requiriera IME, como chino, japonés o coreano. Tampoco era posible que los usuarios cambiaran entre distribuciones 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 distribuciones 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"
```

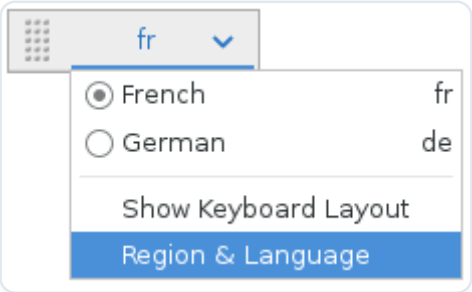
Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000000"
```

Uso

El uso es sencillo.

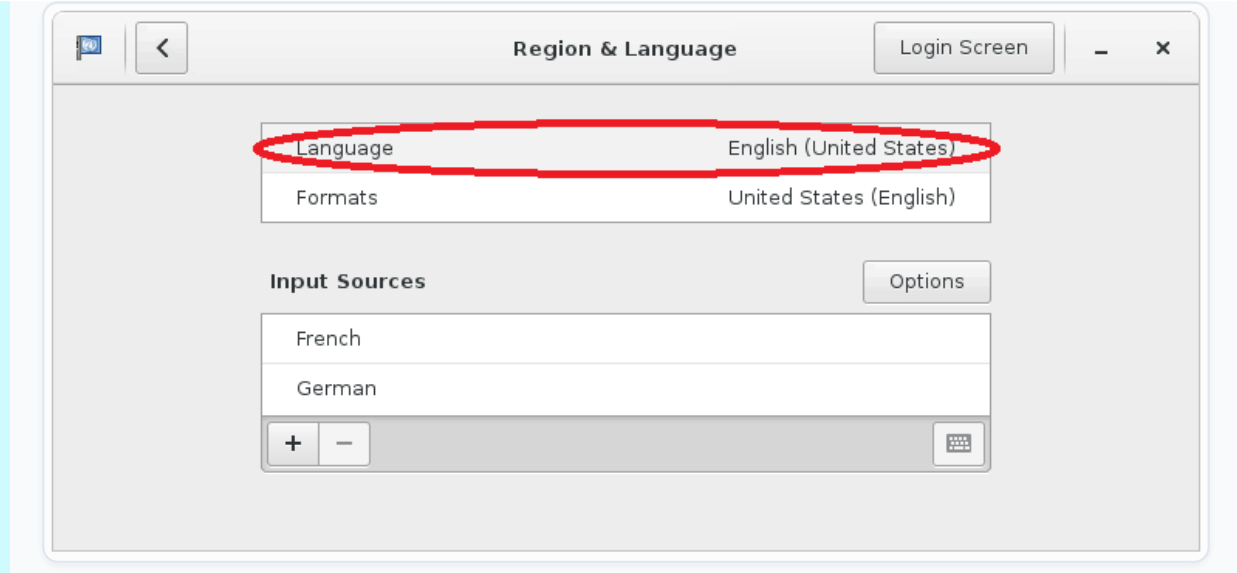
1. Habilite la función.
2. Acceda a una aplicación publicada que pueda aceptar la entrada de texto. Aparece una barra de idioma en la sesión, junto a la aplicación.
3. En el menú desplegable, seleccione **Región e idioma** para agregar el idioma deseado (origen de entrada).



4. Seleccione el IME o la distribución de teclado en el menú desplegable.
5. Escriba un idioma con el IME o la distribución de teclado seleccionados.

Nota:

- Cuando cambie la distribución del teclado en la barra de idioma del VDA, asegúrese de que se utilice la misma distribución del teclado en el lado del cliente (donde se 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**.



Sincronización dinámica de la distribución del teclado

Anteriormente, las distribuciones de teclado en el VDA de Linux y en el dispositivo cliente tenían que ser las mismas. Por ejemplo, cuando la distribución del teclado cambiaba de inglés a francés en el dispositivo cliente pero no en el VDA, podían producirse problemas de asignación de teclas y persistir hasta que el VDA también cambiara a francés.

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 edite el registro mediante la utilidad `ctxreg`.

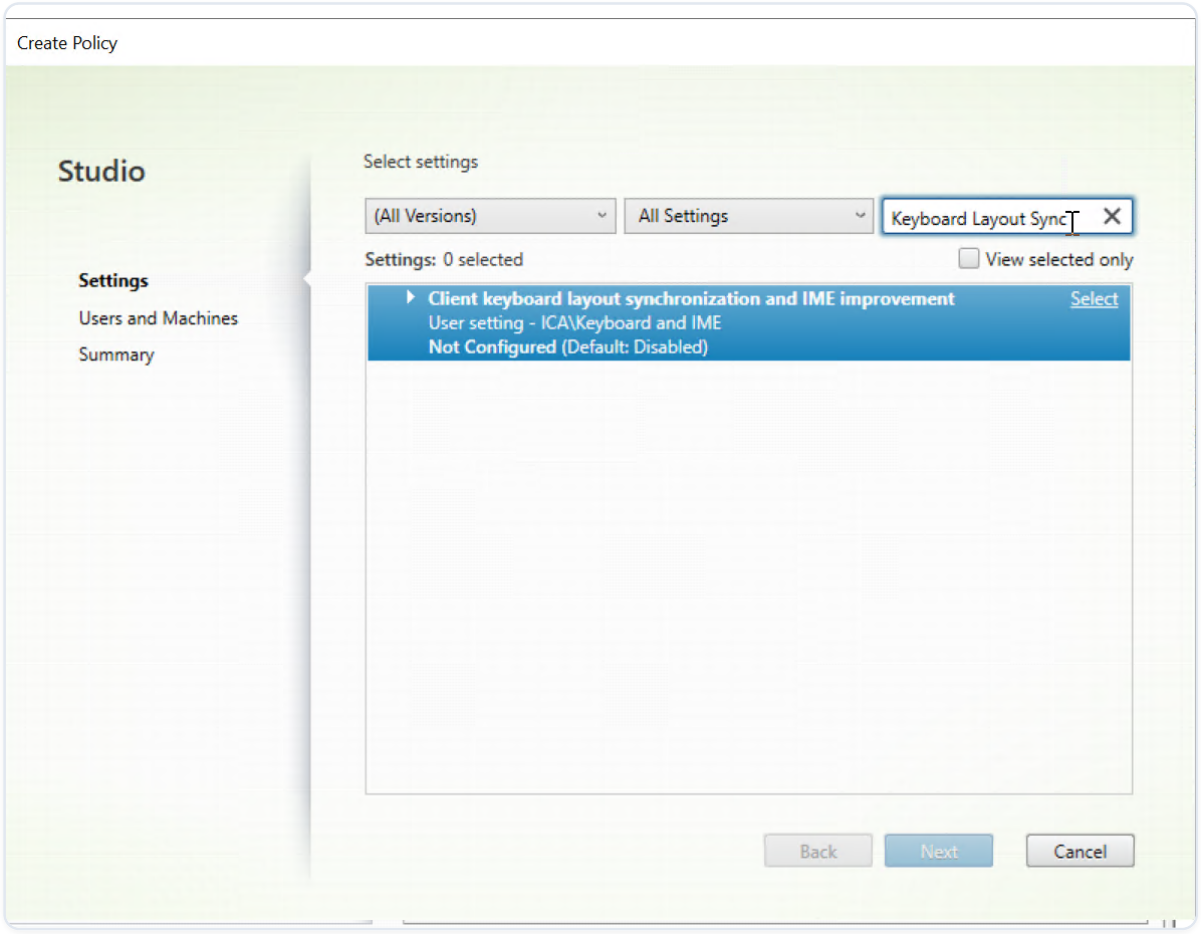
> **Nota:**

> 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:

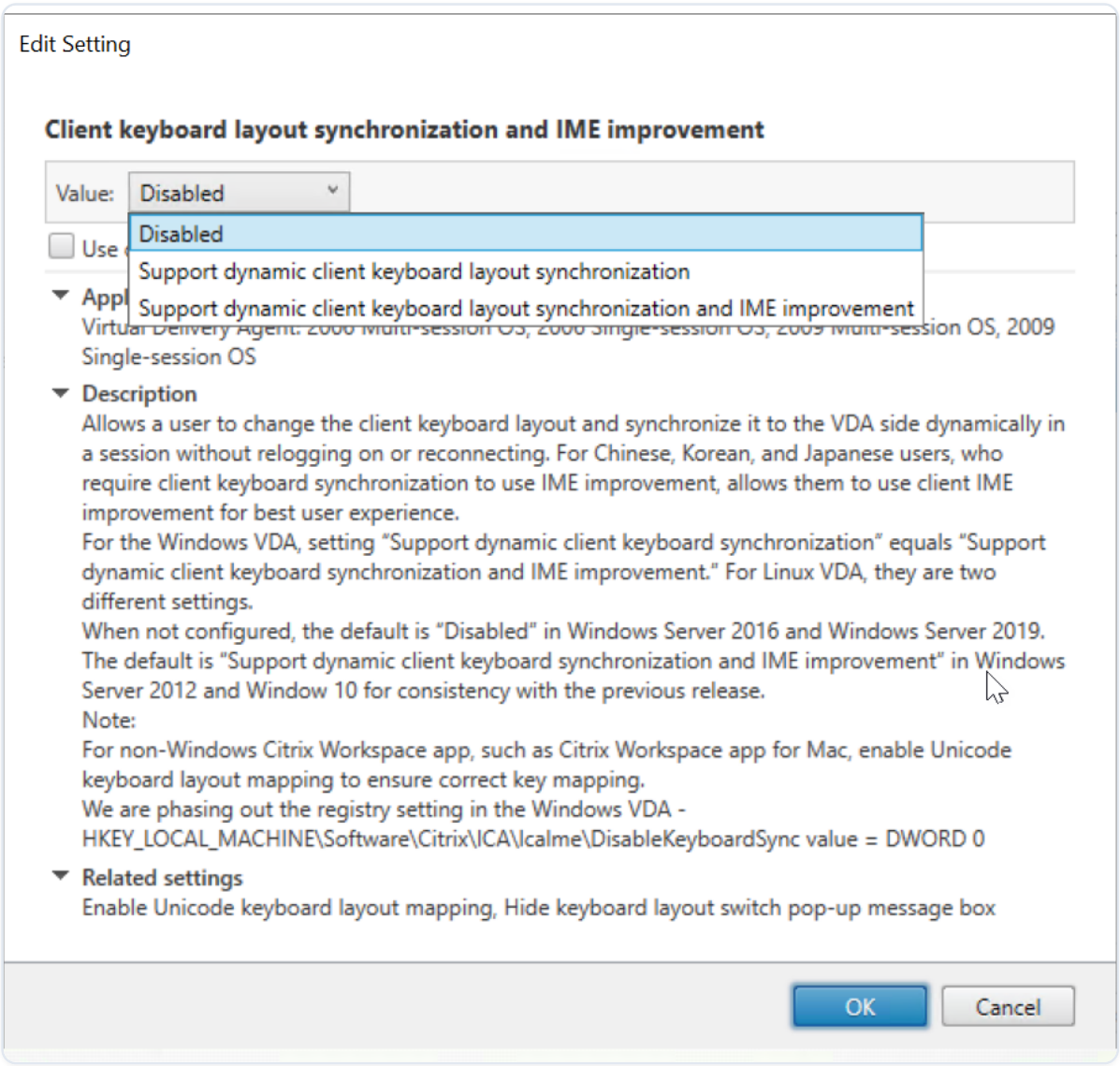
  a. En Studio, haga clic con el botón secundario en **Directivas** y seleccione **Crear directiva**.

  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:

- **Inhabilitado**: 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 de registro **SyncKeyboardLayout** en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- **Compatibilidad con la sincronización dinámica de la distribución del teclado del cliente y mejora del IME**: habilita la sincronización dinámica de la distribución 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 a través de la utilidad `ctxreg` para habilitar o inhabilitar la función de sincronización dinámica de la distribución 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"
  ```

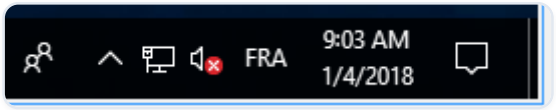
  Para inhabilitar esta función, ejecute el comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000000"
  ```

Uso

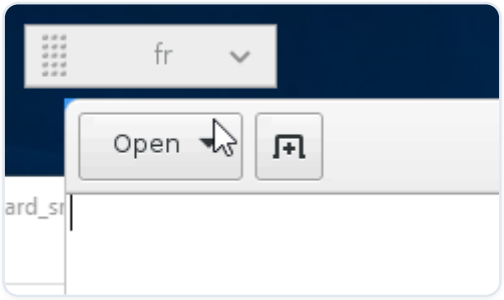
Con esta función habilitada, cuando la distribución del teclado cambia en el dispositivo cliente durante una sesión, la distribución del teclado de la sesión cambia en consecuencia.

Por ejemplo, si cambia la distribución del teclado en un dispositivo cliente a francés (FR):



Entonces, la distribución 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:



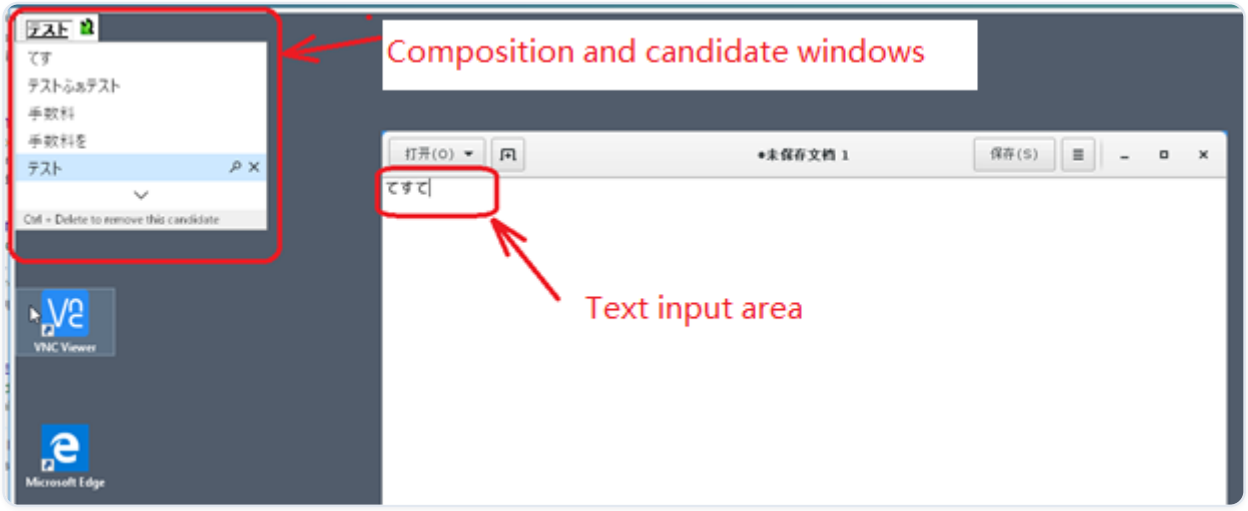
En una sesión de escritorio, puede ver este cambio automático en la barra de tareas:



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 usabilidad 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 VDA de Linux. 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

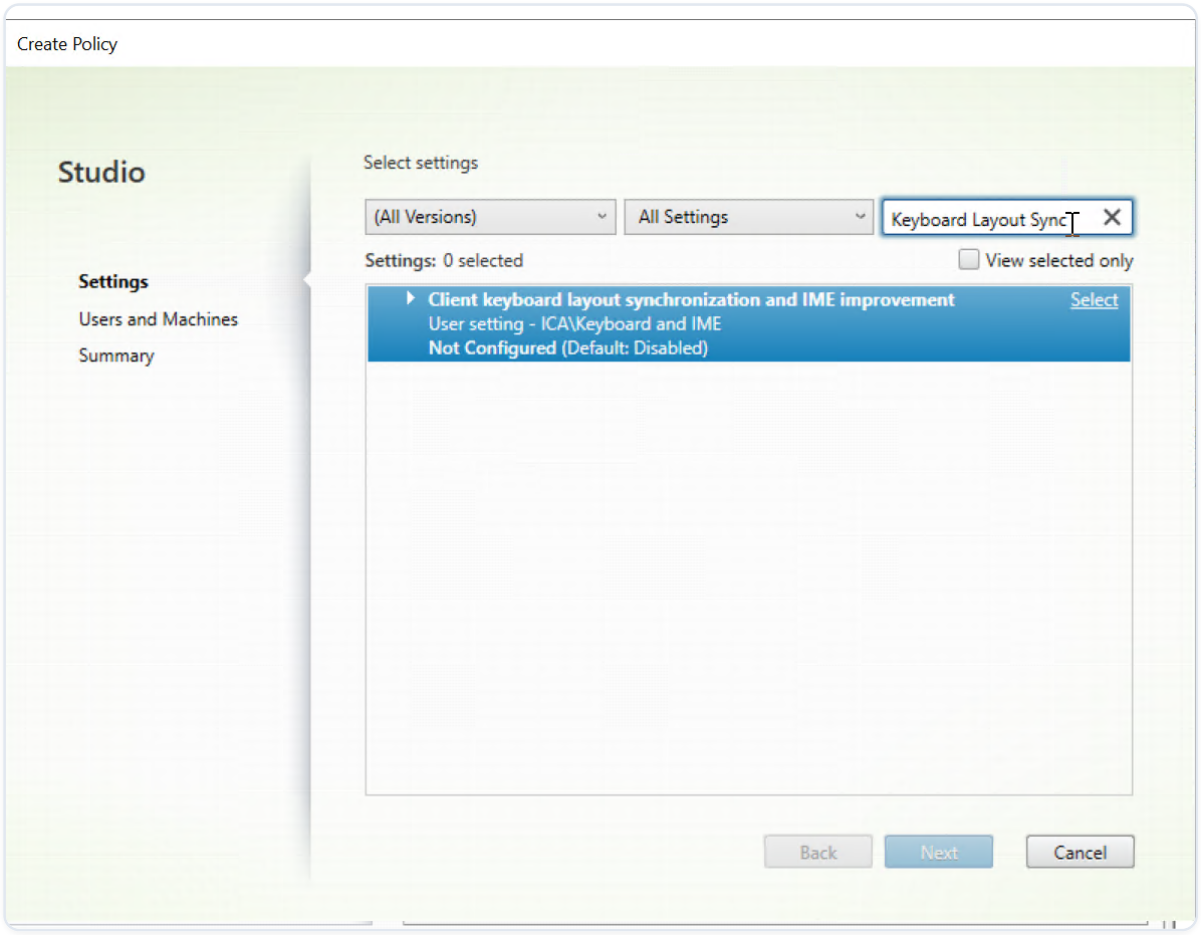
La función de sincronización de la interfaz de usuario del IME del cliente está deshabilitada de forma predeterminada. Para habilitar o deshabilitar la función, configure la directiva **Sincronización del diseño del teclado del cliente y mejora del IME** o edite el registro a través de la utilidad `ctxreg`.

> **Nota:**
>
> La directiva **Sincronización del diseño 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.

- Establezca la directiva **Sincronización del diseño del teclado del cliente y mejora del IME** para habilitar o inhabilitar la función de sincronización de la interfaz de usuario del IME del cliente:

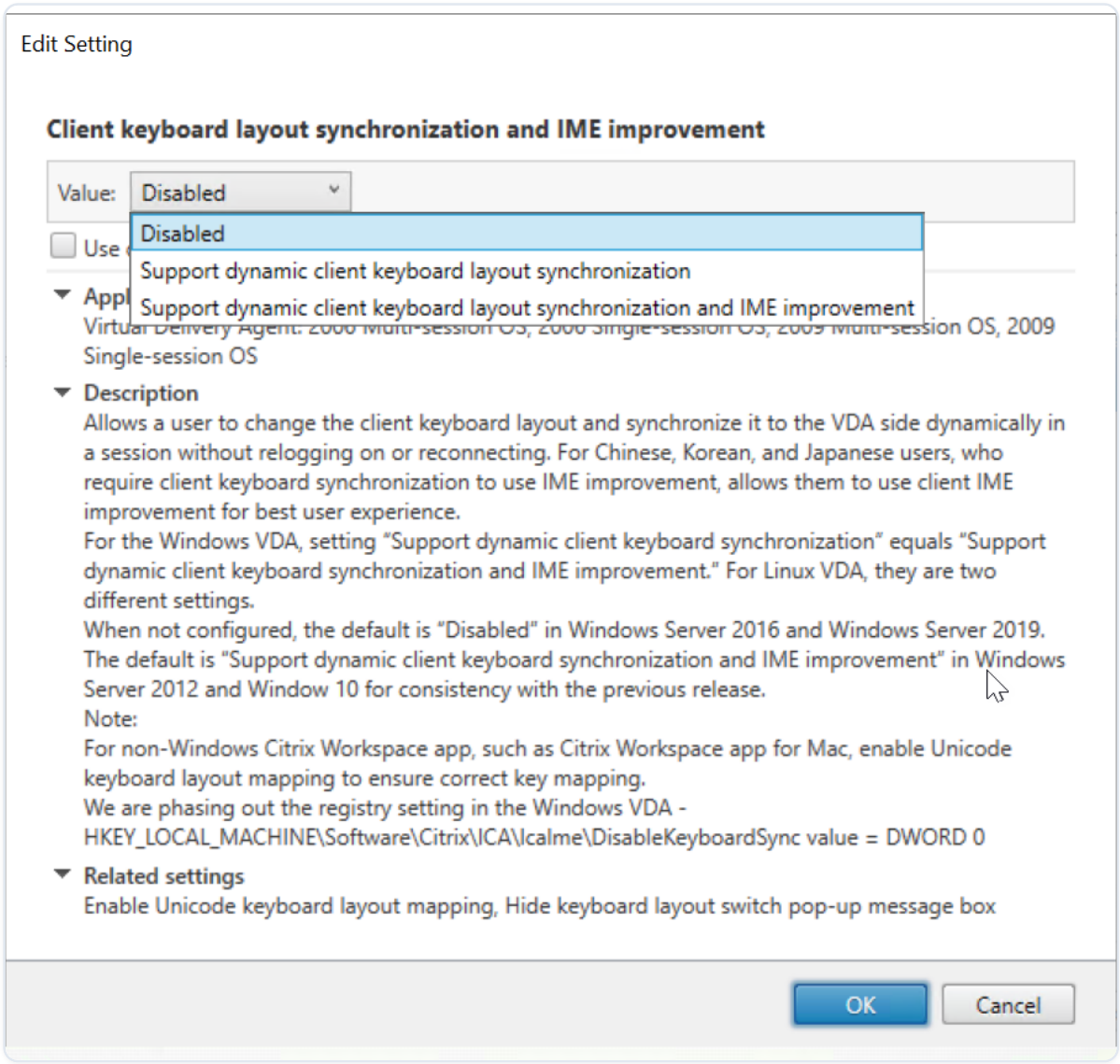
  a. En Studio, haga clic con el botón derecho en **Directivas** y seleccione **Crear directiva**.

  b. Busque la directiva **Sincronización del diseño del teclado del cliente y mejora del IME**.



c. Haga clic en **Seleccionar** junto al nombre de la directiva.

d. Establezca la directiva.



Hay tres opciones disponibles:

- **Inhabilitado**: inhabilita la sincronización dinámica del diseño del teclado y la sincronización de la interfaz de usuario del IME del cliente.
- **Admitir la sincronización dinámica del diseño del teclado del cliente**: 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`.
- **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 inhabilitar la función de sincronización de la interfaz de usuario del 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 inhabilitar la función, ejecute el comando:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncClientIME" -d "0x00000000"
  ```

HDX™ Insight

Información general

El VDA de Linux admite parcialmente la función HDX Insight. HDX Insight forma parte de Citrix Application Delivery Management (ADM) y se basa en el popular estándar del sector AppFlow. Permite a TI ofrecer una experiencia de usuario excepcional al proporcionar una visibilidad de extremo a extremo sin precedentes del tráfico ICA de Citrix que pasa a través del tejido de red de aplicaciones de Citrix ADC o Citrix SD-WAN. Para obtener más información, consulte HDX Insight

Instalación

No es necesario instalar ningún paquete dependiente.

Uso

HDX Insight analiza los mensajes ICA® que pasan a través de 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 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 esté habilitado y que una aplicación seamless se haya iniciado durante un tiempo.

Rendezvous V1

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.

Requisitos

- Acceso al entorno mediante Citrix Workspace™ y el servicio Citrix Gateway.
- Plano de control: Servicio Citrix Virtual Apps and Desktops™ (Citrix Cloud).
- Linux VDA versión 2112 o posterior.
- 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 incluir todos los subdominios en la lista de permitidos de esa manera, utilice `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 Desktops) y el artículo del Knowledge Center CTX270584.
- Los Cloud Connectors deben obtener los FQDN de los VDA al intermediar una sesión. Para lograr este objetivo, habilite la resolución DNS para el sitio: Con el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops, 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.

Configuración del proxy

El VDA admite el establecimiento de conexiones Rendezvous a través de un proxy HTTP.

Consideraciones sobre el proxy

Tenga en cuenta lo siguiente al utilizar proxies con Rendezvous:

- Se admiten proxies HTTP no transparentes.
- 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 Linux VDA.

  > **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 directiva **Proxy de Rendezvous**. Si no crea un SPN, la autenticación falla.

- Para un proxy HTTP, utilice TCP como protocolo de transporte para ICA.

Proxy no transparente

Cuando utilice un proxy no transparente en su red, configure el ajuste Configuración del proxy de Rendezvous. Cuando el ajuste esté habilitado, especifique la dirección del proxy HTTP para que el VDA sepa qué proxy utilizar. Por ejemplo:

- Dirección del proxy: `http://<URL or IP>:<port>`

Validación de Rendezvous

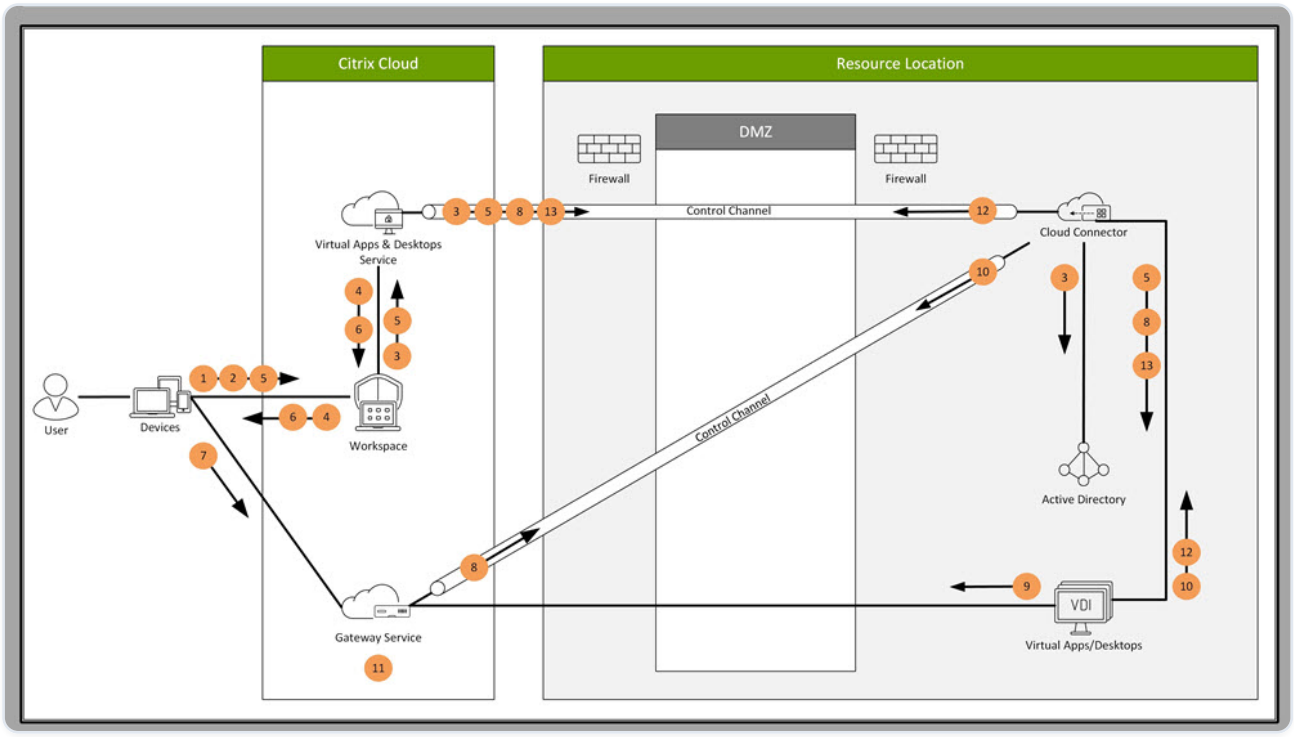
Si cumple todos los requisitos, siga estos pasos para validar si Rendezvous está en uso:

1. Inicie un terminal en el VDA.
2. Ejecute `/opt/Citrix/VDA/bin/ctxqurey -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 - CGP - ICA

> **Sugerencia:**
>
> Si habilita Rendezvous y el VDA no puede llegar directamente al servicio Citrix Gateway, el VDA recurre a la sesión HDX™ de proxy 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, el servicio Citrix Virtual Apps™ and Desktops autentica las credenciales con Active Directory mediante el canal de Cloud Connector.
4. Citrix Workspace muestra los recursos enumerados del servicio Citrix Virtual Apps and Desktops.
5. Seleccione los recursos de Citrix Workspace. El servicio Citrix Virtual Apps and Desktops envía un mensaje al VDA para prepararse para una sesión entrante.
6. Citrix Workspace envía un archivo ICA al punto final que contiene un tíquet STA generado por Citrix Cloud.
7. El punto final se conecta al servicio Citrix Gateway, proporciona el tíquet para conectarse al VDA y Citrix Cloud valida el tíquet.
8. El servicio Citrix Gateway envía información de conexión al Cloud Connector. El Cloud Connector determina si la conexión debe ser 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 como proxy.
11. El servicio Citrix Gateway establece una conexión entre el dispositivo de punto final y el VDA.

12. El VDA verifica su licencia con el servicio Citrix Virtual Apps and Desktops a través del Cloud Connector.
13. El servicio Citrix Virtual Apps and Desktops envía las directivas de sesión al VDA a través del Cloud Connector. Esas directivas se aplican.

Rendezvous V2 (vista previa)

Al usar 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.

Las máquinas unidas a un dominio de AD estándar y las máquinas no unidas a un dominio son compatibles para usar Rendezvous V2 con VDA de Linux de sesión única y multisesión. 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: Servicio Citrix Virtual Apps and Desktops™ (Citrix Cloud).
- VDA versión 2201 o posterior.
- 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 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 de Linux actualmente no admite conexiones Rendezvous V2 a través de un proxy.

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 de Protocolo Rendezvous en **Permitido**.
   - 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/ctxqurey -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
- No Rendezvous: TCP - CGP - ICA

Si Rendezvous V2 está en uso, la versión del protocolo muestra 2.0.

> **Sugerencia:**
>
> Si habilita Rendezvous y el VDA no puede acceder directamente al servicio Citrix Gateway, el VDA recurre a la intermediación de la sesión HDX a través del Cloud Connector.

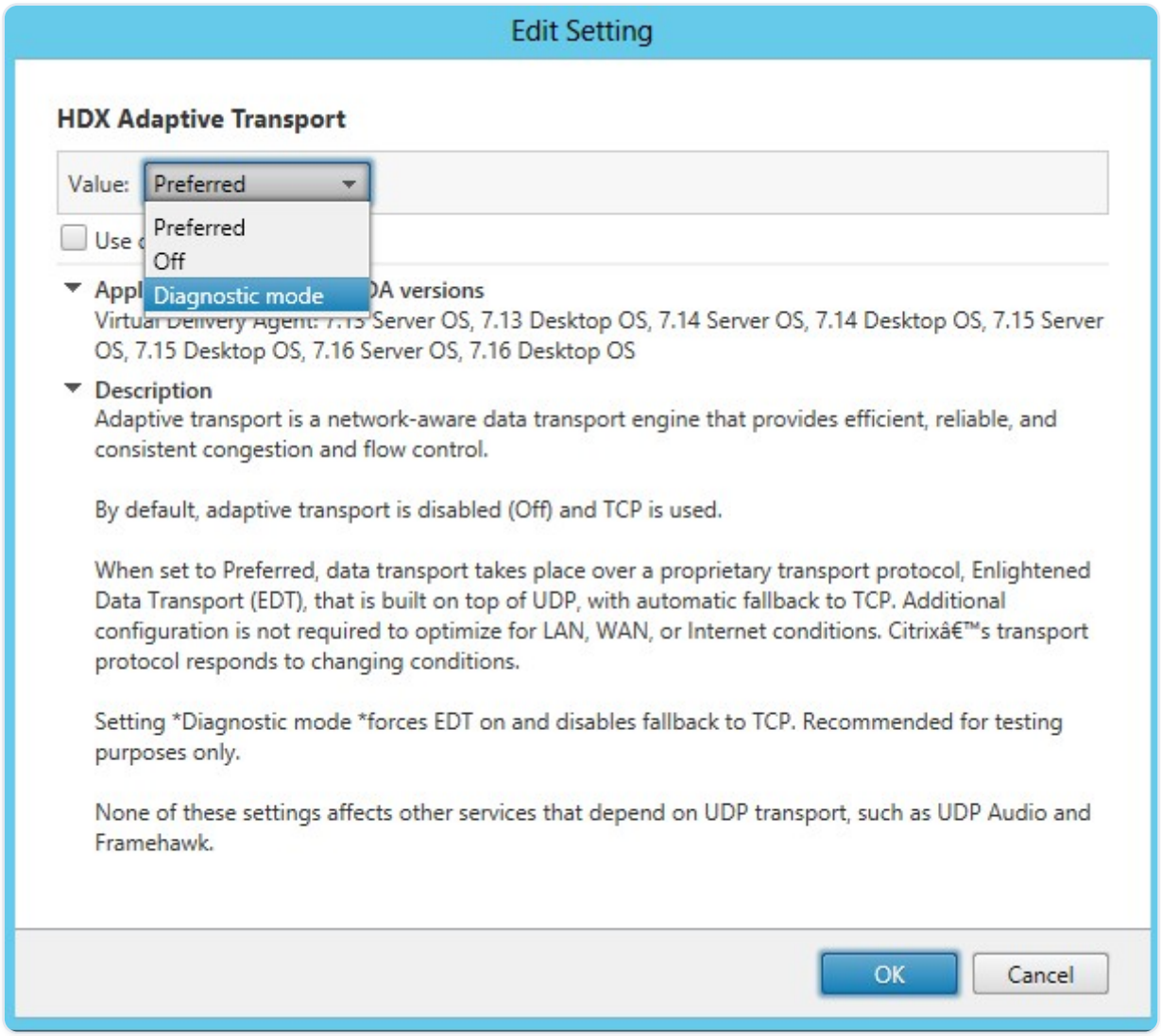
Transporte adaptable

El transporte adaptativo es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops. Es más rápido, más escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones WAN e Internet de larga distancia desafiantes. Para obtener más información sobre el transporte adaptativo, consulte Transporte adaptativo.

Habilitar el transporte adaptativo

En Citrix Studio, verificar que la directiva **HDX™ Adaptive Transport** esté establecida en **Preferred** o **Diagnostic mode**. **Preferred** está seleccionada de forma predeterminada.

- **Preferred**: El transporte adaptativo a través de Enlightened Data Transport (EDT) se utiliza cuando es posible, con un mecanismo de reserva a TCP.
- **Diagnostic mode**: Se fuerza el uso de EDT y se deshabilita el mecanismo de reserva a TCP.



Deshabilitar el transporte adaptativo

Para deshabilitar el transporte adaptativo, establezca la directiva **HDX Adaptive Transport** en **Off** en Citrix Studio.

Comprobar si el transporte adaptativo está habilitado

Para comprobar si los oyentes UDP están en ejecución, ejecute el siguiente comando.

```
netstat -an | grep "1494\|2598"
```

En circunstancias normales, la salida es similar a la siguiente.

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*
```

```
udp        0      0 :::1494                 :::*
```

Detección de MTU de 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.

Requisitos mínimos:

- Linux VDA 2012
- Aplicación Citrix Workspace™ 1911 para Windows
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- La fiabilidad de la sesión debe estar habilitada

Si utiliza plataformas o versiones de cliente que no admiten esta función, consulte el artículo del Knowledge Center CTX231821 para obtener detalles sobre cómo configurar una MTU EDT personalizada que sea adecuada para su entorno.

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 derivados 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.

Habilitar o inhabilitar la detección de MTU EDT en el VDA

La detección de MTU EDT está inhabilitada de forma predeterminada.

- Para habilitar la detección de MTU EDT, establezca la clave de Registro `MtuDiscovery` mediante el siguiente comando, reinicie el VDA y espere a que 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 EDT, elimine el valor de Registro `MtuDiscovery`.

Esta configuración es para toda la máquina y afecta a todas las sesiones que se conectan desde un cliente compatible.

Controlar la detección de MTU EDT en el cliente

Puede controlar la detección de MTU EDT de forma selectiva en el cliente agregando el parámetro `MtuDiscovery` en el archivo ICA®. Para inhabilitar la función, establezca lo siguiente en la sección `Application`:

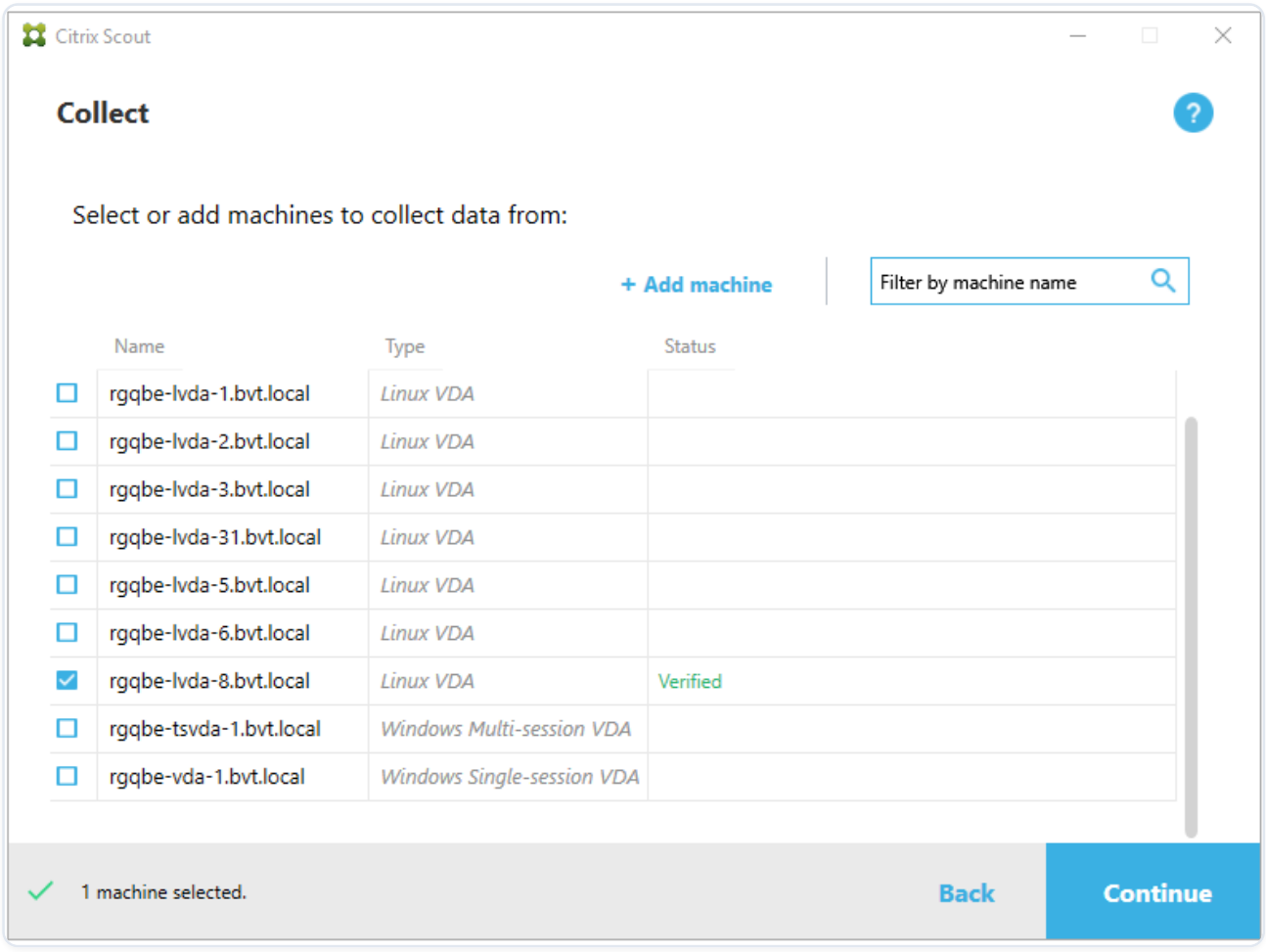
```
MtuDiscovery=Off
```

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 EDT en el VDA. Si la detección de MTU EDT no está habilitada en el VDA, el parámetro del archivo ICA no tiene ningún efecto.

Integrar 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.



Nota:

Después de actualizar desde Linux VDA 1912 y versiones anteriores, debe volver a ejecutar /opt/Citrix/VDA/sbin/ctxsetup.sh para configurar las variables del servicio de telemetría de Citrix (ctxtelemetry). Para obtener más información sobre las variables, consulte Instalación sencilla.

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.

Puede usar los puertos predeterminados o cambiar los puertos a través de las siguientes variables al instalar el Linux VDA.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** – El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT** – El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

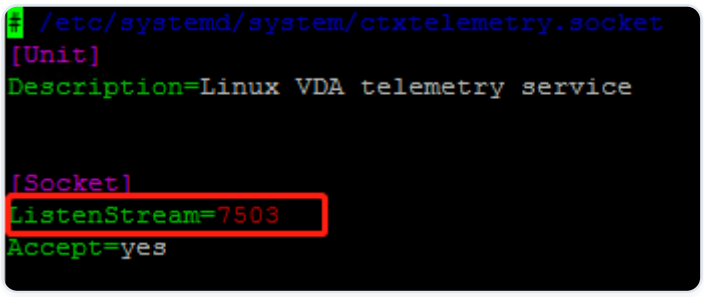
Para cambiar los puertos después de instalar el VDA, haga lo siguiente:

1. Para cambiar un puerto para comunicarse con Scout, ejecute el siguiente comando.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\Software\Citrix\VirtualDesktopAgent" -v "TelemetryServicePort" -d
   <port number> -t REG_DWORD
   ```

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.

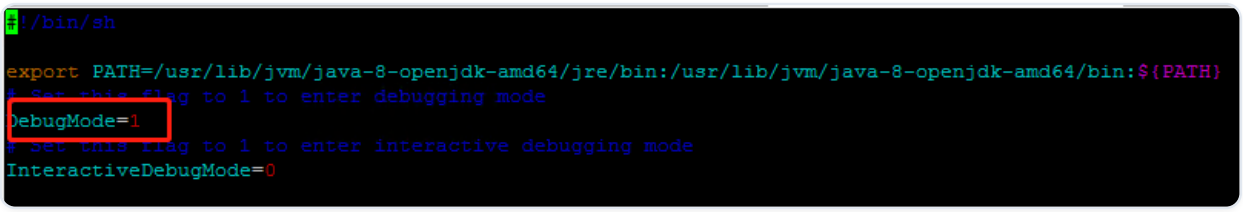
   Si utiliza una distribución de Ubuntu, por ejemplo, ejecute el comando **sudo ufw allow 7503** para habilitar el puerto 7503.

Modo de depuración

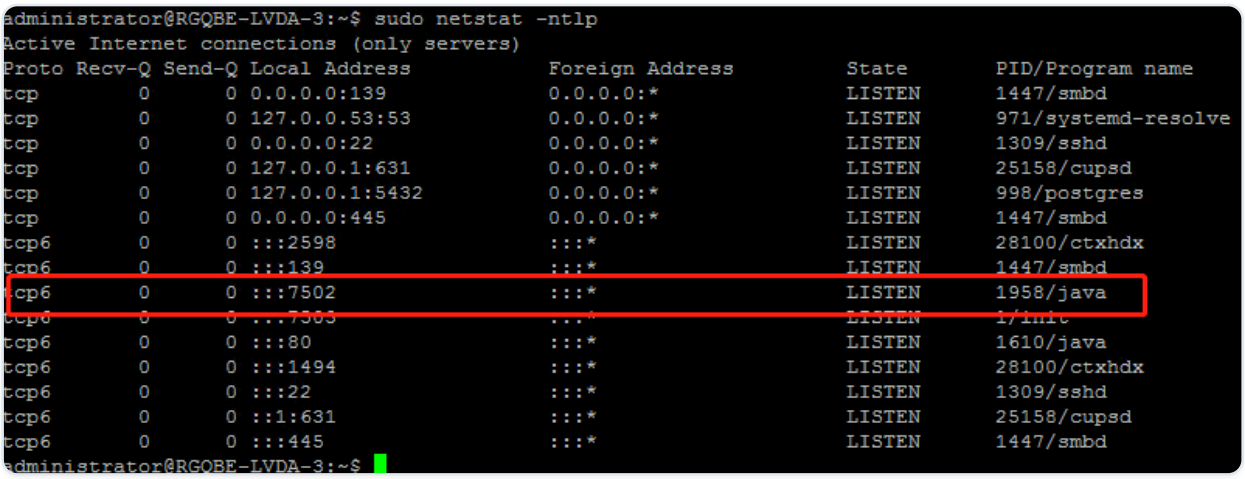
Si el Servicio de telemetría de Citrix no funciona como se espera, puede habilitar el modo de depuración para determinar las causas.

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
```



2. Detenga manualmente el Servicio de telemetría de Citrix o espere 15 minutos a que el servicio se detenga automáticamente.



En este ejemplo, puede ejecutar los siguientes comandos para detener el Servicio de telemetría de Citrix.

```
sudo netstat -ntlp

Kill -9 1958
```

3. Para reiniciar el Servicio de telemetría de Citrix, 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 de telemetría de Citrix se detiene de forma predeterminada y solo se inicia 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.

Seguimiento activado

Información general

La recopilación de registros y la reproducción de problemas ralentizan el diagnóstico y degradan la experiencia del usuario. La función de seguimiento activado facilita estos esfuerzos. El seguimiento está habilitado para Linux VDA de forma predeterminada.

Configuración

El demonio `ctxlogd` y la utilidad `setlog` ahora se incluyen en el paquete de la versión de Linux VDA. De forma predeterminada, el demonio `ctxlogd` se inicia después de instalar y configurar Linux VDA.

Demonio ctxlogd

Todos los demás servicios que se rastrean dependen del demonio `ctxlogd`. Puede detener el demonio `ctxlogd` si no desea mantener el seguimiento de Linux VDA.

Utilidad setlog

El seguimiento activado se configura mediante la utilidad `setlog`, que se encuentra 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 las configuraciones. Ejecute el siguiente comando para obtener ayuda con la utilidad `setlog`:

```
setlog help
```

Valores

De forma predeterminada, la **Ruta de salida del registro** se establece en **/var/log/xdl/hdx.log**, el **Tamaño máximo del registro** se establece en 200 MB, y puede guardar hasta dos archivos de registro antiguos en la **Ruta de salida del registro**.

Ver los valores actuales de `setlog`:

```
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
```

Ver o establecer un único valor de `setlog`:

```
setlog value <name> [<value>]
```

Por ejemplo:

```
setlog value log_size 100
```

Niveles

De forma predeterminada, los niveles de registro se establecen en **warning** (sin distinción entre mayúsculas y minúsculas).

Para ver los niveles de registro establecidos para los diferentes componentes, ejecute el siguiente comando:

```
setlog levels
```

Para establecer los niveles de registro (incluidos Deshabilitado, Heredado, Detallado, Información, Advertencias, Errores y Errores graves), ejecute el siguiente comando:

```
setlog level <class> [<level>]
```

NIVEL DE REGISTRO	PARÁMETRO DE COMANDO (NO DISTINGUE MAYÚSCULAS DE MINÚSCULAS)
Deshabilitado	ninguno
Heredado	heredar
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
```

Marcas

De forma predeterminada, las marcas se establecen de la siguiente manera:

```
setlog flags


DATE = true


TIME = true


NAME = true


PID = true


TID = false


SID = true


UID = false


GID = false


CLASS = false
```

```
LEVEL = false



FUNC = true



FILE = false
```

Ver las marcas actuales:

```
setlog flags
```

Ver o establecer un único indicador de registro:

```
setlog flag <flag> [<state>]
```

Restaurar valores predeterminados

Revertir todos los niveles, indicadores y valores a la configuración predeterminada:

```
setlog default
```

Importante:

El servicio `ctxlogd` se configura utilizando el archivo **/var/xdl/.ctxlog**, que solo los usuarios root pueden crear. Otros usuarios no tienen permiso de escritura para este archivo. Recomendamos que los usuarios root no otorguen permiso de escritura a otros usuarios. El incumplimiento puede hacer que la configuración arbitraria o maliciosa `ctxlogd`, lo que puede afectar el rendimiento del servidor y, por lo tanto, la experiencia del usuario.

Solución de problemas

El demonio `ctxlogd` falla y no se puede reiniciar el servicio `ctxlogd` si 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 solucionar este problema, ejecute `setlog` como usuario root para recrear el archivo **/var/xdl/.ctxlog**. Luego, reinicie el servicio `ctxlogd` del que dependen otros servicios.

Sesiones en la sombra

La función de shadowing 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 de shadowing de sesiones, utilice `Citrix Director` 7.16 o posterior.

Instalación y configuración

Dependencias

Se requieren dos nuevas dependencias, `python-websockify` y `x11vnc`, para el shadowing de sesiones. Las dependencias `python-websockify` y `x11vnc` se instalan automáticamente al instalar el VDA de Linux en Ubuntu 16.04. En las demás distribuciones compatibles, debe instalar `python-websockify` y `x11vnc` manualmente después de instalar el VDA de Linux.

Para RHEL 7.x y 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 resolver `python-websockify` y `x11vnc`, habilite los repositorios Extra Packages for Enterprise Linux (EPEL) y RPM opcionales en RHEL 7.x:

- EPEL

  El repositorio EPEL es necesario para `x11vnc`. Ejecute el siguiente comando para habilitar el repositorio EPEL:

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  ```

- RPM opcionales

  Ejecute el siguiente comando para habilitar el repositorio opcional `RPMs` para instalar algunos paquetes de dependencia de `x11vnc`:

  ```
  subscription-manager repos --enable rhel-7-server-optional-rpms --enable rhel-7-server-extras-rpms
  ```

Para RHEL 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
```

Para resolver `x11vnc`, habilite 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:

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:

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 de `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 utilizar `ws://`.

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. En su lugar,

puede utilizar un certificado comodín para todo el dominio. En este caso, debe conocer al menos el nombre de 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 cuál de los 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 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.

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 reciba un certificado de una CA, puede reiniciar el Asistente para certificados de servidor web en IIS y el asistente instalará el certificado. Alternativamente, puede ver e importar certificados en el equipo mediante 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 raíz SSL en la ficha **Autoridades** del Administrador de certificados.

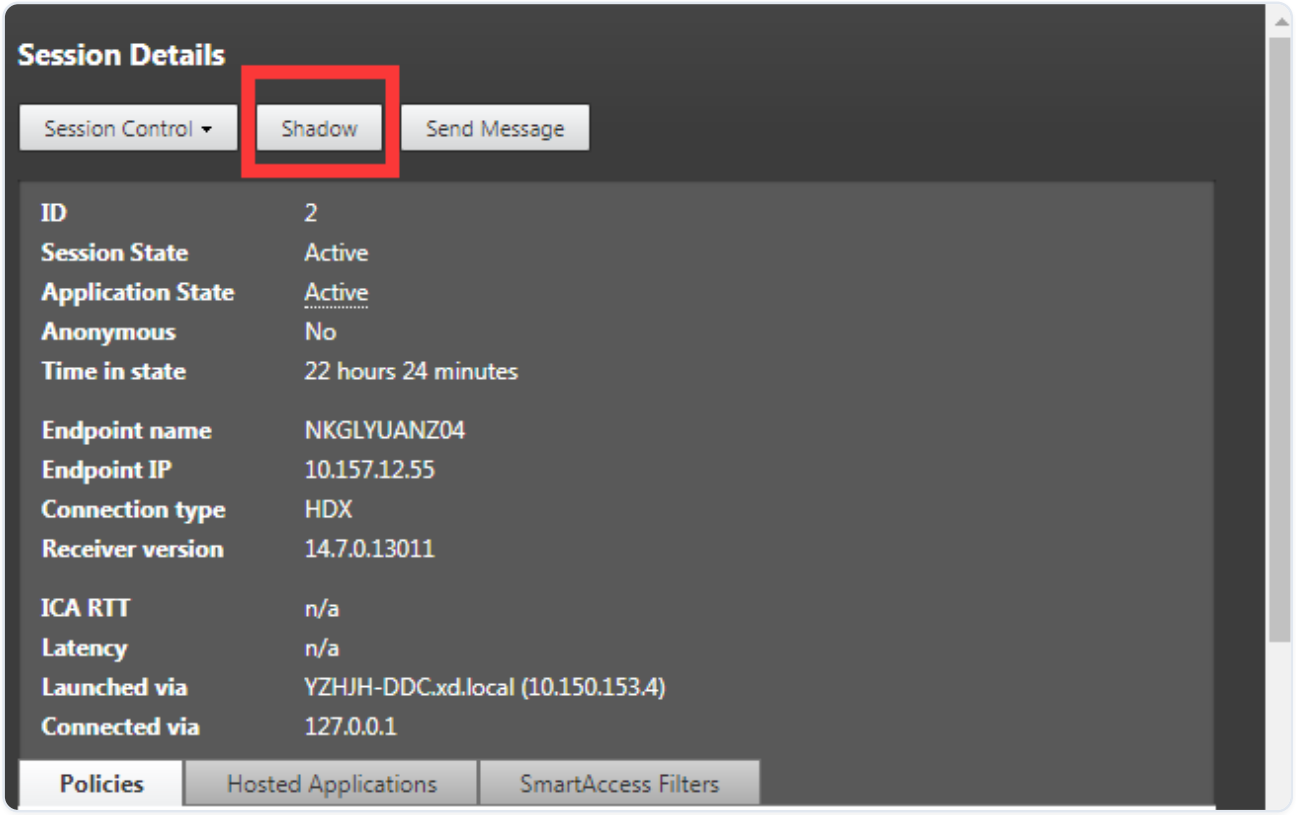
Instalar un certificado de servidor y su clave en cada servidor Linux VDA

Asigne a los certificados de servidor el nombre "shadowingcert.*" y al archivo de clave "shadowingkey.*" (* 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. Un nombre o una ruta incorrectos impiden

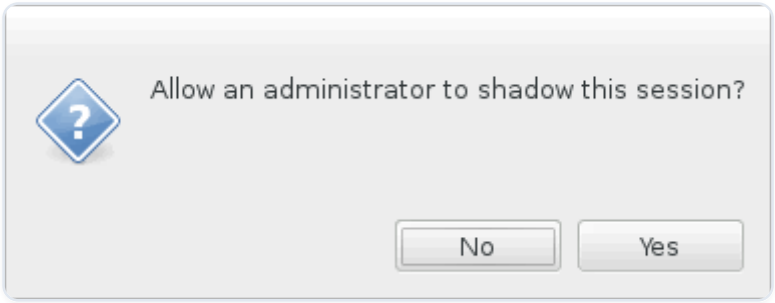
que el Linux VDA encuentre un certificado o un archivo de clave específicos y, por lo tanto, provocan un error de conexión con `Citrix Director`.

Uso

Desde `Citrix Director`, busque la sesión de destino y haga clic en **Shadow** en la vista **Session Details** para enviar una solicitud de shadowing al Linux VDA.



Una vez que se inicializa la conexión, aparece una confirmación en el cliente de sesión ICA (no en el cliente `Citrix Director`) para solicitar al usuario permiso para hacer shadowing de la sesión.



Si el usuario hace clic en **Yes**, aparece una ventana en el lado de `Citrix Director`, que indica que se está haciendo shadowing de la sesión ICA.

Para obtener más información sobre el uso, consulte la documentación de Citrix Director.

Limitaciones

- 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 ni controlarlas.
- Después de que un administrador haga clic en **Shadow** desde `Citrix Director`, aparece una confirmación para solicitar al usuario permiso para hacer shadowing de la sesión. Una sesión solo se puede sombrear cuando el usuario de la sesión da el permiso.
- La confirmación mencionada anteriormente tiene un límite de tiempo de espera de 20 segundos. Una solicitud de shadowing falla cuando se agota el tiempo.
- Una sesión solo puede ser objeto de shadowing por un único administrador. Por ejemplo, si el administrador B envía una solicitud de shadowing para una sesión de la que el administrador A está haciendo shadowing, 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 posterior.
- Un cliente `Citrix Director` utiliza un FQDN en lugar de una dirección IP para conectarse al servidor VDA de Linux de destino. Por lo tanto, el cliente `Citrix Director` debe poder resolver el FQDN del servidor VDA de Linux.

Solución de problemas

Si el shadowing de sesión falla, depure tanto en el cliente `Citrix Director` como en el VDA de Linux.

En el cliente de Citrix Director

A través de las herramientas de desarrollador del navegador, compruebe los registros de salida en la pestaña **Console**. O bien, compruebe la respuesta de la API ShadowLinuxSession en la pestaña **Network**. Si aparece la confirmación para obtener el permiso del usuario pero la conexión falla, 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 VDA de Linux

verificar que la confirmación para obtener el permiso del usuario aparece en respuesta a una solicitud de shadowing. Si no es así, compruebe los archivos vda.log y hdx.log en busca de pistas. Para obtener el archivo vda.log, haga lo siguiente:

1. Busque el archivo /etc/xdl/ctx-vda.conf. Quite el comentario de la siguiente línea para habilitar la configuración de vda.log:

   `Log4jConfig="/etc/xdl/log4j.xml"`

2. Abra /etc/xdl/log4j.xml, localice la parte com.citrix.dmc y cambie "info" a "trace" de la siguiente manera:

```
<!-- Broker Agent Plugin - Director VDA plugin Logger -->

 <logger name="com.citrix.dmc">

   <level value="trace"/>

 </logger>
```

3. Ejecute el comando `service ctxvda restart` para reiniciar el servicio `ctxvda`.

Si hay un error durante el establecimiento de la conexión:

1. Compruebe si hay alguna limitación del firewall que impida que el shadowing de sesión abra el puerto.
2. verificar que ha nombrado los certificados y los archivos de clave correctamente y los ha colocado en la ruta correcta si se trata del escenario SSL.
3. verificar que quedan suficientes puertos entre 6001 y 6099 para nuevas solicitudes de shadowing.

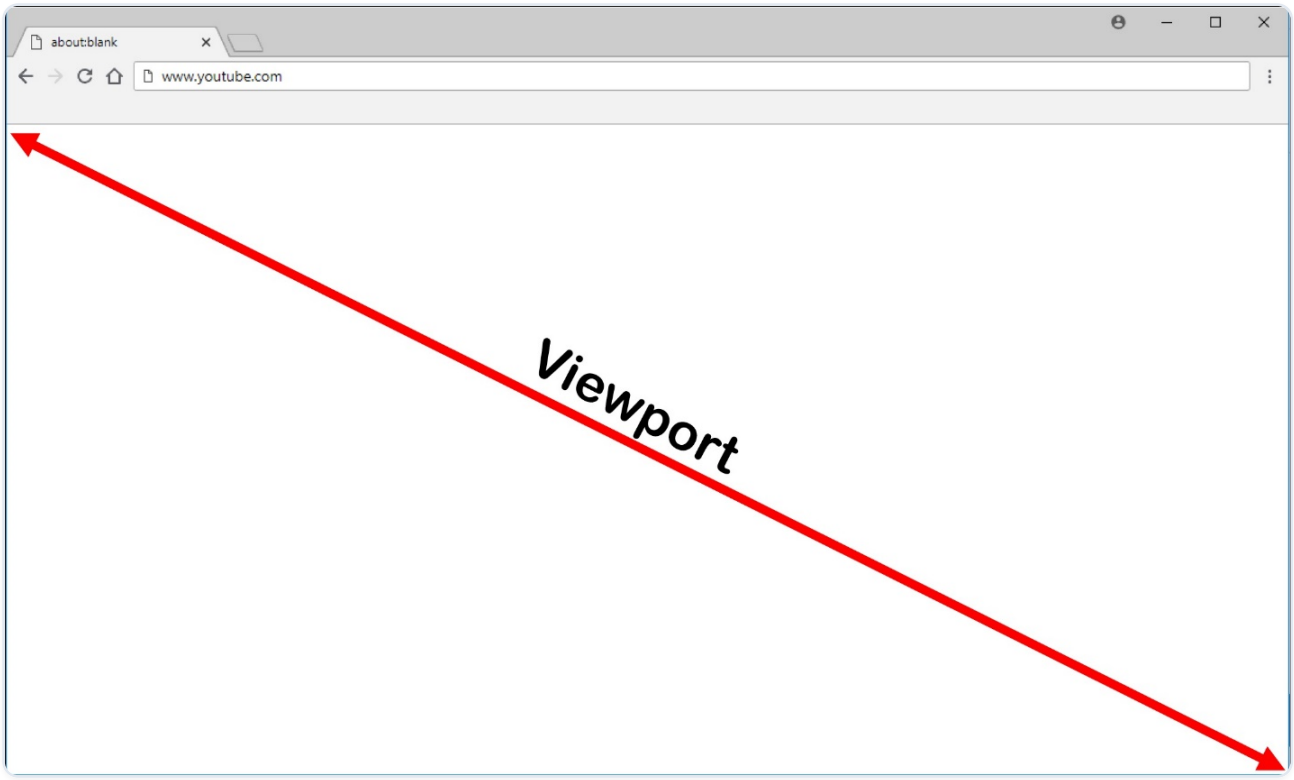
Redirección de contenido del navegador

Información general

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. 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:**
>
> Puede especificar qué páginas web se redirigen al lado del cliente mediante una lista de permitidos. Por el contrario, puede especificar qué páginas web no se redirigen al lado del cliente mediante una lista de bloqueados.
>
> Este motor de diseño web superpuesto se ejecuta en el cliente en lugar de en el VDA y utiliza la CPU, la GPU, la RAM y la red del cliente.

Solo se redirige la ventana gráfica del explorador. La ventana gráfica es el área rectangular del explorador 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 explorador del VDA.



Requisitos del sistema

Cliente Windows:

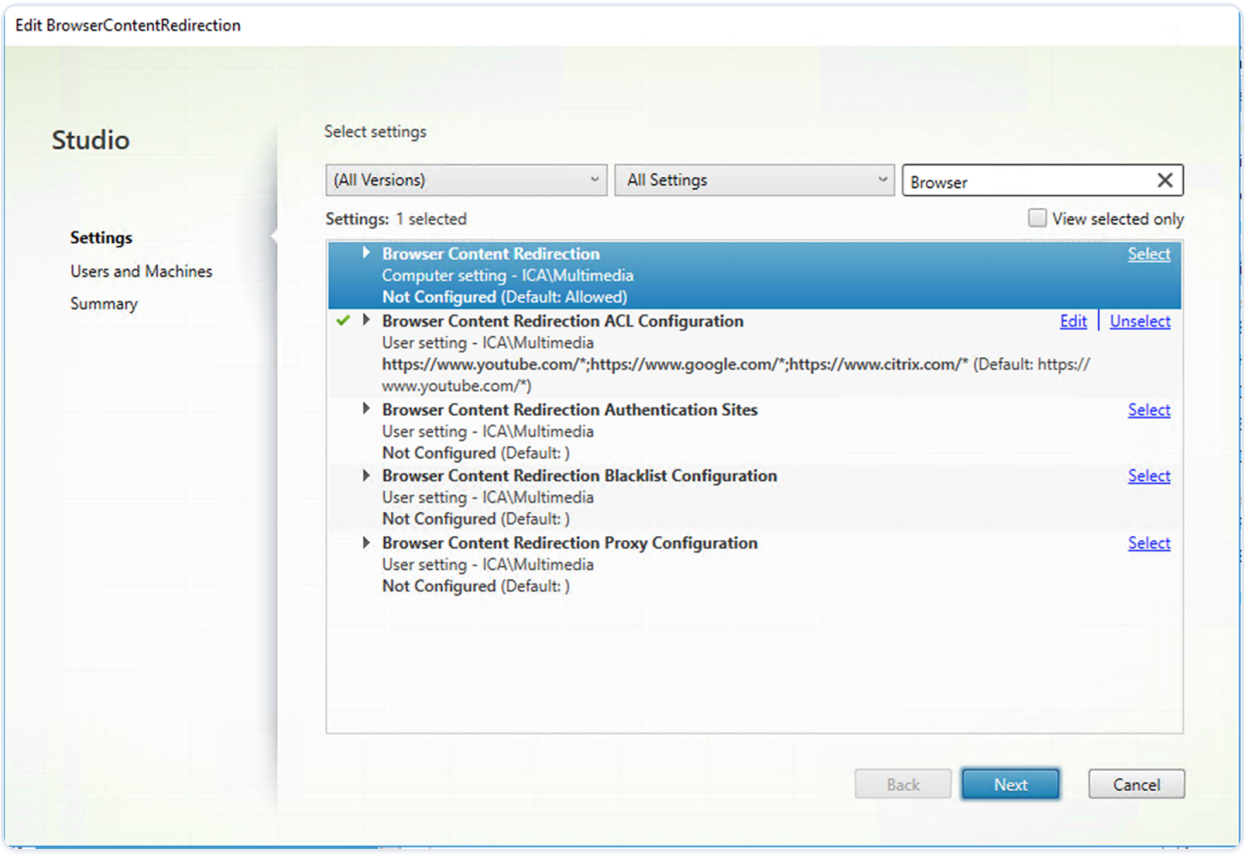
- Citrix Workspace app 1809 para Windows o posterior

VDA de Linux:

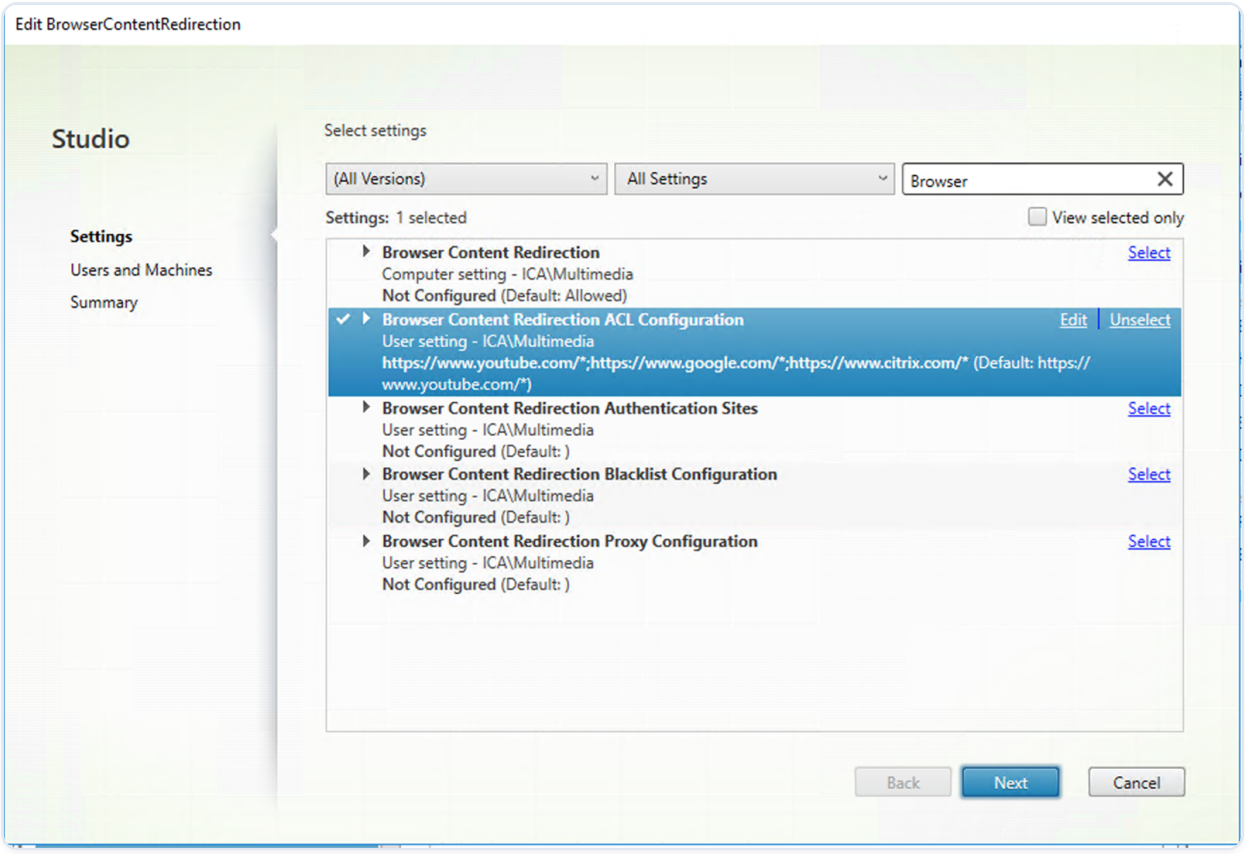
- Sistema operativo VDA: Ubuntu 16.04, Ubuntu 18.04, RHEL 7.8, RHEL 8.2, RHEL 8.1, SLES 12.5
- Explorador en el VDA: Google Chrome v66 o posterior con la extensión de redirección de contenido del explorador de Citrix® agregada

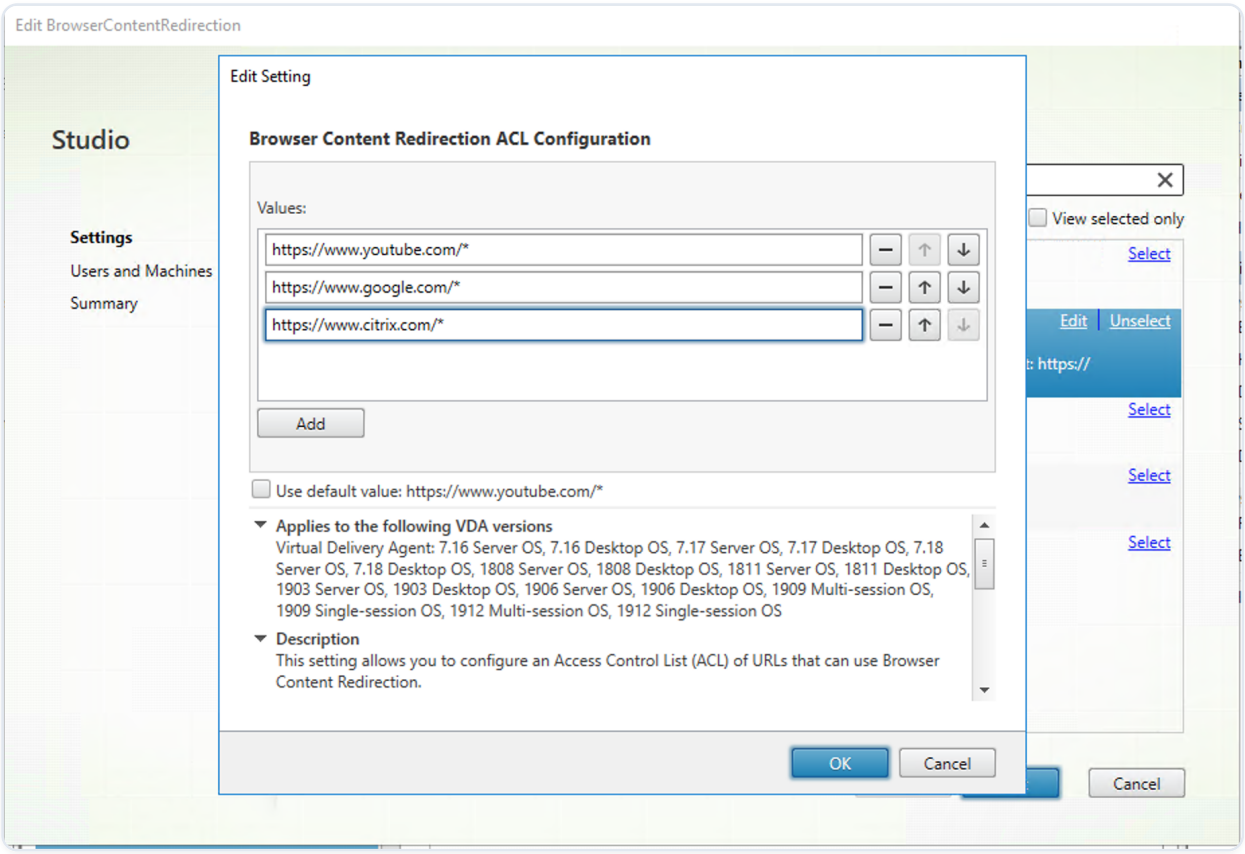
Configurar la redirección de contenido del explorador

1. En Citrix Studio, configure una directiva que especifique una lista de permitidos de URL que pueden usar la redirección de contenido del explorador y una lista de bloqueados de URL que no pueden. La redirección de contenido del explorador está establecida en **Permitido** de forma predeterminada.

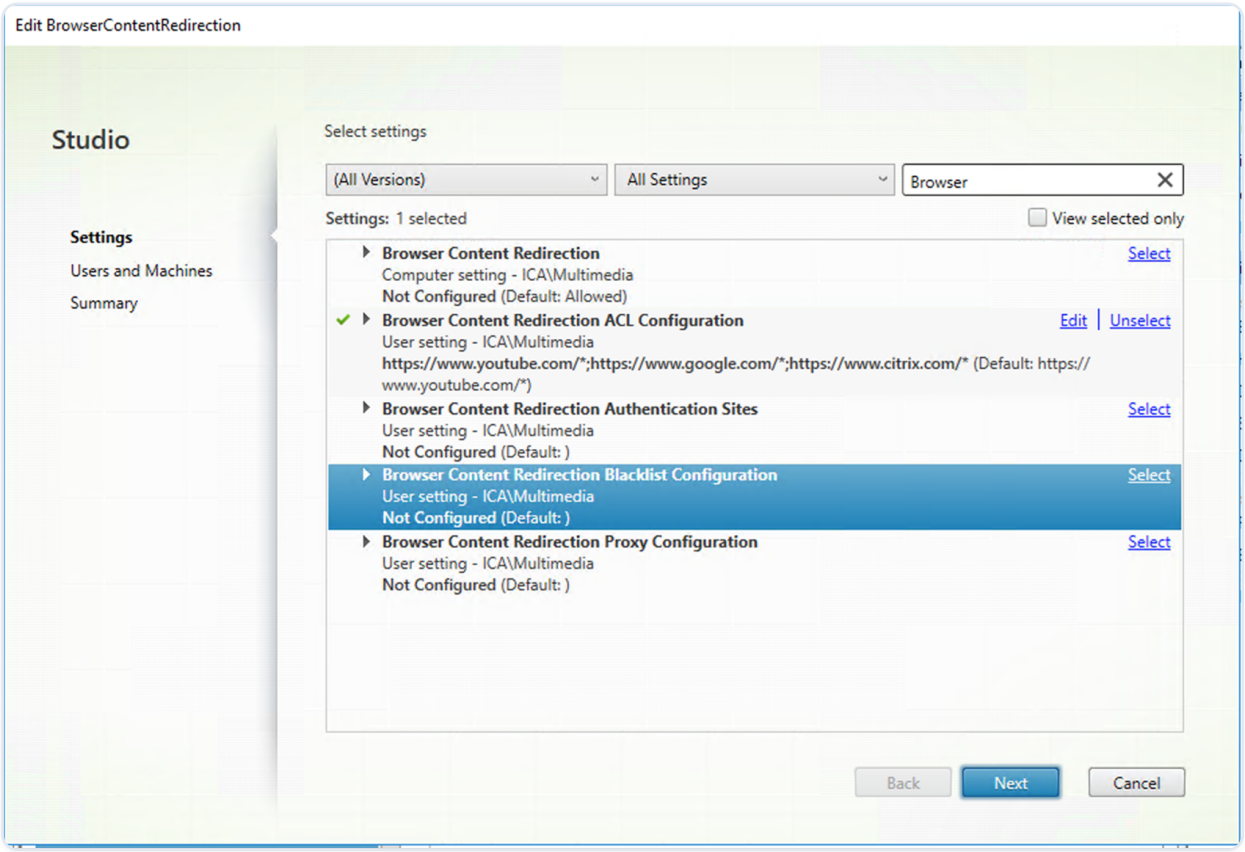


La configuración **Configuración de ACL de redirección de contenido del explorador** especifica una lista de permitidos de URL que pueden usar la redirección de contenido del explorador.





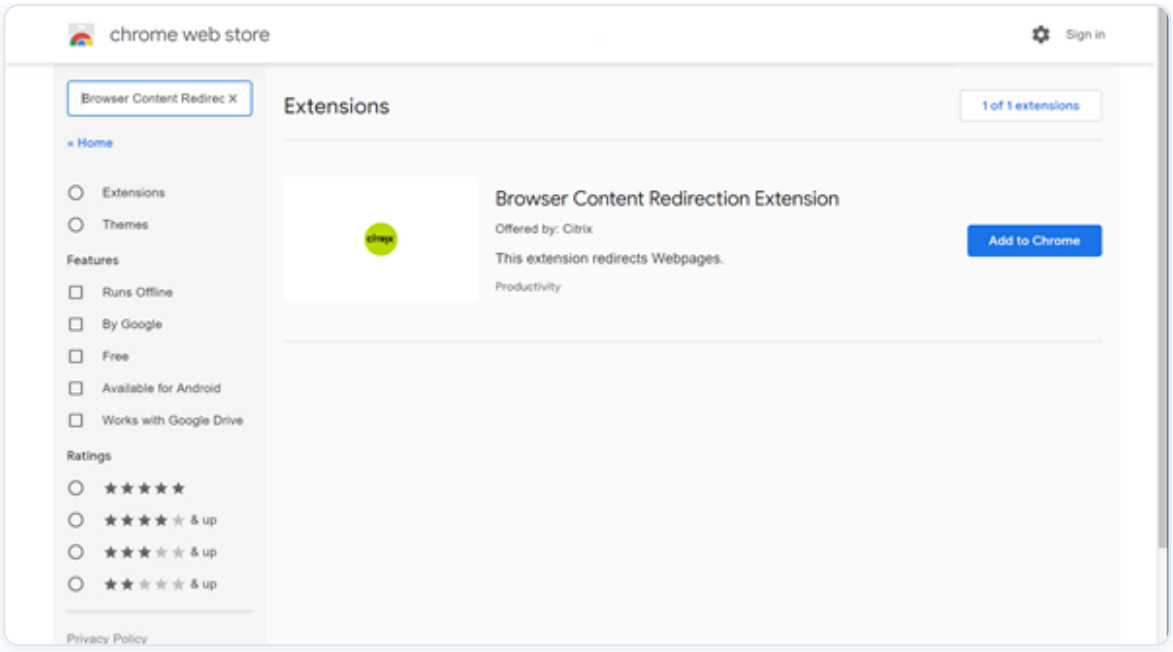
La configuración **Browser Content Redirection Blacklist Configuration** especifica una lista de bloqueo de URL que no pueden usar la redirección de contenido del navegador.



> **Nota:**
>
> Actualmente, el Linux VDA no admite la configuración **Browser Content Redirection Proxy Configuration**.

2. Para que el navegador del VDA detecte si una URL (a la que se está navegando) coincide con una lista de permitidos o una lista de bloqueo, agregue la extensión de redirección de contenido del navegador de Citrix desde Chrome Web Store. Haga clic en **Añadir a Chrome** en el VDA.

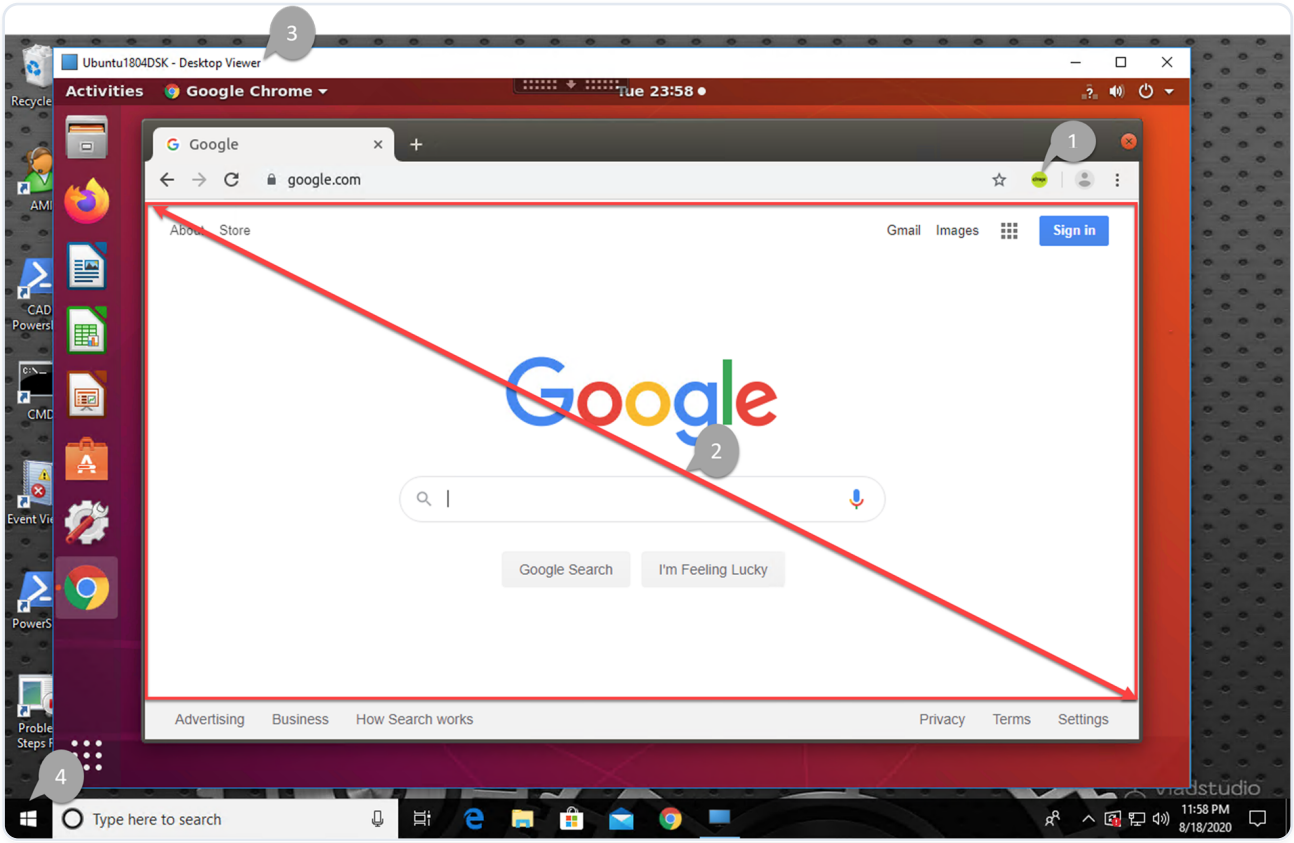
> **Importante:**
>
> La extensión no es necesaria en el cliente. Agréguela solo en el VDA.
>
> \>
>
> Las extensiones de Chrome se instalan por usuario. No es necesario actualizar una imagen dorada para agregar o quitar una extensión.



Si se encuentra una coincidencia con una URL en una lista de permitidos (por ejemplo, `https://www.mycompany.com/`) 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. A continuación, la aplicación Citrix Workspace crea una instancia de 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

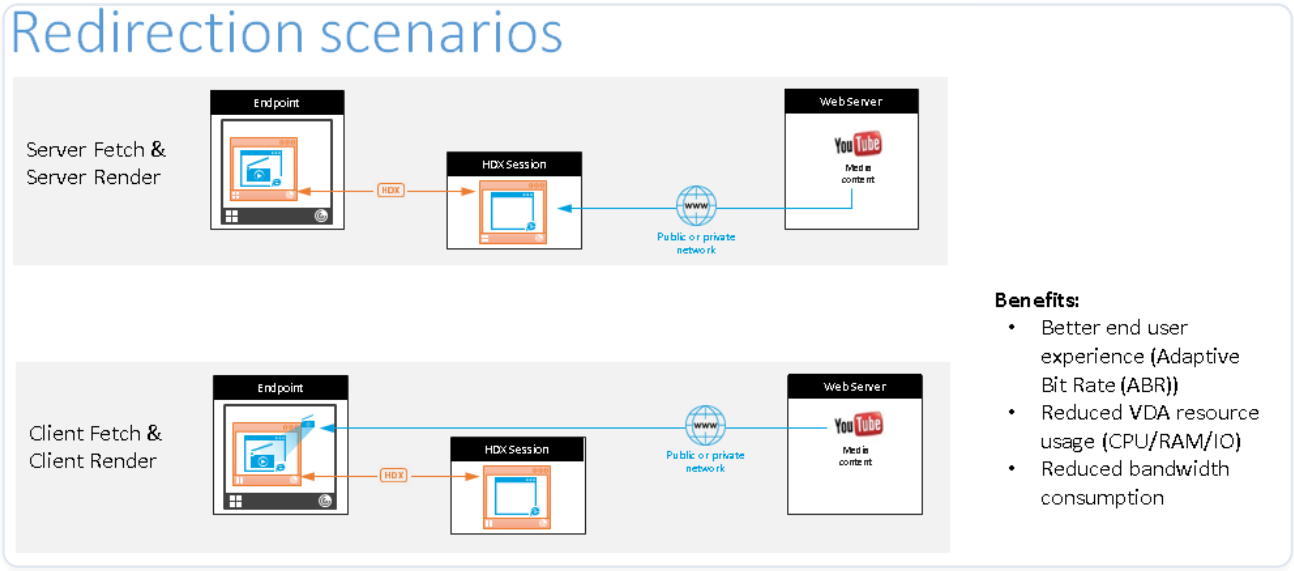
   El color del icono de la extensión especifica el estado de la extensión de Chrome. Es uno de los tres colores:

   - Verde: Activo y conectado
   - Gris: Inactivo/sin actividad en la ficha 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

Escenarios de redirección

Aquí hay escenarios de cómo la aplicación Citrix Workspace obtiene contenido:



- **Captura y representación en el servidor:** No hay redirección porque no agregó el sitio a la lista de permitidos o la redirección falló. Volvemos a representar la página web en el VDA y usamos Thinwire para la transmisión remota de 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.
- **Captura y representación en el cliente:** Como la aplicación Citrix Workspace se comunica 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™.

Mecanismo de reserva

Puede haber ocasiones en las que la redirección del cliente falle. Por ejemplo, si la máquina cliente no tiene acceso directo a Internet, es posible que se envíe una respuesta de error al VDA. En tales casos, el explorador del VDA puede volver a cargar y representar la página en el servidor.

Soporte para la aplicación Citrix Workspace™ para HTML5

A partir de esta versión, puede usar la aplicación Citrix Workspace para HTML5 para acceder directamente a las aplicaciones y escritorios virtuales de 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 el procedimiento detallado, consulte el Paso 1 del artículo de Knowledge Center CTX208163.

2. Habilitar 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 sesiones de usuario con TLS.

Supervisar máquinas virtuales Linux y sesiones Linux

La siguiente tabla enumera algunas métricas disponibles para máquinas virtuales Linux y sesiones Linux.

MÉTRICA	VERSIÓN MÍNIMA DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
Duración del inicio de sesión	2109	Es una medida del proceso de inicio de sesión desde el momento en que un usuario se conecta desde la aplicación Citrix Workspace	Disponible solo en Monitor.

MÉTRICA	VERSIÓN MÍNIMA DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		hasta el momento en que una sesión está lista para usarse. Para ver la métrica de una sesión, vaya a la ficha Monitor del servicio Citrix Virtual Apps and Desktops. Monitor está disponible como la consola de Director para supervisar y solucionar problemas de implementaciones de Citrix Virtual Apps and Desktops Current Release y LTSR. En la ficha Monitor, haga clic en **Ver tendencia histórica** en la sección **Duración media del inicio de sesión**. En la página **Rendimiento del inicio de sesión**, establezca las condiciones del filtro y haga clic en **Aplicar** para visualizar las métricas.	
Recuento de reconexiones automáticas de sesión	2109	Para ver el número de reconexiones automáticas en una sesión, acceda a la vista **Tendencias**.	Disponible tanto en Citrix Director como en Monitor.

MÉTRICA	VERSIÓN MÍNIMA DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		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 número de reconexiones automáticas en una sesión. 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 directiva de reconexión automática de clientes y Configuración de	

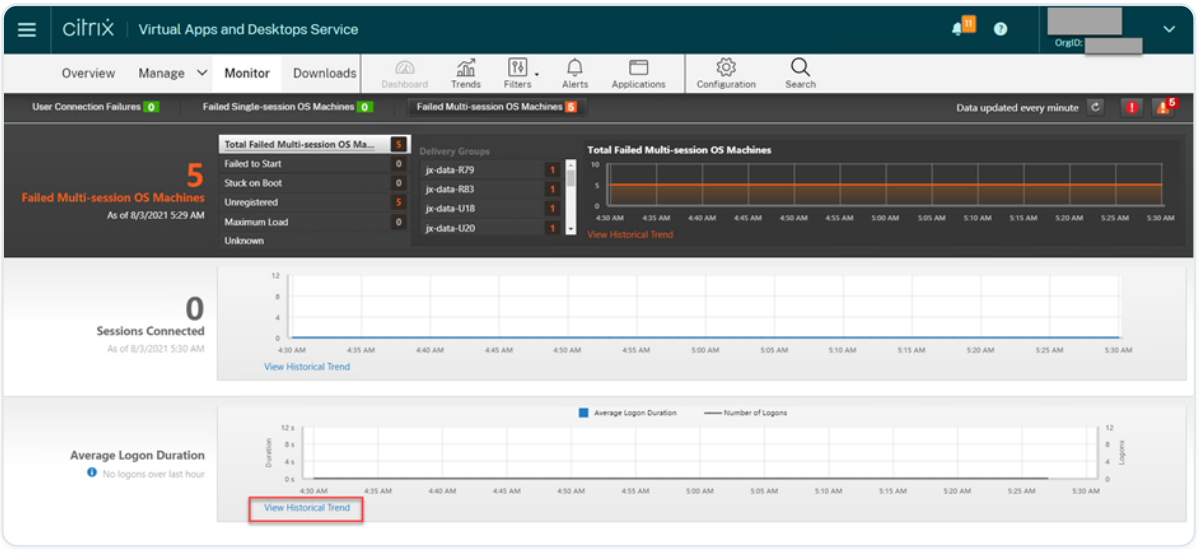
MÉTRICA	VERSIÓN MÍNIMA DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		directiva de fiabilidad de la sesión	
Tiempo de inactividad	2103	Para acceder a esta métrica, abra la página **Todas las sesiones** seleccionando **Filtros > Sesiones > Todas las sesiones**.	Disponible tanto en Citrix Director como en Monitor.
Métricas de una máquina virtual Linux	2103	Las siguientes métricas están disponibles para las máquinas virtuales Linux: número de núcleos de CPU, tamaño de la memoria, capacidad del disco duro y utilización actual e histórica de CPU y memoria.	Disponible tanto en Citrix Director como en Monitor.
Protocolo	1909	El protocolo de transporte de una sesión de Linux aparece como UDP o TCP en el panel **Detalles de la sesión**.	Disponible tanto en Citrix Director como en 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.	Disponible tanto en Citrix Director como en Monitor.

MÉTRICA	VERSIÓN MÍNIMA DE VDA REQUERIDA	DESCRIPCIÓN	OBSERVACIONES
		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.	

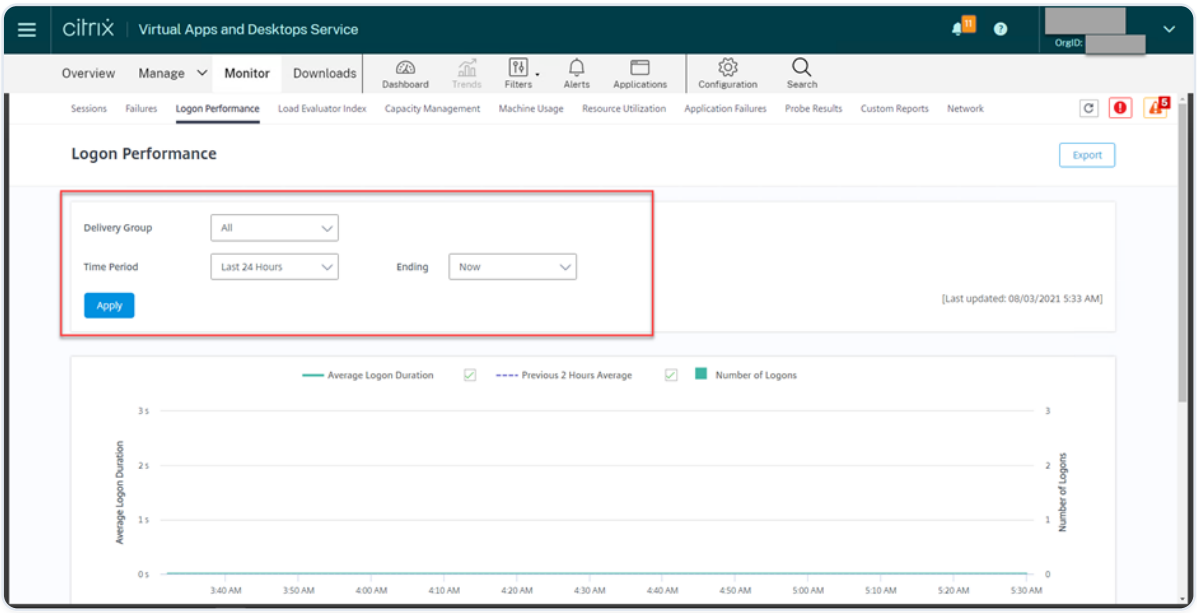
Ejemplos de cómo acceder a las distintas métricas en Citrix Director y Monitor

- Duración del inicio de sesión

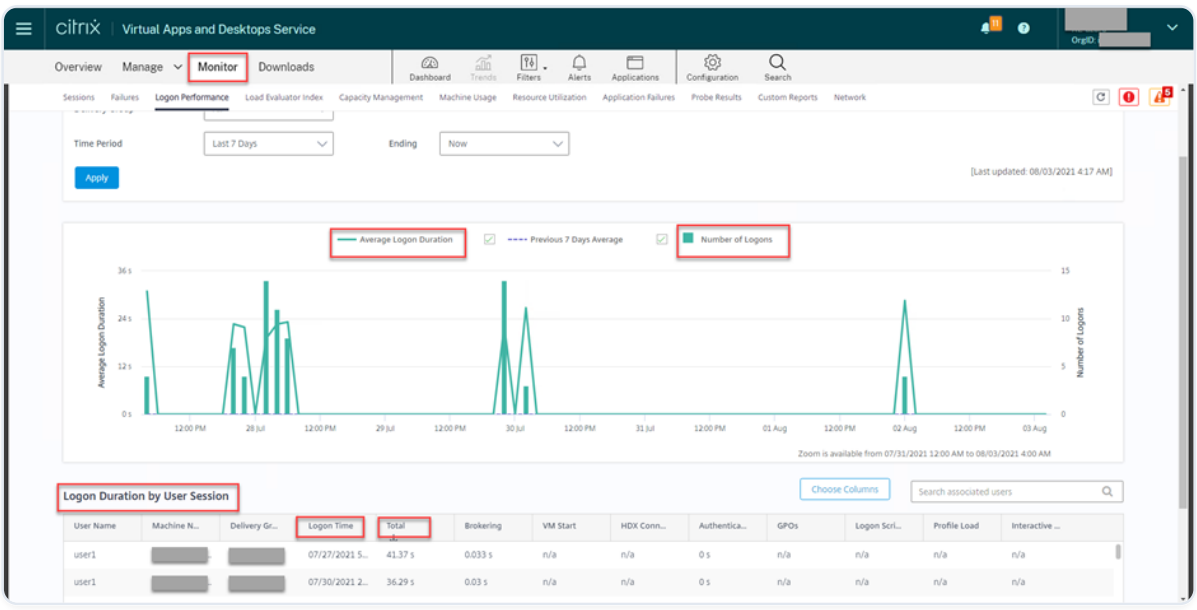
a. En la ficha Monitor del servicio Citrix Virtual Apps and Desktops, haga clic en **Ver tendencia histórica** en la sección **Duración media del inicio de sesión**.



b. En la página **Rendimiento de inicio de sesión**, establezca las condiciones del filtro.

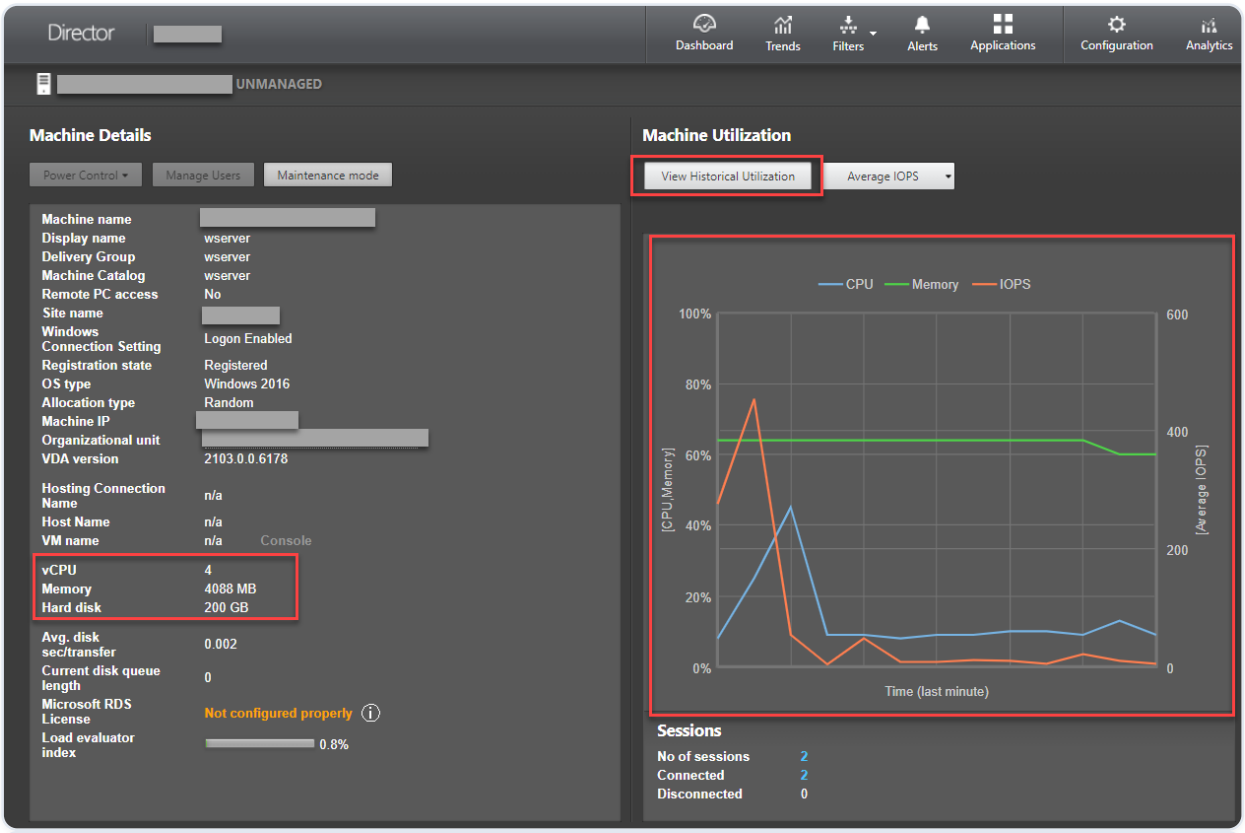


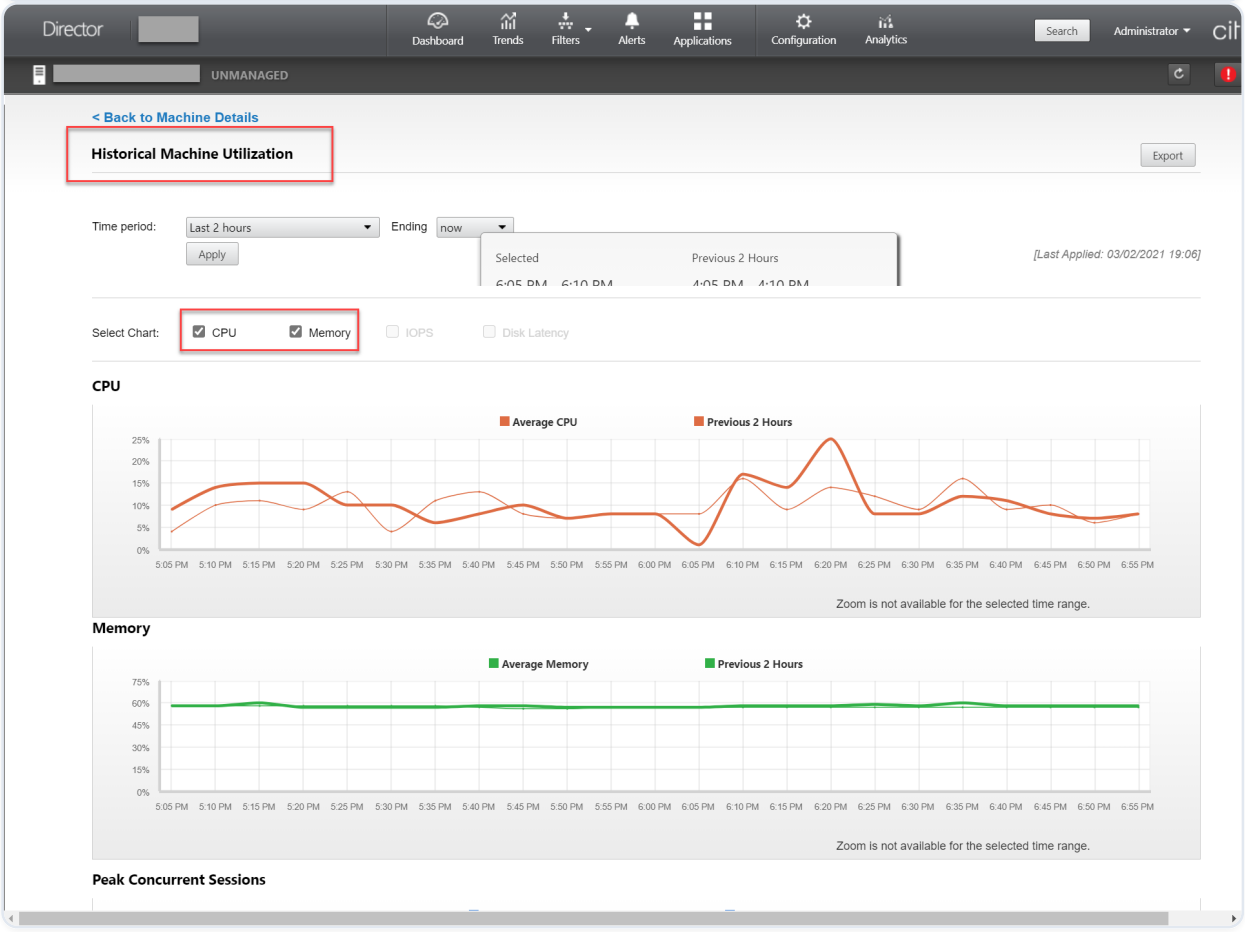
c. Haga clic en **Aplicar** para visualizar las métricas de duración del inicio de sesión.



- El número de núcleos de CPU, el tamaño de la memoria, la capacidad del disco duro y la utilización actual e histórica de CPU y memoria de una VM Linux

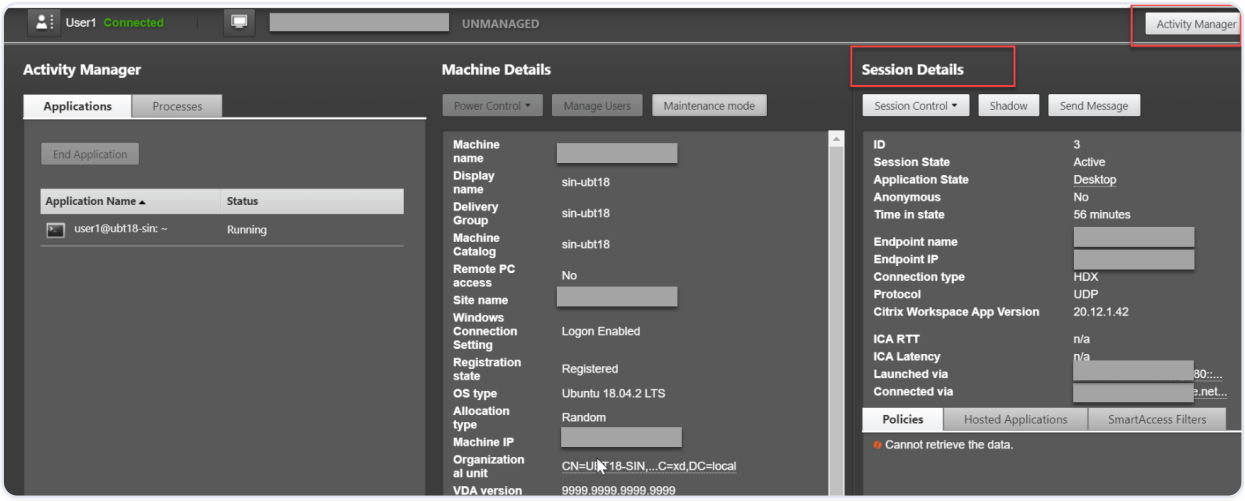
  Para acceder a estas métricas de una VM Linux, busque la VM en Citrix Director o Monitor y consulte el panel **Detalles de la máquina**. Por ejemplo:





- ICA RTT, Protocolo

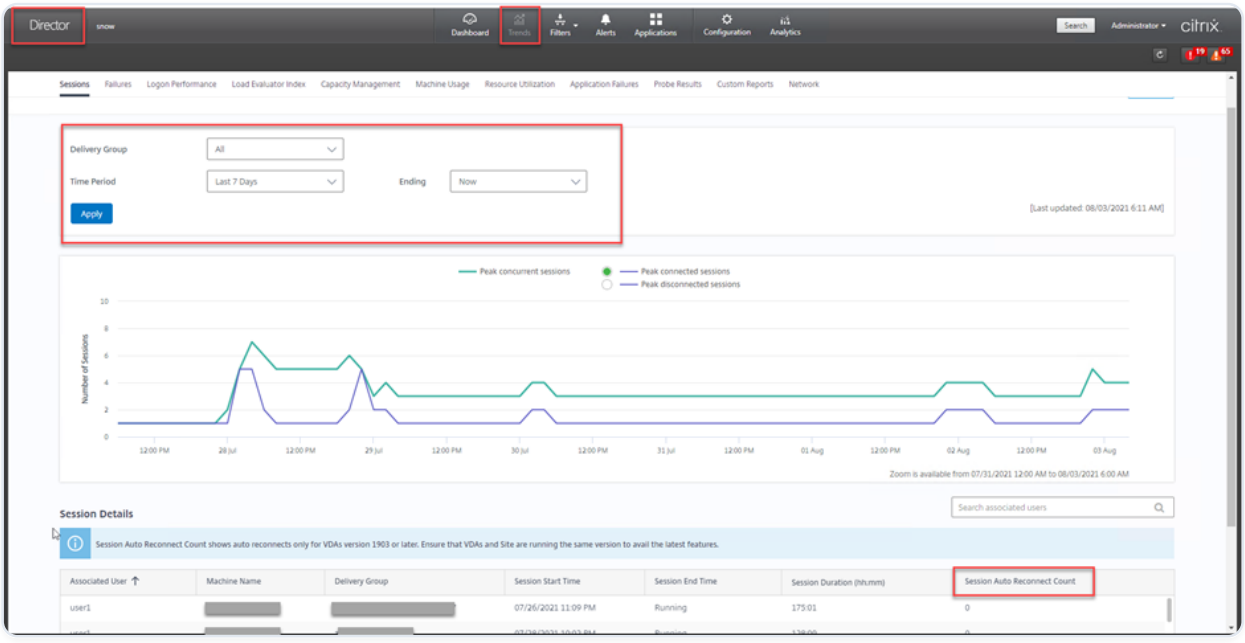
Para ver las métricas de una sesión Linux, abra la página **Todas las sesiones** seleccionando **Filtros > Sesiones > Todas las sesiones**, o acceda al panel **Detalles de la sesión**. Para acceder al panel **Detalles de la sesión**, abra la página **Todas las sesiones** y haga clic en una sesión de destino para acceder a su vista **Administrador de actividad**. Por ejemplo:



- Recuento de reconexiones automáticas de sesión

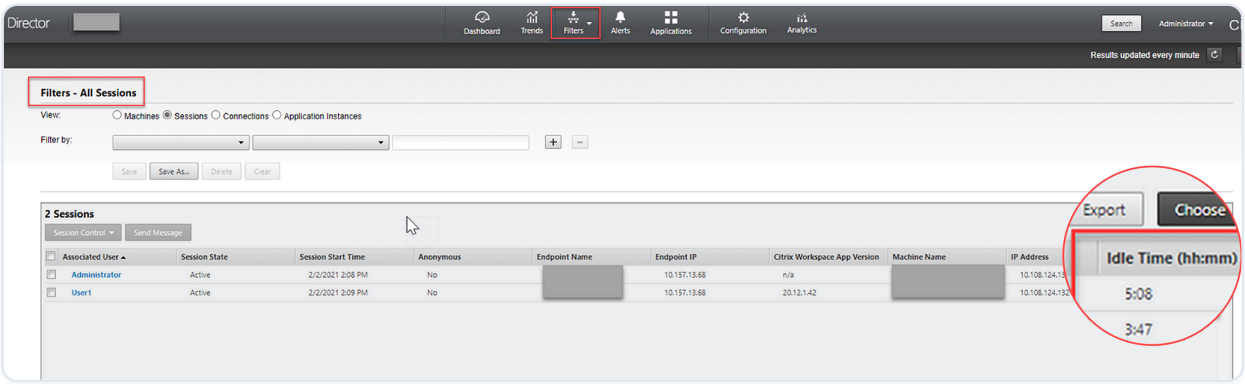
Para ver el número de reconexiones automáticas en una sesión, acceda a la vista **Tendencias**. Establezca las condiciones y haga clic en **Aplicar** para acotar los resultados de la búsqueda.

La columna **Recuento de reconexiones automáticas de sesión** muestra el número de reconexiones automáticas en una sesión. Por ejemplo:



- Tiempo de inactividad

Por ejemplo:



Demonio de servicio de monitorización

El demonio de servicio de monitorización supervisa los servicios clave mediante la realización de análisis periódicos. Cuando detecta excepciones, el demonio reinicia o detiene los procesos del servicio y limpia los residuos de los procesos para liberar recursos. Las excepciones detectadas se registran en el archivo **/var/log/xdl/ms.log**.

Configuración

El demonio de servicio de monitorización se inicia automáticamente cuando se inicia el VDA.

Puede configurar la función a través de los archivos **scanningpolicy.conf**, **rulesets.conf** y **whitelist.conf** con privilegios de administrador. Los archivos de configuración se encuentran en **/opt/Citrix/VDA/sbin**.

Para que los cambios en los archivos **scanningpolicy.conf**, **rulesets.conf** y **whitelist.conf** surtan efecto, ejecute el siguiente comando para reiniciar el demonio de servicio de monitorización.

```
service ctxmonitorservice restart
```

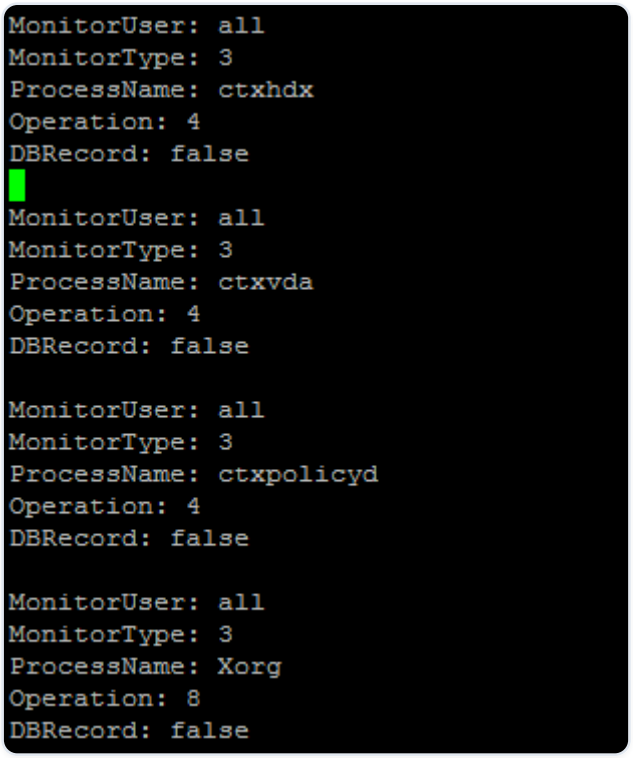
- **scanningpolicy.conf**

  Este archivo de configuración habilita o deshabilita el demonio de servicio de monitorización. Establece el intervalo de detección del servicio y especifica si se deben reparar las excepciones detectadas.

  - MonitorEnable: true/false (true de forma predeterminada)
  - DetectTime: 20 (unidad: segundos, valor predeterminado: 20, valor mínimo: 5)
  - AutoRepair: true/false (true de forma predeterminada)
  - MultBalance: falso
  - ReportAlarm: falso

- **rulesets.conf**

  Este archivo de configuración especifica los servicios de destino que se van a monitorizar. Hay cuatro servicios monitorizados de forma predeterminada, como se muestra en la siguiente captura de pantalla.



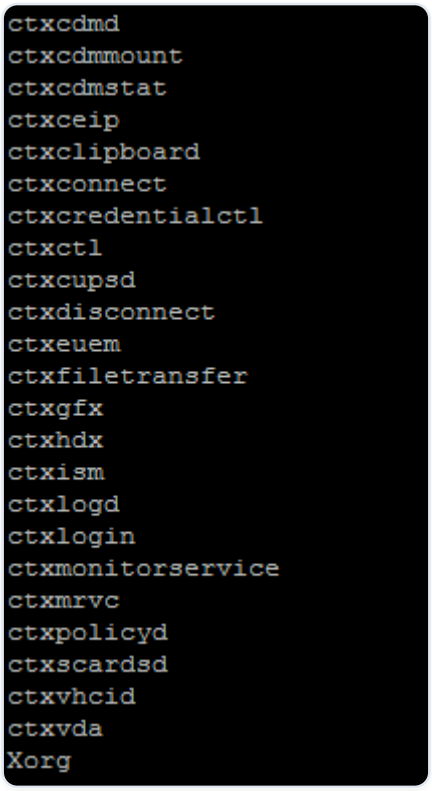
  Para configurar cada servicio a supervisar, establezca los siguientes campos.

  - MonitorUser: todos
  - MonitorType: 3
  - ProcessName: <> (El nombre del proceso no puede dejarse en blanco y debe coincidir exactamente.)
  - Operation: 1/2/4/8 (1 = detener el servicio cuando se detectan excepciones. 2 = finalizar el servicio cuando se detectan excepciones. 4 = reiniciar el servicio. 8 = limpiar los residuos del proceso Xorg.)
  - DBRecord: falso

- **whitelist.conf**

  Los servicios de destino especificados en el archivo **rulesets.conf** también deben configurarse en el archivo **whitelist.conf**. La configuración de la lista blanca es un filtro secundario de seguridad.

Para configurar la lista blanca, incluya solo los nombres de los procesos (que deben coincidir exactamente) en el archivo **whitelist.conf**. Para ver un ejemplo, consulte la siguiente captura de pantalla.



Nota:

Antes de detener los servicios `ctxvda`, `ctxhdx` y `ctxpolicyd`, ejecute el comando `service ctxmonitorservice stop` para detener el demonio del servicio de supervisión. De lo contrario, el demonio del servicio de supervisión reiniciará los servicios que haya detenido.

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 proteger las sesiones de usuario, 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` del 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 los certificados raíz se deben instalar en cada servidor y cliente Linux VDA.

Habilitar el cifrado TLS en el Controller

> **Nota:**
>
> Puede habilitar el cifrado TLS solo para grupos de entrega completos. No puede habilitar el cifrado TLS para aplicaciones específicas.

> En una ventana de PowerShell en el 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`

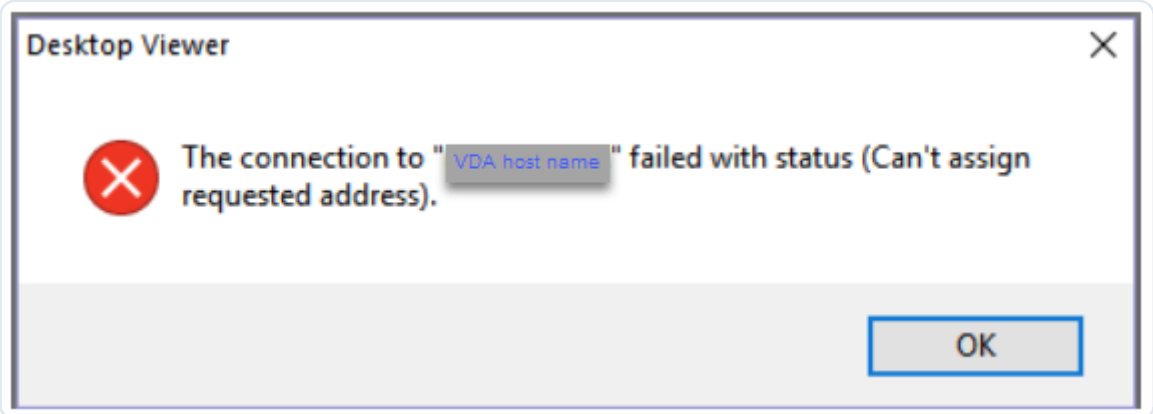
> **Nota:**
>
> Para asegurarse de que solo los FQDN de VDA estén contenidos en un archivo de sesión ICA®, también puede ejecutar el comando `Set-BrokerSite –DnsResolutionEnabled $true`. El comando habilita la resolución DNS. Si deshabilita la resolución DNS, un archivo de sesión ICA revela las direcciones IP de VDA y proporciona FQDN solo para los elementos relacionados con TLS, como `SSLProxyHost` y `UDPDTLSPort`.

> Para deshabilitar 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

Puede producirse el siguiente error "Can't assign requested address" en la aplicación Citrix Workspace™ para Windows cuando intente acceder a una sesión de escritorio publicada:



Como solución alternativa, agregue una entrada al archivo **hosts**, similar a:

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

En máquinas Windows, el archivo **hosts** se encuentra normalmente en `C:\Windows\System32\drivers\etc\hosts`.

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 habilitada en Linux VDA. Para obtener más información, consulte Transport Layer Security.

Habilitar el cifrado DTLS

verificar que el transporte adaptativo está habilitado

En Citrix Studio, verificar que la directiva **HDX™ Adaptive Transport** esté establecida en **Preferred** o **Diagnostic mode**.

Habilitar el cifrado SSL en Linux VDA

En Linux VDA, utilice la herramienta `enable_vdassl.sh` para habilitar (o inhabilitar) el cifrado SSL. La herramienta se encuentra en **/opt/Citrix/VDA/sbin**. Para obtener información sobre las opciones disponibles en la herramienta, ejecute el comando `/opt/Citrix/VDA/sbin/enable_vdassl.sh –h`.

> **Nota:**

> Actualmente, Linux VDA admite DTLS 1.0 y DTLS 1.2. DTLS 1.2 requiere Citrix Receiver para Windows 4.12, o Citrix Workspace app 1808 para Windows o posterior. Si su cliente solo admite DTLS 1.0 (por ejemplo, Citrix Receiver para Windows 4.11), establezca `SSLMinVersion` en `TLS_1.0` y `SSLCipherSuite` en `COM` o `ALL` mediante la herramienta `enable_vdassl.sh`.

Marca de agua de sesión basada en texto

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 quienes utilizan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto, que se muestra sobre toda la pantalla de la sesión sin cambiar el contenido del documento original.

> **Importante:**

> Las marcas de agua de sesión basadas en texto no son una función de seguridad. La solución no evita completamente el robo de datos, pero proporciona cierto nivel de disuasión y trazabilidad. No garantizamos la trazabilidad completa de la información al utilizar esta función. Sin embargo, le recomendamos que combine esta función con otras soluciones de seguridad según corresponda.

> La marca de agua de sesión es texto y se aplica a la sesión que se entrega al usuario. La marca de agua de sesión contiene información para rastrear el robo de datos. Los datos más importantes son la identidad del usuario que inició sesión en la sesión actual en la que se tomó la imagen de la pantalla. Para rastrear la fuga de datos de forma más eficaz, incluya otra información, como la dirección IP del servidor o del cliente y la hora de conexión.

Para ajustar la experiencia del usuario, utilice la (/es-es/citrix-virtual-apps-desktops/policies/reference/ica-policy-settings/session-watermark-policy-setting.html) para configurar la ubicación y la apariencia de la marca de agua en la pantalla.

Limitaciones

- Las marcas de agua de sesión no son compatibles 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 es compatible 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).
- Las marcas de agua no son visibles para el shadowing de sesiones.
- Si pulsa la tecla Imprimir pantalla para capturar una pantalla, la pantalla capturada en el lado del VDA no incluye las marcas de agua. Le recomendamos que tome medidas para evitar que se copien las capturas de pantalla.

Soporte para tarjetas inteligentes

Puede usar una tarjeta inteligente conectada al dispositivo cliente para la autenticación al iniciar sesión en una sesión de escritorio virtual 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 y 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.

Requisitos previos

La disponibilidad de la autenticación de paso de tarjeta inteligente depende de las siguientes condiciones:

- Su VDA de Linux está instalado en una de las siguientes distribuciones:
  - RHEL 8
  - RHEL 7/CentOS 7
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Ubuntu 16.04
  - Debian 10.9

  Después de completar la instalación del VDA, verificar que su VDA puede registrarse con el Delivery Controller™ y que puede abrir las sesiones de escritorio Linux publicadas con 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.
- Se utiliza la aplicación Citrix Workspace™ para Windows.

Asegúrese de que OpenSC sea compatible con su tarjeta inteligente

OpenSC es un controlador de tarjeta inteligente muy utilizado en RHEL 7.4+. Como reemplazo totalmente compatible de CoolKey, OpenSC admite muchos tipos de tarjetas inteligentes (consulte Compatibilidad con tarjetas inteligentes en Red Hat Enterprise Linux).

En este artículo, la tarjeta inteligente YubiKey 4 se utiliza como ejemplo para ilustrar la configuración. YubiKey 4 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 4.



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

Preparar un certificado raíz

Se utiliza un certificado raíz para verificar el certificado de la tarjeta inteligente. Siga los pasos a continuación 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>`.

Compilar el módulo pam_krb5 en RHEL 8

La autenticación con tarjeta inteligente depende del módulo pam_krb5, que está obsoleto en RHEL 8. Para usar la autenticación con tarjeta inteligente en RHEL 8, compile el módulo pam_krb5 de la siguiente manera:

1. Descargue el código fuente de pam_krb5-2.4.8-6 de `<https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html>`.
2. Compile e instale el módulo pam_krb5 en RHEL 8.

```
yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools

yum install gcc krb5-devel pam-devel autoconf libtool

rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio –div

tar xvzf pam_krb5-2.4.8.tar.gz

cd pam_krb5-2.4.8

./configure --prefix=/usr

make

make install
```

3. verificar que pam_krb5.so existe en /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
```

Configurar el entorno de la tarjeta inteligente

Puede usar el script ctxsmartlogon.sh para configurar el entorno de la tarjeta inteligente o completar la configuración manualmente.

(Opción 1) Usar el script ctxsmartlogon.sh para configurar el entorno de la tarjeta inteligente

> **Nota:**

> El script ctxsmartlogon.sh agrega información PKINIT al dominio predeterminado. Puede cambiar esta configuración a través del archivo de configuración **/etc/krb5.conf**.

> Antes de usar 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.

```
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.
```

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 la 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, los Servicios de información de Internet, Citrix StoreFront y la aplicación Citrix Workspace. Para obtener información sobre la configuración basada en la tarjeta inteligente YubiKey 4, consulte el artículo de Knowledge Center CTX206156.

Antes de pasar al siguiente paso, asegúrese de haber configurado correctamente todos los componentes, de haber descargado la clave privada y el certificado de usuario en la tarjeta inteligente, y de poder iniciar sesión correctamente en el VDA de Windows mediante la tarjeta inteligente.

INSTALAR LOS PAQUETES PC/SC LITE

PCSC Lite es una implementación de la especificación Personal Computer/Smart Card (PC/SC) en Linux. Proporciona una interfaz de tarjeta inteligente de Windows para comunicarse con tarjetas inteligentes y lectores. La redirección de tarjetas inteligentes en Linux VDA se implementa a nivel de PC/SC.

Ejecute el siguiente comando para instalar los paquetes PC/SC Lite:

RHEL 7/CentOS 7, RHEL 8:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04, Debian 10.9:

```
apt-get install -y libpcsclite1 libccid
```

INSTALAR EL CONTROLADOR DE TARJETA INTELIGENTE

OpenSC es un controlador de tarjeta inteligente muy utilizado. Si OpenSC no está instalado, ejecute el siguiente comando para instalarlo:

RHEL 7/CentOS 7, RHEL 8:

```
yum install opensc
```

Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04, Debian 10.9:

```
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 7/CentOS 7:

```
yum install pam_krb5 krb5-pkinit
```

RHEL 8:

```
yum install krb5-pkinit
```

Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04:

```
apt-get install libpam-krb5 krb5-pkinit
```

Debian 10.9:

```
apt-get install -y libpam-krb5 krb5-pkinit
```

El módulo pam_krb5 es un módulo de autenticación conectable que las aplicaciones compatibles con PAM pueden usar 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 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:

regla-de-componente …

donde `relation-operator` puede ser `&&`, lo que significa que todas las reglas de componente 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 es similar 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 agregar pam_krb5 como módulo de autenticación, agregue 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 es similar 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

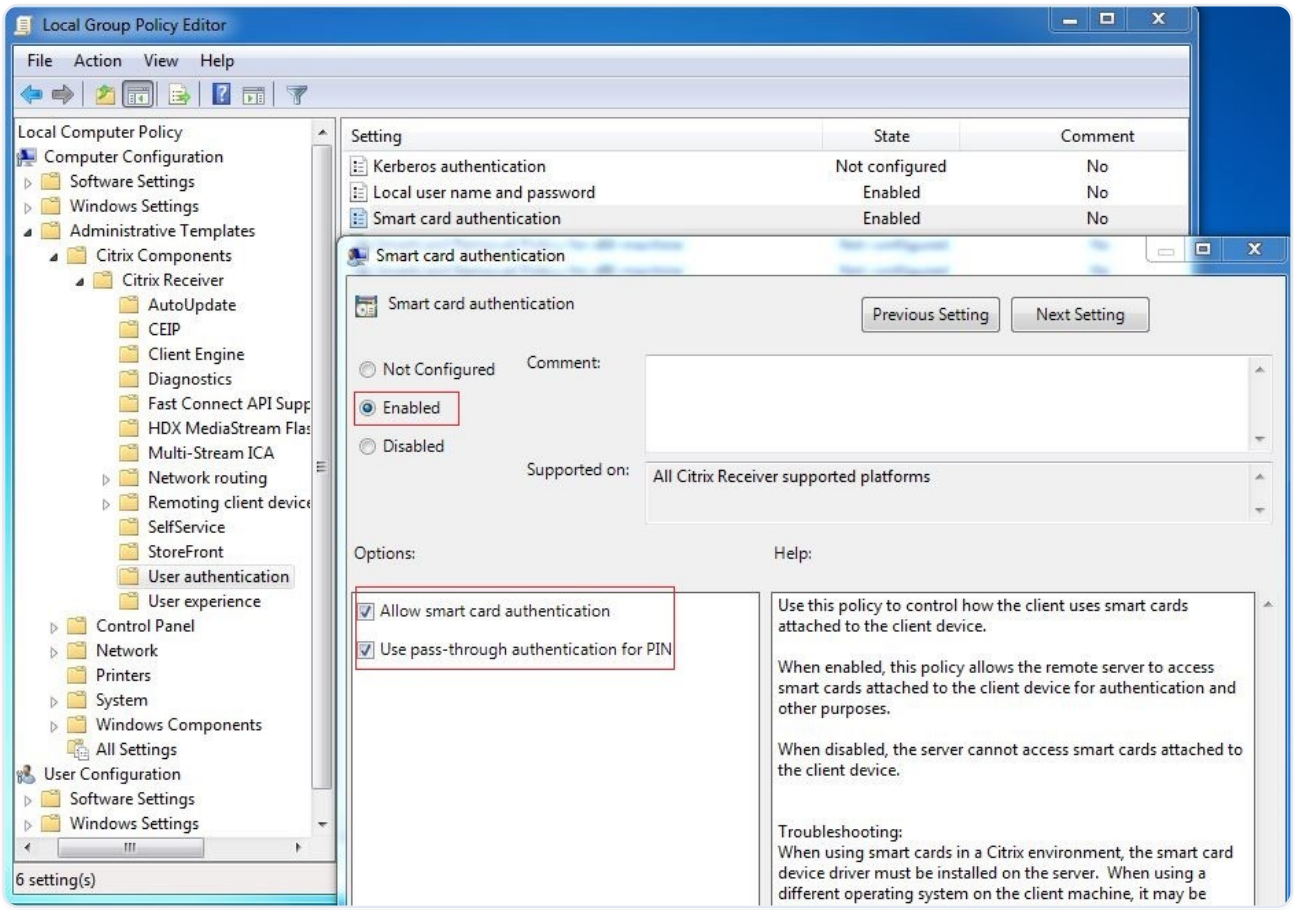
account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
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 inicios de escritorios y aplicaciones virtuales. 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 VDA de Linux 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

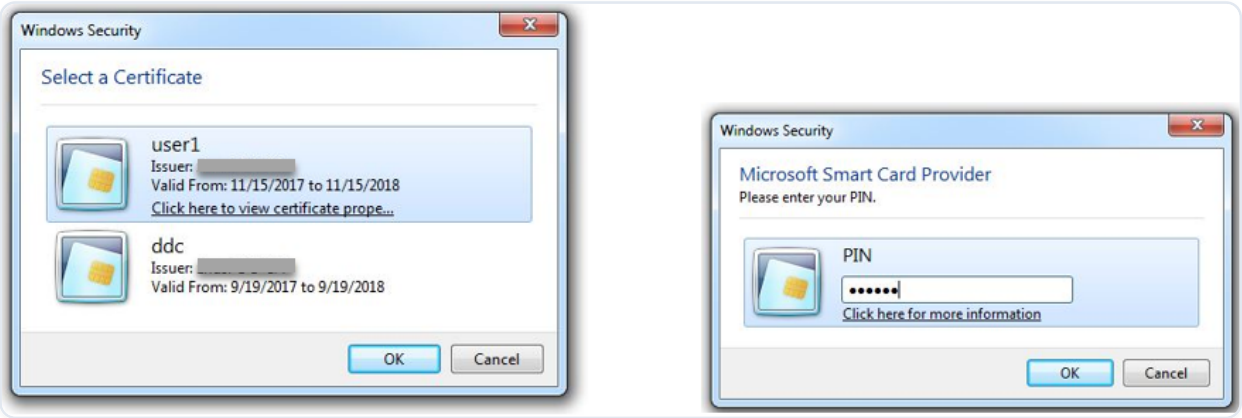
Para deshabilitar el inicio de sesión rápido con tarjeta inteligente en el cliente, elimine el parámetro **SmartCardCryptographicRedirection** del archivo default.ica del sitio de StoreFront asociado.

Uso

Iniciar sesión en el VDA de Linux mediante una tarjeta inteligente

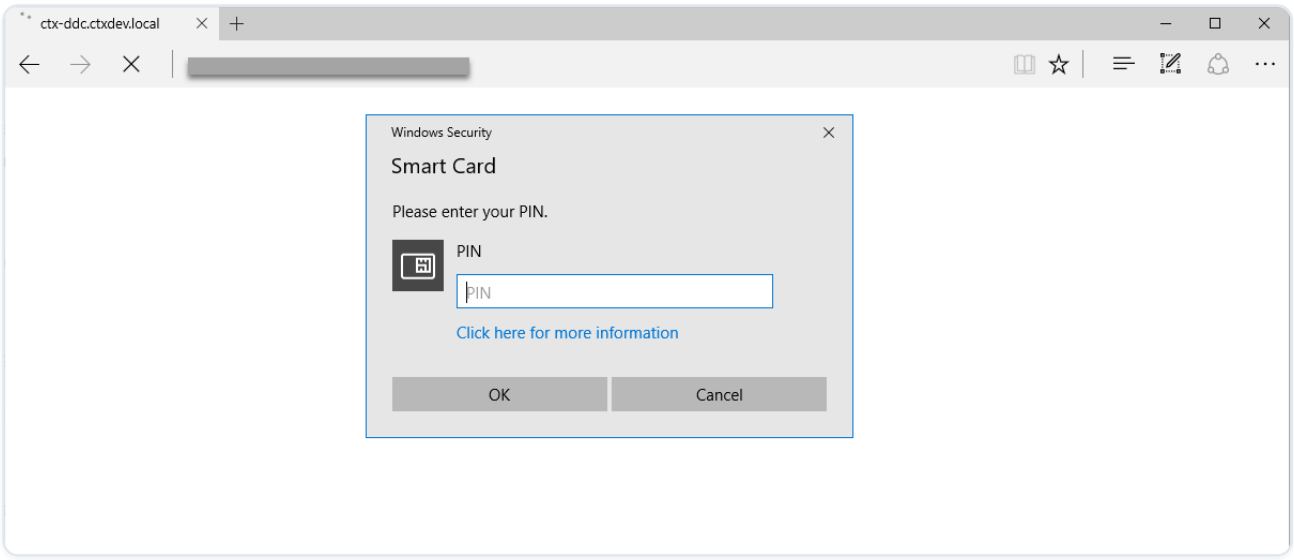
Puede usar una tarjeta inteligente para iniciar sesión en el VDA de Linux tanto en escenarios SSO como no SSO.

- En el escenario 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 no SSO, se le pedirá que seleccione un certificado e introduzca 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 como se muestra a continuación. El nombre de usuario se extrae del certificado de la tarjeta inteligente y debe escribir el PIN de nuevo para la autenticación de inicio de sesión.

Este comportamiento es el mismo que con el VDA de Windows.



Volver a conectar a una sesión mediante 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 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 cuando intenta volver a conectar a una sesión, la web de StoreFront podría mostrar una alerta como la siguiente.



Limitación

Directiva de extracción de tarjetas inteligentes

Ahora, el VDA de Linux solo utiliza el comportamiento predeterminado para la extracción de tarjetas inteligentes. Cuando extrae la tarjeta inteligente después de iniciar sesión correctamente en el VDA de Linux, la sesión permanece conectada y la pantalla de la sesión no se bloquea.

Compatibilidad con otras tarjetas inteligentes y la biblioteca PKCS#11

Aunque solo la tarjeta inteligente OpenSC aparece en nuestra lista de compatibilidad, puede intentar usar otras tarjetas inteligentes y la biblioteca PKCS#11 porque Citrix proporciona una solución genérica de redirección de tarjetas inteligentes. Para cambiar a su tarjeta inteligente específica o a la biblioteca PKCS#11:

1. Reemplace todas las instancias de `opensc-pkcs11.so` con 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. Deshabilite el inicio de sesión rápido con tarjeta inteligente en el cliente.

Autenticación de inicio de sesión único de doble salto

Esta función inyecta las credenciales de usuario introducidas para acceder a un almacén de StoreFront en el módulo AuthManager de Citrix Workspace app para Linux y Citrix Receiver para Linux 13.10. Después de la inyección, puede utilizar el cliente para acceder a escritorios virtuales y aplicaciones desde una sesión de escritorio virtual de Linux, sin introducir las credenciales de usuario por segunda vez.

Nota:

Esta función es compatible con Citrix Workspace app para Linux y Citrix Receiver para Linux 13.10.

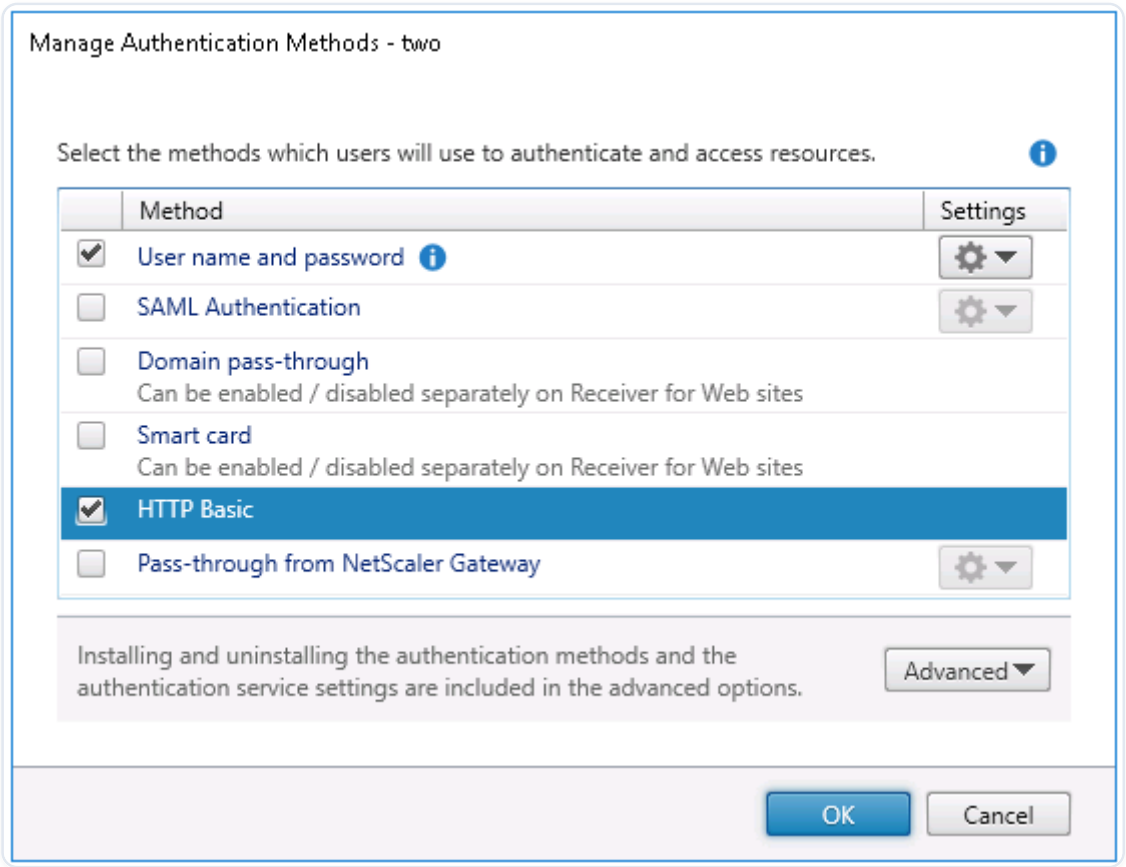
Para habilitar la función:

1. En el VDA de Linux, instale Citrix Workspace app para Linux o Citrix Receiver para Linux 13.10.

   Descargue la aplicación desde la página de descargas de Citrix para Citrix Workspace app 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 Citrix Workspace app 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 Citrix Workspace app para Linux o Citrix Receiver para Linux 13.10 dentro de una sesión de escritorio virtual de Linux. Más tarde, se iniciará sesión automáticamente en el almacén que especificó anteriormente.

   Nota:

   Introduzca una URL HTTPS como su cuenta de almacén.

   imagen de cómo iniciar sesión en su cuenta de tienda(/en-us/linux-virtual-delivery-agent/2201/media/store-account.png)

Configurar sesiones no autenticadas

Utilice la información de este artículo para configurar sesiones no autenticadas. No se requieren configuraciones especiales al instalar el VDA de Linux para usar esta función.

> **Nota:**
>
> Al configurar sesiones no autenticadas, tenga en cuenta que el inicio previo de sesión no es compatible. El inicio previo de sesión tampoco es compatible con la aplicación Citrix Workspace™ para Android.

Crear un almacén no autenticado

Para admitir una sesión no autenticada en el VDA de Linux, cree un almacén no autenticado con StoreFront.

Habilitar usuarios no autenticados en un grupo de entrega

Después de crear un almacén no autenticado, habilite los usuarios no autenticados en un grupo de entrega para admitir una sesión no autenticada. Para habilitar usuarios no autenticados en un grupo de entrega, siga las instrucciones de la documentación de Citrix Virtual Apps and Desktops.

Establecer el tiempo de inactividad de la sesión no autenticada

Una sesión no autenticada tiene un tiempo de espera de inactividad predeterminado de 10 minutos. Este valor se configura mediante la clave de registro **AnonymousUserIdleTime**. Utilice la herramienta **ctxreg** para cambiar este valor. Por ejemplo, para establecer esta clave de registro en cinco minutos:

```
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 de registro **MaxAnonymousUserNumber**. Esta configuración limita el número de sesiones no autenticadas que se ejecutan simultáneamente en un único VDA de Linux. Utilice la herramienta **ctxreg** para configurar esta clave de registro. Por ejemplo, para establecer el valor en 32:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber
 -d  0x00000020
```

Importante:

Limite el número de sesiones 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 no autenticadas:

- **Error al iniciar sesión en una sesión 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** esté en ejecución y configurado para habilitar la caché de **passwd**:

```
ps  uax | grep nscd

cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

Establezca la variable de caché de **passwd** en **no** si está habilitada, luego 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 no autenticada con KDE**.

El botón y el menú de bloqueo de pantalla están deshabilitados de forma predeterminada en una sesión no autenticada. Sin embargo, aún pueden mostrarse en KDE. En KDE, para deshabilitar 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 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 use directamente la configuración de todo el sistema para deshabilitar el botón y el menú de bloqueo de pantalla. Para obtener detalles sobre la configuración de KDE, consulte la página KDE System Administration/Kiosk/Keys.

Configurar LDAPS

LDAP seguro (LDAPS) le permite habilitar el Protocolo ligero de acceso a directorios seguro para sus dominios administrados por Active Directory a fin de proporcionar comunicaciones a través de SSL (Secure Socket Layer)/TLS (Transport Layer Security).

De forma predeterminada, las comunicaciones LDAP entre las aplicaciones cliente y servidor no están cifradas. LDAP mediante SSL/TLS (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/deshabilitar 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 autoridad de certificación (CA) de Microsoft o de una CA que no sea de Microsoft.

Sugerencia:

LDAP a través de SSL/TLS (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 autoridad de certificación de terceros en el sitio de soporte de Microsoft.

Cuando tiene una jerarquía de autoridad de certificación de varios niveles (como de dos o tres niveles), no dispone automáticamente del 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 autoridad de certificación de varios niveles, consulte el artículo Certificado LDAP a través de SSL (LDAPS) en el sitio de Microsoft TechNet.

Habilitar la autoridad de certificación raíz para uso del cliente

El cliente debe utilizar 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 autoridad de certificación raíz en el sitio web de soporte de Microsoft.

Habilitar o inhabilitar LDAPS en el VDA de Linux

Para habilitar o inhabilitar LDAPS en el VDA de Linux, ejecute el siguiente script (mientras haya iniciado sesión como administrador):

La sintaxis de este comando incluye lo siguiente:

- Habilitar LDAP a través de SSL/TLS con el certificado de CA raíz proporcionado:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- Habilitar LDAP a través de SSL/TLS con enlace de canal:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
```

> **Nota:**
>
> El certificado de CA raíz para la vinculación de canal debe estar en formato PEM. Si la habilitación de LDAPS no crea un entorno virtual de Python3 correctamente, 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`

- Volver a LDAP sin SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
```

El almacén de claves de Java dedicado para LDAPS se encuentra 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 RHEL) o **/etc/ldap/ldap.conf** (para 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, LDAP seguro se puede configurar 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 es compatible con 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 es compatible con LDAPS en el puerto 636, pero proporciona cifrado seguro en el puerto 389 mediante un método diferente.

Solución de problemas

Los siguientes problemas pueden surgir al utilizar 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 del VDA de Linux 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 las claves relacionadas con LDAPS se actualizaron por accidente sin usar **enable_ldaps.sh**, podría romperse 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 deshabilitado. 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 realiza el registro del VDA de Linux y la evaluación de la directiva de grupo.

- **No se pudo 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 es 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**

Al habilitar LDAPS ejecutando `/opt/Citrix/VDA/sbin/enable_ldaps.sh`, el certificado se importa a /etc/xdl/.keystore y la contraseña se establece para proteger el almacén de claves. Si olvida la contraseña, puede volver a ejecutar el script para crear un almacén de claves.

Crear un entorno virtual de Python3

Si se está conectando a la red, la ejecución del comando `sudo /opt/Citrix/VDA/bin/xdping` o `/opt/Citrix/VDA/sbin/enable_ldaps.sh` puede crear un entorno virtual de Python3. Sin embargo, si los comandos no logran 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:

   ```
   yum -y install python36-devel krb5-devel gcc
   ```

   Nota:

   Es posible que deba 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 Ubuntu, Debian:

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
```

Para SUSE:

```
zypper -i -n install python3-devel python3-setuptools krb5-devel gcc
libffi48-devel
```

Nota:

Es posible que deba habilitar el repositorio `SUSE_Linux_Enterprise_Software_Development_Kit_12_SP5_x86_64` para instalar algunas dependencias.

2. Cree 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 RHEL, Ubuntu, Debian:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

Para SUSE:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
setuptools==40.6.2
```

3. Instale las dependencias de LDAPS.

   Para RHEL, Ubuntu, Debian:

   ```
   sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
   cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
   ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
   pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
   termcolor==1.1.0
   ```

   Para SUSE:

   ```
   sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install
   cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
   ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
   pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
   termcolor==1.1.0
   ```

4. Instale las dependencias de `XDPing`.

   Para RHEL, Ubuntu, Debian:

   ```
   sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
   cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
   ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
   pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
   termcolor==1.1.0



   ```

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Para SUSE:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install
cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
termcolor==1.1.0



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Herramientas y utilidades

Utilidad de consulta de datos de sesión

Proporcionamos una utilidad (`ctxsdcutil`) que puede utilizar para consultar datos de sesión en cada VDA de Linux. 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 entrada de la sesión**
- **Ancho de banda de salida de la sesión**
- **Velocidad de línea de salida de la sesión**
- **Latencia - Último registro**
- **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**

El script Bash xdlcollect

El script Bash `xdlcollect` utilizado para recopilar registros está integrado en el software de Linux VDA y se encuentra en /opt/Citrix/VDA/bin. Después de instalar el Linux VDA, puede ejecutar el comando `bash /opt/Citrix/VDA/bin/xdlcollect.sh` para recopilar registros. Una vez finalizada la recopilación de registros, se genera un archivo de registro comprimido en la misma carpeta que el script. `xdlcollect` puede preguntarle si desea cargar o no el archivo de registro comprimido en Citrix Insight Services (CIS). Si acepta, `xdlcollect` devuelve un upload_ID una vez completada la carga. La carga no elimina el archivo de registro comprimido de su máquina local. Otros usuarios pueden utilizar el upload_ID para acceder al archivo de registro en CIS.

XDPing

La herramienta Linux XDPing es una aplicación de línea de comandos. Automatiza el proceso de comprobación de problemas de configuración comunes en un entorno Linux VDA.

La herramienta Linux XDPing 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 Linux VDA
- Identificar y mostrar información de la máquina, incluidas las distribuciones de Linux
- Comprobar la compatibilidad del kernel de Linux
- Comprobar si hay problemas conocidos de distribución de Linux que puedan afectar al funcionamiento de Linux VDA
- Comprobar el modo y la compatibilidad de Security-Enhanced Linux (SELinux)
- Identificar interfaces de red y comprobar la configuración de red
- Comprobar el particionamiento del almacenamiento y el espacio en disco disponible
- Comprobar el host de la máquina y la configuración del nombre de dominio
- Comprobar la configuración de DNS y realizar pruebas de búsqueda
- Identificar hipervisores subyacentes y comprobar la configuración de la máquina virtual. Compatibilidad con:
    - Citrix Hypervisor™
    - Microsoft HyperV
    - VMware vSphere
- Comprobar la configuración de la hora y si la sincronización de la hora de red está operativa

- Comprobar si el servicio de PostgreSQL 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 si la máquina actual está unida al dominio. Compatibilidad con:
  - Samba Winbind
  - Dell Quest Authentication Services
  - 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 del VDA de Linux y comprobar la integridad de la instalación
- Comprobar la integridad de la base de datos del registro de PostgreSQL
- Comprobar si los servicios de Linux VDA 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 Linux VDA
- Comprobar si la versión de Xorg es adecuada

Usar la herramienta XDPing de Linux

> **Nota:**

> La ejecución de ctxsetup.sh 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. Si este comando no puede crear 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`

> XDPing incluye un único ejecutable llamado `xdping` que se ejecuta desde el shell de comandos.

Para mostrar las opciones de línea de comandos, use la opción `--help`:

```
sudo /opt/Citrix/VDA/bin/xdping --help
```

Para ejecutar el conjunto completo de pruebas, ejecute `xdping` sin ninguna opción de línea de comandos:

```
sudo /opt/Citrix/VDA/bin/xdping
```

Para comprobar el entorno antes de instalar el paquete Linux VDA, ejecute las pruebas `pre-flight`:

```
sudo /opt/Citrix/VDA/bin/xdping --preflight
```

Para ejecutar solo categorías de prueba específicas, por ejemplo, las pruebas de tiempo y Kerberos, use la opción `-T`:

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
```

Para sondear un determinado XenDesktop® Controller:

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
```

Salida de ejemplo

A continuación se muestra una salida de ejemplo de la ejecución de la prueba de Kerberos:

Primera parte de la salida de ejemplo de la prueba de Kerberos(/en-us/linux-virtual-delivery-agent/2201/media/kerberos-test-sample-output-1.png)

Segunda parte de la salida de ejemplo de la prueba de Kerberos(/en-us/linux-virtual-delivery-agent/2201/media/kerberos-test-sample-output-2.png)

Tercera parte de la salida de ejemplo de la prueba de Kerberos(/en-us/linux-virtual-delivery-agent/2201/media/kerberos-test-sample-output-3.png)

Configurar Xauthority

El VDA de Linux admite entornos que utilizan la funcionalidad de visualización X11 (incluidos `xterm` y `gvim`) para el acceso remoto interactivo. Esta función proporciona un mecanismo de seguridad necesario para garantizar una comunicación segura entre XClient y XServer.

Existen dos métodos para proteger 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, alternativamente, puede usar **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 usando 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 de 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 utilizando 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 (por ejemplo, 10.158.11.11) y el número de pantalla del escritorio publicado (por ejemplo, 160).

   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.

Configurar Federated Authentication Service

Puede usar Federated Authentication Service (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 Federated Authentication Service. Este artículo proporciona información adicional específica para el VDA de Linux.

> **Nota**
>
> El VDA de Linux no admite la directiva **Comportamiento en la sesión**.
>
> El VDA de Linux utiliza conexiones cortas para transmitir datos con los servidores FAS.

Configurar FAS en el VDA de Linux

Compatibilidad de FAS en RHEL 8

FAS depende del módulo pam_krb5, que está obsoleto en RHEL 8. Para usar FAS en RHEL 8, compile el módulo pam_krb5 de la siguiente manera:

1. Descargue el código fuente de pam_krb5-2.4.8-6 del siguiente sitio web:

   `<https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html>`.

2. Compile e instale el módulo pam_krb5 en RHEL 8.

```
yum install make gcc krb5-devel pam-devel autoconf libtool

rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div

tar xvzf pam_krb5-2.4.8.tar.gz

cd pam_krb5-2.4.8

./configure --prefix=/usr

make

make install
```

3. verificar que pam_krb5.so existe en /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
```

Configurar servidores FAS

Para usar FAS en una nueva instalación de VDA de Linux, escriba el FQDN de cada servidor FAS al ejecutar ctxinstall.sh o ctxsetup.sh. Dado que el VDA de Linux no admite la directiva de grupo de AD, puede proporcionar una lista de servidores FAS separada por punto y coma. Si se elimina alguna dirección de servidor, rellene el espacio en blanco con la cadena de texto **\<none\>** y no modifique el orden de las direcciones de los servidores.

Para actualizar una instalación existente de VDA de Linux, puede volver a ejecutar `ctxsetup.sh` para configurar los servidores FAS. O bien, 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\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force
```

```
service ctxjproxy restart


service ctxvda restart
```

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\UserCredentialSer
vice" -v "Addresses" -d "<Your-FAS-Server-List>"


service ctxjproxy restart


service ctxvda restart
```

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 **Recuperar el certificado de CA de Microsoft CA (en AD)**, o descargue su formato DER del servidor de CA raíz `http://CA-SERVER/certsrv`.

> **Nota:**

> Los siguientes comandos también se aplican a la configuración de un certificado intermedio.

> Convierta un archivo DER (.crt, .cer, .der) a PEM ejecutando 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 los parámetros de FAS:

```
sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
```

Se añaden variables de entorno para que `ctxfascfg.sh` se pueda ejecutar en modo silencioso:

- **CTX_FAS_ADINTEGRATIONWAY=winbind \| sssd \| centrify \| pbis**: 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.
- **CTX_FAS_PKINIT_KDC_HOSTNAME**: Especifica el nombre de host de PKINIT KDC, que es igual a CTX_FAS_KDC_HOSTNAME a menos que se especifique lo contrario.

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.

Limitación

- FAS admite plataformas Linux y métodos de integración de AD limitados. Consulte la siguiente matriz:

	WINBIND	SSSD	CENTRIFY	PBIS
Amazon Linux 2	Sí	Sí	Sí	Sí
RHEL 8.4	Sí	Sí	Sí	Sí
RHEL 8.3	Sí	Sí	Sí	Sí
RHEL 8.2	Sí	Sí	Sí	Sí
RHEL 8.1	Sí	Sí	Sí	Sí
RHEL 7.9 / CentOS 7.9	Sí	Sí	Sí	Sí
RHEL 7.8 / CentOS 7.8	Sí	Sí	Sí	Sí
SLES 15.3	Sí	No	Sí	No
SLES 15.2	Sí	No	Sí	No
SLES 12.5	Sí	No	Sí	No
Ubuntu 20.04	Sí	No	Sí	No
Ubuntu 18.04	Sí	No	Sí	No
Ubuntu 16.04	Sí	No	Sí	No

- FAS aún no es compatible con la pantalla de bloqueo. Si hace clic en el botón de bloqueo en una sesión, no podrá volver a iniciar sesión en ella mediante FAS.
- Esta versión solo admite las implementaciones comunes de FAS resumidas en el artículo Información general sobre la arquitectura de Federated Authentication Service y no incluye **Windows 10 Azure AD Join**.

Solución de problemas

Antes de solucionar problemas de FAS, asegúrese de que el VDA de Linux esté instalado y configurado correctamente y que se pueda 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 HDX de la clase **Login** en VERBOSE y el nivel de registro del 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.

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

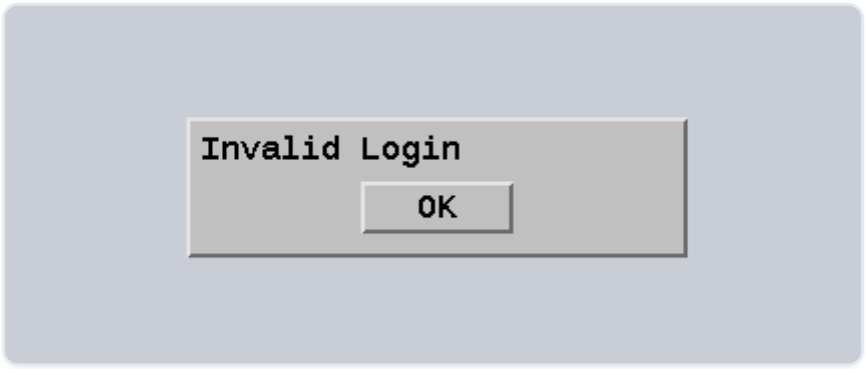
Ejecute el siguiente comando para verificar que el valor del Registro de Citrix "HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\VirtualDesktopAgent\\Authentication\ \UserCredentialService" está establecido en \<Your-FAS-Server-List\>.

```
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 configurarlo.

Configuración incorrecta del certificado de CA

No se puede iniciar una sesión desde el almacén de FAS. Aparece una ventana gris que 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 establecido 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/


    ......

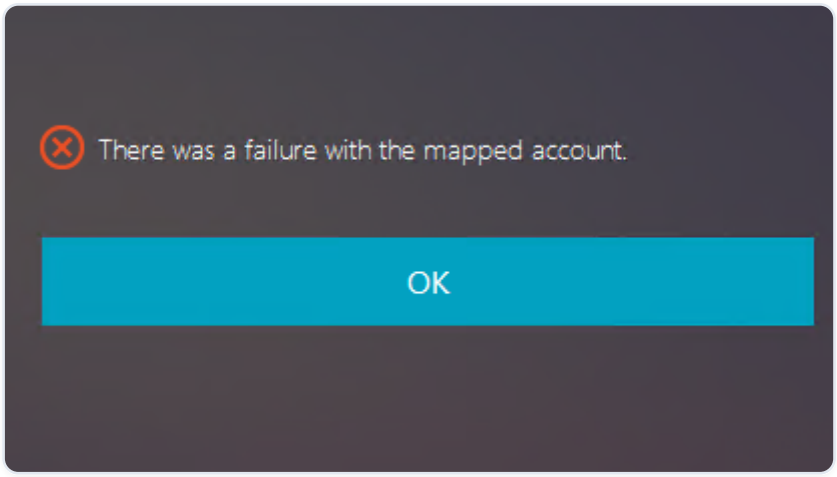

}
```

Si la configuración existente es incorrecta, siga el paso anterior Instalar certificados para volver a configurarla.

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.



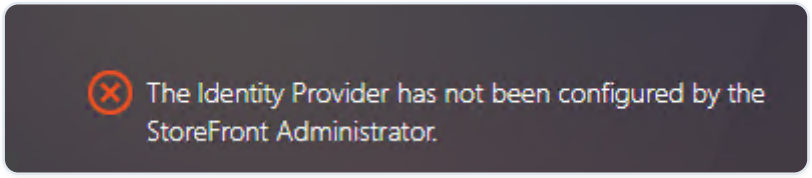
Este error indica que el usuario de ADFS se ha verificado correctamente, pero no hay ningún usuario de sombra configurado en AD.

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 el almacén de FAS está configurado 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.

- Los artículos de "Cómo hacer" se presentan en el capítulo Configuración avanzada del Servicio de autenticación federada.

Problema conocido

Cuando FAS está en uso, puede fallar al intentar iniciar un escritorio publicado o una sesión de aplicación con caracteres no ingleses.

Error al iniciar sesiones con caracteres no ingleses(/en-us/linux-virtual-delivery-agent/2201/media/launching-nonenglish-session-fails.png)

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**:

La opción de suministrar en la solicitud(/en-us/linux-virtual-delivery-agent/2201/media/supply-in-the-request.png)

VDA no unidos a un dominio

Resumen de configuración

Los VDA no unidos a un dominio solo son compatibles con el servicio Citrix Virtual Apps and Desktops™. Para crear VDA no unidos a un dominio en el servicio Citrix Virtual Apps and Desktops, debe usar Machine Creation Services (MCS). Los pasos resumidos son:

1. Cree una imagen maestra en una VM de plantilla donde también instale el paquete VDA. Puede usar una sola imagen para crear VDA unidos a un dominio y no unidos a un dominio.
2. Use la imagen maestra para crear un catálogo de máquinas. 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.

Para obtener más información, consulte Usar Machine Creation Services (MCS) para crear máquinas virtuales Linux y Identidades de máquinas.

Funciones disponibles para VDA no unidos a un dominio

Crear 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™. 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.
`homedir`	Opcional	El directorio personal de Linux es un directorio para un usuario en particular.
`shell`	Opcional	Un shell de inicio de sesión es un shell que se le asigna

ATRIBUTO	OBLIGATORIO U OPCIONAL	DESCRIPCIÓN
		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
```

Historial de documentos de Linux Virtual Delivery Agent

En la siguiente tabla se describen cambios importantes en la documentación de Linux Virtual Delivery Agent 2201. Para recibir notificaciones sobre estas novedades, suscríbase al feed RSS.

FECHA	CAMBIO	DESCRIPCIÓN
19 Jan 2022	Publicación de Linux Virtual Delivery Agent 2201	Novedades en Linux Virtual Delivery Agent 2201