Linux Virtual Delivery Agent 7.15

Contents

Novedades

October 3, 2022

Fecha de publicación: 7 de julio de 2022

Novedades de 7.15

La actualización Cumulative Update 9 (CU9) es la versión más reciente de Linux VDA 7.15 LTSR. CU9 agrega una corrección a la actualización CU8 de Linux VDA 7.15.

Impresión de PDF

Antes disponible como una función experimental, la impresión PDF es una función totalmente disponible en esta versión. Permite que los usuarios de Citrix Receiver para Chrome y HTML5 impriman archivos PDF convertidos desde dentro de las sesiones de Linux VDA.

Cambio en el comportamiento del sistema

A partir de esta versión, no es necesario ejecutar el script ctxsetup.sh después de actualizar Linux VDA.

Problemas resueltos

August 8, 2022

Problemas resueltos en CU9

- Es posible que la desinstalación de Linux VDA en SUSE o RHEL no elimine carpetas vacías de la ubicación /opt/Citrix/. [CVADHELP-18241]

Problemas resueltos en CU8

- Con la vinculación de canales habilitada, puede que los Linux VDA no se registren en el Delivery Controller. [CVADHELP-14481]

Problemas resueltos en CU6

- Una sesión de Linux podría dejar de responder si el mouse y el teclado no están centrados en la misma ventana o si el mouse no cambia el foco. [CVADHELP-12768]
- Es posible que no se redirija genéricamente una unidad USB extraíble a un Linux VDA. El problema ocurre cuando la unidad USB tiene formato NTFS (New Technology File System). [CVADHELP-13675]
- Es posible que los agentes Linux VDA no alcancen los fotogramas por segundo que se especifican en el parámetro **Velocidad de fotogramas de destino** (FramesPerSecond). El problema se produce cuando se instala una GPU en un agente Linux VDA. [CVADHELP-14267]

Problemas resueltos en CU5

- Los intentos de copiar y pegar contenido entre un cliente y una sesión con mediante la función Portapapeles pueden fallar. [LD2047]
- Cuando inicia una sesión en una instancia de Linux VDA y realiza una acción, es posible que la sesión se desconecte. [LD2257]

Problemas resueltos en CU4

- Cuando intenta copiar contenido de un dispositivo de punto final y pegarlo en una aplicación que se ejecuta en un Linux VDA, es posible que el contenido no se copie. [LC8760]
- El teclado podría no funcionar en SUSE Linux Enterprise Server 11 Service Pack 4. Como resultado, las pulsaciones de teclas no se muestran en la pantalla y la distribución del teclado no está configurada correctamente. [LC9906]
- Es posible que el proceso **ctxctl** no se ejecute en una sesión de usuario de Linux VDA. [LD0353]

Problemas resueltos en CU3

- Linux VDA podría no aplicar las directivas Citrix. El problema ocurre cuando se configura una directiva para que use el tipo de conexión del elemento de control de acceso con NetScaler Gateway. [LC9842]

Problemas resueltos en CU2

- Es posible que la operación de registro de un Linux VDA mediante el Delivery Controller falle intermitentemente. [LC7982]

- Un Citrix Director 7.13 que se ejecuta en Red Hat Enterprise Linux Server 7.3 podría no mostrar los detalles de la sesión de la máquina. Aparece el siguiente mensaje de error:

  No se puede obtener los datos. [LC8204]

- Un Linux VDA puede registrarse en el Delivery Controller y cancelar el registro más adelante. [LC8205]
- Puede que algunas aplicaciones de terceros que se utilizan para consultar la pantalla de una sesión en Linux VDA no muestren todos los píxeles. [LC8419]
- Cuando hay varios servidores LDAP, pueden fallar los intentos de iniciar una aplicación en un Linux VDA después de que se actualicen las directivas y se agote el tiempo de espera de la sesión. [LC8444]
- El proceso ctxhdx puede cerrarse inesperadamente con un fallo de segmentación **segfault** cuando la sesión está conectada a un Linux VDA. [LC8611]
- Al utilizar la versión Linux VDA 7.16 Early Access Release, es posible que el agente del broker no obtenga el nombre de la aplicación. Este error hace que Director muestre el error **Agente solicitado**, después de lo cual se inicia de nuevo el proceso de registro. [LC9243]

Problemas resueltos en CU1

- Un Linux VDA puede registrarse en el Delivery Controller y cancelar el registro más adelante. [LC8205]
- Puede que algunas aplicaciones de terceros que se utilizan para consultar la pantalla de una sesión en Linux VDA no muestren todos los píxeles. [LC8419]
- Cuando hay varios servidores LDAP, pueden fallar los intentos de iniciar una aplicación en un Linux VDA después de que se actualicen las directivas y se agote el tiempo de espera de la sesión. [LC8444]

Problemas resueltos en 7.15 LTSR

Se han resuelto los siguientes problemas en esta versión de Linux VDA:

- La instalación fácil (Easy Install) de Linux VDA puede provocar la desconexión de red cuando introduce la dirección IP de DNS. [LNXVDA-2152]
- Al reproducir un vídeo, falla el roaming de sesiones desde Citrix Receiver para Windows a Citrix Receiver para Android. [LNXVDA-2164]

Problemas conocidos

August 8, 2022

Se han identificado los problemas siguientes en esta versión:

- Citrix Scout integrado con XenApp y XenDesktop 7.15 LTSR CU6 no puede recopilar registros de Linux VDA 7.15. Linux VDA 7.15 no es compatible con el servicio Citrix Telemetry Service que Citrix Scout utiliza para recopilar registros.
- El proceso `indicator-datetime-service` no consume la variable de entorno $TZ. Cuando el cliente y la sesión se encuentran en diferentes zonas horarias, el panel de Unity en Ubuntu 16.04 Unity Desktop no muestra la hora del cliente. [LNXVDA-2128]
- Gráficos en Ubuntu: En HDX 3D Pro, puede aparecer un marco negro alrededor de las aplicaciones después de redimensionar Desktop Viewer o, en algunos casos, el fondo puede aparecer en negro.
- Es posible que las impresoras creadas por la redirección de impresoras de Linux VDA no se eliminen después de cerrar una sesión.
- No se encuentran los archivos de asignación de unidades del cliente si un directorio contiene varios archivos y subdirectorios. Este problema puede ocurrir si hay demasiados archivos o directorios en el lado del cliente.
- En esta versión, solo se admite la codificación UTF-8 para aquellos idiomas que no sean inglés.
- El estado Bloq Mayús de Citrix Receiver para Android se puede invertir durante el roaming de la sesión. Es posible que se pierda el estado Bloq Mayús cuando se mueve la conexión a Citrix Receiver para Android. La solución temporal es usar la tecla Mayús en el teclado extendido para alternar entre mayúsculas y minúsculas.
- Los atajos de teclado que contienen ALT no siempre funcionan cuando el usuario se conecta a Linux VDA desde Citrix Receiver para Mac. De forma predeterminada, Citrix Receiver para Mac envía Alt Gr para las teclas Opciones o Alt de izquierda y derecha. Puede cambiar este comportamiento en la configuración de la aplicación Citrix Receiver, pero los resultados varían según las diferentes aplicaciones.
- Falla la captura de registros cuando Linux VDA se vuelve a unir al dominio. Volver a unirse genera un nuevo conjunto de claves Kerberos. Sin embargo, el Broker puede utilizar un tíquet de servicio de VDA guardado en caché que se ha quedado obsoleto porque está 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 en la devolución al VDA. El síntoma habitual de este problema es que falla el registro del VDA.

Este problema se resolverá por sí solo cuando el tíquet de servicio del VDA caduque y se renueve. Aunque esos tíquets suelen durar mucho tiempo, por lo que el problema puede tardar en resolverse.

Como solución temporal, borre la caché de tíquets del Broker. Reinicie el Broker o ejecute en él lo siguiente desde un símbolo del sistema como administrador:

```
klist -li 0x3e4 purge
<!--NeedCopy-->
```

Esta acción purga todos los tíquets de servicio que guarda en la memoria caché de LSA la entidad de servicio de red donde se ejecuta Citrix Broker Service. Quita los tíquets de servicio de otros VDA y, posiblemente, de otros servicios. No obstante, se trata de un proceso inofensivo, ya que los tíquets de servicio se pueden obtener de nuevo de KDC cuando sea necesario.

- No se admiten los dispositivos de sonido Plug and Play. Puede conectar un dispositivo de captura de sonido a la máquina cliente antes de empezar a grabar el sonido en una sesión ICA. Si el dispositivo de captura de sonido se conecta una vez iniciada la aplicación de grabación de sonido, esa aplicación puede dejar de responder y deberá reiniciarla. Podría darse un problema similar si el dispositivo de captura se desconecta durante la grabación.
- Puede producirse un sonido distorsionado en Citrix Receiver para Windows durante la grabación de sonido.

Avisos legales de terceros

December 12, 2022

Linux Virtual Desktop 7.15 (Descarga en PDF)

Esta versión de Linux VDA puede incluir software de terceros con licencias definidas en los términos del documento.

Requisitos del sistema

November 3, 2021

Distribuciones de Linux

Linux VDA admite las siguientes distribuciones de Linux:

- SUSE Linux Enterprise:
  - Desktop 12 Service Pack 2
  - Server 12 Service Pack 2
  - Server 11 Service Pack 4
- Red Hat Enterprise Linux
  - Workstation 7.3
  - Workstation 6.9
  - Workstation 6.6
  - Server 7.3
  - Server 6.9
  - Server 6.6
- CentOS Linux
  - CentOS 7.3
  - CentOS 6.6
- Ubuntu Linux
  - Escritorio Ubuntu 16.04 (con el kernel 4.4.x)
  - Servidor Ubuntu 16.04 (con el kernel 4.4.x)

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

Distribución de Linux	Versión de Xorg
RHEL 7.3, CentOS 7.3	1.17
RHEL 6.9	1.17
RHEL 6.6, CentOS 6.6	1.15
Ubuntu 16.04	1.18
SUSE 12.2	1.18
SUSE 11.4	1.6.5

No use el servidor HWE Xorg 1.19 en Ubuntu 16.04.

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

> **Nota:**
>
> El desarrollo que ofrece Citrix para una plataforma y versión de SO Linux caduca cuando caduca, a su vez, el desarrollo por parte del proveedor del sistema operativo.
>
> **Importante:**
>
> Los escritorios Gnome y KDE son compatibles en SUSE, RHEL y CentOS. El escritorio de Unity solo se admite en Ubuntu. Debe instalarse al menos un escritorio.

XenDesktop

El VDA de Linux es compatible con todas las versiones actualmente admitidas de XenDesktop. Para obtener más información acerca de la vida útil del producto XenDesktop y para determinar cuándo deja Citrix de admitir versiones específicas de los productos, consulte Citrix Product Lifecycle Matrix.

El proceso de configuración para los agentes Linux VDA difiere ligeramente del proceso para los VDA de Windows. No obstante, cualquier comunidad de Delivery Controllers puede intermediar tanto para escritorios Windows como para escritorios Linux.

> **Nota:**
>
> Linux VDA no es compatible con XenDesktop 7.0 ni con versiones anteriores.

Citrix Receiver

Se admiten las siguientes versiones de Citrix Receiver:

- Citrix Receiver para UWP (Plataforma universal de Windows) 1.0
- Citrix Receiver para Windows 4.8 o versiones posteriores
- Citrix Receiver para Linux 13.5
- Citrix Receiver para Mac OS X 12.6
- Citrix Receiver para Android 3.11
- Citrix Receiver para iOS 7.2
- Citrix Receiver para Chrome 2.5
- Citrix Receiver para HTML5 2.5 (solo a través de Access Gateway)

Hipervisores

Se admiten los siguientes hipervisores para alojar máquinas virtuales invitadas con Linux VDA:

- XenServer

- VMware ESX y ESXi
- Microsoft Hyper-V
- Nutanix AHV

También se admite el alojamiento en máquinas sin sistema operativo.

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

Paquetes de integración de Active Directory

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

- Samba Winbind
- Quest Authentication Services 4.1 o una versión posterior
- Centrify DirectControl
- SSSD

> **Sugerencia:**
>
> Consulte la documentación del proveedor del paquete de integración de Active Directory para ver la lista de las plataformas admitidas.

HDX 3D Pro

Se necesitan los siguientes hipervisores, distribuciones de Linux y GPU de NVIDIA GRID para admitir HDX 3D Pro.

Hipervisores

Se admiten los siguientes hipervisores:

- XenServer
- VMware ESX y ESXi
- Nutanix AHV

Distribuciones de Linux

Las siguientes distribuciones de Linux admiten HDX 3D Pro:

- Red Hat Enterprise Linux - Workstation 7.3
- Red Hat Enterprise Linux - Server 7.3

- Red Hat Enterprise Linux - Workstation 6.9
- Red Hat Enterprise Linux - Server 6.9
- Red Hat Enterprise Linux - Workstation 6.6
- Red Hat Enterprise Linux - Server 6.6
- SUSE Linux Enterprise Desktop 12 Service Pack 2
- SUSE Linux Enterprise Server 12 Service Pack 2
- Ubuntu Linux Desktop 16.04
- Ubuntu Linux Server 16.04

GPU

Se admiten las siguientes GPU para la función GPU PassThrough:

- NVIDIA GTX750Ti
- NVIDIA GRID: Tesla M60
- NVIDIA GRID: K2

Se admiten las siguientes GPU para vGPU:

- NVIDIA GRID: Tesla M60
- NVIDIA GRID: Tesla M10

Información general de la instalación

November 21, 2020

La instalación de Linux Virtual Delivery Agent (VDA) sigue los mismos pasos generales para todas las distribuciones de Linux compatibles.

1. Prepararse para la instalación.
2. Preparar el hipervisor.
3. Agregar la máquina virtual (VM) Linux al dominio de Windows.
4. Instalar Linux VDA.
5. Configurar Linux VDA.
6. Crear el catálogo de máquinas en XenApp o XenDesktop.
7. Crear el grupo de entrega en XenApp o XenDesktop.

Las variantes y comandos específicos se documentan para cada distribución.

Configurar Delivery Controllers

May 6, 2020

XenDesktop 7.6 y versiones anteriores requieren ciertos cambios para ser compatibles con Linux VDA. Para estas versiones es necesario instalar un parche rápido o un script de actualización. Las instrucciones de instalación y verificación se ofrecen en este artículo.

Actualización de la configuración del Delivery Controller

Para XenDesktop 7.6 SP2, aplique el parche rápido Hotfix Update 2 y, así, actualizar el Broker para escritorios virtuales con Linux. El parche rápido Hotfix Update 2 está disponible aquí:

- CTX142438: Hotfix Update 2 para Delivery Controller 7.6 (32 bits), en inglés
- CTX142439: Hotfix Update 2 para Delivery Controller 7.6 (64 bits), en inglés

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

- citrix-linuxvda-scripts.zip

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

1. Copie el script **Update-BrokerServiceConfig.ps1** a la máquina de 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
<!--NeedCopy-->
```

> **Consejo:**
>
> De forma predeterminada, PowerShell está configurado para impedir la ejecución de scripts de PowerShell. Si el script no se ejecuta, cambie la directiva de ejecución de PowerShell y vuelva a intentarlo:
>
> ```
> Set-ExecutionPolicy Unrestricted
> <!--NeedCopy-->
> ```

El script **Update-BrokerServiceConfig.ps1** actualiza el archivo de configuración del servicio de broker con nuevos puntos finales WCF que necesita Linux VDA y después reinicia el servicio del broker. El

script determina automáticamente la ubicación del archivo de configuración del servicio del broker. Se crea una copia de seguridad del archivo de configuración original en el mismo directorio con la extensión **.prelinux**.

Estos cambios no afectan la intermediación (broker) de agentes VDA con Windows configurados para usar la misma comunidad de Delivery Controller. Con lo que una sola comunidad de Controllers puede administrar y actuar de broker en sesiones de agentes VDA con Windows y con Linux.

Comprobación de la configuración del Delivery Controller

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

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

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\
findstr EndpointLinux BrokerService.exe.config
<!--NeedCopy-->
```

Easy Install

June 17, 2022

Easy Install se admite oficialmente a partir de la versión 7.13 de Linux VDA. Easy Install le ayuda a configurar el entorno de ejecución de Linux VDA mediante la instalación de los paquetes necesarios y la personalización automática de los archivos de configuración.

Distribuciones compatibles

	Winbind	SSSD	Centrify
RHEL 7.3	Sí	Sí	Sí
RHEL 6.9	Sí	Sí	Sí
RHEL 6.6	Sí	Sí	Sí
CentOS 7.3	Sí	Sí	Sí
Ubuntu 16.04	Sí	Sí	Sí
SUSE 12.2	Sí	No	Sí

Uso de Easy Install

Para usar esta función, lleve a cabo lo siguiente:

1. Prepare la información de configuración y la máquina Linux.
2. Instale el paquete de Linux VDA.
   Vaya a la página web de Citrix y descargue el paquete de Linux VDA adecuado según su distribución de Linux.
3. Configure el entorno en tiempo de ejecución para completar la instalación de Linux VDA.

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

Recopile la siguiente información de configuración necesaria para Easy Install:

- Nombre de host: El nombre de host de la máquina en la que se instalará Linux VDA
- Dirección IP del servidor de nombres de dominio
- Dirección IP o cadena de nombre del servidor NTP
- Nombre de dominio: El nombre NetBIOS del dominio
- Nombre de territorio: El nombre del territorio Kerberos
- FQDN del dominio activo. Nombre de dominio completo

> **Importante:**
>
> - Para instalar Linux VDA, compruebe que los repositorios se agregan correctamente en la máquina Linux.
> - Para lanzar una sesión, compruebe que se instalan los entornos de escritorio y sistema X Windows están instalados.

Paso 2: Instale el paquete de Linux VDA

Ejecute los siguientes comandos para configurar el entorno para Linux VDA.

Para distribuciones RHEL y CentOS:

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

Para distribuciones Ubuntu:

```
sudo dpkg -i <PATH>/<Linux VDA deb>
sudo apt-get install -f
<!--NeedCopy-->
```

Para las distribuciones SUSE:


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

Paso 3: Configure el entorno en tiempo de ejecución para completar la instalación

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.

Modo interactivo:

Para una configuración manual, ejecute el siguiente comando y escriba el parámetro correspondiente cuando lo solicite el sistema.

```
sudo /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--NeedCopy-->
```

Modo silencioso:

Para usar Easy Install de manera silenciosa, establezca las siguientes variables de entorno antes de ejecutar ctxinstall.sh.

- **CTX_EASYINSTALL_HOSTNAME**=host-name: El nombre de host del servidor Linux VDA.
- **CTX_EASYINSTALL_DNS**=ip-address-of-dns: La dirección IP de DNS.
- **CTX_EASYINSTALL_NTPS**=address-of-ntps: La dirección IP o cadena de nombre del servidor NTP.
- **CTX_EASYINSTALL_DOMAIN**=domain-name: El nombre NetBIOS del dominio.
- **CTX_EASYINSTALL_REALM**=realm-name: El nombre del territorio Kerberos.
- **CTX_EASYINSTALL_FQDN**=ad-fqdn-name
- **CTX_EASYINSTALL_ADINTEGRATIONWAY=**winbind | sssd | centrify: 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: Indica la contraseña del usuario de dominio; se utiliza para unirse al dominio.

Las siguientes variables se usan en ctxsetup.sh:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME**=Y | N: Linux VDA permite especificar un nombre de Delivery Controller mediante un registro CNAME de DNS.
- **CTX_XDL_DDC_LIST=**list-ddc-fqdns: Linux VDA necesita una lista de nombres de dominio completo de Delivery Controllers, separados por espacios, para registrarse en un Delivery Controller. Se debe especificar al menos un nombre FQDN o CNAME.
- **CTX_XDL_VDA_PORT**=port-number: Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP.

- **CTX_XDL_REGISTER_SERVICE**=Y | N: Los servicios de Linux Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES**=Y | N: Los servicios de Linux Virtual Desktop requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema para Linux Virtual Desktop.
- **CTX_XDL_HDX_3D_PRO**=Y | N: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. 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: Indica si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos alojados. Para entornos HDX 3D Pro, establézcalo en Y.
- **CTX_XDL_SITE_NAME**=dns-name: Linux VDA detecta los servidores LDAP mediante DNS. Para limitar los resultados de búsqueda de DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, se puede establecer en **<none>**.
- **CTX_XDL_LDAP_LIST=**list-ldap-servers: Linux VDA consulta a DNS para detectar servidores LDAP. Sin embargo, si el DNS no puede proporcionar registros del servicio LDAP, se puede suministrar una lista de nombres FQDN de LDAP, separados por espacios, con el puerto de LDAP. Por ejemplo, ad1.miempresa.com:389. Si no es necesario, se puede establecer en **<none>**.
- **CTX_XDL_SEARCH_BASE**=search-base-set: Linux VDA consulta a LDAP a partir de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=miempresa,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar otra base de búsqueda (por ejemplo, OU=VDI,DC=miempresa,DC=com). Si no es necesario, se puede establecer en **<none>**.
- **CTX_XDL_START_SERVICE**=Y | N: Indica si los servicios de Linux VDA se inician cuando se complete su configuración.

Si algún parámetro no se ha definido, la instalación revierte al modo interactivo, con una pregunta para que el usuario introduzca una respuesta. El script ctxinstall.sh no solicita respuestas, siempre que todos los parámetros puedan ser suministrados a través de variables de entorno.

En el modo silencioso, se deben 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

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_START_SERVICE=Y | N

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--NeedCopy-->
```

Cuando ejecute el comando sudo, escriba la opción -E para pasar las variables de entorno existentes al nuevo shell que se crea. Citrix recomienda crear un archivo de script shell a partir de los comandos anteriores con **#!/bin/bash** en la primera línea.

También puede especificar todos los parámetros con un único comando:

```
sudo CTX_EASYINSTALL_HOSTNAME=host-name \

CTX_EASYINSTALL_DNS=ip-address-of-dns \

CTX_EASYINSTALL_NTPS=address-of-ntps \

CTX_EASYINSTALL_DOMAIN=domain-name \

CTX_EASYINSTALL_REALM=realm-name \

......
```



```
12
13 CTX_XDL_SEARCH_BASE=search-base-set \
14
15 CTX_XDL_START_SERVICE=Y \
16
17 /opt/Citrix/VDA/sbin/ctxinstall.sh
18 <!--NeedCopy-->
```

Consideraciones

- El nombre de grupo de trabajo es el nombre de dominio de forma predeterminada. Para personalizar el grupo de trabajo en el entorno, lleve a cabo lo siguiente:

  a. Cree el archivo /tmp/ctxinstall.conf en la máquina Linux VDA.
  b. Agregue la línea workgroup=\<su grupo de trabajo\> al archivo.

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

- Para Centrify en CentOS, Easy Install puede fallar en `adcheck`, la herramienta de comprobación del entorno de Centrify, y notificar el siguiente error:

  Registro:

  ```
  1 ADSITE    : Check that this machine's subnet is in a site known by
        AD    : Failed
  2           : This machine's subnet is not known by AD.
  3           : We guess you should be in the site Site1.
  4 <!--NeedCopy-->
  ```

  Este problema se debe a la configuración especial de Centrify. Haga lo siguiente para resolver este problema:

  a. Abra **Herramientas administrativas** en Delivery Controller.
  b. Seleccione **Sitios y servicios de Active Directory**.
  c. Agregue una dirección de subred correcta para **Subredes**.

- Si elige Centrify como el método para unirse a un dominio, el script ctxinstall.sh necesita el paquete de Centrify. ctxinstall.sh puede obtener el paquete de Centrify de dos formas:

  - Easy Install ayuda a descargar el paquete de Centrify desde Internet automáticamente. Las direcciones URL especificadas para cada distribución son:

    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

    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

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

Ubuntu: wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-deb7-x86_64.tgz?_ga=1.178323680.558673738.1478847956

- Obtenga el paquete Centrify desde un directorio local. Haga lo siguiente para designar el directorio del paquete Centrify:

  a. Cree el archivo /tmp/ctxinstall.conf en el servidor Linux VDA si no existe todavía.
  b. Agregue la línea “centrifypkgpath=\<nombre de ruta\>”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
<!--NeedCopy-->
```

Solución de problemas

Use la información de esta sección para solucionar los problemas que puedan surgir en el uso de esta función.

Falla el proceso de unirse a un dominio mediante SSSD

Puede producirse un error al intentar unirse a un dominio, con un resultado parecido al siguiente (verifique los registros para la impresión en pantalla):

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

/var/log/xdl/vda.log:

```
2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service
    successfully obtained the following list of 1 delivery controller(s)
     with which to register: 'CTXDDC.citrixlab.local (10.158.139.214)'.
2016-11-04 02:11:52.362 [ERROR] - RegistrationManager.
    AttemptRegistrationWithSingleDdc: Failed to register with http://
    CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar. Error:
    General security error (An error occurred in trying to obtain a TGT:
     Client not found in Kerberos database (6))
2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
    connect to the delivery controller 'http://CTXDDC.citrixlab.local
    :80/Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')
Check the following:- The system clock is in sync between this machine
    and the delivery controller.
-  The Active Directory provider (e.g. winbind daemon) service is
    running and correctly configured.
-  Kerberos is correctly configured on this machine.
If the problem persists, please refer to Citrix Knowledge Base article
    CTX117248 for further information.
Error Details:
Exception 'General security error (An error occurred in trying to
    obtain a TGT: Client not found in Kerberos database (6))' of type '
    class javax.xml.ws.soap.SOAPFaultException'.
2016-11-04 02:11:52.362 [INFO ] - RegistrationManager.
    AttemptRegistrationWithSingleDdc: The current time for this VDA is
    Fri Nov 04 02:11:52 EDT 2016.
Ensure that the system clock is in sync between this machine and the
    delivery controller.
Verify the NTP daemon is running on this machine and is correctly
    configured.
2016-11-04 02:11:52.364 [ERROR] - Could not register with any
    controllers. Waiting to try again in 120000 ms. Multi-forest - false
2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
    register with any controllers in the last 470 minutes.
<!--NeedCopy-->
```

/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 solucionar 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. Ejecute /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 en Ubuntu muestran una pantalla gris

Este problema ocurre cuando se lanza una sesión, que luego se bloquea en un escritorio vacío. Además, la consola de la máquina de SO de servidor también muestra una pantalla en gris cuando usted inicia sesión con una cuenta de usuario local.

Para solucionar 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

Falla el lanzamiento de sesiones de escritorio en Ubuntu porque falta el directorio home

/var/log/xdl/hdx.log:

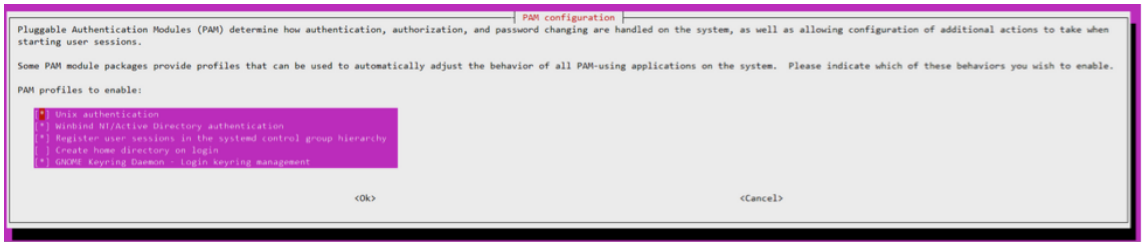
```
2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
   failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)

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.
<!--NeedCopy-->
```

> **Consejo:**

> La causa raíz de este problema es que el directorio home no se crea para el administrador de dominio.

Para solucionar este problema:

1. En una línea de comandos, escriba **pam-auth-update**.
2. En la ventana emergente resultante, compruebe si **Create home directory on login** está seleccionado.



La sesión no puede iniciarse o finaliza rápidamente con el error 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.
<!--NeedCopy-->
```

O bien, para distribuciones de Ubuntu, use los registros de /var/log/syslog:

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

```



```
3  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.
4
5  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.
6
7  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.
8
9  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.]
10
11 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
12 <!--NeedCopy-->
```

Algunos grupos o módulos no tienen efecto hasta que se reinicia la máquina. Cuando aparecen mensajes de error de **dbus** en los registros, Citrix recomienda reiniciar el sistema e intentarlo de nuevo.

SELinux impide que SSHD acceda al directorio particular (home)

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

/var/log/ctxinstall.log:

```
1  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
2
3  Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
       sbin/sshd from setattr access on the directory /root.
4
5  *****  Plugin catchall_boolean (89.3 confidence) suggests
       ******************
6
7  If you want to allow polyinstantiation to enabled
8
9     Then you must tell SELinux about this by enabling the '
       polyinstantiation_enabled' boolean.
```



```
10
11 You can read 'None' man page for more details.
12
13     Do
14
15        setsebool -P polyinstantiation_enabled 1
16
17 *****  Plugin catchall (11.6 confidence) suggests
    **************************
18
19 If you believe that sshd should be allowed setattr access on the root
    directory by default.
20
21 Then you should report this as a bug.
22
23 You can generate a local policy module to allow this access.
24
25       Do
26
27        allow this access for now by executing:
28
29        # grep sshd /var/log/audit/audit.log | audit2allow -M mypol
30
31 # semodule -i mypol.pp
32 <!--NeedCopy-->
```

Para solucionar este problema:

1. Inhabilite SELinux cambiando lo siguiente en /etc/selinux/config

   SELINUX=disabled

2. Reinicie el VDA.

Instalar Linux Virtual Delivery Agent para RHEL o CentOS

June 17, 2022

Puede elegir entre seguir los pasos de este artículo para la instalación manual o utilizar Easy Install para la instalación y configuración automáticas. Easy Install ahorra tiempo y trabajo y es menos propenso a errores que la instalación manual.

> **Nota** Use Easy Install solo para instalaciones nuevas. No utilice Easy Install para actualizar una instalación existente.

Paso 1: Prepare RHEL 7/CentOS 7 o RHEL 6/CentOS 6 para la instalación del VDA

Paso 1a: Verifique la configuración de red

Citrix recomienda que la red esté conectada y correctamente configurada antes de continuar.

Paso 1b: Establezca el nombre de host

> **Nota:**
>
> Actualmente, Linux VDA no admite el truncamiento del nombre de NetBIOS. Por lo tanto, el nombre de host no debe superar los 15 caracteres.

Para que el nombre de host de la máquina se notifique correctamente, cambie el archivo **/etc/hostname** para que solo contenga el nombre de host de la máquina.

`HOSTNAME`=**nombre del host**

Paso 1c: Asigne una dirección de bucle invertido al nombre de host

> **Nota:**
>
> Actualmente, Linux VDA no admite el truncamiento del nombre de NetBIOS. Por lo tanto, el nombre de host no debe superar los 15 caracteres.

Para que se notifiquen correctamente el nombre de dominio DNS y el nombre de dominio completo de la máquina (FQDN), cambie la siguiente línea del archivo **/etc/hosts** para que contenga el nombre de dominio completo y el nombre de host en 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

Quite las demás referencias a **hostname-fqdn** o **hostname** de otras entradas del archivo.

> **Consejo:**
>
> Use solamente caracteres de "a"a "z", de "A"a "Z", de 0 a 9 y guiones (-). No utilice guiones bajos (_), espacios ni otros símbolos. No inicie un nombre de host con un número ni lo termine con un guión. Esta regla también se aplica a nombres de host de Delivery Controller.

Paso 1d: Compruebe el nombre de host

Compruebe que el nombre de host está definido correctamente:


```
hostname
<!--NeedCopy-->
```

Este comando devuelve solo el nombre de host de la máquina, no su nombre de dominio completo (FQDN).

Compruebe que el nombre de dominio completo (FQDN) está definido correctamente:

```
hostname -f
<!--NeedCopy-->
```

Este comando devuelve el nombre de dominio completo de la máquina.

Paso 1e: Compruebe la resolución de nombres y la disponibilidad del servicio

Compruebe que se puede resolver el nombre de dominio completo (FQDN) y haga ping al controlador de dominio y al Delivery Controller:

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

Si no puede resolver el FQDN o hacer ping en alguna de estas máquinas, revise los pasos antes de continuar.

Paso 1f: Configure la sincronización horaria

Mantener sincronizados los relojes de los VDA, los Delivery Controllers y los controladores de dominio es fundamental. Ahora bien, alojar Linux VDA como una máquina virtual puede causar problemas de reloj sesgado. Por este motivo, se recomienda sincronizar la hora con un servicio remoto de sincronización horaria.

RHEL 6.x y las versiones anteriores usan el demonio de NTP (`ntpd`) para la sincronización del reloj, mientras que el entorno RHEL 7.x predeterminado utiliza un demonio más reciente, Chrony (`chronyd`). La configuración y el proceso de funcionamiento de los dos servicios son similares.

Configurar el servicio NTP (solo RHEL 6/CentOS 6) Como usuario root, modifique **/etc/ntp.conf** y agregue una entrada de servidor para cada servidor horario remoto:


```
server peer1-fqdn-or-ip-address iburst

server peer2-fqdn-or-ip-address iburst
<!--NeedCopy-->
```

En una implementación típica, sincronice la hora con los controladores del dominio local, no directamente con grupos públicos de servidores NTP. Agregue una entrada de servidor para cada controlador de dominio de Active Directory que tenga en el dominio.

Quite todas las demás entradas **server** de la lista, incluidas las entradas ***.pool.ntp.org** de loopback IP address, localhost y public server.

Guarde los cambios y reinicie el demonio de NTP:

```
sudo /sbin/service ntpd restart
<!--NeedCopy-->
```

Configurar el servicio Chrony (solo RHEL 7/CentOS 7) Como usuario root, modifique **/etc/chrony.conf** y agregue una entrada de servidor para cada servidor horario remoto:

```
server peer1-fqdn-or-ip-address iburst

server peer2-fqdn-or-ip-address iburst
<!--NeedCopy-->
```

En una implementación típica, sincronice la hora con los controladores del dominio local, no directamente con grupos públicos de servidores NTP. Agregue una entrada de servidor para cada controlador de dominio de Active Directory que tenga en el dominio.

Quite todas las demás entradas server de la lista, incluidas las entradas ***.pool.ntp.org** de loopback IP address, localhost y public server.

Guarde los cambios y reinicie el demonio de Chrony:

```
sudo /sbin/service chronyd restart
<!--NeedCopy-->
```

Paso 1g: Instale OpenJDK

Linux VDA depende de OpenJDK. Por regla general, el entorno en tiempo de ejecución se instala durante la instalación del sistema operativo.

Confirme la versión correcta:

- RHEL 7/CentOS 7:


```
sudo yum info java-1.8.0-openjdk
<!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
sudo yum info java-1.7.0-openjdk
<!--NeedCopy-->
```

El OpenJDK previamente empaquetado puede ser una versión anterior. Actualice a la versión más reciente como se requiere:

- RHEL 7/CentOS 7:

```
sudo yum -y update java-1.8.0-openjdk
<!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
sudo yum -y update java-1.7.0-openjdk
<!--NeedCopy-->
```

Establezca la variable de entorno **JAVA_HOME** agregando la siguiente línea al archivo **~/.bashrc**:

```
export JAVA\\_HOME=/usr/lib/jvm/java
```

Abra un nuevo shell y compruebe la versión de Java:

```
java -version
<!--NeedCopy-->
```

> **Tip:**
>
> Para evitar problemas, compruebe que solo ha instalado OpenJDK 1.7.0 o 1.8.0 en el caso de RHEL 6/CentOS 6, o solo OpenJDK 1.8.0 en el caso de RHEL 7/CentOS 7. Quite todas las demás versiones de Java que haya en su sistema.

Paso 1h: Instale PostgreSQL

Linux VDA requiere PostgreSQL 8.4 (o una versión posterior) en RHEL 6 o PostgreSQL 9.2 (o una versión posterior) en RHEL 7.

Instale los siguientes paquetes:

```
sudo yum -y install postgresql-server

sudo yum -y install postgresql-jdbc
<!--NeedCopy-->
```


El siguiente paso posterior a la instalación es necesario para inicializar la base de datos y para que el servicio se inicie en el inicio de la máquina. Los archivos de base de datos se crean en **/var/lib/pgsql/-data**. El comando difiere de PostgreSQL 8 a PostgreSQL 9:

- Solo RHEL 7: PostgreSQL 9

```
sudo postgresql-setup initdb
<!--NeedCopy-->
```

- Solo RHEL 6: PostgreSQL 8

```
sudo /sbin/service postgresql initdb
<!--NeedCopy-->
```

Paso 1i: Inicie PostgreSQL

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

- Solo RHEL 7: PostgreSQL 9

```
sudo systemctl enable postgresql

sudo systemctl start postgresql
<!--NeedCopy-->
```

- Solo RHEL 6: PostgreSQL 8

```
sudo /sbin/chkconfig postgresql on

sudo /sbin/service postgresql start
<!--NeedCopy-->
```

Compruebe la versión de PostgreSQL con:

```
psql --version
<!--NeedCopy-->
```

Compruebe que se ha definido el directorio de datos mediante la utilidad de línea de comandos **psql**:

```
sudo -u postgres psql -c 'show data_directory'
<!--NeedCopy-->
```

> **Importante:**
>
> En esta versión, se ha agregado una dependencia nueva para gperftools-libs. Esta dependencia no existe en el repositorio original. Agregue un repositorio nuevo mediante el comando `sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-`

> `latest-6.noarch.rpm`.
> Solo afecta a RHEL 6/CentOS 6. Ejecute el comando antes de instalar el paquete de Linux VDA.

Paso 2: Prepare el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Realice los siguientes cambios en función de la plataforma del hipervisor que utilice. No se requieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix XenServer

Si está habilitada la funcionalidad de sincronización horaria de XenServer, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como XenServer intentarán administrar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

En algunas distribuciones de Linux, si se ejecuta un kernel Linux paravirtualizado con XenServer Tools instalado, puede comprobar si la función de sincronización horaria de XenServer está presente y habilitarla en la máquina virtual de Linux:

```
su -
cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Este comando devuelve 0 o 1:

- 0. La funcionalidad de sincronización horaria está habilitada, por lo que se debe inhabilitar.
- 1. La funcionalidad de sincronización horaria está inhabilitada, por lo que no es necesaria ninguna otra acción.

Si el archivo /proc/sys/xen/independent_wallclock no está presente, no es necesario que siga estos pasos.

Si se habilita, inhabilite la función de sincronización de tiempo con un 1 en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:


```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux que tienen instalados los servicios de integración de Hyper-V para Linux pueden aplicar la funcionalidad de sincronización horaria de Hyper-V para usar la hora del sistema operativo del host. Para que el reloj del sistema no se desincronice, esta funcionalidad se debe habilitar junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para ver la configuración de una máquina virtual Linux, seleccione **Integration Services**.
3. Compruebe que **Time synchronization** está seleccionado.

> **Nota** Este método difiere de XenServer y VMware, donde se inhabilita la sincronización horaria del host para evitar conflictos con NTP. La sincronización horaria de Hyper-V puede coexistir y complementarse con la sincronización horaria de NTP.

Corregir la sincronización horaria en ESX y ESXi

Si está habilitada la funcionalidad de sincronización horaria de VMware, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como el hipervisor intentarán sincronizar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host.

Si ejecuta un kernel Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Modifique 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 **Advanced**, desmarque la casilla **Synchronize guest time with host**.

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

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

- Samba Winbind
- Servicio de autenticación Quest
- Centrify DirectControl
- SSSD

Siga las instrucciones en función del método elegido.

> **Nota:**
>
> Los inicios de sesión pueden fallar cuando se usa el mismo nombre de usuario para la cuenta local en el Linux VDA y la cuenta en AD.

Samba Winbind

Instale o actualice los paquetes requeridos:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-
    workstation authconfig oddjob-mkhomedir
<!--NeedCopy-->
```

Habilitar el demonio de Winbind para que se inicie a la misma vez que la máquina El demonio de Winbind debe configurarse para iniciarse en el arranque:

```
sudo /sbin/chkconfig winbind on
<!--NeedCopy-->
```

Configurar la autenticación de Winbind Configure la máquina para la autenticación Kerberos mediante Winbind:

```
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
<!--NeedCopy-->
```

Donde **REALM** es el nombre del territorio Kerberos en mayúsculas y **domain** es el nombre NetBIOS del dominio.

Si se necesitan las búsquedas basadas en DNS del nombre de territorio Kerberos y del servidor KDC, agregue las dos opciones siguientes al comando anterior:

```
--enablekrb5kdcdns --enablekrb5realmdns
```


Ignore los errores que devuelva el comando `authconfig` que indican que el servicio `winbind` no se puede iniciar. Estos errores ocurren cuando `authconfig` intenta iniciar el servicio `winbind` cuando la máquina aún no está unida al dominio.

Abra **/etc/samba/smb.conf** y agregue las siguientes entradas en la sección [Global], pero después de la sección que haya generado la herramienta `authconfig`:

```
kerberos method = secrets and keytab
winbind refresh tickets = true
```

Linux VDA necesita el archivo de sistema /etc/krb5.keytab para autenticarse y registrarse en Delivery Controller. El parámetro anterior de método Kerberos obliga a Winbind a crear el archivo de sistema keytab la primera vez que la máquina se une al dominio.

Unirse al dominio de Windows Se requiere que el controlador de dominio esté accesible y se necesita disponer de una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

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

Configurar PAM para Winbind De forma predeterminada, la configuración del módulo Winbind PAM (pam_winbind) no permite el almacenamiento en caché de tíquets de Kerberos ni la creación del directorio principal. Abra `/etc/security/pam_winbind.conf` y agregue o cambie las siguientes entradas en la sección [Global]:

```
krb5_auth = yes
krb5_ccache_type = FILE
mkhomedir = yes
```

Compruebe que no hay signos de punto y coma al principio de cada parámetro. Estos cambios requieren reiniciar el demonio de Winbind:

```
1 sudo /sbin/service winbind restart
2 <!--NeedCopy-->
```

> **Consejo:**
>
> El demonio winbind permanece en ejecución solo si la máquina está unida a un dominio.

Abra **/etc/krb5.conf** y edite el siguiente parámetro en la sección [libdefaults], cambiando el tipo KEYRING por FILE:


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

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA, Windows y Linux, tengan un objeto de equipo en Active Directory.

Ejecute el comando **net ads** de Samba para comprobar que la máquina está unida a un dominio:

```
1 sudo net ads testjoin
2 <!--NeedCopy-->
```

Ejecute el siguiente comando para comprobar la información adicional de dominio y objeto de equipo:

```
1 sudo net ads info
2 <!--NeedCopy-->
```

Verificar la configuración de Kerberos Para verificar que Kerberos está configurado correctamente para su uso con Linux VDA, compruebe que el archivo del sistema keytab se ha creado y contiene claves válidas:

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando `kinit` de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (\) al signo de dólar ($) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

Compruebe que el tíquet de TGT de la cuenta de la máquina se ha almacenado en caché:

```
1 sudo klist
2 <!--NeedCopy-->
```

Examine los datos de la cuenta de la máquina:

```
1 sudo net ads status
2 <!--NeedCopy-->
```


Verificar la autenticación de usuario Use la herramienta **wbinfo** para comprobar que los usuarios de dominio pueden autenticarse en el dominio:

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

El dominio especificado es el nombre de dominio de AD, no el nombre del territorio Kerberos. Para shell de Bash, debe anteponerse una barra diagonal inversa (\) a otra barra diagonal inversa. Este comando devuelve un mensaje que indica si la operación se ha realizado correctamente o no.

Para verificar que el módulo Winbind PAM está configurado correctamente, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

Compruebe que los vales que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado:

```
klist
<!--NeedCopy-->
```

Salga de la sesión:

```
exit
<!--NeedCopy-->
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Servicio de autenticación Quest

Configurar Quest en el controlador de dominio Se asume que se ha instalado y configurado el software de Quest en los controladores de dominio de Active Directory, y que se han recibido los privilegios administrativos necesarios para crear objetos de equipo en Active Directory.

Permitir que los usuarios de dominio inicien sesión en máquinas con Linux VDA Para permitir que los usuarios de dominio puedan establecer sesiones HDX en una máquina con Linux VDA:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory correspondientes a esa cuenta de usuario.
2. Seleccione la ficha **Unix Account**.
3. Active **Unix-enabled**.

4. Defina **Primary GID Number** con el ID de grupo de un grupo de usuarios real del dominio.

> **Nota:**
>
> Estas instrucciones son equivalentes a definir usuarios de dominio para que inicien sesión desde la consola, RDP, SSH u otro protocolo de comunicación remota.

Configurar Quest en Linux VDA

Solución a la aplicación de la directiva de SELinux En el entorno predeterminado de RHEL, SELinux se aplica en su totalidad. Esto interfiere con los mecanismos de IPC de sockets para dominios Unix que utiliza Quest y evita que los usuarios inicien sesión.

Lo más conveniente para solucionar este problema es inhabilitar SELinux. Como usuario root, modifique **/etc/selinux/config** y cambie el parámetro **SELinux**:

```
SELINUX=permissive
```

Este cambio requiere un reinicio de la máquina:

```
reboot
<!--NeedCopy-->
```

> **Importante:**
>
> Utilice esta opción con cuidado. Habilitar la directiva de SELinux tras haberla inhabilitado puede causar un bloqueo absoluto, incluso para el usuario root y otros usuarios locales.

Configurar el demonio de VAS La renovación automática de tíquets de Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar inhabilitada.

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```

Este comando establece el intervalo de renovación a nueve horas (32 400 segundos), es decir, una hora menos que la validez predeterminada de 10 horas del tíquet. Establezca esta opción en un valor inferior en sistemas con una validez más corta de tíquets.

Configurar PAM y NSS Para habilitar el inicio de sesión del usuario de dominio mediante HDX y otros servicios como su, ssh y RDP, ejecute los siguientes comandos para configurar PAM y NSS de forma manual:


```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

El parámetro user es un usuario de dominio con permisos para unir equipos al dominio de Active Directory. La variable **domain-name** es el nombre DNS del dominio; por ejemplo, ejemplo.com.

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA, Windows y Linux, tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Quest en el dominio:

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. En cambio, 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 pueda autenticar usuarios de dominio a través de PAM, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```


Compruebe que los vales que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Salga de la sesión:

```
exit
<!--NeedCopy-->
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Centrify DirectControl

Unirse al dominio de Windows Con el agente 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
<!--NeedCopy-->
```

El parámetro "user"es un 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, Windows y Linux, tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Centrify en el dominio:

```
su -

adinfo
<!--NeedCopy-->
```

Compruebe que el valor Joined to domain sea válido y que el modo CentrifyDC devuelva el valor connected. Si el modo se queda bloqueado en el estado inicial, el cliente Centrify tiene problemas de conexión o autenticación en el servidor.

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo -diag
<!--NeedCopy-->
```


Pruebe la conectividad a los distintos servicios de Active Directory y Kerberos: Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

```
adinfo --test
<!--NeedCopy-->
```

SSSD

Si utiliza SSSD, siga las instrucciones de esta sección. Esta sección contiene instrucciones para unir una máquina Linux VDA a un dominio Windows, y ofrece instrucciones para configurar la autenticación de Kerberos.

Para configurar SSSD en RHEL y CentOS, lleve a cabo lo siguiente:

1. Unirse al dominio y crear un keytab de host con Samba
2. Configurar SSSD
3. Configurar NSS/PAM
4. Verificar la configuración de Kerberos
5. Verificar la autenticación de usuario

Software requerido El proveedor de Active Directory se introdujo por primera vez con SSSD 1.9.0. Si usa una versión anterior, siga las instrucciones proporcionadas en Configurar el proveedor de LDAP con Active Directory.

Se han probado y verificado los siguientes entornos con las instrucciones de este artículo:

- RHEL 7.3 o versiones posteriores/CentOS 7.3 o versiones posteriores
- Linux VDA versión 1.3 o posterior

Unirse al dominio y crear un keytab de host con Samba SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo de sistema keytab. Puede usar `adcli`, `realmd`, `Winbind` o `Samba` en su lugar.

En esta sección, se describe solo el enfoque de `Samba`. Para `realmd`, consulte la documentación de RHEL o CentOS. Debe seguir estos pasos para configurar SSSD.

En el cliente Linux, con archivos correctamente configurados:

- /etc/krb5.conf
- /etc/samba/smb.conf:

Configure la máquina para la autenticación Kerberos y Samba:


```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
   REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
<!--NeedCopy-->
```

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

Si se necesitan las búsquedas basadas en DNS del nombre de territorio Kerberos y del servidor KDC, 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 que haya generado la herramienta **authconfig**:

```
kerberos method = secrets and keytab
```

Únase al dominio de Windows. Para ello, se requiere que el controlador de dominio esté accesible y se necesita disponer de una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

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

Configurar SSSD Configurar SSSD consta de los siguientes pasos:

- Instale el paquete **sssd-ad** en Linux VDA.
- Realice cambios de configuración en varios archivos (por ejemplo, sssd.conf).
- Inicie el **servicio sssd**.

A continuación, se ofrece un ejemplo de configuración de **sssd.conf** (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
<!--NeedCopy-->
```

Reemplace **ad.domain.com** y **server.ad.example.com** por los valores correspondientes. Para obtener más información, consulte sssd-ad(5) - Linux man page.

Establezca la pertenencia y los permisos de archivos 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 que la creación del directorio de inicio sea compatible con SELinux:

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir – -update

sudo service sssd start

sudo chkconfig sssd on
<!--NeedCopy-->
```

Verificar la configuración de Kerberos Compruebe que el archivo **keytab** del sistema se haya creado y contenga claves válidas:

```
sudo klist -ke
<!--NeedCopy-->
```


Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando **kinit** de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:

```
sudo kinit  – k MACHINE$@REALM
<!--NeedCopy-->
```

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (****) al signo de dólar (**$**) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

Compruebe que el tíquet de TGT de la cuenta de la máquina se ha almacenado en caché:

```
sudo klist
<!--NeedCopy-->
```

Verificar la autenticación de usuario Use el comando **getent** para saber si se admite el formato del inicio de sesión y si funciona NSS:

```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

El parámetro **DOMAIN** indica la versión corta del nombre de dominio. Si se necesita otro formato de inicio de sesión, compruébelo 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 del sufijo NetBIOS: `username@DOMAIN`

Para verificar que el módulo SSSD PAM está configurado correctamente, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
sudo ssh localhost  – l DOMAIN\username

id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el **uid** devuelto por el comando:

```
ls /tmp/krb5cc_{
 uid }
```



```
3
4 <!--NeedCopy-->
```

Compruebe que los vales que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

```
1 klist
2 <!--NeedCopy-->
```

Paso 4: Instale Linux VDA

Paso 4a: Desinstale la versión anterior

Si ya ha instalado una versión anterior de Linux VDA, desinstálela antes de instalar la nueva versión.

1. Detenga los servicios de Linux VDA:

   ```
   1 sudo /sbin/service ctxvda stop
   2
   3 sudo /sbin/service ctxhdx stop
   4 <!--NeedCopy-->
   ```

2. Desinstale el paquete:

   ```
   1 sudo rpm -e XenDesktopVDA
   2 <!--NeedCopy-->
   ```

> **Nota:**
>
> Se admite la actualización de las dos versiones anteriores.
>
> **Nota:**
>
> A partir de la versión 1.3, ha cambiado la ruta de instalación. En las versiones anteriores, los componentes de instalación se encontraban en **/usr/local/**. En cambio, la nueva ubicación es **/opt/Citrix/VDA/**.
>
> Para ejecutar un comando, se necesita la ruta completa. Como alternativa, puede agregar **/opt/Citrix/VDA/sbin** y **/opt/Citrix/VDA/bin** a la ruta del sistema.

Paso 4b: Descargue el paquete de Linux VDA

Vaya a la página web de Citrix y descargue el paquete de Linux VDA adecuado según su distribución de Linux.

Paso 4c: Instale Linux VDA

Instale el software de Linux VDA mediante Yum:

Para RHEL 7/CentOS 7:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.9:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.6/CentOS 6.6:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

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

Para RHEL 7/CentOS 7:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.9:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.6/CentOS 6.6:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

Lista de dependencias RPM para RHEL 7:

```
postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-1.8.0-openjdk >= 1.8.0

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

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

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

```



```
rpmlib(PayloadIsXz) <= 5.2-1
<!--NeedCopy-->
```

Lista de dependencias RPM para RHEL 6.9:

```
postgresql-jdbc >= 8.4

postgresql-server >= 8.4

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.5.4.7

GConf2 >= 2.28.0

system-config-firewall-base >= 1.2.27

policycoreutils-python >= 2.0.83

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

```



```
openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
<!--NeedCopy-->
```

Lista de dependencias RPM para RHEL 6.6/CentOS 6.6:

```
postgresql-jdbc >= 8.4

postgresql-server >= 8.4

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.5.4.7

GConf2 >= 2.28.0

system-config-firewall-base >= 1.2.27

policycoreutils-python >= 2.0.83

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

libXpm >= 3.5.10

```



```
libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0

xorg-x11-server-Xorg >= 1.15

xorg-x11-server-Xorg < 1.16

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
<!--NeedCopy-->
```

Paso 4d: Actualice la versión de Linux VDA (optativo)

Puede actualizar el software de Linux VDA desde las versiones 7.14 y 7.13 mediante Yum:

Para RHEL 7/CentOS 7:


```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.9:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.6/CentOS 6.6:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

Actualice el software de Linux VDA desde el administrador de paquetes RPM:

Para RHEL 7/CentOS 7:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.9:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

Para RHEL 6.6/CentOS 6.6:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

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

Paso 5: Instale controladores NVIDIA GRID

Para habilitar HDX 3D Pro, se requieren pasos adicionales para instalar los controladores de gráficos requeridos en el hipervisor y en las máquinas VDA.

Configure las siguientes opciones:

1. Citrix XenServer
2. VMware ESX

Siga las instrucciones para el hipervisor que haya elegido.

Citrix XenServer:

En esta sección, se detalla el proceso de instalación y configuración de los controladores NVIDIA GRID en Citrix XenServer.

VMware ESX:

Siga los pasos descritos en esta guía para instalar y configurar los controladores NVIDIA GRID para VMware ESX.

Máquinas VDA:

Siga estos pasos para instalar y configurar los controladores de cada invitado de VM de Linux:

1. Antes de comenzar, compruebe que la VM de Linux está apagada.
2. En XenCenter, agregue a la VM una GPU en el modo GPU PassThrough.
3. Inicie la VM de RHEL.

Ejecute los siguientes comandos para preparar la máquina para los controladores NVIDIA GRID:

```
yum install gcc

yum install "kernel-devel-$(uname -r)"

systemctl set-default multi-user.target
<!--NeedCopy-->
```

Siga los pasos indicados en el documento de Red Hat Enterprise Linux para instalar el controlador NVIDIA GRID.

> **Nota:**
>
> Durante la instalación de controladores de GPU, seleccione la opción predeterminada (“no”) para cada pregunta.
>
> **Importante:**
>
> Una vez habilitado GPU PassThrough, ya no se puede acceder a la máquina virtual Linux 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 capacidades de varios monitores y altas resoluciones, necesitará una licencia válida de NVIDIA. Para aplicar la licencia, siga la documentación del producto de "GRID Licensing Guide.pdf - DU-07757-001"de septiembre de 2015 (en inglés).

Paso 6: Configure Linux VDA

Después de instalar el paquete, debe configurar Linux VDA. Para ello, ejecute el script ctxsetup.sh. Antes de realizar cambios, este script examina el entorno existente y verifica si están instaladas todas las dependencias. Si fuera necesario, puede volver a ejecutar este script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manual o automáticamente con respuestas preconfiguradas. Consulte la ayuda del script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Configuración automatizada

En caso de una instalación automática, proporcione las opciones necesarias para el script de instalación con variables de entorno. Si están presentes todas las variables necesarias, el script no pide ninguna información.

Las variables de entorno admitidas son:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME** = **Y | N**: Linux VDA permite especificar 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**: Linux VDA necesita una lista de nombres de dominio completo de Delivery Controllers, separados por espacios, para registrarse en un Delivery Controller. Se debe especificar al menos un FQDN o alias de CNAME.

- **CTX_XDL_VDA_PORT** = **port-number**: Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP. Este 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 está 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 automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema para Linux Virtual Desktop. Se establece en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION** = **1 | 2 | 3 | 4**: Linux VDA requiere parámetros de configuración Kerberos para autenticarse en 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 admitido de integración de Active Directory que se va a utilizar:
  - 1 –Samba Winbind
  - 2 –Servicio de autenticación Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO** = **Y | N**: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. Si se selecciona HDX 3D Pro, Virtual Delivery Agent se configura para el modo de escritorios VDI (sesión única); es decir, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE** = **Y | N**: Indica si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos alojados. Para entornos HDX 3D Pro, establezca esta variable en Y. De forma predeterminada, esta variable está establecida en N.
- **CTX_XDL_SITE_NAME** = **dns-name**: Linux VDA detecta los servidores LDAP mediante DNS. Para limitar los resultados de 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**: Linux VDA consulta a DNS para detectar servidores LDAP. Sin embargo, si el DNS no puede proporcionar registros del servicio LDAP, se puede suministrar una lista de nombres FQDN de LDAP, separados por espacios, con el puerto de LDAP. Por ejemplo, ad1.miempresa.com:389. Esta variable está establecida en **<none>** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE** = **search-base-set**: Linux VDA consulta a LDAP a partir de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=miempresa,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar otra base de búsqueda (por ejemplo, OU=VDI,DC=miempresa,DC=com). Esta variable está establecida en **<none>** de forma predeterminada.
- **CTX_XDL_START_SERVICE** = **Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.

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-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Cuando ejecute el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que se crea. Citrix recomienda crear un archivo de script shell a partir de los comandos anteriores con **#!/bin/bash** en la primera línea.

También puede especificar todos los parámetros con un único 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_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Quitar cambios de configuración

En algunos casos, puede que sea necesario quitar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete de Linux VDA.

Consulte la ayuda de este script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
<!--NeedCopy-->
```

Para quitar los cambios de configuración:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--NeedCopy-->
```

> **Importante:**
>
> Este script elimina todos los datos de configuración de la base de datos y provoca que Linux VDA deje de funcionar.

Registros de configuración

Los scripts **ctxcleanup.sh** y **ctxsetup.sh** muestran errores en la consola, con información adicional que se enviará a un archivo de registros de configuración **/tmp/xdl.configure.log**.

Reinicie los servicios de Linux VDA para que los cambios surtan efecto.

Paso 7: Ejecute Linux VDA

Una vez configurado Linux VDA mediante el script **ctxsetup.sh**, utilice los siguientes comandos para controlarlo.

Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxhdx start

```



```
sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Comprobar el estado de Linux VDA:

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

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

Paso 8: Cree el catálogo de máquinas en XenApp o XenDesktop

El proceso de creación de catálogos de máquinas y de incorporación de máquinas Linux es similar al proceso habitual de VDA para Windows. Para ver una descripción detallada sobre cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Existen restricciones que diferencian el proceso de creación de catálogos de máquinas con VDA para Windows del mismo proceso con VDA para Linux:

- Para el sistema operativo, seleccione:
  - La opción de SO de servidor para un modelo de entrega de escritorios compartidos alojados.
  - La opción de SO de escritorio para un modelo de entrega de escritorios VDI dedicados.
- Compruebe que las máquinas están establecidas como máquinas cuyas opciones de administración de energía no están administradas.

- Como los agentes Linux VDA no admiten MCS, elija el método de implementación PVS u **Otro servicio o tecnología** (imágenes existentes).
- No mezcle máquinas con agentes VDA para Windows y Linux en el mismo catálogo.

> **Nota:**
>
> Las primeras versiones de Citrix Studio no admitían el concepto de "SO Linux". Sin embargo, seleccionar la opción SO de servidor Windows o SO de servidor implica un modelo equivalente de entrega de escritorios compartidos alojados. Seleccionar la opción SO de escritorio Windows o SO de escritorio implica un modelo de entrega de un usuario por máquina.
>
> **Sugerencia:**
>
> Si quita una máquina y luego la vuelve a unir al dominio de Active Directory, esa máquina se debe quitar y volver a agregar al catálogo de máquinas.

Paso 9: Cree el grupo de entrega en XenApp o XenDesktop

El proceso de creación de un grupo de entrega y de incorporación de catálogos de máquinas con agentes VDA para Linux es muy similar al proceso de máquinas con agentes VDA para Windows. Para ver una descripción detallada sobre cómo completar estas tareas, consulte Crear grupos de entrega.

Se aplican las siguientes restricciones para crear grupos de entrega que contengan catálogos de máquinas con Linux VDA:

- Para el tipo de entrega, seleccione Escritorios o Aplicaciones.
- Los grupos y usuarios de AD que seleccione deben estar correctamente configurados para poder iniciar sesión en las máquinas con VDA para Linux.
- No permita que usuarios no autenticados (anónimos) inicien sesión.
- No mezcle el grupo de entrega con catálogos de máquinas que contienen máquinas Windows.

> **Importante:**
>
> Se admite la publicación de aplicaciones con Linux VDA 1.4 y versiones posteriores. Linux VDA no admite la entrega de escritorios ni aplicaciones a la misma máquina.

Instalar Linux Virtual Delivery Agent para SUSE

February 12, 2024

Puede elegir entre seguir los pasos de este artículo para la instalación manual o utilizar Easy Install para la instalación y configuración automáticas. Easy Install ahorra tiempo y trabajo y es menos propenso a errores que la instalación manual.

> **Nota** Use Easy Install solo para instalaciones nuevas. No utilice Easy Install para actualizar una instalación existente.

Paso 1: Prepare la instalación

Paso 1a: Inicie 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 de texto:

```
su -

yast
<!--NeedCopy-->
```

Para iniciar la herramienta YaST de interfaz gráfica:

```
su -

yast2 &
<!--NeedCopy-->
```

Paso 1b: Configure la red

En las siguientes secciones, se ofrece información sobre la configuración de las opciones y los servicios de red que usa el VDA para Linux. Utilice la herramienta YaST para configurar las opciones de red, no otros métodos del tipo Network Manager. Estas instrucciones se basan en la herramienta YaST de interfaz de usuario. Se puede usar la herramienta YaST de texto, pero tiene otro método de navegación que no se documenta aquí.

Configurar el nombre de host y DNS

1. Abra las opciones de red de YaST.
2. Solo SLED 12: En la ficha **Global Options**, cambie **Network Setup Method** a **Wicked Service**.
3. Abra la ficha **Hostname/DNS**.
4. Desactive **Change hostname via DHCP**.
5. Active **Assign Hostname to Loopback IP**.
6. Modifique lo siguiente para que refleje su propia configuración de red:

- Host name: Agregue el nombre de host DNS de la máquina.
- Domain name: Agregue el nombre de dominio DNS de la máquina.
- Name server: Agregue la dirección IP del servidor DNS. Por regla general, es la dirección IP del controlador de dominio de Active Directory.
- Domain search list: Agregue el nombre de dominio DNS.

> **Nota:**
>
> Actualmente, Linux VDA no admite el truncamiento del nombre NetBIOS. Por lo tanto, el nombre de host no debe superar los 15 caracteres.
>
> **Consejo:**
>
> Use solamente caracteres de "a"a "z", de "A"a "Z", de 0 a 9 y guiones (-). No utilice guiones bajos (_), espacios ni otros símbolos. No inicie un nombre de host con un número ni lo termine con un guión. Esta regla también se aplica a nombres de host de Delivery Controller.

Inhabilitar DNS de multidifusión Solo en SLED, la configuración predeterminada tiene habilitado DNS de multidifusión (mDNS), lo que puede dar lugar a resoluciones de nombres incoherentes. mDNS no está habilitado en SLES de forma predeterminada, por lo que no es necesario hacer nada.

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

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

Para:

```
hosts: files dns
```

Comprobar el nombre de host Compruebe que el nombre de host está definido correctamente:

```
1 hostname
2 <!--NeedCopy-->
```

Este comando devuelve solo el nombre de host de la máquina, no su nombre de dominio completo (FQDN).

Compruebe que el nombre de dominio completo (FQDN) está definido correctamente:

```
1 hostname -f
2 <!--NeedCopy-->
```

Este comando devuelve el nombre de dominio completo (FQDN) de la máquina.

Comprobar la resolución de nombres y la disponibilidad del servicio Compruebe que se puede resolver el nombre de dominio completo (FQDN) y haga ping al controlador de dominio y al Delivery Controller:


```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

Si no puede resolver el FQDN o hacer ping en alguna de estas máquinas, revise los pasos antes de continuar.

Paso 1c: Configure el servicio NTP

Mantener sincronizados los relojes de los VDA, los Delivery Controllers y los controladores de dominio es fundamental. Ahora bien, alojar Linux VDA como una máquina virtual puede causar problemas de reloj sesgado. Por eso, se prefiere mantener la hora sincronizada mediante un servicio remoto de NTP. Algunos cambios podrían ser necesarios en la configuración predeterminada de NTP:

1. Abra la configuración de NTP de YaST y seleccione la ficha **General Settings**.
2. En la sección "Start NTP Daemon", active **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 tipo de servidor en **Server Type** y haga clic en **Next**.
6. Escriba el nombre DNS del servidor NTP en el campo Address. Por regla general, este servicio se aloja en el controlador de dominio de Active Directory.
7. Deje el campo de opciones sin cambios.
8. Haga clic en **Test** para comprobar la disponibilidad del servicio NTP.
9. Haga clic en **OK** en las ventanas para guardar los cambios.

> **Nota:**
>
> En caso de implementaciones de SLES 12, puede que el demonio de NTP no se inicie. Este es un problema conocido de SUSE con directivas de AppArmor. Consulte la solución del problema para obtener más información.

Paso 1d: Instale paquetes dependientes de Linux VDA

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

- PostgreSQL

  - SLED/SLES 11: versión 9.1 o posterior
  - SLED/SLES 12: Versión 9.3 o una posterior

- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 o una versión posterior
- Cups
  - SLED/SLES 11: versión 1.3.7 o posterior
  - SLED/SLES 12: Versión 1.6.0 o una posterior
- Filtros Foomatic
  - SLED/SLES 11: versión 3.0.0 o posterior
  - SLED/SLES 12: Versión 1.0.0 o una posterior
- ImageMagick
  - SLED/SLES 11: versión 6.4.3.6 o posterior
  - SLED/SLES 12: Versión 6.8 o una posterior

Agregar repositorios Algunos paquetes necesarios no están disponibles en todos los repositorios de SUSE Linux Enterprise:

- SLED 11: PostgreSQL está disponible para SLES 11, pero no para SLED 11.
- SLES 11: OpenJDK y Open Motif están disponibles para SLED 11, pero no para SLES 11.
- SLED 12: PostgreSQL está disponible para SLES 12, pero no para SLED 12. ImageMagick está disponible mediante la ISO del SDK de SLE 12 o mediante el repositorio en línea.
- SLES 12: No presenta problemas. Todos los paquetes están disponibles. ImageMagick está disponible mediante la ISO del SDK de SLE 12 o mediante el repositorio en línea.

Para resolver este problema, obtenga los paquetes que faltan en la edición que quiere instalar de los medios pertenecientes a la edición alternativa de SLE. Es decir, obtener los paquetes que faltan para instalar SLED de los medios de SLES y, viceversa, es decir, obtener los paquetes que faltan para instalar SLES de los medios de SLED. El enfoque siguiente monta los archivos ISO de SLED y SLES, y agrega los repositorios.

- En SLED 11, ejecute los comandos:

```
sudo mkdir -p /mnt/sles

sudo mount -t iso9660 path-to-iso/SLES-11-SP4-DVD-x86_64-GM-DVD1.iso /
   mnt/sles

sudo zypper ar -f /mnt/sles sles
<!--NeedCopy-->
```


- En SLES 11, ejecute los comandos:

```
sudo mkdir -p /mnt/sled

sudo mount -t iso9660 path-to-iso/SLED-11-SP4-DVD-x86_64-GM-DVD1.iso /
   mnt/sled

sudo zypper ar -f /mnt/sled sled
<!--NeedCopy-->
```

- En SLED 12, ejecute los comandos:

```
sudo mkdir -p /mnt/sles

sudo mount -t iso9660 path-to-iso/SLES-12-SP2-DVD-x86_64-GM-DVD1.iso /
   mnt/sles

sudo zypper ar -f /mnt/sles sles
<!--NeedCopy-->
```

- En SLED/SLES 12, ejecute los comandos:

```
sudo mkdir -p /mnt/sdk

sudo mount -t iso9660 path-to-iso/SLE-12-SP3-SDK-DVD-x86_64-GM-DVD1.iso
    /mnt/sdk

sudo zypper ar -f /mnt/sdk sdk
<!--NeedCopy-->
```

Instalar el cliente Kerberos Instale el cliente Kerberos para la autenticación mutua entre el Linux VDA y los Delivery Controllers:

```
sudo zypper install krb5-client
<!--NeedCopy-->
```

La configuración del cliente Kerberos depende de la integración de Active Directory que se use. Consulte la siguiente descripción.

Instalar OpenJDK Linux VDA depende de OpenJDK 1.7.0.

> **Consejo:**
>
> Para evitar problemas, instale solo la versión 1.7.0 de OpenJDK. Quite todas las demás versiones de Java que haya en su sistema.

- **SLED:**

1. En SLED, Java Runtime Environment suele instalarse con el sistema operativo. Compruebe si se ha instalado:

```
sudo zypper info java-1_7_0-openjdk
<!--NeedCopy-->
```

2. Actualice a la versión más reciente si se notifica el estado como no actualizado:

```
sudo zypper update java-1_7_0-openjdk
<!--NeedCopy-->
```

3. Compruebe la versión de Java:

```
java -version
<!--NeedCopy-->
```

- **SLES:**

1. En SLES, instale Java Runtime Environment:

```
sudo zypper install java-1_7_0-openjdk
<!--NeedCopy-->
```

2. Compruebe la versión de Java:

```
java -version
<!--NeedCopy-->
```

Instalar PostgreSQL

- En SLED/SLES 11, instale los paquetes:

```
 sudo zypper install libecpg6

 sudo zypper install postgresql-init

 sudo zypper install postgresql

 sudo zypper install postgresql-server

 sudo zypper install postgresql-jdbc
 <!--NeedCopy-->
```

Tras la instalación, se requieren pasos adicionales para inicializar el servicio de la base de datos y para que PostgreSQL se inicie durante el arranque de la máquina:

```
 sudo /sbin/insserv postgresql

 sudo /etc/init.d/postgresql restart
 <!--NeedCopy-->
```


- En SLED/SLES 12, instale los paquetes:

```
sudo zypper install postgresql-init

sudo zypper install postgresql-server

sudo zypper install postgresql-jdbc
<!--NeedCopy-->
```

Tras la instalación, se requieren pasos adicionales para inicializar el servicio de la base de datos y para que PostgreSQL se inicie durante el arranque de la máquina:

```
sudo systemctl enable postgresql

sudo systemctl restart postgresql
<!--NeedCopy-->
```

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

Quitar repositorios Una vez instalados los paquetes dependientes, se pueden quitar los repositorios de la edición alternativa que se hayan instalado antes. Asimismo, se pueden desmontar los medios que se hayan montado:

- en SLED 11, ejecute los comandos para quitar los paquetes:

```
sudo zypper rr sles

sudo umount /mnt/sles

sudo rmdir /mnt/sles
<!--NeedCopy-->
```

- en SLES 11, ejecute los comandos para quitar los paquetes:

```
sudo zypper rr sled

sudo umount /mnt/sled

sudo rmdir /mnt/sled
<!--NeedCopy-->
```

- en SLED 12, ejecute los comandos para quitar los paquetes:

```
sudo zypper rr sles

sudo umount /mnt/sles

sudo rmdir /mnt/sles
<!--NeedCopy-->
```

- en SLED/SLES 12, ejecute los comandos para quitar los paquetes:


```
sudo zypper rr sdk

sudo umount /mnt/sdk

sudo rmdir /mnt/sd
<!--NeedCopy-->
```

Paso 2: Prepare la máquina virtual Linux para el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Realice los siguientes cambios en función de la plataforma del hipervisor que utilice. No se requieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix XenServer

Si está habilitada la funcionalidad de sincronización horaria de XenServer, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como XenServer intentarán administrar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

En algunas distribuciones de Linux, si se ejecuta un kernel Linux paravirtualizado con XenServer Tools instalado, puede comprobar si la función de sincronización horaria de XenServer está presente y habilitarla en la máquina virtual de Linux:

```
su -



cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Este comando devuelve 0 o 1:

- 0. La funcionalidad de sincronización horaria está habilitada, por lo que se debe inhabilitar.
- 1. La funcionalidad de sincronización horaria está inhabilitada, por lo que no es necesaria ninguna otra acción.

Si el archivo **/proc/sys/xen/independent_wallclock** no está presente, no es necesario que siga estos pasos.

Si se habilita, inhabilite la función de sincronización horaria con un **1** en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```


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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

```
reboot
<!--NeedCopy-->
```

Después de reiniciar, compruebe que la configuración es correcta:

```
su -
cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux que tienen instalados los servicios de integración de Hyper-V para Linux pueden aplicar la funcionalidad de sincronización horaria de Hyper-V para usar la hora del sistema operativo del host. Para que el reloj del sistema no se desincronice, esta funcionalidad se debe habilitar junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para ver la configuración de una máquina virtual Linux, seleccione **Integration Services**.
3. Compruebe que **Time synchronization** está seleccionado.

> **Nota:**
>
> Este método difiere de XenServer y VMware, donde se inhabilita la sincronización horaria del host para evitar conflictos con NTP. La sincronización horaria de Hyper-V puede coexistir y complementarse con la sincronización horaria de NTP.

Corregir la sincronización horaria en ESX y ESXi

Si está habilitada la funcionalidad de sincronización horaria de VMware, se dan problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como el hipervisor intentan sincronizar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host.

Si ejecuta un kernel Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Modifique 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 **Advanced**, desmarque la casilla **Synchronize guest time with host**.

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

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

- Samba Winbind
- Servicio de autenticación Quest
- Centrify DirectControl

Siga las instrucciones en función del método elegido.

Samba Winbind

Unirse al dominio de Windows Se requiere que el controlador de dominio esté accesible y se necesita disponer de una cuenta de usuario de Active Directory con permisos para agregar máquinas al dominio:

1. Abra YaST Windows Domain Membership.
2. Realice los siguientes cambios:
    - Establezca **Domain o Workgroup** en el nombre de su dominio de Active Directory o la dirección IP del controlador de dominio. El nombre del dominio debe escribirse en letras mayúsculas.
    - Marque **Also Use SMB information for Linux Authentication**.
    - Marque **Create Home Directory on Login**.
    - Marque **Single Sign-On for SSH**.
    - Compruebe que **Offline Authentication** no está marcada. Esta opción no es compatible con el VDA para Linux.
3. Haga clic en **Aceptar**. Si se solicita que instale algunos paquetes, haga clic en **Install**.
4. Si se encuentra un controlador de dominio, se le pregunta si quiere unirse al dominio. Haga clic en **Sí**.
5. Cuando se le solicite, introduzca las credenciales de un usuario de dominio con permisos para agregar equipos al dominio y haga clic en **OK**.
6. Aparecerá un mensaje con la indicación de que la operación se ha completado correctamente.

7. Si se solicita que instale paquetes samba y krb5, haga clic en **Install**.

Es posible que YaST haya indicado que estos cambios necesitan el reinicio de algunos servicios o que la máquina debe reiniciarse. Le recomendamos que reinicie la máquina:

```
su -

reboot
<!--NeedCopy-->
```

Solo SLED/SLES 12: Revisión del nombre de la caché de credenciales de Kerberos SLED/SLES 12 ha cambiado la especificación de nombre de la caché de credenciales de Kerberos predeterminada de **FILE:/tmp/krb5cc_%{uid}** a **DIR:/run/user/%{uid}/krb5cc**. Este nuevo método de caché DIR no es compatible con Linux VDA y se debe cambiar manualmente. Como usuario root, modifique **/etc/krb5.conf** y agregue la siguiente opción de configuración en la sección **[libdefaults]** si no está definida:

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

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA, 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
<!--NeedCopy-->
```

Ejecute el siguiente comando para comprobar la información adicional de dominio y objeto de equipo:

```
sudo net ads info
<!--NeedCopy-->
```

Verificar la configuración de Kerberos Para verificar que Kerberos está configurado correctamente para su uso con Linux VDA, compruebe que el archivo del sistema keytab se haya creado y contenga claves válidas:

```
sudo klist -ke
<!--NeedCopy-->
```

Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando `kinit` de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:


```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (\) al signo de dólar ($) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

Compruebe que el tíquet de TGT de la cuenta de la máquina se ha almacenado en caché:

```
sudo klist
<!--NeedCopy-->
```

Examine los datos de la cuenta de la máquina:

```
sudo net ads status
<!--NeedCopy-->
```

Verificar la autenticación de usuario Use la herramienta `wbinfo` para comprobar que los usuarios de dominio pueden autenticarse en el dominio:

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

El dominio especificado es el nombre de dominio de AD, no el nombre del territorio Kerberos. Para shell de Bash, debe anteponerse una barra diagonal inversa (\) a otra barra diagonal inversa. Este comando devuelve un mensaje que indica si la operación se ha realizado correctamente o no.

Para verificar que el módulo Winbind PAM está configurado correctamente, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Compruebe que los tíquets que se encuentran en la memoria caché de credenciales de Kerberos del usuario son válidos y no han caducado:


```
klist
<!--NeedCopy-->
```

Salga de la sesión

```
exit
<!--NeedCopy-->
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Servicio de autenticación Quest

Configurar Quest en el controlador de dominio Se asume que se ha instalado y configurado el software de Quest en los controladores de dominio de Active Directory, y que se han recibido los privilegios administrativos necesarios para crear objetos de equipo en Active Directory.

Permitir que los usuarios de dominio inicien sesión en máquinas con Linux VDA Para permitir que los usuarios de dominio puedan establecer sesiones HDX en una máquina con Linux VDA:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory correspondientes a esa cuenta de usuario.
2. Seleccione la ficha **Unix Account**.
3. Active **Unix-enabled**.
4. Defina **Primary GID Number** con el ID de grupo de un grupo de usuarios real del dominio.

> **Nota:**
>
> Estas instrucciones son equivalentes a definir usuarios de dominio para que inicien sesión desde la consola, RDP, SSH u otro protocolo de comunicación remota.

Configurar Quest en Linux VDA

Configurar el demonio de VAS La renovación automática de tíquets de Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar inhabilitada:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```


Este comando establece el intervalo de renovación a nueve horas (32 400 segundos), es decir, una hora menos que la validez predeterminada de 10 horas del tíquet. Establezca esta opción en un valor inferior en sistemas con una validez más corta de tíquets.

Configurar PAM y NSS Para habilitar el inicio de sesión del usuario de dominio mediante HDX y otros servicios como su, ssh y RDP, ejecute los siguientes comandos para configurar PAM y NSS de forma manual:

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

El parámetro **user** es un usuario de dominio con permisos para unir equipos al dominio de Active Directory. La variable **domain-name** es el nombre DNS del dominio; por ejemplo, ejemplo.com.

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA, Windows y Linux, tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Quest en el dominio:

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. En cambio, 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 pueda autenticar usuarios de dominio a través de PAM, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

```



```
id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Compruebe que los vales que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Salga de la sesión.

```
exit
<!--NeedCopy-->
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Centrify DirectControl

Unirse al dominio de Windows Con el agente 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
<!--NeedCopy-->
```

El parámetro **user** es un 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, Windows y Linux, tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Centrify en el dominio:

```
su -

adinfo
<!--NeedCopy-->
```


Compruebe que el valor **Joined to domain** sea válido y el modo **CentrifyDC mode** devuelva el valor **connected**. Si el modo se queda bloqueado en el estado inicial, el cliente Centrify tiene problemas de conexión o autenticación en el servidor.

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo  – diag
<!--NeedCopy-->
```

Pruebe la conectividad a los distintos servicios de Active Directory y Kerberos:

```
adinfo --test
<!--NeedCopy-->
```

Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Paso 4: Instale Linux VDA

Paso 4a: Desinstale la versión anterior

Si ya ha instalado una versión anterior a las dos versiones anteriores y una versión LTSR, desinstálela antes de instalar la nueva versión.

1. Detenga los servicios de Linux VDA:

   ```
   sudo /sbin/service ctxvda stop

   sudo /sbin/service ctxhdx stop
   <!--NeedCopy-->
   ```

2. Desinstale el paquete:

   ```
   sudo rpm -e XenDesktopVDA
   <!--NeedCopy-->
   ```

> **Importante:**
>
> Se admite la actualización de las dos versiones anteriores.
>
> **Nota:**
>
> Los componentes de instalación se encuentran en **/opt/Citrix/VDA/**.
>
> Para ejecutar un comando, se necesita la ruta completa. Como alternativa, puede agregar **/opt/Citrix/VDA/sbin** y **/opt/Citrix/VDA/bin** a la ruta del sistema.

Paso 4b: Descargue el paquete de Linux VDA

Vaya a la página web de Citrix y descargue el paquete de Linux VDA adecuado según su distribución de Linux.

Paso 4c: Instale Linux VDA

Instalar el software de Linux VDA mediante Zypper:

Para SUSE 12:

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

Para SUSE 11:

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

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

Para SUSE 12:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

Para SUSE 11:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

Paso 4d: Actualice la versión de Linux VDA (optativo)

Puede actualizar el software de Linux VDA desde las versiones 7.14 y 7.13 con el administrador de paquetes RPM:

Para SUSE 12:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

Para SUSE 11:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

Lista de dependencias RPM para SUSE 12:


```
postgresql-server >= 9.3

postgresql-jdbc >= 9.2

java-1.7.0-openjdk >= 1.7.0

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

python-requests >= 2.8.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1
<!--NeedCopy-->
```

Lista de dependencias RPM para SUSE 11:


```
postgresql-server >= 9.1.

postgresql-jdbc >= 9.1

java-1_7_0-openjdk >= 1.7.0.6

ImageMagick >= 6.4.3.6

ConsoleKit >= 0.2.10

dbus-1 >= 1.2.10

dbus-1-x11 >= 1.2.10

xorg-x11-libXpm >= 7.4

xorg-x11-libs >= 7.4

openmotif-libs >= 2.3.1

pam >= 1.1.5

libdrm >= 2.4.41

libpixman-1-0 >= 0.24.4

Mesa >= 9.0

openssl >= 0.9.8j

xorg-x11 >= 7.4

xorg-x11-fonts-core >= 7.4

xorg-x11-libXau >= 7.4

xorg-x11-libXdmcp >= 7.4

bash >= 3.2

findutils >= 4.4

gawk >= 3.1

sed >= 4.1

cups >= 1.3.7

foomatic-filters >= 3.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1
```



```
54
55 cyrus-sasl-gssapi >= 2.1
56
57 libxml2 >= 2.7
58
59 python-requests >= 2.0.1
60
61 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
62
63 rpmlib(CompressedFileNames) <= 3.0.4-1
64
65 rpmlib(PayloadIsLzma) <= 4.4.6-1
66 <!--NeedCopy-->
```

> **Importante:**
>
> Reinicie la máquina Linux VDA después de actualizar.

Paso 5: Configure Linux VDA

Después de instalar el paquete, debe configurar Linux VDA. Para ello, ejecute el script ctxsetup.sh. Antes de realizar cambios, este script examina el entorno existente y verifica si están instaladas todas las dependencias. Si fuera necesario, puede volver a ejecutar este script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manual o automáticamente con respuestas preconfiguradas. Consulte la ayuda del script antes de continuar:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
2 <!--NeedCopy-->
```

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--NeedCopy-->
```

Configuración automatizada

En caso de una instalación automática, proporcione las opciones necesarias para el script de instalación con variables de entorno. Si están presentes todas las variables necesarias, el script no pide ninguna información.

Las variables de entorno admitidas son:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N**: Linux VDA permite especificar 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**: Linux VDA necesita una lista de nombres de dominio completo de Delivery Controllers, separados por espacios, para registrarse en un Delivery Controller. Se debe especificar al menos un FQDN o alias de CNAME.
- **CTX_XDL_VDA_PORT = port-number**: Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP. Este 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 está 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 automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema para Linux Virtual Desktop. Se establece en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4**: Linux VDA requiere parámetros de configuración Kerberos para autenticarse en 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 admitido de integración de Active Directory que se va a utilizar:
  - 1 –Samba Winbind
  - 2 –Servicio de autenticación Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N**: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. Si se selecciona HDX 3D Pro, Virtual Delivery Agent se configura para el modo de escritorios VDI (sesión única); es decir, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE = Y | N**: Indica si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos alojados. Para entornos HDX 3D Pro, establezca esta variable en Y. De forma predeterminada, esta variable está establecida en N.
- **CTX_XDL_SITE_NAME = dns-name**: Linux VDA detecta los servidores LDAP mediante DNS. Para limitar los resultados de 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**: Linux VDA consulta a DNS para detectar servidores LDAP. Sin embargo, si el DNS no puede proporcionar registros del servicio LDAP, se puede suministrar una lista de nombres FQDN de LDAP, separados por espacios, con el puerto de LDAP. Por ejemplo, ad1.miempresa.com:389. Esta variable está establecida en **<none>** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE = search-base-set**: Linux VDA consulta a LDAP a partir de una

base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=miempresa,DC=com). Para mejorar el rendimiento de la búsqueda, puede especificar otra base de búsqueda (por ejemplo, OU=VDI,DC=miempresa,DC=com). Esta variable está establecida en **<none>** de forma predeterminada.

- **CTX_XDL_START_SERVICE = Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.

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-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Cuando ejecute el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que se crea. Citrix recomienda crear un archivo de script shell a partir de los comandos anteriores con **#!/bin/bash** en la primera línea.

También puede especificar todos los parámetros con un único 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 \
```



```
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST=list-ldap-servers \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_START_SERVICE=Y|N \
24
25 /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

Quitar cambios de configuración

En algunos casos, puede que sea necesario quitar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete de Linux VDA.

Consulte la ayuda de este script antes de continuar:

```
1 sudo /usr/local/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

Para quitar los cambios de configuración:

```
1 sudo /usr/local/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

> **Importante:**
>
> Este script elimina todos los datos de configuración de la base de datos y provoca que Linux VDA deje de funcionar.

Registros de configuración

Los scripts **ctxcleanup.sh** y **ctxsetup.sh** muestran errores en la consola, con información adicional que se enviará a un archivo de registro de configuración:

`/tmp/xdl.configure.log`

Reinicie los servicios de Linux VDA para que los cambios surtan efecto.

Paso 6: Ejecute Linux VDA

Una vez configurado Linux VDA mediante el script **ctxsetup.sh**, utilice los siguientes comandos para controlarlo.

Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Comprobar el estado de Linux VDA:

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

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

Paso 7: Cree el catálogo de máquinas en XenApp o XenDesktop

El proceso de creación de catálogos de máquinas y de incorporación de máquinas Linux es similar al proceso habitual de VDA para Windows. Para ver una descripción detallada sobre cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Existen restricciones que diferencian el proceso de creación de catálogos de máquinas con VDA para Windows del mismo proceso con VDA para Linux:

- Para el sistema operativo, seleccione:
  - La opción de SO de servidor para un modelo de entrega de escritorios compartidos alojados.
  - La opción de SO de escritorio para un modelo de entrega de escritorios VDI dedicados.
- Compruebe que las máquinas están establecidas como máquinas cuyas opciones de administración de energía no están administradas.
- Como los agentes Linux VDA no admiten MCS, elija el método de implementación PVS u **Otro servicio o tecnología** (imágenes existentes).
- No mezcle máquinas con agentes VDA para Windows y Linux en el mismo catálogo.

> **Nota:**
>
> Las primeras versiones de Citrix Studio no admitían el concepto de "SO Linux". Sin embargo, seleccionar la opción SO de servidor Windows o SO de servidor implica un modelo equivalente de entrega de escritorios compartidos alojados. Seleccionar la opción SO de escritorio Windows o SO de escritorio implica un modelo de entrega de un usuario por máquina.
>
> **Consejo:**
>
> Si quita una máquina y luego la vuelve a unir al dominio de Active Directory, esa máquina se debe quitar y volver a agregar al catálogo de máquinas.

Paso 8: Cree el grupo de entrega en XenApp o XenDesktop

El proceso de creación de un grupo de entrega y de incorporación de catálogos de máquinas con agentes VDA para Linux es muy similar al proceso de máquinas con agentes VDA para Windows. Para ver una descripción detallada sobre cómo completar estas tareas, consulte Crear grupos de entrega.

Se aplican las siguientes restricciones para crear grupos de entrega que contengan catálogos de máquinas con Linux VDA:

- Para el tipo de entrega, seleccione Escritorios o Aplicaciones.
- Los grupos y usuarios de AD que seleccione deben estar correctamente configurados para poder iniciar sesión en las máquinas con VDA para Linux.
- No permita que usuarios no autenticados (anónimos) inicien sesión.
- No mezcle el grupo de entrega con catálogos de máquinas que contienen máquinas Windows.

> **Importante:**
>
> Se admite la publicación de aplicaciones con Linux VDA 1.4 y versiones posteriores. Linux VDA no admite la entrega de escritorios ni aplicaciones a la misma máquina.

Instalar Linux Virtual Delivery Agent para Ubuntu

June 17, 2022

Puede elegir entre seguir los pasos de este artículo para la instalación manual o utilizar Easy Install para la instalación y configuración automáticas. Easy Install ahorra tiempo y trabajo y es menos propenso a errores que la instalación manual.

> **Nota** Use Easy Install solo para instalaciones nuevas. No utilice Easy Install para actualizar una instalación existente.

Paso 1: Prepare Ubuntu para la instalación del VDA

Paso 1a: Verifique la configuración de red

Compruebe que la red esté conectada y correctamente configurada antes de continuar.

Paso 1b: Establezca el nombre de host

Para que el nombre de host de la máquina se notifique correctamente, cambie el archivo **/etc/hostname** para que solo contenga el nombre de host de la máquina.

```
hostname
```

Paso 1c: Asigne una dirección de bucle invertido al nombre de host

Para que se notifiquen correctamente el nombre de dominio DNS y el nombre de dominio completo de la máquina (FQDN), cambie la siguiente línea del archivo **/etc/hosts** para que contenga el nombre de dominio completo y el nombre de host en las dos primeras entradas:

```
127.0.0.1 hostname-fqdn hostname localhost
```

Por ejemplo:

```
127.0.0.1 vda01.example.com vda01 localhost
```

Quite las demás referencias a **hostname-fqdn** o **hostname** de otras entradas del archivo.

> **Nota:**
>
> Actualmente, Linux VDA no admite el truncamiento del nombre NetBIOS. Por lo tanto, el nombre de host no debe superar los 15 caracteres.
>
> **Sugerencia:**

> Use solamente caracteres de "a"a "z", de "A"a "Z", de 0 a 9 y guiones (-). No utilice guiones bajos (_), espacios ni otros símbolos. No inicie un nombre de host con un número ni lo termine con un guión. Esta regla también se aplica a nombres de host de Delivery Controller.

Paso 1d: Compruebe el nombre de host

Compruebe que el nombre de host está definido correctamente:

```
hostname
<!--NeedCopy-->
```

Este comando devuelve solo el nombre de host de la máquina, no su nombre de dominio completo.

Compruebe que el nombre de dominio completo (FQDN) está definido correctamente:

```
hostname -f
<!--NeedCopy-->
```

Este comando devuelve el nombre de dominio completo de la máquina.

Paso 1e: Inhabilite el DNS de multidifusión

Con la configuración predeterminada, el DNS de multidifusión (**mDNS**) está habilitado, lo que puede dar lugar a resoluciones de nombres incoherentes.

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

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

A:

```
hosts: files dns
```

Paso 1f: Compruebe la resolución de nombres y la disponibilidad del servicio

Compruebe que se puede resolver el nombre de dominio completo (FQDN) y haga ping al controlador de dominio y al Delivery Controller:

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```


Si no puede resolver el FQDN o hacer ping en alguna de estas máquinas, revise los pasos antes de continuar.

Paso 1g: Configure la sincronización del reloj (chrony)

Mantener sincronizados los relojes de los VDA, los Delivery Controllers y los controladores de dominio es fundamental. Ahora bien, alojar Linux VDA como una máquina virtual puede causar problemas de reloj sesgado. Por este motivo, se recomienda sincronizar la hora con un servicio remoto de sincronización horaria.

Instalar Chrony:

```
apt-get install chrony
<!--NeedCopy-->
```

Como usuario root, modifique **/etc/chrony/chrony.conf** y agregue una entrada de servidor para cada servidor horario remoto:

```
server peer1-fqdn-or-ip-address iburst
server peer2-fqdn-or-ip-address iburst
```

En una implementación típica, sincronice la hora con los controladores del dominio local, no directamente con grupos públicos de servidores NTP. Agregue una entrada de servidor para cada controlador de dominio de Active Directory que tenga en el dominio.

Quite las demás entradas **server** o **pool** de la lista, incluidas las entradas loopback IP address, localhost y public server ***.pool.ntp.org**.

Guarde los cambios y reinicie el demonio de Chrony:

```
sudo systemctl restart chrony
<!--NeedCopy-->
```

Paso 1h: Instale OpenJDK

Linux VDA depende de OpenJDK. Por regla general, el entorno en tiempo de ejecución se instala durante la instalación del sistema operativo. Compruebe si se ha instalado:

```
sudo apt-get install -y default-jdk
<!--NeedCopy-->
```

Paso 1i: Instale PostgreSQL

Linux VDA requiere PostgreSQL 9.x en Ubuntu 16.04:


```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--NeedCopy-->
```

Paso 1j: Instale Motif

```
sudo apt-get install -y libxm4
<!--NeedCopy-->
```

Paso 1k: Instale 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 cups
<!--NeedCopy-->
```

Paso 2: Prepare el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Realice los siguientes cambios en función de la plataforma del hipervisor que utilice. No se requieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix XenServer

Si está habilitada la funcionalidad de sincronización horaria de XenServer, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como XenServer intentarán administrar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

En algunas distribuciones de Linux, si se ejecuta un kernel Linux paravirtualizado con XenServer Tools instalado, puede comprobar si la función de sincronización horaria de XenServer está presente y habilitarla en la máquina virtual de Linux:


```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Este comando devuelve 0 o 1:

- 0. La funcionalidad de sincronización horaria está habilitada, por lo que se debe inhabilitar.
- 1. La funcionalidad de sincronización horaria está inhabilitada, por lo que no es necesaria ninguna otra acción.

Si el archivo /proc/sys/xen/independent_wallclock no está presente, no es necesario que siga estos pasos.

Si se habilita, inhabilite la función de sincronización de tiempo con un 1 en el archivo:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux que tienen instalados los servicios de integración de Hyper-V para Linux pueden utilizar la funcionalidad de sincronización horaria de Hyper-V para usar la hora del sistema operativo del host. Para que el reloj del sistema no se desincronice, se debe habilitar esta funcionalidad junto con los servicios NTP.

Desde el sistema operativo de administración:

1. Abra la consola del Administrador de Hyper-V.
2. Para ver la configuración de una máquina virtual Linux, seleccione **Integration Services**.
3. Compruebe que **Time synchronization** está seleccionado.

> **Nota** Este método difiere de XenServer y VMware, donde se inhabilita la sincronización horaria del host para evitar conflictos con NTP. La sincronización horaria de Hyper-V puede coexistir y complementarse con la sincronización horaria de NTP.

Corregir la sincronización horaria en ESX y ESXi

Si está habilitada la funcionalidad de sincronización horaria de VMware, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como el hipervisor intentarán sincronizar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host.

Si ejecuta un kernel Linux paravirtualizado con VMware Tools instalado:

1. Abra vSphere Client.
2. Modifique 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 **Advanced**, desmarque la casilla **Synchronize guest time with host**.

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

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

- Samba Winbind
- Servicio de autenticación Quest
- Centrify DirectControl
- SSSD

Siga las instrucciones en función del método elegido.

Samba Winbind

Instalar o actualizar los paquetes requeridos

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
<!--NeedCopy-->
```

Habilitar el demonio de Winbind para que se inicie a la misma vez que la máquina El demonio de Winbind debe configurarse para iniciarse en el arranque:


```
sudo systemctl enable winbind
<!--NeedCopy-->
```

Configurar Kerberos Abra /etc/krb5.conf como usuario root y configure los parámetros siguientes:

```
[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
<!--NeedCopy-->
```

La propiedad **domain-dns-name** en este contexto es el nombre de dominio DNS (por ejemplo, **ejemplo.com**). **REALM** es el nombre del territorio Kerberos en mayúsculas, como **EJEMPLO.COM**.

Configurar la autenticación de Winbind Debe configurar Windbind manualmente, ya que Ubuntu no tiene una herramienta como authconfig en RHEL y yast2 en SUSE.

Abra /etc/samba/smb.conf y configure los parámetros siguientes:

```
[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
<!--NeedCopy-->
```

WORKGROUP es el primer campo de **REALM**, y REALM es el nombre del territorio Kerberos en mayúsculas.

Configurar nsswitch Abra `/etc/nsswitch.conf` y agregue `winbind` a las siguientes líneas:

```
passwd: compat winbind
group: compat winbind
```

Unirse al dominio de Windows Se requiere que el controlador de dominio esté accesible y se necesita disponer de una cuenta de usuario de Active Directory con permisos para agregar equipos al dominio:

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

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

Reiniciar Winbind

```
sudo systemctl restart winbind
<!--NeedCopy-->
```

Configurar PAM para Winbind Ejecute el siguiente comando, compruebe que las opciones **Winbind NT/Active Directory authentication** y **Create home directory on login** están seleccionadas:

```
sudo pam-auth-update
<!--NeedCopy-->
```

> **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, Windows o Linux, tengan un objeto de equipo en Active Directory.

Ejecute el comando `net ads` de Samba para comprobar que la máquina está unida a un dominio:

```
sudo net ads testjoin
<!--NeedCopy-->
```

Ejecute el siguiente comando para comprobar la información adicional de dominio y objeto de equipo:

```
sudo net ads info
<!--NeedCopy-->
```

Verificar la configuración de Kerberos Para verificar que Kerberos está configurado correctamente para su uso con Linux VDA, compruebe que el archivo del sistema **keytab** se ha creado y contiene claves válidas:

```
sudo klist -ke
<!--NeedCopy-->
```

Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando `kinit` de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (\) al signo de dólar ($) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

Compruebe que el tíquet de TGT de la cuenta de la máquina se ha almacenado en caché:

```
sudo klist
<!--NeedCopy-->
```

Examine los datos de la cuenta de la máquina:

```
sudo net ads status
<!--NeedCopy-->
```

Verificar la autenticación de usuario Use la herramienta **wbinfo** para comprobar que los usuarios de dominio pueden autenticarse en el dominio:


```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

El dominio especificado es el nombre de dominio de AD, no el nombre del territorio Kerberos. Para shell de Bash, debe anteponerse una barra diagonal inversa (\) a otra barra diagonal inversa. Este comando devuelve un mensaje que indica si la operación se ha realizado correctamente o no.

Para verificar que el módulo Winbind PAM está configurado correctamente, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Compruebe que los tíquets que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado:

```
klist
<!--NeedCopy-->
```

Salga de la sesión.

```
exit
<!--NeedCopy-->
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

> **Sugerencia:**
>
> Si la autenticación de usuario se realizó correctamente pero no aparece su escritorio al iniciar sesión con una cuenta de dominio, reinicie la máquina e inténtelo de nuevo.

Servicio de autenticación Quest

Configurar Quest en el controlador de dominio Se asume que se ha instalado y configurado el software de Quest en los controladores de dominio de Active Directory, y que se han recibido los privilegios administrativos necesarios para crear objetos de equipo en Active Directory.

Permitir que los usuarios de dominio inicien sesión en máquinas con Linux VDA Para permitir que los usuarios de dominio puedan establecer sesiones HDX en una máquina con Linux VDA:

1. En la consola de administración Usuarios y equipos de Active Directory, abra las propiedades de usuario de Active Directory correspondientes a esa cuenta de usuario.
2. Seleccione la ficha **Unix Account**.
3. Active **Unix-enabled**.
4. Defina **Primary GID Number** con el ID de grupo de un grupo de usuarios real del dominio.

> **Nota:**
>
> Estas instrucciones son equivalentes a definir usuarios de dominio para que inicien sesión desde la consola, RDP, SSH u otro protocolo de comunicación remota.

Configurar Quest en Linux VDA

Solución a la aplicación de la directiva de SELinux En el entorno predeterminado de RHEL, SELinux se aplica en su totalidad. Esto interfiere con los mecanismos de IPC de sockets para dominios Unix que utiliza Quest y evita que los usuarios inicien sesión.

Lo más conveniente para solucionar este problema es inhabilitar SELinux. Como usuario root, modifique **/etc/selinux/config** y cambie el parámetro **SELinux**:

```
SELINUX=disabled
```

Este cambio requiere un reinicio de la máquina:

```
reboot
<!--NeedCopy-->
```

> **Importante:**
>
> Utilice esta opción con cuidado. Habilitar la directiva de SELinux tras haberla inhabilitado puede causar un bloqueo absoluto, incluso para el usuario root y otros usuarios locales.

Configurar el demonio de VAS La renovación automática de tíquets de Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar inhabilitada:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```


Este comando establece el intervalo de renovación a nueve horas (32 400 segundos), es decir, una hora menos que la validez predeterminada de 10 horas del tíquet. Establezca esta opción en un valor inferior en sistemas con una validez más corta de tíquets.

Configurar PAM y NSS Para habilitar el inicio de sesión del usuario de dominio mediante HDX y otros servicios como su, ssh y RDP, ejecute los siguientes comandos para configurar PAM y NSS de forma manual:

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

El usuario es un usuario de dominio con permisos para unir equipos al dominio de Active Directory. La variable domain-name es el nombre DNS del dominio; por ejemplo, ejemplo.com.

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA, Windows o Linux, tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Quest en el dominio:

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. En cambio, 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 pueda autenticar usuarios de dominio a través de PAM, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

```



```
id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el UID devuelto por el comando **id -u**:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Compruebe que los vales que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado:

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Salga de la sesión.

```
exit
<!--NeedCopy-->
```

Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Centrify DirectControl

Unirse al dominio de Windows Con el agente 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
<!--NeedCopy-->
```

El parámetro **user** es un 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, Windows o Linux, tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Centrify en el dominio:

```
su -

adinfo
<!--NeedCopy-->
```

Compruebe que el valor **Joined to domain** sea válido y que el **modo CentrifyDC** devuelva el valor **connected**. Si el modo se queda bloqueado en el estado inicial, el cliente Centrify tiene problemas

de conexión o autenticación en el servidor.

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

Pruebe la conectividad a los distintos servicios de Active Directory y Kerberos:

```
adinfo --test
<!--NeedCopy-->
```

Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

SSSD

Configurar Kerberos Ejecute el siguiente comando para instalar Kerberos:

```
sudo apt-get install krb5-user
<!--NeedCopy-->
```

Para configurar Kerberos, abra `/etc/krb5.conf` como root y configure los siguientes parámetros:

```
[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
<!--NeedCopy-->
```


La propiedad `domain-dns-name` en este contexto es el nombre de dominio DNS (por ejemplo, `example.com`). `REALM` es el nombre del territorio Kerberos en mayúsculas, como `EXAMPLE.COM`.

Unirse al dominio SSSD debe estar configurado para usar Active Directory como su proveedor de identidades y Kerberos para la autenticación. SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo de sistema keytab. Puede usar `adcli`, `realmd` o `Samba` en su lugar.

> **Nota:**
>
> En esta sección, solo se proporciona información para `adcli` y `Samba`.

Use adcli para unirse al dominio:

Instale adcli:

Instale el paquete requerido:

```
sudo apt-get install adcli
<!--NeedCopy-->
```

Únase al dominio con adcli:

Quite el antiguo archivos keytab de sistema y únase al dominio con:

```
su -

rm -rf /etc/krb5.keytab

adcli join domain-dns-name -U user -H hostname-fqdn
<!--NeedCopy-->
```

El parámetro **user** es un usuario del dominio con permisos para agregar máquinas al dominio. El parámetro **hostname-fqdn** es el nombre de host en formato FQDN (nombre de dominio completo) de la máquina.

La opción **-H** es necesaria para que adcli genere SPN en este formato: host/hostname-fqdn@REALM, que es el requerido por Linux VDA.

Compruebe el archivo keytab del sistema:

Las capacidades de la herramienta **adcli** son limitadas y no proporciona ninguna forma para probar si una máquina se ha unido al dominio. La mejor opción para asegurarse de que el archivo keytab del sistema se ha creado es la siguiente:

```
sudo klist -ket
<!--NeedCopy-->
```


Compruebe que la fecha y hora para cada clave coinciden con el momento en que la máquina se unió al dominio.

Use samba para unirse al dominio:

Instale el paquete:

```
sudo apt-get install samba
<!--NeedCopy-->
```

Configure samba:

Abra `/etc/samba/smb.conf` y configure los parámetros siguientes:

```
[global]

   workgroup = WORKGROUP

   security = ADS

   realm = REALM

   client signing = yes

   client use spnego = yes

   kerberos method = secrets and keytab
<!--NeedCopy-->
```

WORKGROUP es el primer campo de **REALM**, y REALM es el nombre del territorio Kerberos en mayúsculas.

Únase al dominio con samba:

Para ello, se requiere que el controlador de dominio esté accesible y se necesita disponer de una cuenta de Windows con permisos para agregar equipos al dominio.

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

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

Configurar SSSD Instalar o actualizar los paquetes requeridos:

Instale los paquetes de configuración y SSSD requeridos si aún no están instalados:

```
sudo apt-get install sssd
<!--NeedCopy-->
```

Si los paquetes ya están instalados, se recomienda actualizarlos:


```
sudo apt-get update sssd
<!--NeedCopy-->
```

> **Nota:**
>
> De forma predeterminada, el proceso de instalación en Ubuntu configura automáticamente **nss-witch.conf** y el módulo de PAM de inicio de sesión.

Configurar SSSD Es necesario hacer los cambios en la configuración de SSSD antes de iniciar el demonio SSSD. En algunas versiones de SSSD, el archivo de configuración **/etc/sssd/sssd.conf** no se instala de forma predeterminada y se debe crear manualmente. Como usuario root, cree o abra el archivo **/etc/sssd/sssd.conf** y configure los siguientes parámetros:

```
[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
```



```
36
37 default_shell = /bin/bash
38
39 ad_gpo_map_remote_interactive = +ctxhdx
40 <!--NeedCopy-->
```

> **Nota:**
>
> ldap_id_mapping tiene el valor **true**, de forma que el propio SSSD se ocupa de asignar los SID de Windows a UID de Unix. De lo contrario, Active Directory debe ser capaz de proporcionar extensiones POSIX. El `ctxhdx` de servicio PAM se agrega a ad_gpo_map_remote_interactive.

La propiedad **domain-dns-name** en este contexto es el nombre de dominio DNS (por ejemplo, ejemplo.com). **REALM** es el nombre del territorio Kerberos en mayúsculas, como EJEMPLO.COM. No es necesario configurar el nombre de dominio NetBIOS.

> **Sugerencia:**
>
> Para obtener más información sobre estas opciones de configuración, consulte las páginas man de sssd.conf y sssd-ad.

El demonio SSSD requiere que el archivo de configuración tenga permisos de lectura de propietario solamente:

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
2 <!--NeedCopy-->
```

Iniciar el demonio de SSSD Ejecute los siguientes comandos para iniciar el demonio SSSD ahora y para permitir que el demonio se inicie al iniciar la máquina:

```
1 sudo systemctl start sssd
2
3 sudo systemctl enable sssd
4 <!--NeedCopy-->
```

Configuración de PAM Ejecute el siguiente comando y compruebe que las opciones **SSS authentication** y **Create home directory on login** están seleccionadas:

```
1 sudo pam-auth-update
2 <!--NeedCopy-->
```

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA, Windows y Linux, tengan un objeto de equipo en Active Directory.

Use adcli para verificar la pertenencia al dominio:

Vea la información de dominio, mediante la ejecución del siguiente comando:

```
sudo adcli info domain-dns-name
<!--NeedCopy-->
```

Use samba para verificar la pertenencia al dominio:

Ejecute el comando `net ads` de Samba para comprobar que la máquina está unida a un dominio:

```
sudo net ads testjoin
<!--NeedCopy-->
```

Ejecute el siguiente comando para comprobar la información adicional de dominio y objeto de equipo:

```
sudo net ads info
<!--NeedCopy-->
```

Verificar la configuración de Kerberos Para verificar que Kerberos está configurado correctamente para su uso con Linux VDA, compruebe que el archivo del sistema keytab se ha creado y contiene claves válidas:

```
sudo klist -ke
<!--NeedCopy-->
```

Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando `kinit` de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (\) al signo de dólar ($) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

Compruebe que el tíquet de TGT de la cuenta de la máquina se ha almacenado en la caché mediante lo siguiente:

```
sudo klist
<!--NeedCopy-->
```

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 mediante PAM.

Para verificar que el módulo SSSD PAM está configurado correctamente, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
ssh localhost -l domain\username

id -u

klist

exit
<!--NeedCopy-->
```

Compruebe que los tíquets de Kerberos devueltos por el comando **klist** son correctos para ese usuario y no han caducado.

Como usuario root, compruebe que se ha creado el archivo de caché de tíquets correspondiente para el uid devuelto por el comando **id -u** previo:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Se puede realizar una prueba similar iniciando sesión en KDE o Gnome Display Manager. Continúe con el Paso 4: Instale Linux VDA después de la verificación de unión al dominio.

Paso 4: Instale Linux VDA

Paso 4a: Descargue el paquete de Linux VDA

Vaya a la página web de Citrix y descargue el paquete de Linux VDA adecuado según su distribución de Linux.

Paso 4b: Instale Linux VDA

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

```
sudo dpkg -i xendesktopvda_7.15.0.404-1.ubuntu16.04_amd64.deb
<!--NeedCopy-->
```

Lista de dependencias de Debian para Ubuntu:

```
postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

default-jdk >= 2:1.8

```



```
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~
<!--NeedCopy-->
```

Paso 4c: Configure Linux VDA

Después de instalar el paquete, debe configurar Linux VDA. Para ello, ejecute el script ctxsetup.sh. Antes de realizar cambios, este script examina el entorno existente y verifica si están instaladas todas las dependencias. Si fuera necesario, puede volver a ejecutar este script en cualquier momento para cambiar la configuración.

Puede ejecutar el script manual o automáticamente con respuestas preconfiguradas. Consulte la ayuda del script antes de continuar:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
<!--NeedCopy-->
```

Configuración con preguntas Ejecute una configuración manual con preguntas para el usuario:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```


Configuración automatizada En caso de una instalación automática, las opciones necesarias para el script de instalación pueden especificarse con variables de entorno. Si están presentes todas las variables necesarias, el script no solicita al usuario ninguna otra información, lo que permite que el proceso de instalación se realice mediante los scripts.

Las variables de entorno admitidas son:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N**: Linux VDA permite especificar 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**: Linux VDA necesita una lista de nombres de dominio completo de Delivery Controllers, separados por espacios, para registrarse en un Delivery Controller. Se debe especificar al menos un FQDN o alias de CNAME.
- **CTX_XDL_VDA_PORT** = **port-number**: Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP. Este 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 automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema para Linux Virtual Desktop. Se establece en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION** = **1 | 2 | 3 | 4**: Linux VDA requiere parámetros de configuración Kerberos para autenticarse en 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 admitido de integración de Active Directory que se va a utilizar:
  - 1 –Samba Winbind
  - 2 –Servicio de autenticación Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO** = **Y | N**: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. Si se selecciona HDX 3D Pro, Virtual Delivery Agent se configura para el modo de escritorios VDI (sesión única); es decir, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE** = **Y | N**: Indica si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos alojados. Para entornos HDX 3D Pro, establezca esta variable en Y. De forma predeterminada, esta variable está establecida en N.
- **CTX_XDL_SITE_NAME** = **dns-name**: Linux VDA detecta los servidores LDAP mediante DNS. Para limitar los resultados de 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**: Linux VDA consulta a DNS para detectar servidores LDAP. Sin embargo, si el DNS no puede proporcionar registros del servicio LDAP, se puede suministrar una lista de nombres FQDN de LDAP, separados por espacios, con el puerto de LDAP. Por ejemplo, ad1.miempresa.com:389. Esta variable está establecida en **<none>** de forma predeterminada.
- **CTX_XDL_SEARCH_BASE** = **search-base-set**: Linux VDA consulta a LDAP a partir de una base de búsqueda establecida en la raíz del dominio de Active Directory (por ejemplo, DC=miempresa,DC=com). Sin embargo, para mejorar el rendimiento de la búsqueda, puede especificar otra base de búsqueda (por ejemplo, OU=VDI,DC=mycompany,DC=com). Esta variable está establecida en **<none>** de forma predeterminada.
- **CTX_XDL_START_SERVICE** = **Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.

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-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Cuando ejecute el comando sudo, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que se crea. Citrix recomienda crear un archivo de script shell a partir de los comandos anteriores con **#!/bin/bash** en la primera línea.

También puede especificar todos los parámetros con un único comando:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
```



```
2
3  CTX_XDL_DDC_LIST=list-ddc-fqdns \
4
5  CTX_XDL_VDA_PORT=port-number \
6
7  CTX_XDL_REGISTER_SERVICE=Y|N \
8
9  CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST=list-ldap-servers \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_START_SERVICE=Y|N \
24
25 /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

Quitar cambios de configuración En algunos casos, puede que sea necesario quitar los cambios de configuración realizados por el script **ctxsetup.sh** sin desinstalar el paquete de Linux VDA.

Consulte la ayuda de este script antes de continuar:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

Para quitar los cambios de configuración:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

> **Importante:**
>
> Este script elimina todos los datos de configuración de la base de datos y provoca que Linux VDA deje de funcionar.

Registros de configuración Los scripts **ctxcleanup.sh** y **ctxsetup.sh** muestran errores en la consola, con información adicional que se enviará a un archivo de registros 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 para ver la versión del paquete instalado:

```
dpkg -l xendesktopvda
<!--NeedCopy-->
```

Para ver información más detallada:

```
apt-cache show xendesktopvda
<!--NeedCopy-->
```

Para desinstalar el software de Linux VDA:

```
dpkg -r xendesktopvda
<!--NeedCopy-->
```

> **Nota:**
>
> La desinstalación del software de VDA para Linux elimina los datos asociados con PostgreSQL y otros datos de configuración. Sin embargo, no se elimina el paquete de PostgreSQL ni los demás paquetes dependientes que se configuraron antes de instalar Linux VDA.
>
> **Sugerencia:**
>
> La información en esta sección no cubre la eliminación de paquetes dependientes incluido el de PostgreSQL.

Paso 5: Ejecute Linux VDA

Una vez configurado Linux VDA mediante el script **ctxsetup.sh**, utilice los siguientes comandos para controlarlo.

Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```


Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Paso 6: Cree el catálogo de máquinas en XenApp o XenDesktop

El proceso de creación de catálogos de máquinas y de incorporación de máquinas Linux es similar al proceso habitual de VDA para Windows. Para ver una descripción detallada sobre cómo completar estas tareas, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Existen restricciones que diferencian el proceso de creación de catálogos de máquinas con VDA para Windows del mismo proceso con VDA para Linux:

- Para el sistema operativo, seleccione:
  - La opción de SO de servidor para un modelo de entrega de escritorios compartidos alojados.
  - La opción de SO de escritorio para un modelo de entrega de escritorios VDI dedicados.
- Compruebe que las máquinas están establecidas como máquinas cuyas opciones de administración de energía no están administradas.
- Como los agentes Linux VDA no admiten MCS, elija el método de implementación PVS u **Otro servicio o tecnología** (imágenes existentes).
- No mezcle máquinas con agentes VDA para Windows y Linux en el mismo catálogo.

> **Nota:**
>
> Las primeras versiones de Citrix Studio no admitían el concepto de "SO Linux". Sin embargo, seleccionar la opción SO de servidor Windows o SO de servidor implica un modelo equivalente de entrega de escritorios compartidos alojados. Seleccionar la opción SO de escritorio Windows o SO de escritorio implica un modelo de entrega de un usuario por máquina.

> **Sugerencia:**
>
> Si quita una máquina y luego la vuelve a unir al dominio de Active Directory, esa máquina se debe quitar y volver a agregar al catálogo de máquinas.

Paso 7: Cree el grupo de entrega en XenApp o XenDesktop

El proceso de creación de un grupo de entrega y de incorporación de catálogos de máquinas con agentes VDA para Linux es muy similar al proceso de máquinas con agentes VDA para Windows. Para ver una descripción detallada sobre cómo completar estas tareas, consulte Crear grupos de entrega.

Se aplican las siguientes restricciones para crear grupos de entrega que contengan catálogos de máquinas con Linux VDA:

- Para el tipo de entrega, seleccione **Desktops**. Linux VDA para Ubuntu no admite la entrega de aplicaciones.
- Los grupos y usuarios de AD que seleccione deben estar correctamente configurados para poder iniciar sesión en las máquinas con VDA para Linux.
- No permita que usuarios no autenticados (anónimos) inicien sesión.
- No mezcle el grupo de entrega con catálogos de máquinas que contienen máquinas Windows.

Configurar Linux VDA

November 21, 2020

En esta sección, se detallan las funciones de Linux VDA, incluida su descripción, su configuración y la resolución de problemas relacionados.

Integrar NIS en Active Directory

November 30, 2022

En este tema, se describe cómo integrar NIS con Windows Active Directory (AD) en Linux VDA mediante SSSD. Linux VDA es un componente de Citrix XenApp y XenDesktop. Por eso, encaja bien en el entorno de Active Directory (AD) de Windows.

Para usar NIS como un proveedor de UID y GID en lugar de Active Directory, se necesita que la información de cuenta (la combinación de nombre de usuario y contraseña) sea la misma tanto en AD como en NIS.

> **Nota:**
>
> El servidor de Active Directory sigue encargándose de la autenticación. No se admite NIS+. Si se utiliza NIS como el UID y el proveedor GID, ya no se usan los atributos de POSIX procedentes del servidor Windows.
>
> **Sugerencia:**
>
> Este método representa un modo ya retirado de implementar Linux VDA, que solo debe usarse en casos especiales. Para una distribución RHEL/CentOS, siga las instrucciones de Instalar Linux Virtual Delivery Agent para RHEL/CentOS. Para una distribución Ubuntu, siga las instrucciones de Instalar Linux Virtual Delivery Agent para Ubuntu.

SSSD:

SSSD es un demonio del sistema, cuya función principal es ofrecer acceso para identificar y autenticar recursos remotos en un marco común que incluya almacenamiento en caché y la opción sin conexión para el sistema. Proporciona los módulos PAM y NSS y, más adelante, puede ofrecer interfaces D-BUS con información adicional para el usuario. También incluye una base de datos mejor para almacenar cuentas de usuarios locales y datos de usuario extendidos.

Software requerido

El proveedor de AD se introdujo por primera vez con SSSD 1.9.0.

Se han probado y verificado los siguientes entornos con las instrucciones de este artículo:

- RHEL 7.3 o versiones posteriores/CentOS 7.3 o versiones posteriores
- Linux VDA versión 1.3 o posterior

Integrar NIS con AD

Para integrar NIS con AD, haga lo siguiente:

1. Agregue el Linux VDA como cliente NIS
2. Unirse al dominio y crear una tabla keytab de host mediante Samba
3. Configuración de SSSD
4. Configurar NSS/PAM
5. Verificar la configuración de Kerberos
6. Verificar la autenticación de usuarios

Agregue el Linux VDA como cliente NIS

Configure el cliente NIS:

```
yum –y install ypbind rpcbind oddjob-mkhomedir
<!--NeedCopy-->
```

Establezca el dominio NIS:

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--NeedCopy-->
```

Agregue la dirección IP para el cliente y el servidor NIS en **/etc/hosts**:

```
{ NIS server IP address }    server.nis.domain nis.domain
```

Configure NIS con authconfig:

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
   nis.domain --enablemkhomedir --update
<!--NeedCopy-->
```

nis.domain representa el nombre de dominio del servidor NIS. **server.nis.domain** es el nombre de host del servidor NIS, que puede ser también la dirección IP del servidor NIS.

Configure los servicios de NIS:

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

Compruebe que la configuración de NIS es correcta:

```
ypwhich
<!--NeedCopy-->
```

Valide que la información de la cuenta esté disponible desde el servidor NIS:

```
getent passwd nisaccount
<!--NeedCopy-->
```

> **Nota:**
>
> El valor de **nisaccount** representa la verdadera cuenta de NIS en el servidor NIS. Compruebe que el GID, el UID, el directorio principal y el shell de inicio de sesión están configurados correctamente.

Unirse al dominio y crear una tabla keytab de host mediante Samba

SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo de sistema keytab. Existen varios métodos para conseguir estas funciones:

- adcli
- realmd
- Winbind
- Samba

En esta sección, se describe solo el enfoque de Samba. Para **realmd**, consulte la documentación de RHEL o CentOS. Debe seguir estos pasos para configurar SSSD.

Unirse al dominio y crear una tabla keytab de host mediante Samba:

En el cliente Linux, con archivos correctamente configurados:

- /etc/krb5.conf
- /etc/samba/smb.conf:

Configure la máquina para la autenticación Kerberos y Samba:

```
1 sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
     REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
2 <!--NeedCopy-->
```

Donde **REALM** es el nombre del territorio Kerberos en mayúsculas y **domain** es el nombre NetBIOS del dominio.

Si se necesitan las búsquedas basadas en DNS del nombre de territorio Kerberos y del servidor KDC, 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 que haya generado la herramienta **authconfig**:

```
kerberos method = secrets and keytab
```

Para unirse a un dominio Windows, el controlador de dominio debe ser accesible y usted debe tener una cuenta de usuario de Active Directory con permisos para agregar máquinas al dominio:

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

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

Configuración de SSSD

Configurar SSSD consta de los siguientes pasos:

- Instalar 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 A continuación, se ofrece un ejemplo de configuración de **sssd.conf** (se pueden agregar opciones adicionales, 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 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
<!--NeedCopy-->
```

Reemplace **ad.domain.com**, **server.ad.example.com** por el valor correspondiente. Para obtener más información, consulte sssd-ad(5) - Linux man page.

Establezca la pertenencia y los permisos de archivos 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 que la creación del directorio de inicio sea compatible con SELinux:

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

> **Sugerencia:**
>
> Al configurar Linux VDA, tenga en cuenta que, para SSSD, no hay ninguna configuración especial para el cliente Linux VDA. Para soluciones adicionales en el script **ctxsetup.sh**, use el valor predeterminado.

Verificar la configuración de Kerberos

Para verificar que Kerberos está configurado correctamente para su uso con Linux VDA, compruebe que el archivo keytab del sistema** se ha creado y contiene claves válidas:

```
sudo klist -ke
<!--NeedCopy-->
```

Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado. Ejecute el comando **kinit** de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:

```
sudo kinit  – k MACHINE$@REALM
<!--NeedCopy-->
```

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (\) al signo de dólar ($) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

Compruebe que el vale de concesión de vales de la cuenta de la máquina se ha almacenado en caché:

```
sudo klist -ke
<!--NeedCopy-->
```

Verificar la autenticación de usuarios

Use el comando **getent** para saber si se admite el formato del inicio de sesión y si funciona NSS:

```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

El parámetro **DOMAIN** indica la versión corta del nombre de dominio. Si se necesita otro formato de inicio de sesión, compruébelo 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 del sufijo NetBIOS: `username@DOMAIN`

Para verificar que el módulo SSSD PAM está configurado correctamente, use una cuenta de usuario de dominio para iniciar sesión en Linux VDA. La cuenta de usuario de dominio no se ha utilizado anteriormente.

```
sudo localhost  – l DOMAIN\username

id -u
<!--NeedCopy-->
```

Compruebe que se ha creado el archivo de caché con las credenciales de Kerberos para el **uid** devuelto por el comando:

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

Compruebe que los vales que se encuentran en la memoria caché de credenciales de Kerberos son válidos y no han caducado:

```
klist
<!--NeedCopy-->
```


Publicar aplicaciones

July 6, 2022

Con la versión 7.13 de Linux VDA, Citrix agregó la función de aplicaciones integradas a todas las plataformas Linux compatibles. No se requieren procedimientos de instalación específicos para utilizar esta funcionalidad.

> **Sugerencia:**
>
> Con la versión 1.4 de Linux VDA, Citrix comenzó a admitir el uso compartido de sesiones y el uso de aplicaciones publicadas no integradas.

Publicar aplicaciones mediante Citrix Studio

Puede publicar aplicaciones instaladas en un Linux VDA creando un grupo de entrega o agregando esas aplicaciones a un grupo de entrega existente. Este proceso es similar a la publicación de aplicaciones instaladas en el agente VDA para Windows. Para obtener más información, consulte la documentación de Citrix Virtual Apps and Desktops (basada en la versión de Citrix Virtual Apps and Desktops que esté utilizando).

> **Sugerencia:**
>
> Cuando configure grupos de entrega, compruebe que el tipo de entrega está establecido en **Escritorio y aplicaciones** o **Aplicaciones**.
>
> **Importante:**
>
> Se admite la publicación de aplicaciones con Linux VDA 1.4 y versiones posteriores. Linux VDA no admite la entrega de escritorios ni aplicaciones a la misma máquina. Para solucionar este problema, Citrix recomienda crear grupos de entrega separados para las entregas de escritorios y aplicaciones.
>
> **Nota:**
>
> Para usar aplicaciones integradas, no inhabilite el modo de ventanas integradas en StoreFront. El modo de ventanas integradas está habilitado de forma predeterminada. Si ya ha inhabilitado la opción configurando "TWIMode=Off", quite este parámetro en lugar de cambiarlo a "TWIMode=On". De lo contrario, es posible que no pueda lanzar un escritorio publicado.

Solución de problemas

El lanzamiento de una aplicación publicada puede tardar más de dos minutos y puede que las ventanas no aparezcan integradas. Si ocurre el problema, verifique que el modo integrado se haya habil-

itado tanto en Linux VDA como en StoreFront.

El comando para comprobar si el modo integrado está habilitado en Linux VDA:

```
sudo /opt/Citrix/VDA/bin/ctxreg list -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix"  |  grep "SeamlessEnabled"
<!--NeedCopy-->
```

Si muestra "SeamlessEnabled = 0x00000000", el modo integrado está habilitado. Para habilitarlo, ejecute el comando siguiente:

```
sudo /opt/Citrix/VDA/bin/ctxreg update  -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix"  -v "SeamlessEnabled" -d "0
    x00000001"
<!--NeedCopy-->
```

Problemas conocidos

A continuación, se presentan los problemas conocidos en la publicación de aplicaciones:

- Las aplicaciones publicadas no integradas no se lanzan cuando el modo de ventanas integradas se inhabilita en StoreFront, pero sigue habilitado en Linux VDA. Habilite o inhabilite el modo de ventanas integradas en Linux VDA y en StoreFront al mismo tiempo.
- No se admiten ventanas no rectangulares. Las esquinas de una ventana pueden dejar ver el fondo del lado del servidor.
- No se admite la vista previa del contenido de una ventana de una aplicación publicada.
- Actualmente, el modo integrado admite los siguientes administradores de ventanas: Mutter (CentOS7.3\RHEL7.3\SUSE12.2), Metacity (CentOS6.6\RHEL6.6\SUSE 11.4) y Compiz (Ubuntu 16.04). No se admiten Kwin y otros administradores de ventanas. Compruebe que el administrador de ventanas está establecido en uno que sea compatible.
- Al ejecutar varias aplicaciones LibreOffice, solo la que se lanza en primer lugar se muestra en Citrix Studio, porque estas aplicaciones comparten el proceso.
- Las aplicaciones publicadas basadas en Qt5 como "Dolphin"pueden no mostrar iconos. Para resolver el problema, consulte el artículo que se encuentra en https://wiki.archlinux.org/index.php/Qt.
- Todos los botones de barra de tareas de aplicaciones publicadas que se ejecutan en la misma sesión ICA se combinan en el mismo grupo. Para resolver este problema, establezca la propiedad de la barra de tareas en no combinar sus botones.

Imprimir

November 3, 2021

En este artículo, se ofrecen los procedimientos recomendados de impresión.

Instalación

Linux VDA requiere los filtros **cups** y **foomatic**. Ejecute los siguientes comandos en función de la distribución de Linux:

Compatibilidad con la impresión con RHEL 7:

```
sudo yum –y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

Compatibilidad con la impresión con RHEL 6:

```
sudo yum –y install cups

sudo yum -y install foomatic
<!--NeedCopy-->
```

Uso

Puede imprimir desde escritorios publicados y aplicaciones publicadas. En una sesión de Linux VDA, solo se asigna la impresora de cliente predeterminada. El nombre de la impresora debe ser diferente entre los escritorios y las aplicaciones. Se deben tener en cuenta las siguientes cuestiones:

- Para los escritorios publicados:
  `CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`
- Para las aplicaciones publicadas:
  `CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

> **Nota:**
>
> Si el mismo usuario abre un escritorio publicado y una aplicación publicada, ambas impresoras estarán disponibles para la sesión. No se puede imprimir en una impresora de escritorio cuando se está en una sesión de aplicación publicada; tampoco se puede imprimir en una impresora de aplicación cuando se está en un escritorio publicado.

Solución de problemas

No se puede imprimir

Hay una serie de elementos que comprobar cuando la impresión no funciona correctamente. El demonio de impresión es un proceso que se ejecuta para cada sesión y debe ejecutarse durante toda la sesión. Compruebe que el demonio de impresión se esté ejecutando.

```
ps –ef | grep ctxlpmngt
<!--NeedCopy-->
```

Si el proceso **ctxlpmngt** no se está ejecutando, inicie **ctxlpmngt** manualmente desde una línea de comandos. Si la impresión sigue sin funcionar, compruebe el marco CUPS. El servicio **ctxcups** sirve para la administración de impresoras y se comunica con el marco CUPS de Linux. Este es un proceso único por máquina y se puede comprobar con:

```
service ctxcups status
<!--NeedCopy-->
```

Registro adicional al imprimir CUPS

Al ser un componente de Linux VDA, el método para obtener el registro de un componente de impresión es similar al de los demás componentes.

Para RHEL, se necesitan pasos adicionales para configurar el archivo del servicio de CUPS. De lo contrario, algunos registros no se capturarán 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
<!--NeedCopy-->
```

> **Nota:**
>
> Esta configuración es solo para recopilar el registro completo de impresión cuando surja un problema. Por regla general, esta configuración no se recomienda porque afecta negativamente a la seguridad de CUPS.

La salida de impresión no se ha descifrado correctamente

Las impresiones ilegibles pueden deberse a un controlador de impresora incompatible. Se puede definir una configuración de controladores por usuario si se modifica el archivo de configuración **~/.CtxlpProfile$CLIENT_NAME**:

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
<!--NeedCopy-->
```

> **Importante:**
>
> El campo **printername** contiene el nombre de la impresora actual predeterminada del cliente. Es un valor de solo lectura. No debe modificarlo.
>
> Los campos **ppdpath**, **model** y **drivertype** no se pueden establecer a la vez, ya que solo uno tiene efecto en la impresora asignada.

Si el controlador de impresora universal no es compatible con la impresora cliente, configure el modelo del controlador de la impresora nativa con la opción **model**=. Puede buscar el nombre del modelo actual de la impresora con 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
<!--NeedCopy-->
```

A continuación, puede configurar el modelo para que coincida con la impresora:

```
Model=xerox/ph3115.ppd.gz
<!--NeedCopy-->
```

Si el controlador de impresora universal no es compatible con la impresora cliente, configure la ruta al archivo PPD del controlador nativo de la impresora. El valor de **ppdpath** es la ruta absoluta al archivo del controlador nativo de la impresora.

Por ejemplo, hay un controlador **PPD** en /home/tester/NATIVE_PRINTER_DRIVER.ppd:


```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
<!--NeedCopy-->
```

Existen tres tipos de controlador de impresora universal suministrados por Citrix (postscript, pcl5 y pcl6). Puede configurar el tipo de controlador si no hay disponible ningún controlador nativo de impresora.

Por ejemplo, si el tipo de controlador de la impresora predeterminada del cliente es PCL5:

```
drivertype=pcl5
<!--NeedCopy-->
```

El tamaño de la salida es cero

Pruebe diferentes tipos de impresoras. Asimismo, pruebe una impresora virtual (como CutePDF y PDFCreator) para averiguar si el problema está relacionado con el controlador de la impresora.

El trabajo de impresión depende del controlador de impresora establecido en la impresora predeterminada del cliente. Es importante identificar el tipo de controlador activo actual. Si la impresora cliente usa un controlador PCL5, pero Linux VDA elige un controlador PostScript, se puede producir un problema.

Si el tipo de controlador de la impresora es correcto, puede identificar el problema siguiendo estos pasos:

Para identificar este problema:

1. Inicie sesión en el escritorio de la sesión ICA.
2. vi ~/.CtxlProfile$CLIENT_NAME
3. Agregue el siguiente campo al archivo de grupo guardado en el Linux VDA:

   ```
   deletespoolfile=no
   <!--NeedCopy-->
   ```

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, habrá un archivo de cola de impresión guardado en **/var/spool/cups-ctx/$logon_user/$spool_file**.
6. Compruebe si la cola de impresión está vacía. Un archivo de cola de impresión vacío representa un problema. Póngase en contacto con la asistencia de Citrix (y facilite el registro de impresión) para obtener más información.
7. Si la cola de impresión no es cero, copie el archivo al cliente. El archivo de cola de impresión depende del tipo de controlador de impresora establecido en la impresora predeterminada del cliente. Si el controlador de la impresora asignada (nativa) es PostScript, el archivo de cola

de impresión se puede abrir directamente en el sistema operativo Linux. Compruebe que el contenido sea correcto.

Si el archivo de cola de impresión es PCL o si el sistema operativo del cliente es Windows, copie el archivo de cola de impresión al cliente e imprímalo mediante la impresora del cliente. Una vez completado este paso, pruebe con el otro controlador de la impresora.

8. Para cambiar la impresora asignada a un controlador externo de impresora, use 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
   <!--NeedCopy-->
   ```

   c) Elija la impresora asignada **CitrixUniversalPrinter:$ClientName:app/dek$SESSION_ID** y **Modify Printer**. Esta operación requiere privilegios de administrador.

   d) Conserve la conexión cups-ctx y, a continuación, haga clic en "Continue"para modificar el controlador de la impresora.

   e) En la página "Make and Model", elija otro controlador PostScript en lugar del controlador de impresora universal Citrix (por ejemplo, el controlador universal de Citrix PostScript). Por ejemplo, si está instalada la impresora virtual CUPS-PDF, puede seleccionar la impresora genérica CUPS-PDF. Guarde la modificación.

   f) Si este proceso se realiza correctamente, configure la ruta al archivo PPD del controlador en **.CtxlpProfile$CLIENT_NAME** para permitir que la impresora asignada use este controlador de terceros.

Problemas conocidos

Se han identificado los siguientes problemas al imprimir con Linux VDA:

El controlador CTXPS no es compatible con algunas impresoras PLC

Si se dañan las impresiones, establezca el controlador de impresora al controlador nativo que haya proporcionado el fabricante.

Impresión lenta de documentos grandes

Al imprimir un documento grande en una impresora local del cliente, el archivo que debe imprimirse se transfiere a través de una conexión de servidor. En conexiones lentas, esta transferencia puede

tardar mucho tiempo.

La impresora y las notificaciones de trabajos de impresión aparecen en otras sesiones

Linux no tiene el mismo concepto de sesión que Windows. Por lo tanto, todos los usuarios reciben notificaciones de todo el sistema. Para inhabilitar esas notificaciones, debe modificar el archivo de configuración CUPS: **/etc/cups/cupsd.conf**.

En el archivo, busque el nombre de la directiva actual configurada:

```
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>
<!--NeedCopy-->
```


Impresión de PDF

November 3, 2021

Con una versión de la aplicación Citrix Workspace que admita la impresión de PDF, puede imprimir archivos PDF convertidos en 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 los archivos PDF desde su visor de PDF e imprimirlos en la impresora que elija.

Linux VDA admite la impresión de archivos PDF en las siguientes versiones de la aplicación Citrix Workspace:

- Citrix Receiver para HTML5 de la versión 2.4 a la 2.6.9, la aplicación Citrix Workspace 1808 para HTML5 y versiones posteriores
- Citrix Receiver para Chrome de la versión 2.4 a la 2.6.9, la aplicación Citrix Workspace 1808 para Chrome y versiones posteriores
- Aplicación Citrix Workspace 1905 para Windows y versiones posteriores

Configuración

Aparte de usar una versión de la aplicación Citrix Workspace que admita la impresión de PDF, habilite las siguientes directivas en Citrix Studio:

- **Redirección de impresoras del cliente** (habilitada de forma predeterminada)
- **Crear automáticamente la impresora universal de PDF** (inhabilitada de forma predeterminada)

Con esas directivas habilitadas, si hace clic en **Imprimir** dentro de la sesión iniciada, aparecerá una vista previa de impresión en la máquina local para que seleccione una impresora. Consulte la documentación de la aplicación Citrix Workspace para obtener más información sobre la configuración de impresoras predeterminadas.

Configurar gráficos

November 30, 2022

En este artículo se ofrece una guía para configurar los gráficos y ajustes precisos en Linux VDA.

Para obtener más información, consulte Requisitos del sistema y la sección Información general de la instalación.

Parámetros de configuración

Existen varios parámetros de configuración referentes a gráficos en **HKEY_LOCAL_MACHINE\System\CurrentCon** que puede ajustar con la herramienta **ctxreg**.

Cómo habilitar Thinwire Plus

Thinwire Plus se habilita de forma predeterminada para VDA estándar y 3D Pro.

Cómo habilitar H.264

Además de los requisitos del sistema operativo, H.264 tiene un requisito mínimo para la versión de la aplicación Citrix Workspace (antes, Citrix Receiver). Si el cliente no cumple los requisitos, recurrirá a Thinwire Plus.

Sistema operativo	Requisito mínimo para H.264
Windows	3.4 o posterior
Mac OS X	11.8 o posterior
Linux	13.0 o posterior
Android	3.5
iOS	5.9
Chrome OS	1.4

La tabla de funciones más reciente de la aplicación Citrix Workspace está disponible en https://docs.citrix.com/es-es/citrix-workspace-app/citrix-workspace-app-feature-matrix.html.

Ejecute el siguiente comando para anunciar la codificación H.264 en el VDA:

```
1 sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\
     Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Cómo habilitar la codificación por hardware en HDX 3D Pro

Para HDX 3D Pro, el parámetro **AdvertiseH264** solo habilita la codificación H.264 de software. Ejecute este comando para habilitar la codificación por hardware:


```
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    Thinwire" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --
    force
<!--NeedCopy-->
```

> **Nota:**
>
> Si aparece el error `ctxreg command can't be found`, use el comando `ctxreg` con una ruta completa. Por ejemplo, use `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "REG_DWORD"-v "AdvertiseH264"-d "0x00000001"–force` en lugar de `sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "REG_DWORD"-v "AdvertiseH264"-d "0x00000001"–force`.

Cómo ajustar Thinwire Plus para un menor ancho de banda

- MaxColorDepth

  ```
  Default 0x20, type DWORD
  <!--NeedCopy-->
  ```

  Esta opción especifica la profundidad de color en gráficos transferidos al cliente a través del protocolo Thinwire.

  Para ahorrar ancho de banda, establézcalo en 0x10 (que representa la mejor profundidad de color para gráficos sencillos) o 0x8 (el modo experimental para anchos de banda bajos).

- Calidad

  Calidad visual

  ```
  Default: 0x1(medium), type: DWORD, valid values: 0x0(low), 0x1(
      medium), 0x2(high), 0x3(build to lossless), 0x4 always
      lossless.
  <!--NeedCopy-->
  ```

  Para ahorrar ancho de banda, configure la calidad en 0x0(low).

- Más parámetros

  - TargetFPS

    Velocidad de fotogramas de destino

    ```
    Default: 0x1e (30), Type: DWORD
    <!--NeedCopy-->
    ```

  - MinFPS

Velocidad de fotogramas mínima de destino

```
Default: 0xa (10), Type: DWORD
<!--NeedCopy-->
```

- MaxScreenNum

  La cantidad máxima de monitores que puede tener el cliente

```
Default: 0x2, Type: DWORD
<!--NeedCopy-->
```

  Para un VDA estándar, puede establecer un valor máximo de hasta 10. Para 3D Pro, el valor máximo permitido es de 4.

Solución de problemas

Compruebe qué codificación se utiliza

Ejecute el siguiente comando para comprobar si se utiliza la codificación H.264 (**1** significa H.264 y **0** significa Thinwire+):

```
sudo ctxreg dump | grep H264
<!--NeedCopy-->
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
```

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "
REG_DWORD"-v "AdvertiseH264"-d "0x00000001"--force
```

Compruebe si se utiliza la codificación por hardware para 3D Pro

Ejecute el siguiente comando (**0** significa que no se usa, **1** significa que sí se usa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
<!--NeedCopy-->
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

Otra forma de averiguarlo es usar el comando **nvidia-smi**. Los resultados son similares a lo siguiente si se utiliza la codificación por hardware:


```
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 |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Compruebe si el controlador de gráficos NVIDIA GRID se ha instalado correctamente

Para verificar si el controlador de gráficos NVIDIA GRID se ha instalado correctamente, ejecute **nvidia-smi**. El resultado es similar a:

```
+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  Tesla M60           Off  | 0000:00:05.0     Off |
                     Off |
```



```
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+
| Processes:                                                                  GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|
|  No running processes found
                                 |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Establezca la configuración correcta para la tarjeta:

`etc/X11/ctx-nvidia.sh`

Problemas de actualización de pantalla en varios monitores con HDX 3D Pro

Si ve problemas de actualización en pantallas que no sean el monitor principal, compruebe que la licencia de NVIDIA GRID está disponible.

Comprobar registros de error Xorg

El archivo de registro Xorg recibe un nombre similar a **Xorg.{DISPLAY}.log** en la carpeta **/var/log/**.

Problemas conocidos y limitaciones

Para vGPU, la consola local de XenServer muestra la pantalla de la sesión de escritorio ICA

Solución temporal: Inhabilite la consola VGA local de la máquina virtual ejecutando el siguiente comando:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
<!--NeedCopy-->
```


No se admite la API de NVENC en los perfiles de vGPU que no sean 8Q

Los perfiles vGPU de la tarjeta NVIDIA Tesla M60 que no sean 8Q no admiten CUDA. Por eso, no está disponible ni la API de NVENC ni la codificación por hardware de Citrix 3D Pro.

Las tarjetas gráficas NVIDIA K2 no admiten la codificación por hardware YUV444 en el modo PassThrough

Es una limitación de las tarjetas gráficas NVIDIA K2.

Los elementos emergentes de escritorio Gnome 3 son lentos cuando se inicia sesión

Esta es una limitación del inicio de sesiones en escritorios Gnome 3.

Algunas aplicaciones OpenGL o WebGL no se generan correctamente después de cambiar el tamaño de la ventana de Citrix Receiver

Si cambia el tamaño de la ventana de Citrix Receiver, cambiará la resolución de pantalla. El controlador propietario NVIDIA cambia algunos estados internos y puede requerir que las aplicaciones respondan adecuadamente. Por ejemplo, el elemento de la biblioteca WebGL. **lightgl.js** podría generar el error '`Rendering to this texture is not supported (incomplete frame buffer)`'.

Gráficos 3D sin cuadrícula

March 11, 2024

Información general

Con esta mejora de funcionalidad, Linux VDA admite no solo las tarjetas NVIDIA GRID 3D, sino también tarjetas 3D que no sean GRID.

Instalación

Para utilizar la función de gráficos en 3D sin cuadrícula, debe:

- Instale XDamage como requisito previo. Por lo general, XDamage existe como una extensión de XServer.
- Establezca `CTX_XDL_HDX_3D_PRO` en `Y` al instalar Linux VDA. Para obtener información sobre las variables de entorno, consulte Paso 3: Configure el entorno en tiempo de ejecución para completar la instalación.

Configuración

Archivos de configuración de Xorg

Si el controlador de tarjeta 3D es NVIDIA, los archivos de configuración están instalados y definidos automáticamente.

Otros tipos de tarjetas 3D

Si el controlador de 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

Con **ctx-driver_name-1.conf** como ejemplo, siga los pasos a continuación para modificar los archivos de configuración de plantillas:

1. Reemplace ***driver_name*** por el nombre del controlador real.

   Por ejemplo, si el nombre del 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 excluida de la ejecución mediante marcas de comentario. Esta sección describe la información del controlador de vídeo. Habilite esta sección antes de agregar la información del controlador de vídeo. Para habilitar esta sección:

   a) Consulte la guía de la tarjeta 3D proporcionada por el fabricante para obtener la información de configuración. Se puede generar un archivo de configuración nativo. Verifique que su tarjeta 3D funciona en un entorno local con el archivo de configuración nativo cuando no está usando una sesión ICA de Linux VDA.

   b) Copie la sección "Device"del archivo de configuración nativo a **ctx-driver_name-1.conf**.

3. Ejecute el siguiente comando para establecer la clave de Registro y permitir que Linux VDA reconozca el nombre del archivo de configuración modificado en el paso 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
     DriverName" -d "intel" --force
2 <!--NeedCopy-->
```

Habilitar la función de gráficos 3D sin cuadrícula

La función de gráficos 3D sin cuadrícula está inhabilitada de forma predeterminada. Puede ejecutar el siguiente comando para habilitar esta función estableciendo XDamageEnabled en 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
     XDamageEnabled" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Solución de problemas

No hay salida gráfica, o esta no se descifró correctamente

Si se pueden ejecutar aplicaciones 3D localmente y todas las configuraciones son correctas, cuando no hay ninguna salida gráfica o ésta es ilegible, es posible que sea resultado de un fallo. Use /opt/Citrix/VDA/bin/setlog y establezca GFX_X11 con el valor “verbose”para recopilar la información de seguimiento para la depuración.

La codificación por hardware no funciona

Esta función admite solamente la codificación por software.

Configurar directivas

November 3, 2021

Instalación

Consulte los artículos de instalación para preparar Linux VDA.

Dependencias

Debe instalar estas dependencias antes de instalar el paquete de Linux VDA.

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
<!--NeedCopy-->
```

SLES/SELD:

```
sudo zypper install openldap2

sudo zypper install libxml2

sudo zypper install cyrus-sasl

sudo zypper install cyrus-sasl-gssapi
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Configuración

Configuración de directivas en Citrix Studio

Para configurar directivas en Citrix Studio, lleve a cabo lo siguiente:

1. Abra **Citrix Studio**.
2. Seleccione el panel **Directivas**.
3. Haga clic en **Crear directiva**.
4. Establezca la directiva según la Lista de directivas disponibles.

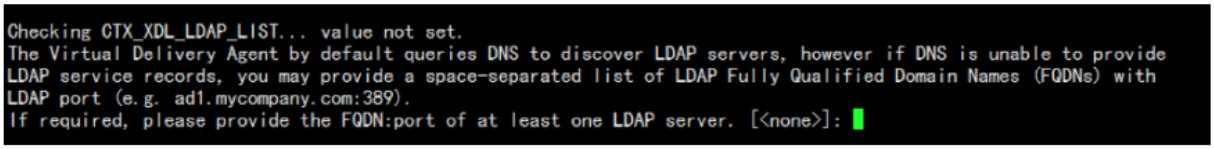
Configuración del servidor LDAP en el VDA

En caso de entornos de dominio único, configurar el servidor LDAP en Linux VDA es optativo; es obligatorio en caso de entornos con varios dominios y varios bosques. Esta configuración es necesaria para que el servicio de directiva realice una búsqueda LDAP en esos entornos.

Después de instalar el paquete de Linux VDA, ejecute el comando:

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Escriba todos los servidores LDAP en este formato: lista de nombres de dominio completos (FQDN) de LDAP, separados por espacios, con el puerto de LDAP (p. ej.: ad1.miempresa.com:389 ad2.miempresa.com:389).



También puede ejecutar el comando **ctxreg** para escribir este parámetro 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
<!--NeedCopy-->
```

Las siguientes directivas solamente se aplican a Linux VDA y solo se pueden configurar desde Citrix Studio versión 7.12 y posteriores:

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

Se ofrece una descripción de esas directivas en la Lista de directivas disponibles. Si usa Citrix Studio versión 7.11 o versiones anteriores, debe configurar estas directivas localmente en el Linux VDA mediante el comando **ctxreg**.

> **Nota:**
>
> Los valores están limitados a un intervalo determinado. Para ver descripciones detalladas, consulte la Lista de directivas disponibles.

Lista de directivas disponibles

November 3, 2021

Lista de directivas admitidas en Linux VDA

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
ICA Keep Alive	SendICAKeepAlives	Equipo	ICA Keep-Alive	No enviar mensajes de ICA Keep Alive (0)
Tiempo de espera de ICA Keep Alive	ICAKeepAliveTimeout	Equipo	ICA Keep-Alive	60 segundos
Número de puerto de escucha ICA	IcaListenerPortNumber	Equipo	ICA	1494
Límite de ancho de banda de redirección de sonido	LimitAudioBw	Usuario	Audio	0 Kbps
Redirección de audio del cliente	AllowAudioRedirection	Usuario	Audio	Permitido (1)
Redirección de impresoras del cliente	AllowPrinterRedir	Usuario	Impresión	Permitido (1)
Redirección del portapapeles del cliente	AllowClipboardRedir	Usuario	Portapapeles	Permitido (1)
Redirección de dispositivos USB del cliente	AllowUSBRedir	Usuario	USB	Prohibido (0)
Reglas de redirección de dispositivos USB del cliente	USBDeviceRules	Usuario	USB	“\0”
Compresión de imágenes en movimiento	MovingImageCompression	Usuario	Configuration Thinwire	Habilitado (1)

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Velocidad de fotogramas mínima de destino	TargetedMinimumFramesPerSecond	Usuario	Thinwire	10 fps
Velocidad de fotogramas de destino	FramesPerSecond	Usuario	Thinwire	30 fps
Calidad visual	VisualQuality	Usuario	Thinwire	Media (3)
Usar códec de vídeo para compresión	VideoCodec	Usuario	Thinwire	Usar si se prefiere (3)
Usar codificación por hardware para códec de vídeo	UseHardwareEncodingForVideoCodec	Usuario	Thinwire	Habilitado (1)
Profundidad de color preferida para gráficos simples	PreferredColorDepth	Usuario	Thinwire	24 bits por píxel (1)
Calidad de audio	SoundQuality	Usuario	Audio	Alto –Sonido de alta definición (2)
Redirección de micrófonos del cliente	AllowMicrophoneRedir	Usuario	Audio	Permitido (1)
Número máximo de sesiones	MaximumNumberOfSessions	Equipo	Administración de carga	250
Tolerancia de inicios de sesión simultáneos	ConcurrentLogonsTolerance	Equipo	Administración de carga	2
Habilitar actualización automática de Controllers	EnableAutoUpdateOfControllers	Equipo	Parámetros de Virtual Delivery Agent	Permitido (1)
Modo de actualización de la selección del portapapeles	ClipboardSelectionUpdateMode	Usuario	Portapapeles	3

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Modo de actualización de la selección primaria	PrimarySelectionUpdateMode	DataMode	Portapapeles	3
Calidad máxima de Speex	MaxSpeexQuality	Usuario	Audio	5
Conectar automáticamente las unidades del cliente	AutoConnectDrives	Usuario	ICA\Redirección de archivos	Habilitado (1)
Unidades ópticas del cliente	AllowCdromDrives	Usuario	ICA\Redirección de archivos	Permitido (1)
Unidades fijas del cliente	AllowFixedDrives	Usuario	ICA\Redirección de archivos	Permitido (1)
Unidades de disco flexible del cliente	AllowFloppyDrives	Usuario	ICA\Redirección de archivos	Permitido (1)
Unidades de red del cliente	AllowNetworkDrives	Usuario	ICA\Redirección de archivos	Permitido (1)
Unidades extraíbles del cliente	AllowRemoveableDrives	Usuario	ICA\Redirección de archivos	Permitido (1)
Redirección de unidades del cliente	AllowDriveRedir	Usuario	ICA\Redirección de archivos	Permitido (1)
Acceso de lectura solamente a unidades del cliente	ReadOnlyMappedDrive	Usuario	ICA\Redirección de archivos	Inhabilitado (0)

Se pueden configurar las siguientes directivas en la versión 7.12 de Citrix Studio o versiones posteriores.

- MaxSpeexQuality

  Valor (entero): [0 a 10]

  Valor predeterminado: 5

  Detalles:

La redirección de sonido codifica los datos de sonido con el códec Speex cuando la calidad del sonido es media o baja (consulte la directiva Calidad de sonido). Speex es un códec de compresión con pérdida, lo que significa que comprime datos a expensas de la fidelidad respecto a la señal de entrada de voz. A diferencia de otros códecs, con él se puede controlar la compensación entre calidad y velocidad de bits. El proceso de codificación de Speex se controla generalmente gracias a un parámetro de calidad que oscila entre 0 y 10. Cuanto mayor sea la calidad, mayor es la velocidad de bits.

Calidad máxima de Speex elige la mejor calidad de Speex para codificar los datos de sonido en función de la calidad de sonido y del límite de ancho de banda (consulte la directiva Límite de ancho de banda de redirección de sonido). Si la calidad del sonido es media, el codificador se coloca en el modo de banda ancha, lo que implica una mayor frecuencia de muestreo. Si la calidad del sonido es baja, el codificador se coloca en el modo de banda estrecha, lo que implica una menor frecuencia de muestreo. La misma calidad Speex tiene diferentes velocidades de bits según el modo. La mejor calidad Speex es cuando el valor más alto cumple las siguientes condiciones:

- Es igual o menor que la calidad máxima de Speex.
- Su velocidad de bits es igual o menor que el límite del ancho de banda.

Configuraciones relacionadas: Calidad de audio, Límite de ancho de banda de redirección de sonido.

- PrimarySelectionUpdateMode

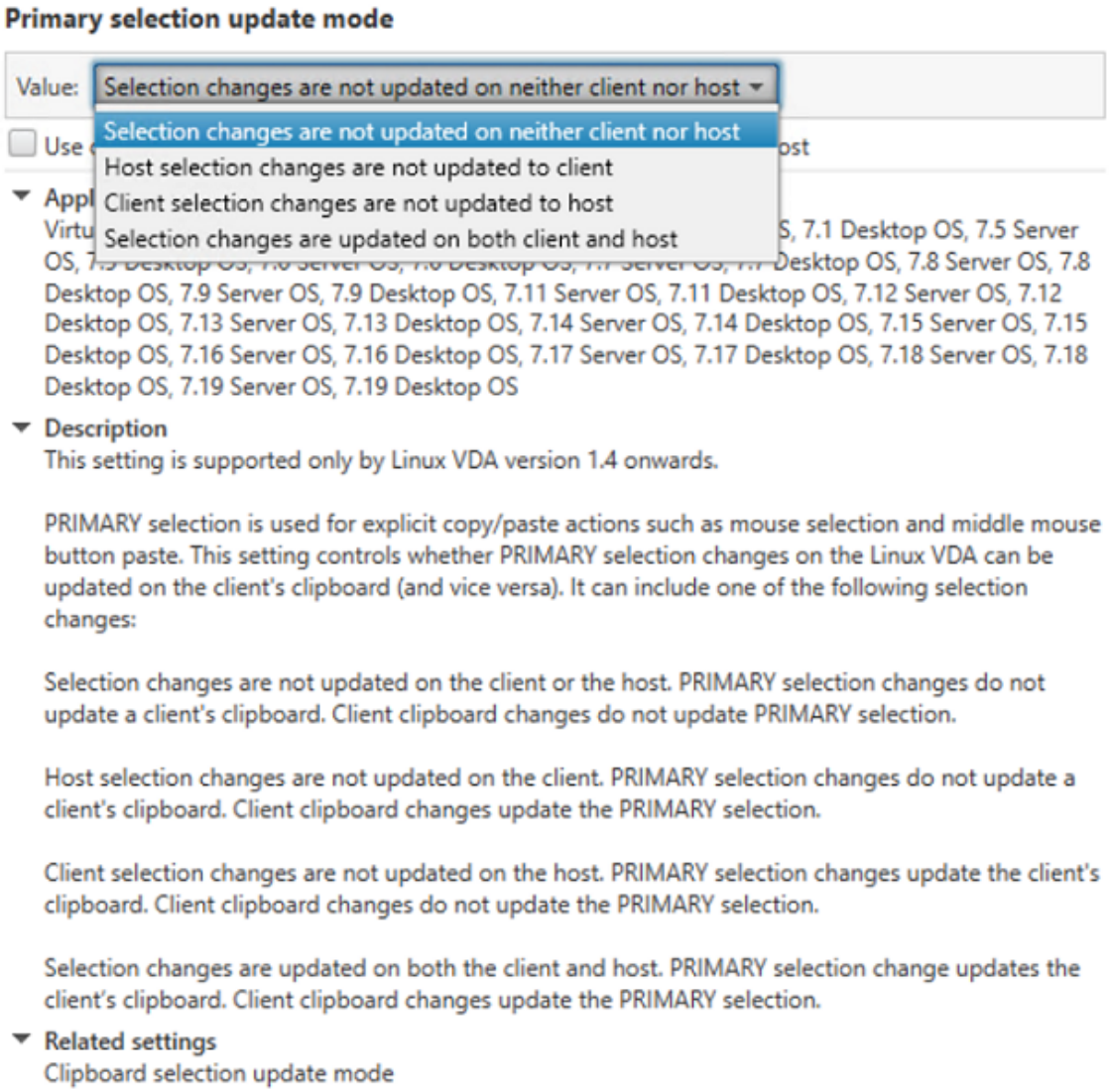
  Valor (enumeración): [0, 1, 2, 3]

  Valor predeterminado: 3

  Detalles:

  La selección principal se utiliza al seleccionar datos y pegarlos pulsando el botón central del ratón.

  Esta directiva controla si los cambios realizados con la selección principal en Linux VDA se pueden actualizar en el portapapeles del cliente (y viceversa). Hay cuatro opciones de valores:



- **Los cambios de selección no se actualizan ni en el cliente ni en el host**
  Los cambios realizados con la selección principal en Linux VDA no actualizan el portapapeles en el cliente. Los cambios realizados con la selección principal en el cliente no actualizan el portapapeles en Linux VDA.
- **Los cambios de selección en el host no se actualizan en el cliente**
  Los cambios realizados con la selección principal en Linux VDA no actualizan el portapapeles en el cliente. Los cambios realizados con la selección principal en el cliente actualizan el portapapeles en Linux VDA.
- **Los cambios de selección realizados en el cliente no se actualizan en el host**
  Los cambios realizados con la selección principal en Linux VDA actualizan el portapapeles en el cliente. Los cambios realizados con la selección principal en el cliente no actualizan el portapapeles en Linux VDA.

- **Los cambios de selección se actualizan tanto en el cliente como en el host**
  Los cambios realizados con la selección principal en Linux VDA actualizan el portapapeles en el cliente. Los cambios realizados con la selección principal en el cliente actualizan el portapapeles en Linux VDA. Esta opción es el valor predeterminado.

Parámetro relacionado: Modo de actualización de la selección de portapapeles

- ClipboardSelectionUpdateMode

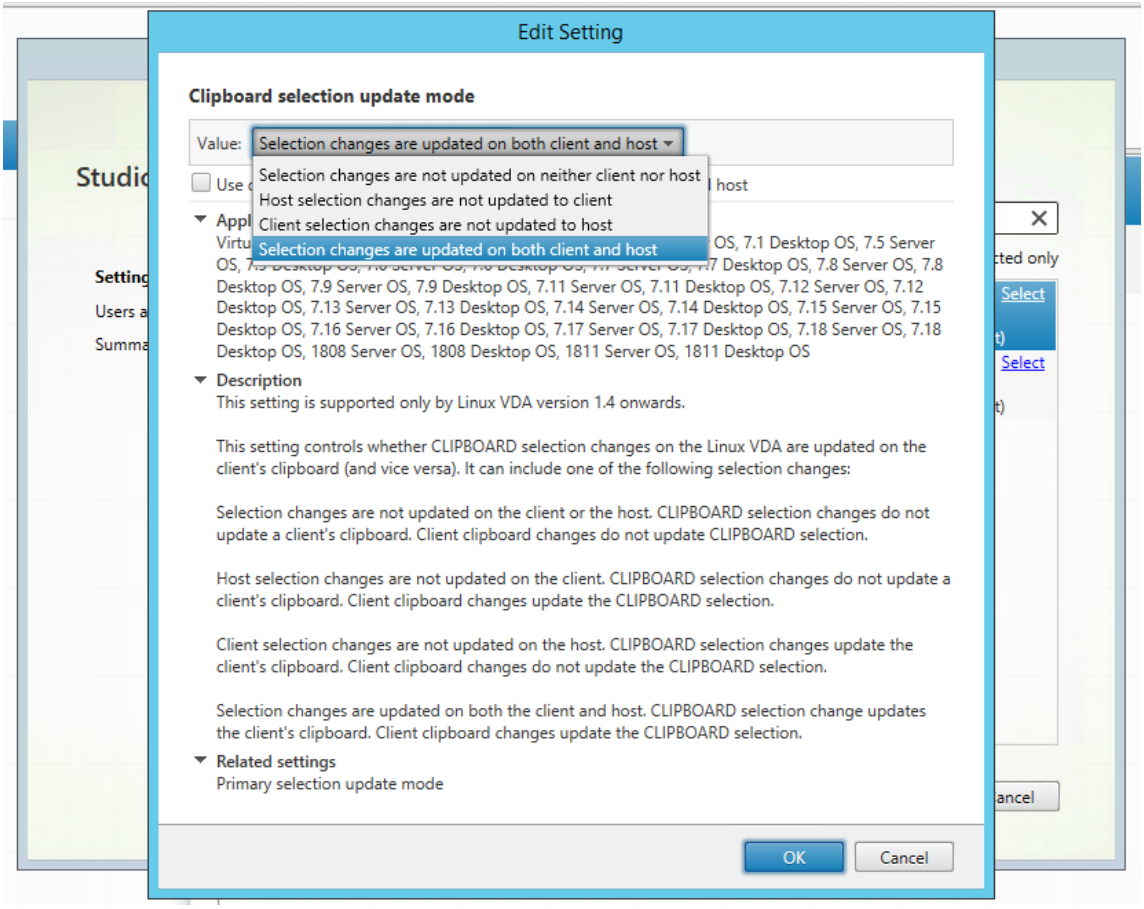
  Valor (enumeración): [0, 1, 2, 3]

  Valor predeterminado: 3

  Detalles:

  La selección de portapapeles se utiliza cuando selecciona datos y solicita explícitamente que se "copien"en el portapapeles, por ejemplo, seleccionando "Copiar"en el menú contextual. La selección de 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 realizados con la selección de portapapeles en Linux VDA se pueden actualizar en el portapapeles del cliente (y viceversa). Hay cuatro opciones de valores:



- **Los cambios de selección no se actualizan ni en el cliente ni en el host**
  Los cambios realizados con la selección de portapapeles en Linux VDA no actualizan el portapapeles en el cliente. Los cambios realizados con la selección de portapapeles en el cliente no actualizan el portapapeles en Linux VDA.
- **Los cambios de selección en el host no se actualizan en el cliente**
  Los cambios realizados con la selección de portapapeles en Linux VDA no actualizan el portapapeles en el cliente. Los cambios realizados con la selección de portapapeles en el cliente actualizan el portapapeles en Linux VDA.
- **Los cambios de selección realizados en el cliente no se actualizan en el host**
  Los cambios realizados con la selección de portapapeles en Linux VDA actualizan el portapapeles en el cliente. Los cambios realizados con la selección de portapapeles en el cliente no actualizan el portapapeles en Linux VDA.
- **Los cambios de selección se actualizan tanto en el cliente como en el host**
  Los cambios realizados con la selección de portapapeles en Linux VDA actualizan el portapapeles en el cliente. Los cambios realizados con la selección de portapapeles en el cliente actualizan el portapapeles en Linux VDA. Esta opción es el valor predeterminado.

Parámetro relacionado: Modo de actualización para la selección primaria

> **Nota:**
>
> Linux VDA admite tanto la selección del portapapeles como la selección primaria. Para controlar los comportamientos de las funciones copiar y pegar entre Linux VDA y el cliente, se recomienda que configure el modo de actualización de selección de portapapeles y el modo de actualización de selección principal con el mismo valor.

Configurar IPv6

November 3, 2021

Linux VDA ofrece soporte para que IPv6 admita XenApp y XenDesktop. Cuando use esta función, tenga en cuenta lo siguiente:

- Para entornos de doble pila, se usa IPv4 a menos que se habilite IPv6 de forma explícita.
- Si se habilita IPv6 en un entorno de IPv4, el Linux VDA no funciona.

> **Importante:**
>
> - Todo el entorno de red debe ser IPv6, no solo el entorno para Linux VDA.

> • Centrify no admite el uso de IPv6 puro.

No se requieren tareas de configuración especiales para IPv6 cuando se instala Linux VDA.

Configurar IPv6 para Linux VDA

Antes de cambiar la configuración para Linux VDA, asegúrese de que la máquina virtual Linux ya funcionó anteriormente en una red IPv6. Hay dos claves del Registro relacionadas con la configuración IPv6:

```
1 “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
    -v “OnlyUseIPv6ControllerRegistration”
2
3 “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
    -v “ControllerRegistrationIPv6Netmask”
4 <!--NeedCopy-->
```

OnlyUseIPv6ControllerRegistration debe establecerse en 1 para que Linux VDA pueda usar IPv6:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
    OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Si Linux VDA tiene más de una interfaz de red, se puede usar **ControllerRegistrationIPv6Netmask** para especificar cuál se utiliza para el registro de Linux VDA:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "
    ControllerRegistrationIPv6Netmask " -d "{
2  IPv6 netmask }
3  " --force
4 <!--NeedCopy-->
```

Sustituya **{IPv6 netmask}** por la máscara de red real (por ejemplo, 2000::/64).

Para obtener más información acerca de la implementación de IPv6 en XenApp y XenDesktop, consulte Compatibilidad con IPv4/IPv6.

Solución de problemas

Compruebe el entorno básico de red IPv6 y use el comando ping6 para comprobar si se puede establecer contacto con AD y el Delivery Controller.

Configurar el programa Customer Experience Improvement Program (CEIP) de Citrix

February 11, 2021

Cuando participa en el programa CEIP, se envían estadísticas e información de uso anónimas a Citrix para ayudar a mejorar la calidad y el rendimiento de los productos Citrix.

Parámetros del Registro

De forma predeterminada, la participación en el programa CEIP es automática al instalar Linux VDA. La primera carga de datos tiene lugar aproximadamente siete días después de instalar Linux VDA. Puede cambiar esta opción predeterminada en el Registro del sistema.

- **CEIPSwitch**

Parámetro de Registro que habilita o inhabilita el programa CEIP (predeterminado = 0):

Ubicación: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nombre: CEIPSwitch

Valor: 1 = inhabilitado, 0 = habilitado

Si no se especifica, significa que CEIP está habilitado.

Puede ejecutar el siguiente comando en un cliente para inhabilitar el programa CEIP:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "CEIPSwitch" -d "1"
2 <!--NeedCopy-->
```

- **DataPersistPath**

Parámetro de Registro que controla la ruta de persistencia de datos (predeterminado = /var/xdl/-ceip):

Ubicación: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nombre: DataPersistPath

Valor: cadena

Puede ejecutar el comando siguiente para establecer esta ruta:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "DataPersistPath" -d "your_path"
2 <!--NeedCopy-->
```


Si la ruta configurada no existe o no se puede acceder a ella, los datos se guardan en la ruta predeterminada.

Datos CEIP recopilados de Linux VDA

La siguiente tabla ofrece un ejemplo de los tipos de información anónima que se recopilan. Los datos no contienen detalles que lo identifiquen a usted como cliente.

Punto de datos	Nombre de la clave	Descripción
GUID de la máquina	machine_guid	Identificación de la máquina donde se originan los datos
Solución AD	ad_solution	Cadena de texto que indica el método por el que se unió la máquina al dominio
Versión de kernel de Linux	kernel_version	Cadena de texto que indica la versión de kernel de la máquina
Versión LVDA	vda_version	Cadena de texto que indica la versión instalada de Linux VDA
LVDA es actualización o instalación nueva	update_or_fresh_install	Cadena de texto que indica si el paquete de Linux VDA actual se instaló como nuevo o si es una actualización
Método de LVDA instalado	install_method	Cadena de texto que indica que el paquete de Linux VDA se instala mediante MCS, PVS, Easy Install, 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
Último reinicio de los servicios principales de LVDA	ctxhdx ctxvda	La fecha y hora a la que se reiniciaron por última vez los servicios `ctxhdx` y `ctxvda`, en el formato dd-hh:mm:ss, por ejemplo, 10-17:22:19

Punto de datos	Nombre de la clave	Descripción
Tipo de GPU	gpu_type	Indica el tipo GPU de la máquina
Núcleos de CPU	cpu_cores	Número entero que indica la cantidad de núcleos de CPU de la máquina
Frecuencia de CPU	cpu_frequency	Número decimal 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 activas	active_session_number	Número entero que indica la cantidad de sesiones activas en la máquina en el momento de recopilar los datos
Versión y nombre 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	Identificación de la sesión donde se originan los datos
Coste de tiempo de reconexión	econnect_time_cost	Se usa para guardar el coste del tiempo de reconexión de la sesión. El tamaño de la matriz es 5, y en ella se registran el valor actual, el valor mínimo, el valor máximo, la suma corriente y el recuento de actualización de este punto de datos.
Tiempo de sesión activa	active_session_time	Se utiliza para guardar los tiempos de sesión activa. Una sesión puede tener varios periodos activos, porque la sesión puede desconectarse o reconectarse.
Duración de sesión	session_duration_time	Utilizado para guardar la duración de la sesión desde que se inicia la sesión hasta que se cierra

Punto de datos	Nombre de la clave	Descripción
Tipo de cliente Receiver	receiver_type	Número entero que indica la versión de Citrix Receiver utilizada para lanzar la sesión
Versión de cliente de Receiver	receiver_version	Cadena de texto que indica la versión de Citrix Receiver utilizada para lanzar la sesión
Recuento de impresión	printing_count	Número entero que indica cuántas veces se usó la funcionalidad de impresión en la sesión
Recuento de redirección USB	usb_redirecting_count	Número entero que indica cuántas veces la sesión usa un dispositivo USB

Configurar la redirección USB

November 3, 2021

Los dispositivos USB se comparten entre Citrix Receiver y el escritorio de Linux VDA. Cuando un dispositivo USB se redirige al escritorio, el usuario puede usar ese dispositivo como si estuviera conectado localmente.

La redirección USB incluye tres áreas principales de funcionalidad:

- Implementación de proyectos de código abierto (VHCI)
- Servicio VHCI
- Servicio USB

VHCI de código abierto:

Esta parte de la redirección USB desarrolla un sistema general para compartir dispositivos USB a través de una red IP. Se compone de un controlador de kernel Linux y algunas bibliotecas de modo usuario, que le permiten comunicarse con el controlador del kernel para obtener todos los datos de USB. En la implementación de Linux VDA, Citrix reutiliza el controlador del kernel de VHCI. Todas las transferencias de datos USB que se realizan entre el Linux VDA y Citrix Receiver se encapsulan en el paquete del protocolo ICA de Citrix.

Servicio VHCI:

El servicio VHCI es un servicio de código abierto que proporciona Citrix para comunicarse con el módulo de kernel VHCI. Este servicio funciona como una puerta de enlace entre VHCI y el servicio USB de Citrix.

Servicio USB:

El servicio USB de Citrix representa un módulo que administra la virtualización y las transferencias de datos en el dispositivo USB.

Cómo funciona la redirección USB

Por lo general, si un dispositivo USB se redirige correctamente a Linux VDA, se crean uno o varios nodos de dispositivos en la ruta /dev del sistema. Sin embargo, hay veces en que el dispositivo redirigido no puede utilizarse para una sesión activa de Linux VDA. Los dispositivos USB necesitan los controladores pertinentes para poder funcionar correctamente; algunos dispositivos requieren incluso controladores especiales. Por eso, si no se proporcionan los controladores adecuados, los dispositivos USB redirigidos resultan inaccesibles para una sesión activa de Linux VDA. Para garantizar la conectividad del dispositivo USB, instale los controladores y configure el sistema correctamente.

Linux VDA admite una lista de dispositivos USB que se redirigen correctamente a y desde el cliente. Además, el dispositivo se monta correctamente (sobre todo el disco USB), lo que permite a los usuarios acceder al disco sin ninguna configuración adicional.

Dispositivos USB admitidos

Se ha comprobado que los dispositivos siguientes admiten esta versión de VDA para Linux. Los demás dispositivos se pueden usar libremente, pero con resultados inesperados:

> **Nota:**
>
> Linux VDA solo admite protocolos USB 2.0.

Dispositivos de almacenamiento 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
Unidad flash SanDisk SDCZ80	0781:5580	FAT32
WD HDD	1058:10B8	FAT32

Mouse 3D por USB	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

Escáner USB	VID:PID
Epson Perfection V330 Photo	04B8: 0142

Configurar la redirección USB

Una directiva de Citrix controla si la redirección de dispositivos USB está habilitada o inhabilitada. Además, el tipo de dispositivo también se puede especificar con una directiva de Delivery Controller. Cuando configure la redirección USB para Linux VDA, defina la directiva y las reglas siguientes:

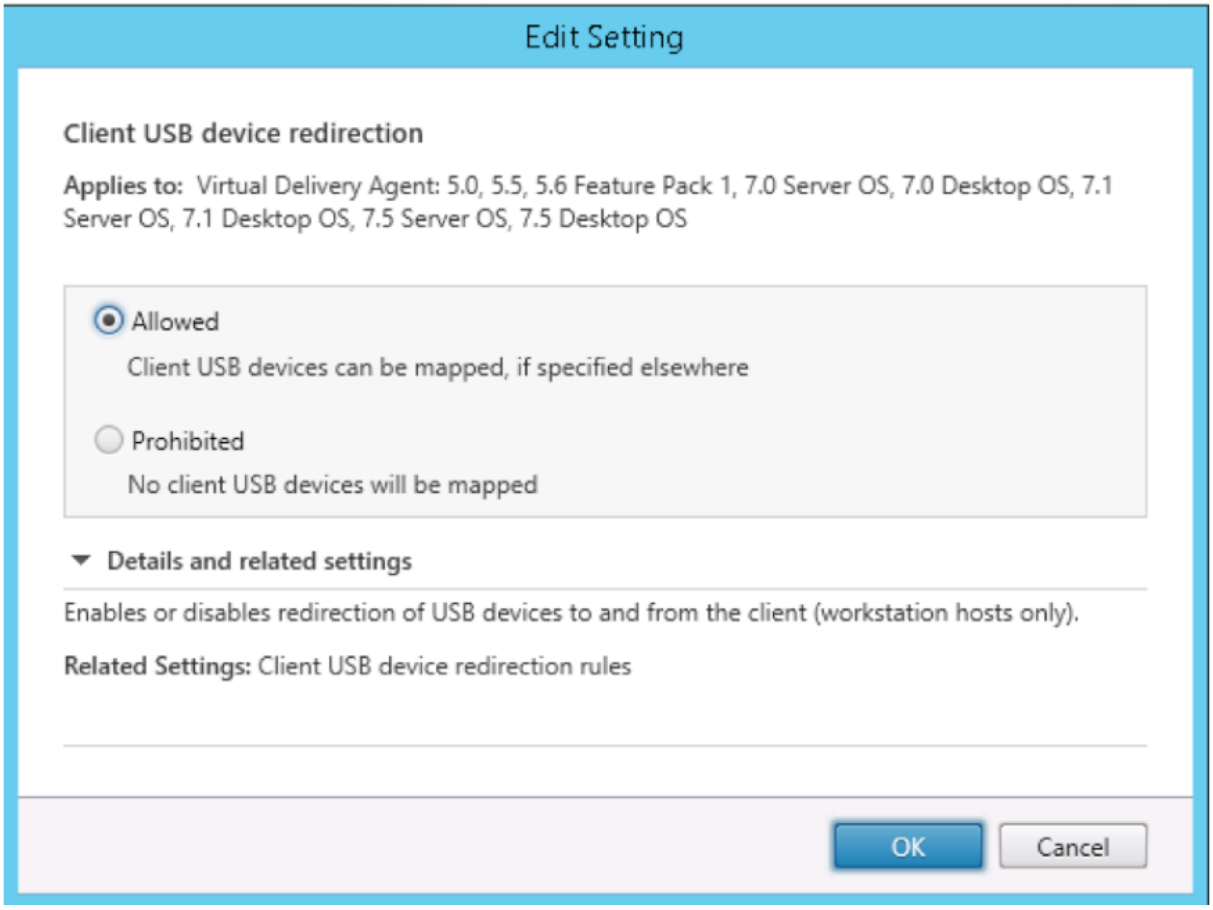
- Directiva de Redirección de dispositivos USB del cliente
- Reglas de redirección de dispositivos USB del cliente

Habilitar la directiva de redirección USB

En Citrix Studio, habilite (o inhabilite) la redirección de dispositivos USB desde y hacia el cliente (solo para hosts de estación de trabajo).

En el diálogo **Modificar configuración**:

1. Seleccione la opción **Permitido**.
2. Haga clic en **Aceptar**.

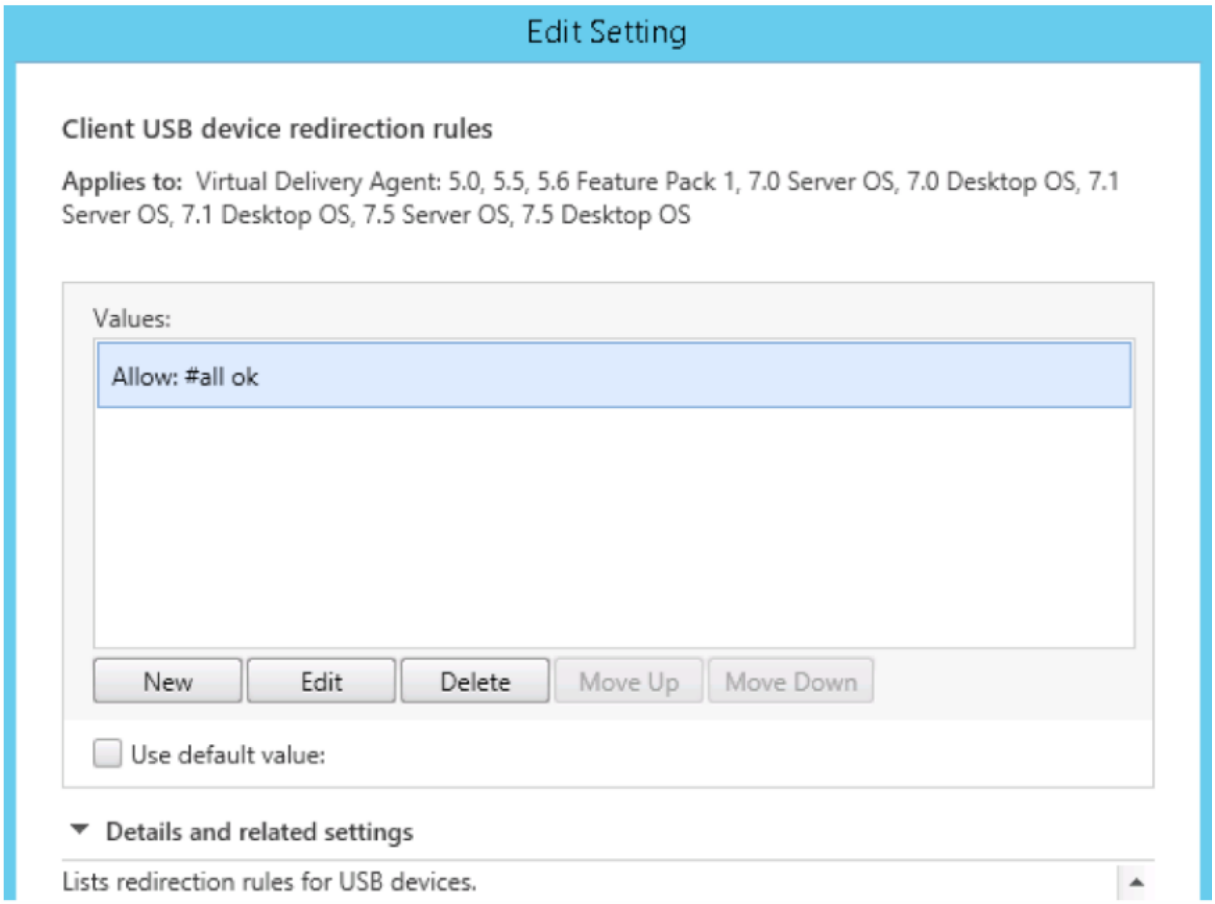


Configurar reglas de redirección USB

Después de habilitar la directiva de redirección USB, configure las reglas de redirección mediante Citrix Studio. Para ello, deberá especificar los dispositivos permitidos (o denegados) en el Linux VDA.

En el diálogo de reglas de redirección de dispositivos USB del cliente:

1. Haga clic en **Nueva** para agregar una regla de redirección, o bien haga clic en **Modificar** para revisar una regla existente.
2. Después de crear o modificar una regla, haga clic en **Aceptar**.



Para obtener más información sobre la configuración de la redirección de USB genérico, consulte Citrix Generic USB Redirection Configuration Guide.

Compilación del módulo de kernel VHCI

La redirección USB depende de los módulos de kernel VHCI (**usb-vhci-hcd.ko** y **usb-vhci-iocif.ko**). Esos módulos forman parte de la distribución de Linux VDA (como parte del paquete RPM). Se compilan en función de los kernels de la distribución oficial de Linux y se indican en la siguiente tabla:

Distribución compatible de Linux	Versión de kernel
RHEL 7.3	3.10.0-514.el7.x86_64
RHEL 6.6	2.6.32-504.el6.x86_64
SUSE 12.2	4.4.49-92.11-default
SUSE 11.4	3.0.101-0.47.55-default
Ubuntu 16.04	4.4.0-45-generic

> **Importante:**
>
> Si el kernel de la máquina no es compatible con el controlador creado por Citrix para Linux VDA, es posible que el servicio USB no se inicie. En este caso, puede utilizar la funcionalidad Redirección USB solamente si compila sus propios módulos de kernel VHCI.

Compruebe si el kernel es coherente con los módulos generados por Citrix

En la línea de comandos, ejecute el siguiente comando para comprobar si el kernel es coherente:

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
<!--NeedCopy-->
```

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, significa que el kernel no es coherente con el módulo de Citrix y se debe volver a generar.

Recompilación del módulo de kernel VHCI

Si el módulo de kernel no corresponde a la versión de Citrix, lleve a cabo lo siguiente:

1. Descargue el código fuente de LVDA desde el sitio de descargas de Citrix. Seleccione el archivo incluido en la sección "**Linux Virtual Delivery Agent (orígenes)**".
2. Restaure los archivos desde el archivo citrix-linux-vda-sources.zip; puede obtener los archivos de origen VHCI en **linux-vda-sources/vhci-hcd-1.15.tar.bz2**; puede restaurar los archivos VHCI mediante **tar xvfvhci-hcd-1.15.tar.bz2**.
3. Compile el módulo de kernel en función de los archivos de encabezado y del archivo **Module.symvers**. Siga estos pasos para instalar los archivos de encabezado del kernel y crear **Module.symvers** en función de la distribución pertinente de Linux:

   RHEL 7.3/RHEL 6.9/RHEL 6.6:

   ```
   yum install kernel-devel
   <!--NeedCopy-->
   ```

   SUSE 12.2:

   ```
   zypper install kernel-devel

   zypper install kernel-source
   <!--NeedCopy-->
   ```

   SUSE 11.4:


```
zypper install kernel-source
<!--NeedCopy-->
```

Ubuntu 16.04:

```
apt-get install linux-headers
<!--NeedCopy-->
```

> **Sugerencia:**
>
> Si la instalación se realiza correctamente, se creará una carpeta de kernel como:
>
> /usr/src/kernels/3.10.0-327.10.1.el7.x86_64

4. En la carpeta /usr/src/kernels/3.10.0-327.10.1.el7.x86_64, verifique que el archivo **Module.symvers** está presente. Si este archivo no está en la carpeta, compile el kernel para obtenerlo (por ejemplo, `make oldconfig`; `make prepare`; `make modules`; `make`) o cópielo desde **/usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.***
5. En el archivo **vhci-hcd-1.15/Makefile**, cambie el Makefile de VCHI y defina KDIR con el directorio de kernel:

```
#KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build

KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
<!--NeedCopy-->
```

6. En la carpeta **vhci-hcd-1.15/**, ejecute **make** para crear el kernel de VHCI.

> **Nota:**
>
> Si la compilación es correcta, **usb-vhci-hcd.ko** y **usb-vhci-iocifc.ko** se crean en la carpeta **vhci-hcd-1.15/**.

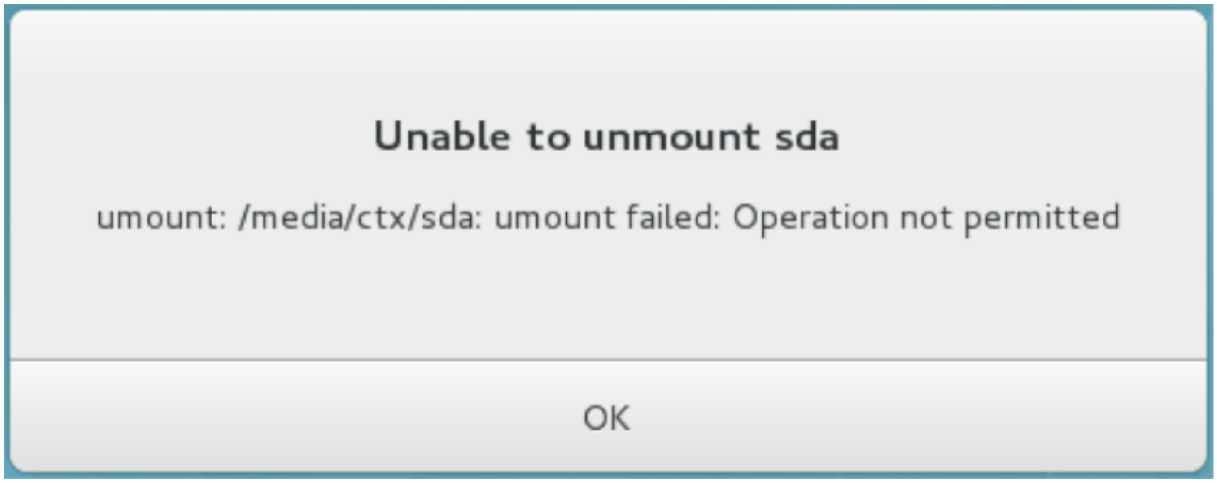
7. Reemplace el módulo de kernel con el recién compilado: **cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/**
8. Reinicie el servicio USB: **service ctxusbsd restart**.
9. Cierre la sesión y vuelva a iniciarla. Compruebe si la redirección USB está funcionando.

Solucionar problemas de redirección USB

Use la información de esta sección para solucionar problemas que puedan surgir al usar Linux VDA.

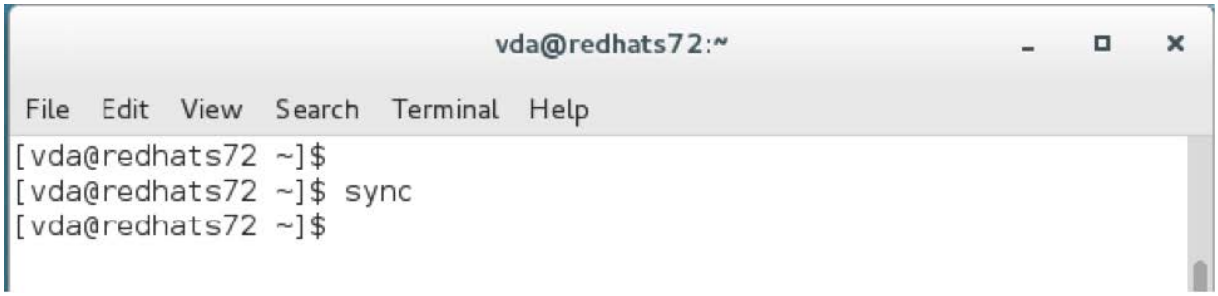
No se puede desmontar el disco USB redirigido

Para controlar el acceso a todos los discos USB redirigidos desde Citrix Receiver, Linux VDA administra todos esos dispositivos con privilegios administrativos para que solo el propietario pueda acceder al dispositivo redirigido. Por eso, el usuario no puede desmontar el dispositivo sin privilegios administrativos.



Se pierde el archivo cuando se detiene la redirección de un disco USB

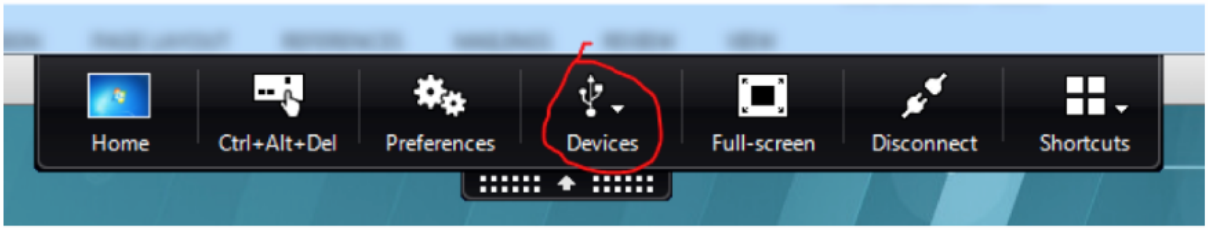
Si redirige un disco USB a una sesión y lo modifica (por ejemplo, crea archivos en él) y, justo después, detiene la redirección en la barra de herramientas de Citrix Receiver, el archivo modificado (o creado) se puede perder. Este problema se produce porque, cuando escribe datos en un sistema de archivos, el sistema monta la memoria caché en el sistema de esos archivos. Los datos no se escriben en el disco en sí. Si deja de redirigir el dispositivo desde la barra de herramientas de Citrix Receiver, no hay tiempo para que los datos se vuelquen en el disco, por lo que se pierden. Para resolver este problema, use el comando de sincronización en un terminal para vaciar datos en el disco antes de detener la redirección USB.



No hay dispositivos en la barra de herramientas de Citrix Receiver

En algunos casos, puede que no aparezcan dispositivos en la barra de herramientas de Citrix Receiver, lo que indica que no se está realizando la redirección USB. Si tiene este problema, compruebe lo siguiente:

- La directiva está configurada para permitir la redirección USB
- El módulo Kernel es compatible con su kernel



> **Nota:**
>
> La ficha **Dispositivos** no está disponible en la aplicación Citrix Receiver para Linux.

Los dispositivos USB se ven en la barra de herramientas de Citrix Receiver, pero tienen la etiqueta de *restringidos por directiva*, lo que provoca un error de redirección

Este problema ocurre por la configuración de directiva del dispositivo. En tales casos:

- Configure la directiva de Linux VDA para habilitar la redirección
- Compruebe si se han configurado restricciones de directiva adicionales en el Registro de Citrix Receiver. Puede que sea un parámetro del Registro de Citrix Receiver el que bloquee el dispositivo. Consulte **DeviceRules** en la ruta de Registro para comprobar que no se haya denegado el acceso del dispositivo mediante este parámetro:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Para obtener más información, consulte How to Configure Automatic Redirection of USB Devices en el sitio de asistencia técnica de Citrix.

El dispositivo USB se redirige correctamente, pero no lo puedo usar en mi sesión

Por lo general, solo se pueden redirigir los dispositivos USB admitidos. Sin embargo, en algunos casos, otros tipos de dispositivo pueden redirigirse a una sesión activa de Linux VDA. En esos casos, por cada dispositivo redirigido, se crea en la ruta **/dev** del sistema un nodo cuyo propietario es el usuario. Sin embargo, son los controladores y la configuración los que determinan si el usuario puede usar el dispositivo. Si hay un dispositivo conectado pero inaccesible, agréguelo a una directiva sin restricciones.

> **Nota:**
>
> En el caso de unidades USB, Linux VDA configura y monta el disco. El usuario (y solo el propietario que lo instaló) puede acceder al disco sin ninguna configuración adicional. Puede que no sea el caso para dispositivos que no consten en la lista de los dispositivos admitidos.

Editor de métodos de entrada (IME) de cliente

November 3, 2021

Introducción

Los caracteres de doble byte (por ejemplo, los caracteres de los idiomas chino, japonés y coreano) deben introducirse a través de un IME. Esos caracteres se pueden introducir con cualquier IME compatible con la aplicación Citrix Workspace en el lado del cliente, como el IME de CJK nativo de Windows.

Instalación

Esta función se instala automáticamente al instalar Linux VDA.

Uso

Abra una sesión de XenDesktop o XenApp de la forma habitual.

Cambie el método de entrada según sea necesario en el lado del cliente para empezar a usar el IME del cliente.

Problemas conocidos

- Es necesario hacer doble clic en una celda en una hoja de cálculo de Google para poder usar el IME del cliente para introducir caracteres en la celda.
- El IME del cliente no se inhabilita automáticamente en los campos de contraseña.
- La interfaz de usuario de IME no sigue al cursor en el área de entrada.
- El IME del cliente no se admite en una distribución SUSE 11.

HDX Insight

November 30, 2022

Información general

HDX Insight forma parte de Citrix Application Delivery Management (ADM) y se basa en el estándar más popular de la industria AppFlow. Esta función permite a los departamentos de TI ofrecer una experiencia de usuario excepcional, proporcionando una visibilidad completa de extremo a extremo en el tráfico ICA de Citrix que se transfiere a través del tejido de red de aplicaciones de NetScaler o Citrix SD-WAN.

En esta versión, Linux VDA admite parcialmente la funcionalidad de HDX Insight. Debido a que la función de administración de la experiencia de usuario final (End User Experience Management o EUEM) no está implementada, no están disponibles los puntos de datos de duración.

Instalación

No es necesario instalar paquetes dependientes.

Uso

HDX Insight analiza los mensajes de ICA pasados a través de NetScaler entre la aplicación Citrix Workspace y el Linux VDA.

Debe configurar una implementación de NetScaler Insight Center con Linux VDA y habilitar la función de HDX Insight. Puede migrar la implementación de NetScaler Insight Center a Citrix ADM sin perder la configuración, los parámetros o los datos existentes. Para obtener más información, consulte [Migrate from NetScaler Insight Center to Citrix ADM].(/es-es/citrix-application-delivery-management-software/current-release/deploy/migrating-netscaler-insight-center-to-mas.html)

Solución de problemas

No se muestran los puntos de datos

Puede haber dos motivos:

- HDX Insight no está configurado correctamente.

  Por ejemplo, AppFlow no está habilitado en NetScaler, o se ha configurado una instancia incorrecta de NetScaler en Insight Center.

- El canal virtual de control de ICA no se ha iniciado en Linux VDA.

  ```
  ps aux | grep -i ctxctl
  ```

  Si no se está ejecutando `ctxctl`, póngase en contacto con el administrador para notificar un fallo a Citrix.

No se muestran puntos de datos de aplicaciones

Compruebe que el canal virtual integrado está habilitado y que se lanza una aplicación integrada durante un tiempo.

Problema conocido

No se pueden ver los puntos de datos relacionados con la duración. Debido a que la función de EUEM no está implementada, los puntos de datos de duración (por ejemplo, el tiempo de retorno RTT de ICA) no están disponibles y aparecen como "N/A".

Rastreo activado

November 3, 2021

Introducción

Recopilar registros y reproducir problemas ralentiza los diagnósticos y degrada la experiencia del usuario. La función Rastreo activado permite reducir la carga. De forma predeterminada, el rastreo está habilitado para el VDA de Linux.

Configuración

A partir de ahora, el demonio `ctxlogd` y la utilidad setlog se incluyen en el paquete de la versión de Linux VDA. De forma predeterminada, el demonio `ctxlogd` se inicia después de instalar y configurar el VDA de Linux.

demonio ctxlogd

Todos los demás servicios que se rastrean dependen del demonio `ctxlogd`. Puede detener el demonio `ctxlogd` si no quiere rastrear Linux VDA.

Utilidad setlog

Rastreo activado se configura con la utilidad `setlog`, ubicada en la ruta **/opt/Citrix/VDA/bin/**. Solo el usuario root tiene privilegios para ejecutarla. Puede utilizar la interfaz gráfica o ejecutar comandos para ver y cambiar las configuraciones. Ejecute el siguiente comando para obtener ayuda con la utilidad `setlog`:

```
setlog help
<!--NeedCopy-->
```

Valores De forma predeterminada, la ruta de salida **Log Output Path** está establecida en **/var/log/xdl/hdx.log**, el tamaño máximo **Max Log Size** está establecido en 200 MB, y puede guardar dos archivos antiguos de registro como máximo en **Log Output Path**.

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
<!--NeedCopy-->
```

Ver o establecer un solo valor de `setlog`:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

Por ejemplo:

```
setlog value log_size 100
<!--NeedCopy-->
```

Niveles De forma predeterminada, el nivel de registro se establece en Advertencias o **Warnings**.

Ver los niveles de registro establecidos para los componentes:

```
setlog levels
<!--NeedCopy-->
```

Puede configurar todos los niveles de registro (incluidos Disable, Inherited, Verbose, Information, Warnings, Errors y Fatal Errors) con el siguiente comando:

```
setlog level <class> [<level>]
<!--NeedCopy-->
```


La variable **<class>** especifica un componente de Linux VDA. Para cubrir todos los componentes, establézcalos todos como:

```
setlog level all error

Setting log class ALL to ERROR.
<!--NeedCopy-->
```

Marcas De forma predeterminada, las marcas se configuran como se muestra a continuación:

```
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
<!--NeedCopy-->
```

Ver las marcas actuales:

```
setlog flags
<!--NeedCopy-->
```

Ver o establecer una sola marca de registro:

```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

Restaurar valores predeterminados Revertir todos los niveles, las marcas y los valores a los parámetros predeterminados:


```
setlog default
<!--NeedCopy-->
```

> **Importante:**
>
> El servicio `ctxlogd` se configura desde el archivo **/var/xdl/.ctxlog**, que solo puede crear el usuario root. Los demás usuarios no tienen el permiso de escritura en este archivo. Citrix recomienda que los usuarios root no otorguen permisos de escritura a otros usuarios. No seguir esta premisa puede derivar en una configuración arbitraria o malintencionada de `ctxlogd`, que puede afectar al rendimiento del servidor y, por lo tanto, a la experiencia del usuario.

Solución de problemas

El demonio `ctxlogd` falla y el servicio `ctxlogd` no se puede reiniciar si falta el archivo **/var/xdl/.ctxlog** (por ejemplo, si se ha eliminado por accidente).

/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.
<!--NeedCopy-->
```

Para resolver este problema, ejecute `setlog` como usuario root para volver a crear el archivo **/var/xdl/.ctxlog**. A continuación, reinicie el servicio `ctxlogd`, del que dependen los demás servicios.

Configurar sesiones no autenticadas

April 18, 2024

Use la información de este artículo para configurar sesiones no autenticadas. No se necesita ninguna configuración especial cuando se instala Linux VDA para usar esta función.

> **Nota:**
>
> Cuando configure sesiones no autenticadas, tenga en cuenta que la funcionalidad Preinicio de

> sesiones no está admitida. El preinicio de sesiones tampoco es compatible con la aplicación Citrix Receiver para Android.

Crear un almacén no autenticado

Para admitir una sesión no autenticada en Linux VDA, cree un almacén no autenticado con StoreFront.

Habilitar usuarios no autenticados en un grupo de entrega

Después de crear un almacén no autenticado, habilite usuarios no autenticados en un grupo de entrega para admitir sesiones no autenticadas. Para habilitar usuarios no autenticados en un grupo de entrega, siga las instrucciones indicadas en la documentación de XenApp y XenDesktop.

Establecer el tiempo de inactividad de la sesión no autenticada

El tiempo de inactividad predeterminado de una sesión no autenticada es de 10 minutos. Este valor se configura mediante el parámetro de Registro **AnonymousUserIdleTime**. Use la herramienta **ctxreg** para cambiar este valor. Por ejemplo, para establecer el parámetro de Registro en cinco minutos:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k  "HKLM\System\
     CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime  -d 0
     x00000005
2 <!--NeedCopy-->
```

Establecer la cantidad máxima de usuarios no autenticados

Para establecer la cantidad máxima de usuarios no autenticados, use la clave de Registro **MaxAnonymousUserNumber**. Esta configuración limita la cantidad de sesiones no autenticadas que se ejecutan a la vez en un Linux VDA. Use la herramienta **ctxreg** para configurar este parámetro de registro. Por ejemplo, para establecer el valor en 32:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k  "HKLM\System\
     CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber  -d  0
     x00000020
2 <!--NeedCopy-->
```

> **Importante:**
>
> Limite la cantidad de sesiones no autenticadas. El inicio simultáneo de demasiadas sesiones puede provocar problemas en el VDA (por ejemplo, que se agote la memoria disponible).

Solución de problemas

Tenga en cuenta lo siguiente al configurar sesiones no autenticadas:

- **No se pudo iniciar sesión en una sesión no autenticada**.

Compruebe que el Registro se haya actualizado para incluir lo siguiente (establecer en 0):

```
sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
    \Control\Citrix" -v MaxAnonymousUserNumber
<!--NeedCopy-->
```

Compruebe que el servicio **ncsd** se está ejecutando y está configurado para habilitar la memoria caché de **passwd**:

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
<!--NeedCopy-->
```

Establezca la variable de la memoria caché de **passwd** en **no** si está habilitado y, a continuación, reinicie el servicio **ncsd**. Es posible que tenga que volver a instalar Linux VDA después de cambiar esta configuración.

- **El botón de pantalla de bloqueo aparece con KDE en una sesión no autenticada**.

El menú y el botón de la pantalla de bloqueo están inhabilitados de forma predeterminada en una sesión no autenticada. Sin embargo, pueden aparecer en KDE. En KDE, para inhabilitar el menú y el botón de la pantalla de bloqueo de un usuario concreto, agregue las siguientes líneas al archivo de configuración **$Home/.kde/share/config/kdeglobals**. Por ejemplo:

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

Sin embargo, si el parámetro **KDE Action Restrictions** está configurado como inalterable en un archivo global **kdeglobals** como el de **/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals**, la configuración del usuario no tiene ningún efecto.

Para resolver este problema, modifique el archivo **kdeglobals** a nivel del sistema para quitar la etiqueta **\$i]** de la sección **[KDE Action Restrictions]**, o bien, use directamente la configuración a nivel del sistema para inhabilitar el menú y el botón de pantalla de bloqueo. Para obtener más información acerca de la configuración de KDE, consulte [KDE System Administration/Kiosk/Keys page.

Configurar LDAPS

April 18, 2024

LDAP seguro (LDAPS) permite habilitar el protocolo LDAP seguro (Secure Lightweight Directory Access Protocol) para sus dominios administrados con Active Directory para ofrecer comunicación a través de SSL (Secure Socket Layer) o TLS (Transport Layer Security).

De forma predeterminada, las comunicaciones LDAP entre las aplicaciones de cliente y de servidor no están cifradas. El protocolo LDAP con SSL/TLS (LDAPS) permite proteger el contenido de la consulta LDAP entre Linux VDA y los servidores LDAP.

Los siguientes componentes de Linux VDA tienen dependencias en LDAPS:

- Broker Agent: Registro de Linux VDA en Delivery Controller
- Servicio de directivas: Evaluación de directivas

La configuración de LDAPS implica lo siguiente:

- Habilitar LDAPS en Active Directory (AD) o el servidor LDAP
- Exportar la entidad de certificación (CA) raíz para uso del cliente
- Habilitar o inhabilitar LDAPS en Linux VDA
- Configurar LDAPS para plataformas de terceros
- Configurar SSSD
- Configurar Winbind
- Configurar Centrify
- Configurar Quest

Habilitar LDAPS en el servidor AD/LDAP

Puede habilitar el protocolo LDAP a través de SSL (LDAPS) instalando un certificado con el formato adecuado desde una entidad de certificación (CA) de Microsoft o una entidad de certificación (CA) de otro proveedor distinto de Microsoft.

> **Sugerencia:**
>
> LDAP a través de SSL/TLS (LDAPS) se habilita automáticamente al instalar una entidad de certificación raíz empresarial en un controlador de dominio.

Para obtener más información sobre cómo instalar el certificado y comprobar la conexión de LDAPS, consulte How to enable LDAP over SSL with a third-party certification authority en el sitio de asistencia técnica de Microsoft.

Si dispone de una jerarquía de entidades de certificación multicapa (por ejemplo, en dos o tres capas), no tiene automáticamente el certificado apropiado para la autenticación LDAPS en el controlador de dominio.

Para obtener información sobre cómo habilitar LDAPS para los controladores de dominio mediante una jerarquía de entidades de certificación multicapa, consulte el artículo LDAP over SSL (LDAPS) Certificate en el sitio de Microsoft TechNet.

Habilitar la entidad de certificación raíz para el uso del cliente

El cliente debe utilizar un certificado de una entidad de certificación en la que confíe el servidor LDAP. Para habilitar la autenticación LDAPS para el cliente, importe el certificado de la entidad de certificación (CA) raíz en el almacén de claves de confianza.

Para obtener más información sobre cómo exportar la entidad de certificación raíz, consulte Cómo exportar el certificado de entidad emisora de certificados raíz en el sitio Web de asistencia técnica de Microsoft.

Habilitar o inhabilitar LDAPS en Linux VDA

Para habilitar o inhabilitar LDAPS para Linux VDA, ejecute el siguiente script (habiendo iniciado una sesión como administrador):

La sintaxis del comando es la siguiente:

- Habilitar LDAP por SSL/TLS con el certificado de CA raíz suministrado:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- Recurrir a LDAP sin SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```


Configurar LDAPS para una plataforma de terceros

Además de componentes de Linux VDA, hay varios componentes de software de terceros que se adhieren a Linux VDA y pueden requerir también LDAP seguro, tales como SSSD, Winbind, Centrify y Quest. En las secciones siguientes se describe cómo configurar LDAP seguro con LDAPS, STARTTLS o sellado SASL.

> **Sugerencia:**
>
> No todos estos componentes de software prefieren usar el puerto SSL 636 para garantizar LDAP seguro. La mayoría de las veces, LDAPS (LDAP por SSL en el puerto 636) no puede coexistir con STARTTLS en 389.

SSSD

Configure el tráfico de LDAP seguro de SSSD en el puerto 636 o 389, según las opciones. Para obtener más información, consulte SSSD LDAP Linux man page.

Winbind

La consulta LDAP en Winbind utiliza el método ADS. Winbind solo admite el método StartTLS en el puerto 389. Los archivos de configuración afectados son **ldap.conf** y **smb.conf**. Cambie los archivos de la siguiente manera:

```
ldap.conf:

TLS_REQCERT never

smb.conf:

ldap ssl = start tls

ldap ssl ads = yes

client ldap sasl wrapping = plain
<!--NeedCopy-->
```

De forma alternativa, se puede configurar LDAP seguro mediante firma y sello de SASL GSSAPI, pero no puede coexistir con TLS/SSL. Para usar el cifrado SASL, cambie la configuración de **smb.conf**:

```
smb.conf:

ldap ssl = off

ldap ssl ads = no

client ldap sasl wrapping = seal
```



```
<!--NeedCopy-->
```

Centrify

Centrify no admite LDAPS en el puerto 636. No obstante, sí que ofrece cifrado seguro en el puerto 389. Para obtener más información, visite el sitio de Centrify.

Quest

Quest Authentication Service no admite LDAPS en el puerto 636, pero proporciona cifrado seguro en el puerto 389 mediante un método diferente.

Solución de problemas

Pueden producirse los siguientes problemas cuando se usa esta función:

- **Disponibilidad del servicio LDAPS**

  Compruebe que la conexión de LDAPS está disponible en el servidor AD/LDAP. El puerto está en 636 de forma predeterminada.

- **El registro de Linux VDA falla cuando LDAPS está habilitado**

  Verifique si el servidor LDAP y el puerto o los puertos están configurados correctamente. Compruebe primero el certificado de CA raíz y asegúrese de que coincide con el servidor de AD/LDAP.

- **Registro incorrecto cambiado por accidente**

  Si las claves relacionadas con LDAPS se actualizaron accidentalmente sin usar **enable_ldaps.sh**, esto puede romper la dependencia de los componentes de LDAPS.

- **El tráfico LDAP no se cifra mediante SSL/TLS desde Wireshark ni ninguna otra herramienta de supervisión de red**

  De forma predeterminada, LDAPS está inhabilitado. Ejecute **/opt/Citrix/VDA/sbin/enable_ldaps.sh** para forzarlo.

- **No hay tráfico LDAPS desde Wireshark o cualquier otra herramienta de supervisión de red**

  El tráfico de LDAP o LDAPS ocurre cuando tienen lugar el registro de Linux VDA y la evaluación de las directivas de grupo.

- **No se pudo comprobar la disponibilidad de LDAPS ejecutando “ldp connect”en el servidor de Active Directory**

  Use el nombre de dominio completo (FQDN) de AD en lugar de la dirección IP.

- **No se pudo importar el certificado de CA raíz ejecutando el script /opt/Citrix/VDA/sbin/enable_ldaps.sh**

  Proporcione la ruta de acceso completa del certificado de CA y compruebe si el certificado raíz de la CA es del tipo correcto. Por lo general, debería admitir la mayoría de los tipos de Java Keytool disponibles. Si no aparece en la lista de compatibilidad, puede convertir el tipo. Citrix recomienda el formato PEM con codificación base64 si encuentra algún problema de formato del certificado.

- **No se puede ver el certificado de CA raíz con el parámetro de 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.

Configurar Xauthority

November 3, 2021

Linux VDA admite los entornos que utilizan la funcionalidad de pantalla X11 (incluidos `xterm` y `gvim`) para la comunicación remota interactiva. Esta función proporciona un mecanismo de seguridad necesario para proteger la comunicación entre XClient y XServer.

Existen dos métodos para garantizar este permiso para la comunicación segura:

- **Xhost**. De forma predeterminada, Xhost solo permite al XClient de localhost la comunicación con XServer. Si elige permitir el acceso a XServer a un XClient remoto, el comando Xhost tiene que ser ejecutado para conceder permiso a esa máquina concreta. O bien, 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 usa para almacenar credenciales en las cookies utilizadas por xauth para la autenticación de XServer. Una vez que una instancia de XServer (Xorg) se ha iniciado, la cookie se usa para autenticar las conexiones específicas a esa pantalla concreta.

Funcionamiento

Cuando se inicia Xorg, se pasa un archivo `.Xauthority` a Xorg. Este archivo `.Xauthority` contiene los siguientes elementos:

- Número de pantalla
- Protocolo de solicitud remota

- Número de cookie

Puede examinar este archivo mediante el comando **xauth**. Por ejemplo:

```
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1
      fb228d1b695729242616c5908f11624b
<!--NeedCopy-->
```

Si XClient se conecta de forma remota a Xorg, deben cumplirse dos requisitos previos:

- Definir la variable de entorno **DISPLAY** con el valor del XServer remoto.
- Obtener el archivo `.Xauthority` que contiene uno de los números de cookie en Xorg.

Configurar Xauthority

Para habilitar Xauthority en Linux VDA para la pantalla X11 remota, deben crearse dos claves de Registro:

```
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
<!--NeedCopy-->
```

Después de habilitar Xauthority, pase el archivo `.Xauthority` a XClient manualmente o mediante el montaje de un directorio particular (home) compartido:

- Pasar el archivo `.Xauthority` a XClient manualmente

  Después de iniciar una sesión ICA, el Linux VDA genera el archivo `.Xauthority` para el XClient y almacena el archivo en el directorio home del usuario de inicio de sesión. Puede copiar este archivo `.Xauthority` en la máquina del XClient remoto 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 de archivo de Xauthority. Por ejemplo, fíjese en el comando siguiente:

  ```
  export DISPLAY={
  Display number stored in the Xauthority file }


  export XAUTHORITY={
  the file path of .Xauthority }
  ```



```
7
8  <!--NeedCopy-->
```

> **Nota:**
>
> Si la variable de entorno `XAUTHORITY` no está establecida, se usa el archivo `~/.Xauthority` de forma predeterminada.

- Pasar el archivo `.Xauthority` a XClient con el montaje de un directorio particular (home) compartido

  El método más cómodo es montar un directorio home compartido para el usuario que inicia la sesión. Cuando el Linux VDA inicia una sesión ICA, se crea el archivo `.Xauthority` en el directorio home del usuario de inicio de sesión. Si el directorio particular está compartido con XClient, el usuario no necesita transmitir este archivo `.Xauthority` manualmente a XClient. Una vez configuradas correctamente las variables de entorno DISPLAY y XAUTHORITY, la interfaz gráfica de usuario se muestra en el escritorio de XServer automáticamente.

Solución de problemas

Si Xauthority no funciona, siga los pasos indicados a continuación:

1. Como administrador con privilegios de root, recupere todas las cookies de Xorg:

   ```
   1 ps aux | grep -i xorg
   2 <!--NeedCopy-->
   ```

   Este comando muestra el proceso Xorg y los parámetros pasados a Xorg al iniciar. Otro parámetro muestra qué archivo `.Xauthority` se utiliza. Por ejemplo:

   ```
   1 /var/xdl/xauth/.Xauthority110
   2 <!--NeedCopy-->
   ```

   Muestre las cookies mediante el comando **Xauth**:

   ```
   1 Xauth -f /var/xdl/xauth/.Xauthority110
   2 <!--NeedCopy-->
   ```

2. Utilice el comando **Xauth** para mostrar las cookies contenidas en `~/.Xauthority`. Para el mismo número de pantalla, las cookies que se muestran deben ser las mismas en los archivos `.Xauthority` de Xorg y de XClient.
3. Si las cookies son las mismas, compruebe la accesibilidad del puerto de pantalla remota con la dirección IP del Linux VDA (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
<!--NeedCopy-->
```

El número de puerto es la suma de 6000 + \<número de pantalla\>.

Si se produce un error en la operación de Telnet, el firewall puede estar bloqueando la solicitud.