



# **Linux Virtual Delivery Agent 1912 LTSR**

## Contents

<b>Novedades</b>	<b>4</b>
<b>Cumulative Update 9 (CU9)</b>	<b>4</b>
<b>Cumulative Update 8 (CU8)</b>	<b>5</b>
<b>Cumulative Update 7 (CU7)</b>	<b>6</b>
<b>Problemas resueltos en el parche rápido 1 (19.12.7001) de la versión 1912 LTSR CU7</b>	<b>6</b>
<b>Cumulative Update 6 (CU6)</b>	<b>7</b>
<b>Cumulative Update 5 (CU5)</b>	<b>7</b>
<b>Problemas resueltos en la versión 1912 LTSR CU5</b>	<b>8</b>
<b>Cumulative Update 4 (CU4)</b>	<b>8</b>
<b>Problemas resueltos en la versión 1912 LTSR CU4</b>	<b>9</b>
<b>Cumulative Update 3 (CU3)</b>	<b>9</b>
<b>Problemas resueltos en la versión 1912 LTSR CU3</b>	<b>10</b>
<b>Cumulative Update 2 (CU2)</b>	<b>11</b>
<b>Problemas resueltos en la versión 1912 LTSR CU2</b>	<b>11</b>
<b>Cumulative Update 1 (CU1)</b>	<b>12</b>
<b>Problemas resueltos en la versión 1912 LTSR CU1</b>	<b>12</b>
<b>Acerca de esta versión</b>	<b>13</b>
<b>Problemas resueltos en la versión 1912 LTSR</b>	<b>14</b>
<b>Problemas conocidos</b>	<b>15</b>
<b>Avisos legales de terceros</b>	<b>17</b>
<b>Elementos retirados</b>	<b>17</b>
<b>Requisitos del sistema</b>	<b>18</b>
<b>Información general de la instalación</b>	<b>22</b>

<b>Instalación rápida con Easy Install (recomendado)</b>	<b>23</b>
<b>Instalar Linux Virtual Delivery Agent para RHEL o CentOS manualmente</b>	<b>41</b>
<b>Instalar Linux Virtual Delivery Agent para SUSE manualmente</b>	<b>74</b>
<b>Instalar Linux Virtual Delivery Agent para Ubuntu manualmente</b>	<b>98</b>
<b>Utilice Machine Creation Services (MCS) para crear máquinas virtuales Linux</b>	<b>129</b>
<b>Configurar Delivery Controllers</b>	<b>157</b>
<b>Configurar Linux VDA</b>	<b>159</b>
<b>Integrar NIS en Active Directory</b>	<b>159</b>
<b>Publicar aplicaciones</b>	<b>165</b>
<b>Acceso con Remote PC</b>	<b>167</b>
<b>Imprimir</b>	<b>177</b>
<b>Transferencia de archivos</b>	<b>184</b>
<b>Impresión de PDF</b>	<b>188</b>
<b>Configurar gráficos</b>	<b>189</b>
<b>Presentación progresiva de Thinwire</b>	<b>199</b>
<b>Gráficos 3D sin cuadrícula</b>	<b>201</b>
<b>Configurar directivas</b>	<b>204</b>
<b>Lista de directivas disponibles</b>	<b>205</b>
<b>Configurar IPv6</b>	<b>216</b>
<b>Configurar el programa Customer Experience Improvement Program (CEIP) de Citrix</b>	<b>217</b>
<b>Configurar la redirección USB</b>	<b>221</b>
<b>Configurar la fiabilidad de la sesión</b>	<b>231</b>
<b>Teclado de software</b>	<b>233</b>
<b>Editor de métodos de entrada (IME) de cliente</b>	<b>236</b>

<b>Compatibilidad con entradas en varios idiomas</b>	<b>237</b>
<b>Sincronización de la distribución de teclado dinámico</b>	<b>239</b>
<b>Sincronización de la interfaz de usuario IME del cliente</b>	<b>241</b>
<b>HDX Insight</b>	<b>242</b>
<b>Transporte adaptable</b>	<b>244</b>
<b>Rastreo activado</b>	<b>246</b>
<b>Remedar sesiones</b>	<b>249</b>
<b>Compatibilidad de la aplicación Citrix Workspace para HTML5</b>	<b>255</b>
<b>Supervisar sesiones de Linux en Citrix Director</b>	<b>256</b>
<b>Demonio del servicio de supervisión</b>	<b>257</b>
<b>Proteger sesiones de usuario con TLS</b>	<b>259</b>
<b>Proteger sesiones de usuario con DTLS</b>	<b>263</b>
<b>Compatibilidad con tarjetas inteligentes</b>	<b>264</b>
<b>Autenticación Single Sign-On de dos saltos</b>	<b>275</b>
<b>Configurar sesiones no autenticadas</b>	<b>278</b>
<b>Configurar LDAPS</b>	<b>280</b>
<b>Configurar Xauthority</b>	<b>285</b>
<b>Servicio de autenticación federada</b>	<b>288</b>

## Novedades

May 30, 2024

Cumulative Update 9 (CU9) es la versión más reciente de Linux Virtual Delivery Agent 1912 LTSR. CU9 no contiene problemas resueltos.

**Nota:**

A partir de la versión CU3, instale .NET Core Runtime 3.1 como requisito previo antes de poder instalar Linux VDA.

## Cumulative Update 9 (CU9)

May 30, 2024

Fecha de publicación: 30 de abril de 2024

### Acerca de esta versión

Cumulative Update 9 (CU9) es la versión más reciente de Linux Virtual Delivery Agent 1912 LTSR. CU9 no contiene problemas resueltos.

## Novedades

### Escalabilidad CPB/WCF mejorada

Ahora se incluye una mejora de escalabilidad CPB/WCF de Linux VDA y cada Citrix Cloud Connector puede admitir 3000 Linux VDA. Puede implementar dos Cloud Connector en cada ubicación del sitio para lograr una alta disponibilidad y también implementar un máximo de 3000 Linux VDA en cada ubicación de sitio.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 8 \(CU8\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 7 \(CU7\), parche 1 \(19.12.7001\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 7 \(CU7\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 6 \(CU6\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Cumulative Update 8 (CU8)

May 30, 2024

Fecha de publicación: 11 de septiembre de 2023

### Acerca de esta versión

Cumulative Update 8 (CU8) es la versión más reciente de Linux Virtual Delivery Agent 1912 LTSR. En CU8 se han resuelto varios problemas para mejorar la estabilidad, la seguridad y el rendimiento general.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 7 \(CU7\), parche 1 \(19.12.7001\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 7 \(CU7\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 6 \(CU6\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Cumulative Update 7 (CU7)

July 14, 2023

Fecha de publicación: 15 de marzo de 2023

### Acerca de esta versión

El parche rápido 1 (19.12.7001) de la actualización Cumulative Update 7 (CU7) es la versión más reciente de Linux Virtual Delivery Agent 1912 LTSR. Este parche rápido corrige un [problema](#) notificado desde la publicación de la versión 1912 LTSR CU7.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 7 \(CU7\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 6 \(CU6\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Problemas resueltos en el parche rápido 1 (19.12.7001) de la versión 1912 LTSR CU7

July 14, 2023

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1912 LTSR CU7:

- Esta corrección soluciona un problema de seguridad. Para obtener más información, consulte el artículo [CTX559370](#) de Knowledge Center.

## Problemas resueltos en la versión 1912 LTSR CU7

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1912 LTSR CU6:

- Al conectarse a una sesión de Linux VDA desde un equipo portátil con Microsoft Windows y la acción de cerrar la tapa del equipo portátil se configura en **No hacer nada**, **Hibernar** o **Suspender**, es posible que se inyecten claves aleatorias en la sesión de VDA. [CVADHELP-18438]
- Al conectar ciertos equipos portátiles a un Linux VDA y presionar la tecla **Fn**, es posible que esta funcione como la tecla **Eliminar**. [CVADHELP-21630]

## Cumulative Update 6 (CU6)

November 8, 2022

Fecha de publicación: 31 de octubre de 2022

### Acerca de esta versión

CU6 no contiene problemas resueltos.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Cumulative Update 5 (CU5)

March 11, 2022

Fecha de publicación: 9 de marzo de 2022

## Acerca de esta versión

Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 5 (CU5) corrige dos [problemas](#) notificados desde la publicación de la versión 1912 LTSR CU4.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Problemas resueltos en la versión 1912 LTSR CU5

March 11, 2022

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1912 LTSR CU4:

- Es posible que un escritorio Linux VDA no responda a las entradas del teclado ni del mouse. [CVADHELP-18498]
- Es posible que, al apagar un controlador de dominio en un entorno con varios controladores de dominio, no se puedan iniciar sesiones en Linux VDA. [CVADHELP-18900]

## Cumulative Update 4 (CU4)

January 24, 2022

Fecha de publicación: 03 de noviembre de 2021

## Acerca de esta versión

Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 4 (CU4) corrige tres [problemas](#) notificados desde la publicación de la versión 1912 LTSR CU3.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Problemas resueltos en la versión 1912 LTSR CU4

January 24, 2022

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1912 LTSR CU3:

- En Linux VDA conectado mediante la aplicación Citrix Workspace para Mac o Linux, es posible que, al presionar Mayús + Tab, se registre una doble pulsación de la tecla **Mayús**. [CVADHELP-16831]
- Es posible que no se puedan iniciar sesiones de Linux VDA en RHEL si se utilizan Machine Creation Services para crear máquinas virtuales de Linux en Azure. [CVADHELP-17244]
- Es posible que la desinstalación de Linux VDA en SUSE o RHEL no elimine carpetas vacías de la ubicación /opt/Citrix/. [CVADHELP-18241]

## Cumulative Update 3 (CU3)

January 24, 2022

Fecha de publicación: 12 de mayo de 2021

### Acerca de esta versión

Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 3 (CU3) corrige nueve [problemas](#) notificados desde la publicación de la versión 1912 LTSR CU2.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Problemas resueltos en la versión 1912 LTSR CU3

January 24, 2022

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1912 LTSR CU2:

- Una vez actualizada la versión de Linux VDA de 64 bits, es posible que los usuarios no puedan iniciar aplicaciones. Ven un mensaje que indica que la aplicación se está iniciando y, a continuación, el mensaje desaparece. Como resultado, quedan varias sesiones obsoletas en el VDA. [CVADHELP-15899]
- Después de realizar los análisis, el proceso `ctxmonitorservice` podría cerrarse de manera imprevista con un error SIGABRT. [CVADHELP-15969]
- Es posible que no puedan seleccionarse las opciones de conexión USB PTP (protocolo de transferencia de imágenes) y MTP (protocolo de transferencia de medios) en un teléfono Xiaomi Mi 10. [CVADHELP-16188]
- Cuando desaparece la ventana de Citrix Desktop Viewer (CDViewer.exe), es posible que no se pueda volver a conectar con Linux VDA. [CVADHELP-16239]
- En los Linux VDA, es posible que algunas aplicaciones no reconozcan un dispositivo de cámara web que aparezca en la opción Dispositivo. [CVADHELP-16247]
- Cuando se utiliza la redirección USB con una cámara web en una sesión de Linux VDA, el proceso `ctxusbdsd` podría cerrarse de manera imprevista con un error `segfault`. [CVADHELP-16366]
- Es posible que el proceso `ctxcmd` no se ejecute en el contexto de seguridad correcto de SELinux. [CVADHELP-16381]
- Es posible que haya tarjetas inteligentes que no funcionen cuando están configuradas para Linux VDA. [CVADHELP-16488]
- Es posible que el texto que aparece en las sesiones de Linux VDA se vea distorsionado y borroso. [CVADHELP-17199]

## Cumulative Update 2 (CU2)

January 24, 2022

Fecha de publicación: 19 de noviembre de 2020

### Acerca de esta versión

Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 2 (CU2) corrige cinco [problemas](#) notificados desde la publicación de la versión 1912 LTSR CU1.

[Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 \(CU1\)](#)

[Versión inicial de Linux Virtual Delivery Agent 1912 LTSR](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Problemas resueltos en la versión 1912 LTSR CU2

January 24, 2022

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1912 LTSR CU1:

- Con firmas LDAP habilitadas, puede que los Linux VDA no se registren en el Delivery Controller. [CVADHELP-14481]
- Los intentos de iniciar un VDA pueden dar lugar a una pantalla gris. El problema es resultado de un tiempo de espera de validación agotado para la directiva de usuario HDX. El agotamiento del tiempo de espera puede producirse cuando hay muchos servidores LDAP y uno o más servidores no son accesibles para el VDA. [CVADHELP-14746]
- Es posible que Linux VDA solamente reconozca las **Reglas de redirección de dispositivos USB del cliente**, la primera regla de la configuración de directiva HDX. Las demás reglas se descartan. [CVADHELP-14971]
- Cuando se inicia una aplicación publicada en modo integrado, la aplicación publicada siempre está en la parte superior y aparece sobre las aplicaciones locales. Solo podrá llevar las aplicaciones locales al primer plano cuando minimice la aplicación publicada. [CVADHELP-15134]

- Al iniciar sesión en una máquina virtual Ubuntu creada por Machine Creation Services (MCS), ciertos archivos, como .bashrc y .profile, podrían no copiarse automáticamente en la carpeta particular de la manera prevista. [CVADHELP-15306]
- Con una tarjeta gráfica NVIDIA GRID instalada en un Linux VDA con Ubuntu, puede que la sesión se cierre inesperadamente cuando intente cambiar el tamaño de la sesión. [CVADHELP-15664]
- Cambiar la configuración regional a un idioma que no sea el inglés puede provocar que los contadores de rendimiento no puedan convertir un valor de cadena en un valor numérico y se genere el siguiente error en el registro de VDA.

**[PerfCounter] [Error] SysStat.ReadUpTime: Converting element '29363.68' resulted in a NumberFormatException. Error: Input string was not in a correct format.**

[CVADHELP-15767]

## Cumulative Update 1 (CU1)

November 21, 2020

Fecha de publicación: 7 de mayo de 2020

### Acerca de esta versión

Linux Virtual Delivery Agent 1912 LTSR Cumulative Update 1 (CU1) corrige más de ocho problemas notificados desde la publicación de la versión inicial de 1912 LTSR.

[Linux Virtual Delivery Agent \(versión inicial\)](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Problemas resueltos en la versión 1912 LTSR CU1

January 24, 2022

Se han resuelto estos problemas desde la versión inicial de Linux Virtual Delivery Agent 1912 LTSR:

- Es posible que los Linux VDA no muestren una lista de los usuarios que han iniciado sesión. [CVADHELP-13659]

- 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]
- Los Linux VDA pueden tardar mucho tiempo en inicializarse después de la actualización a la versión 1909 o a la versión 1912. [CVADHELP-13802]
- Los agentes VDA de Linux que utilizan Quest Authentication Services podrían no registrarse con un Delivery Controller. El problema se produce cuando utiliza Linux VDA versión 1909, 1912 LTSR versión inicial y 2003. [CVADHELP-14027]
- Es posible que los agentes Linux VDA no alcancen los fotogramas por segundo que se especifican en el parámetro `Target frame rate` (FramesPerSecond). El problema se produce cuando se instala una GPU en un agente Linux VDA. [CVADHELP-14267]
- Es posible que el servicio `ctxjproxy` no encuentre el servidor LDAP después de reiniciar el sistema. [CVADHELP-14269]
- Es posible que los agentes VDA para Linux no se registren con Delivery Controllers. El problema ocurre cuando no se utiliza el puerto 80 para la comunicación de los agentes VDA para Linux con los Delivery Controllers. [CVADHELP-14270]
- Es posible que los scripts de .NET Core Runtime no se comprueben para autenticación al instalar un agente Linux VDA. [CVADHELP-14424]

## Acerca de esta versión

May 15, 2020

### Novedades

#### Novedades en la versión 1912 LTSR

La versión 1912 de Linux VDA ofrece las siguientes funciones nuevas y mejoradas:

#### MCS disponible en la plataforma AWS

Puede utilizar Machine Creation Services (MCS) para crear máquinas virtuales Linux en la plataforma AWS. Para obtener más información, consulte [Usar MCS para crear máquinas virtuales Linux](#).

## Se puede utilizar un VDA en ejecución como plantilla

Al utilizar MCS para crear máquinas virtuales Linux, puede utilizar un VDA activo como plantilla y heredar todas sus configuraciones existentes. Este VDA en ejecución se puede instalar manualmente o de forma simplificada. Para obtener más información, consulte [Usar MCS para crear máquinas virtuales Linux](#).

## Asignación de unidades del cliente: Para transferencias de archivos grandes

Ahora la asignación de unidades del cliente admite transferencias de archivos de 4 GB o más entre Linux VDA y su dispositivo cliente. Esta mejora requiere que el cliente ejecute la aplicación Citrix Workspace para Windows 1808 o una versión posterior.

### Nota:

Esta versión actualiza la versión de OpenJDK a 1.8.0 en todas las distribuciones compatibles.

## Problemas resueltos en la versión 1912 LTSR

January 24, 2022

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 1909:

- En un monitor 4K, es posible que sufra problemas de rendimiento de la GPU asociados a las pulsaciones de teclas y a la frecuencia de actualización. [CVADHELP-12661]
- Una sesión de Linux VDI 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 el registro de Linux VDA falle cuando se utilizan máquinas virtuales (VM) que solamente emplean direcciones IPv6. [CVADHELP-13103]
- Al establecer una directiva como **Predeterminada**, es posible que Linux VDA no actualice la base de datos. El problema se produce porque las directivas de mayor prioridad no pueden restablecer las directivas de menor prioridad establecidas como **Predeterminadas**. [CVADHELP-13107]
- Con la función de distribución de teclado local habilitada, es posible que la sincronización de la distribución de teclado no funcione en entornos con el cliente en húngaro. Al iniciar una aplicación con **DE** (alemán) como configuración regional, el idioma se sincroniza, pero no funciona para la distribución en húngaro. [CVADHELP-13199]

- Al configurar `Xauthority` para proteger la comunicación entre XClient y XServer, solo se agregan direcciones IPv4. No se agregan direcciones IPv6. [CVADHELP-13255]
- En Ubuntu 18.04, los intentos de crear o actualizar catálogos de máquinas mediante Machine Creation Services (MCS) podrían fallar. [CVADHELP-13178]

## Problemas conocidos

July 14, 2023

Se han identificado los problemas siguientes en esta versión:

- Las aplicaciones publicadas no integradas podrían cerrarse poco después del inicio. El problema se produce después de una actualización de Mutter a una versión posterior a `mutter-3.28.3-4`. Para evitar el problema, use `mutter-3.28.3-4` o anterior. [LNXVDA-6967]
- Linux VDA no funciona como se esperaba cuando se utilizan tarjetas NVIDIA GRID 3D sin habilitar HDX 3D Pro. El problema ocurre en RHEL 7.5 y versiones anteriores, SUSE 12.3 y versiones anteriores, y Ubuntu 16.04. La razón es que varias bibliotecas OpenGL no pueden coexistir en los sistemas gráficos de estas distribuciones Linux.
- Aparece una ventana inesperada durante la descarga de archivos. La ventana no afecta al rendimiento de la descarga de archivos y desaparece automáticamente al cabo de un rato. [LNXVDA-5646]
- La configuración predeterminada de PulseAudio hace que el programa de servidor de sonido se cierre tras 20 segundos de inactividad. Cuando se cierra PulseAudio, el audio no funciona. Para solucionar este problema, establezca el tiempo de inactividad (`exit-idle-time`) en `-1` en el archivo `/etc/pulse/daemon.conf`. [LNXVDA-5464]
- Con `libtcmalloc` 4.3.0 en SUSE 12.3, los procesos se pueden cerrar de manera imprevista.
- El servicio `ctxhdx` puede cerrarse inesperadamente en agentes VDA con Ubuntu 16.04 y SUSE 12.3. Este problema ocurre con GNU C Library (`glibc`) de la versión 2.22 a la versión 2.24. El problema se corrige en `glibc` 2.25. Si utiliza la distribución SUSE 12.3, puede instalar el parche que SUSE proporciona para solucionar el problema. No hay solución disponible para Ubuntu 16.04 en el momento de publicación de Linux VDA 7.17. [LNXVDA-4481]
- No se pueden iniciar sesiones en la aplicación Citrix Workspace para Linux cuando el cifrado SSL está habilitado y la fiabilidad de la sesión está inhabilitada. [RFLNX-1557]

- 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 la aplicación Citrix Workspace para Android se podría invertir durante la itinerancia de la sesión. Es posible que se pierda el estado Bloq Mayús cuando se mueve la conexión a Citrix Workspace 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 la aplicación Citrix Workspace para Mac. De forma predeterminada, la aplicación Citrix Workspace 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 Workspace, 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:

```
1 klist -li 0x3e4 purge
2 <!--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 la aplicación Citrix Workspace para Windows durante la grabación de sonido.

## Avisos legales de terceros

December 12, 2022

[Linux Virtual Delivery Agent 1912 LTSR](#) (descarga en PDF)

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

## Elementos retirados

November 3, 2021

Los siguientes anuncios tienen por objeto avisarle por adelantado acerca de las plataformas, los productos y las funciones de Citrix que se están retirando progresivamente, de modo que pueda tomar a tiempo las decisiones empresariales pertinentes. Citrix examina el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas.

Para obtener información detallada acerca del ciclo de vida útil admitido del producto, consulte el artículo [Política de soporte técnico de la vida útil del producto](#).

## Elementos eliminados y obsoletos

En la siguiente tabla, se muestran las plataformas, las funciones y los productos Citrix que se han retirado o eliminado. Los elementos

**obsoletos** no se eliminan inmediatamente. Citrix sigue ofreciéndolos en la presente versión, pero se quitarán en una versión Current Release futura.

**Los elementos eliminados** se quitan o ya no se ofrecen o admiten en Linux VDA.

Elemento	Retirada anunciada en	Eliminado en
Se admite en RHEL 6.9	1909	1909
Se admite en RHEL 7.5, CentOS 7.5	1903	1903
Se admite en RHEL 7.4, CentOS 7.4	1811	1811
Se admite en RHEL 6.8	1811	1811
Se admite en RHEL 7.3, CentOS 7.3	7.18	7.18
Se admite en RHEL 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

## Requisitos del sistema

January 24, 2022

### Distribuciones de Linux

**Nota:**

Aquellos componentes de los requisitos del sistema que no se incluyen aquí (por ejemplo, la aplicación Citrix Workspace y Citrix Provisioning) se describen en su documentación respectiva.

A partir de la versión CU3, instale .NET Core Runtime 3.1 como requisito previo antes de poder instalar Linux VDA. Para obtener más información, consulte <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Linux VDA no admite el cifrado SecureICA. Al habilitar SecureICA en Linux VDA, se produce un error en el inicio de la sesión.

Para obtener información sobre cómo utilizar una versión Current Release (CR) en un entorno Long Term Service (LTSR) y sobre otras preguntas frecuentes, consulte el [artículo de Knowledge Center](#).

Linux VDA admite las siguientes distribuciones de Linux:

**Importante:**

Cuando caduque el desarrollo por parte del proveedor del sistema operativo, Citrix podría ver limitada su capacidad para solucionar problemas.

Para plataformas obsoletas o eliminadas, consulte [Elementos retirados](#).

- SUSE Linux Enterprise:
  - Desktop 12 Service Pack 3
  - Server 12 Service Pack 3
- Red Hat Enterprise Linux
  - Workstation 7.7
  - Workstation 6.10
  - Server 7.7
  - Server 6.10
- CentOS Linux
  - CentOS 7.7
  - CentOS 6.10
- Ubuntu Linux
  - Ubuntu Desktop 18.04
  - Ubuntu Server 18.04
  - Ubuntu Live Server 18.04
  - Ubuntu Desktop 16.04
  - Ubuntu Server 16.04
- Pardus Linux
  - Pardus 17 (Para obtener información sobre el ámbito de funciones que se admite, consulte el artículo [CTX238492](#) de Knowledge Center).

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 7.7, CentOS 7.7	1.20
RHEL 6.10, CentOS 6.10	1.17

Distribución de Linux	Versión de Xorg
Ubuntu 18.04	1.19
Ubuntu 16.04	1.18
SUSE 12.3	1.18
Pardus 17	1.19

---

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:**

- Si instala Linux VDA 1912 LTSR Cumulative Update 2 (CU2) en CentOS 7.4 y quiere usarlo con Citrix Virtual Apps and Desktops Service, debe instalar estos componentes antes del VDA:
  - Xorg 1.20.4
  - SELinux policy 3.13.1-268
  - .NET Core Runtime 2.1
  - GNOME 3.28.3 or later
- Los escritorios Gnome y KDE son compatibles en SUSE, RHEL y CentOS. El escritorio Unity es compatible con Ubuntu 16.04. El escritorio Gnome es compatible con Ubuntu 18.04. Debe instalarse al menos un escritorio.

## Citrix Virtual Desktops

El VDA de Linux es compatible con todas las versiones actualmente admitidas de Citrix Virtual Desktops. Para obtener información sobre la vida útil de los productos Citrix Virtual Desktops y determinar cuándo deja Citrix de desarrollar 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.

## Plataformas de host y entornos de virtualización compatibles

- Servidores bare metal
- Citrix Hypervisor
- VMware ESX y ESXi

- Microsoft Hyper-V
- Nutanix AHV
- Microsoft Azure Resource Manager
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

**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 o paquetes de integración de Active Directory:

- Samba Winbind
- Quest Authentication Services 4.1 o una versión posterior
- Centrify DirectControl
- SSSD
- PBIS (compatible con RHEL 7 y Ubuntu)

**Sugerencia:**

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

## HDX 3D Pro

Las prestaciones de HDX 3D Pro de Citrix Virtual Apps and Desktops le permiten entregar escritorios y aplicaciones que rinden más gracias a una unidad de procesamiento de gráficos (GPU) para la aceleración de hardware.

## Hipervisores

Para Linux VDA, HDX 3D Pro es compatible con las tecnologías PassThrough de GPU y virtualización de GPU que ofrecen estos hipervisores:

- Citrix Hypervisor
- VMware ESX y ESXi
- Nutanix AHV

**Nota** Los hipervisores son compatibles con algunas distribuciones de Linux.

## GPU

Para saber qué tarjetas GPU de NVIDIA admite su distribución de Linux, vaya a la [tabla de compatibilidad con productos NVIDIA](#) y consulte las columnas **Hypervisor or Bare-Metal OS, Software Product Deployment, Hardware Supported** y **Guest OS Support**. Asegúrese de instalar el controlador de vGPU más reciente para la tarjeta GPU. Para obtener más información, consulte [NVIDIA Virtual GPU Software Supported GPUs](#).

Estas son las tarjetas GPU que hemos probado para la compatibilidad con la virtualización y PassThrough de GPU.

GPU que hemos probado para PassThrough de GPU:

- NVIDIA GRID: Tesla T4
- NVIDIA GTX750Ti
- NVIDIA GRID: Tesla M60
- NVIDIA GRID: K2
- NVIDIA GRID: Tesla P40
- NVIDIA GRID: Tesla P4
- NVIDIA GRID: Tesla P100

GPU que hemos probado para vGPU:

- NVIDIA GRID: Tesla T4
- NVIDIA GRID: Tesla V100
- NVIDIA GRID: Tesla M60
- NVIDIA GRID: Tesla M10
- NVIDIA GRID: Tesla P40
- NVIDIA GRID: Tesla P4
- NVIDIA GRID: Tesla P100

## Información general de la instalación

September 30, 2021

Esta sección le guía a través de los siguientes procedimientos:

- Instalación rápida con Easy Install (recomendado para instalaciones nuevas)
- Instalación manual conforme a diversas distribuciones de Linux
- Usar MCS para crear máquinas virtuales Linux
- Configurar Delivery Controllers para XenDesktop 7.6 y versiones anteriores

## Instalación rápida con Easy Install (recomendado)

March 9, 2023

### Importante:

Para instalaciones nuevas, le recomendamos que consulte este artículo para una instalación rápida. En este artículo, se describe cómo instalar y configurar Linux VDA con Easy Install. Easy Install ahorra tiempo y trabajo y es menos propenso a errores que la instalación manual. Así, le ayuda a configurar un 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	PBIS
RHEL 7.7	Sí	Sí	Sí	Sí
RHEL 6.10	Sí	Sí	Sí	No
CentOS 7.7	Sí	Sí	Sí	Sí
CentOS 6.10	Sí	Sí	Sí	No
Ubuntu 18.04	Sí	Sí	Sí	Sí
Ubuntu 16.04	Sí	Sí	Sí	Sí
SUSE 12.3	Sí	No	Sí	No

---

### 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 de descargas de Citrix Virtual Apps and Desktops](#). Expanda la versión adecuada de Citrix Virtual Apps and Desktops. Haga clic en **Componentes** para descargar el paquete Linux VDA que coincida con 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
- Nombre de dominio completo (FQDN) del dominio

### 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.

## Consideraciones

- El nombre de grupo de trabajo es, de forma predeterminada, el nombre de dominio. 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 y guarde los cambios.
- 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.

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

- a. Abra **Herramientas administrativas** en el controlador del dominio.
  - b. Seleccione **Sitios y servicios de Active Directory**.
  - c. Agregue una dirección de subred adecuada para **Subredes**.
- Easy Install admite IPv6 puro a partir de Linux VDA 7.16. Se aplican las siguientes condiciones previas y limitaciones:

- Debe configurar el repositorio de Linux para que la máquina pueda descargar los paquetes requeridos en redes de IPv6 puro.
- Centrifly no se admite en redes únicamente de IPv6.

**Nota:**

Si la red es solo de IPv6 y todas las entradas tienen el formato adecuado de IPv6, el VDA se registra en el Delivery Controller a través de IPv6. Si la red tiene una combinación híbrida de IPv4 e IPv6, el tipo de la primera dirección IP de DNS determina si se usa IPv4 o IPv6 para el registro.

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

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

RHEL: `wget http://edge.centrifly.com/products/centrifly-suite/2016-update-1/installers/centrifly-suite-2016.1-rhel4-x86\_64.tgz?\_ga=1.178323680.558673738.1478847956`

CentOS: `wget http://edge.centrifly.com/products/centrifly-suite/2016-update-1/installers/centrifly-suite-2016.1-rhel4-x86\_64.tgz?\_ga=1.186648044.558673738.1478847956`

SUSE: `wget http://edge.centrifly.com/products/centrifly-suite/2016-update-1/installers/centrifly-suite-2016.1-suse10-x86\_64.tgz?\_ga=1.10831088.558673738.1478847956`

Ubuntu: `wget http://edge.centrifly.com/products/centrifly-suite/2016-update-1/installers/centrifly-suite-2016.1-deb7-x86\_64.tgz?\_ga=1.178323680.558673738.1478847956`

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

```

1 cat /tmp/ctxinstall.conf
2 set "centrifypkgpath=/home/mydir"
3 ls -ls /home/mydir
4 9548 -r-xr-xr-x. 1 root root 9776688 May 13 2016
   adcheck-rhel4-x86_64
5 4140 -r--r--r--. 1 root root 4236714 Apr 21 2016
   centriflyda-3.3.1-rhel4-x86_64.rpm
6 33492 -r--r--r--. 1 root root 34292673 May 13 2016
   centriflydc-5.3.1-rhel4-x86_64.rpm
7 4 -rw-rw-r--. 1 root root 1168 Dec 1 2015
   centriflydc-install.cfg
8 756 -r--r--r--. 1 root root 770991 May 13 2016
   centriflydc-ldaproxy-5.3.1-rhel4-x86_64.rpm

```

```

 9      268 -r--r--r--. 1 root root    271296 May 13  2016
centrifdc-nis-5.3.1-rhel4-x86_64.rpm
10     1888 -r--r--r--. 1 root root    1930084 Apr 12  2016
centrifdc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
11     124 -rw-rw-r--. 1 root root    124543 Apr 19  2016
centrifdc-suite.cfg
12      0 lrwxrwxrwx. 1 root root         10 Jul  9  2012 install-
express.sh -> install.sh
13     332 -r-xr-xr--. 1 root root    338292 Apr 10  2016 install
.sh
14      12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-
notes-agent-rhel4-x86_64.txt
15      4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-
notes-da-rhel4-x86_64.txt
16      4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-
notes-nis-rhel4-x86_64.txt
17      12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-
notes-openssh-rhel4-x86_64.txt
18 <!--NeedCopy-->

```

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

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

RHEL 7 / CentOS 7: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86\_64.rpm.sh`

Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86\_64.deb.sh`

- Obtenga una versión específica del paquete PBIS desde Internet. Para ello, cambie la línea “`pbisDownloadPath`” del archivo `/opt/Citrix/VDA/sbin/ctxinstall.sh` para designar la dirección URL del paquete PBIS.

La siguiente captura de pantalla le sirve de ejemplo:

## 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 Hypervisor

Si está habilitada la funcionalidad de sincronización horaria de Citrix Hypervisor, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como Citrix Hypervisor in-

tentarán 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 Citrix VM Tools instalado, puede comprobar si la función de sincronización horaria de Citrix Hypervisor está presente y habilitarla en la máquina virtual de Linux:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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, inhabilita la función de sincronización horaria con un 1 en el archivo:

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor 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: Instale .NET Core Runtime como requisito previo

Antes de instalar Linux VDA, instale .NET Core Runtime conforme a las instrucciones de <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

- Para la versión inicial de 1912 LTSR, CU1 y CU2, instale .NET Core Runtime 2.1.
- Para CU3 y versiones posteriores, instale .NET Core Runtime 3.1.

Después de instalar .NET Core Runtime, ejecute el comando `which dotnet` para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de runtime de .NET Core. Por ejemplo, si el resultado del comando es `/aa/bb/dotnet`, use `/aa/bb` como ruta binaria de .NET.

## Paso 4: Descargue el paquete de Linux VDA

Vaya a la [página de descargas de Citrix Virtual Apps and Desktops](#). Expanda la versión correcta de Citrix Virtual Apps and Desktops y haga clic en **Componentes** para descargar el paquete Linux VDA correspondiente a su distribución Linux.

## Paso 5: Instale el paquete de Linux VDA

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

Para distribuciones RHEL y CentOS:

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

Para distribuciones Ubuntu:

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

Para las distribuciones SUSE:

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

## Paso 6: Instale controladores NVIDIA GRID

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

Para instalar y configurar el administrador de GPU virtual de NVIDIA GRID (el controlador de hosts) en los hipervisores específicos, consulte estas guías:

- [Citrix Hypervisor](#)
- [VMware ESX](#)

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

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

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

### Nota:

Antes de configurar el entorno en tiempo de ejecución, asegúrese de que la configuración regional `en_US.UTF-8` se ha instalado en el sistema operativo. Si la configuración regional no está disponible en su sistema operativo, ejecute el comando `sudo locale-gen en_US.UTF-8`.

Después de instalar el paquete de Linux VDA, configure el entorno de ejecución mediante el script `ctxinstall.sh`. Puede ejecutar el script en modo interactivo o en modo silencioso.

### Nota:

Puede parecer que Easy Install no responde mientras descarga .NET Core Runtime, que tiene más de 27 MB de tamaño. Consulte `/var/log/ctxinstall.log` para ver el progreso de descarga.

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

```
1 sudo /opt/Citrix/VDA/sbin/ctxinstall.sh
2 <!--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 | pbis:** Indica el método de integración de Active Directory.
- **CTX\_EASYINSTALL\_USERNAME=domain-user-name:** Indica el nombre del usuario de dominio; se utiliza para unirse al dominio.
- **CTX\_EASYINSTALL\_PASSWORD=password:** Indica la contraseña del usuario de dominio; se utiliza para unirse al dominio.

El script `ctxsetup.sh` utiliza las siguientes variables:

- **CTX\_XDL\_SUPPORT\_DDC\_AS\_CNAME=Y | N:** 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 VDA se inician después del arranque de la máquina.
- **CTX\_XDL\_ADD\_FIREWALL\_RULES=Y | N**: Los servicios de Linux VDA requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema de Linux VDA.
- **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, establézcalo 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 los puertos de LDAP. Por ejemplo, ad1.miempresa.com:389. Si no es necesario, establézcalo 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\_FAS\_LIST='list-fas-servers'**: Los servidores del Servicio de autenticación federada (FAS) se configuran a través de la directiva de grupo de AD. Linux VDA no admite las directivas de grupo de AD, pero usted puede suministrar una lista de servidores FAS, separados por punto y coma. La secuencia debe ser la misma que la configurada en la directiva de grupo de AD. Si alguna dirección de servidor está eliminada, complete el espacio en blanco correspondiente con la cadena de texto **<none>** y no cambie el orden de las direcciones de servidor.
- **CTX\_XDL\_DOTNET\_RUNTIME\_PATH=path-to-install-dotnet-runtime**: La ruta de instalación de .NET Core Runtime para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es `/usr/bin`.

- **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. Cuando todos los parámetros ya están configurados mediante las variables de entorno, el script `ctxinstall.sh` sigue solicitando la entrada manual por parte del usuario de la ruta de instalación de .NET Core Runtime.

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

```
1 export CTX_EASYINSTALL_HOSTNAME=host-name
2
3 export CTX_EASYINSTALL_DNS=ip-address-of-dns
4
5 export CTX_EASYINSTALL_NTFS=address-of-ntfs
6
7 export CTX_EASYINSTALL_DOMAIN=domain-name
8
9 export CTX_EASYINSTALL_REALM=realm-name
10
11 export CTX_EASYINSTALL_FQDN=ad-fqdn-name
12
13 export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify |
    pbis
14
15 export CTX_EASYINSTALL_USERNAME=domain-user-name
16
17 export CTX_EASYINSTALL_PASSWORD=password
18
19 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
20
21 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
22
23 export CTX_XDL_VDA_PORT=port-number
24
25 export CTX_XDL_REGISTER_SERVICE=Y | N
26
27 export CTX_XDL_ADD_FIREWALL_RULES=Y | N
28
29 export CTX_XDL_HDX_3D_PRO=Y | N
30
31 export CTX_XDL_VDI_MODE=Y | N
32
33 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
34
35 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
36
37 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
38
39 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
40
```

```
41 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
42
43 export CTX_XDL_START_SERVICE=Y | N
44
45 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
46 <!--NeedCopy-->
```

Cuando ejecute el comando `sudo`, escriba la opción `-E` para pasar las variables de entorno existentes al nuevo shell que se crea. Se 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:

```
1 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_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--NeedCopy-->
```

## Paso 8: Ejecute XDPing

Proporcionamos una utilidad de línea de comandos, la herramienta Linux XDPing, para comprobar la presencia de problemas de configuración comunes en un entorno Linux VDA. Puede instalar el paquete XDPing en cualquier máquina que ejecute una distribución Linux compatible. XDPing no requiere que el paquete Linux VDA esté instalado en el equipo. Para obtener más información acerca de

la herramienta, consulte el artículo [CTX202015](#) de Knowledge Center.

## Paso 9: Ejecute Linux VDA

### Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

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

### Detener Linux VDA:

Para detener los servicios de Linux VDA:

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

#### Nota:

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

### Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

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

### Comprobar el estado de Linux VDA:

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

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

## Paso 10: Cree el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops

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 **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios VDI dedicados.
- 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 11: Cree el grupo de entrega en Citrix Virtual Apps y Citrix Virtual Desktops

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:

- 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.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte [Citrix Virtual Apps and Desktops 7 1912 LTSR](#).

## 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:

```
1 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)'.
2 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))
3 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')
4 Check the following:- The system clock is in sync between this machine
  and the delivery controller.
5 - The Active Directory provider (e.g. winbind daemon) service is
  running and correctly configured.
6 - Kerberos is correctly configured on this machine.
7 If the problem persists, please refer to Citrix Knowledge Base article
  CTX117248 for further information.
8 Error Details:
9 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'.
```

```
10 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.  
11 Ensure that the system clock is in sync between this machine and the  
    delivery controller.  
12 Verify the NTP daemon is running on this machine and is correctly  
    configured.  
13 2016-11-04 02:11:52.364 [ERROR] - Could not register with any  
    controllers. Waiting to try again in 120000 ms. Multi-forest - false  
14 2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to  
    register with any controllers in the last 470 minutes.  
15 <!--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 inicia una sesión, que luego se bloquea en un escritorio vacío. Además, la consola de la máquina 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`

### Los intentos de iniciar sesiones de escritorio en Ubuntu fallan porque falta el directorio home

/var/log/xdl/hdx.log:

```

1 2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
    failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)
2
3 2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
    Session started for user ctxadmin.
4
5 2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
    Login Process died: normal.
6
7 2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting
    normally.
8 <!--NeedCopy-->

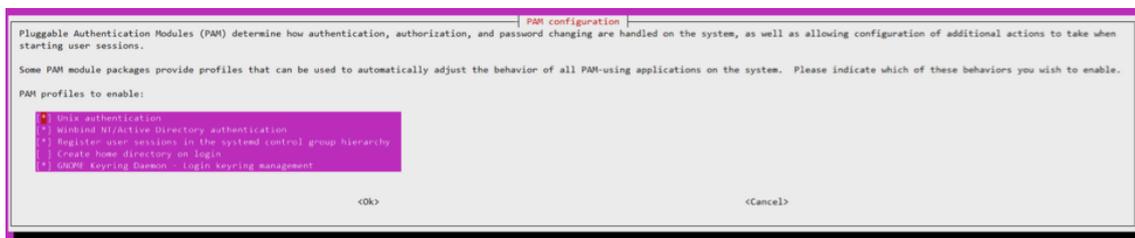
```

**Sugerencia:**

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 el cuadro de diálogo resultante, compruebe si **Create home directory on login** está seleccionado.

**La sesión no se inicia o finaliza rápidamente con el error dbus**

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

```

1 Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
    CITRIXLAB\ctxadmin.
2
3 Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
    ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0
4
5 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...
6

```

```
7 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)
8
9 Oct 27 04:17:18 CentOS7 gnome-session: aborting...
10
11 Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.
12
13 Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
  CITRIXLAB\ctxadmin.
14 <!--NeedCopy-->
```

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

```
1 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
  Stale PID file, overwriting.
2
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, se 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 manualmente

June 17, 2022

### Importante:

Para instalaciones nuevas, se recomienda usar [Easy Install](#) para una instalación rápida. Easy Install ahorra tiempo y esfuerzo, y es menos propenso a errores que la instalación manual descrita en este artículo.

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

#### Paso 1a: Verifique la configuración de red

Compruebe que la red esté conectada y correctamente configurada. Por ejemplo, debe configurar el servidor DNS en el Linux VDA.

#### Paso 1b: Establezca el nombre de host

Para que se notifique correctamente el nombre de host de la máquina, cambie el archivo **/etc/hostname** (para RHEL 7 y CentOS 7) o el archivo **/etc/sysconfig/network** (para RHEL 6 y CentOS 6) para que contenga solamente 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 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.

**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:

```
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 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:

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--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:

```
1 server peer1-fqdn-or-ip-address iburst
2
3 server peer2-fqdn-or-ip-address iburst
4 <!--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:

```
1 sudo /sbin/service ntpd restart
2 <!--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:

```
1 server peer1-fqdn-or-ip-address iburst
2
3 server peer2-fqdn-or-ip-address iburst
4 <!--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:

```
1 sudo /sbin/service chronyd restart
2 <!--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:

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

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

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

Abra un nuevo shell y compruebe la versión de Java:

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

#### Sugerencia:

Para evitar errores de registro con el Delivery Controller, compruebe que solo ha instalado OpenJDK 1.8.0. Quite todas las demás versiones de Java que haya presentes 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:

```
1 sudo yum -y install postgresql-server
2
3 sudo yum -y install postgresql-jdbc
4 <!--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 9:

- Solo RHEL 7: PostgreSQL 9

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

- Solo RHEL 6: PostgreSQL 8

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

### Paso 1i: Inicie PostgreSQL

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

- Solo RHEL 7: PostgreSQL 9

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

- Solo RHEL 6: PostgreSQL 8

```
1 sudo /sbin/chkconfig postgresql on
2
3 sudo /sbin/service postgresql start
4 <!--NeedCopy-->
```

Compruebe la versión de PostgreSQL con:

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

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

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

#### Importante:

En esta versión, se ha agregado una dependencia nueva para `gperftools-libs`, pero no existe en el repositorio original. Agregue el repositorio 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 Hypervisor

Si está habilitada la funcionalidad de sincronización horaria de Citrix Hypervisor, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como Citrix Hypervisor 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 Citrix VM Tools instalado, puede comprobar si la función de sincronización horaria de Citrix Hypervisor está presente y habilitarla en la máquina virtual de Linux:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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:

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor 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](#)

- [Quest Authentication Services](#)
- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#) (compatible solo con RHEL 7)

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:

```
1 sudo yum -y install samba-winbind samba-winbind-clients krb5-  
   workstation authconfig oddjob-mkhomedir  
2 <!--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:

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

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

```
1 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  
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
```

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 tiquets 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-->
```

#### Sugerencia:

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 keytab del sistema se haya creado y contenga 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:

```
1 wbinfo --krb5auth=domain\username%password
2 <!--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 comprobar que el módulo Winbind PAM está configurado correctamente, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--NeedCopy-->
```

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

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

Salga de la sesión.

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

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## Quest Authentication Services

**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:

```
1 reboot
2 <!--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.

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
   interval 32400
2
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
   auth false
4 <!--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:

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

**Unirse al dominio de Windows** Una la máquina Linux al dominio de Active Directory mediante el comando `vastool` de Quest:

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
2 <!--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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 comprobar que Quest puede autenticar usuarios de dominio a través de PAM, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--NeedCopy-->
```

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

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

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

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

Salga de la sesión.

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

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el [Paso 6: 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:

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--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:

```
1 su -
2 adinfo
3 <!--NeedCopy-->
```

Verifique 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:

```
1 adinfo --sysinfo all
2 adinfo -diag
3 <!--NeedCopy-->
```

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

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

Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## 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
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 al seguir las instrucciones de este artículo:

- RHEL 7.7 y versiones posteriores
- CentOS 7.7 y versiones posteriores

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

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

Instale o actualice los paquetes requeridos:

```
1 sudo yum -y install krb5-workstation authconfig oddjob-mkhomedir samba-  
   common-tools  
2 <!--NeedCopy-->
```

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 corto Net-BIOS 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:

```
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 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):

```
1 [sssd]
2 config_file_version = 2
3 domains = ad.example.com
4 services = nss, pam
5
6 [domain/ad.example.com]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9
10 id_provider = ad
11 auth_provider = ad
12 access_provider = ad
13 ldap_id_mapping = true
```

```

14 ldap_schema = ad
15
16 # Should be specified as the lower-case version of the long version of
    the Active Directory domain.
17 ad_domain = ad.example.com
18
19 # Kerberos settings
20 krb5_ccachedir = /tmp
21 krb5_ccname_template = FILE:%d/krb5cc_%U
22
23 # Uncomment if service discovery is not working
24 # ad_server = server.ad.example.com
25
26 # Comment out if the users have the shell and home dir set on the AD
    side
27 default_shell = /bin/bash
28 fallback_homedir = /home/%d/%u
29
30 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
    available
31 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
32 <!--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/sss/sss.conf
chmod 0600 /etc/sss/sss.conf
restorecon /etc/sss/sss.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:

```

1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo service sssd start
4
5 sudo chkconfig sssd on
6 <!--NeedCopy-->

```

**Verificar la configuración de Kerberos** Compruebe que el archivo **keytab** del sistema se haya creado y contenga 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-->
```

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

```
1 sudo getent passwd DOMAIN\username
2 <!--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 comprobar que el módulo SSSD PAM está configurado correctamente, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 sudo ssh localhost -l DOMAIN\username
2
3 id -u
4 <!--NeedCopy-->
```

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

```
1 ls /tmp/krb5cc_{
2 uid }
3
4 <!--NeedCopy-->
```

Compruebe que los tiquets que se encuentran en la memoria caché de credenciales de Kerberos que pertenece al usuario son válidos y no han caducado.

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

Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## PBIS

**Descargar el paquete PBIS requerido** Por ejemplo:

```
1 wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/
  pbis-open-8.8.0.506.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

**Convertir el script de instalación de PBIS en ejecutable** Por ejemplo:

```
1 chmod +x pbis-open-8.8.0.506.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

**Ejecutar el script de instalación de PBIS** Por ejemplo:

```
1 sh pbis-open-8.8.0.506.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

**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 /opt/pbis/bin/domainjoin-cli join domain-name user
2 <!--NeedCopy-->
```

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

**Nota:** Para establecer Bash como el shell predeterminado, ejecute el comando **/opt/pbis/bin/config LoginShellTemplate/bin/bash**.

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

```
1 /opt/pbis/bin/domainjoin-cli query
2 <!--NeedCopy-->
```

Si la máquina está unida a un dominio, este comando devuelve la información sobre el dominio de AD y la unidad organizativa a los que está unida actualmente. De lo contrario, solo aparece el nombre de host.

**Verificar la autenticación de usuario** Para comprobar que PBIS puede autenticar usuarios de dominio a través de PAM, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\user
2
3 id -u
4 <!--NeedCopy-->
```

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

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

Salga de la sesión.

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

Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

#### **Paso 4: Instale .NET Core Runtime como requisito previo**

Antes de instalar Linux VDA, instale .NET Core Runtime conforme a las instrucciones de <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

- Para la versión inicial de 1912 LTSR, CU1 y CU2, instale .NET Core Runtime 2.1.
- Para CU3 y versiones posteriores, instale .NET Core Runtime 3.1.

Después de instalar .NET Core Runtime, ejecute el comando `which dotnet` para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de runtime de .NET Core. Por ejemplo, si el resultado del comando es `/aa/bb/dotnet`, use `/aa/bb` como ruta binaria de .NET.

## Paso 5: Descargue el paquete de Linux VDA

Vaya a la [página de descargas de Citrix Virtual Apps and Desktops](#). Expanda la versión correcta de Citrix Virtual Apps and Desktops y haga clic en **Componentes** para descargar el paquete Linux VDA correspondiente a su distribución Linux.

## Paso 6: Instale Linux VDA

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

### Para llevar a cabo una nueva instalación

#### 1. (Opcional) Desinstalación de 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.

##### a) Detenga los servicios de Linux VDA:

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

#### Nota:

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

##### b) Desinstale el paquete:

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

#### Nota:

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.

#### 2. Instalación de Linux VDA

- Instale el software de Linux VDA mediante Yum:

**Para RHEL 7/CentOS 7:**

```
1 sudo yum install -y XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.  
rpm  
2 <!--NeedCopy-->
```

**Para RHEL 6/CentOS 6:**

```
1 sudo yum install -y XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.  
rpm  
2 <!--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:**

```
1 sudo rpm -i XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm  
2 <!--NeedCopy-->
```

**Para RHEL 6/CentOS 6:**

```
1 sudo rpm -i XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm  
2 <!--NeedCopy-->
```

**Lista de dependencias RPM para RHEL 7/CentOS 7:**

```
1 postgresql-server >= 9.2  
2  
3 postgresql-jdbc >= 9.2  
4  
5 java-1.8.0-openjdk >= 1.8.0  
6  
7 ImageMagick >= 6.7.8.9  
8  
9 firewalld >= 0.3.9  
10  
11 policycoreutils-python >= 2.0.83  
12  
13 dbus >= 1.6.12  
14  
15 dbus-x11 >= 1.6.12  
16  
17 xorg-x11-server-utils >= 7.7  
18  
19 xorg-x11-xinit >= 1.3.2  
20  
21 libXpm >= 3.5.10  
22  
23 libXrandr >= 1.4.1  
24
```

```
25 libXtst >= 1.2.2
26
27 motif >= 2.3.4
28
29 pam >= 1.1.8
30
31 util-linux >= 2.23.2
32
33 bash >= 4.2
34
35 findutils >= 4.5
36
37 gawk >= 4.0
38
39 sed >= 4.2
40
41 cups >= 1.6.0
42
43 foomatic-filters >= 4.0.9
44
45 openldap >= 2.4
46
47 cyrus-sasl >= 2.1
48
49 cyrus-sasl-gssapi >= 2.1
50
51 libxml2 >= 2.9
52
53 python-requests >= 2.6.0
54
55 gperftools-libs >= 2.4
56
57 rpmlib(FileDigests) <= 4.6.0-1
58
59 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
60
61 rpmlib(CompressedFileNames) <= 3.0.4-1
62
63 rpmlib(PayloadIsXz) <= 5.2-1
64 <!--NeedCopy-->
```

**Nota** Para ver una matriz de las distribuciones de Linux y las versiones de Xorg que admite esta versión de Linux VDA, consulte los [requisitos del sistema](#).

#### Lista de dependencias RPM para RHEL 6/CentOS 6:

```
1 postgresql-jdbc >= 8.4
2
3 postgresql-server >= 8.4
4
5 java-1.8.0-openjdk >= 1.8.0
6
7 ImageMagick >= 6.5.4.7
```

```
8
9  GConf2 >= 2.28.0
10
11  system-config-firewall-base >= 1.2.27
12
13  polycoreutils-python >= 2.0.83
14
15  xorg-x11-server-utils >= 7.7
16
17  xorg-x11-xinit >= 1.0.9
18
19  ConsoleKit >= 0.4.1
20
21  dbus >= 1.2.24
22
23  dbus-x11 >= 1.2.24
24
25  libXpm >= 3.5.10
26
27  libXrandr >= 1.4.1
28
29  libXtst >= 1.2.2
30
31  openmotif >= 2.3.3
32
33  pam >= 1.1.1
34
35  util-linux-ng >= 2.17.2
36
37  bash >= 4.1
38
39  findutils >= 4.4
40
41  gawk >= 3.1
42
43  sed >= 4.2
44
45  cups >= 1.4.0
46
47  foomatic >= 4.0.0
48
49  openldap >= 2.4
50
51  cyrus-sasl >= 2.1
52
53  cyrus-sasl-gssapi >= 2.1
54
55  libxml2 >= 2.7
56
57  python-requests >= 2.6.0
58
59  gperftools-libs >= 2.0
60
```

```
61  rpmlib(FileDigests) <= 4.6.0-1
62
63  rpmlib(PayloadFilesHavePrefix) <= 4.0-1
64
65  rpmlib(CompressedFileNames) <= 3.0.4-1
66
67  rpmlib(PayloadIsXz) <= 5.2-1
68  <!--NeedCopy-->
```

**Nota:**

Después de instalar Linux VDA en RHEL 7.x, ejecute el comando `sudo yum install -y python-websockify x11vnc`. El objetivo es instalar `python-websockify` y `x11vnc` manualmente para utilizar la función de remedo de sesiones. Para obtener más información, consulte [Remedar sesiones](#).

**Para actualizar una instalación existente**

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

- Para actualizar el software con Yum:

**Para RHEL 7/CentOS 7:**

```
1  sudo yum install -y XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm
2  <!--NeedCopy-->
```

**Para RHEL 6/CentOS 6:**

```
1  sudo yum install -y XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm
2  <!--NeedCopy-->
```

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

**Para RHEL 7/CentOS 7:**

```
1  sudo rpm -U XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm
2  <!--NeedCopy-->
```

**Para RHEL 6/CentOS 6:**

```
1  sudo rpm -U XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm
2  <!--NeedCopy-->
```

**Importante:**

Reinicie la máquina Linux VDA después de actualizar el software.

## Paso 7: Instale controladores NVIDIA GRID

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

Para instalar y configurar el administrador de GPU virtual de NVIDIA GRID (el controlador de hosts) en los hipervisores específicos, consulte estas guías:

- [Citrix Hypervisor](#)
- [VMware ESX](#)

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

1. Asegúrese de que la máquina virtual invitada esté apagada.
2. En XenCenter, asigne una GPU a la VM.
3. Inicie la VM.
4. Prepare la VM para el controlador de NVIDIA GRID:

```
1 yum install gcc
2
3 yum install "kernel-devel-$(uname -r)"
4
5 systemctl set-default multi-user.target
6 <!--NeedCopy-->
```

5. 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 |                    |
| 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 8: 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 | 5:** 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 –Quest Authentication Services
  - 3 –Centrify DirectControl
  - 4 –SSSD
  - 5 –PBIS
- **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, 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\_FAS\_LIST='list-fas-servers'**: Los servidores del Servicio de autenticación federada (FAS) se configuran a través de la directiva de grupo de AD. Como Linux VDA no admite las directivas de grupo de AD, en su lugar, se puede suministrar una lista de servidores FAS, separados por punto y coma. La secuencia debe ser la misma que la configurada en la directiva de grupo de AD. Si alguna dirección de servidor está eliminada, complete el espacio en blanco correspondiente con la cadena de texto **<none>** y no cambie la secuencia de las direcciones de servidor.
- **CTX\_XDL\_DOTNET\_RUNTIME\_PATH=path-to-install-dotnet-runtime**: La ruta de instalación de .NET Core Runtime para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es `/usr/bin`.
- **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:

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
20
```

```
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_START_SERVICE=Y|N
28
29 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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:

```
1 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|5 \
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_FAS_LIST= ' list-fas-servers ' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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.

## Paso 9: Ejecute XDPing

Proporcionamos una utilidad de línea de comandos, la herramienta **XDPing** de Linux, para comprobar la presencia de problemas de configuración comunes en un entorno Linux VDA. Puede instalar el paquete **XDPing** en cualquier máquina que ejecute una distribución de Linux compatible. **XDPing** no requiere que el paquete de Linux VDA esté instalado en la máquina. Para obtener más información acerca de la herramienta, consulte el artículo [CTX202015](#) de Knowledge Center.

## Paso 10: 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:

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

### Detener Linux VDA:

Para detener los servicios de Linux VDA:

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

#### Nota:

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

### Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

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

### Comprobar el estado de Linux VDA:

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

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

## Paso 11: Cree el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops

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 **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios VDI dedicados.
- 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 12: Cree el grupo de entrega en Citrix Virtual Apps y Citrix Virtual Desktops

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:

- 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.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte [Citrix Virtual Apps and Desktops 7 1912 LTSR](#).

## Instalar Linux Virtual Delivery Agent para SUSE manualmente

June 17, 2022

### Importante:

Para instalaciones nuevas, se recomienda usar [Easy Install](#) para una instalación rápida. Easy Install ahorra tiempo y esfuerzo, y es menos propenso a errores que la instalación manual descrita en este artículo.

### 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:

```
1 su -
2
3 yast
4 <!--NeedCopy-->
```

Para iniciar la herramienta YaST de interfaz gráfica:

```
1 su -
2
3 yast2 &
4 <!--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.

**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.

**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
```

A:

```
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:

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--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 12: Versión 9.3 o una posterior
- OpenJDK 1.8.0
- Open Motif Runtime Environment 2.3.1 o una versión posterior
- Cups
  - SLED/SLES 12: Versión 1.6.0 o una posterior
- Filtros Foomatic
  - SLED/SLES 12: Versión 1.0.0 o una posterior
- ImageMagick
  - 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 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 12, ejecute los comandos:

```
1 sudo mkdir -p /mnt/sles
2
3 sudo mount -t iso9660 path-to-iso/SLES-12-SP3-DVD-x86_64-GM-DVD1.iso /
  mnt/sles
4
5 sudo zypper ar -f /mnt/sles sles
6 <!--NeedCopy-->
```

- En SLED/SLES 12, ejecute los comandos:

```
1 sudo mkdir -p /mnt/sdk
2
3 sudo mount -t iso9660 path-to-iso/SLE-12-SP3-SDK-DVD-x86_64-GM-DVD1.iso
  /mnt/sdk
4
5 sudo zypper ar -f /mnt/sdk sdk
6 <!--NeedCopy-->
```

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

```
1 sudo zypper install krb5-client
2 <!--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 1.8.0.

**Sugerencia:**

Para evitar errores de registro con el Delivery Controller, compruebe que solo ha instalado OpenJDK 1.8.0. Quite todas las demás versiones de Java que haya presentes en su sistema.

- **SLED:**

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

```
1 sudo zypper info java-1_8_0-openjdk
2 <!--NeedCopy-->
```

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

```
1 sudo zypper update java-1_8_0-openjdk
2 <!--NeedCopy-->
```

3. Compruebe la versión de Java:

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

- **SLES:**

1. En SLES, instale Java Runtime Environment:

```
1 sudo zypper install java-1_8_0-openjdk
2 <!--NeedCopy-->
```

2. Compruebe la versión de Java:

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

**Instalar PostgreSQL** En SLED/SLES 12, instale los paquetes:

```
1 sudo zypper install postgresql-init
2
3 sudo zypper install postgresql-server
4
5 sudo zypper install postgresql-jdbc
6 <!--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:

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl restart postgresql
4 <!--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 12, ejecute los comandos para quitar los paquetes:

```
1 sudo zypper rr sles
2
3 sudo umount /mnt/sles
4
5 sudo rmdir /mnt/sles
6 <!--NeedCopy-->
```

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

```
1 sudo zypper rr sdk
2
3 sudo umount /mnt/sdk
4
5 sudo rmdir /mnt/sdk
6 <!--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 Hypervisor

Si está habilitada la funcionalidad de sincronización horaria de Citrix Hypervisor, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como Citrix Hypervisor intentarán administrar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, sincronice el reloj del sistema de cada invitado Linux 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 Citrix VM Tools instalado, puede comprobar si la función de sincronización horaria de Citrix Hypervisor está presente y habilitarla en la máquina virtual de Linux:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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:

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--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:

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

Después de reiniciar, compruebe que la configuración es correcta:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor 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](#)
- [Quest Authentication Services](#)
- [Centrify DirectControl](#)

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

**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 **Yes**.
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:

```
1 su -
2
3 reboot
4 <!--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 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 keytab del sistema se haya creado y contenga 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:

```
1 wbinfo --krb5auth=domain\username%password
2 <!--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 comprobar que el módulo Winbind PAM está configurado correctamente, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--NeedCopy-->
```

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

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

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

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

Salga de la sesión.

```
1 exit
```

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

Se puede realizar una prueba similar iniciando sesión directamente en la consola GNOME o KDE. Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## Quest Authentication Services

**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 tickets de Kerberos debe estar habilitada y desconectada. La autenticación (inicio de sesión sin conexión) debe estar inhabilitada:

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-  
   interval 32400  
2  
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-  
   auth false  
4 <!--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 ticket. Establezca esta opción en un valor inferior en sistemas con una validez más corta de tickets.

**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:

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

**Unirse al dominio de Windows** Una la máquina Linux al dominio de Active Directory mediante el comando `vastool` de Quest:

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
2 <!--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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 comprobar que Quest puede autenticar usuarios de dominio a través de PAM, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--NeedCopy-->
```

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

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

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

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

Salga de la sesión.

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

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el [Paso 6: 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:

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--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:

```
1 su -
2
3 adinfo
4 <!--NeedCopy-->
```

Verifique 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:

```
1 adinfo --sysinfo all
```

```
2
3 adinfo -diag
4 <!--NeedCopy-->
```

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

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

Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## Paso 4: Instale .NET Core Runtime como requisito previo

Antes de instalar Linux VDA, instale .NET Core Runtime conforme a las instrucciones de <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

- Para la versión inicial de 1912 LTSR, CU1 y CU2, instale .NET Core Runtime 2.1.
- Para CU3 y versiones posteriores, instale .NET Core Runtime 3.1.

Después de instalar .NET Core Runtime, ejecute el comando `which dotnet` para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de runtime de .NET Core. Por ejemplo, si el resultado del comando es `/aa/bb/dotnet`, use `/aa/bb` como ruta binaria de .NET.

## Paso 5: Descargue el paquete de Linux VDA

Vaya a la [página de descargas de Citrix Virtual Apps and Desktops](#). Expanda la versión correcta de Citrix Virtual Apps and Desktops y haga clic en **Componentes** para descargar el paquete Linux VDA correspondiente a su distribución Linux.

## Paso 6: Instale Linux VDA

### Paso 6a: 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:

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

**Nota:**

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

2. Desinstale el paquete:

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

**Importante:**

Se admite la actualización desde las dos últimas versiones.

**Nota:**

Los componentes de instalación se encuentran en `/opt/Citrix/VDA/`.

Para ejecutar un comando, se necesita la ruta completa. Como alternativa, puede agregar `/opt/Citrix/VDA/sbin` y `/opt/Citrix/VDA/bin` a la ruta del sistema.

### Paso 6b: Instale Linux VDA

Instalar el software de Linux VDA mediante Zypper:

**Para SUSE 12:**

```
1 sudo zypper install XenDesktopVDA-19.12.0.50-1.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

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

**Para SUSE 12:**

```
1 sudo rpm -i XenDesktopVDA-19.12.0.50-1.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

### Paso 6c: Actualice la versión de Linux VDA (optativo)

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

**Para SUSE 12:**

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

### Lista de dependencias RPM para SUSE 12:

```
1 postgresql-server >= 9.3
2
3 postgresql-jdbc >= 9.2
4
5 java-1.8.0-openjdk >= 1.8.0
6
7 ImageMagick >= 6.8
8
9 dbus-1 >= 1.8.8
10
11 dbus-1-x11 >= 1.8.8
12
13 libXpm4 >= 3.5.11
14
15 libXrandr2 >= 1.4.2
16
17 libXtst6 >= 1.2.2
18
19 motif >= 2.3
20
21 pam >= 1.1.8
22
23 bash >= 4.2
24
25 findutils >= 4.5
26
27 gawk >= 4.1
28
29 sed >= 4.2
30
31 cups >= 1.6.0
32
33 cups-filters-foomatic-rip >= 1.0.0
34
35 openldap2 >= 2.4
36
37 cyrus-sasl >= 2.1
38
39 cyrus-sasl-gssapi >= 2.1
40
41 libxml2 >= 2.9
42
43 python-requests >= 2.8.1
44
45 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
46
47 rpmlib(CompressedFileNames) <= 3.0.4-1
48
49 rpmlib(PayloadIsLzma) <= 4.4.6-1
50
51 libtcmalloc4 >= 2.5
52
```

```
53 libcap-progs >= 2.22
54
55 xorg-x11-server >= 7.6_1.18.3-76.15
56
57 ibus >= 1.5
58 <!--NeedCopy-->
```

**Importante:**

Reinicie la máquina Linux VDA después de actualizar.

## Paso 7: Instale controladores NVIDIA GRID

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

Para instalar y configurar el administrador de GPU virtual de NVIDIA GRID (el controlador de hosts) en los hipervisores específicos, consulte estas guías:

- [Citrix Hypervisor](#)
- [VMware ESX](#)

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

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

## Paso 8: 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 –Quest Authentication Services
  - 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, 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, 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\_FAS\_LIST='list-fas-servers'**: Los servidores del Servicio de autenticación federada (FAS) se configuran a través de la directiva de grupo de AD. Como Linux VDA no admite las directivas de grupo de AD, en su lugar, se puede suministrar una lista de servidores FAS, separados por punto y coma. La secuencia debe ser la misma que la configurada en la directiva de grupo de AD. Si alguna dirección de servidor está eliminada, complete el espacio en blanco correspondiente con la cadena de texto **<none>** y no cambie la secuencia de las direcciones de servidor.
- **CTX\_XDL\_DOTNET\_RUNTIME\_PATH=path-to-install-dotnet-runtime**: La ruta de instalación de .NET Core Runtime para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es `/usr/bin`.
- **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:

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
```

```
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_START_SERVICE=Y|N
28
29 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--NeedCopy-->
```

Cuando ejecute el comando `sudo`, escriba la opción **-E** para pasar las variables de entorno existentes al nuevo shell que se crea. Se 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:

```
1 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_FAS_LIST= ' list-fas-servers ' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

```
30 <!--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 9: Ejecute XDPing

Proporcionamos una utilidad de línea de comandos, la herramienta **XDPing** de Linux, para comprobar la presencia de problemas de configuración comunes en un entorno Linux VDA. Puede instalar el paquete **XDPing** en cualquier máquina que ejecute una distribución de Linux compatible. **XDPing** no requiere que el paquete de Linux VDA esté instalado en la máquina. Para obtener más información acerca de la herramienta, consulte el artículo [CTX202015](#) de Knowledge Center.

## Paso 10: 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:

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

### Detener Linux VDA:

Para detener los servicios de Linux VDA:

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

#### Nota:

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

### Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

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

### Comprobar el estado de Linux VDA:

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

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

## Paso 11: Cree el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops

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 **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios VDI dedicados.
- 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 12: Cree el grupo de entrega en Citrix Virtual Apps y Citrix Virtual Desktops**

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:

- 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.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte [Citrix Virtual Apps and Desktops 7 1912 LTSR](#).

## Instalar Linux Virtual Delivery Agent para Ubuntu manualmente

June 17, 2022

### Importante:

Para instalaciones nuevas, se recomienda usar [Easy Install](#) para una instalación rápida. Easy Install ahorra tiempo y esfuerzo, y es menos propenso a errores que la instalación manual descrita en este artículo.

### 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. Por ejemplo, debe configurar el servidor DNS en el Linux VDA.

Si está utilizando un Ubuntu 18.04 Live Server, realice el siguiente cambio en el archivo de configuración `/etc/cloud/cloud.cfg` antes de establecer el nombre de host:

```
preserve_hostname: true
```

#### Paso 1b: 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

Asegúrese de que el nombre de dominio DNS y el nombre de dominio completo (FQDN) de la máquina se notifiquen correctamente. Para eso, cambie la siguiente línea del archivo `/etc/hosts`, de manera que incluya el FQDN y el nombre de host como las dos primeras entradas:

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

Por ejemplo:

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

Quite 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:

```
1 hostname
2 <!--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:

```
1 hostname -f
2 <!--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:

```
1 nslookup domain-controller-fqdn
2
```

```
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--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:

```
1 apt-get install chrony
2 <!--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:

```
1 sudo systemctl restart chrony
2 <!--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.

En Ubuntu 16.04, instale OpenJDK con:

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

En Ubuntu 18.04, instale OpenJDK con:

```
1 sudo apt-get install -y openjdk-8-jdk
2 <!--NeedCopy-->
```

### **Paso 1i: Instale PostgreSQL**

Linux VDA requiere PostgreSQL 9.x en Ubuntu:

```
1 sudo apt-get install -y postgresql
2
3 sudo apt-get install -y libpostgresql-jdbc-java
4 <!--NeedCopy-->
```

### **Paso 1j: Instale Motif**

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

### **Paso 1k: Instale otros paquetes**

```
1 sudo apt-get install -y libsasl2-2
2
3 sudo apt-get install -y libsasl2-modules-gssapi-mit
4
5 sudo apt-get install -y libldap-2.4-2
6
7 sudo apt-get install -y krb5-user
8
9 sudo apt-get install -y cups
10 <!--NeedCopy-->
```

### **Paso 1l: Instale el siguiente paquete (solo Ubuntu 18.04)**

```
1 sudo apt-get install -y libgtk2.0-0
2 <!--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 Hypervisor

Si está habilitada la funcionalidad de sincronización horaria de Citrix Hypervisor, se darán problemas en las máquinas virtuales Linux paravirtualizadas debido a que tanto NTP como Citrix Hypervisor 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 Citrix VM Tools instalado, puede comprobar si la función de sincronización horaria de Citrix Hypervisor está presente y habilitarla en la máquina virtual de Linux:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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:

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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, 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 Citrix Hypervisor 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](#)

- [Quest Authentication Services](#)
- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#)

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

### Instalar o actualizar los paquetes requeridos

```
1 sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-  
   config krb5-locales krb5-user  
2 <!--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:

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

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

```
1 [libdefaults]  
2  
3 default_realm = REALM  
4  
5 dns_lookup_kdc = false  
6  
7  
8  
9 [realms]  
10  
11 REALM = {  
12  
13  
14 admin_server = domain-controller-fqdn  
15  
16 kdc = domain-controller-fqdn  
17  
18 }  
19
```

```
20
21
22
23 [domain_realm]
24
25 domain-dns-name = REALM
26
27 .domain-dns-name = REALM
28 <!--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 Winbind 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:

```
1 [global]
2
3 workgroup = WORKGROUP
4
5 security = ADS
6
7 realm = REALM
8
9 encrypt passwords = yes
10
11 idmap config *:range = 16777216-33554431
12
13 winbind trusted domains only = no
14
15 kerberos method = secrets and keytab
16
17 winbind refresh tickets = yes
18
19 template shell = /bin/bash
20 <!--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 líneas siguientes:

```
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:

```
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.

#### Reiniciar winbind

```
1 sudo systemctl restart winbind
2 <!--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:

```
1 sudo pam-auth-update
2 <!--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:

```
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, verifique que el archivo del sistema **keytab** se haya creado y contenga 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:

```
1 wbinfo --krb5auth=domain\username%password
2 <!--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 comprobar que el módulo Winbind PAM está configurado correctamente, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

**Nota:**

Para ejecutar correctamente un comando SSH, asegúrese de que SSH está habilitado y funciona correctamente.

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

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

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

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

Salga de la sesión.

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

Se puede realizar una prueba similar iniciando sesión directamente en la consola Gnome o KDE. Continúe con el [Paso 6: 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.

## **Quest Authentication Services**

**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:

```
1 reboot
2 <!--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:

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
   interval 32400
2
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
   auth false
4 <!--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:

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

**Unirse al dominio de Windows** Una la máquina Linux al dominio de Active Directory mediante el comando `vastool` de Quest:

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
```

```
2 <!--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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 comprobar que Quest puede autenticar usuarios de dominio a través de PAM, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

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

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

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

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

Salga de la sesión.

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

Continúe con el [Paso 6: 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:

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--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:

```
1 su -
2
3 adinfo
4 <!--NeedCopy-->
```

Verifique 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:

```
1 adinfo --sysinfo all
2
3 adinfo --diag
4 <!--NeedCopy-->
```

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

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

## SSSD

**Configurar Kerberos** Ejecute el siguiente comando para instalar Kerberos:

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

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

```
1 [libdefaults]
2
3 default_realm = REALM
4
5 dns_lookup_kdc = false
6
7 [realms]
8
9 REALM = {
10
11     admin_server = domain-controller-fqdn
12
13     kdc = domain-controller-fqdn
14
15 }
16
17
18
19 [domain_realm]
20
21 domain-dns-name = REALM
22
23 .domain-dns-name = REALM
24 <!--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`.

- **Si utiliza `adcli` para unirse al dominio, complete los siguientes pasos:**

1. Instale `adcli`.

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

2. Únase al dominio con `adcli`.

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

```
1 su -
```

```
2
3 rm -rf /etc/krb5.keytab
4
5 adcli join domain-dns-name -U user -H hostname-fqdn
6 <!--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.

### 3. Compruebe el archivo keytab del sistema.

Las capacidades de la herramienta `adcli` son limitadas y no proporcionan 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:

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

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

#### • Si utiliza Samba para unirse al dominio, complete los siguientes pasos:

##### 1. Instale el paquete.

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

##### 2. Configure Samba.

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

```
1 [global]
2
3 workgroup = WORKGROUP
4
5 security = ADS
6
7 realm = REALM
8
9 client signing = yes
10
11 client use spnego = yes
12
13 kerberos method = secrets and keytab
14 <!--NeedCopy-->
```

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

### 3. 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.

```
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 SSSD Instalar o actualizar los paquetes requeridos:

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

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

Si los paquetes ya están instalados, se recomienda actualizarlos:

```
1 sudo apt-get install --only-upgrade sssd
2 <!--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/sss/sss.conf** no se instala de forma predeterminada y se debe crear manualmente. Como usuario root, cree o abra el archivo **/etc/sss/sss.conf** y configure los siguientes parámetros:

```
1 [sss]
2
3 services = nss, pam
4
5 config_file_version = 2
6
7 domains = domain-dns-name
8
9 [domain/domain-dns-name]
10
11 id_provider = ad
12
13 access_provider = ad
```

```
14
15 auth_provider = krb5
16
17 krb5_realm = REALM
18
19 # Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
    than 14 days
20
21 krb5_renewable_lifetime = 14d
22
23 # Set krb5_renew_interval to lower value if TGT ticket lifetime is
    shorter than 2 hours
24
25 krb5_renew_interval = 1h
26
27 krb5_ccachedir = /tmp
28
29 krb5_ccname_template = FILE:%d/krb5cc_%U
30
31 # This ldap_id_mapping setting is also the default value
32
33 ldap_id_mapping = true
34
35 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, el servidor de 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, `example.com`). `REALM` es el nombre del territorio Kerberos en mayúsculas, como `EXAMPLE.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.

- Si utiliza `adcli` para verificar la pertenencia al dominio, ejecute el comando `sudo adcli info domain-dns-name` para mostrar la información del dominio.
- Si utiliza `Samba` para verificar la pertenencia al dominio, ejecute el comando `sudo net ads testjoin` para verificar que la máquina está unida a un dominio y el comando `sudo net ads info` para verificar información adicional sobre el dominio y el objeto de equipo.

**Verificar la configuración de Kerberos** Para verificar que Kerberos está configurado correctamente para su uso con Linux VDA, verifique que el archivo del sistema keytab se haya creado y contenga 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 vale de concesión de vales de la cuenta de la máquina se ha almacenado en caché:

```
1 sudo klist
2 <!--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 comprobar que el módulo SSSD PAM está configurado correctamente, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
8 <!--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:

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

Se puede realizar una prueba similar iniciando sesión en KDE o Gnome Display Manager. Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## PBIS

**Descargar el paquete PBIS requerido** Por ejemplo:

```
1 sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
  /8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

**Convertir el script de instalación de PBIS en ejecutable** Por ejemplo:

```
1 sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

**Ejecutar el script de instalación de PBIS** Por ejemplo:

```
1 sudo sh pbis-open-8.8.0.506.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

**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 /opt/pbis/bin/domainjoin-cli join domain-name user
2 <!--NeedCopy-->
```

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

**Nota:** Para establecer Bash como el shell predeterminado, ejecute el comando **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**.

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

```
1 /opt/pbis/bin/domainjoin-cli query
2 <!--NeedCopy-->
```

Si la máquina está unida a un dominio, este comando devuelve la información sobre el dominio de AD y la unidad organizativa a los que está unida actualmente. De lo contrario, solo aparece el nombre de host.

**Verificar la autenticación de usuario** Para comprobar que PBIS puede autenticar usuarios de dominio a través de PAM, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
1 sudo ssh localhost -l domain\user
2
3 id -u
4 <!--NeedCopy-->
```

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

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

Salga de la sesión.

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

Continúe con el [Paso 6: Instale Linux VDA](#) después de la verificación de unión al dominio.

## Paso 4: Instale .NET Core Runtime como requisito previo

Antes de instalar Linux VDA, instale .NET Core Runtime conforme a las instrucciones de <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

- Para la versión inicial de 1912 LTSR, CU1 y CU2, instale .NET Core Runtime 2.1.
- Para CU3 y versiones posteriores, instale .NET Core Runtime 3.1.

Después de instalar .NET Core Runtime, ejecute el comando `which dotnet` para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de runtime de .NET Core. Por ejemplo, si el resultado del comando es `/aa/bb/dotnet`, use `/aa/bb` como ruta binaria de .NET.

## Paso 5: Descargue el paquete de Linux VDA

Vaya a la [página de descargas de Citrix Virtual Apps and Desktops](#). Expanda la versión correcta de Citrix Virtual Apps and Desktops y haga clic en **Componentes** para descargar el paquete Linux VDA correspondiente a su distribución Linux.

## Paso 6: Instale Linux VDA

### Paso 6a: Instale Linux VDA

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

#### Para Ubuntu 18.04:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu18.04_amd64.deb
2 <!--NeedCopy-->
```

#### Para Ubuntu 16.04:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu16.04_amd64.deb
2 <!--NeedCopy-->
```

Lista de dependencias de Debian para Ubuntu 18.04:

```
1 postgresql >= 9.5
2
3 libpostgresql-jdbc-java >= 9.2
4
5 openjdk-8-jdk >= 1.8.0
6
7 gtk3-nocsd >=3
8
9 imagemagick >= 8:6.8.9.9
10
11 ufw >= 0.35
12
13 ubuntu-desktop >= 1.361
14
15 libxrandr2 >= 2:1.5.0
16
17 libxtst6 >= 2:1.2.2
18
19 libxm4 >= 2.3.4
20
21 util-linux >= 2.27.1
22
23 bash >= 4.3
24
25 findutils >= 4.6.0
26
27 sed >= 4.2.2
28
29 cups >= 2.1
30
31 libldap-2.4-2 >= 2.4.42
32
33 libsasl2-modules-gssapi-mit >= 2.1.~
34
35 python-requests >= 2.9.1
36
37 libgoogle-perftools4 >= 2.4~
38
39 xserver-xorg-core >= 2:1.18
40
41 xserver-xorg-core << 2:1.19
42
43 x11vnc>=0.9.13
44
45 python-websocketify >= 0.6.1
46 <!--NeedCopy-->
```

Lista de dependencias de Debian para Ubuntu 16.04:

```
1 postgresql >= 9.5
2
3 libpostgresql-jdbc-java >= 9.2
```

```
4
5 default-jdk >= 2:1.8
6
7 imagemagick >= 8:6.8.9.9
8
9 ufw >= 0.35
10
11 ubuntu-desktop >= 1.361
12
13 libxrandr2 >= 2:1.5.0
14
15 libxtst6 >= 2:1.2.2
16
17 libxm4 >= 2.3.4
18
19 util-linux >= 2.27.1
20
21 bash >= 4.3
22
23 findutils >= 4.6.0
24
25 sed >= 4.2.2
26
27 cups >= 2.1
28
29 libldap-2.4-2 >= 2.4.42
30
31 libsasl2-modules-gssapi-mit >= 2.1.~
32
33 python-requests >= 2.9.1
34
35 libgoogle-perftools4 >= 2.4~
36
37 xserver-xorg-core >= 2:1.18
38
39 xserver-xorg-core << 2:1.19
40
41 x11vnc>=0.9.13
42
43 python-websocketify >= 0.6.1
44 <!--NeedCopy-->
```

**Nota:**

Para ver una matriz de las distribuciones de Linux y las versiones de Xorg que admite esta versión de Linux VDA, consulte los [requisitos del sistema](#).

**Paso 6b: Actualice la versión de Linux VDA (optativo)**

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

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
2 <!--NeedCopy-->
```

## Paso 7: Instale controladores NVIDIA GRID

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

Para instalar y configurar el administrador de GPU virtual de NVIDIA GRID (el controlador de hosts) en los hipervisores específicos, consulte estas guías:

- [Citrix Hypervisor](#)
- [VMware ESX](#)

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

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

## Paso 8: 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, 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 | 5**: 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 –Quest Authentication Services
  - 3 –Centrify DirectControl
  - 4 –SSSD
  - 5 –PBIS
- **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, 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\_FAS\_LIST='list-fas-servers':** Los servidores del Servicio de autenticación federada (FAS) se configuran a través de la directiva de grupo de AD. Como Linux VDA no admite las directivas de grupo de AD, en su lugar, se puede suministrar una lista de servidores FAS, separados por punto y coma. La secuencia debe ser la misma que la configurada en la directiva de grupo de AD. Si alguna dirección de servidor está eliminada, complete el espacio en blanco correspondiente con la cadena de texto **<none>** y no cambie la secuencia de las direcciones de servidor.
- **CTX\_XDL\_DOTNET\_RUNTIME\_PATH=path-to-install-dotnet-runtime:** La ruta de instalación de .NET Core Runtime para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es `/usr/bin`.
- **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:

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
```

```
19 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_START_SERVICE=Y|N
28
29 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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:

```
1 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|5 \
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_FAS_LIST= ' list-fas-servers ' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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:

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

Para ver información más detallada:

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

Para desinstalar el software de Linux VDA:

```
1 dpkg -r xendesktopvda
2 <!--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 9: Ejecute XDPing

Proporcionamos una utilidad de línea de comandos, la herramienta `XDPing` de Linux, para comprobar la presencia de problemas de configuración comunes en un entorno Linux VDA. Puede instalar el paquete `XDPing` en cualquier máquina que ejecute una distribución de Linux compatible. `XDPing` no requiere que el paquete de Linux VDA esté instalado en la máquina. Para obtener más información acerca de la herramienta, consulte el artículo [CTX202015](#) de Knowledge Center.

## Paso 10: 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:

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
4 <!--NeedCopy-->
```

### Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
4 <!--NeedCopy-->
```

### Nota:

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

### Reiniciar Linux VDA:

Para reiniciar los servicios de Linux VDA:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl restart ctxvda
6 <!--NeedCopy-->
```

### Comprobar el estado de Linux VDA:

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

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
4 <!--NeedCopy-->
```

## Paso 11: Cree el catálogo de máquinas en Citrix Virtual Apps o Citrix Virtual Desktops

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 **SO multisesión** para un modelo de entrega de escritorios compartidos alojados.
  - La opción **SO de sesión única** para un modelo de entrega de escritorios VDI dedicados.
- 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 12: Cree el grupo de entrega en Citrix Virtual Apps y Citrix Virtual Desktops**

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:

- 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.

Para obtener información sobre cómo crear catálogos de máquinas y grupos de entrega, consulte [Citrix Virtual Apps and Desktops 7 1912 LTSR](#).

## **Utilice Machine Creation Services (MCS) para crear máquinas virtuales Linux**

May 4, 2023

A partir de la versión 7.18, puede usar MCS para crear máquinas virtuales Linux.

### **Hipervisores compatibles**

- AWS
- Citrix Hypervisor
- Microsoft Azure
- VMware vSphere

Se pueden producir resultados imprevistos si intenta preparar una imagen maestra en hipervisores que no sean compatibles.

### **Usar MCS para crear máquinas virtuales Linux en Citrix Hypervisor**

#### **Paso 1: Prepare una imagen maestra**

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

**Paso 1a: Instale Citrix VM Tools** Citrix VM Tools se debe instalar en la VM de plantilla para que cada VM pueda usar la CLI de Xen o XenCenter. El rendimiento de la VM puede ser lento a menos que se instalen las herramientas. Sin las herramientas, no puede hacer nada de lo siguiente:

- Apagar, reiniciar ni suspender una máquina virtual de manera sencilla.
- Ver los datos de rendimiento de la VM en XenCenter.
- Migrar una VM en ejecución (a través de XenMotion).
- Crear instantáneas o instantáneas con memoria (puntos de control) y revertir a ellas.
- Ajustar la cantidad de vCPU en una VM Linux en ejecución.

1. Ejecute el siguiente comando para montar Citrix VM Tools, cuyo archivo se llama guest-tools.iso.

```
1 sudo mount /dev/cdrom /mnt
2 <!--NeedCopy-->
```

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

**Para RHEL/CentOS:**

```
1 sudo rpm -i /mnt/Linux/xe-guest-utilities_{
2 package-version }
3 _all.rpm
4 <!--NeedCopy-->
```

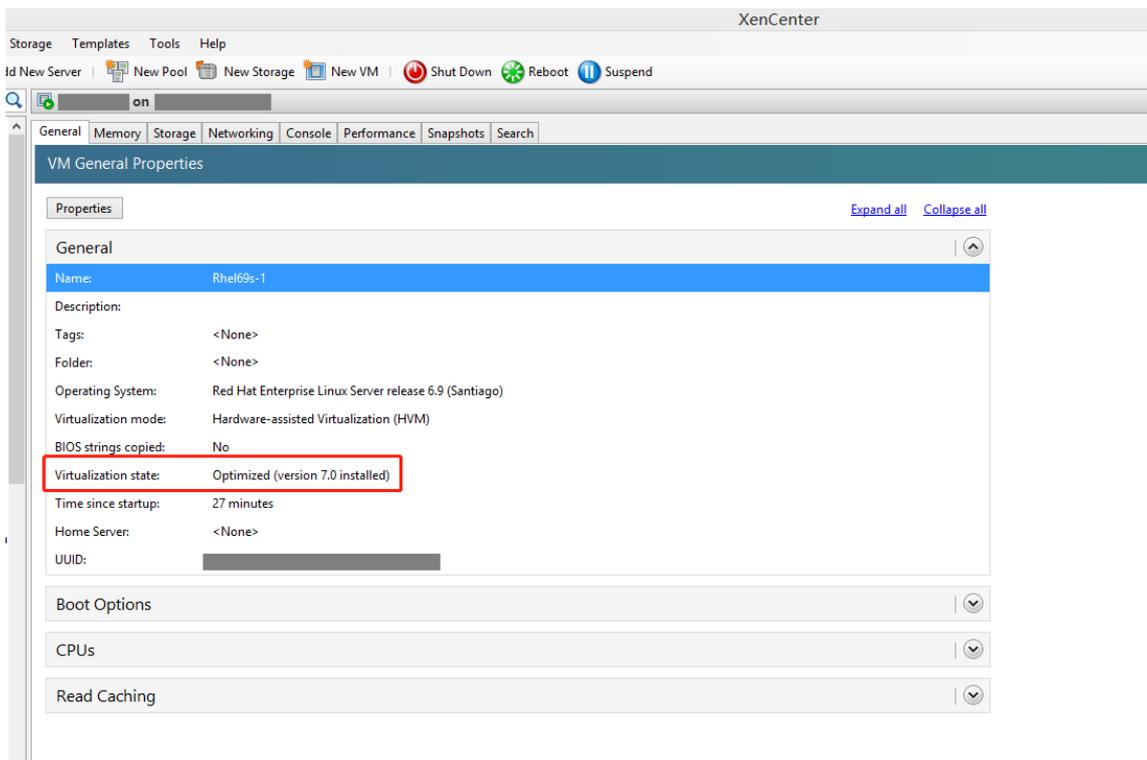
**Para Ubuntu:**

```
1 sudo dpkg -i /mnt/Linux/xe-guest-utilities_{
2 package-version }
3 _all.deb
4 <!--NeedCopy-->
```

**Para SUSE 12:**

```
1 sudo rpm -i /mnt/Linux/xe-guest-utilities_{
2 package-version }
3 _all.rpm
4 <!--NeedCopy-->
```

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



## Paso 1b: Instale el paquete de Linux VDA en la VM de la plantilla

### Nota:

Para utilizar un VDA que se ejecuta como una VM de plantilla, omita este paso.

Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Core Runtime 3.1.

Para obtener más información, consulte [Información general de la instalación](#).

En función de su distribución de Linux, ejecute el siguiente comando para configurar el entorno para Linux VDA:

### Para RHEL/CentOS:

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

### Para Ubuntu:

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2
3 apt-get install -f
4 <!--NeedCopy-->
```

### Para SUSE 12:

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

**Paso 1c: Habilite repositorios para instalar el paquete tdb-tools** Para el servidor de RHEL 7:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

**Para la estación de trabajo de RHEL 7:**

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

**Paso 1d: Instale el repositorio EPEL que contiene ntfs-3g** Instale el repositorio EPEL en RHEL 6/CentOS 6, RHEL 7/CentOS 7 para que la ejecución posterior de `deploymcs.sh` instale el paquete `ntfs-3g` que contiene.

**Paso 1e: Instale manualmente ntfs-3g en SUSE 12** En la plataforma SUSE 12, no hay ningún repositorio que ofrezca `ntfs-3g`. Debe descargar el código fuente, compilarlo e instalar `ntfs-3g` de forma manual:

1. Instale el sistema de compilación GNU Compiler Collection (GCC) y cree el paquete:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. Descargue el paquete `ntfs-3g`.

3. Descomprima el paquete `ntfs-3g`:

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. Escriba la ruta del paquete `ntfs-3g`:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

5. Instale `ntfs-3g`:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

**Paso 1f: Configure el entorno en tiempo de ejecución** Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie variables en **/etc/xdl/mcs/mcs.conf**. El archivo de configuración **mcs.conf** contiene variables para configurar MCS y Linux VDA. A continuación, dispone de las variables que puede establecer según sea necesario:
  - **Use\_Existing\_Configurations\_Of\_Current\_VDA**: Determina si se deben utilizar las configuraciones existentes del VDA que se ejecuta actualmente. Si se define con el valor Y, los archivos de configuración de las máquinas creadas por MCS son los mismos que los del VDA que se ejecuta actualmente. Sin embargo, aún debe configurar las variables **dns** y **AD\_INTEGRATION**. El valor predeterminado es N, lo que significa que los archivos de configuración de máquinas creadas por MCS están determinados por plantillas de configuración de la imagen maestra.
  - **dns**: Establece la dirección IP de DNS
  - **AD\_INTEGRATION**: Establece Winbind o SSSD.
  - **WORKGROUP**: Establece el nombre del grupo de trabajo, que es el nombre NetBIOS (distingue entre mayúsculas y minúsculas) si se configura en AD. De lo contrario, de forma predeterminada, es el nombre de dominio.
- En la máquina de la plantilla, agregue líneas de comandos al archivo **/etc/xdl/mcs/mcs\_local\_setting.reg** para escribir o actualizar los valores del Registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina aprovisionada con MCS.

Cada línea del archivo **/etc/xdl/mcs/mcs\_local\_setting.reg** es un comando para configurar o actualizar un valor del Registro.

Por ejemplo: Puede agregar las siguientes líneas de comando al archivo **/etc/xdl/mcs/mcs\_local\_setting.reg** para escribir o actualizar un archivo del Registro respectivamente:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
  VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
  v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
  VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
  x00000003"
2 <!--NeedCopy-->
```

### Paso 1g: Cree una imagen maestra

1. Ejecute **/opt/Citrix/VDA/sbin/deploymcs.sh**.
2. (Opcional) En la máquina virtual de la plantilla, actualice las plantillas de configuración para personalizar los archivos **/etc/krb5.conf**, **/etc/samba/smb.conf** y **/etc/sss/sss.conf** pertinentes en todas las máquinas virtuales creadas.

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

Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sss.conf.tmpl`, `/etc/xdl/mcs/sss_krb5.conf.tmpl` y `/etc/xdl/mcs/sss_smb.conf.tmpl`.

**Nota:** Mantenga el formato utilizado en los archivos de plantilla y utilice variables como `$WORKGROUP`, `$REALM`, `$realm` y `$AD_FQDN`.

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

## Paso 2: Cree un catálogo de máquinas

En Citrix Studio, cree un catálogo de máquinas y especifique la cantidad de máquinas virtuales que se van a crear en el catálogo. Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte [Crear un catálogo de máquinas mediante Studio](#).

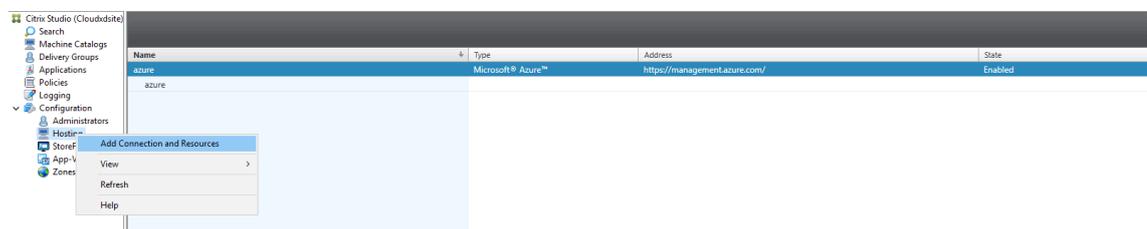
## Paso 3: Cree un grupo de entrega

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica los usuarios que pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios. Para obtener más información, consulte [Crear grupos de entrega](#).

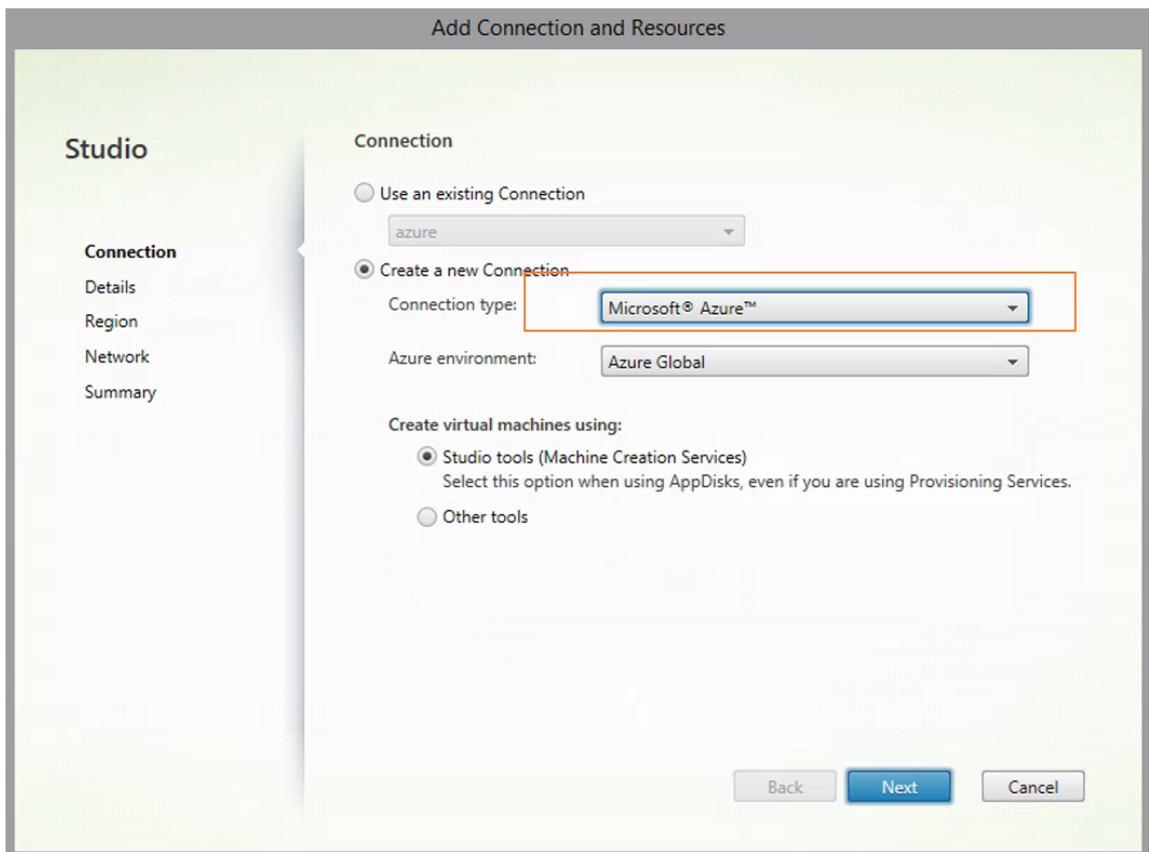
## Usar MCS para crear máquinas virtuales Linux en Azure

### Paso 1: Cree una conexión de alojamiento con Azure en Citrix Studio

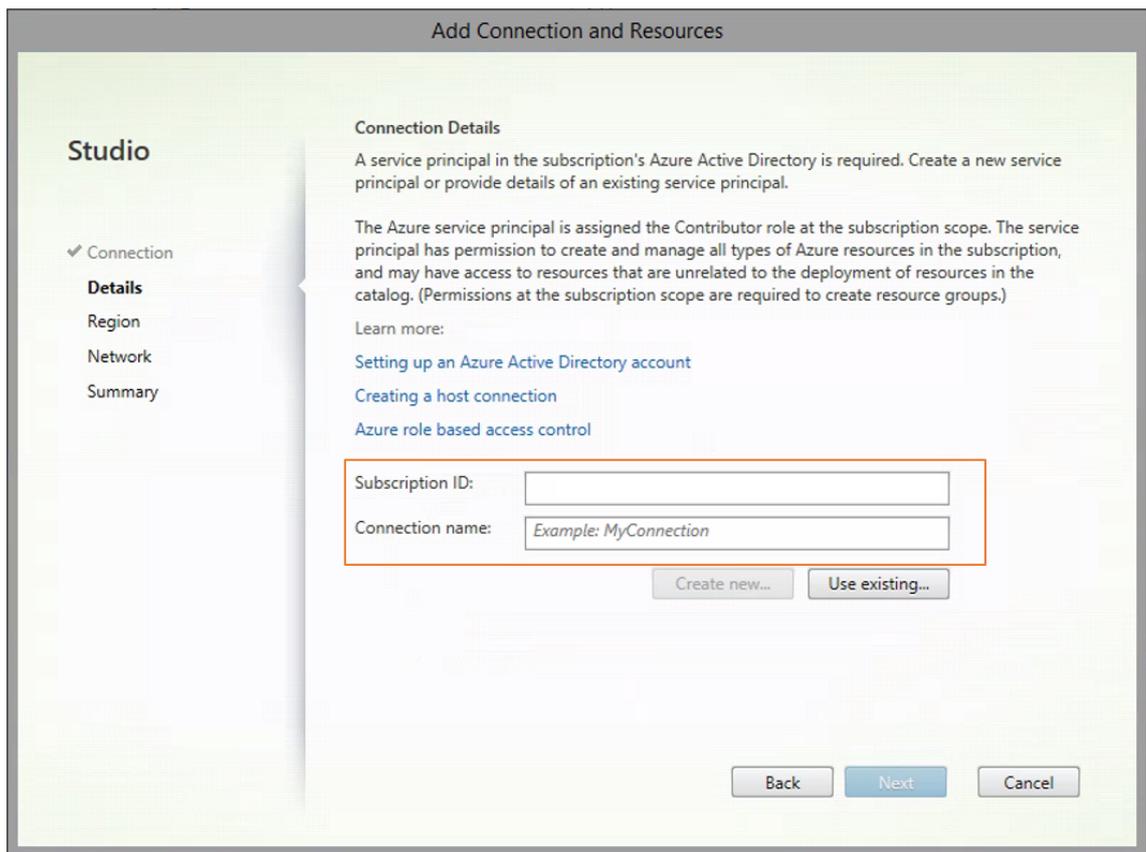
1. En Citrix Studio, elija **Configuración > Alojamiento > Agregar conexión y recursos** para crear una conexión con Azure.



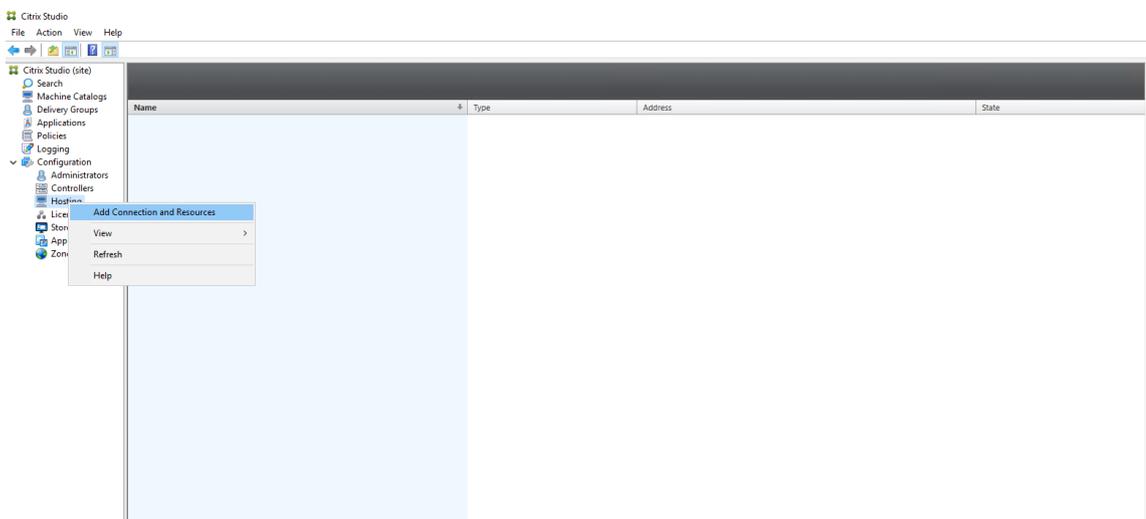
2. Elija Microsoft Azure como el tipo de conexión.



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



Aparece una nueva conexión en el panel de alojamiento.



## Paso 2: Prepare una imagen maestra en la VM de la plantilla

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

**Paso 2a: Configure cloud-init para Ubuntu 18.04** Para asegurarse de que el nombre de host de un VDA persiste cuando se reinicia o se detiene una máquina virtual, ejecute el siguiente comando.

```
1 echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.  
   cfg  
2 <!--NeedCopy-->
```

Compruebe que estas líneas se encuentran en la sección **system\_info** del archivo `/etc/cloud/cloud.cfg`:

```
1 system_info:  
2   network:  
3     renderers: ['netplan', 'eni', 'sysconfig']  
4 <!--NeedCopy-->
```

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

#### Nota:

Para utilizar un VDA que se ejecuta como una VM de plantilla, omita este paso.

Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Core Runtime 3.1.

Para obtener más información, consulte [Información general de la instalación](#).

En función de su distribución de Linux, ejecute el siguiente comando para configurar el entorno para Linux VDA:

#### Para RHEL/CentOS:

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

#### Para Ubuntu:

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>  
2  
3 apt-get install -f  
4 <!--NeedCopy-->
```

#### Para SUSE 12:

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

### Paso 2c: Habilite repositorios para instalar el paquete tdb-tools Para el servidor de RHEL 7:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms  
2 <!--NeedCopy-->
```

#### Para la estación de trabajo de RHEL 7:

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

**Paso 2d: Instale el repositorio EPEL que contiene ntfs-3g** Instale el repositorio EPEL en RHEL 6/CentOS 6, RHEL 7/CentOS 7 para que la ejecución posterior de `deploymcs.sh` instale el paquete `ntfs-3g` que contiene.

**Paso 2e: Instale manualmente ntfs-3g en SUSE 12** En la plataforma SUSE 12, no hay ningún repositorio que ofrezca `ntfs-3g`. Debe descargar el código fuente, compilarlo e instalar `ntfs-3g` de forma manual:

1. Instale el sistema de compilación GNU Compiler Collection (GCC) y cree el paquete:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. Descargue el paquete `ntfs-3g`.

3. Descomprima el paquete `ntfs-3g`:

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. Escriba la ruta del paquete `ntfs-3g`:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

5. Instale `ntfs-3g`:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

**Paso 2f: Configure el entorno en tiempo de ejecución** Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` contiene variables para configurar MCS y Linux VDA. He aquí algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben definirse:

**Nota:** Si una variable se puede definir con varios valores, coloque los valores entre comillas simples y sepárelos con un espacio. Por ejemplo: `LDAP_LIST='aaa.lab:389 bbb.lab:389'`.

- `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben utilizar las configuraciones existentes del VDA que se ejecuta actualmente. Si se define con el valor Y, los archivos de configuración de las máquinas creadas por MCS son los mismos que los del VDA que se ejecuta actualmente. Sin embargo, aún debe configurar las variables `dns` y `AD_INTEGRATION`. El valor predeterminado es N, lo que significa que los archivos de configuración de máquinas creadas por MCS están determinados por plantillas de configuración de la imagen maestra.
  - `dns`: Establece la dirección IP de DNS
  - `AD_INTEGRATION`: Establece Winbind o SSSD (SSSD no se admite en SUSE)
  - `WORKGROUP`: Establece el nombre del grupo de trabajo, que es el nombre NetBIOS (distingue entre mayúsculas y minúsculas) si se configura en AD. De lo contrario, de forma predeterminada, es el nombre de dominio.
- En la máquina de la plantilla, agregue líneas de comandos al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar los valores del Registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina provisionada con MCS.

Cada línea del archivo `/etc/xdl/mcs/mcs_local_setting.reg` es un comando para configurar o actualizar un valor del Registro.

Por ejemplo: Puede agregar las siguientes líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar un archivo del Registro respectivamente:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
   v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
   VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
   x00000003"
2 <!--NeedCopy-->
```

## Paso 2g: Cree una imagen maestra

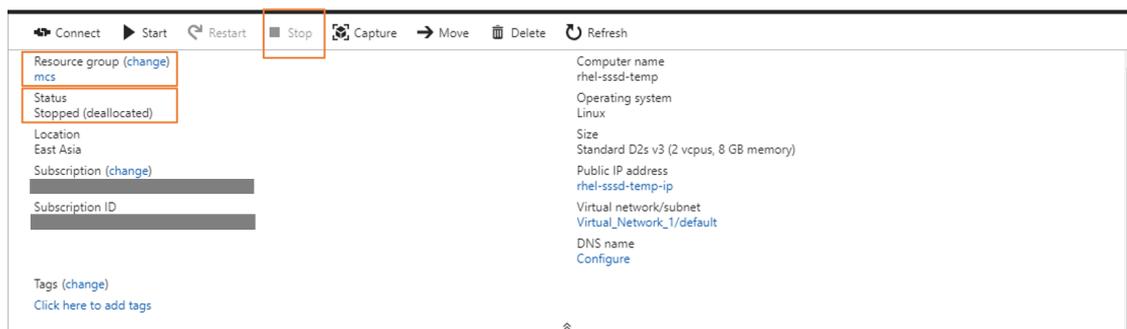
1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Opcional) En la máquina virtual de la plantilla, actualice las plantillas de configuración para personalizar los archivos `/etc/krb5.conf`, `/etc/samba/smb.conf` y `/etc/sss/sss.conf` pertinentes en todas las máquinas virtuales creadas.

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

Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sssdc.conf.tmpl`, `/etc/xdl/mcs/sssdc_krb5.conf.tmpl` y `/etc/xdl/mcs/sssdc_smb.conf.tmpl`.

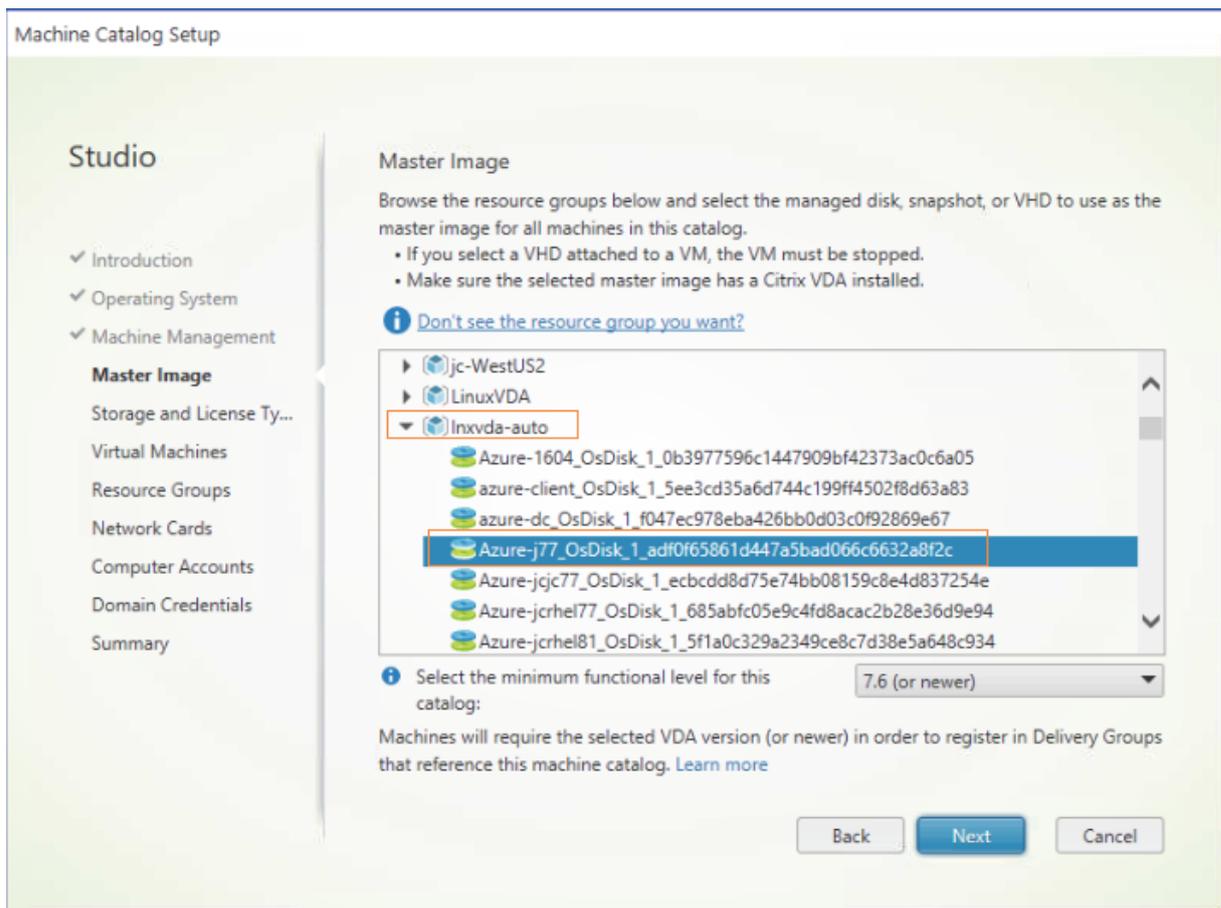
**Nota:** Mantenga el formato utilizado en los archivos de plantilla y utilice variables como `$WORKGROUP`, `$REALM`, `$realm` y `$AD_FQDN`.

3. Instale aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de Azure. Compruebe que el estado de administración de energía de la máquina virtual de plantilla es **Detenida (desasignada)**. Debe recordar el nombre del grupo de recursos indicado aquí. Necesitará ese nombre para localizar la imagen maestra en Azure.



### Paso 3: Cree un catálogo de máquinas

En Citrix Studio, cree un catálogo de máquinas y especifique la cantidad de máquinas virtuales que se van a crear en el catálogo. Al crear el catálogo de máquinas, elija su imagen maestra en el grupo de recursos al que pertenece la VM de plantilla y busque el VHD de la VM de plantilla. Consulte la siguiente captura de pantalla.



Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte [Crear un catálogo de máquinas mediante Studio](#).

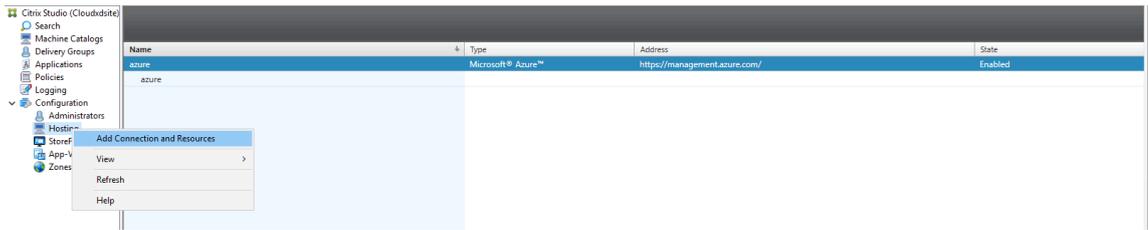
#### Paso 4: Cree un grupo de entrega

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica los usuarios que pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios. Para obtener más información, consulte [Crear grupos de entrega](#).

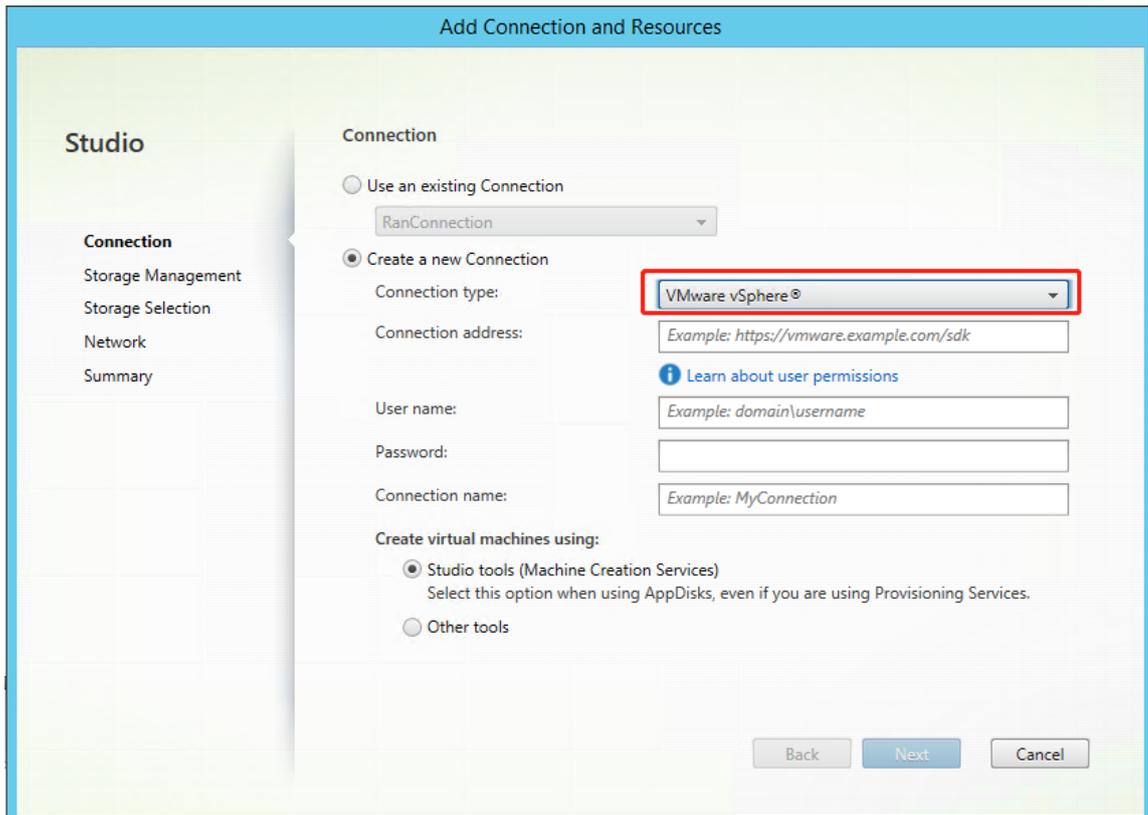
### Usar MCS para crear máquinas virtuales Linux en VMware vSphere

#### Paso 1: Cree una conexión de alojamiento con VMware en Citrix Studio

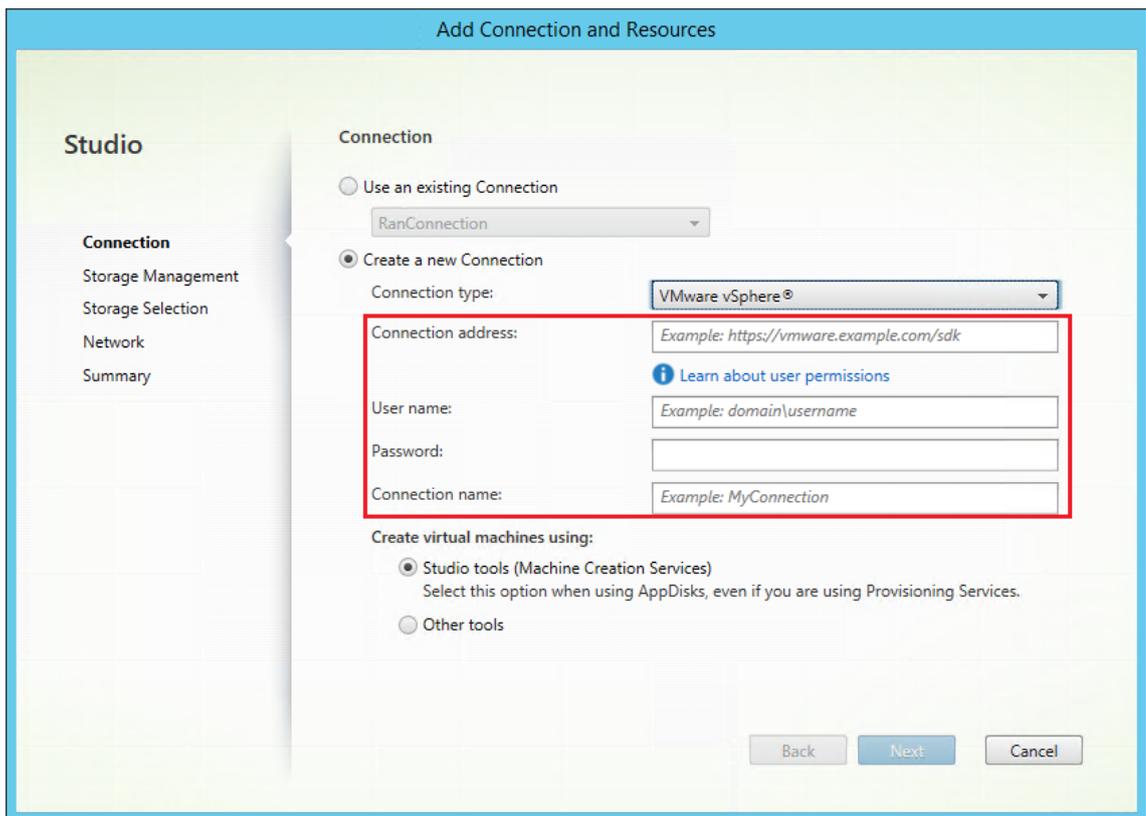
1. Instale vCenter Server en el entorno vSphere. Para obtener más información, consulte [VMware vSphere](#).
2. En Citrix Studio, elija **Configuración > Alojamiento > Agregar conexión y recursos** para crear una conexión con VMware vSphere.



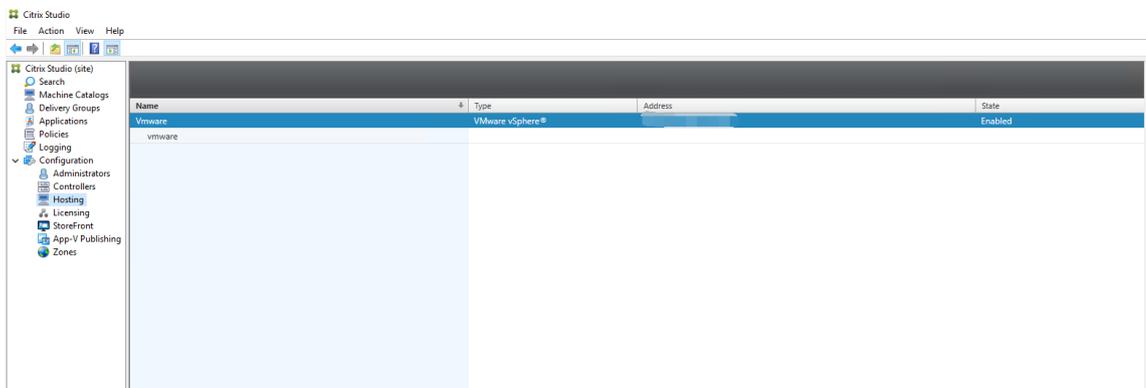
3. Elija VMware vSphere como tipo de conexión.



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



Aparece una nueva conexión en el panel de alojamiento.



## Paso 2: Prepare una imagen maestra

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

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

**Nota:**

Para utilizar un VDA que se ejecuta como una VM de plantilla, omita este paso.

Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Core Runtime 3.1.

Para obtener más información, consulte [Información general de la instalación](#).

En función de su distribución de Linux, ejecute el siguiente comando para configurar el entorno para Linux VDA:

**Para RHEL/CentOS:**

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

**Para Ubuntu:**

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2
3 apt-get install -f
4 <!--NeedCopy-->
```

**Para SUSE 12:**

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

**Paso 2b: Habilite repositorios para instalar el paquete tdb-tools** Para el servidor de RHEL 7:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

**Para la estación de trabajo de RHEL 7:**

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

**Paso 2c: Instale el repositorio EPEL que contiene ntfs-3g** Instale el repositorio EPEL en RHEL 6/CentOS 6, RHEL 7/CentOS 7 para que la ejecución posterior de `deploymcs.sh` instale el paquete `ntfs-3g` que contiene.

**Paso 2d: Instale manualmente ntfs-3g en SUSE 12** En la plataforma SUSE 12, no hay ningún repositorio que ofrezca `ntfs-3g`. Debe descargar el código fuente, compilarlo e instalar `ntfs-3g` de forma manual:

1. Instale el sistema de compilación GNU Compiler Collection (GCC) y cree el paquete:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. Descargue el paquete ntfs-3g.

3. Descomprima el paquete ntfs-3g:

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. Escriba la ruta del paquete ntfs-3g:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

5. Instale ntfs-3g:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

**Paso 2e: Configure el entorno en tiempo de ejecución** Antes de ejecutar **deploymcs.sh**, haga lo siguiente:

- Cambie variables en **/etc/xdl/mcs/mcs.conf**. El archivo de configuración **mcs.conf** contiene variables para configurar MCS y Linux VDA. He aquí algunas de las variables, de las cuales **dns** y **AD\_INTEGRATION** deben definirse:

**Nota:** Si una variable se puede definir con varios valores, coloque los valores entre comillas simples y sepárelos con un espacio. Por ejemplo: `LDAP_LIST='aaa.lab:389 bbb.lab:389'`.

- **Use\_Existing\_Configurations\_Of\_Current\_VDA:** Determina si se deben utilizar las configuraciones existentes del VDA que se ejecuta actualmente. Si se define con el valor Y, los archivos de configuración de las máquinas creadas por MCS son los mismos que los del VDA que se ejecuta actualmente. Sin embargo, aún debe configurar las variables **dns** y **AD\_INTEGRATION**. El valor predeterminado es N, lo que significa que los archivos de configuración de máquinas creadas por MCS están determinados por plantillas de configuración que hubiera en la imagen maestra.
- **dns:** Establece la dirección IP de DNS
- **AD\_INTEGRATION:** Establece Winbind o SSSD (SSSD no se admite en SUSE)
- **WORKGROUP:** Establece el nombre del grupo de trabajo, que es el nombre NetBIOS (distingue entre mayúsculas y minúsculas) si se configura en AD. De lo contrario, de forma predeterminada, es el nombre de dominio.

- En la máquina de la plantilla, agregue líneas de comandos al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar los valores del Registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina provisionada con MCS.

Cada línea del archivo `/etc/xdl/mcs/mcs_local_setting.reg` es un comando para configurar o actualizar un valor del Registro.

Por ejemplo: Puede agregar las siguientes líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar un archivo del Registro respectivamente:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\  
VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -  
v "Flags" -d "0x00000003" --force  
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\  
VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0  
x00000003"  
2 <!--NeedCopy-->
```

## Paso 2f: Cree una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Opcional) En la máquina virtual de la plantilla, actualice las plantillas de configuración para personalizar los archivos `/etc/krb5.conf`, `/etc/samba/smb.conf` y `/etc/sss/sss.conf` pertinentes en todas las máquinas virtuales creadas.

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

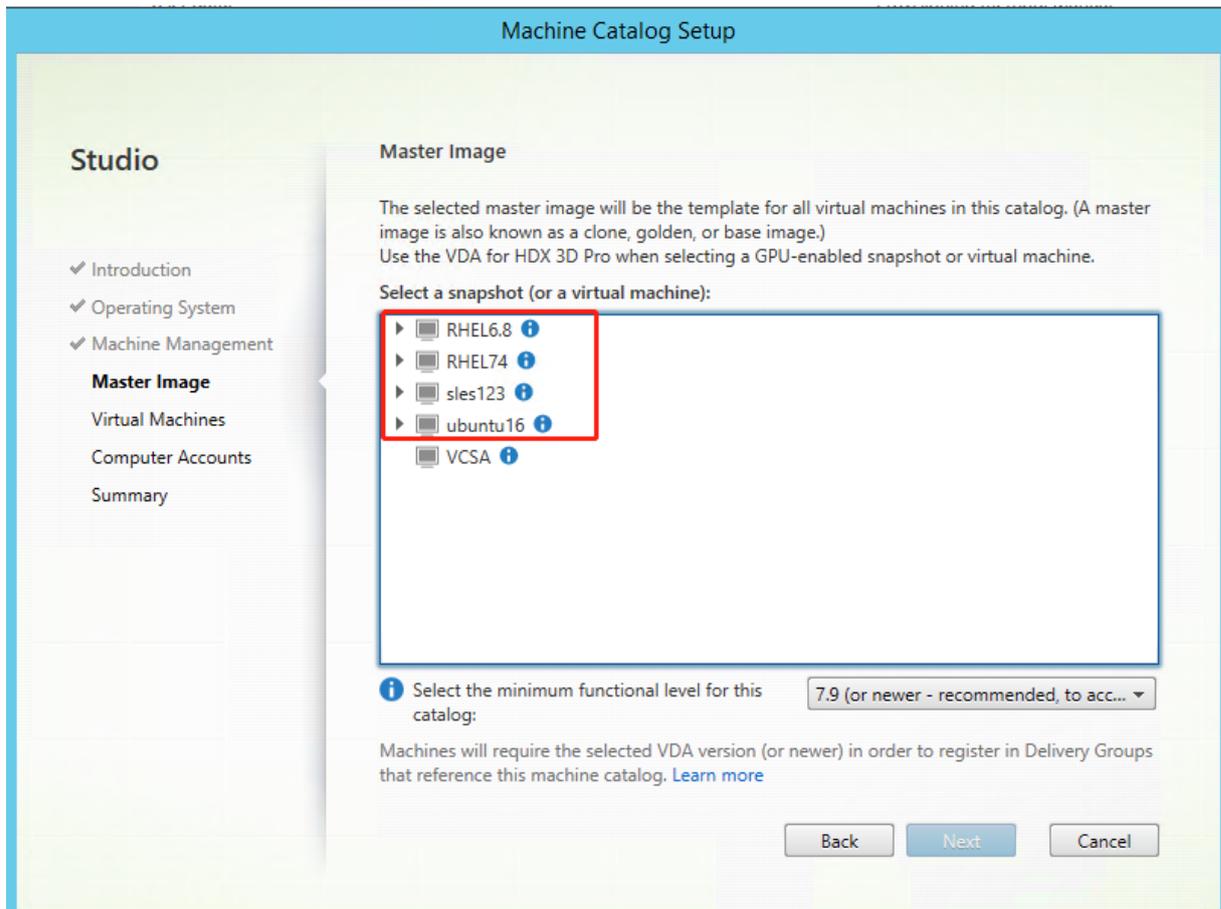
Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sss.conf.tmpl`, `/etc/xdl/mcs/sss_krb5.conf.tmpl` y `/etc/xdl/mcs/sss_smb.conf.tmpl`.

**Nota:** Mantenga el formato utilizado en los archivos de plantilla y utilice variables como `$WORKGROUP`, `$REALM`, `$realm` y `$AD_FQDN`.

3. Después de finalizar la instalación de aplicaciones en la máquina virtual de plantilla, apague la máquina virtual de plantilla desde el portal de VMware. Cree una instantánea de la máquina virtual de plantilla.

## Paso 3: Cree un catálogo de máquinas

En Citrix Studio, cree un catálogo de máquinas y especifique la cantidad de máquinas virtuales que se van a crear en el catálogo. Al crear el catálogo de máquinas, elija la imagen maestra de la lista de instantáneas.



Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte [Crear un catálogo de máquinas mediante Studio](#).

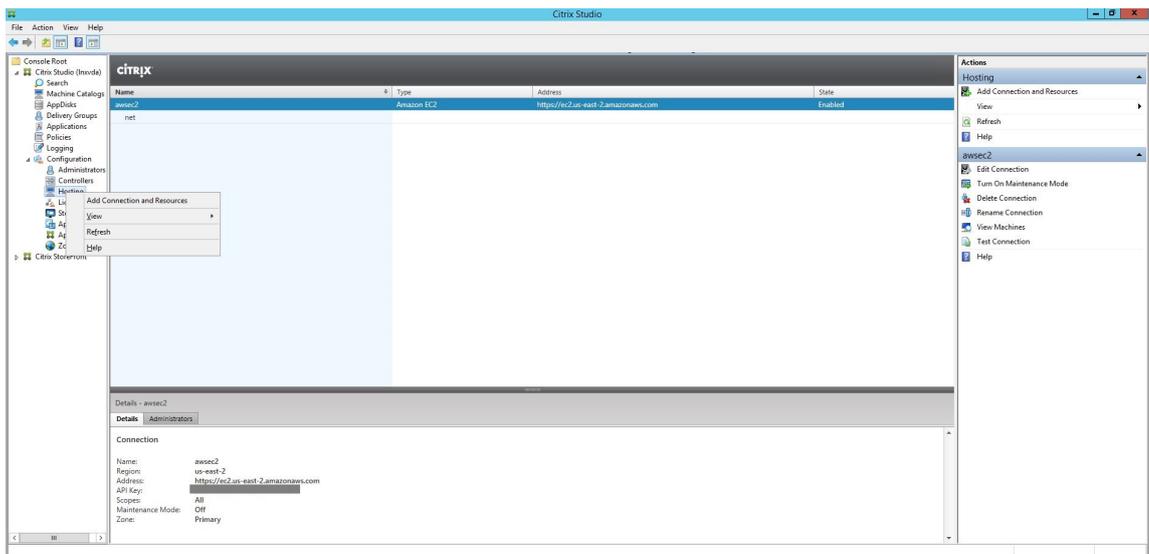
#### **Paso 4: Cree un grupo de entrega**

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica los usuarios que pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios. Para obtener más información, consulte [Crear grupos de entrega](#).

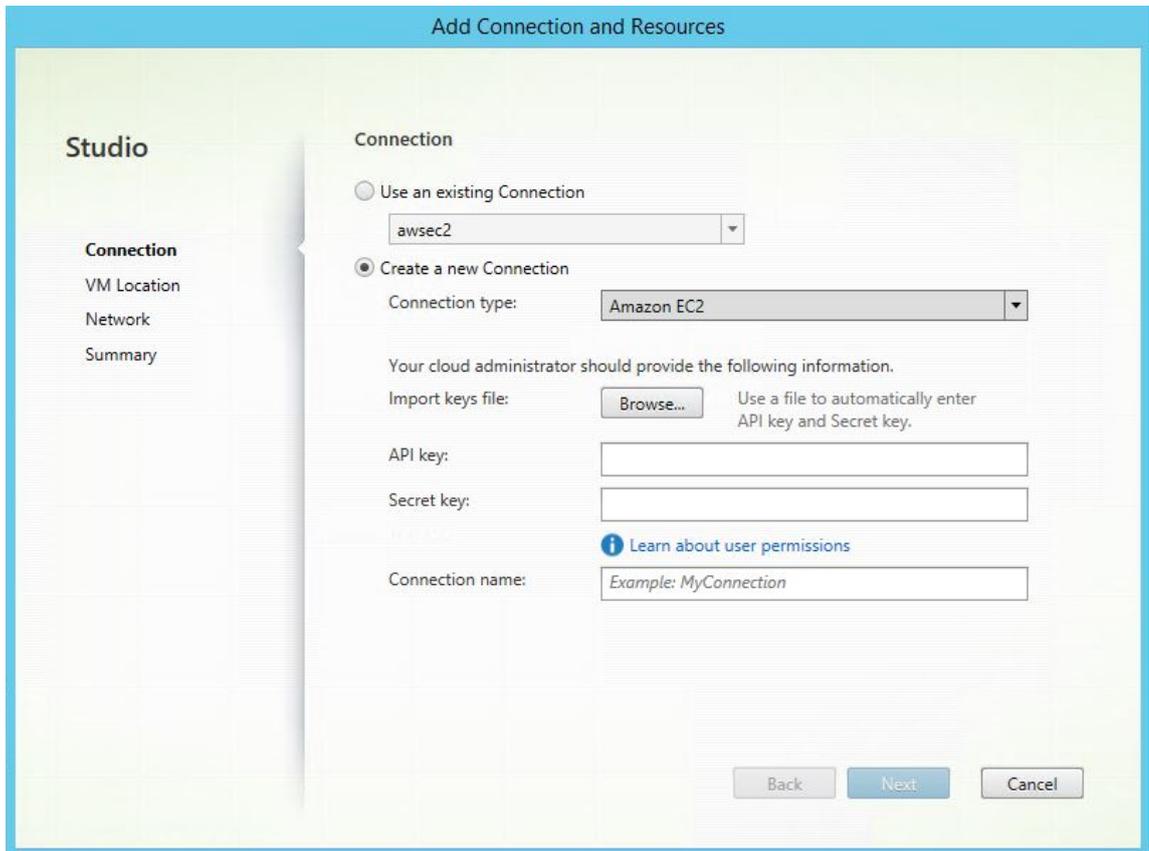
### **Usar MCS para crear máquinas virtuales Linux en AWS**

#### **Paso 1: Cree una conexión de alojamiento con AWS en Citrix Studio**

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



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



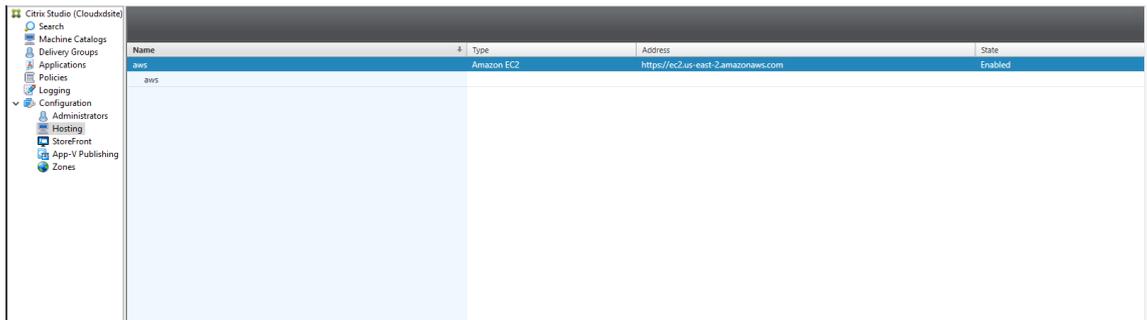
3. Escriba la clave API y la clave secreta de su cuenta de AWS y, también, el nombre de la conexión.

The screenshot shows the 'Add Connection and Resources' dialog in Studio. The 'Connection' section is active, and the 'Create a new Connection' option is selected. The 'Connection type' is set to 'Amazon EC2'. The 'Import keys file' field has a 'Browse...' button. The 'API key' and 'Secret key' fields are empty. The 'Connection name' field has the placeholder text 'Example: MyConnection'. The 'Next' button is highlighted.

La **clave API** es el ID de la clave de acceso y la **clave secreta** es la clave de acceso secreta. Se las considera un par de claves de acceso. Si pierde su clave de acceso secreta, puede eliminar la clave de acceso y crear otra. Para crear una clave de acceso, haga lo siguiente:

- Inicie sesión en los servicios de AWS.
- Vaya a la consola de Identity and Access Management (IAM).
- En el panel de navegación de la izquierda, elija **Users**.
- Seleccione el usuario de destino y desplácese hacia abajo para seleccionar la ficha **Security credentials**.
- Desplácese hacia abajo de nuevo y haga clic en **Create access key**. Aparecerá una ventana.
- Haga clic en **Download .csv file** y guarde la clave de acceso en una ubicación segura.

Aparece una nueva conexión en el panel de alojamiento.



## Paso 2: Prepare una imagen maestra

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

### Paso 2a: Configure cloud-init

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

```
1 echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99
  _hostname.cfg
2 <!--NeedCopy-->
```

Para Ubuntu 18.04, compruebe que estas líneas se encuentran en la sección `system_info` del archivo `/etc/cloud/cloud.cfg`:

```
1 system_info:
2   network:
3     renderers: ['netplan', 'eni', 'sysconfig']
4 <!--NeedCopy-->
```

2. Para utilizar SSH con el objetivo de acceder de forma remota a las máquinas virtuales creadas por MCS en AWS, habilite la autenticación de contraseñas porque no hay ningún nombre de clave asociado a dichas máquinas virtuales. Siga estos procedimientos si es necesario.
  - Modifique el archivo de configuración de cloud-init: `/etc/cloud/cloud.cfg`. Compruebe que la línea **`ssh_pwauth: true`** esté presente. Quite o comente la línea **`set-password`** y las líneas siguientes (si existen).

```
1 users:
2   - default
3 <!--NeedCopy-->
```

- Si piensa usar el usuario predeterminado `ec2-user` o `ubuntu` creado por cloud-init, puede cambiar la contraseña de usuario mediante el comando `passwd`. No se olvide de

la nueva contraseña para poder utilizarla luego al iniciar sesión en las máquinas virtuales creadas por MCS.

- Modifique el archivo `/etc/ssh/sshd_config` para comprobar que esta línea está presente:

```
1 PasswordAuthentication yes
2 <!--NeedCopy-->
```

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

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

### Nota:

Para utilizar un VDA que se ejecuta como una VM de plantilla, omita este paso.

Antes de instalar el paquete de Linux VDA en la VM de plantilla, instale .NET Core Runtime 3.1.

Para obtener más información, consulte [Información general de la instalación](#).

En función de su distribución de Linux, ejecute el siguiente comando para configurar el entorno para Linux VDA:

### Para RHEL/CentOS:

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

### Para Ubuntu:

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2
3 apt-get install -f
4 <!--NeedCopy-->
```

### Para SUSE 12:

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

## Paso 2c: Habilite repositorios para instalar el paquete `tdb-tools` Para el servidor de RHEL 7:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

### Para la estación de trabajo de RHEL 7:

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

**Paso 2d: Instale el repositorio EPEL que contiene ntfs-3g** Instale el repositorio EPEL en RHEL 6/CentOS 6, RHEL 7/CentOS 7 para que la ejecución posterior de `deploymcs.sh` instale el paquete `ntfs-3g` que contiene.

**Paso 2e: Instale manualmente ntfs-3g en SUSE 12** En la plataforma SUSE 12, no hay ningún repositorio que ofrezca `ntfs-3g`. Debe descargar el código fuente, compilarlo e instalar `ntfs-3g` de forma manual:

1. Instale el sistema de compilación GNU Compiler Collection (GCC) y cree el paquete:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. Descargue el paquete `ntfs-3g`.

3. Descomprima el paquete `ntfs-3g`:

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. Escriba la ruta del paquete `ntfs-3g`:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

5. Instale `ntfs-3g`:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

**Paso 2f: Configure el entorno en tiempo de ejecución** Antes de ejecutar `deploymcs.sh`, haga lo siguiente:

- Cambie variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` contiene variables para configurar MCS y Linux VDA. He aquí algunas de las variables, de las cuales `dns` y `AD_INTEGRATION` deben definirse:

**Nota:** Si una variable se puede definir con varios valores, coloque los valores entre comillas simples y sepárelos con un espacio. Por ejemplo: `LDAP_LIST='aaa.lab:389 bbb.lab:389'`.

- `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben utilizar las configuraciones existentes del VDA que se ejecuta actualmente. Si se define con el valor `Y`, los archivos de configuración de las máquinas creadas por MCS son los mismos

que los del VDA que se ejecuta actualmente. Sin embargo, aún debe configurar las variables `dns` y `AD_INTEGRATION`. El valor predeterminado es N, lo que significa que los archivos de configuración de máquinas creadas por MCS están determinados por plantillas de configuración de la imagen maestra.

- `dns`: Establece la dirección IP de DNS
- `AD_INTEGRATION`: Establece Winbind o SSSD (SSSD no se admite en SUSE)
- `WORKGROUP`: Establece el nombre del grupo de trabajo, que es el nombre NetBIOS (distingue entre mayúsculas y minúsculas) si se configura en AD. De lo contrario, de forma predeterminada, es el nombre de dominio.

- En la máquina de la plantilla, agregue líneas de comandos al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar los valores del Registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina aprovisionada con MCS.

Cada línea del archivo `/etc/xdl/mcs/mcs_local_setting.reg` es un comando para configurar o actualizar un valor del Registro.

Por ejemplo: Puede agregar las siguientes líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar un archivo del Registro respectivamente:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
   v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
   VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
   x00000003"
2 <!--NeedCopy-->
```

## Paso 2g: Cree una imagen maestra

1. Ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Opcional) En la máquina virtual de la plantilla, actualice las plantillas de configuración para personalizar los archivos `/etc/krb5.conf`, `/etc/samba/smb.conf` y `/etc/sss/sss.conf` pertinentes en todas las máquinas virtuales creadas.

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

Para los usuarios de SSSD, actualice las plantillas `/etc/xdl/mcs/sss.conf.tmpl`, `/etc/xdl/mcs/sss_krb5.conf.tmpl` y `/etc/xdl/mcs/sss_smb.conf.tmpl`.

**Nota:** Mantenga el formato utilizado en los archivos de plantilla y utilice variables como `$WORKGROUP`, `$REALM`, `$realm` y `$AD_FQDN`.

3. Instale aplicaciones en la VM de plantilla y apague la VM de plantilla desde el portal de AWS EC2. Compruebe que el estado de la instancia de la VM de plantilla es **Detenido**.
4. Haga clic con el botón secundario en la VM de plantilla y seleccione **Imagen > Crear imagen**. Escriba la información y realice los ajustes necesarios. Haga clic en **Crear imagen**.

**Create Image** [X]

Instance ID ⓘ i-011f...

Image name ⓘ

Image description ⓘ

No reboot ⓘ

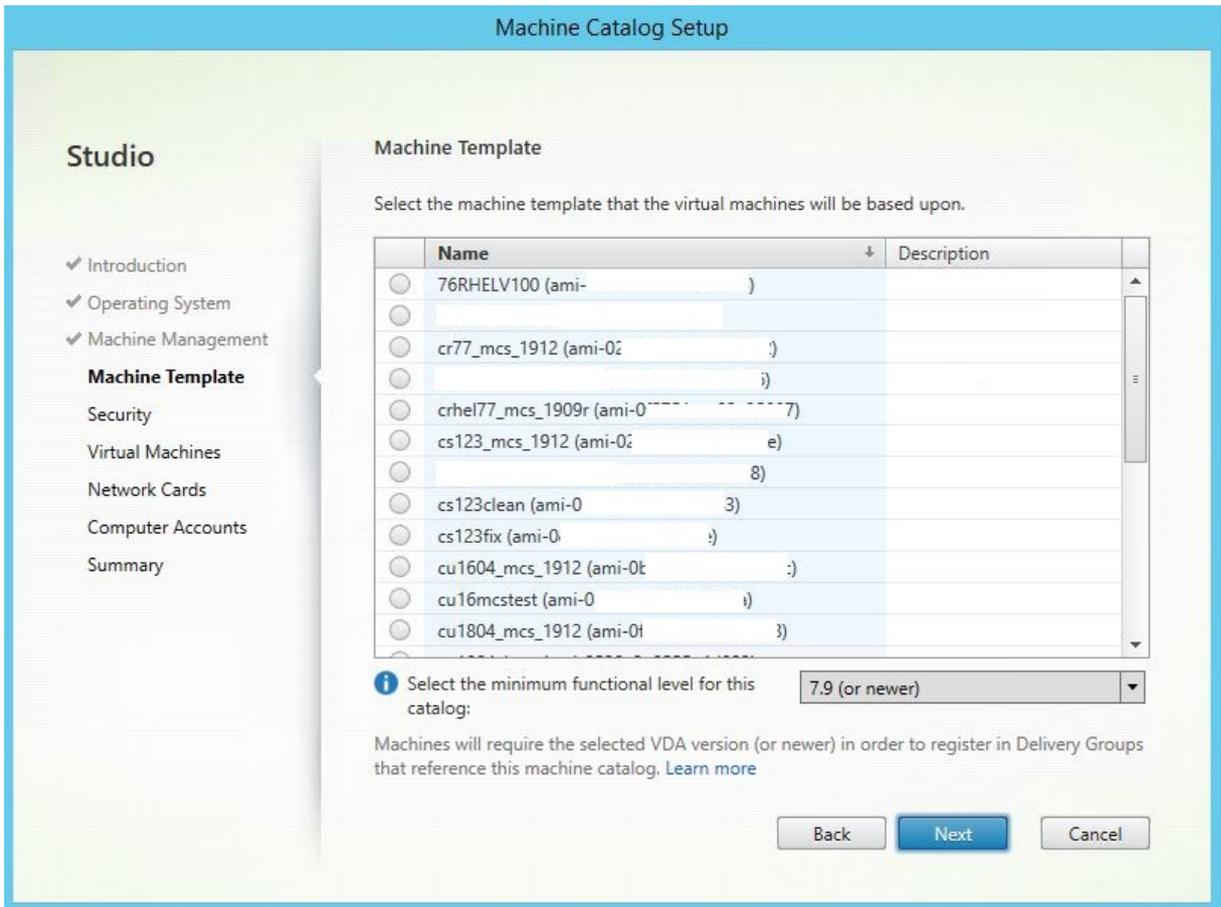
Instance Volumes

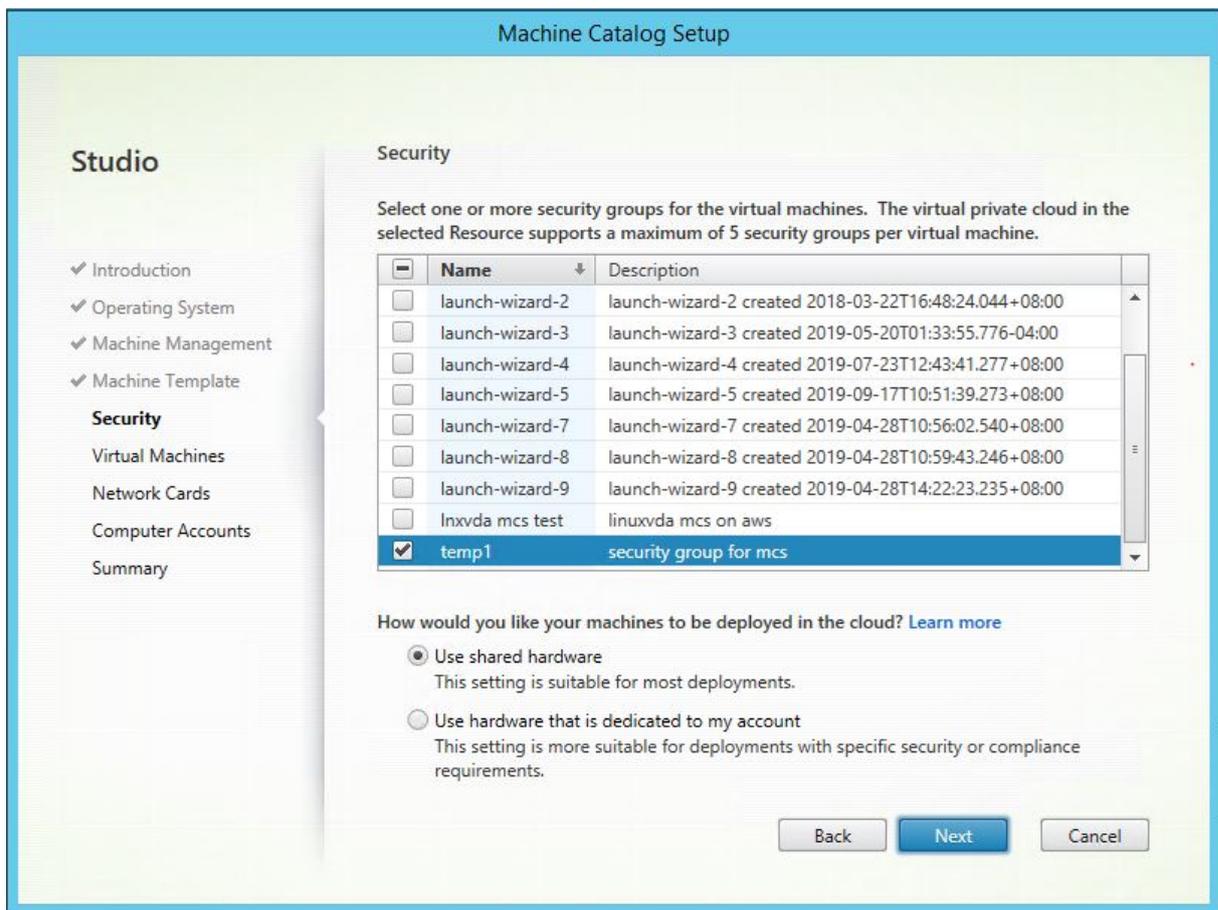
Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-02...	40	General Purpose SSD (gp2)	120 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Total size of EBS Volumes: 40 GiB  
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

### Paso 3: Cree un catálogo de máquinas

En Citrix Studio, cree un catálogo de máquinas y especifique la cantidad de máquinas virtuales que se van a crear en el catálogo. Al crear el catálogo de máquinas, elija la plantilla de la máquina (la imagen maestra que creó anteriormente) y seleccione uno o varios grupos de seguridad.





Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte [Crear un catálogo de máquinas mediante Studio](#).

#### Paso 4: Cree un grupo de entrega

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. Especifica los usuarios que pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios. Para obtener más información, consulte [Crear grupos de entrega](#).

#### Usar MCS para actualizar la versión de Linux VDA

Para usar MCS para actualizar la versión de su Linux VDA, haga lo siguiente:

1. Actualice su Linux VDA en la plantilla de máquina:

##### Para RHEL 7/CentOS 7:

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm
2 <!--NeedCopy-->
```

#### Para RHEL 6/CentOS 6:

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm
2 <!--NeedCopy-->
```

#### Para SUSE 12:

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

#### Para Ubuntu 16.04:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu16.04_amd64.deb
2 <!--NeedCopy-->
```

#### Para Ubuntu 18.04:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu18.04_amd64.deb
2 <!--NeedCopy-->
```

2. Modifique **/etc/xdl/mcs/mcs.conf** y **/etc/xdl/mcs/mcs\_local\_setting.reg**.
3. Tome una nueva instantánea.
4. En Citrix Studio, seleccione la nueva instantánea para actualizar su catálogo de máquinas. Espere a que se reinicie cada máquina. No reinicie ninguna máquina manualmente.

## Configurar Delivery Controllers

May 15, 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**:

```
1 .\Update-BrokerServiceConfig.ps1
2 <!--NeedCopy-->
```

#### Sugerencia:

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:

```
1 Set-ExecutionPolicy Unrestricted
2 <!--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.

#### Nota:

Linux VDA no admite el cifrado Secure ICA. Al habilitar Secure ICA en Linux VDA, se produce un error en el inicio de sesión.

## 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\BrokerServiceConfig.xml**.

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

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

## Configurar Linux VDA

November 3, 2021

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

### Consejo:

El script `xdlcollect` de Bash que se usa para recopilar registros está integrado en el software de Linux VDA y se encuentra en `/opt/Citrix/VDA/bin`. Después de instalar Linux VDA, puede ejecutar el comando `bash /opt/Citrix/VDA/bin/xdlcollect.sh` para recopilar registros.

Una vez completada la recopilación de registros, se genera un archivo de registro comprimido en la misma carpeta que el script. `xdlcollect` puede preguntarle si quiere cargar o no el archivo de registro comprimido en Citrix Insight Services (CIS). Si está de acuerdo, `xdlcollect` devuelve un `upload_ID` una vez completada la carga. La carga no elimina el archivo de registro comprimido de su máquina local. Otros usuarios pueden usar este `upload_ID` para acceder al archivo de registro en CIS.

## Integrar NIS en Active Directory

November 3, 2021

En este tema, se describe cómo integrar NIS con Windows Active Directory (AD) en Linux VDA mediante SSSD. Linux VDA se considera un componente de Citrix Virtual Apps and Desktops. 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](#).

¿Qué es 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 al seguir las instrucciones de este artículo:

- RHEL 7.7 y versiones posteriores
- CentOS 7.7 y versiones posteriores

**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:

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

Establezca el dominio NIS:

```
1 ypdomainname nis.domain
2 echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
3 <!--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`:

```
1 sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
  nis.domain --enablemkhomedir --update
2 <!--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:

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

Compruebe que la configuración de NIS es correcta:

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

Valide que la información de la cuenta esté disponible desde el servidor NIS:

```
1 getent passwd nisaccount
2 <!--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:

```
--enablekrb5kcdns --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/sss/sss.conf** A continuación, se ofrece un ejemplo de configuración de **sss.conf** (se pueden agregar opciones adicionales, según sea necesario):

```

1 [sss]
2 config_file_version = 2
3 domains = EXAMPLE
4 services = nss, pam
5
6 [domain/EXAMPLE]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9 re_expression = (((?P<domain>[^\[]+)\)(?P<name>.+))|((?P<name>[^\@]+)@
10 (?P<domain>.+))|(^(?P<name>[^\[]+)\))
11 id_provider = proxy
12 proxy_lib_name = nis
13 auth_provider = ad
14 access_provider = ad
15 # Should be specified as the long version of the Active Directory
16 # domain.
17 ad_domain = EXAMPLE.COM
18 # Kerberos settings
19 krb5_ccachedir = /tmp
20 krb5_ccname_template = FILE:%d/krb5cc_%U
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
26 # side
27 default_shell = /bin/bash
28 fallback_homedir = /home/%d/%u
29
30 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
31 # available
32 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
33 <!--NeedCopy-->

```

Reemplace **ad.domain.com**, **server.ad.example.com** por el valor correspondiente. Para obtener más información, consulte [sss-ad\(5\) - Linux man page](#).

Establezca la pertenencia y los permisos de archivos en **sss.conf**:

```

chown root:root /etc/sss/sss.conf
chmod 0600 /etc/sss/sss.conf
restorecon /etc/sss/sss.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:

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
6 <!--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:

```
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 vale de concesión de vales de la cuenta de la máquina se ha almacenado en caché:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo getent passwd DOMAIN\username
2 <!--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.

```
1 sudo ssh localhost -l DOMAIN\username
2
3 id -u
4 <!--NeedCopy-->
```

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

```
1 ls /tmp/krb5cc_{
2   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:

```
1 klist
2 <!--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.

## **Limitación**

Linux VDA no admite el inicio de varias instancias simultáneas de la misma aplicación procedentes de un solo usuario.

## **Problemas conocidos**

A continuación, se presentan los problemas conocidos en la publicación de aplicaciones:

- 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, Metacity 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/title/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.

## Acceso con Remote PC

November 3, 2021

### Introducción

Acceso con Remote PC es una extensión de Citrix Virtual Apps and Desktops. Permite a las organizaciones conceder a los empleados un acceso fácil a sus equipos físicos de oficina de forma remota y segura. Si los usuarios pueden acceder a sus PC de oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para hacer su trabajo.

Acceso con Remote PC utiliza los mismos componentes de Citrix Virtual Apps and Desktops que facilitan aplicaciones y escritorios virtuales. Los requisitos y el proceso de implementación y configuración de Acceso con Remote PC son los mismos que los necesarios para implementar Citrix Virtual Apps and Desktops para la entrega de recursos virtuales. Esta uniformidad ofrece una experiencia de administración homogénea y unificada. Los usuarios disfrutan de la mejor experiencia posible al utilizar Citrix HDX para la entrega de sesiones de PC de oficina.

Para obtener más información, consulte [Acceso con Remote PC](#) en la documentación de Citrix Virtual Apps and Desktops.

### Configuración

Para entregar sesiones de PC Linux, instale Linux VDA en los equipos correspondientes, cree un catálogo de máquinas de tipo **Acceso con Remote PC** y cree un grupo de entrega para que los equipos

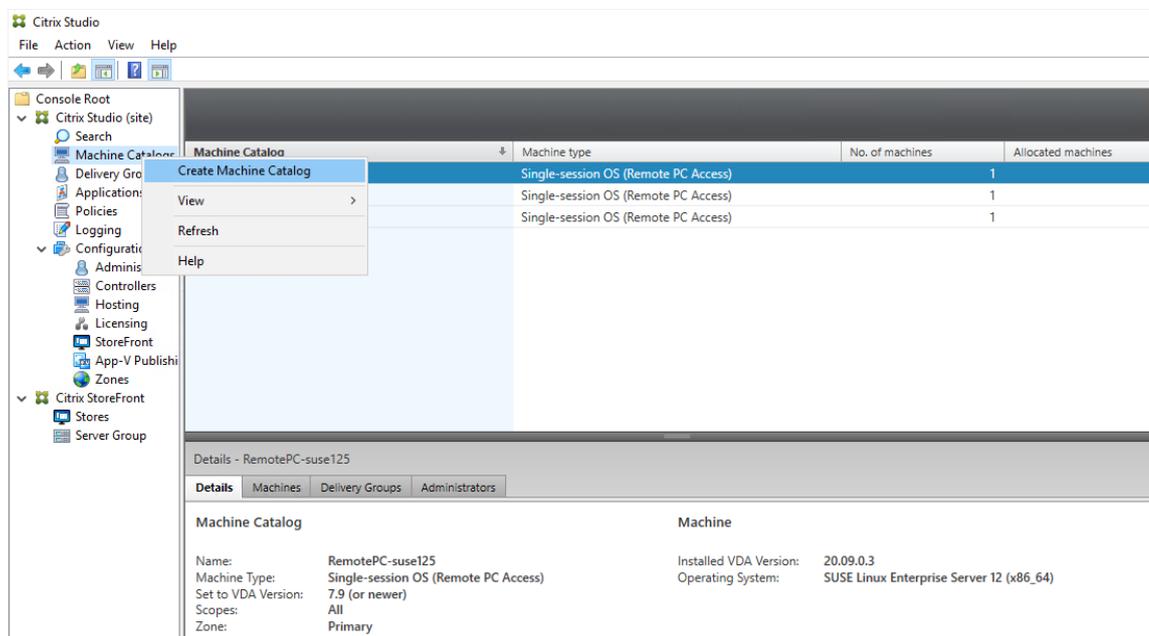
del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso. En la siguiente sección, se muestra el procedimiento:

### Paso 1 - Instalar Linux VDA en los equipos de destino

Se recomienda utilizar [Easy Install](#) para instalar Linux VDA. Durante la instalación, establezca el valor de la variable `CTX_XDL_VDI_MODE` en `Y`.

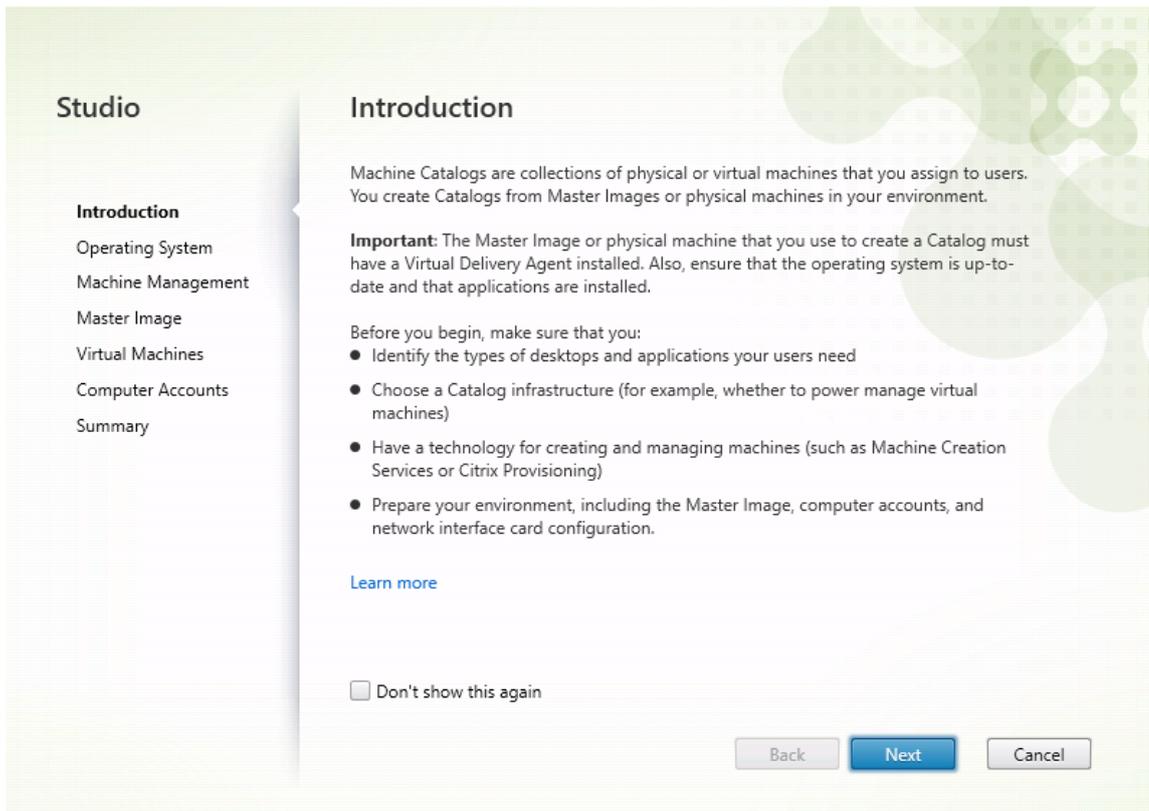
### Paso 2 - Crear un catálogo de máquinas de tipo Acceso con Remote PC

1. En Citrix Studio, haga clic con el botón secundario en **Catálogos de máquinas** y seleccione **Crear catálogo de máquinas** en el menú contextual.



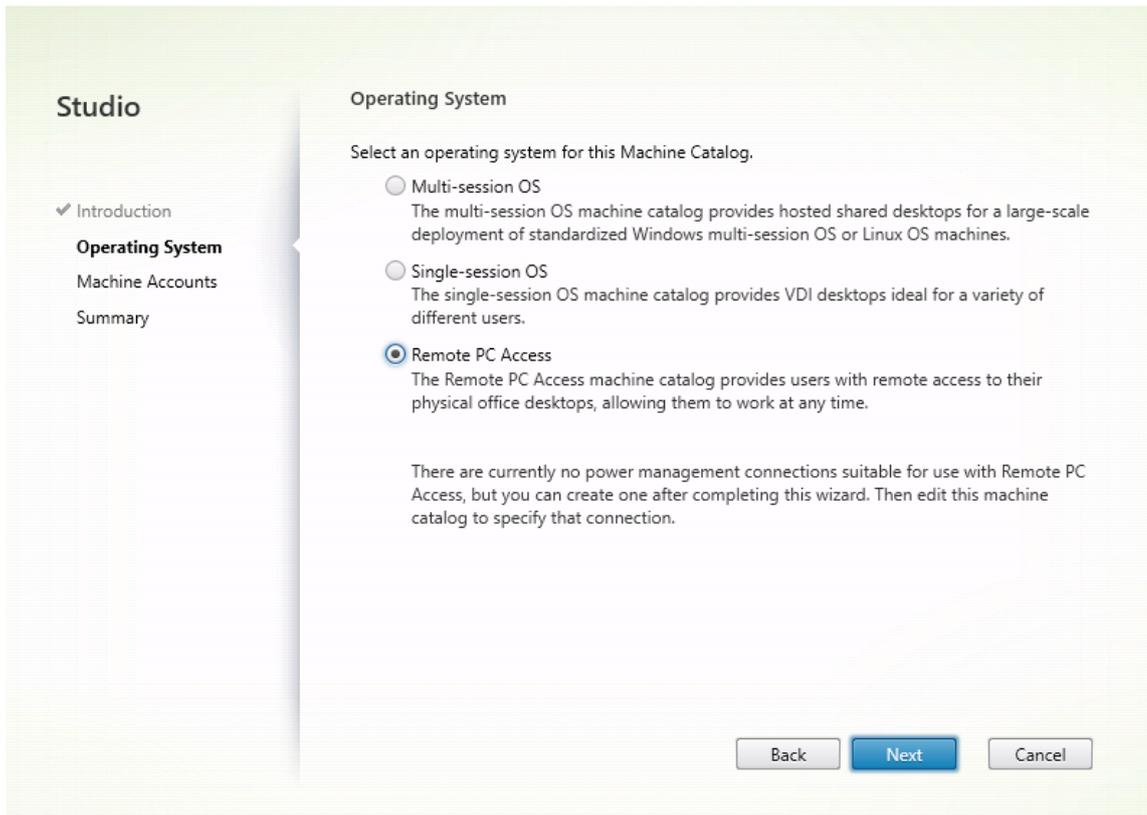
2. En la página **Introducción**, haga clic en **Siguiente**.

Machine Catalog Setup



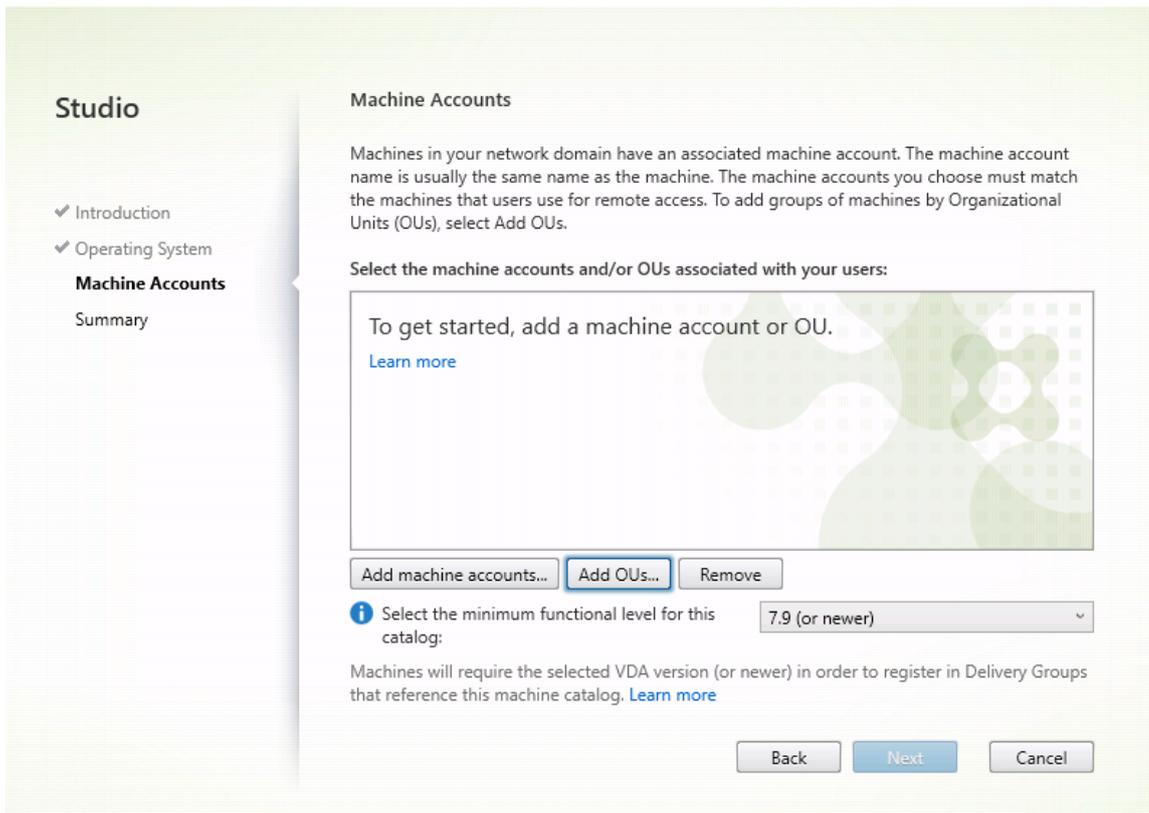
3. En la página **Sistema operativo**, seleccione **Acceso con Remote PC**.

Machine Catalog Setup



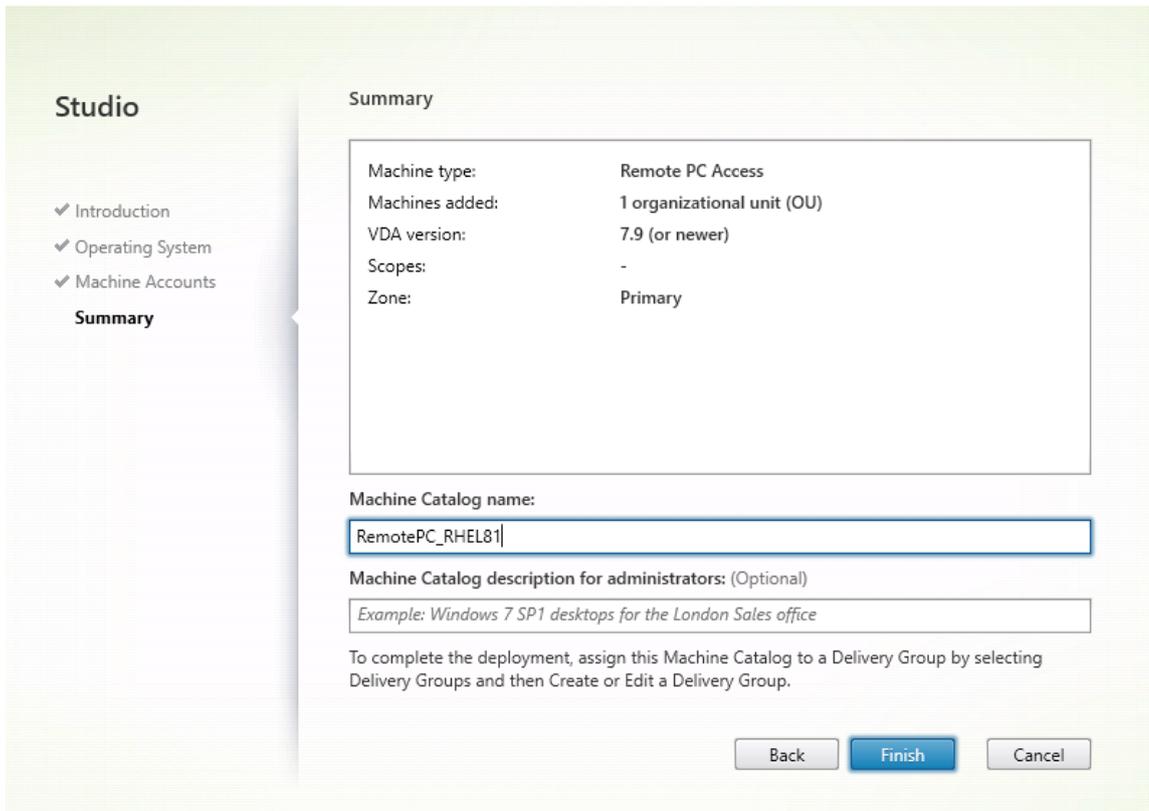
4. Haga clic en **Agregar unidades organizativas** para seleccionar las unidades organizativas que contendrán los equipos de destino o haga clic en **Agregar cuentas de máquina** para agregar máquinas individuales al catálogo de máquinas.

Machine Catalog Setup

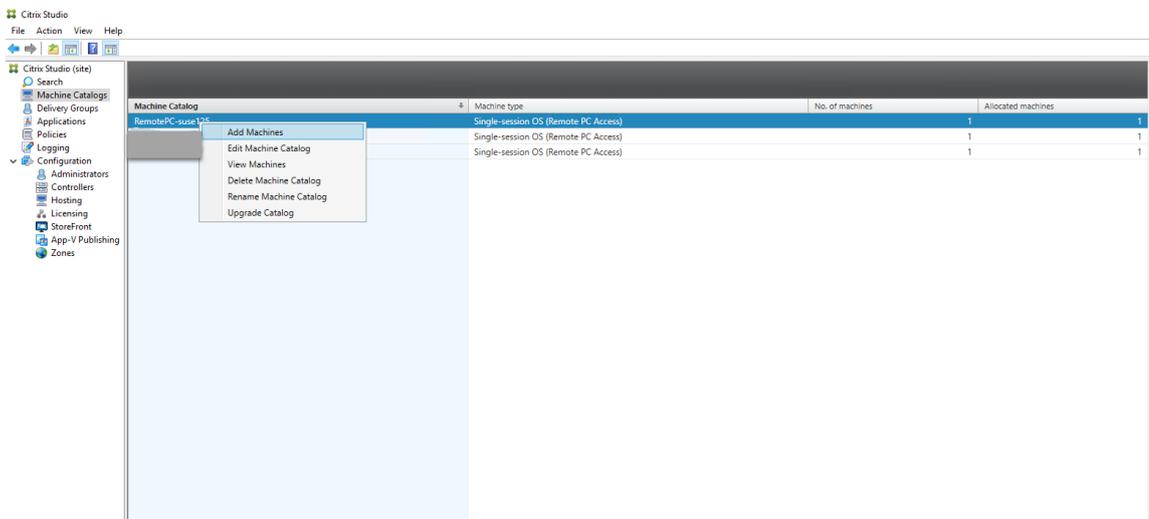


5. Asigne un nombre al catálogo de máquinas.

Machine Catalog Setup

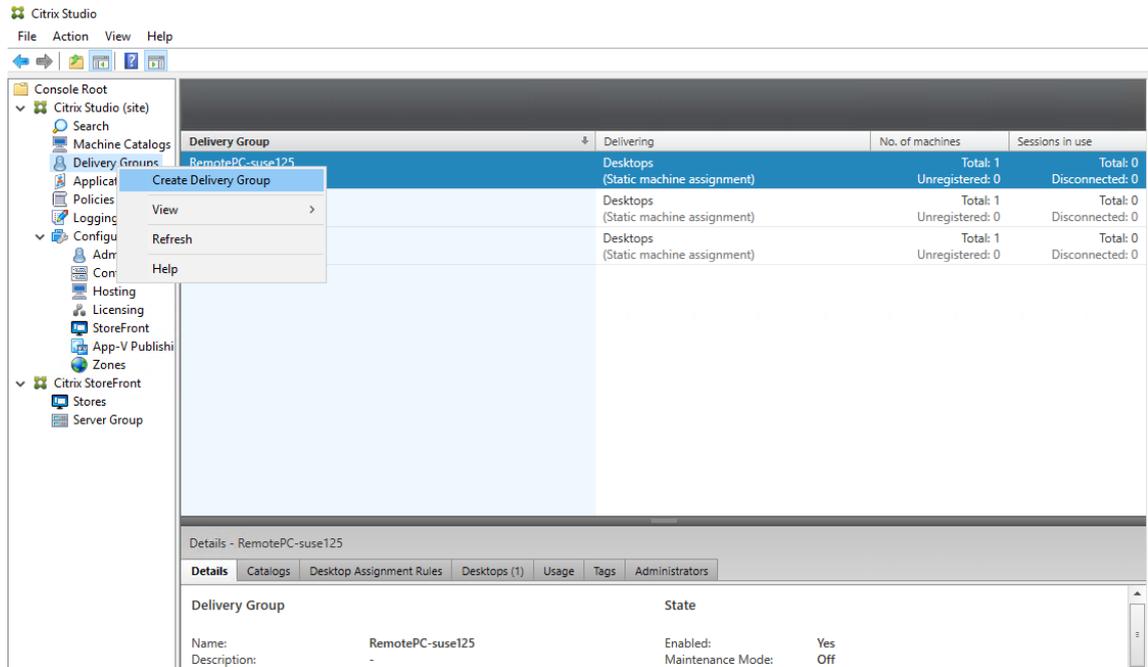


- (Opcional) Haga clic con el botón secundario en el catálogo de máquinas para realizar las operaciones relevantes.

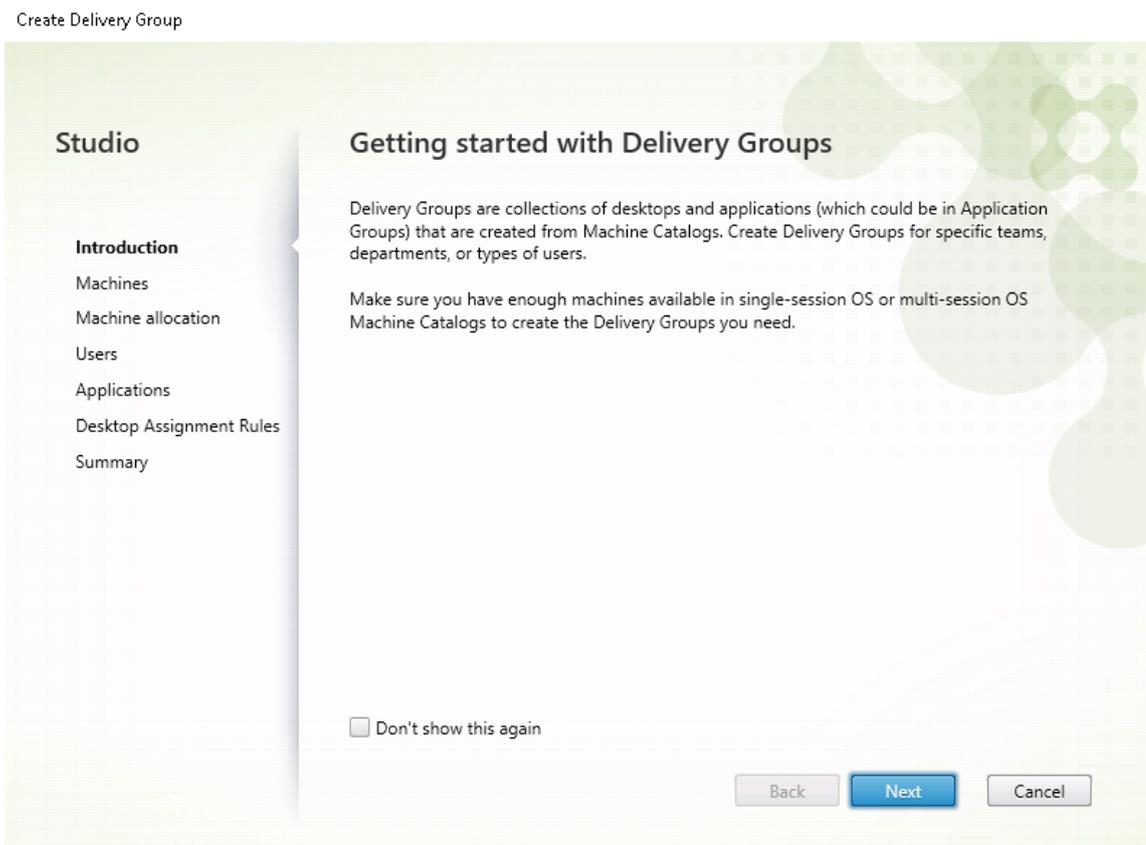


### Paso 3 - Crear un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso

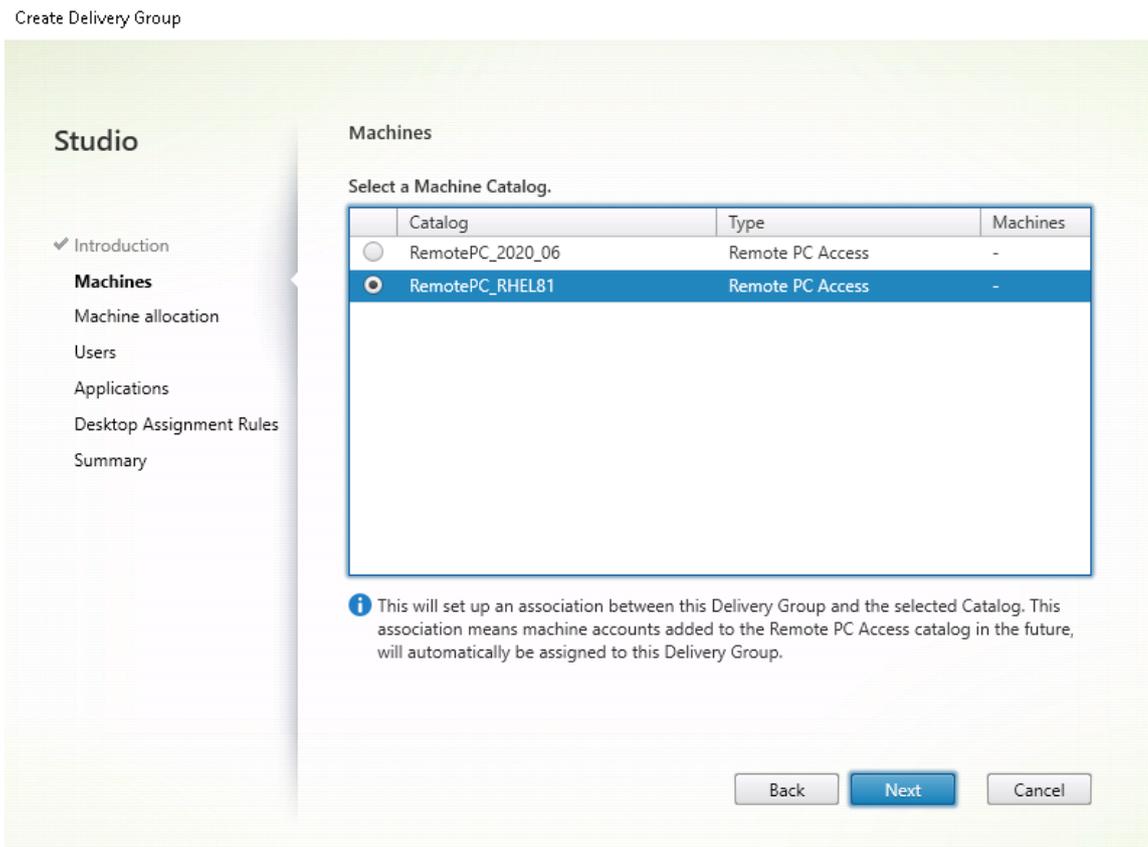
1. En Citrix Studio, haga clic con el botón secundario en **Grupos de entrega** y seleccione **Crear grupo de entrega** en el menú contextual.



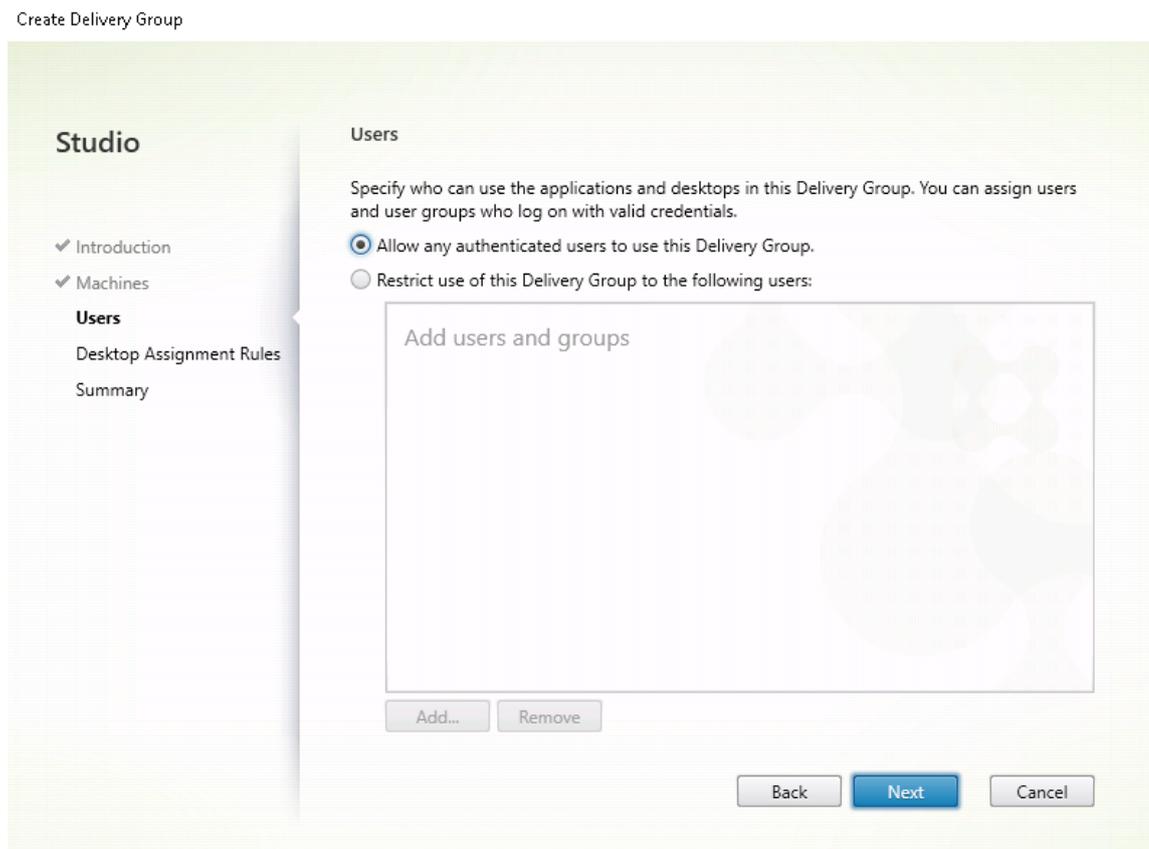
2. Haga clic en **Siguiente** en la página **Introducción a los grupos de entrega**.



3. Seleccione el catálogo de máquinas creado en el paso 2 para asociarlo al grupo de entrega.



4. Agregue usuarios que puedan acceder a los PC del catálogo de máquinas. Los usuarios que agregue pueden usar la aplicación Citrix Workspace en un dispositivo cliente para acceder a los PC de forma remota.



## Consideraciones

Estas consideraciones son específicas de Linux VDA:

- Utilice Linux VDA en máquinas físicas solo en modo no 3D. Debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no se puede oscurecer completamente y muestra las actividades de la sesión cuando el modo HDX 3D está habilitado. Mostrar esta pantalla representa un riesgo para la seguridad.
- Con máquinas Linux físicas, utilice catálogos de máquinas de tipo SO de sesión única.
- La funcionalidad Wake on LAN integrada no está disponible para máquinas Linux.
- La asignación automática de usuarios no está disponible para máquinas Linux. Con la asignación automática de usuarios, los usuarios se asignan automáticamente a sus equipos cuando inician sesión localmente en los equipos. Este inicio de sesión se produce sin intervención del administrador. La aplicación Citrix Workspace, ejecutada en el dispositivo cliente, permite a los usuarios acceder a las aplicaciones y los datos almacenados en el equipo de la oficina desde la sesión de escritorio de acceso con Remote PC.
- Si los usuarios ya han iniciado sesión en sus equipos localmente, los intentos de iniciarlos desde StoreFront fallan.

- Las opciones de ahorro de energía no están disponibles para las máquinas Linux.

## Más recursos

A continuación, se muestran otros recursos para acceso con Remote PC:

- Guía de diseño de soluciones: [Remote PC Access Design Decisions](#).
- Ejemplos de arquitecturas de acceso con Remote PC: [Reference Architecture for Citrix Remote PC Access Solution](#).

## Imprimir

November 3, 2021

En este artículo, se ofrecen los procedimientos recomendados de impresión.

## Instalación

Linux VDA requiere los filtros **cups** y **foomatic**. Los filtros se instalan al instalar el VDA. También puede instalar los filtros manualmente en función de la distribución. Por ejemplo:

### En RHEL 7:

```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic-filters
4 <!--NeedCopy-->
```

### En RHEL 6:

```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic
4 <!--NeedCopy-->
```

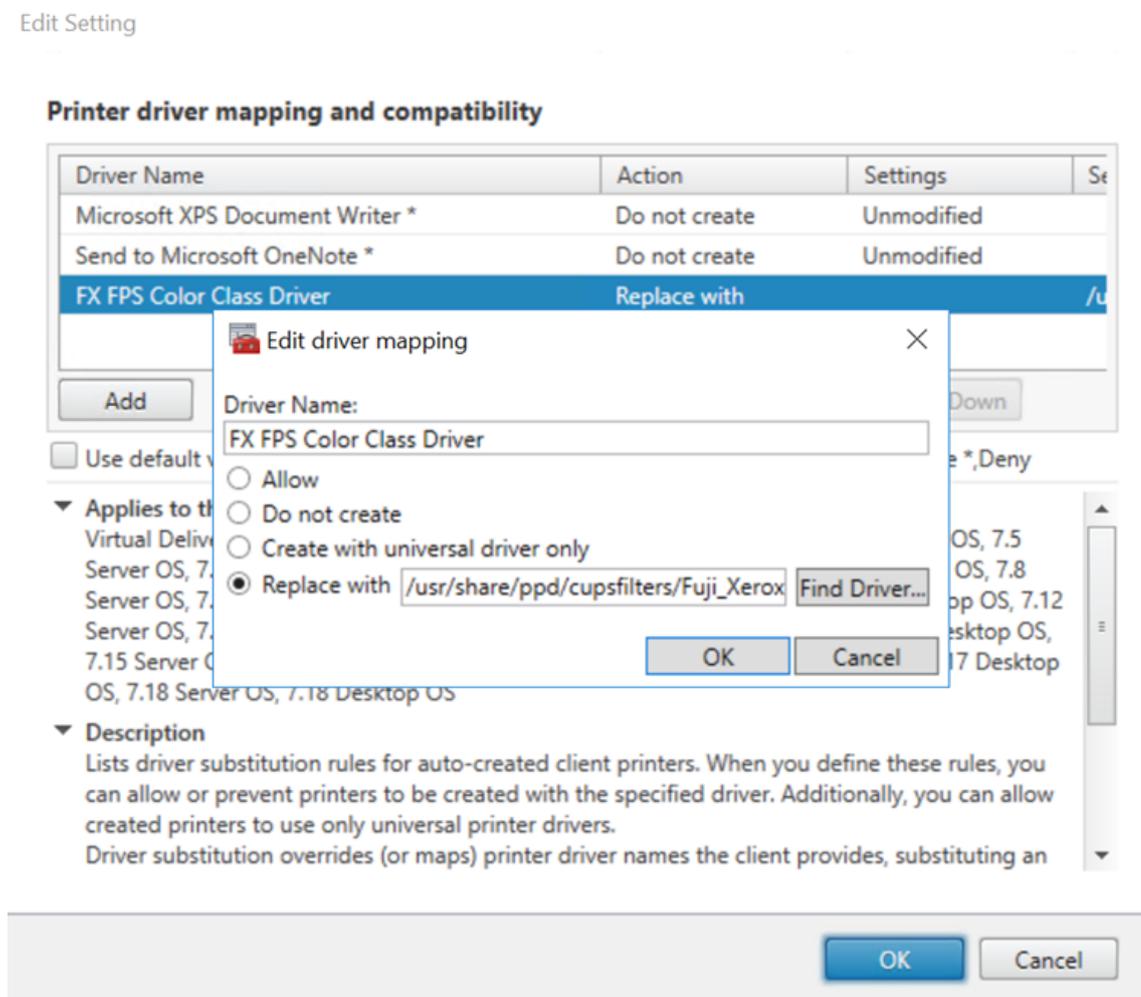
## Configuración

Existen tres tipos de controlador de impresora universal suministrados por Citrix (postscript, pcl5 y pcl6). Sin embargo, es posible que el controlador de impresora universal no sea compatible con la impresora del cliente. En este caso, la única opción posible en versiones anteriores era modificar el archivo de configuración `~/.CtxlpProfile$CLIENT_NAME`. A partir de la versión 1906, en su lugar, puede

configurar la directiva **Asignación y compatibilidad de controladores de impresora** en Citrix Studio.

Para configurar la directiva **Asignación y compatibilidad de controladores de impresora** en Citrix Studio.

1. Seleccione la directiva **Asignación y compatibilidad de controladores de impresora**.
2. Haga clic en **Agregar**.
3. Introduzca el **nombre del controlador** de la impresora del cliente. Si utiliza la aplicación Citrix Workspace para Linux, introduzca el nombre de la impresora.
4. Elija **Reemplazar por** y escriba la ruta absoluta del archivo de controlador en el VDA.



**Nota:**

- Solo se admiten archivos de controlador PPD.
- No se admiten otras opciones de la directiva **Asignación y compatibilidad de contro-**

**ladores de impresora.** Solamente **Reemplazar por** surte efecto.

## 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.

- 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

Cuando la impresión no funcione correctamente, compruebe el demonio de impresión, **ctxlpmngt**, y el marco CUPS.

El demonio de impresión, **ctxlpmngt**, es un proceso que se ejecuta para cada sesión y debe ejecutarse durante toda la sesión. Ejecute el siguiente comando para comprobar que el demonio de impresión se está ejecutando. Si **ctxlpmngt** no se está ejecutando, inicie **ctxlpmngt** manualmente desde una línea de comandos.

```
1 ps -ef | grep ctxlpmngt
2 <!--NeedCopy-->
```

Si la impresión sigue sin funcionar, compruebe el marco CUPS. El servicio **ctxcups** se usa para la administración de impresoras y se comunica con el marco CUPS de Linux. Es un proceso único por máquina y se puede comprobar mediante el siguiente comando:

```
1 service ctxcups status
2 <!--NeedCopy-->
```

## Pasos adicionales para recopilar registros de CUPS

Para recopilar registros de CUPS, ejecute los siguientes comandos para configurar el archivo de servicio de CUPS. De lo contrario, los registros de CUPS no se pueden registrar en **hdx.log**:

```
1 sudo service cups stop
2
3 sudo vi /etc/systemd/system/printer.target.wants/cups.service
4
5 PrivateTmp=false
6
7 sudo service cups start
8
9 sudo systemctl daemon-reload
10 <!--NeedCopy-->
```

### Nota:

Esta configuración solo sirve para recopilar el registro completo de impresión cuando surja algún problema. En circunstancias normales, no se recomienda esta configuración 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 **~/.CtulpProfile\$CLIENT\_NAME**:

```
1 [DEFAULT_PRINTER]
2
3 printername=
4
5 model=
6
7 ppdpath=
8
9 drivertype=
10 <!--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 del 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**:

```
1  lpinfo -m
2
3  ...
4
5  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
6
7  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
8  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
9
10 <!--NeedCopy-->
```

A continuación, puede configurar el modelo para que coincida con la impresora:

```
1  model=xerox/ph3115.ppd.gz
2  <!--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`:

```
1  ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
2  <!--NeedCopy-->
```

- Existen tres tipos de controlador de impresora universal suministrados por Citrix (postscript, pcl5 y pcl6). Puede configurar el tipo de controlador en función de las propiedades de la impresora.

Por ejemplo, si el tipo de controlador de impresora predeterminado del cliente es PCL5, establezca **drivertype** en:

```
1  drivertype=pcl5
2  <!--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:

1. Inicie sesión en una sesión de escritorio publicada.
2. Ejecute el comando **vi ~/.CtxlpProfile\$CLIENT\_NAME**.
3. Agregue el siguiente campo al archivo de cola de impresión guardado en Linux VDA:

```
1 deletespoolfile=no
2 <!--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/\$slogon\_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 en la impresora del cliente con otro controlador de impresora.

8. Cambie la impresora asignada para utilizar otro controlador de impresora. En el ejemplo siguiente se utiliza la impresora del cliente de 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:

```
1 localhost:631
2 <!--NeedCopy-->
```

- c) Elija la impresora asignada **CitrixUniversalPrinter:\$ClientName:app/dsk\$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 los campos **Make** y **Model**, elija otro controlador de impresora del controlador UPD de Citrix. Por ejemplo, si está instalada la impresora virtual CUPS-PDF, puede seleccionar el controlador de impresora genérica CUPS-PDF. Guarde el cambio.
- 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 el controlador recién seleccionado.

## 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:

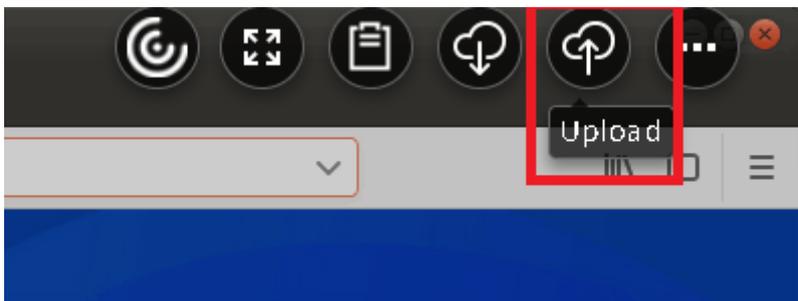
```
1 <Policy default>
2
3     # Job/subscription privacy...
4
5     JobPrivateAccess default
6
7     JobPrivateValues default
8
9     SubscriptionPrivateAccess default
10
11    SubscriptionPrivateValues default
12
13    ... ..
```

```
14
15     <Limit Create-Printer-Subscription>
16
17         Require user @OWNER
18
19         Order deny,allow
20
21     </Limit>
22
23     <Limit All>
24
25         Order deny,allow
26
27     </Limit>
28
29 </Policy>
30 <!--NeedCopy-->
```

## Transferencia de archivos

November 3, 2021

Se admite la transferencia de archivos entre el Linux VDA y el dispositivo cliente. Esta función está disponible cuando el dispositivo cliente ejecuta un explorador web que admite el atributo HTML5 sandbox. El atributo sandbox de HTML5 permite a los usuarios acceder a las aplicaciones y escritorios virtuales mediante la aplicación Citrix Workspace para HTML5 y para Chrome. Desde las sesiones publicadas, puede utilizar la barra de herramientas de la aplicación Citrix Workspace para cargar y descargar archivos entre Linux VDA y el dispositivo cliente. Por ejemplo, puede hacer clic en el icono **Cargar** en la barra de herramientas, elegir un archivo en el dispositivo cliente, y cargar el archivo al Linux VDA.



### Nota:

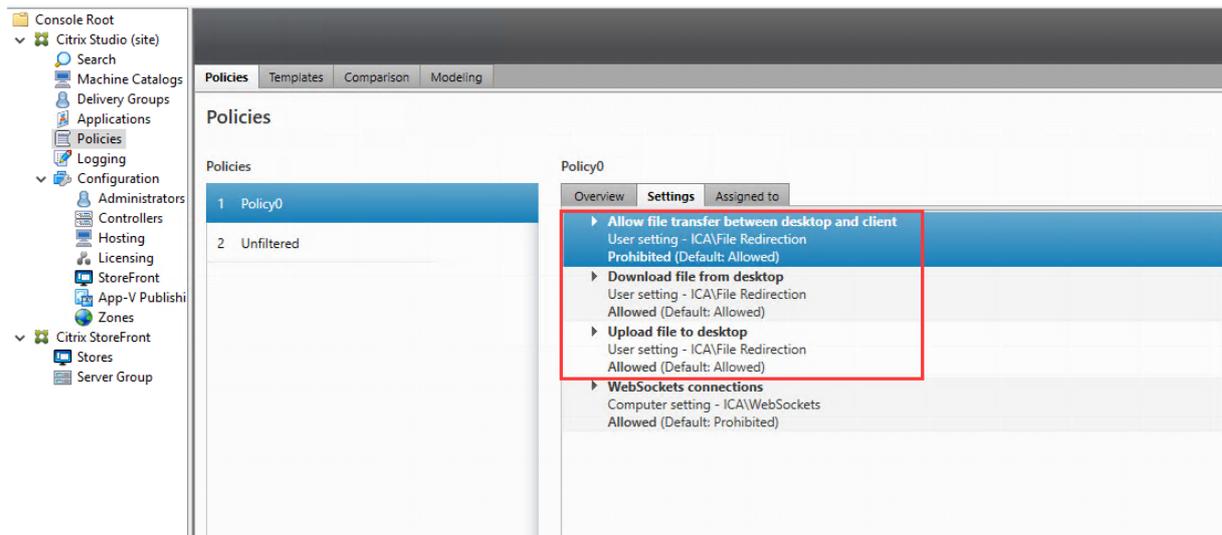
Esta función está disponible para Red Hat 7.7, CentOS 7.6, SUSE 12.3, Ubuntu 16.04 y Ubuntu 18.04.

Para usar esta función, asegúrese de que la barra de herramientas de la aplicación Citrix Work-

space está habilitada.

## Directivas de transferencia de archivos

Puede utilizar Citrix Studio para definir las directivas de transferencia de archivos. De forma predeterminada, la transferencia de archivos está habilitada.



Descripciones de las directivas:

- **Permitir transferencia de archivos entre escritorio y cliente.** Permite o impide que los usuarios transfieran archivos entre una sesión virtual de Citrix Virtual Apps and Desktops y sus dispositivos.
- **Descargar archivos desde el escritorio.** Permite o impide que los usuarios descarguen archivos desde una sesión de Citrix Virtual Apps and Desktops a su dispositivo.
- **Cargar archivos al escritorio.** Permite o impide que los usuarios carguen archivos desde sus dispositivos a una sesión virtual de Citrix Virtual Apps and Desktops.

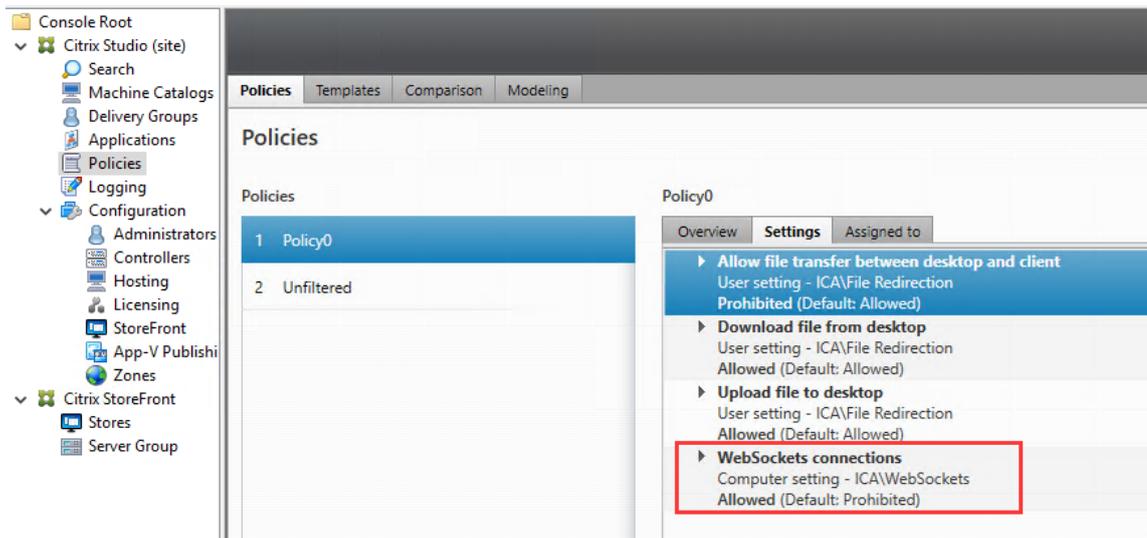
### Nota:

Para asegurarse de que las directivas **Descargar archivos desde el escritorio** y **Cargar archivos al escritorio** surtan efecto, establezca la directiva **Permitir transferencia de archivos entre escritorio y cliente** en **Sí**.

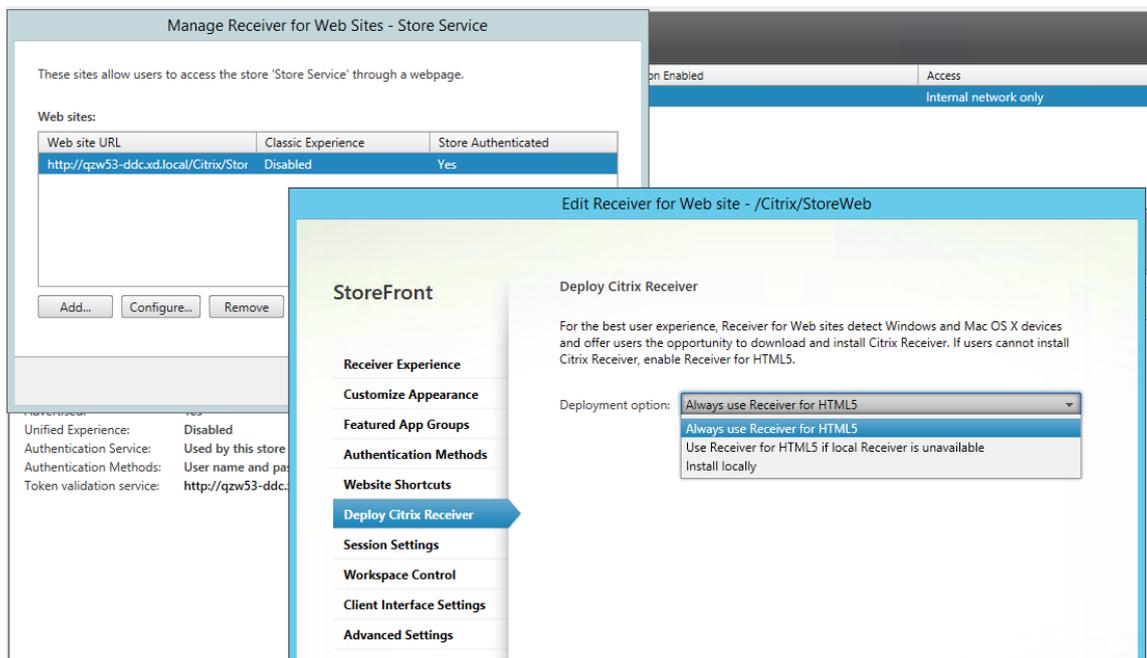
## Uso

Para utilizar la función de transferencia de archivos a través de la aplicación Citrix Workspace para HTML5:

1. En Citrix Studio, establezca la directiva **Conexiones de WebSockets** en **Permitida**.



2. En Citrix Studio, habilite la transferencia de archivos mediante las directivas de transferencia de archivos descritas anteriormente.
3. En la consola de administración de Citrix StoreFront, haga clic en **Almacenes**, seleccione el nodo **Administrar sitios de Receiver para Web**, y habilite Citrix Receiver para HTML5 mediante la opción **Usar siempre Receiver para HTML5**.



4. Inicie una sesión de un escritorio virtual o de una aplicación de explorador web. Cargue y descargue archivos entre el Linux VDA y su dispositivo cliente.

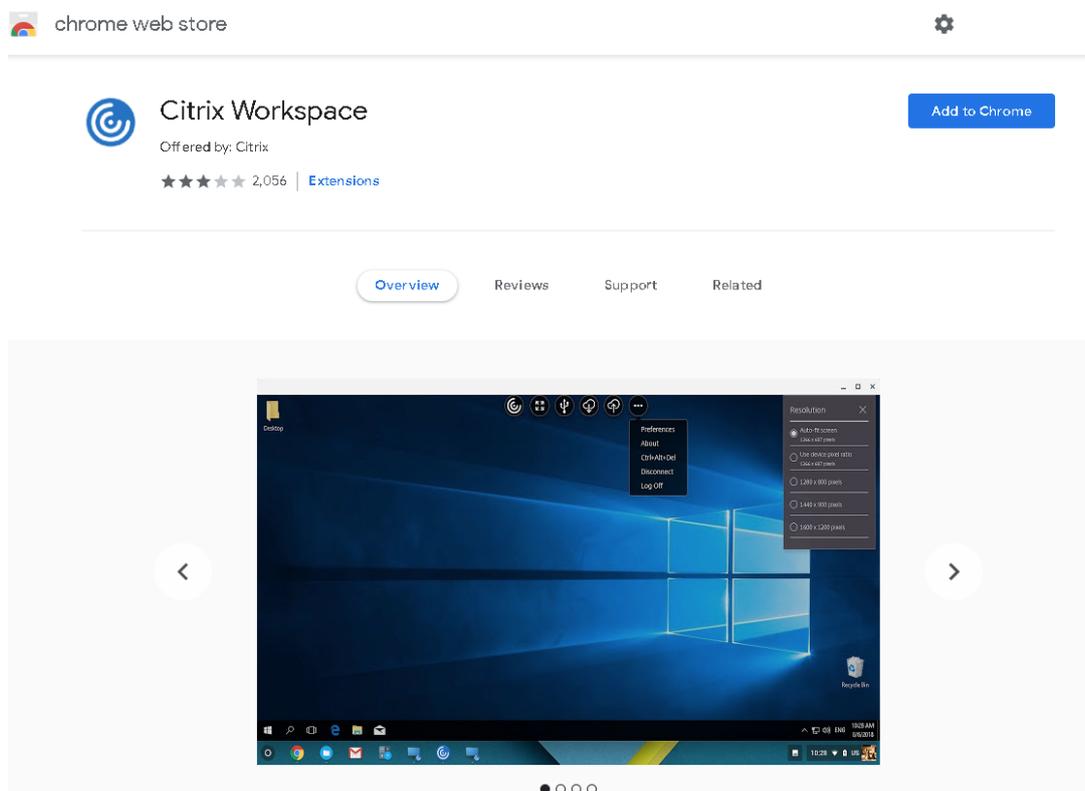
Para utilizar la función de transferencia de archivos a través de la aplicación Citrix Workspace para

Chrome:

1. Habilite la transferencia de archivos mediante las directivas de transferencia de archivos que descritas anteriormente.
2. Adquiera la aplicación Citrix Workspace desde la tienda Chrome Web Store.

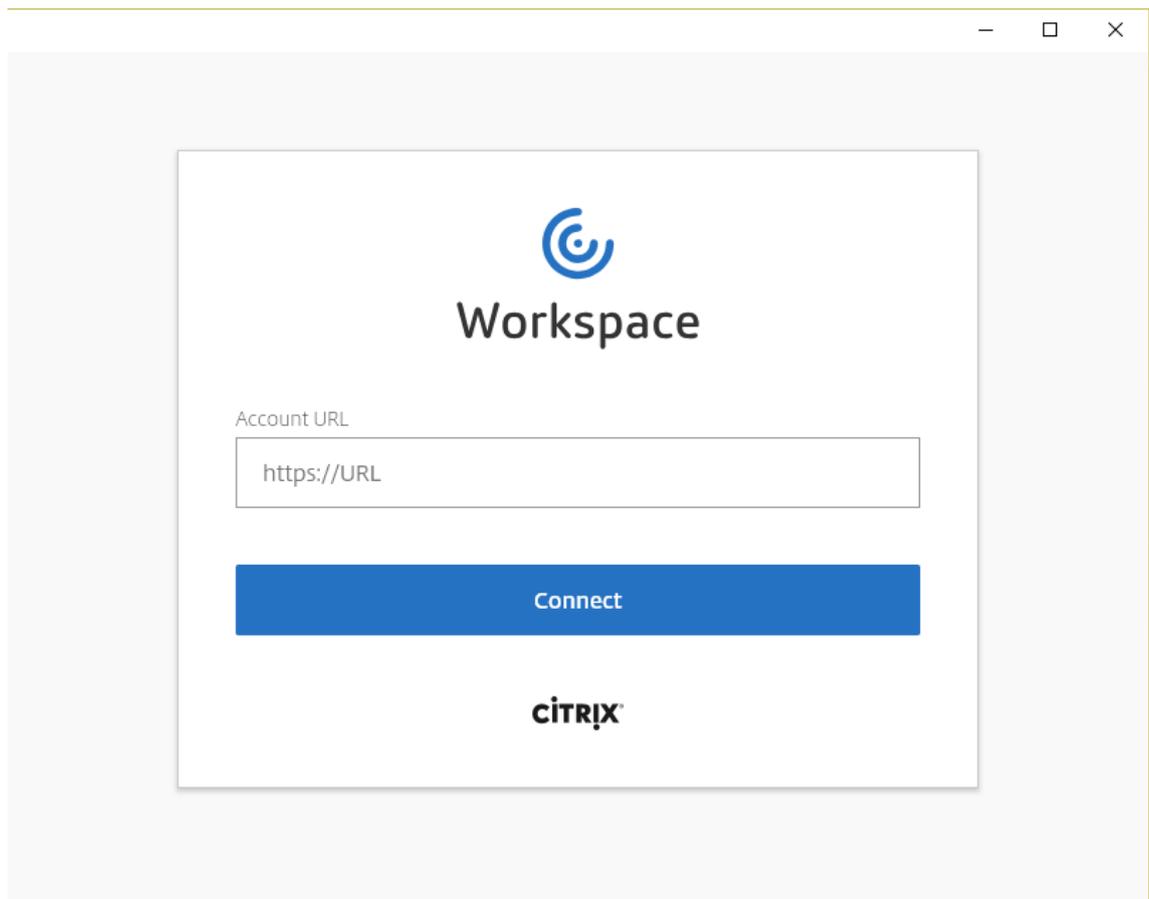
Omita este paso si ya ha agregado la aplicación Citrix Workspace para Chrome a la página Chrome Apps.

- a) Escriba **Citrix Workspace para Chrome** en el cuadro de búsqueda de Google Chrome. Haga clic en el icono de búsqueda.
- b) Entre los resultados de búsqueda, haga clic en la URL de Chrome Web Store, donde encontrará la aplicación Citrix Workspace.



- c) Haga clic en **Agregar a Chrome** para añadir la aplicación Citrix Workspace a Google Chrome.
3. Haga clic en la aplicación Citrix Workspace para Chrome en la página Aplicaciones Chrome.
  4. Escriba la URL de su almacén de StoreFront para conectarse.

Omita este paso si escribió la URL antes.



5. Inicie una sesión de un escritorio virtual o de una aplicación de explorador web. Cargue y descargue archivos entre el Linux VDA y su dispositivo cliente.

## 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

April 18, 2024

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](#).

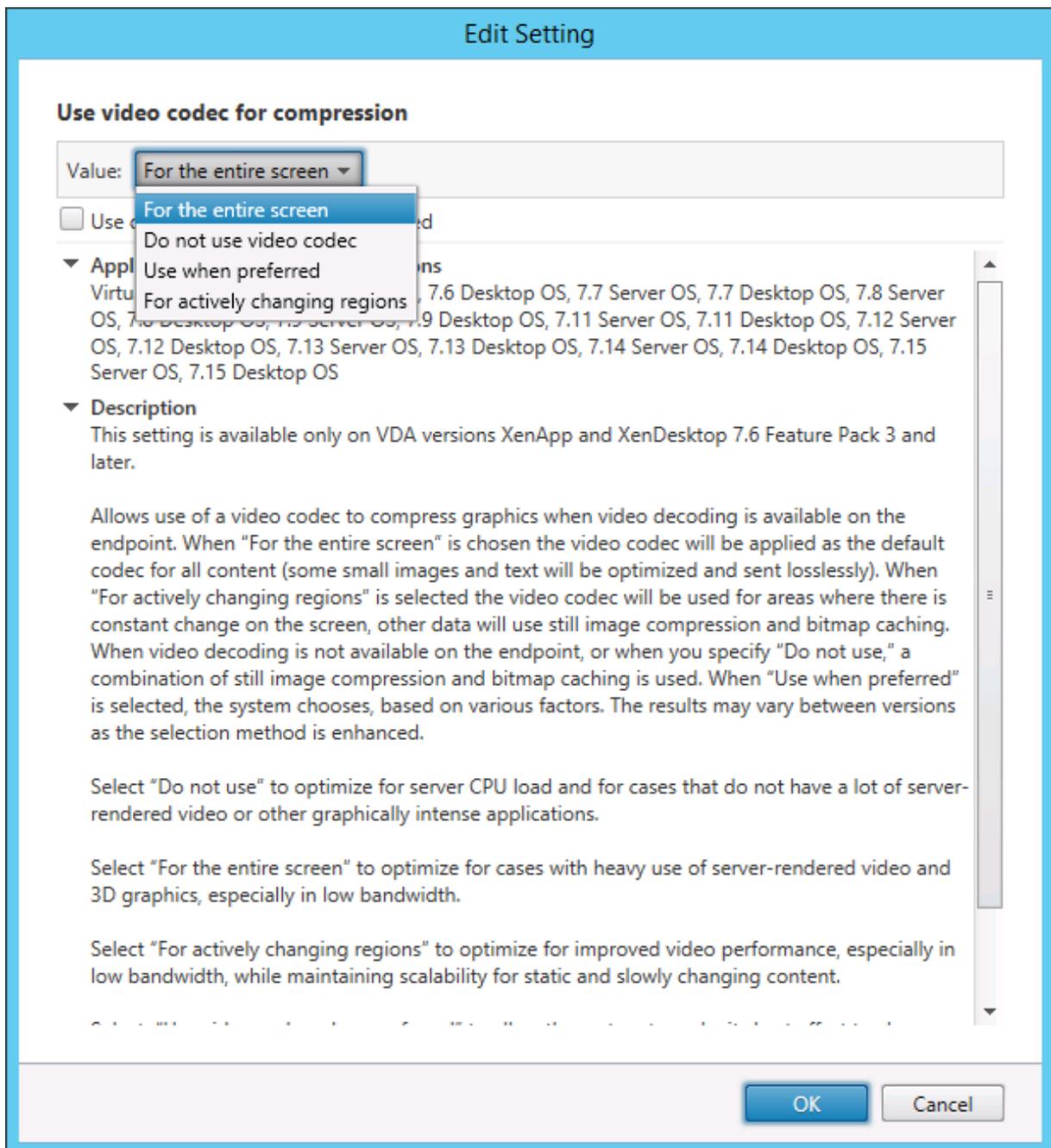
## Configuración

Thinwire es la tecnología de pantallas remotas que se utiliza en Linux Virtual Delivery Agent. Esta tecnología permite que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí.

La directiva **Usar códec de vídeo para compresión** establece el modo de gráficos predeterminado y ofrece estas opciones para diferentes casos de uso:

- **Usar si se prefiere.** Este es el valor predeterminado. No se requiere ninguna configuración adicional. Si mantiene esta configuración, se seleccionará Thinwire para todas las conexiones de Citrix, y se optimizará para la escalabilidad, el ancho de banda y una calidad de imagen superior para cargas de trabajo típicas de escritorio.

- **Para la pantalla entera.** Entrega Thinwire con H.264 o H.265 en pantalla completa para mejorar la experiencia del usuario y optimizar el ancho de banda, sobre todo cuando haya un uso intensivo de gráficos 3D.
- **Para áreas en cambio constante.** En Thinwire, la tecnología de pantalla adaptable identifica imágenes en movimiento (vídeo, 3D en movimiento) y usa H.264 solo en aquella parte de la pantalla donde se mueva la imagen. La función **uso selectivo de un códec de vídeo H..264** permite a HDX Thinwire detectar y codificar partes de la pantalla que se actualizan con frecuencia mediante el códec de vídeo H.264 (por ejemplo, contenido de vídeo). La compresión de imágenes fijas (JPEG, RLE) y el almacenamiento en caché de mapas de bits siguen utilizándose para el resto de la pantalla, incluido el texto y las fotografías. Los usuarios obtienen el beneficio de un menor consumo del ancho de banda y una mejor calidad para el contenido de vídeo, junto con imágenes de alta calidad o texto sin pérdida de calidad. Para habilitar esta funcionalidad, cambie la configuración de la directiva **Usar códec de vídeo para compresión** a **Usar si se prefiere** (predeterminado) o **Para áreas en cambio constante**. Para obtener más información, consulte [Configuraciones de directiva de gráficos](#).



Varias configuraciones de directiva más, incluidas las siguientes configuraciones de directiva de Presentación visual, se pueden usar para optimizar el rendimiento de la tecnología de pantallas remotas:

- **Profundidad de color preferida para gráficos simples**
- **Velocidad de fotogramas de destino**
- **Calidad visual**

## Usar H.264 para una calidad Gradual sin pérdida en Thinwire

De forma predeterminada, la preferencia de **Gradual sin pérdida** de la configuración de directiva **Calidad visual** ahora es H.264, en lugar de JPEG para imágenes en movimiento.

La codificación H.264 ofrece una calidad superior de imagen. Esa preferencia se controla desde la configuración de la directiva **Usar códec de vídeo para compresión**, cuyo valor predeterminado es **Usar si se prefiere**. Para aplicar el uso de JPEG en **Gradual sin pérdida**, establezca la directiva **Usar códec de vídeo para compresión** como **No usar códec de vídeo**. Si su cliente no admite H.264 selectivo, **Gradual sin pérdida** recurre a JPEG independientemente de la configuración que tenga la directiva. El uso de Selective H.264 se admite desde la versión 4.9 a la 4.12 de Citrix Receiver para Windows, desde la versión 13.5 a la 13.10 de Citrix Receiver para Linux, en la aplicación Citrix Workspace 1808 para Windows y versiones posteriores, y en la aplicación Citrix Workspace 1808 para Linux y versiones posteriores. Para obtener más información sobre las configuraciones de directiva **Calidad visual** y **Usar códec de vídeo para compresión**, consulte [Configuraciones de directiva de Presentación visual](#) y [Configuraciones de directiva de Gráficos](#).

## Compatibilidad con el códec de vídeo H.265

A partir de la versión 7.18, Linux VDA admite el códec de vídeo H.265 en la aceleración de hardware para gráficos y vídeos remotos. Puede usar esta función en Citrix Receiver para Windows versiones 4.10 a 4.12 y en la aplicación Citrix Workspace 1808 para Windows y versiones posteriores. Para utilizar esta función, debe habilitarla tanto en Linux VDA como en su cliente. Si la GPU en su dispositivo cliente no admite la decodificación H.265 mediante la interfaz DXVA, la configuración de directiva “Decodificación H.265 para gráficos” se ignora y la sesión recurre al uso del códec de vídeo H.264. Para obtener más información, consulte [Codificación de vídeo H.265](#).

Para habilitar la codificación por hardware H.265 en el VDA:

1. Habilite la directiva **Usar codificación por hardware para códec de vídeo**.
2. Habilite la directiva **Optimizar para cargas de trabajo de gráficos 3D**.
3. Compruebe que la directiva **Usar códec de vídeo para compresión** esté establecida en el valor predeterminado o en **Para la pantalla entera**.
4. Compruebe que la directiva **Calidad visual no** esté establecida en **Gradual sin pérdida** o **Siempre sin pérdida**.

Para habilitar la codificación por hardware H.265 en su dispositivo cliente, consulte [Codificación de vídeo H.265](#).

## Compatibilidad con la codificación por software YUV444

Linux VDA admite la codificación por software YUV444. El esquema de codificación YUV asigna valores de brillo y color a cada píxel. En YUV, “Y” representa el brillo o el valor “luma” y “UV” representa el color o el valor “croma”. Puede usar esta función de Linux VDA en Citrix Receiver para Windows versiones 4.10 a 4.12 y en la aplicación Citrix Workspace 1808 para Windows y versiones posteriores.

Cada valor único de Y, U, y V comprende 8 bits, o un byte, de datos. El formato de datos YUV444 transmite 24 bits por píxel. El formato de datos YUV422 comparte los valores U y V entre dos píxeles, lo que resulta en una velocidad media de transmisión de 16 bits por píxel. La siguiente tabla muestra una comparación intuitiva entre YUV444 y YUV420.

YUV444

	A	B	C
1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix

YUV420

	A	B	C
1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix

Para habilitar la codificación por software YUV444 en el VDA:

1. Compruebe que la directiva **Usar códec de vídeo para compresión** esté establecida en **Para la pantalla entera**.
2. Compruebe que la directiva **Calidad visual** esté establecida en **Siempre sin pérdida** o **Gradual sin pérdida**.

## Ajuste la velocidad media de bits según los cálculos estimados del ancho de banda

Citrix mejora la codificación por hardware HDX 3D Pro mediante el ajuste de la velocidad media de bits según los cálculos estimados de ancho de banda.

Cuando la codificación por hardware HDX 3D Pro se está utilizando, el VDA puede estimar intermitentemente el ancho de banda de la red y ajustar la velocidad de bits de fotogramas codificados, basado en los cálculos estimados de ancho de banda. Esta nueva funcionalidad proporciona un mecanismo para equilibrar la nitidez y la fluidez.

Esta función está habilitada de manera predeterminada. Para inhabilitarlo, ejecute este comando.

```

1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  DisableReconfigureEncoder" -d "0x00000001" --force
2 <!--NeedCopy-->

```

Además de utilizar esta función, también puede ejecutar los siguientes comandos para ajustar entre nitidez y fluidez. Los parámetros **AverageBitRatePercent** y **MaxBitRatePercent** establecen el porcentaje de uso del ancho de banda. Cuanto más altos sean los valores que establezca, obtendrá mejor nitidez y fluidez. El intervalo de parámetros recomendado es de 50 a 100.

```

1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  AverageBitRatePercent" -d "90" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  MaxBitRatePercent" -d "100" --force
4 <!--NeedCopy-->

```

En el ajuste de velocidad media de bits, cuando su pantalla está quieta, el fotograma más reciente se mantiene en un estado de baja calidad porque no se envían fotogramas nuevos. El proceso de nitidez puede solucionar este problema reconfigurando y enviando inmediatamente el fotograma más reciente con la mayor calidad.

Para obtener una lista completa de las directivas disponibles en Linux VDA Thinwire, consulte [Lista de directivas disponibles](#).

Para obtener información sobre la configuración de la compatibilidad con varios monitores en Linux VDA, consulte [CTX220128](#).

## Solución de problemas

### Compruebe el modo de gráficos en uso

Ejecute el siguiente comando para comprobar qué modo de gráficos se está utilizando (**0** significa TW+; **1** significa códec de vídeo para la pantalla entera):

```

1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
2 <!--NeedCopy-->

```

El resultado es similar a:

```

create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force

```

### Compruebe si H.264 se está utilizando

Ejecute el siguiente comando para comprobar si H.264 se está utilizando (**0** significa que no se usa, **1** significa que sí se usa):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
2 <!--NeedCopy-->
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000000"--force
```

### Compruebe si H.265 se está utilizando

Ejecute el siguiente comando para comprobar si H.265 en pantalla completa se está utilizando (**0** significa que no se está utilizando, **1** significa que sí se está utilizando):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
2 <!--NeedCopy-->
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H265"-d "0x00000000"--force
```

### Compruebe qué esquema de codificación YUV se utiliza

Ejecute el siguiente comando para comprobar qué esquema de codificación YUV se está utilizando (**0** significa YUV420; **1** significa YUV422; **2** significa YUV444):

**Nota:** El valor de YUVFormat es importante solo cuando se utiliza el códec de vídeo.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
2 <!--NeedCopy-->
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000000"--force
```

### Compruebe si la codificación por software YUV444 se está utilizando

Ejecute el siguiente comando para comprobar si la codificación por software YUV444 se está utilizando:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
2 <!--NeedCopy-->
```

Cuando YUV444 se está utilizando, el resultado se asemeja a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000000"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--force
```

### 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):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
2 <!--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:

```
1 Tue Apr 12 10:42:03 2016
2 +-----+
3 | NVIDIA-SMI 361.28      Driver Version: 361.28      |
4 |-----+-----+-----+-----+-----+-----+-----+-----+-----+
5 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
6 |   Uncorr. ECC |
7 | Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util
8 | Compute M. |
9 |=====+=====+=====+=====+=====+=====+=====+=====+=====+
10 |    0   GRID K1              Off | 0000:00:05.0   Off |
11 |           N/A |
12 | N/A   42C    P0      14W / 31W |  207MiB / 4095MiB |      8%
13 |           Default |
14 +-----+-----+-----+-----+-----+-----+-----+-----+-----+
15
```

```

12 +-----+
13 | Processes:                                     GPU
    | Memory |
14 | GPU      PID  Type  Process name
    | Usage   |
15 |=====+
16 |    0      2164 C+G   /usr/local/bin/ctxgfx
    | 106MiB |
17 |    0      2187  G    Xorg
    |  85MiB |
18 +-----+
19 <!--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:

```

1 +-----+
2 | NVIDIA-SMI 352.70      Driver Version: 352.70      |
3 |-----+
4 | GPU  Name            Persistence-M| Bus-Id        Disp.A | Volatile
    | Uncorr. ECC |
5 | Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util
    | Compute M. |
6 |=====+=====+=====+=====+=====+
7 |    0  Tesla M60              Off | 0000:00:05.0    Off |
    |          Off |
8 | N/A   20C    P0           37W / 150W |  19MiB /  8191MiB |    0%
    | Default |
9 +-----+-----+-----+-----+-----+
10
11 +-----+
12 | Processes:                                     GPU
    | Memory |
13 | GPU      PID  Type  Process name
    | Usage   |
14 |=====+
15 | No running processes found
    |
16 +-----+
17 <!--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 Citrix Hypervisor muestra la pantalla de la sesión de escritorio ICA

**Solución temporal:** Inhabilite la consola VGA local de la máquina virtual mediante estos comandos:

Para Citrix Hypervisor 8.1 y versiones posteriores:

```
1 [root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
  disable_vnc=1
2 <!--NeedCopy-->
```

Para versiones de Citrix Hypervisor anteriores a 8.1:

```
1 xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
2 <!--NeedCopy-->
```

### Las tarjetas gráficas NVIDIA K2 no admiten la codificación por hardware YUV444 en el modo PassThrough

Con **Gradual sin pérdida** habilitado en la configuración de la directiva, aparece una pantalla en negro o gris cuando los usuarios inician una sesión de aplicación o escritorio con una tarjeta gráfica NVIDIA K2. Este problema se da porque las tarjetas gráficas NVIDIA K2 no admiten la codificación por hardware YUV444 en el modo PassThrough. Para obtener más información, consulte [Video Encode and Decode GPU Support Matrix](#).

## 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 la aplicación Citrix Workspace

Si cambia el tamaño de la ventana de la aplicación Citrix Workspace, 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)’`.

## Presentación progresiva de Thinwire

November 3, 2021

La interactividad de la sesión puede degradarse en conexiones de latencia baja o poco ancho de banda. Por ejemplo, en conexiones con menos de 2 Mbps de ancho de banda o una latencia de más de 200 ms, el desplazamiento por una página Web puede ralentizarse, dejar de responder o aparecer entrecortado. Las operaciones de teclado y mouse pueden retrasarse con respecto a las actualizaciones de gráficos.

Con la versión 7.17, se podían usar las directivas para reducir el consumo del ancho de banda configurando la sesión en una calidad visual **Baja** o establecer una profundidad de color menor (gráficos de 16 u 8 bits). Sin embargo, se tenía que saber que un usuario tenía poca conectividad. HDX Thinwire no ajustaba dinámicamente la calidad de la imagen estática en función de las condiciones de red.

A partir de la versión 7.18, HDX Thinwire cambia de forma predeterminada a un modo de actualización progresiva cuando el ancho de banda disponible baja de 2 Mbps o la latencia de red excede los 200 ms. En este modo:

- Todas las imágenes estáticas se comprimen mucho.
- La calidad del texto se reduce.

Por ejemplo, en el siguiente gráfico, donde el modo de actualización progresiva está activo, las letras **F** y **e** tienen artefactos azules, y la imagen está muy comprimida. Este mecanismo reduce significativamente el consumo del ancho de banda, lo que permite que las imágenes y el texto se reciban más rápidamente, y la interactividad de la sesión mejora.

## Features



Cuando deja de interactuar con la sesión, las imágenes y el texto degradados pasan a mostrarse progresivamente sin pérdida. Por ejemplo, en el siguiente gráfico, las letras ya no contienen artefactos azules y la imagen aparece con la calidad de origen.

## Features



Para ofrecer imágenes más nítidas, se utiliza un método aleatorio por bloques. Para el texto, se definen letras individuales o partes de palabras. El proceso de nitidez se produce en varias tramas. De esta manera, se evita el retraso que conlleva usar una sola trama grande para la nitidez.

Las imágenes transitorias (vídeo) se siguen gestionando con la pantalla adaptable o H.264 selectivo.

### Cómo se usa el modo progresivo

De forma predeterminada, el modo progresivo está en espera en las configuraciones de la directiva **Calidad visual: Alta, Media** (predeterminado) y **Baja**.

El modo progresivo se desactiva (no se usa) cuando:

- **Calidad visual = Siempre sin pérdida** o **Gradual sin pérdida**
- **Preferencia de profundidad de color para gráficos sencillos = 8 bits**
- **Usar códec de vídeo para compresión = Para la pantalla entera** (cuando se prefiere H.264 a pantalla completa)

Si el modo progresivo está en espera, se habilita de forma predeterminada cuando se da una de las siguientes condiciones:

- El ancho de banda disponible baja a menos de 2 Mbps

- La latencia de red aumenta por encima de 200 ms

Después de un cambio de modo, transcurre un mínimo de 10 segundos en ese modo, aunque las condiciones adversas de la red fueran temporales.

## Cambiar el comportamiento del modo progresivo

Para cambiar el comportamiento del modo progresivo, ejecute el siguiente comando:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  ProgressiveDisplay" -d "<value>" --force
2 <!--NeedCopy-->
```

donde <value>:

0 = Siempre desactivado (no usar en ninguna circunstancia)

1 = Automático (alternar según las condiciones de la red, valor predeterminado)

2 = Siempre activado

Cuando está en el modo automático (1), puede ejecutar cualquiera de los siguientes comandos para cambiar los umbrales en los que se alterna al modo progresivo:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

donde <value> es <umbral en Kbps> (predeterminado = 2,048)

Ejemplo: 4096 = activa el modo progresivo si el ancho de banda baja de 4 Mbps

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE
  \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  ProgressiveDisplayLatencyThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

donde <value> es <umbral en ms> (predeterminado = 200)

Ejemplo: 100 = activa el modo progresivo si la latencia de la red baja de 100 ms.

## 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 7: 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:

```
1 sudo yum -y install openldap
2
3 sudo yum -y install libxml2
4
5 sudo yum -y install cyrus-sasl
6
7 sudo yum -y install cyrus-sasl-gssapi
8 <!--NeedCopy-->
```

#### SLES/SELD:

```
1 sudo zypper install openldap2
2
3 sudo zypper install libxml2
4
5 sudo zypper install cyrus-sasl
6
7 sudo zypper install cyrus-sasl-gssapi
8 <!--NeedCopy-->
```

#### Ubuntu:

```
1 sudo apt-get install -y libldap-2.4-2
2
3 sudo apt-get install -y libsasl2-2
4
5 sudo apt-get install -y libsasl2-modules-gssapi-mit
6 <!--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:

```
1 /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--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).

```
Checking GTX_XDL_LDAP_LIST... value not set.
The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide
LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with
LDAP port (e.g. ad1.mycompany.com:389).
If required, please provide the FQDN:port of at least one LDAP server. [<none>]: █
```

También puede ejecutar el comando **ctxreg** para escribir este parámetro directamente en el Registro:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -t "REG_SZ" -v "ListOfLDAPServers" -d "ad1.
  mycompany.com:389 ad2.mycompany.com:389" --force
2 <!--NeedCopy-->
```

## 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
Usar la hora local del cliente	UseLocalTimeOfClient	Usuario	ICA/Control de zona horaria	Usar zona horaria del servidor
Cálculo del tiempo de retorno ICA	IcaRoundTripCheckEnabled	Equipo	ICA/Supervisión de usuario final	Habilitado (1)
Intervalo de cálculo del tiempo de retorno ICA	IcaRoundTripCheckPeriod	Equipo	ICA/Supervisión de usuario final	15
Cálculo del tiempo de retorno ICA para conexiones inactivas	IcaRoundTripCheckTimeout	Equipo	ICA/Supervisión de usuario final	Inhabilitado (0)
Límite de ancho de banda global de la sesión	LimitOverallBw	Usuario	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de sonido	LimitAudioBw	Usuario	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de sonido	LimitAudioBwPercent	Usuario	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de dispositivos USB del cliente	LimitUSBBw	Usuario	ICA\Ancho de banda	0
Porcentaje de ancho de banda de redirección de dispositivos USB del cliente	LimitUSBBwPercent	Usuario	ICA\Ancho de banda	0

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Límite de ancho de banda de redirección del portapapeles	LimitClipbdBW	Usuario	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección del portapapeles	LimitClipbdBWPercent	Usuario	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de archivos	LimitCdmBw	Usuario	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de archivos	LimitCdmBwPercent	Usuario	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de impresoras	LimitPrinterBw	Usuario	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de impresoras	LimitPrinterBwPercent	Usuario	ICA\Ancho de banda	0
Conexiones con WebSockets	AcceptWebSocketsConnections	Equipo	ICA\WebSockets	Prohibida
Número de puerto de WebSockets	WebSocketsPort	Equipo	ICA\WebSockets	8008
Lista de servidores de origen de WebSockets de confianza	WSTrustedOriginServers	Equipo	ICA\WebSockets	*

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
Transporte adaptable HDX	HDXoverUDP	Equipo	ICA	Preferido (2)
Conexiones de fiabilidad de la sesión	AcceptSessionReliabilityConnections	Equipo	ICA/Fiabilidad de la sesión	Permitido (1)
Nivel de transparencia de la interfaz de usuario durante la reconexión	ReconnectionUITransparencyLevel	Equipo	ICA/Reconexión automática de clientes	80 %
Número de puerto para fiabilidad de la sesión	SessionReliabilityPort	Equipo	ICA/Fiabilidad de la sesión	2598
Tiempo de espera de fiabilidad de la sesión	SessionReliabilityTimeout	Equipo	ICA/Fiabilidad de la sesión	180 segundos
Reconexión automática de clientes	AllowAutoClientReconnections	Usuario	ICA/Reconexión automática de clientes	Permitido (1)
Redirección de audio del cliente	AllowAudioRedirection	Usuario	Audio	Permitido (1)
Redirección de impresoras del cliente	AllowPrinterRedirection	Usuario	Impresión	Permitido (1)
Crear automáticamente la impresora universal de PDF	AutoCreatePDFPrinter	Usuario	Impresión	Inhabilitado (0)

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Asignación y compatibilidad de controladores de impresora	DriverMappingList	Usuario	Impresión	"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"
Redirección del portapapeles del cliente	AllowClipboardRedir	Usuario	Portapapeles	Permitido (1)
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	Thinwire	Habilitado (1)
Compresión de color adicional	ExtraColorCompression	Usuario	Thinwire	Inhabilitado (0)
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)

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Permitir compresión sin pérdida visual	AllowVisuallyLosslessCompression	Usuario	Thinwire	Inhabilitado (0)
Optimizar para cargas de trabajo de gráficos 3D	OptimizeFor3dWorkload	Usuario	Thinwire	Inhabilitado (0)
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	AllowMicrophoneRedirection	Usuario	Audio	Permitido (1)
Número máximo de sesiones	MaximumNumberOfSessions	Administración de carga	Administración de carga	250
Tolerancia de inicios de sesión simultáneos	ConcurrentLogonsToMachine	Administración de carga	Administración de carga	2
Habilitar actualización automática de Controlllers	EnableAutoUpdateOfControllers	Equipos	Parámetros de Virtual Delivery Agent	Permitido (1)
Modo de actualización de la selección del portapapeles	ClipboardSelectionUpdateMode	Equipos	Portapapeles	3
Modo de actualización de la selección primaria	PrimarySelectionUpdateMode	Equipos	Portapapeles	3
Calidad máxima de Speex	MaxSpeexQuality	Usuario	Audio	5

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Conectar automáticamente las unidades del cliente	AutoConnectDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Habilitado (1)
Unidades ópticas del cliente	AllowCdromDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades fijas del cliente	AllowFixedDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades de disco flexible del cliente	AllowFloppyDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades de red del cliente	AllowNetworkDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Redirección de unidades del cliente	AllowDriveRedir	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Acceso de lectura solamente a unidades del cliente	ReadOnlyMappedDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Inhabilitado (0)
Presentación automática del teclado	AllowAutoKeyboardRepeat	Propio	MRVC	Inhabilitado (0)

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Permitir transferencia de archivos entre escritorio y cliente.	AllowFileTransfer	Usuario	Transferencia de archivos	Se permite
Descargar archivos desde el escritorio	AllowFileDownload	Usuario	Transferencia de archivos	Se permite
Cargar archivos al escritorio	AllowFileUpload	Usuario	Transferencia de archivos	Se permite

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]

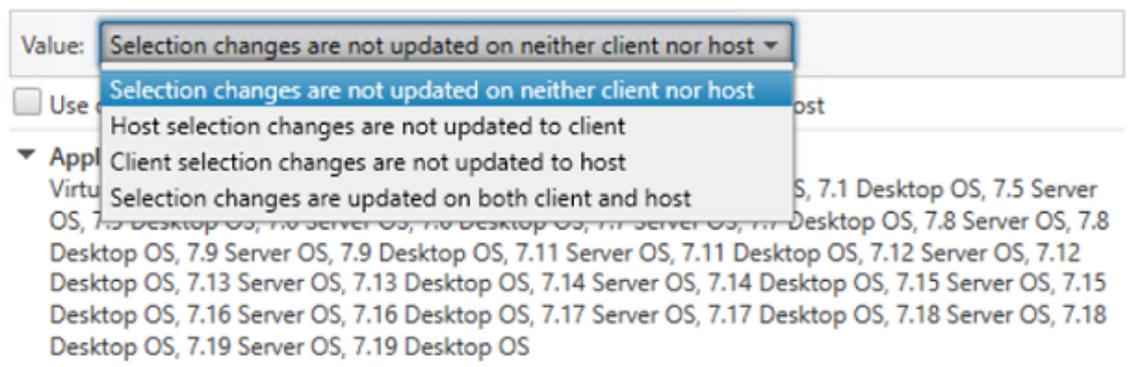
**Valor predeterminado:** 3

**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:

**Primary selection update mode**



Value: Selection changes are not updated on neither client nor host

Use Selection changes are not updated on neither client nor host

▼ Appl Host selection changes are not updated to client

Virtu Client selection changes are not updated to host

OS, 7.1 Desktop OS, 7.5 Server OS, 7.2 Desktop OS, 7.6 Server OS, 7.3 Desktop OS, 7.7 Server OS, 7.4 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 7.19 Server OS, 7.19 Desktop OS

▼ Description

This setting is supported only by Linux VDA version 1.4 onwards.

PRIMARY selection is used for explicit copy/paste actions such as mouse selection and middle mouse button paste. This setting controls whether PRIMARY selection changes on the Linux VDA can be updated on the client's clipboard (and vice versa). It can include one of the following selection changes:

Selection changes are not updated on the client or the host. PRIMARY selection changes do not update a client's clipboard. Client clipboard changes do not update PRIMARY selection.

Host selection changes are not updated on the client. PRIMARY selection changes do not update a client's clipboard. Client clipboard changes update the PRIMARY selection.

Client selection changes are not updated on the host. PRIMARY selection changes update the client's clipboard. Client clipboard changes do not update the PRIMARY selection.

Selection changes are updated on both the client and host. PRIMARY selection change updates the client's clipboard. Client clipboard changes update the PRIMARY selection.

▼ Related settings

Clipboard selection update mode

– **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

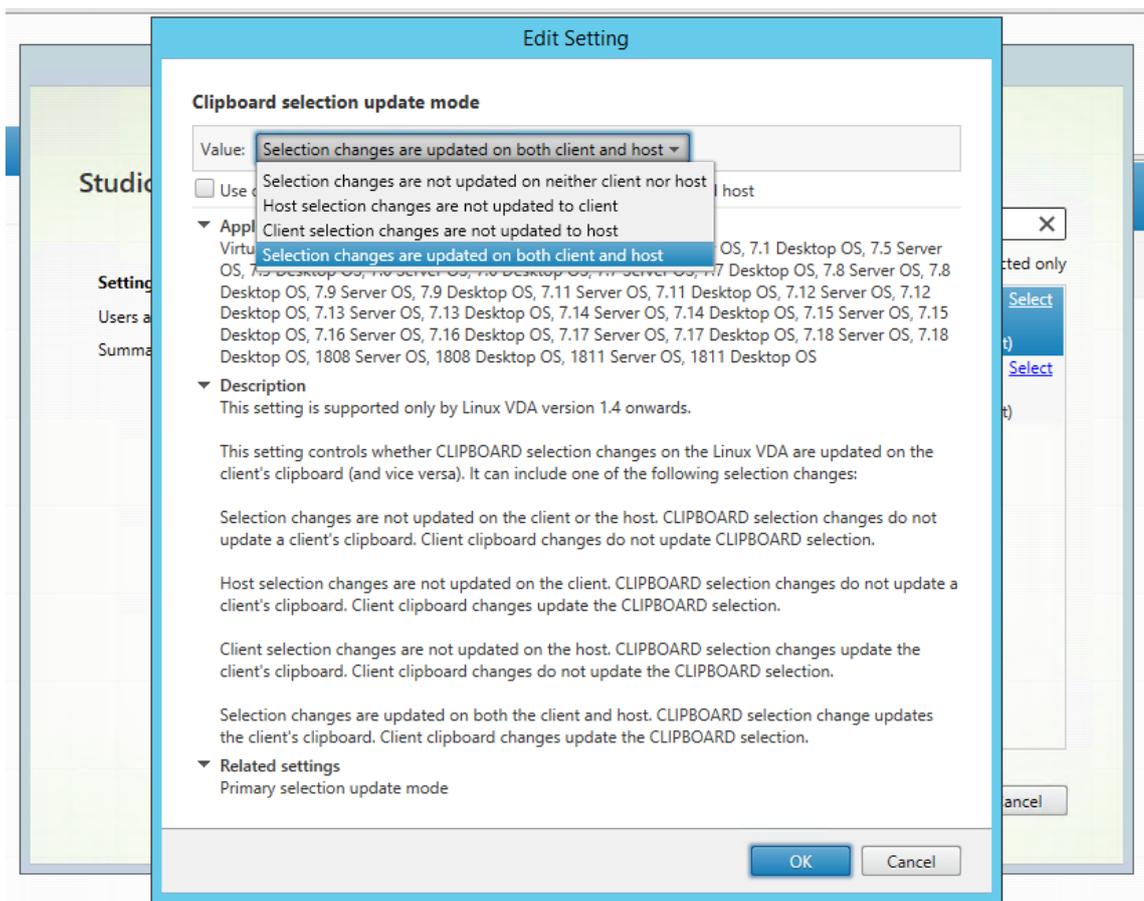
**Valor (enumeración):** [0, 1, 2, 3]

**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, Citrix 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 admite IPv6 para equipararse con Citrix Virtual Apps and Desktops. 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 "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD"
  -v "ControllerRegistrationIPv6Netmask"
3 <!--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 sobre IPv6 en Citrix Virtual Apps and Desktops, 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. Además, se envía una copia de los datos anónimos a Google Analytics (GA) para un análisis rápido y eficiente.

### 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-->
```

- **GASwitch**

Parámetro de Registro que habilita o inhabilita el programa GA (predeterminado = 0):

Ubicación: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CEIP

Nombre: GASwitch

Valor: 1 = inhabilitado, 0 = habilitado

Si no se especifica, significa que GA está habilitado.

Puede ejecutar el siguiente comando en un cliente para inhabilitar el programa GA:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\  
Citrix\CEIP" -v "GASwitch" -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
Configuración regional del sistema	system_locale	Cadena de texto que indica la configuración regional de esta máquina
Último reinicio de los servicios principales de LVDA	ctxhdx ctxvda	La fecha y hora a la que se reiniciaron por última vez los servicios <code>ctxhdx</code> y <code>ctxvda</code> , en el formato dd-hh:mm:ss, por ejemplo, 10-17:22:19
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

Punto de datos	Nombre de la clave	Descripción
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 iniciadas	session_launch	Número entero que indica la cantidad de sesiones iniciadas (o reconectadas) 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
Tipo de recurso	resource_type	Cadena de texto que indica el tipo de sesión iniciada: escritorio o <appname>
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
Tipo de cliente Receiver	receiver_type	Número entero que indica el tipo de aplicación Citrix Workspace utilizada para iniciar la sesión
Versión de cliente de Receiver	receiver_version	Cadena de texto que indica la versión de la aplicación Citrix Workspace utilizada para lanzar la sesión

---

Punto de datos	Nombre de la clave	Descripción
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
Tipo de proveedor Gfx	gfx_provider_type	Cadena de texto que indica el tipo de proveedor de gráficos de la sesión
Recuento de remedos	shadow_count	Número entero que indica cuántas veces se ha remedado la sesión
Idioma seleccionado por el usuario	ctxism_select	Cadena compuesta larga que contiene todos los idiomas que han seleccionado los usuarios
Recuento de redirección de tarjetas inteligentes	scard_redirecting_count	Número entero que indica la cantidad de veces que se utiliza la redirección de tarjetas inteligentes para inicio de sesión y autenticación de usuario en aplicaciones durante la sesión

---

## Configurar la redirección USB

November 15, 2021

Los dispositivos USB se comparten entre la aplicación Citrix Workspace y el escritorio de Linux VDA. Cuando un dispositivo USB se dirige 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 la aplicación Citrix Workspace 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 dirige 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 dirigen 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:

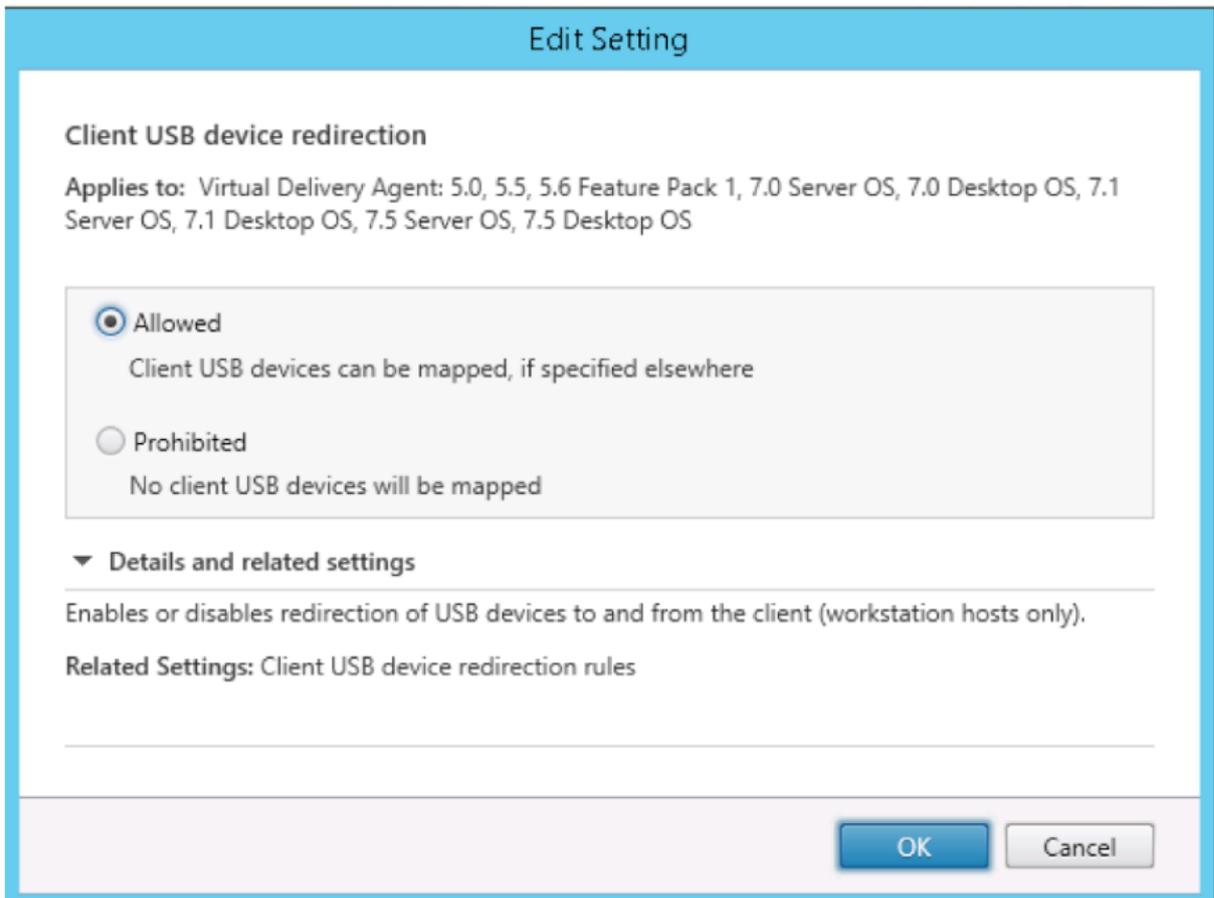
- Directiva de Redirección de dispositivos USB del cliente
- Reglas de redirección de dispositivos USB del cliente

## 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**.

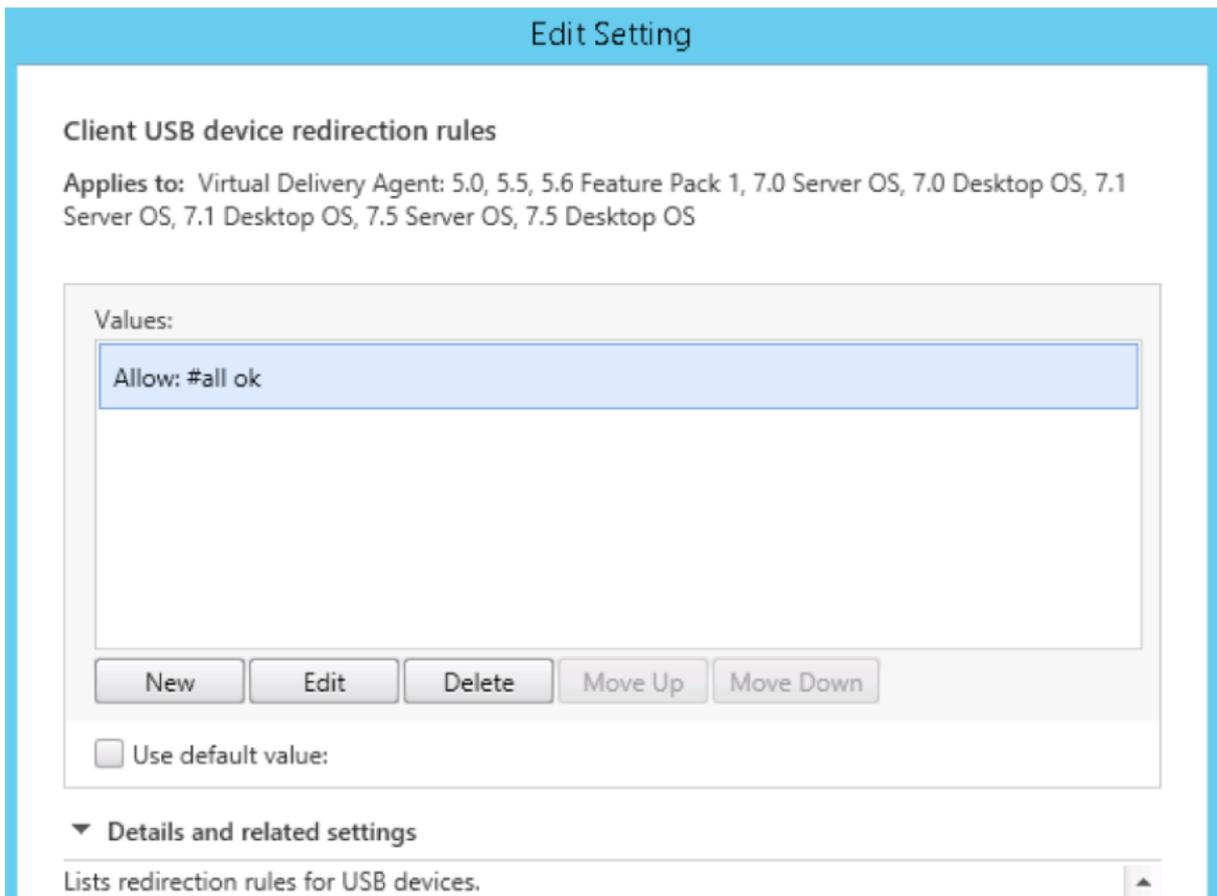


### Configurar reglas de redirección USB

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-ioctl.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 7.7, CentOS 7.7	3.10.0-1062
SUSE 12.3	4.4.73-5-default
Ubuntu 18.04	4.15.0-45-generic
Ubuntu 16.04	4.4.0-142-generic

**Importante:**

Si el kernel de la máquina no es compatible con el controlador creado 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:

```
1 insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
2 <!--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. Descomprima el archivo **citrix-linux-vda-sources.zip**. Vaya a **linux-vda-sources/vhci-hcd-1.15.tar.bz2** y descomprima los archivos de origen VHCI mediante **tar xvf vhci-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/CentOS:**

```
1 yum install kernel-devel
2 <!--NeedCopy-->
```

**SUSE 12:**

```
1 zypper install kernel-devel
2
3 zypper install kernel-source
4 <!--NeedCopy-->
```

**Ubuntu:**

```
1 apt-get install linux-headers
2 <!--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 (ejecutando los comandos siguientes en secuencia: `make oldconfig`; `make prepare`; `make modules`; `make`) para obtenerlo o cópielo desde `/usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.*`
5. Ejecute los siguientes comandos para instalar las herramientas de desarrollador.

**RHEL/CentOS:**

```
1 yum groupinstall 'Development Tools'
2 <!--NeedCopy-->
```

**Ubuntu 18.04:**

```
1 apt install build-essential
2 apt install libelf-dev
3 <!--NeedCopy-->
```

**Ubuntu 16.04:**

```
1 apt install build-essential
2 <!--NeedCopy-->
```

6. En el archivo `vhci-hcd-1.15/Makefile`, cambie el Makefile de VCHI y defina KDIR con el directorio de kernel:

```
1 #KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build
2
3 KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
4 <!--NeedCopy-->
```

7. En la carpeta `vhci-hcd-1.15/`, ejecute `make` para crear el kernel de VCHI.

**Nota:**

Si la compilación es correcta, `usb-vhci-hcd.ko` y `usb-vhci-iocifc.ko` se crean en la carpeta `vhci-hcd-1.15/`.

8. Reemplace el módulo de kernel con el recién compilado: `cp -f usb-vhci-*.ko /opt/Citrix/VA/DA/lib64/`

9. Reinicie el servicio USB:

```
1 service ctxusbsd restart
2 <!--NeedCopy-->
```

10. Cierre la sesión y vuelva a iniciarla. Compruebe si la redirección USB está funcionando.

### Solucionar problemas con la generación de kernels

- **Se puede producir un error de generación para kernels específicos de Ubuntu 16.** El error aparece como `implicit declaration of function 'copy_to_user'`, tal y como se muestra en la siguiente captura de pantalla.

```
usb-vhci-iocifc.c:216:5: error: implicit declaration of function 'copy_to_user'
```

El error ocurre debido a cambios en el archivo de encabezado en los kernels. Como solución temporal, agregue la línea `#include <linux/uaccess.h>` al archivo `vhci-hcd-1.15/usb-vhci-iocifc.c`.

```
#include <linux/fs.h>
#include <linux/uaccess.h>
#include "usb-vhci-hcd.h"
```

- **Se puede producir un error de generación para kernels 4.15.0-29-generic de Ubuntu 16.** El error aparece como `'driver_attr_debug_output' undeclared`, tal y como se muestra en la siguiente captura de pantalla.

```
error: 'driver_attr_debug_output' undeclared (first use in this function)
```

El error se produce cuando faltan símbolos en el kernel. Como solución temporal, inhabilite la definición macro para DEPURAR en los archivos `vhci-hcd-1.15/usb-vhci-iocifc.c` y `vhci-hcd-1.15/usb-vhci-hcd.c`.

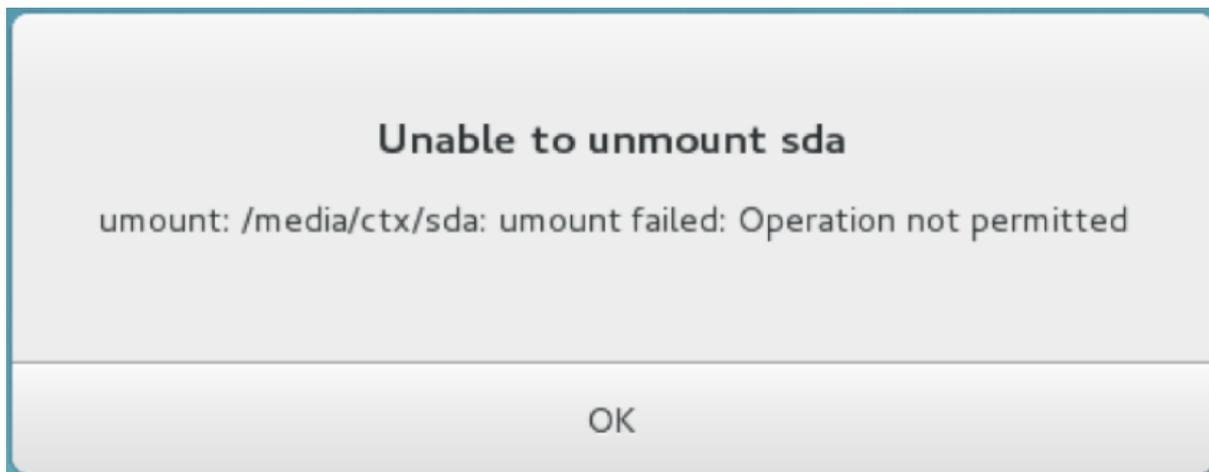
```
22
23 // #define DEBUG
24
25 #include <linux/module.h>
```

### Solucionar problemas de redirección USB

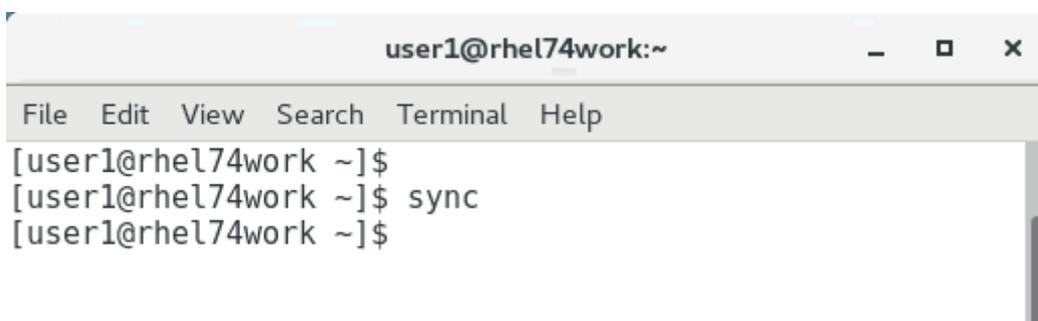
Use la información de esta sección para solucionar problemas que puedan surgir al usar Linux VDA.

**No se puede desmontar el disco USB redirigido\*\***

Para controlar el acceso a todos los discos USB redirigidos desde la aplicación Citrix Workspace, 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**

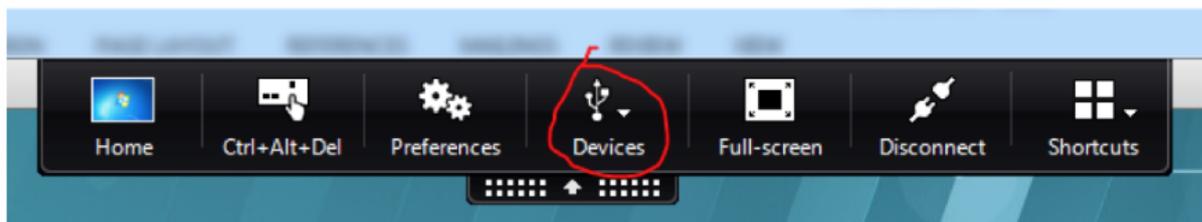
Si redirige un disco USB a una sesión y lo modifica (por ejemplo, crea archivos en él) y, justo después, detiene la redirección en la barra de herramientas de la aplicación Citrix Workspace, el archivo modificado (o creado) se puede perder. Este problema se produce porque, cuando escribe datos en un 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 la aplicación Citrix Workspace, 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 ningún dispositivo en la barra de herramientas de la aplicación Citrix Workspace

En algunos casos, puede que no aparezcan dispositivos en la barra de herramientas de la aplicación Citrix Workspace, 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 Workspace para Linux.

## Los dispositivos USB se ven en la barra de herramientas de la aplicación Citrix Workspace, pero tienen la etiqueta de restringidos por directiva, lo que provoca un error de redirección

Cuando ocurra el problema, haga lo siguiente:

- Configure la directiva de Linux VDA para habilitar la redirección
- Compruebe que no se hayan configurado directivas adicionales en el Registro de la aplicación Citrix Workspace. Busque **DeviceRules** en la ruta del Registro para asegurarse de que este parámetro no esté denegando el acceso a su dispositivo.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Para obtener más información, consulte el artículo de Knowledge Center [How to Configure Automatic Redirection of USB Devices](#).

## 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](#). También es posible que otros tipos de dispositivos se redirijan a una sesión activa de Linux VDA. En este caso, 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.

## Configurar la fiabilidad de la sesión

November 3, 2021

Citrix introduce la función Fiabilidad de la sesión para todas las plataformas Linux compatibles. De forma predeterminada, Fiabilidad de sesión está habilitada.

La fiabilidad de la sesión vuelve a conectar sesiones ICA sin problemas cuando se producen interrupciones de red. Para obtener más información sobre la fiabilidad de la sesión, consulte [Reconexión automática de clientes y fiabilidad de la sesión](#).

**Nota:** Los datos que se transmiten a través de una conexión de fiabilidad de la sesión están en texto sin formato de forma predeterminada. Por motivos de seguridad, se recomienda habilitar el cifrado TLS. Para obtener más información acerca del cifrado TLS, consulte [Proteger sesiones de usuario con TLS](#).

## Configuración

### Configuración de directivas en Citrix Studio

Puede configurar estas directivas para la fiabilidad de la sesión en Citrix Studio:

- Conexiones de fiabilidad de la sesión
- Tiempo de espera de fiabilidad de la sesión
- Número de puerto para fiabilidad de la sesión
- Nivel de transparencia de la interfaz de usuario durante la reconexión

Para obtener más información, consulte las directivas [Fiabilidad de la sesión](#) y [Reconexión automática de clientes](#).

**Nota:** Después de definir las directivas **Conexiones de fiabilidad de la sesión** o **Número de puerto para fiabilidad de la sesión**, reinicie los servicios VDA y HDX, en este orden, para que la configuración surta efecto.

## Configuración en Linux VDA

- **Habilitar o inhabilitar la escucha TCP de fiabilidad de la sesión**

De forma predeterminada, el agente de escucha TCP para fiabilidad de la sesión está habilitado y escucha en el puerto 2598. Para inhabilitar este agente de escucha, ejecute este comando.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\WinStations\cgp" -v "
  fEnableWinStation" -d "0x00000000"
2 <!--NeedCopy-->
```

**Nota:** Reinicie el servicio HDX para que la configuración surta efecto. Inhabilitar la escucha TCP no inhabilita la fiabilidad de la sesión. La fiabilidad de la sesión seguirá estando disponible a través de otros agentes de escucha (por ejemplo, SSL) si la función sigue habilitada en la directiva **Conexiones de fiabilidad de la sesión**.

- **Número de puerto para fiabilidad de la sesión**

También puede definir el número de puerto para la fiabilidad de la sesión con este comando (en el ejemplo, se utiliza el puerto 2599).

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\WinStations\cgp" -v "PortNumber"
  -d "2599"
2 <!--NeedCopy-->
```

**Nota:** Reinicie el servicio HDX para que la configuración surta efecto. Si el número de puerto se ha establecido a través de la configuración de directiva en Citrix Studio, se ignorará su configuración en Linux VDA. Compruebe que el firewall presente en el VDA está configurado para no prohibir el tráfico de red a través de ese puerto.

- **Intervalo Keep Alive del servidor al cliente**

Si no hay actividad en la sesión (por ejemplo, no hay movimientos del puntero ni ninguna actualización de pantalla), se envían mensajes de Keep Alive para la fiabilidad de la sesión entre Linux VDA y el cliente ICA. Los mensajes de Keep Alive se usan para detectar si el cliente sigue operativo. Si no hay respuesta por parte del cliente, la sesión se suspende hasta que el cliente vuelve a conectarse. Esta configuración permite especificar cuántos segundos deben transcurrir entre los mensajes sucesivos de Keep Alive. De manera predeterminada, esta configuración no está definida. Para definirla, ejecute este comando (se utilizan 10 segundos como ejemplo).

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  Citrix\XTEConfig" -t "REG_DWORD" -v "CgpServerToClientKeepAlive"
  -d "10" --force
```

- **Intervalo Keep Alive del cliente al servidor**

Esta configuración permite especificar cuántos segundos deben transcurrir entre cada envío de mensajes sucesivos de Keep Alive desde el cliente ICA al Linux VDA. De manera predeterminada, esta configuración no está definida. Para definirla, ejecute este comando (se utilizan 10 segundos como ejemplo).

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\XTEConfig" -t "REG_DWORD" -v "CgpClientToServerKeepAlive"
   -d "10" --force
2 <!--NeedCopy-->
```

## Solución de problemas

### No se pueden iniciar sesiones después de habilitar la fiabilidad de la sesión a través de la configuración de directiva.

Para solucionar temporalmente este problema, lleve a cabo lo siguiente:

1. Compruebe que el servicio VDA y el servicio HDX se han reiniciado, en este orden, después de habilitar la fiabilidad de la sesión a través de la configuración de directiva en Citrix Studio.
2. En el VDA, ejecute el siguiente comando para comprobar que el agente de escucha TCP para la fiabilidad de la sesión se está ejecutando (se utiliza el puerto 2598 como ejemplo).

```
1 netstat -an | grep 2598
2 <!--NeedCopy-->
```

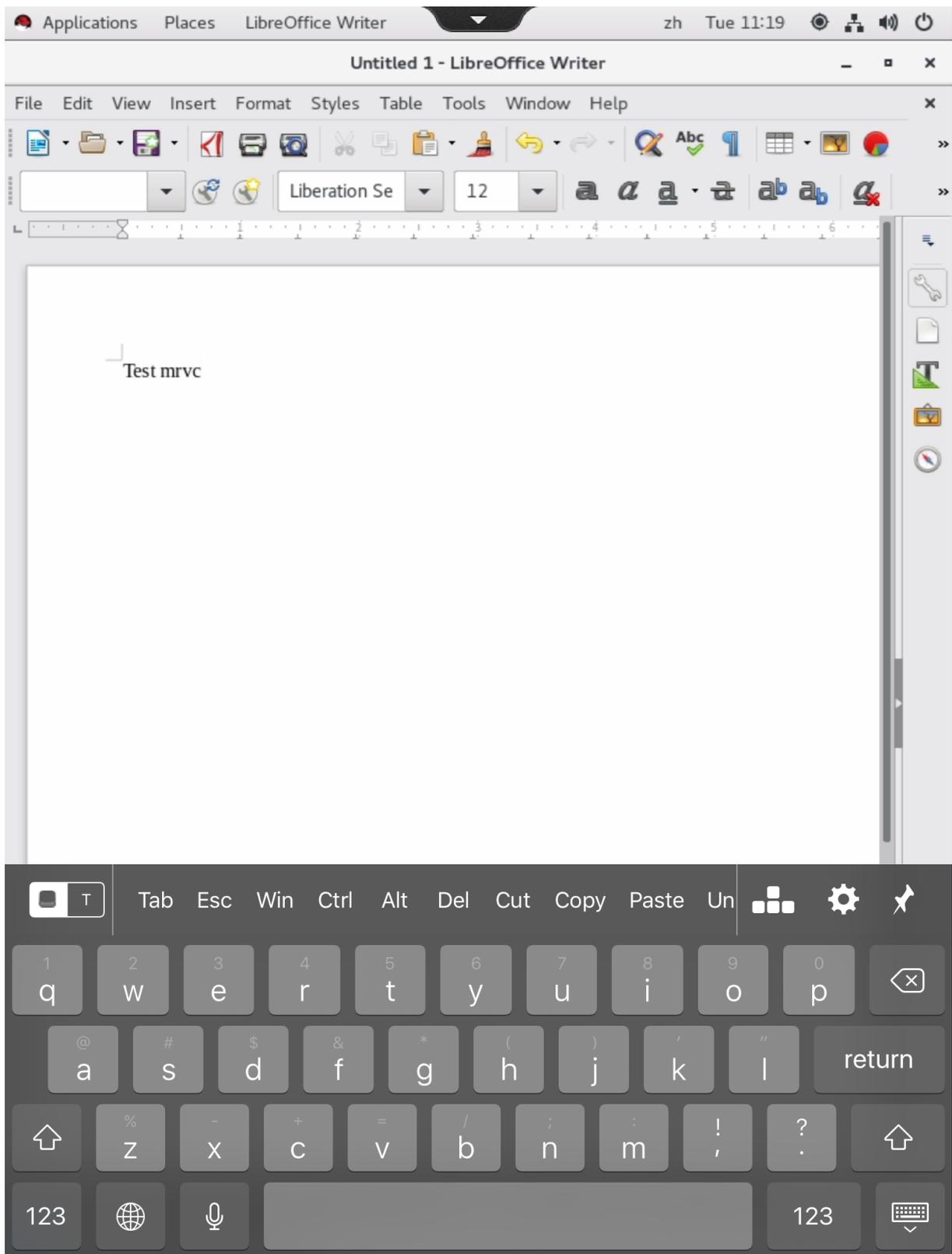
Si no hay ningún agente de escucha TCP en el puerto de la fiabilidad de la sesión, habilítelo con este comando.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\WinStations\cgp" -v "
   fEnableWinStation" -d "0x00000001"
2 <!--NeedCopy-->
```

## Teclado de software

March 11, 2022

La función de teclado de software está disponible en sesiones de Linux Virtual Desktop o Linux Virtual App. El teclado de software aparece o desaparece de forma automática cuando introduce o abandona un campo de entrada.



**Nota:**

Esta función está disponible para RHEL 7.7, CentOS 7.6, SUSE 12.3, Ubuntu 16.04 y Ubuntu 18.04. Se admite en la aplicación Citrix Workspace para iOS y Android.

**Habilitar e inhabilitar la función**

Esta función está inhabilitada de forma predeterminada. Use la utilidad **ctxreg** para habilitar o inhabilitar esta función. Configurar la función en un Linux VDA determinado significa que esa función se aplicará a todas las sesiones en ese VDA.

Para habilitar la funcionalidad:

1. Ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\MrVc" -v "
  Enabled" -d "0x00000001"
2 <!--NeedCopy-->
```

2. En Citrix Studio, establezca la directiva **Presentación automática del teclado a Permitido**.
3. (Opcional) para RHEL 7 y CentOS 7, ejecute el siguiente comando para configurar el Intelligent Input Bus (IBus) como servicio de mensajería instantánea predeterminado:

```
1 echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
2 <!--NeedCopy-->
```

Para inhabilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
  Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000000"
2 <!--NeedCopy-->
```

**Nota:**

los parámetros anteriores surten efecto cuando inicia una nueva sesión o cuando cierra una sesión y la vuelve a iniciar.

**Limitaciones**

- Puede que la función no funcione correctamente con Google Chrome, LibreOffice, y otras aplicaciones.
- Para visualizar el teclado de software de nuevo después de ocultarlo manualmente, haga clic en un campo que no sea de entrada y luego haga clic de nuevo en el campo de entrada actual.

- Puede que el teclado de software no aparezca cuando pase de un campo de entrada a otro en un explorador web. Para solucionar este problema, haga clic en un campo que no sea de entrada y luego en el campo de entrada de destino.
- La función no admite caracteres Unicode ni caracteres de doble byte (como caracteres chinos, japoneses y coreanos).
- El teclado de software no está disponible en campos de entrada de contraseñas.
- El teclado de software podría solaparse con el campo de entrada actual. En ese caso, mueva la ventana de la aplicación o desplácese hacia arriba en su pantalla para mover el campo de entrada a un lugar accesible.
- Debido a problemas de compatibilidad entre la aplicación Citrix Workspace y las tabletas de Huawei, el teclado de software aparece en las tabletas Huawei incluso cuando hay un teclado físico conectado.

## 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 Citrix Virtual Apps o Citrix Virtual Desktops como de costumbre.

Cambie el método de entrada según sea necesario en el lado del cliente para empezar a usar la funcionalidad 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.

## Compatibilidad con entradas en varios idiomas

November 3, 2021

A partir de Linux VDA 1.4, Citrix ha comenzado a admitir aplicaciones publicadas. Los usuarios pueden acceder a una aplicación Linux sin el entorno de escritorio Linux.

No obstante, la barra de idioma nativo de Linux VDA no estaba disponible para la aplicación publicada porque esa barra está integrada en el entorno de escritorio Linux. En consecuencia, los usuarios no podían introducir texto en un idioma que necesitara IME, como coreano, japonés o chino. Además, los usuarios tampoco podían cambiar de distribuciones de teclado durante una sesión de aplicación.

Para solucionar esos problemas, esta función ofrece una barra de idiomas para las aplicaciones publicadas que acepten la entrada de texto. La barra de idiomas permite a los usuarios seleccionar un IME en el lado del servidor y alternar entre diferentes distribuciones de teclado durante una sesión de aplicación.

## Configuración

Puede usar la utilidad **ctxreg** para habilitar o inhabilitar esta función (inhabilitada de manera predeterminada). Configurar la función en un servidor Linux VDA determinado significa que esa función se aplicará a todas las aplicaciones publicadas en ese VDA.

La clave de configuración es "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar" y el tipo es DWORD.

Para habilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE \SYSTEM\  
   CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0  
   x00000001"  
2 <!--NeedCopy-->
```

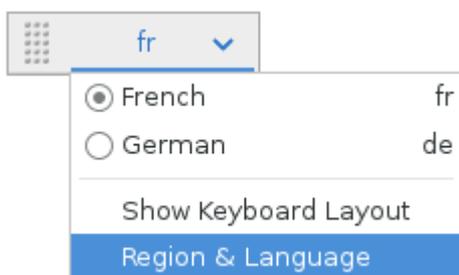
Para inhabilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE \SYSTEM\  
  CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0  
  x00000000"  
2 <!--NeedCopy-->
```

## Uso

El uso es bastante sencillo.

1. Habilite la función.
2. Acceda a una aplicación publicada que acepte la entrada de texto. Aparece una barra de idioma en la sesión, junto a la aplicación.
3. En el menú desplegable, seleccione **Region & Language** (Región e idioma) para agregar el idioma pertinente (origen de entrada).



4. Seleccione la herramienta IME o la distribución de teclado en el menú desplegable.
5. Escriba en un idioma con la herramienta IME o la distribución de teclado seleccionada.

### Nota:

- Si cambia una distribución de teclado en la barra de idioma del lado del agente VDA, compruebe que se utiliza la misma distribución de teclado en el lado del cliente (que ejecuta la aplicación Citrix Workspace).
- Debe actualizar el paquete **accountsservice** a la versión 0.6.37 o versiones posteriores para poder configurar las opciones del cuadro de diálogo **Region & Language** (Región e idioma).



## Sincronización de la distribución de teclado dinámico

November 3, 2021

Anteriormente, las distribuciones del teclado en Linux VDA y en el dispositivo cliente tenían que ser los mismos. Por ejemplo, cuando la distribución del teclado cambiaba de inglés a francés en el dispositivo cliente pero no en el VDA, podían surgir problemas de asignación de teclas y esos problemas persistían hasta que el VDA también se cambiaba a francés.

Citrix ha resuelto el problema sincronizando automáticamente la distribución del teclado del VDA con la distribución del teclado del dispositivo cliente. Cada vez que cambia la distribución del teclado en el dispositivo cliente, cambia también la distribución del teclado en el VDA.

### Sugerencia:

Esta función se ofrece en la aplicación Citrix Workspace para Windows y es compatible tanto con aplicaciones como con escritorios publicados.

## Configuración

Esta función está inhabilitada de forma predeterminada. Use la utilidad **ctxreg** para habilitar o inhabilitar esta función. Configurar la función en un Linux VDA determinado significa que esa función se aplicará a todas las sesiones en ese VDA.

La clave de configuración es “HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SyncKeyboardLa” y el tipo es DWORD.

Para habilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout
   " -d "0x00000001"
2 <!--NeedCopy-->
```

Para inhabilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout
   " -d "0x00000000"
2 <!--NeedCopy-->
```

## Uso

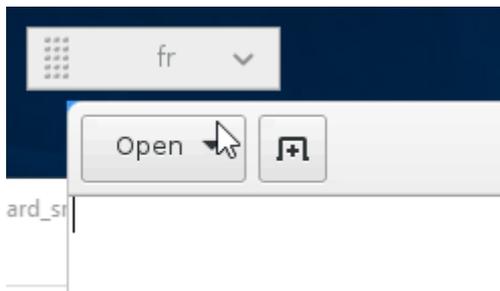
Con esta función habilitada, cuando la distribución del teclado cambia en el dispositivo cliente durante una sesión, también cambia la distribución del teclado de la sesión.

Por ejemplo, si cambia la distribución del teclado en un dispositivo cliente a francés (FR):



La distribución del teclado de la sesión de Linux VDA también cambia a “fr”.

En una sesión de aplicación, puede ver este cambio automático si tiene habilitada la barra de idioma:



En una sesión de escritorio, puede ver este cambio automático en la barra de tareas:

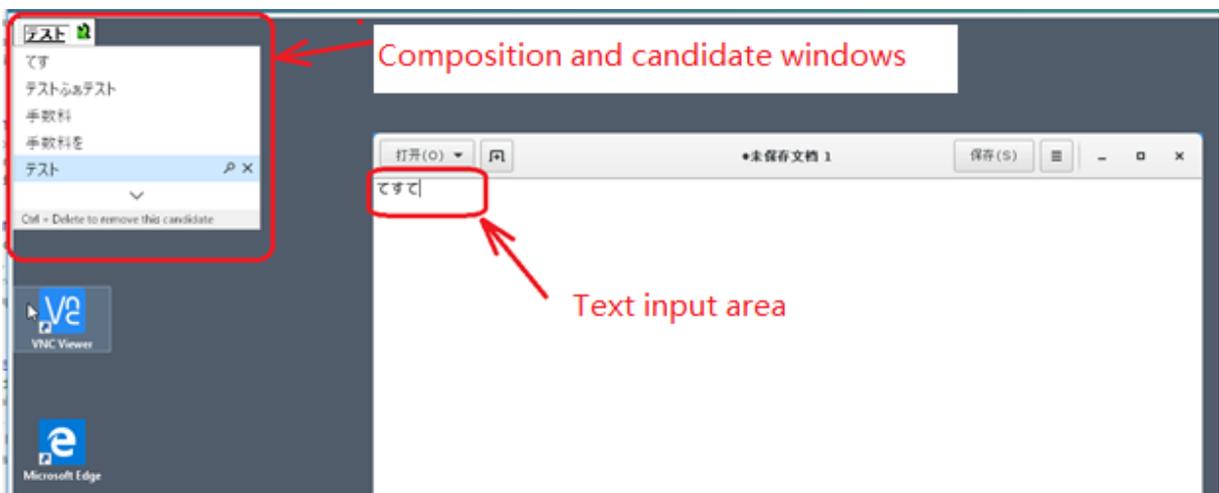


## Sincronización de la interfaz de usuario IME del cliente

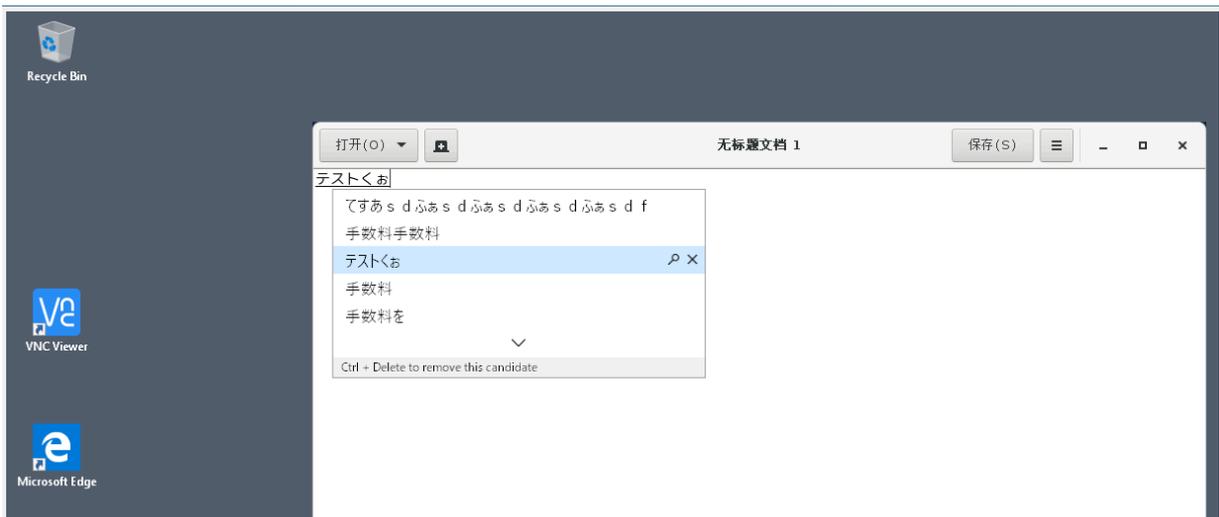
November 3, 2021

### Introducción

Hasta la fecha, la interfaz de usuario IME del cliente (incluida la ventana de redacción y la ventana de candidatos) se situaba en la esquina superior izquierda de la pantalla. No seguía al cursor y, a veces, se situaba lejos del cursor en el área de entrada de texto:



Citrix aumenta la usabilidad y mejora la experiencia de usuario con el cliente IME de la siguiente manera:



**Nota:**

La función está disponible para RHEL 7.x, CentOS 7.x, Ubuntu 16.04, Ubuntu 18.04 y SUSE 12.x. Se admite en la aplicación Citrix Workspace para Windows y para Mac.

Para utilizar la función en sesiones de escritorio con RHEL 7.x, debe habilitar IBus. Por ejemplo, establezca el idioma de la interfaz de usuario en uno que requiera un método de entrada (IME) para escribir texto, o bien agregue **GTK\_IM\_MODULE=ibus** al archivo **`\${HOME}/.config/imsettings/xinputrc**.

La función se instala automáticamente, pero debe habilitarla para poder usarla.

## Habilitar e inhabilitar la función

Esta función está inhabilitada de forma predeterminada. Use la utilidad **ctxreg** para habilitar o inhabilitar esta función. Configurar la función en un Linux VDA determinado significa que esa función se aplicará a todas las sesiones en ese VDA.

Para habilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncClientIME" -d
   "0x00000001"
2 <!--NeedCopy-->
```

Para inhabilitar esta función, ejecute el comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncClientIME" -d
   "0x00000000"
2 <!--NeedCopy-->
```

## HDX Insight

February 12, 2024

### 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 Citrix ADC o Citrix SD-WAN.

Linux VDA admite parcialmente la función 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 algunos puntos de datos de duración.

## Instalación

No es necesario instalar paquetes dependientes.

## Uso

HDX Insight analiza los mensajes de ICA pasados a través de Citrix ADC 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](#).

## 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 Citrix ADC o se ha configurado una instancia de Citrix ADC incorrecta en Citrix ADM.

- 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.

## Transporte adaptable

November 3, 2021

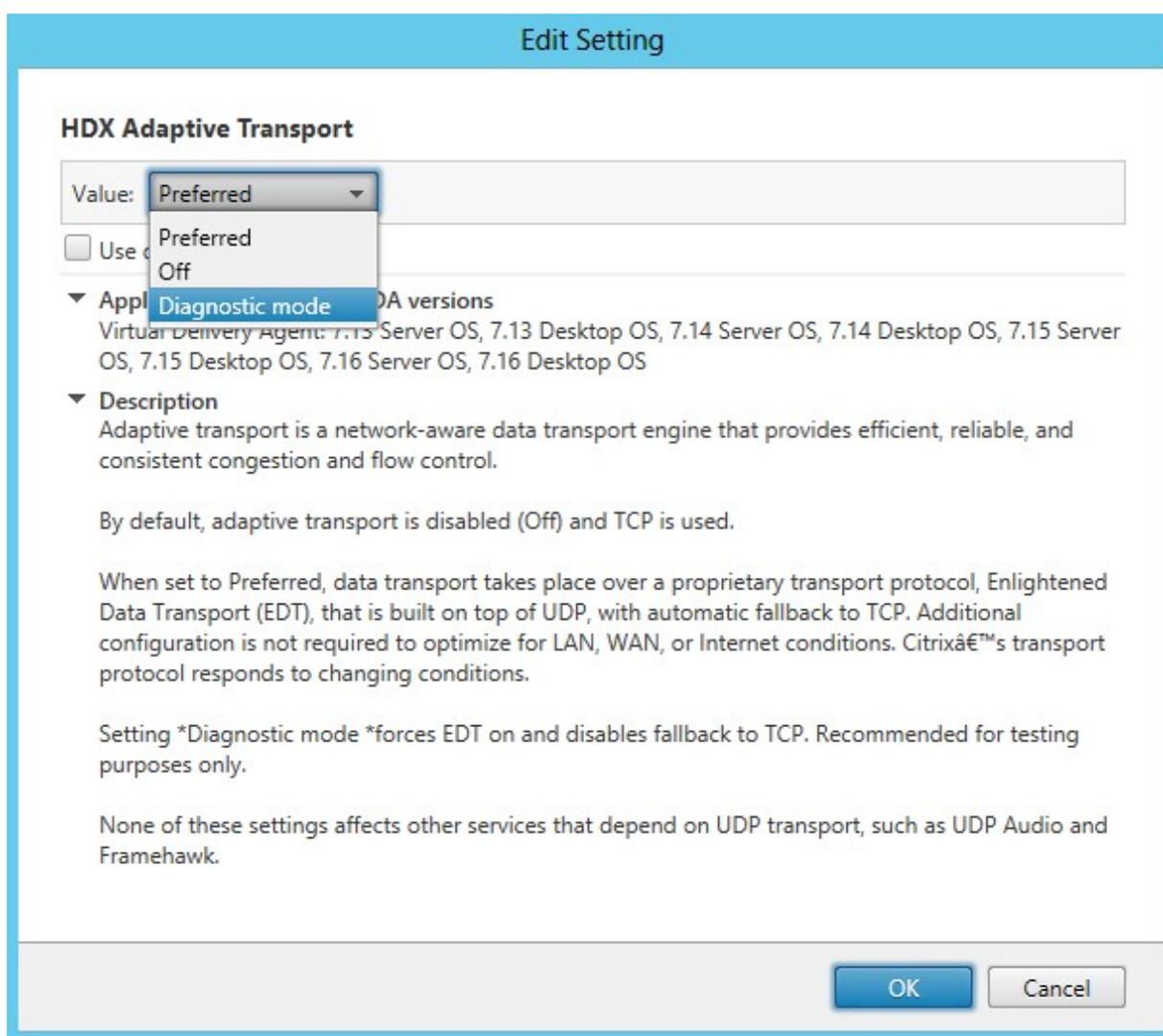
Anteriormente disponible como una función experimental, el transporte adaptable es una función totalmente compatible en esta versión.

El transporte adaptable es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops. Es más rápido, más escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones de Internet y WAN difíciles de largo recorrido. Para obtener más información, consulte [Transporte adaptable](#).

### Habilitar transporte adaptable

En Citrix Studio, compruebe que la directiva **Transporte adaptable HDX** está establecida en el modo **Preferido** o de **Diagnóstico**. Se selecciona **Preferido** de forma predeterminada.

- **Preferido:** se utiliza el transporte adaptable por Enlightened Data Transport (EDT) cuando sea posible; cuando no lo sea, se recurre a TCP.
- **Modo de diagnóstico:** se aplica el uso de EDT y la opción de recurrir a TCP está inhabilitada.



## Inhabilitar el transporte adaptable

Para inhabilitar el transporte adaptable, **desactive** la **directiva de transporte adaptable HDX** en Citrix Studio.

## Solución de problemas

### Comprobar si el transporte adaptable está habilitado

Ejecute este comando para comprobar si los agentes de escucha UDP están en ejecución.

```
1 netstat -an | grep "1494|2598"
2 <!--NeedCopy-->
```

En situaciones habituales, el resultado es similar a este:

```
1  udp          0          0  0.0.0.0:2598          0.0.0.0:*
2
3  udp          0          0  :::1494                :::*
4  <!--NeedCopy-->
```

## Rastreo activado

September 30, 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`:

```
1  setlog help
2  <!--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`:

```
1 setlog values
2
3 log_path (Log Output Path) = /var/log/xdl/hdx.log
4
5 log_size (Max Log Size (MiB)) = 200
6
7 log_count (Max Old Log Files) = 2
8 <!--NeedCopy-->
```

Ver o establecer un solo valor de `setlog`:

```
1 setlog value <name> [<value>]
2 <!--NeedCopy-->
```

Por ejemplo:

```
1 setlog value log_size 100
2 <!--NeedCopy-->
```

**Niveles** De forma predeterminada, los niveles de registro se establecen como **advertencia** (no se distingue entre mayúsculas y minúsculas).

Para ver los niveles de registro establecidos para los distintos componentes, ejecute el siguiente comando:

```
1 setlog levels
2 <!--NeedCopy-->
```

Para configurar los niveles de registro (incluidos Disable, Inherited, Verbose, Information, Warnings, Errors y Fatal Errors), ejecute el siguiente comando:

```
1 setlog level <class> [<level>]
2 <!--NeedCopy-->
```

---

Nivel de registro	Parámetro de comando (no se distingue entre mayúsculas y minúsculas)
Inhabilitado	none
Heredado	inherit
Detallado	verbose

Nivel de registro	Parámetro de comando (no se distingue entre mayúsculas y minúsculas)
Información	info
Advertencia	warning
Errores	error
Errores irreuperables	fatal

---

La variable **<class>** especifica un componente de Linux VDA. Para cubrir todos los componentes, establézcalos todos. Por ejemplo:

```
1 setlog level all error
2 <!--NeedCopy-->
```

**Marcas** De forma predeterminada, las marcas se configuran como se muestra a continuación:

```
1 setlog flags
2
3 DATE = true
4
5 TIME = true
6
7 NAME = true
8
9 PID = true
10
11 TID = false
12
13 SID = true
14
15 UID = false
16
17 GID = false
18
19 CLASS = false
20
21 LEVEL = false
22
23 FUNC = true
24
25 FILE = false
26 <!--NeedCopy-->
```

Ver las marcas actuales:

```
1 setlog flags
2 <!--NeedCopy-->
```

Ver o establecer una sola marca de registro:

```
1 setlog flag <flag> [<state>]
2 <!--NeedCopy-->
```

**Restaurar valores predeterminados** Revertir todos los niveles, las marcas y los valores a los parámetros predeterminados:

```
1 setlog default
2 <!--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`:

```
1 Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
   configuration file.
2
3 Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE
4
5 Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.
6
7 Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
8 <!--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.

## Remedar sesiones

November 3, 2021

La función Remedo de sesiones permite a los administradores de dominio ver las sesiones ICA de los usuarios en una red de intranet. Esta función usa noVNC para conectarse a las sesiones ICA y solo se admite en RHEL 7.x y Ubuntu 16.04.

**Nota:**

Para usar la función de remedo de sesiones, la versión de Citrix Director debe ser 7.16 o una versión posterior.

## Instalación y configuración

### Dependencias

Se requieren dos dependencias nuevas, `python-websockify` y `x11vnc`, para el remedo de sesiones. Las dependencias `python-websockify` y `x11vnc` se instalan automáticamente cuando se instala Linux VDA en Ubuntu 16.04. En RHEL 7.x, debe instalar `python-websockify` y `x11vnc` manualmente después de instalar Linux VDA.

Ejecute el siguiente comando en RHEL 7.x para instalar `python-websockify` y `x11vnc` (`x11vnc` versión 0.9.13 o posterior).

```
1 sudo yum install -y python-websockify x11vnc
2 <!--NeedCopy-->
```

Para resolver `python-websockify` y `x11vnc`, habilite los siguientes repositorios en RHEL 7.x:

- Extra Packages for Enterprise Linux (EPEL)

El repositorio EPEL es necesario tanto para `python-websockify` como para `x11vnc`. Ejecute el siguiente comando para habilitar el repositorio de EPEL:

```
1 sudo yum install https://dl.fedoraproject.org/pub/epel/epel-
   release-latest-$(rpm -E '%{
2   rhel }
3   ').noarch.rpm
4 <!--NeedCopy-->
```

- RPM opcionales

Ejecute uno de estos comandos para habilitar el repositorio de RPM opcionales para instalar algunos paquetes de dependencias de `x11vnc`:

Para la estación de trabajo:

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-
   rpms
2 <!--NeedCopy-->
```

Para el servidor:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

## Port

La función de remedo de sesiones selecciona automáticamente los puertos disponibles desde el puerto 6001 al puerto 6099 para crear las conexiones de Linux VDA a Citrix Director. Por lo tanto, la cantidad de sesiones ICA que puede remedar simultáneamente se limita a 99. Compruebe que haya puertos disponibles suficientes para ajustarse a sus necesidades, sobre todo para el remedo de varias sesiones.

## Registro

Esta tabla contiene los registros relacionados:

Registro	Descripción	Valor predeterminado
EnableSessionShadowing	Activa o desactiva el remedo de sesiones.	1 (Habilitada)
ShadowingUseSSL	Determina si cifrar la conexión entre Linux VDA y Citrix Director.	0 (Inhabilitada)

Ejecute el comando `ctxreg` en Linux VDA para cambiar los valores de Registro. Por ejemplo, para inhabilitar el remedo de sesiones, ejecute el siguiente comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -v "EnableSessionShadowing" -d 0x00000000
```

## SSL

La conexión noVNC entre Linux VDA y Citrix Director usa el protocolo WebSocket. Para el remedo de sesiones, es el registro “ShadowingUseSSL” mencionado anteriormente quien determina si se selecciona `ws://` o `wss://`. De forma predeterminada, se elige `ws://`. Sin embargo, por razones de seguridad, Citrix recomienda usar `wss://` e instalar certificados en cada cliente Citrix Director y en cada servidor Linux VDA. Citrix renuncia a toda responsabilidad de seguridad sobre el remedo de sesiones de Linux VDA mediante `ws://`.

**Obtener certificados SSL raíz y de servidor** Los certificados deben estar firmados por una entidad de confianza llamada Entidad de certificación (CA).

Se necesita un certificado de servidor (clave incluida) por cada servidor Linux VDA donde quiera configurar SSL. Un certificado de servidor identifica a un equipo concreto, de modo que necesita el nombre de dominio completo (FQDN) de cada servidor. Para mayor comodidad, puede usar un certificado comodín para todo el dominio. En ese caso, debe conocer al menos el nombre de dominio.

Además de instalar un certificado de servidor en cada servidor, debe instalar un certificado raíz de la misma autoridad de certificación en cada cliente Citrix Director que se comunice con el servidor Linux VDA. Los certificados de raíz están disponibles en las mismas CA que emiten los certificados de servidor. Puede instalar certificados de servidor y de cliente provenientes de una autoridad de certificación: integrada en el sistema operativo, de la empresa (una autoridad de certificación que su empresa pone a su disposición) o una CA no integrada en el sistema operativo. Consulte al equipo de seguridad de su organización para saber qué método es necesario para obtener certificados.

**Importante:**

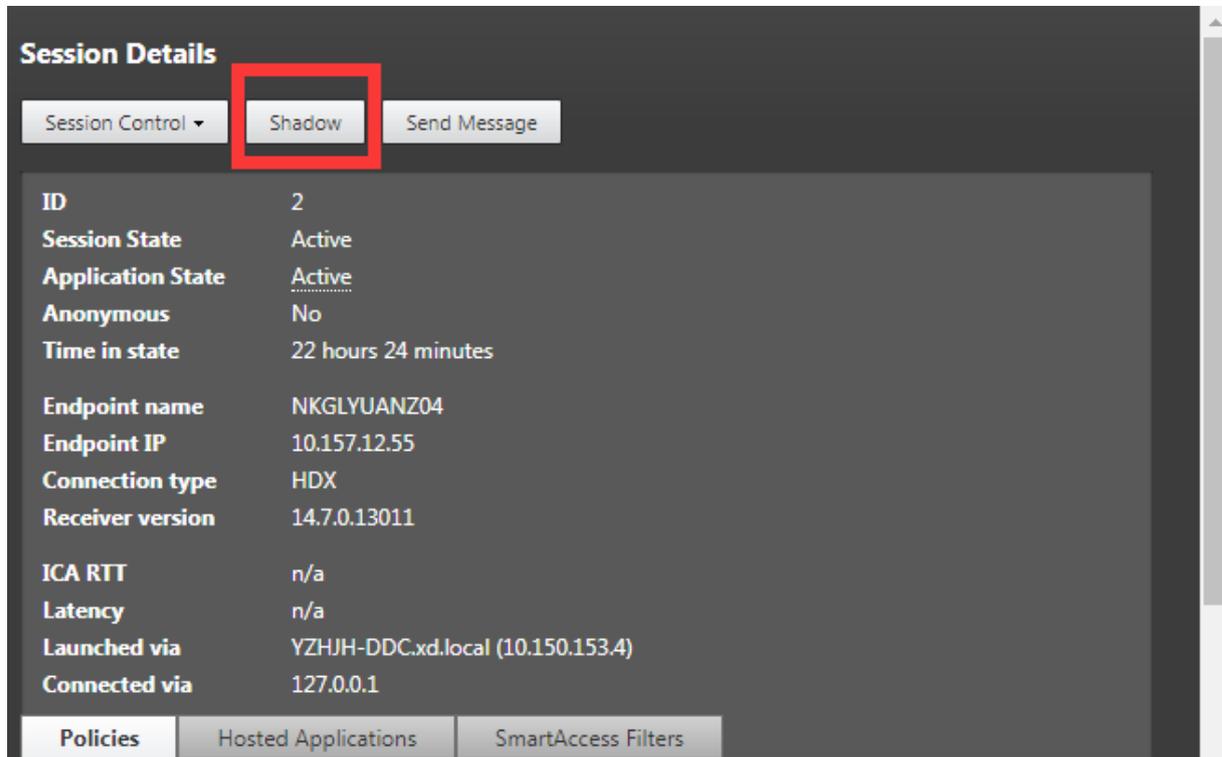
- El nombre común de un certificado de servidor debe contener el FQDN exacto del servidor Linux VDA o, al menos, el comodín y los caracteres de dominio correctos. Por ejemplo, vda1.dominiobase.com o \*.dominiobase.com.
- Algunos exploradores Web no admiten los algoritmos hash, incluidos SHA1 y MD5, porque estos ofrecen demasiado poca seguridad para las firmas en los certificados digitales. Por lo tanto, se especifica SHA-256 como el estándar mínimo.

**Instalar un certificado raíz en cada cliente Citrix Director** El remedio de sesiones usa el mismo almacén de certificados (basado en el registro del sistema) que IIS, de modo que se puede instalar certificados con IIS o el complemento de certificados de Microsoft Management Console (MMC). Cuando reciba un certificado de la entidad de certificación, puede reiniciar el asistente para certificados de servidor web en IIS y será el asistente quien instalará el certificado. Como alternativa, puede ver e importar certificados en el equipo. Para ello, abra MMC y agregue el certificado como un complemento independiente a dicha consola. Internet Explorer y Google Chrome importan los certificados instalados en su sistema operativo de forma predeterminada. Para Mozilla Firefox, debe importar los certificados SSL raíz en la ficha **Autoridades** del Administrador de certificados.

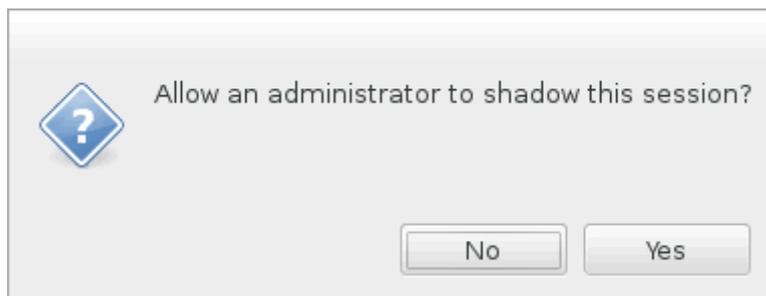
**Instalar un certificado de servidor y su clave en cada servidor Linux VDA** Denomine los certificados de servidor “shadowingcert.\*” y el archivo de clave “shadowingkey.\*” (el asterisco, \*, puede indicar el formato, como en shadowingcert.csr y shadowingkey.key). Coloque los certificados de servidor y los archivos de clave en la ruta **/etc/xdl/shadowingssl** y protéjalos con permisos restringidos. Un nombre o una ruta incorrectos impide a Linux VDA encontrar un certificado o archivo de clave concreto, lo que causa un error de conexión con Citrix Director.

## Uso

Desde Citrix Director, busque la sesión de destino y haga clic en **Remedar** en la vista **Detalles de la sesión** para enviar una solicitud de remedo a Linux VDA.



Una vez inicializada la conexión, aparece una confirmación en el cliente de la sesión ICA (no en el cliente Citrix Director) para solicitar permiso al usuario para remedar la sesión.



Si el usuario hace clic en **Sí**, aparecerá una ventana en la parte de Citrix Director que indicará que se está aplicando el remedo a la sesión ICA.

Para obtener más información de uso, consulte la documentación de [Citrix Director](#).

## Limitaciones

- El remedo de sesiones está pensado para usarlo únicamente en la intranet. No funciona para redes externas, ni siquiera en conexiones a través de Citrix Gateway. Citrix renuncia a cualquier responsabilidad sobre el remedo de sesiones de Linux VDA en una red externa.
- Con el remedo de sesiones habilitado, un administrador de dominio solo puede ver las sesiones ICA (no tiene permiso de escritura en ellas ni las controla).
- Después de que un administrador haga clic en **Remedar** en Citrix Director, aparecerá una confirmación donde se pide permiso al usuario para remedar la sesión. Una sesión solo puede remedarse cuando el usuario de la sesión lo permita.
- La confirmación mencionada tiene 20 segundos de tiempo de espera. Por tanto, una solicitud de remedo falla cuando se agota este tiempo.
- Solo un administrador puede remedar una sesión ICA en una ventana de Citrix Director. Si un administrador A remeda una sesión ICA mientras un administrador B envía una solicitud de remedo, la confirmación para obtener el permiso del usuario vuelve a aparecer en el dispositivo del usuario. Si el usuario permite el segundo remedo, la conexión de remedo del administrador A se detiene y se crea una nueva conexión de remedo para el administrador B. Ocurre lo mismo si un mismo administrador envía otra solicitud de remedo a la misma sesión ICA.
- Para utilizar el remedo de sesiones, instale Citrix Director 7.16 o una versión posterior.
- Un cliente Citrix Director utiliza un FQDN, en lugar de una dirección IP, para conectarse al servidor Linux VDA de destino. Por lo tanto, el cliente Citrix Director debe poder resolver el FQDN del servidor Linux VDA.

## Solución de problemas

Si falla un remedo de sesiones, depure el cliente Citrix Director y el VDA de Linux.

### En el cliente Citrix Director

Con las herramientas de desarrollador que ofrece el explorador Web, consulte los registros de salida en la ficha **Consola**. O bien, consulte la respuesta de la API ShadowLinuxSession en la ficha **Red**. Si la confirmación para obtener el permiso del usuario aparece, pero la conexión no se crea, haga ping manualmente al FQDN del Linux VDA para comprobar si Citrix Director puede resolver el FQDN. En caso de un problema con la conexión `wss://`, compruebe que los certificados están en orden.

### En Linux VDA

Compruebe que la confirmación para obtener el permiso del usuario aparece en respuesta a una solicitud de remedo. Si no aparece, consulte los archivos `vda.log` y `hdx.log` para averiguar el porqué. Para

obtener el archivo vda.log, lleve a cabo lo siguiente:

1. Busque el archivo `/etc/xdl/ctx-vda.conf`. Quite los comentarios de la siguiente línea para habilitar la configuración vda.log:

```
Log4jConfig="/etc/xdl/log4j.xml"
```

2. Abra `/etc/xdl/log4j.xml`, busque la parte `com.citrix.dmc`, y cambie “info” por “trace”, tal como se muestra a continuación:

```
1 <!-- Broker Agent Plugin - Director VDA plugin Logger -->
2
3 <logger name="com.citrix.dmc">
4
5     <level value="trace"/>
6
7 </logger>
8 <!--NeedCopy-->
```

3. Ejecute el comando `service ctxvda restart` para reiniciar el servicio `ctxvda`.

En caso de error durante la creación de la conexión:

1. Compruebe si hay alguna limitación de firewall que impida que el remedio de sesiones abra el puerto.
2. En el caso de utilizar SSL, compruebe que los certificados y los archivos de clave tengan los nombres correctos. Asimismo, compruebe que se encuentran en la ruta adecuada.
3. Compruebe que haya suficientes puertos entre 6001 y 6099 para las nuevas solicitudes de remedio de sesiones.

## Compatibilidad de la aplicación Citrix Workspace para HTML5

November 3, 2021

A partir de esta versión, podrá usar la aplicación Citrix Workspace para HTML5 para acceder a las aplicaciones y escritorios virtuales de Linux de forma directa sin tener que conectar su cliente a Citrix Gateway. Para obtener información acerca de la aplicación Citrix Workspace para HTML5, consulte la [documentación de Citrix](#).

### Habilite esta función

Esta función está inhabilitada de forma predeterminada. Para habilitarla, haga lo siguiente:

1. En Citrix StoreFront, habilite la aplicación Citrix Workspace para HTML5.

Para ver información detallada sobre el procedimiento, consulte el Paso 1 del artículo [CTX208163](#) de Knowledge Center.

2. Habilite las conexiones de WebSocket.

- a) En Citrix Studio, establezca la directiva **Conexiones de WebSockets** en **Permitida**.

También puede configurar las otras directivas de WebSocket. Para obtener una lista completa de las directivas de WebSocket, consulte [Configuraciones de directivas de WebSockets](#).

- b) En el VDA, reinicie el servicio `ctxvda` y el servicio `ctxhdx`, en este orden, para que el parámetro surta efecto.
- c) En el VDA, ejecute el siguiente comando para comprobar si la escucha de WebSocket sigue ejecutándose.

```
netstat -an | grep 8008
```

Cuando se está ejecutando la escucha de WebSocket, el resultado del comando se parece a lo siguiente:

```
tcp 0 0 :::8008 :::* LISTEN
```

**Nota:** También puede habilitar el cifrado TLS para proteger las conexiones WebSocket. Para obtener información sobre cómo habilitar el cifrado TLS, consulte [Proteger sesiones de usuario con TLS](#).

## Supervisar sesiones de Linux en Citrix Director

June 14, 2023

Están disponibles las siguientes métricas para las sesiones de Linux en Citrix Director. Para ver las métricas, busque la sesión en Citrix Director y consulte el panel **Detalles de la sesión**.

- RTT de ICA

A partir de Linux VDA 1903, están disponibles las métricas de RTT de ICA. Para ver las métricas de RTT de ICA, utilice Citrix Director 1903 o una versión posterior y cree las directivas **Cálculo del tiempo de retorno ICA** e **Intervalo de cálculo del tiempo de retorno ICA** en Citrix Studio. Para obtener información acerca de la creación de directivas, consulte [Crear una directiva mediante Studio](#).

- Protocolo

A partir de Linux VDA 1909, dispone de información sobre el protocolo. El protocolo de transporte de una sesión de Linux aparece como **UDP** o **TCP** en el panel **Detalles de la sesión**.

## Demonio del servicio de supervisión

November 3, 2021

El demonio del servicio de supervisión comprueba los servicios clave mediante escaneos periódicos. Al detectar excepciones, el demonio reinicia o detiene los procesos de servicio y limpia los residuos de los procesos para liberar recursos. Las excepciones detectadas se registran en el archivo **/var/log/xdl/ms.log**.

### Configuración

El demonio del servicio de supervisión se inicia automáticamente al iniciar el VDA.

Puede configurar la función a través de los archivos **scanningpolicy.conf**, **rulesets.conf** y **whitelist.conf** con privilegios de administrador. Los archivos de configuración se encuentran en **/opt/Citrix/VDA/sbin**.

Para aplicar los cambios en los archivos **scanningpolicy.conf**, **rulesets.conf** y **whitelist.conf**, ejecute el siguiente comando para reiniciar el demonio del servicio de supervisión.

```
1 service ctxmonitorservice restart
2 <!--NeedCopy-->
```

- **scanningpolicy.conf**

Este archivo de configuración habilita o inhabilita el demonio del servicio de supervisión. Establece el intervalo de detección del servicio y especifica si se deben reparar las excepciones detectadas.

- MonitorEnable: true/false (“true”de forma predeterminada)
- DetectTime: 20 (unidad: segundos, valor predeterminado: 20, valor mínimo: 5)
- AutoRepair: true/false (“true”de forma predeterminada)
- MultBalance: false
- ReportAlarm: false

- **rulesets.conf**

Este archivo de configuración especifica los servicios que se van a supervisar. Hay cuatro servicios supervisados de forma predeterminada, tal y como se muestra en la siguiente captura de pantalla.

```
MonitorUser: all
MonitorType: 3
ProcessName: ctxhdx
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: ctxvda
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: ctxpolicyd
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: Xorg
Operation: 8
DBRecord: false
```

Para configurar cada servicio que se deba supervisar, defina los siguientes campos.

- MonitorUser: all
- MonitorType: 3
- ProcessName: <> (el nombre del proceso no se puede dejar vacío y debe coincidir exactamente)
- Operación: 1/2/4/8 (1 = detiene el servicio cuando se detectan excepciones; 2 = finaliza el servicio cuando se detectan excepciones; 4 = reinicia el servicio; 8 = limpia los residuos de los procesos Xorg)
- DBRecord: false

- **whitelist.conf**

Los servicios especificados en el archivo **rulesets.conf** también deben configurarse en el archivo **whitelist.conf**. La configuración de la lista de permitidos es un filtro secundario por seguridad.

Para configurar la lista de permitidos, incluya solamente los nombres de los procesos (que deben coincidir exactamente) en el archivo **whitelist.conf**. La siguiente captura de pantalla le sirve de ejemplo.

```
ctxcdmd
ctxcdmmount
ctxcdmstat
ctxceip
ctxclipboard
ctxconnect
ctxcredentialctl
ctxctl
ctxcupsd
ctxdisconnect
ctxeuem
ctxfiletransfer
ctxgfx
ctxhdx
ctxism
ctxlogd
ctxlogin
ctxmonitorservice
ctxmrvc
ctxpolicyd
ctxscardsd
ctxvhcid
ctxvda
Xorg
```

**Nota:**

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

## Proteger sesiones de usuario con TLS

February 24, 2022

A partir de la versión 7.16, Linux VDA admite el cifrado TLS para proteger las sesiones de usuario. El cifrado TLS está inhabilitado de forma predeterminada.

### Habilitar el cifrado TLS

Para habilitar el cifrado TLS y proteger las sesiones de usuario, deber obtener certificados y habilitar el cifrado TLS en el Linux VDA y el Delivery Controller (el Controller).

## **Obtener certificados**

Debe obtener los certificados de servidor en formato PEM y los certificados raíz en formato CRT desde una entidad de certificación (CA) de confianza. Un certificado de servidor contiene estas secciones:

- Certificado
- Clave privada no cifrada
- Certificados intermedios (opcional)

Un ejemplo de certificado de servidor:

# Linux Virtual Delivery Agent 1912 LTSR

```
-----BEGIN CERTIFICATE-----
MIIDTCCArAgAwIBAgIJA1uncp1qGXCMa0GCSqGSIb3DQEBAQAgCzA3BgNV
BAYTA1VLMR.IwEAYDVQIEwIDYwL1cm1kZ2UxEjAQBGNVACTCUNhbwJvdXJzTEU
MBIGAlUEChMLQ210cm14IFR1c3QxGjAYBgNVBAMTEWVhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDUwNjE0MDkxNDYwNjE0MDkxNDYwNjE0MDkxNDYwNjE0MDkxNDYw
MR.IwEAYDVQIEwIDYwL1cm1kZ2UxEjAQBGNVACTCUNhbwJvdXJzTEUwBAYTA1VL
CHMLQ210cm14IFR1c3QxGjAYBgNVBAMTEWVhMDAxLmNpdHJpdGUubmV0ZFOZTEgMB4G
A1UEAAMXy2EwMDEtc2MwMDEuY210cm10ZS5uZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
gY0AMIGJAoGBALCTT0dxc1vbI0L0F66xg05gkVeIGKVP+37p5KV8B661wCVzr6p9
t72Fa+9ocCf2x/ue274NXFc4fqGRDsrEw13yxM6COyBf7L6psrCDNnBf1q8TJH
4xoPIUeaw4MvK/3PvyfHhKs4fz8yy1I4VdnXVhHw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwgdKvCQYDVR0TBAlwADABgNVHQ4EFgQUrLi1dzyot+CUXSh9xMfP1M+/08y0w
gZkGAlUdIwSBKTCBj0AU85kN1EP30cVhcoss1s1seDQwGSKha6RpmGcxCzA3BgNV
BAYTA1VLMR.IwEAYDVQIEwIDYwL1cm1kZ2UxEjAQBGNVACTCUNhbwJvdXJzTEU
MBIGAlUEChMLQ210cm14IFR1c3QxGjAYBgNVBAMTEWVhMDAxLmNpdHJpdGUubmV0
ggkAy8nCd8c32EwEQYJYIZIAyB4QgEBAQAgvMA0GCSqGSIb3DQEBAQAA4GB
AD5a8YhWIXJ32Nt2zdXnbp200yUTowE1Bwqe/9cGaP6CpJoxJ7F3a2/8IpaT68
Ve1Bu1SEY1GKGCw93pc7sPKqb8pGBRi5/dygb+geFk1qYvbu0Ijotr3pkXae
b6CF3tNludHUrWf610rB72zbyz3P1Ix+HEwtLj0j5Z4K
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBoGqk0zncXIr2yNc98eusyYUvJDXi811T/t+6u11fAeupvg1c6+q
fBe9HwvvaAnH9s7ntu+DVxxIOH6hk7KxMNd2MTGjsgX+y+qbK7AgzWnT9avEy
R+MaDYf1Hm1uDFZP9z1cn4RyOH8/MstSOFO511R4cPtEUNgatZcLEYZnIDAQAB
AoGBAKwBgZu/bL8edgB8YPU7d1i8X89I0s4b/apJm+Jdmjxb8N96rsP024p9Ea
FTUc9+1L8mEroLubSicCXjsJFc+cxg9VvaNaEeKkBJ73SoCUErQsX0yb/1Adck/
FXzU0tqytUe/KHgcSgjtjrSeqlJqMm+yyzBAatVRRtZGdwAHAKEA311KRZjINSuz
Enm12RTI3ngBhP/S3GEBvJfKsD5n2R190+ooEPxc1vvp5ne8Q0zupshbJfEPbOC
ykZ6UassFwJBAMTISyPnV9ewPzJoanJZIJCMNtXDCsh1xx1j1yzv+Qmr8RuQz9PV
fIenmTrfz+wo4DaKg+8ar20vOnKFOHFAMDECOQDEwR1H6cE3wyCfN1u942M9Xkhr
GvSpr7+//vL6Nwv3CwPv9n8DTP1+wuDKJ29nCVrte119M1aMTYjs3a1NvAKEA
qy5JzZcBnryZMbV032jju7ZPISnhTGO1x0jZMSLLTPGpNLN34b0k3sTc1r8L42E
uQjTQRm+wdsrVF31FazkQJAnudmsUv3gZkHmGaV2hz1dXIhfyOIV++31eZHQY6
h5EmxS2S50TvyNGt2e6m2gaZnjTagH59TCBhV85nof2g==
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDGTCCAKAgAwIBAgIJA1MvJwvHXAd9HMA0GCSqGSIb3DQEBAQAgCzA3BgNV
BAYTA1VLMR.IwEAYDVQIEwIDYwL1cm1kZ2UxEjAQBGNVACTCUNhbwJvdXJzTEU
MBIGAlUEChMLQ210cm14IFR1c3QxGjAYBgNVBAMTEWVhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDUwNjE0MDkxNDYwNjE0MDkxNDYwNjE0MDkxNDYwNjE0MDkxNDYw
EjAQBGNVAgTCUNhbwJyAWRnZTESMBA1UEBXMJQ2FtyM91cm51MRQwEgYDVQK
EwTdaXRYaXgvgVzdDeaMbgAlUEAMRY2EwMDEuY210cm10ZS5uZmVzZmVzZmVzZmVz
KozIhvcNAQEBBQADgY0AMIGJAoGBAKVzmF7Uj7U0nvo3QwdfOnr3qkNzDxpwrZ
zh8cI9Vv+UFRU1C6o87izLtbMFn3FOU712cfkHN3ZG117p89pdyjket1Ms1Ve3w
acoqrVvD+fNsvJjunTbaCywTALjmFSfMHeZJXVScKrpEhKOnkMS16tcrya/K/
oss1zV3AgMBAAGjgCwGckwDAYDVR0TBAlwADABgNVHQ4EFgQU85kN1EP3
0cVhcoss1s1seDQwGSIwZkGAlUdIwSBKTCBj0AU85kN1EP30cVhcoss1s1seDQw
GSKha6RpmGcxCzA3BgNVBAYTA1VLMR.IwEAYDVQIEwIDYwL1cm1kZ2UxEjAQBGNV
BACTCUNhbwJvdXJzTEUwBAYTA1VLMR.IwEAYDVQIEwIDYwL1cm1kZ2UxEjAQBGNV
MDAxLmNpdHJpdGUubmV0ggkAy8nCd8c32EwEQYJkOZiHvcNAQEBBQADgYEAIZ4Z
gXLLXf12RNqh/awtsb41UgV8BZKAsg5zHNA1TiXbz2C13ec53Fb6nigMw5T11
UNCLXmXrNu1D400tESLX9ACUNH3194yXoguJKs08n121jj2TVfB832Rm5DBY3g
UmKORn/hdqM1Cope5w06as6+HN4wU0+HEtUMWE=
-----END CERTIFICATE-----
```

## Habilitar el cifrado TLS

**Habilitar el cifrado TLS en Linux VDA** En Linux VDA, utilice la herramienta **enable\_vdassl.sh** para habilitar (o inhabilitar) el cifrado TLS. La herramienta se encuentra en el directorio **/opt/Citrix/VDA/sbin**. Para obtener información acerca de las opciones disponibles en la herramienta, ejecute el comando **/opt/Citrix/VDA/sbin/enable\_vdassl.sh -help**.

**Sugerencia:** Debe instalar un certificado de servidor cada servidor Linux VDA; debe instalar certificados raíz en cada cliente y servidor Linux VDA.

## Habilitar el cifrado TLS en el Controller

### Nota:

Solo puede habilitar el cifrado TLS para grupos de entrega enteros. No puede habilitar el cifrado TLS para aplicaciones específicas.

En una ventana de PowerShell en el Controller, ejecute estos comandos uno tras otro para habilitar el cifrado TLS para el grupo de entrega de destino.

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true`

### Nota:

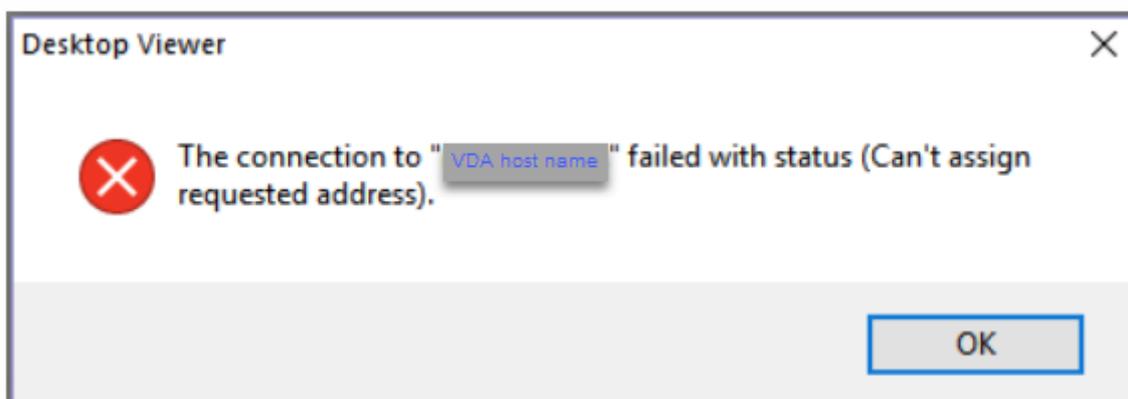
Para asegurarse de que solo los nombres de dominio completos de los VDA están contenidos en el archivo de una sesión ICA, también puede ejecutar el comando **Set-BrokerSite -DnsResolutionEnabled \$true**. Este comando habilita la resolución DNS. Si inhabilita la resolución DNS, el archivo de una sesión ICA revela las direcciones IP los de VDA y proporciona nombres de dominio completos únicamente para los elementos relacionados con TLS, como SSLProxyHost y UDPDTLSport.

Para inhabilitar el cifrado TLS en el Controller, ejecute estos comandos uno tras otro:

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $false`
3. `Set-BrokerSite -DnsResolutionEnabled $false`

## Solución de problemas

Es posible que se produzca el error “Can’t assign requested address” en la aplicación Citrix Workspace para Windows al intentar acceder a una sesión de escritorio pública:



Como solución temporal, agregue una entrada al archivo **hosts**, que sea similar a:

```
<IP address of the Linux VDA> <FQDN of the Linux VDA>
```

En las máquinas Windows, el archivo **hosts** normalmente se encuentra en `C:\Windows\System32\drivers\etc\hosts`.

## Proteger sesiones de usuario con DTLS

November 3, 2021

El cifrado DTLS es una función que se admite totalmente a partir de la versión 7.18. Esta función está habilitada de forma predeterminada en Linux VDA. Para obtener más información, consulte [Transport Layer Security](#).

### Habilitar cifrado DTLS

#### Verificar que el transporte adaptable está habilitado

En Citrix Studio, compruebe que la directiva **Transporte adaptable HDX** está establecida en el modo **Preferido** o de **Diagnóstico**.

### Habilitar cifrado SSL en Linux VDA

En Linux VDA, utilice la herramienta **enable\_vdassl.sh** para habilitar (o inhabilitar) el cifrado SSL. La herramienta se encuentra en `/opt/Citrix/VDA/sbin`. Para obtener información acerca de las opciones disponibles en la herramienta, ejecute el comando `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h`.

**Nota:**

Actualmente, Linux VDA admite DTLS 1.0 y DTLS 1.2. DTLS 1.2 requiere Citrix Receiver para Windows 4.12, o la aplicación Citrix Workspace 1808 para Windows y versiones posteriores. Si su cliente solo admite DTLS 1.0 (por ejemplo, Citrix Receiver para Windows 4.11), establezca **SSLMinVersion** en **TLS\_1.0** y **SSLCipherSuite** en **COM** o **ALL** con la herramienta **enable\_vdassl.sh**.

## Compatibilidad con tarjetas inteligentes

April 18, 2024

Puede usar una tarjeta inteligente conectada al dispositivo del cliente para autenticarse cuando inicie sesión en un escritorio virtual Linux. Esta función se implementa a través de la redirección de tarjetas inteligentes por el canal virtual ICA de tarjetas inteligentes. También puede usar la tarjeta inteligente dentro de la sesión. Los casos de uso pueden ser: agregar una firma digital a un documento, cifrar o descifrar un correo electrónico, o bien, autenticarse en un sitio Web que requiere la autenticación con tarjeta inteligente.

Linux VDA usa la misma configuración que Windows VDA para esta función. Para obtener más información, consulte la sección [Configurar el entorno de tarjeta inteligente](#) de este artículo.

La disponibilidad de la autenticación PassThrough con tarjeta inteligente depende de las condiciones siguientes:

- Linux VDA está instalado en RHEL 7.7.
- Se usan tarjetas inteligentes que admite CoolKey.
- Se usa la aplicación Citrix Workspace para Windows.

**Nota:**

No se admite oficialmente el uso de una tarjeta inteligente asignada dentro de una sesión de Linux VDA para iniciar sesión en Citrix Gateway.

## Instalar el software de Linux VDA en RHEL 7.7

Instale el software de Linux VDA desde el Administrador de paquetes RPM o [Easy Install](#); consulte la sección [Información general de la instalación](#).

Una vez completada la instalación del VDA, verifique que el VDA puede registrarse en el Delivery Controller y que las sesiones de escritorio Linux publicadas se pueden iniciar correctamente con la autenticación por contraseña.

## Comprobar que CoolKey admite la tarjeta inteligente

CoolKey es un controlador de tarjeta inteligente muy utilizado en RHEL. CoolKey admite cuatro tipos de tarjetas inteligentes: tarjetas CoolKey, CAC, PIV y PKCS#15. Sin embargo, la cantidad de tarjetas que se admiten y se validan formalmente sigue siendo limitada (consulte [Smart Card Support in Red Hat Enterprise Linux](#)).

En este artículo, se usa la tarjeta inteligente YubiKey 4 como ejemplo para ilustrar la configuración. YubiKey 4 es un dispositivo USB CCID PIV todo en uno que se puede comprar fácilmente en Amazon u otros vendedores a particulares. El controlador CoolKey admite YubiKey 4.



Si su organización necesita una tarjeta inteligente más avanzada, prepare una máquina física con RHEL 7.7 y el paquete CoolKey instalado. Para obtener información sobre la instalación de CoolKey, consulte [Instalar el controlador de tarjeta inteligente](#). Inserte su tarjeta inteligente y ejecute el siguiente comando para verificar que CoolKey la admite:

```
1 pkcs11-tool --module libcoolkeypk11.so --list-slots
2 <!--NeedCopy-->
```

Si CoolKey admite su tarjeta inteligente, el resultado del comando es similar al siguiente, donde se incluye información de la ranura.

```
[root@rhphy ~]# pkcs11-tool --module libcoolkeypk11.so --list-slots
Available slots:
Slot 0 (0x1): Yubico Yubikey 4 CCID 00 00
  token label      : user1
  token manufacturer :
  token model      :
  token flags      : login required, token initialized, PIN initialized, readonly
  hardware version  : 0.0
  firmware version  : 0.0
  serial num       :
[root@rhphy ~]#
```

utilizadas

## Configuración

### Preparar un certificado raíz

Un certificado raíz se utiliza para verificar el certificado que se encuentra en la tarjeta inteligente. Haga lo siguiente para descargar e instalar un certificado raíz.

1. Obtenga un certificado raíz en formato PEM, generalmente desde su servidor CA.

Puede ejecutar un comando similar al siguiente para convertir un archivo DER (\*.crt, \*.cer, \*.der) a PEM. En el siguiente ejemplo de comando, **certnew.cer** es un archivo DER.

```
1 openssl x509 -inform der -in certnew.cer -out certnew.pem
2 <!--NeedCopy-->
```

2. Instale el certificado raíz en el directorio `openssl`. El archivo **certnew.pem** se usa como ejemplo.

```
1 cp certnew.pem <path where you install the root certificate>
2 <!--NeedCopy-->
```

Para crear una ruta donde instalar el certificado raíz, ejecute `sudo mkdir -p <path where you install the root certificate>`.

### Configurar la base de datos NSS

El módulo de inicio de sesión de Linux VDA se basa en la base de datos NSS para acceder a las tarjetas inteligentes y los certificados. Haga lo siguiente para configurar la base de datos NSS.

1. Agregue el certificado raíz mencionado a la base de datos NSS.

```
1 certutil -A -n "My Corp Root" -t "CT,C,C" -a -d /etc/pki/nssdb -i
   /etc/pki/CA/certs/certnew.pem
2 <!--NeedCopy-->
```

2. Ejecute el siguiente comando para verificar que el certificado raíz se haya agregado correctamente a la base de datos NSS.

```
1 certutil -L -d /etc/pki/nssdb
2 <!--NeedCopy-->
```

El resultado del comando es similar al siguiente si el certificado raíz se agregó correctamente.

```
[root@rh73ws LVDA]# certutil -L -d /etc/pki/nssdb

Certificate Nickname                               Trust Attributes
SSL, S/MIME, JAR/XPI
My Corp Root                                       CT, C, C
```

### 3. Verifique si CoolKey está instalado en la biblioteca NSS PKCS#11.

```
1 modutil -list -dbdir /etc/pki/nssdb
2 <!--NeedCopy-->
```

El resultado del comando es similar al siguiente si el módulo CoolKey está instalado.

```
[root@rh73demo ~]# modutil -list -dbdir /etc/pki/nssdb
Listing of PKCS #11 Modules
-----
 1. NSS Internal PKCS #11 Module
    slots: 2 slots attached
    status: loaded

    slot: NSS Internal Cryptographic Services
    token: NSS Generic Crypto Services

    slot: NSS User Private Key and Certificate Services
    token: NSS Certificate DB

 2. CoolKey PKCS #11 Module
    library name: libcoolkeypk11.so
    slots: There are no slots attached to this module
    status: loaded
-----
```

Si el módulo CoolKey no está instalado, ejecute el siguiente comando para instalarlo manualmente y verifique la instalación nuevamente.

```
1 modutil -add "CoolKey PKCS #11 Module" -libfile libcoolkeypk11.so
  -dbdir /etc/pki/nssdb
2 <!--NeedCopy-->
```

### 4. Configure el módulo pam\_pkcs11.

El módulo pam\_pkcs11 se basa en la configuración del VDA local para verificar los certificados de usuario. El certificado raíz predeterminado que utiliza pam\_pkcs11 se encuentra en **/etc/pam\_pkcs11/cacerts/**. Todos los certificados raíz en esta ruta tienen un enlace hash. Ejecute los siguientes comandos para instalar el certificado raíz preparado y configurar pam\_pkcs11.

```
1 yum install pam_pkcs11
2
3 mkdir /etc/pam_pkcs11/cacerts/
4
5 cp certnew.pem /etc/pam_pkcs11/cacerts/
6
7 cacertdir_rehash /etc/pam_pkcs11/cacerts
8 <!--NeedCopy-->
```

## Configurar el entorno de tarjeta inteligente

Puede utilizar el script `ctxsmartlogon.sh` para configurar el entorno de tarjetas inteligentes o realizar la configuración manualmente.

- Utilice el script `ctxsmartlogon.sh` para configurar el entorno de tarjetas inteligentes

### Nota:

El script `ctxsmartlogon.sh` agrega información sobre PKINIT al dominio predeterminado. Puede cambiar esta configuración a través del archivo de configuración `/etc/krb5.conf`.

Antes de utilizar tarjetas inteligentes por primera vez, ejecute el script `ctxsmartlogon.sh` para configurar el entorno de tarjetas inteligentes.

### Sugerencia:

Si ha utilizado SSSD para unirse a un dominio, reinicie el servicio SSSD después de ejecutar `ctxsmartlogon.sh`.

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

Los resultados se asemejan a esto:

```
*****
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
*****
Step 1:Enable smart card logon.
Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
Please select which Active Directory integration method to use:
  1: Winbind
  2: SSSD
  3: Centrify
Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
Installing, please wait...
[krb5-pkinit][pam_krb5] already installed.
[pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
Packages installed. [Success]
Step 4:Configure krb5.conf.
Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
/etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):usr/lib64/pkcs11/libcoolkeypk11.so
/etc/pam.d/ctxfsc configure successfully.
/etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

También puede inhabilitar las tarjetas inteligentes ejecutando el script `ctxsmartlogon.sh`:

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

Los resultados se asemejan a esto:

```

#*****
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*****
Step 1:Enable smart card logon.
Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.

```

- Configurar manualmente el entorno de tarjetas inteligentes

Linux VDA utiliza el mismo entorno de tarjeta inteligente que Windows VDA. En el entorno, se deben configurar varios componentes, incluidos el controlador de dominio, la entidad de certificación (CA) de Microsoft, Internet Information Services, Citrix StoreFront y la aplicación Citrix Workspace. Para obtener más información sobre la configuración basada en la tarjeta inteligente YubiKey 4, consulte el artículo [CTX206156](#) de Knowledge Center.

Antes de ir al siguiente paso, compruebe que todos los componentes estén correctamente configurados, la clave privada y el certificado de usuario se hayan descargado en la tarjeta inteligente y usted puede iniciar sesión en Windows VDA mediante la tarjeta inteligente.

### Instalar los paquetes PC/SC Lite

PC/SC Lite es una implementación de la especificación Personal Computer/Smart Card (PC/SC) en Linux. Ofrece una interfaz de tarjeta inteligente Windows para comunicarse con tarjetas inteligentes y lectores. La redirección de tarjeta inteligente en Linux VDA se implementa en el nivel de PC/SC.

Ejecute el siguiente comando para instalar los paquetes de PC/SC Lite.

```

1 yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
2 <!--NeedCopy-->

```

### Instale el controlador de tarjeta inteligente

CoolKey es un controlador de tarjeta inteligente muy utilizado en RHEL. Si CoolKey no está instalado, ejecute el siguiente comando para instalarlo.

```

1 yum install coolkey
2 <!--NeedCopy-->

```

## Instalar los módulos PAM para la autenticación con tarjeta inteligente

Ejecute el siguiente comando para instalar los módulos `pam_krb5` y `krb5-pkinit`.

```
1 yum install pam_krb5 krb5-pkinit
2 <!--NeedCopy-->
```

El módulo `pam_krb5` es un módulo de autenticación conectable que las aplicaciones compatibles con PAM pueden utilizar para verificar contraseñas y obtener tíquets de concesión de tíquets desde el Centro de distribución de claves (KDC). El módulo `krb5-pkinit` contiene el plug-in PKINIT, que permite a los clientes obtener credenciales iniciales desde el KDC mediante una clave privada y un certificado.

## Configurar el módulo `pam_krb5`

El módulo `pam_krb5` interactúa con el centro KDC para obtener tíquets Kerberos mediante los certificados ubicados en la tarjeta inteligente. Para permitir la autenticación con `pam_krb5` en PAM, ejecute el siguiente comando:

```
1 authconfig --enablekrb5 --update
2 <!--NeedCopy-->
```

En el archivo de configuración **`/etc/krb5.conf`**, agregue información sobre PKINIT de acuerdo con el territorio real.

### Nota:

La opción **`pkinit_cert_match`** especifica reglas que el certificado de cliente debe cumplir antes de que se utilice para intentar la autenticación PKINIT. La sintaxis de dichas reglas es:

```
[relation-operator] component-rule ...
```

, donde **`relation-operator`** puede ser `&&`, lo que significa que todas las reglas de los componentes deben coincidir, o bien `||`, lo que significa que solo una regla debe coincidir.

He aquí un ejemplo de un archivo `krb5.conf` genérico:

```
1 EXAMPLE.COM = {
2
3
4     kdc = KDC. EXAMPLE.COM
5
6     auth_to_local = RULE:[1:$1@$0]
7
8     pkinit_anchors = FILE:<path where you install the root certificate
9                     >/certnew.pem
10
11     pkinit_kdc_hostname = KDC.EXAMPLE.COM
```

```

12     pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
13
14     pkinit_eku_checking = kpServerAuth
15
16 }
17
18 <!--NeedCopy-->

```

El archivo de configuración se parece a esto después de agregar la información sobre PKINIT.

```

XD.LOCAL = {
  kdc = ██████████
  auth_to_local = RULE:[1:$1@$0]
  pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
  pkinit_kdc_hostname = SZCXC-DOMAINC.XD.LOCAL
  pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
  pkinit_eku_checking = kpServerAuth
}

```

## Configurar la autenticación PAM

Los archivos de configuración PAM indican los módulos que se usan para la autenticación PAM. Para agregar pam\_krb5 como un módulo de autenticación, agregue la siguiente línea al archivo **/etc/pam.d/smartcard-auth**:

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
```

El archivo de configuración se parece al siguiente después de la modificación, si se utiliza SSSD.

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth      sufficient    pam_permit.so
auth      required      pam_deny.so

account   required      pam_unix.so
account   sufficient    pam_localuser.so
account   sufficient    pam_succeed_if.so uid < 1000 quiet
account   [default=bad success=ok user_unknown=ignore] pam_sss.so
account   [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account   required      pam_permit.so

password  required      pam_pkcs11.so

session   optional      pam_keyinit.so revoke
session   required    pam_limits.so
-session  optional      pam_systemd.so
#session  optional      pam_oddjob_mkhomedir.so umask=0077
session   optional      pam_mkhomedir.so umask=0077
session   [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session   required    pam_unix.so
session   optional    pam_sss.so
session   optional    pam_krb5.so

```

El archivo de configuración se parece al siguiente después de la modificación, si se utiliza Winbind.

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_winbind.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account     required      pam_permit.so

password    required      pam_pkcs11.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session    optional      pam_systemd.so
#session    optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_winbind.so
session     optional      pam_krb5.so

```

El archivo de configuración se parece al siguiente después de la modificación, si se utiliza Centrify.

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_nologin.so
account     required      pam_krb5.so
account     required      pam_permit.so

password    required      pam_pkcs11.so

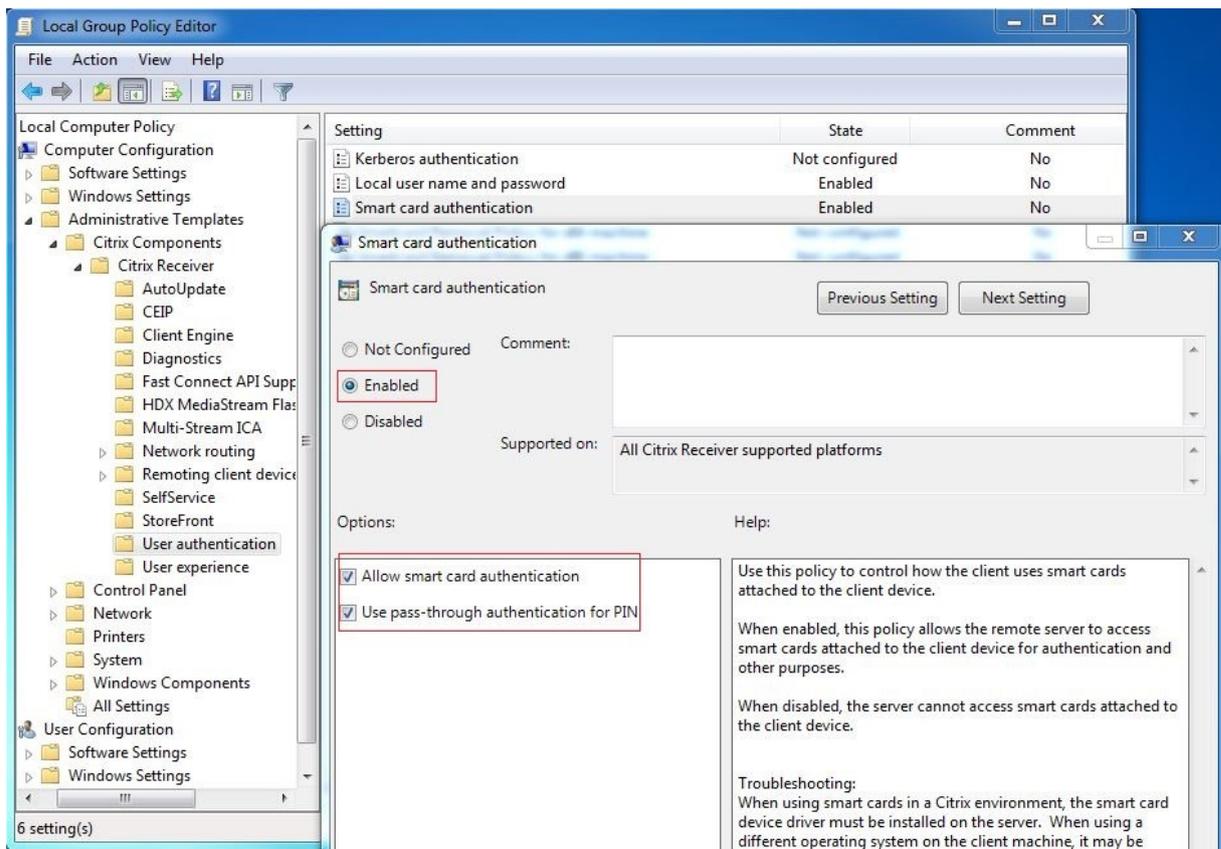
session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session    optional      pam_systemd.so
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_krb5.so

```

### (Opcional) Configurar Single Sign-On con tarjetas inteligentes

Single Sign-On es una función de Citrix que implementa la autenticación PassThrough en el inicio de escritorios virtuales y aplicaciones. Esta función reduce la cantidad de veces que los usuarios deben escribir sus números PIN. Para usar el inicio de sesión SSO (Single Sign-On) con el VDA de Linux, configure la aplicación Citrix Workspace. La configuración es la misma para el VDA de Windows. Para obtener más información, consulte el artículo [CTX133982](#) de Knowledge Center.

Habilite la autenticación con tarjeta inteligente de la siguiente manera cuando configure la directiva de grupo en Citrix Workspace.



## Inicio de sesión con tarjeta inteligente rápida

La tarjeta inteligente rápida es una mejora con respecto a la redirección HDX existente de tarjetas inteligentes basada en PC/SC. Mejora el rendimiento cuando se usan tarjetas inteligentes en entornos WAN con latencia alta. Para obtener más información, consulte [Tarjetas inteligentes](#).

Linux VDA admite las tarjetas inteligentes rápidas en las siguientes versiones de la aplicación Citrix Workspace:

- Citrix Receiver para Windows 4.12
- Aplicación Citrix Workspace para Windows 1808 y versiones posteriores

**Habilitar el inicio de sesión con tarjeta inteligente rápida en el cliente** El inicio de sesión con tarjeta inteligente rápida se habilita de forma predeterminada en el VDA y se inhabilita de forma predeterminada en el cliente. En el cliente, para habilitar el inicio de sesión con tarjeta inteligente rápida, incluya el siguiente parámetro en el archivo default.ica del sitio StoreFront asociado:

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

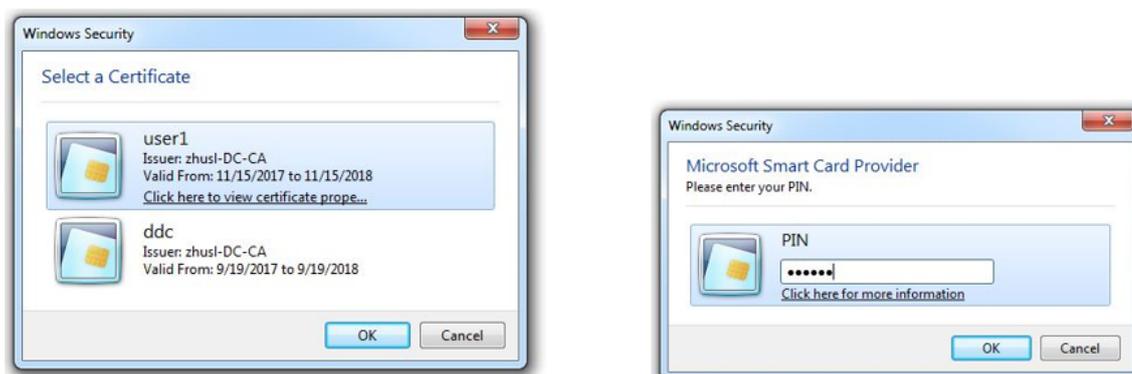
**Inhabilitar el inicio de sesión con tarjeta inteligente rápida en el cliente** Para inhabilitar el inicio de sesión con tarjeta inteligente rápida en el cliente, quite el parámetro **SmartCardCryptography-Redirection** del archivo default.ica del sitio StoreFront asociado.

## Uso

### Iniciar sesión en Linux VDA mediante una tarjeta inteligente

Puede usar una tarjeta inteligente para iniciar sesión en Linux VDA tanto con SSO como sin SSO.

- En el caso de inicio SSO, inicia sesión automáticamente en StoreFront con el PIN y el certificado de la tarjeta inteligente guardados en la caché. Al iniciar una sesión de escritorio virtual Linux en StoreFront, el PIN se pasa al Linux VDA para la autenticación con tarjeta inteligente.
- En el caso de un inicio sin SSO, se le solicita seleccionar un certificado y escribir un PIN para iniciar sesión en StoreFront.



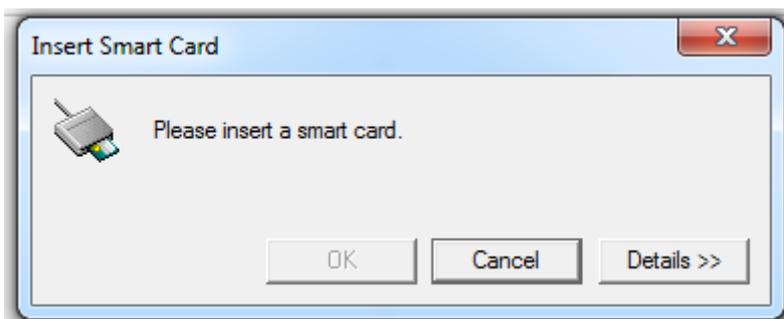
Al iniciar una sesión de escritorio virtual Linux en StoreFront, aparece este cuadro de diálogo para iniciar sesión en Linux VDA. El nombre de usuario se extrae del certificado en la tarjeta inteligente, y debe escribir el PIN nuevamente para la autenticación del inicio de sesión.

Este es el mismo comportamiento que con Windows VDA.

### Reconectarse a una sesión mediante una tarjeta inteligente

Para volver a conectarse a una sesión, la tarjeta inteligente debe estar conectada al dispositivo cliente. De lo contrario, aparece una ventana gris de almacenamiento en caché en el lado del Linux VDA y se cierra rápidamente porque la reautenticación falla si la tarjeta inteligente no está conectada. No aparece ningún otro aviso en este caso para recordarle que conecte la tarjeta inteligente.

Sin embargo, en el lado de StoreFront, si una tarjeta inteligente no está conectada cuando intenta volver a conectarse a una sesión, el sitio Web de StoreFront puede avisarle de la siguiente manera.



## Limitación

### Directiva de extracción de tarjetas inteligentes

Linux VDA solo utiliza el comportamiento predeterminado para la extracción de tarjetas inteligentes. Es decir, cuando extrae la tarjeta inteligente tras haber iniciado sesión correctamente en el Linux VDA, la sesión permanece conectada y la pantalla de sesión no se bloquea.

### Compatibilidad con otras tarjetas inteligentes y la biblioteca PKCS#11

Aunque solo figura la tarjeta inteligente CoolKey en su lista de compatibilidad, puede intentar utilizar otras tarjetas inteligentes en la biblioteca PKCS#11 porque Citrix ofrece una solución genérica de redirección de tarjetas inteligentes. Para cambiar a una tarjeta inteligente en concreto o a su biblioteca PKCS#11:

1. Reemplace todas las `libcoolkeypk11.so` instancias con su biblioteca PKCS#11 .
2. Para establecer la ruta de su biblioteca PKCS#11 al Registro, ejecute el siguiente comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
  PKCS11LibPath" -d "PATH"
2 <!--NeedCopy-->
```

dónde **PATH** apunta a su biblioteca PKCS#11, como, por ejemplo `/usr/lib64/pkcs11/libcoolkeypk11.so`

3. Inhabilite el inicio de sesión con tarjeta inteligente rápida en el cliente.

## Autenticación Single Sign-On de dos saltos

November 3, 2021

La función inserta las credenciales de usuario que se utilizaron para acceder a un almacén de StoreFront en el módulo AuthManager de la aplicación Citrix Workspace para Linux y Citrix Receiver para Linux 13.10. Después de la inserción, puede utilizar el cliente para acceder a escritorios virtuales y aplicaciones desde dentro de una sesión de Linux Virtual Desktop, sin tener que introducir las credenciales de usuario una segunda vez.

**Nota:**

Esta función es compatible con la aplicación Citrix Workspace para Linux y Citrix Receiver para Linux 13.10.

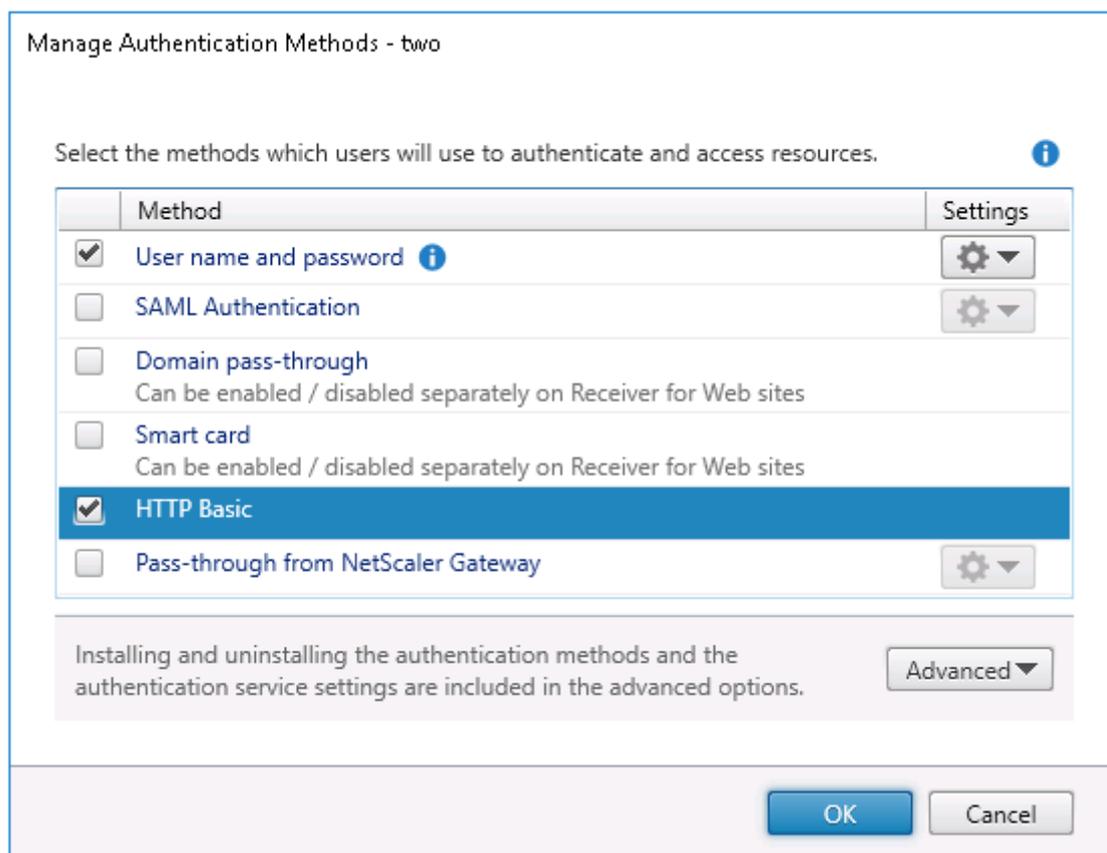
Para habilitar la funcionalidad:

1. En el Linux VDA, instale la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10.

Descargue la aplicación Citrix Workspace o Citrix Receiver desde la [página de descargas de Citrix](#).

La ruta de instalación predeterminada es `/opt/Citrix/ICAClient/`. Si instala la aplicación en una ruta diferente, configure la variable de entorno `ICAROOT` para que apunte a la ruta de instalación correcta.

2. En la consola de administración de Citrix StoreFront, agregue el método de autenticación **HTTP básica** para el almacén de destino.



3. Agregue la siguiente clave al archivo de configuración de AuthManager (\$ICAROOT/config/AuthManConfig.xml) para permitir la autenticación HTTP básica:

```

1 <Protocols>
2   <HTTPBasic>
3     <Enabled>True</Enabled>
4   </HTTPBasic>
5 </Protocols>
6 <!--NeedCopy-->

```

4. Ejecute los siguientes comandos para instalar el certificado raíz en el directorio especificado.

```

1 cp rootcert.pem $ICAROOT/keystore/cacerts/
2 $ICAROOT/util/ctx_rehash $ICAROOT/keystore/cacerts/
3 <!--NeedCopy-->

```

5. Ejecute el siguiente comando para habilitar la función:

```

1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
2 <!--NeedCopy-->

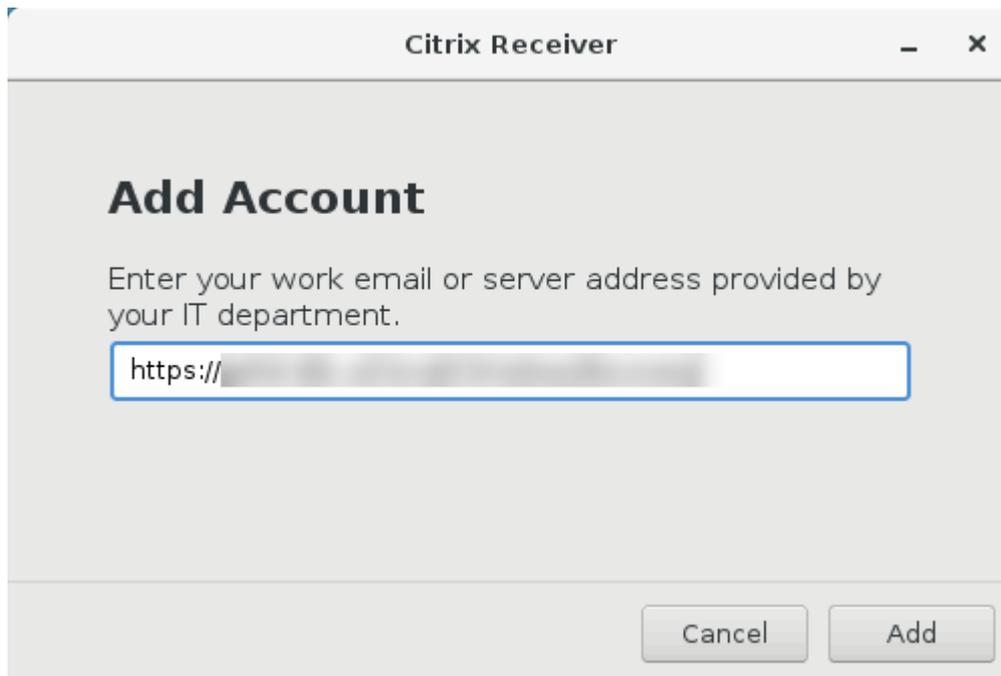
```

6. Inicie una sesión de Linux Virtual Desktop y, a continuación, inicie la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10 dentro de esa sesión.

Se le pedirá una cuenta de almacén la primera vez que inicie la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10 desde una sesión de Linux Virtual Desktop. Más tarde, la sesión se iniciará automáticamente en el almacén que especificó anteriormente.

**Nota:**

introduzca una URL HTTPS como su cuenta de almacén.



## 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 Workspace 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 Citrix Virtual Apps and Desktops](#).

## 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):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
   \Control\Citrix" -v MaxAnonymousUserNumber
2 <!--NeedCopy-->
```

Compruebe que el servicio **nscd** se está ejecutando y está configurado para habilitar la memoria caché de **passwd**:

```
1 ps uax | grep nscd
2 cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
3 <!--NeedCopy-->
```

Establezca la variable de la memoria caché de **passwd** en **no** si está habilitado y, a continuación, reinicie el servicio **nscd**. 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:

```
1 [KDE Action Restrictions]
2 action/lock_screen=false
3 <!--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, intente modificar 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 un 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:

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
2 <!--NeedCopy-->
```

- Recurrir a LDAP sin SSL/TLS

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
2 <!--NeedCopy-->
```

El almacén de claves de Java dedicado para LDAPS se encuentra en **/etc/xdl/.keystore**. Las claves de Registro afectadas incluyen:

```
1 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers
2
3 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy
4
5 HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS
6
7 HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
8 <!--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 **/etc/samba/smb.conf** y **/etc/openldap/ldap.conf** (para RHEL) o **/etc/ldap/ldap.conf** (para Ubuntu). Cambie los archivos de la siguiente manera:

- smb.conf

```
ldap ssl = start tls
ldap ssl ads = yes
client ldap sasl wrapping = plain
```
- ldap.conf

```
TLS_REQCERT never
```

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**:

```
ldap ssl = off
ldap ssl ads = no
client ldap sasl wrapping = seal
```

## 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/xdm/.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:

```
1 # xauth -f ~/.Xauthority
2
3 # > list
4
5 # > us01msip06:107 MIT-MAGIC-COOKIE-1
   fb228d1b695729242616c5908f11624b
6 <!--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:

```

1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
   -d "0x00000001" --force
4 <!--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:

```

1 export DISPLAY={
2   Display number stored in the Xauthority file }
3
4
5 export XAUTHORITY={
6   the file path of .Xauthority }
7
8 <!--NeedCopy-->

```

### Nota:

Si la variable de entorno XAUTHORITY no está definida, 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 raíz, obtenga 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:

```
1 telnet 10.158.11.11 6160
2 <!--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.

## Servicio de autenticación federada

June 14, 2023

### Introducción

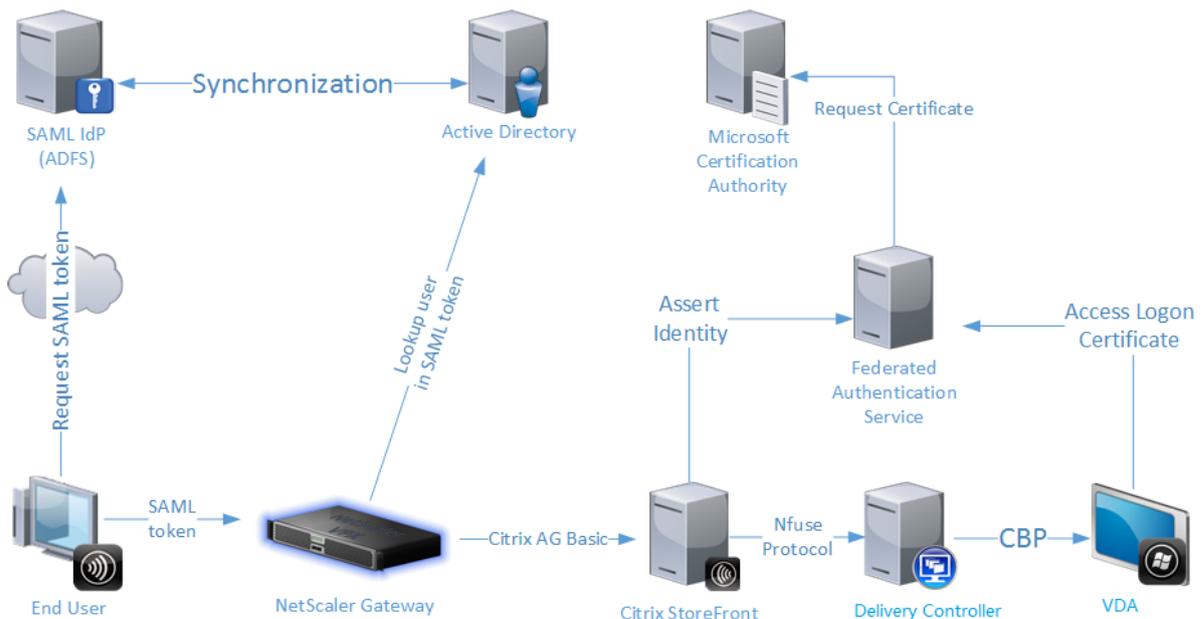
El Servicio de autenticación federada (Federated Authentication Service) de Citrix es un componente con privilegios diseñado para integrarlo con el Servicio de Certificados de Active Directory. Emite certificados para los usuarios de forma dinámica, lo que les permite iniciar sesiones en un entorno de Active Directory como si tuvieran una tarjeta inteligente. Esta función permite a StoreFront usar una gama más amplia de opciones de autenticación, tales como aserciones SAML (Security Assertion Markup Language). SAML se usa normalmente como alternativa a las cuentas de usuario tradicionales de Windows en Internet.

#### Nota:

Para utilizar la autenticación SAML, configure correctamente el Servicio de autenticación federada (FAS) en el VDA.

A partir de la actualización acumulativa CU3, Linux VDA usa conexiones cortas para la transmisión de datos con servidores de FAS.

En el siguiente diagrama se muestra el Servicio de autenticación federada (FAS) integrado con una entidad de certificación de Microsoft y al ofrecer servicios de asistencia para StoreFront y los agentes Virtual Delivery Agent (VDA).



Los servidores StoreFront de confianza contactan con el Servicio de autenticación federada (FAS) cuando los usuarios solicitan acceso a los entornos Citrix. El servicio FAS concede un tíquet que permite que una sola de sesión de Citrix Virtual Apps o Citrix Virtual Desktops se autentique con un certificado para esa sesión. Cuando un agente VDA debe autenticar a un usuario, se conecta al servicio FAS y canjea el tíquet. Solo el servicio FAS tiene acceso a la clave privada del certificado del usuario. El VDA debe enviar cada operación de firma y descifrado que necesita llevar a cabo con el certificado al servicio FAS.

## Requisitos

El servicio FAS es compatible con Windows Server 2008 R2 y versiones posteriores.

- Se recomienda la instalación del servicio FAS en un servidor que no contenga ningún otro componente de Citrix.
- El servidor Windows Server debe estar protegido para el acceso a un certificado de autorización de registro y a una clave privada que permita emitir certificados automáticamente para los usuarios del dominio y para el acceso a esos certificados de usuario y claves privadas.

En un sitio de Citrix Virtual Apps o Citrix Virtual Desktops:

- Los Delivery Controllers deben ser de la versión 7.9 como mínimo.
- El servidor StoreFront debe ser como mínimo de la versión 3.6 (versión suministrada en la imagen ISO de XenApp y XenDesktop 7.9).
- Los Linux VDA deben ser como mínimo de la versión 7.18. Compruebe que la configuración de directiva de grupo del Servicio de autenticación federada se ha aplicado correctamente a los VDA antes de crear catálogos de máquinas de la forma habitual. Para obtener más información, consulte el apartado **Configurar la directiva de grupo** en este artículo.

Referencias:

- Servicios de certificados de Active Directory  
<https://social.technet.microsoft.com/wiki/contents/articles/1137.active-directory-certificate-services-ad-cs-introduction.aspx>
- Configuración de Windows para el inicio de sesión con certificados  
<http://support.citrix.com/article/CTX206156>
- Instalación del Servicio de autenticación federada: consulte [Servicio de autenticación federada](#)

## Configurar Windows para el inicio de sesión con certificados

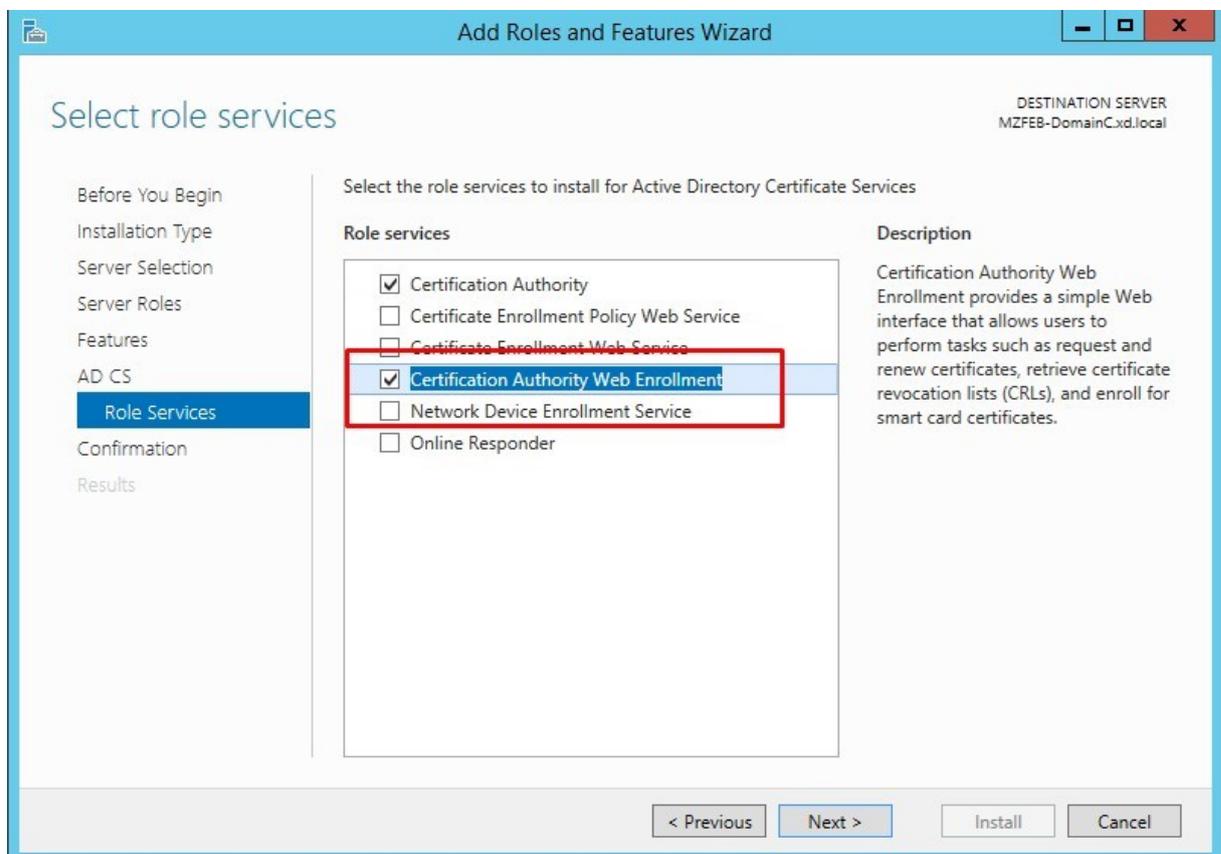
Para obtener información sobre cómo configurar Windows para el inicio de sesión con certificados, abra el artículo [CTX206156](#) de Knowledge Center para descargar y leer el archivo

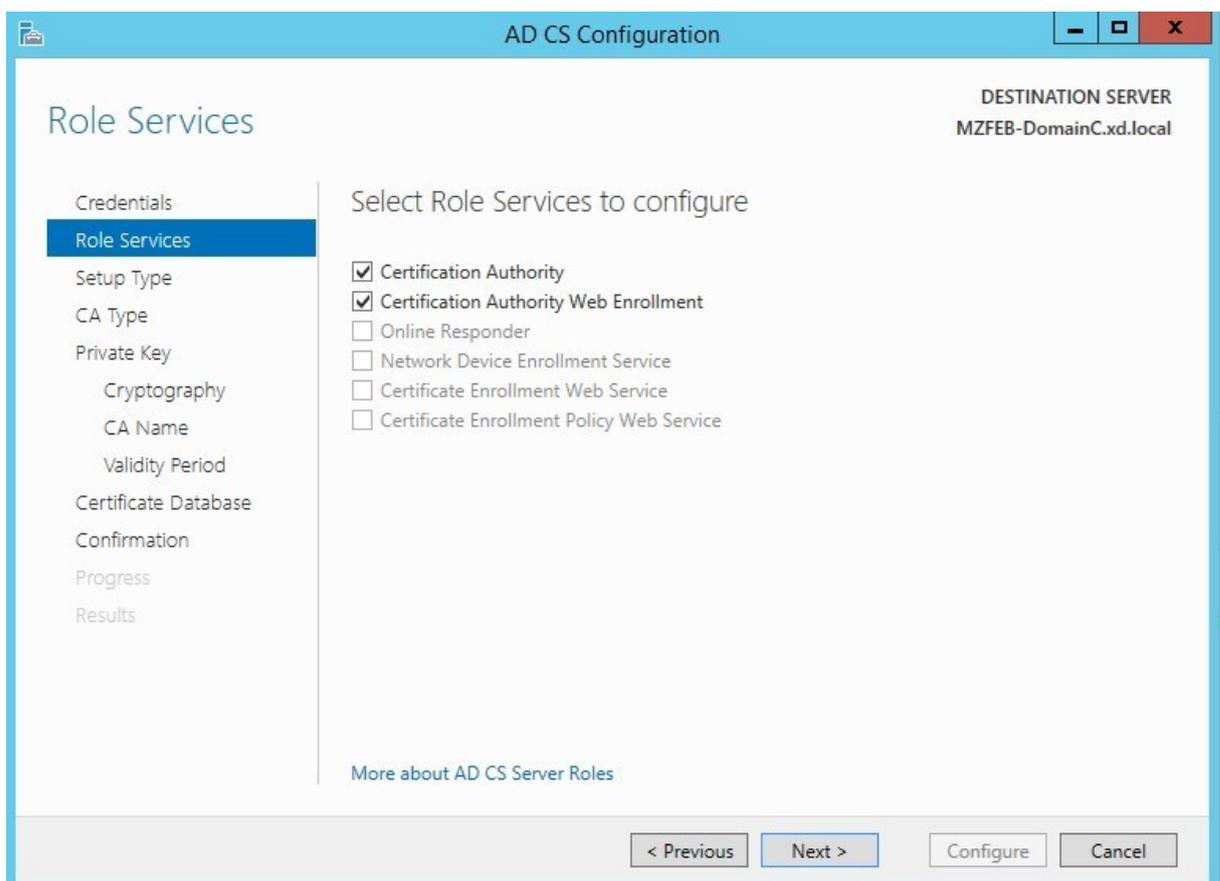
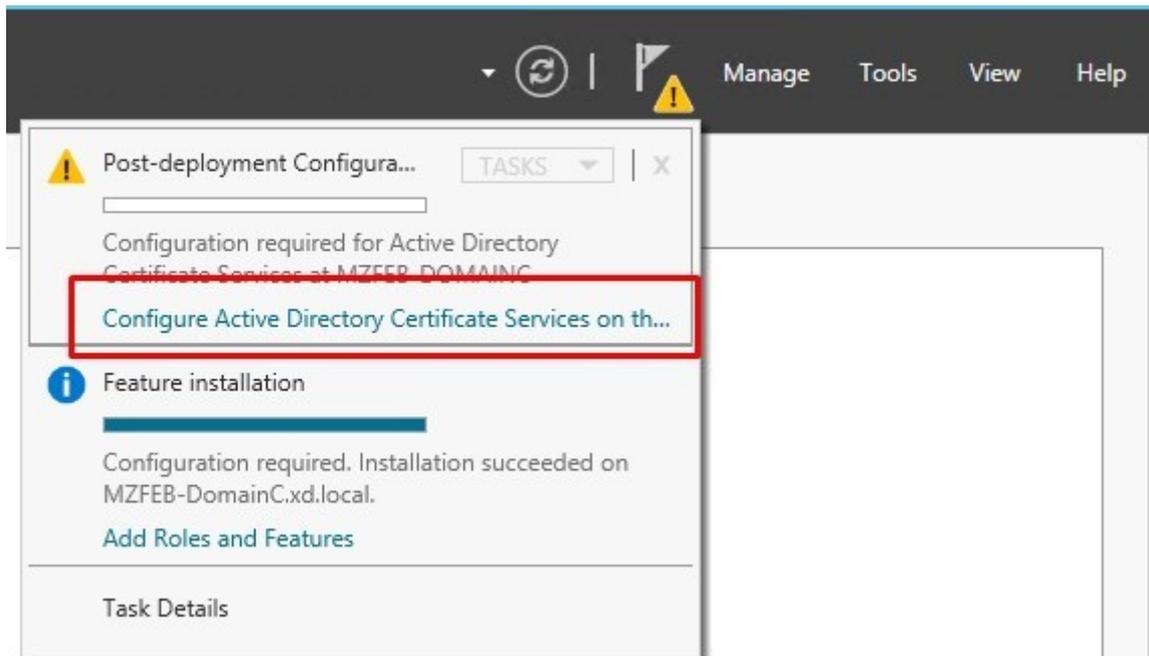
**Smart\_card\_config\_Citrix\_Env.pdf** (en adelante, “el archivo PDF”). Realice los siguientes pasos de acuerdo con el archivo PDF, al mismo tiempo que toma nota de las diferencias o complementos que se dan en cada paso. Preste especial atención a la máquina de destino en la que está operando, por ejemplo, AD, Delivery Controller o StoreFront.

### Configurar un dominio Windows (en AD)

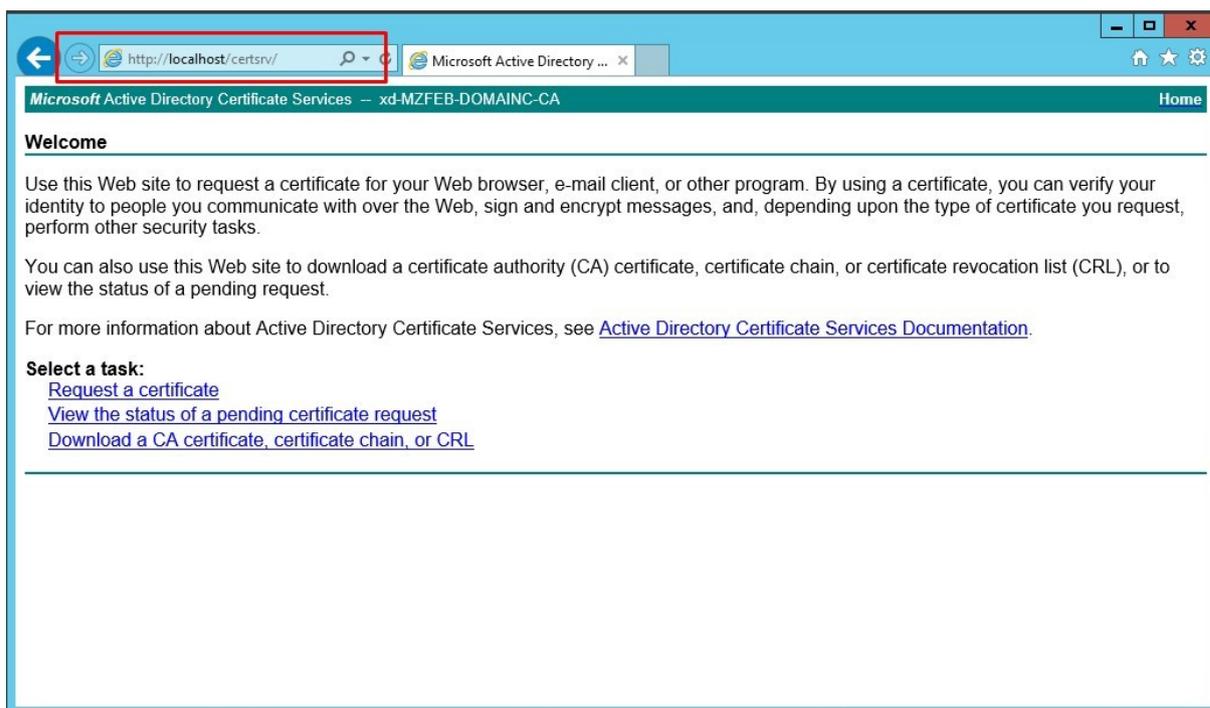
**Instalar roles de controlador de dominio** Consulte la sección **Installing Domain Controller Roles Controller Roles** en el archivo PDF.

Durante la instalación de los Servicios de certificados de Active Directory, compruebe que las siguientes opciones estén seleccionadas:





Abra <http://localhost/certsrv/> para verificar si muestra la siguiente página de bienvenida. En caso afirmativo, los Servicios de certificados de Active Directory se han instalado correctamente.



**Preparar la entidad de certificación para el uso de la tarjeta inteligente** Sin complemento. Consulte la sección **Preparing the Certificate Authority for Smart card usage** del archivo PDF.

**Emitir un certificado de controlador de dominio** Sin complemento. Consulte la sección **Issuing a Domain Controller Certificate** en el archivo PDF.

### **Configurar Microsoft IIS para HTTPS (en StoreFront)**

**Configurar HTTPS en Microsoft IIS** Sin complemento. Consulte la sección **Configuring HTTPS on Microsoft IIS** en el archivo PDF.

### **Equipos sin dominio**

Consulte la sección **Non-Domain Joined Computers** en el archivo PDF.

**Recuperar el certificado CA de la CA de Microsoft (en AD)** Sin complemento. Consulte la sección **Retrieving the CA Certificate from the Microsoft CA** en el archivo PDF.

**Instalar el certificado de CA de confianza en Windows** Sin complemento. Consulte la sección **Installing the Trusted CA Certificate on Windows** en el archivo PDF.

## Configurar Citrix StoreFront (en StoreFront)

**Crear el almacén** Consulte la sección **Creating the Store** en el archivo PDF.

Después de la configuración anterior de IIS, la URL base del almacén común se establece a la fuerza en <https://> en lugar de <http://>. Puesto que FAS no comparte el almacén con tarjetas inteligentes, se necesita un nuevo almacén para FAS. El servicio FAS de Linux VDA es compatible con cualquier método de autenticación de StoreFront. Por ejemplo, el almacén de FAS puede configurarse para usar contraseñas o SAML, pero no puede usar ambos al mismo tiempo. Cuando se selecciona SAML, la URL de StoreFront redirige automáticamente al proveedor de identidades, y se ignora el método de autenticación por contraseña.

Create Store

### StoreFront

- ✓ Getting Started
- Store Name**
- Delivery Controllers
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

#### Store name and access

Enter a name that helps users identify the store. The store name appears in Citrix Receiver as part of the user's account.

**i** Store name and access type cannot be changed, once the store is created.

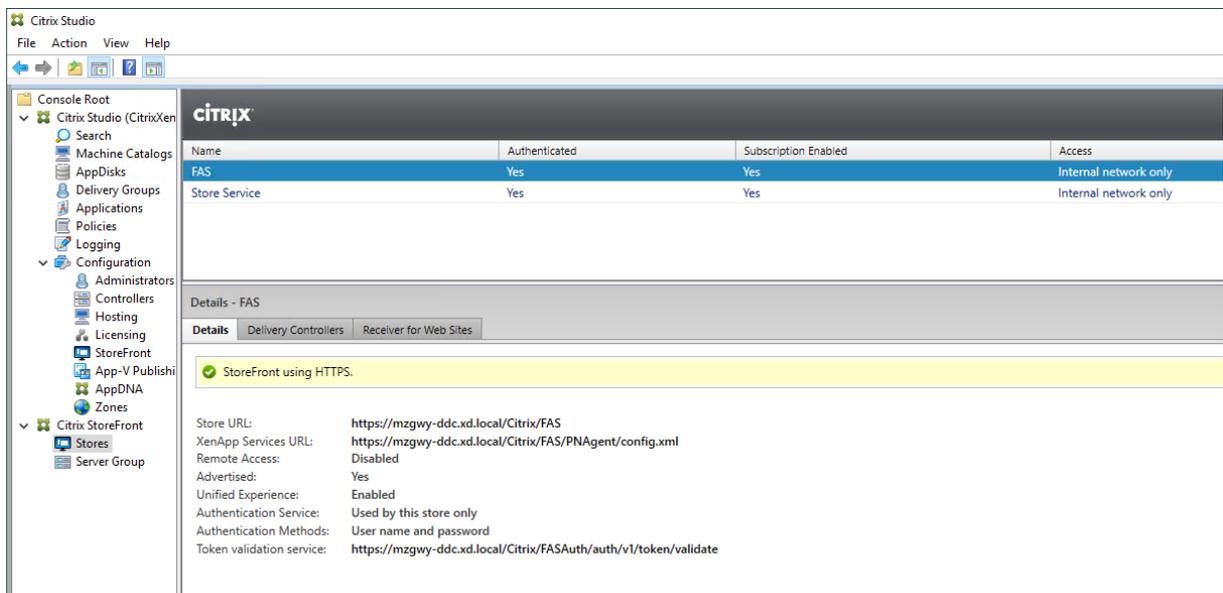
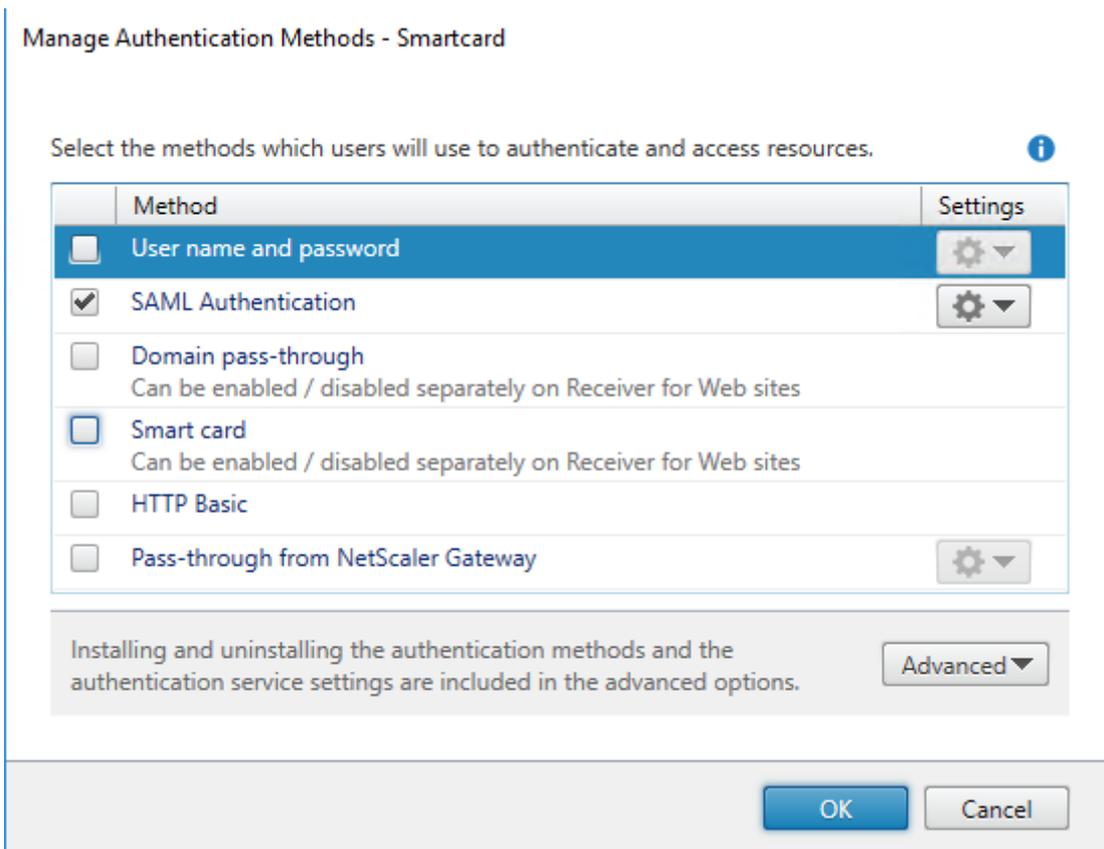
Store Name:

Allow only unauthenticated (anonymous) users to access this store  
Unauthenticated users can access the store without presenting credentials.

#### Receiver for Web Site Settings

Set this Receiver for Web site as IIS default  
When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.

Back Next Cancel



Inicie Internet Explorer y abra la URL del almacén de FAS (por ejemplo, <https://mzgwgy-ddc.xd.local/Citrix/FASWeb>).

**Nota:** La URL del almacén de FAS debe contener **Web**.

## Instalar y configurar FAS

El proceso de instalación y configuración consta de los siguientes pasos:

1. Instalar el Servicio de autenticación federada
2. Habilitar el plug-in del Servicio de autenticación federada en los servidores StoreFront
3. Configurar la directiva de grupo
4. Use la consola de administración del Servicio de autenticación federada para: (a) Implementar las plantillas suministradas, (b) Configurar entidades de certificación y (c) Autorizar al Servicio de autenticación federada a usar su entidad de certificación
5. Configurar reglas de usuario

Para obtener instrucciones sobre cada uno de los pasos, consulte [Servicio de autenticación federada](#). Tenga en cuenta las siguientes diferencias o complementos en cada uno de los pasos. Preste especial atención a la máquina de destino en la que está operando; por ejemplo, AD, Delivery Controller, StoreFront o el servidor FAS.

### Instalar el Servicio de autenticación federada (en el servidor FAS)

Por motivos de seguridad, instale el Servicio de autenticación federada (FAS) en un servidor dedicado que sea seguro y esté protegido del mismo modo que un controlador de dominio o una entidad de certificación.

### Habilitar el plug-in del Servicio de autenticación federada en un almacén de StoreFront (en StoreFront)

El siguiente comando debe usar el mismo nombre de almacén de FAS que usted escribió al configurar StoreFront. Por ejemplo, FAS es el nombre del almacén en este ejemplo:

```
$StoreVirtualPath = "/Citrix/FAS"
```

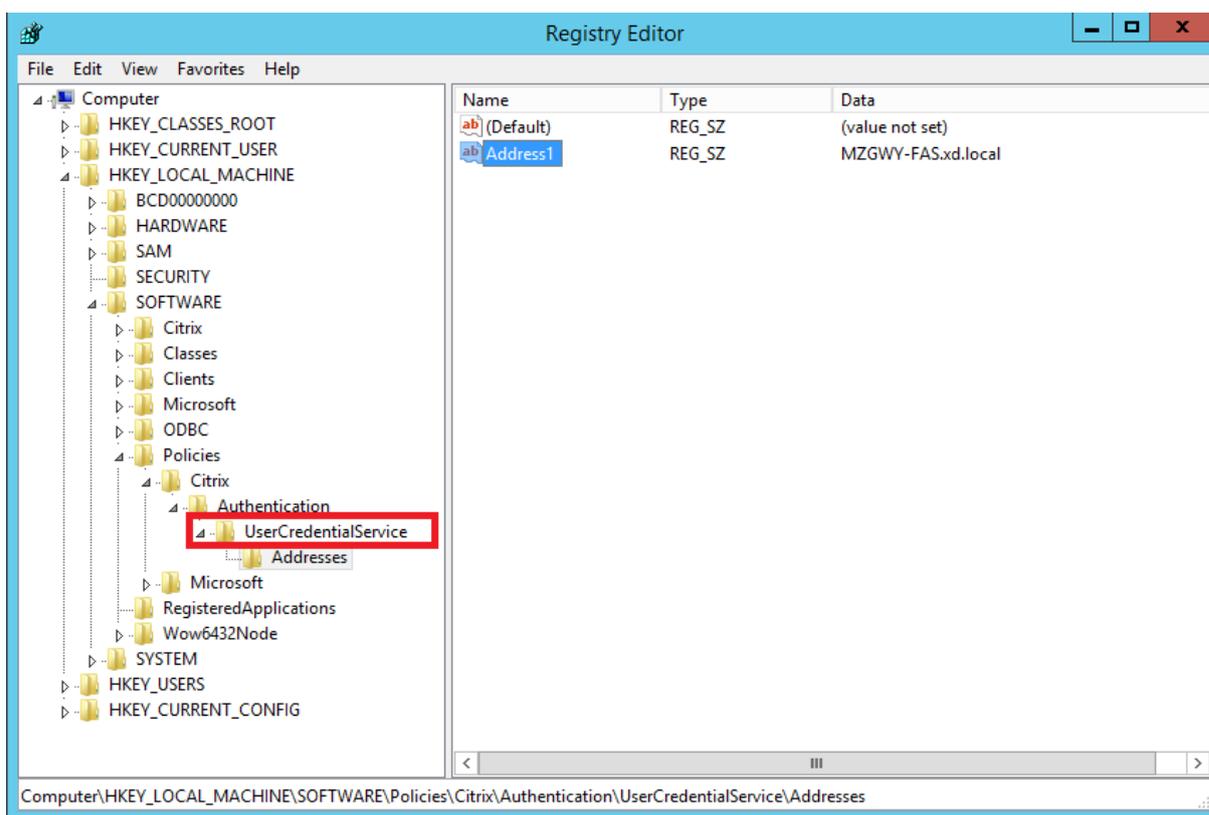
### Configurar el Delivery Controller (en el Delivery Controller)

Para usar el Servicio de autenticación federada, configure el Delivery Controller para que confíe en los servidores StoreFront que pueden conectarse a él: ejecute el cmdlet de PowerShell **Set-BrokerSite-TrustRequestsSentToTheXmlServicePort \$true**. En ocasiones, es posible que necesite ejecutar antes `Add-PSSnapin citrix.*`.

### Configurar la directiva de grupo (en el servidor FAS y en AD)

Debe ser un administrador para poder realizar los pasos del 1 al 7 de esta sección. El paso 1 debe realizarse en el servidor FAS, mientras que los pasos del 2 al 7 deben realizarse en AD.

Después de completar los pasos del 1 al 7, consulte el editor del Registro del servidor FAS para confirmar que la directiva de FAS se ha establecido.



**Habilitar la funcionalidad de certificados en la sesión** Linux VDA no admite certificados en la sesión.

### Usar la consola de administración de los Servicios de autenticación federada (en el servidor FAS)

Sin complemento. Consulte el artículo [Servicio de autenticación federada](#).

### Implementar plantillas de certificado (en el servidor FAS)

Sin complemento. Consulte el artículo [Servicio de autenticación federada](#).

### **Configurar los Servicios de certificados de Active Directory (en el servidor FAS)**

Sin complemento. Consulte el artículo [Servicio de autenticación federada](#).

### **Autorizar el Servicio de autenticación federada (en el servidor FAS)**

Sin complemento. Consulte el artículo [Servicio de autenticación federada](#).

### **Configurar reglas de usuario (en el servidor FAS)**

Sin complemento. Consulte el artículo [Servicio de autenticación federada](#).

Para obtener más información, consulte también los apartados **Agentes de inscripción delegada** y **Configuración de una lista de control de acceso** en la sección **Consideraciones sobre seguridad** del artículo [Servicio de autenticación federada](#).

### **Implementar el Servicio de autenticación federada para ADFS**

Para obtener información sobre cómo implementar el proveedor de identidades de ADFS para el Servicio de autenticación federada, consulte [Implementación ADFS del Servicio de autenticación federada](#).

## **Configurar Linux VDA**

### **Configurar servidores FAS**

Para una nueva instalación de Linux VDA, si quiere usar FAS, escriba el FQDN de cada servidor FAS cuando se le solicite CTX\_XDL\_FAS\_LIST durante la ejecución de `ctxinstall.sh` o `ctxsetup.sh`. Como Linux VDA no admite las directivas de grupo de AD, en su lugar, se puede suministrar una lista de servidores FAS, separados por punto y coma. Si alguna dirección de servidor está eliminada, complete el espacio en blanco correspondiente con la cadena de texto **<none>** y no cambie la secuencia de las direcciones de servidor.

Para actualizar una instalación Linux VDA existente, puede volver a ejecutar `ctxsetup.sh` y configurar los servidores FAS. O puede ejecutar los siguientes comandos para configurar los servidores FAS y reiniciar el servicio `ctxvda` para que los cambios surtan efecto.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\  
VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ"  
" -v "Addresses" -d "<Your-FAS-Server-List>" --force  
2  
3 service ctxvda restart
```

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

Para actualizar los servidores FAS mediante `ctxreg`, ejecute los siguientes comandos:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\  
VirtualDesktopAgent\Authentication\UserCredentialService" -v "  
Addresses" -d "<Your-FAS-Server-List>"  
2  
3 service ctxvda restart  
4 <!--NeedCopy-->
```

## Instalar un certificado raíz de CA

Para la verificación de los certificados de los usuarios, instale el certificado raíz de CA en el VDA. Obtenga el certificado raíz de AD del paso indicado **Recuperar el certificado CA de la CA de Microsoft (en AD)**. También puede descargarlo en formato DER desde el servidor raíz de CA <http://CA-SERVER/certsrv>.

### Nota:

Los siguientes comandos también se aplican a la configuración de un certificado intermedio.

Puede ejecutar un comando similar al siguiente para convertir un archivo DER (.crt, .cer, .der) a PEM.

```
1 sudo openssl x509 -inform der -in root.cer -out root.pem  
2 <!--NeedCopy-->
```

Luego, instale el certificado raíz de CA en el directorio openssl ejecutando un comando similar al siguiente:

```
1 sudo cp root.pem /etc/pki/CA/certs/  
2 <!--NeedCopy-->
```

### Nota:

No coloque el certificado raíz de CA en la ruta `/root`. Si lo hace, FAS no tendrá el permiso de leer el certificado raíz de CA.

## Configurar FAS

Ejecute el siguiente script para configurar FAS:

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

**Nota:**

El script anterior solamente gestiona los supuestos con un único certificado de CA raíz.

Si hay certificados intermedios en su entorno, agregue las rutas intermedias a `/etc/krb5.conf` de la siguiente manera:

```
[territorios]
EJEMPLO.COM = {
...
pkinit_anchors = FILE:/etc/pki/CA/certs/root.pem
pkinit_pool = FILE:/etc/pki/CA/certs/intermediate.pem
...
}
```

Se agregan dos variables de entorno para que `ctxfascfg.sh` pueda ejecutarse en modo silencioso:

- **CTX\_FAS\_ADINTEGRATIONWAY=winbind | sssd | centrify:** Indica el método de integración de Active Directory, que es `CTX_EASYINSTALL_ADINTEGRATIONWAY` cuando se especifica `CTX_EASYINSTALL_ADINTEGRATIONWAY`. Si `CTX_EASYINSTALL_ADINTEGRATIONWAY` no se especifica, `CTX_FAS_ADINTEGRATIONWAY` usa su propio parámetro de valor.
- **CTX\_FAS\_ROOT\_CA\_PATH=<root\_CA\_certificate>:** Especifica la ruta completa del certificado raíz de CA.

Elija el método apropiado de integración en Active Directory y escriba la ruta apropiada al certificado raíz de CA (por ejemplo, `/etc/pki/CA/certs/root.pem`).

El script instala los paquetes `krb5-pkinit` y `pam_krb5`, y establece los archivos de configuración relevantes.

## Limitación

- FAS admite plataformas limitadas y métodos de integración de AD. Consulte la siguiente matriz:

---

	Winbind	SSSD	Centrify
RHEL 7.7 / CentOS 7.7	√	√	√
Ubuntu 18.04	√	×	√
Ubuntu 16.04	√	×	√
SLES 12.3	√	×	√

---

- FAS aún no admite la pantalla de bloqueo. Si hace clic en el botón de bloqueo en una sesión, no podrá volver a iniciar la sesión mediante FAS.
- Esta versión admite solamente las implementaciones más frecuentes del servicio FAS, que se resumen en el artículo [Introducción arquitectural al Servicio de autenticación federada](#), y no incluye **Unión a Azure AD de Windows 10**.

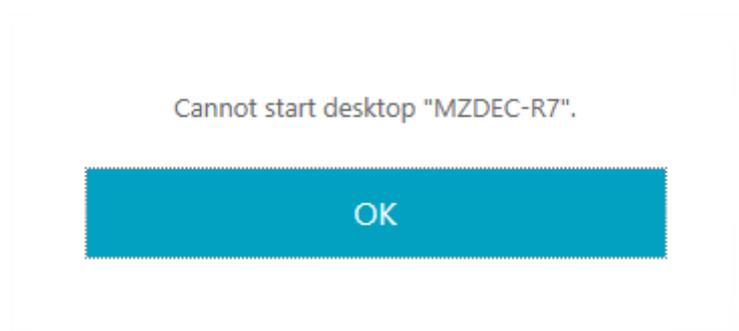
## Solución de problemas

Antes de solucionar problemas en FAS, compruebe que Linux VDA esté instalado y configurado correctamente para que pueda iniciarse una sesión que no sea FAS en el almacén común mediante la autenticación con contraseña.

Si las sesiones que no sean FAS funcionan correctamente, defina el nivel de registro de HDX de la clase **Login** en VERBOSE y el nivel de registro del VDA en TRACE. Para obtener información sobre cómo habilitar el registro de seguimiento para Linux VDA, consulte el artículo [CTX220130](#) de Knowledge Center.

## Error de configuración en el servidor FAS

No se puede iniciar ninguna sesión desde el almacén de FAS. La siguiente captura de pantalla sirve de ejemplo:



Consulte `/var/log/xdl/hdx.log` y busque el registro de errores similar al siguiente:

```
1 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: query2fas: failed
  to retrieve data: No such file or directory.
2
3 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin:
  sayhello2fas_internal: Failed to query.
4
5 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin:
  sayhello2fas_convertcredential: exit.
6
7 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: LoginFasValidate:
  Failed to start FAS.
8
```

```

9 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: receive_data:
    LoginFASValidate - parameters check error.
10
11 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: receive_data: Exit
    FAILURE
12
13 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: main: EXITING
    login process..., FAILURE
14 <!--NeedCopy-->

```

**Solución** Ejecute el siguiente comando para verificar que el valor de Registro de Citrix “HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent\Authentication\UserCredentialService” está establecido en <La-lista-de-servidores-de-FAS>.

```

1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
2 <!--NeedCopy-->

```

Si la configuración existente no es correcta, siga el anterior paso [Configurar servidores FAS](#) para definirla nuevamente.

### Configuración incorrecta del certificado raíz de CA

No se puede iniciar ninguna sesión desde el almacén de FAS. Aparece una ventana gris que desaparece varios segundos después.



Consulte `/var/log/xdl/hdx.log` y busque el registro de errores similar al siguiente:

```

1 2018-03-27 10:15:52.227 <P9099:S3> citrix-ctxlogin: validate_user:
    pam_authenticate err,can retry for user user1@CTXFAS.LAB
2
3 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: logout_user:
    closing session and pam transaction
4
5 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: validate_user: Exit
    (user=user1@CTXFAS.LAB)=INVALID_PASSWORD
6

```

```
7 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: LoginBoxValidate:
   failed validation of user 'user1@CTXFAS.LAB', INVALID_PASSWORD
8
9 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: Audit_login_failure
   : Not yet implemented
10 <!--NeedCopy-->
```

**Solución** Verifique que la ruta completa del certificado raíz de CA esté configurada correctamente en `/etc/krb5.conf`. La ruta completa será parecida a esta:

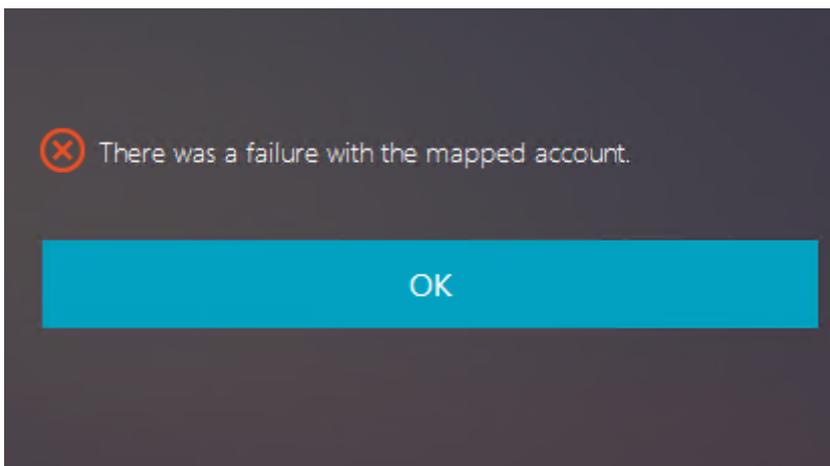
```
1  [realms]
2
3  EXAMPLE.COM = {
4
5
6      .....
7
8      pkinit_anchors = FILE:/etc/pki/CA/certs/root.pem
9
10     .....
11
12 }
13
14 <!--NeedCopy-->
```

Si la configuración existente no es correcta, siga el anterior paso [Instalar un certificado raíz de CA](#) para definirla nuevamente.

Como alternativa, compruebe si el certificado raíz de CA es válido.

### **Error en la asignación de cuentas sombra**

FAS está configurado con la autenticación SAML. Puede ocurrir el siguiente error después de que un usuario de ADFS introduzca el nombre de usuario y la contraseña en la página de inicio de sesión de ADFS.

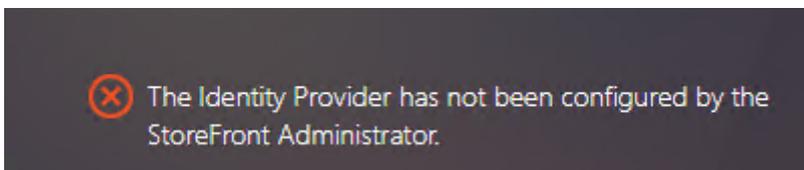


Este error indica que el usuario de ADFS se ha verificado correctamente, pero no hay ningún usuario sombra configurado en AD.

**Solución** Establezca la cuenta sombra en AD.

### **ADFS no configurado**

Durante el inicio de sesión en el almacén de FAS, ocurre el siguiente error:



El motivo es que el almacén de FAS está configurado para usar la autenticación de SAML, pero falta la implementación de ADFS.

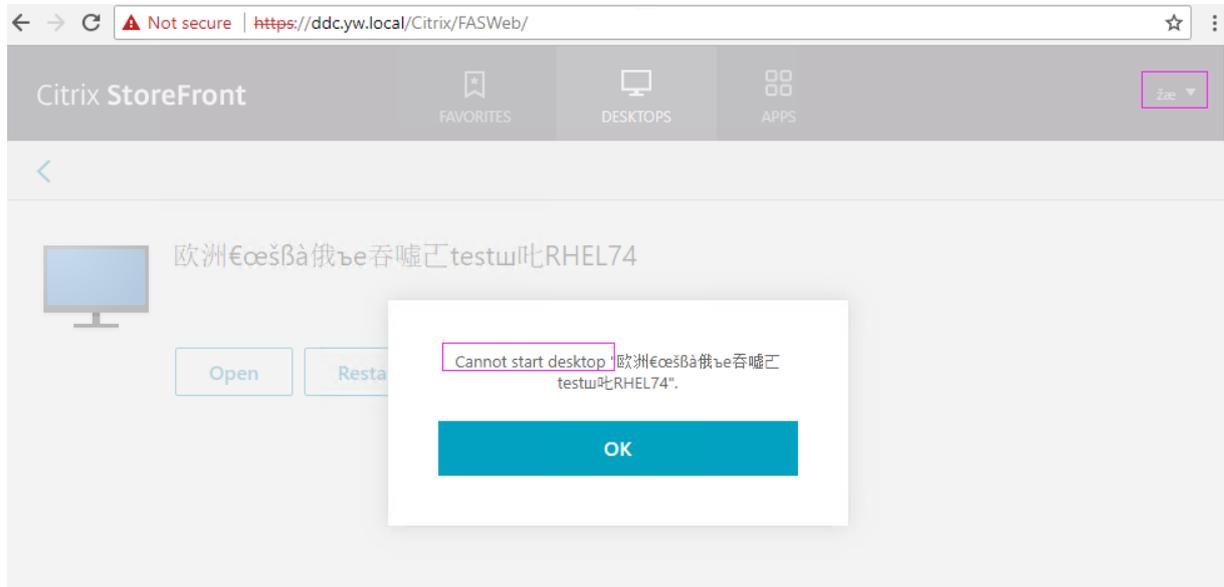
**Solución** Implemente el proveedor de identidades de ADFS para el Servicio de autenticación federada. Para obtener más información, consulte el artículo [Implementación ADFS del Servicio de autenticación federada](#).

### **Información relacionada**

- Las implementaciones más comunes del servicio FAS se resumen en el artículo [Información general arquitectural del Servicio de autenticación federada](#).
- Los artículos de procedimientos se presentan en el capítulo [Configuración avanzada del Servicio de autenticación federada](#).

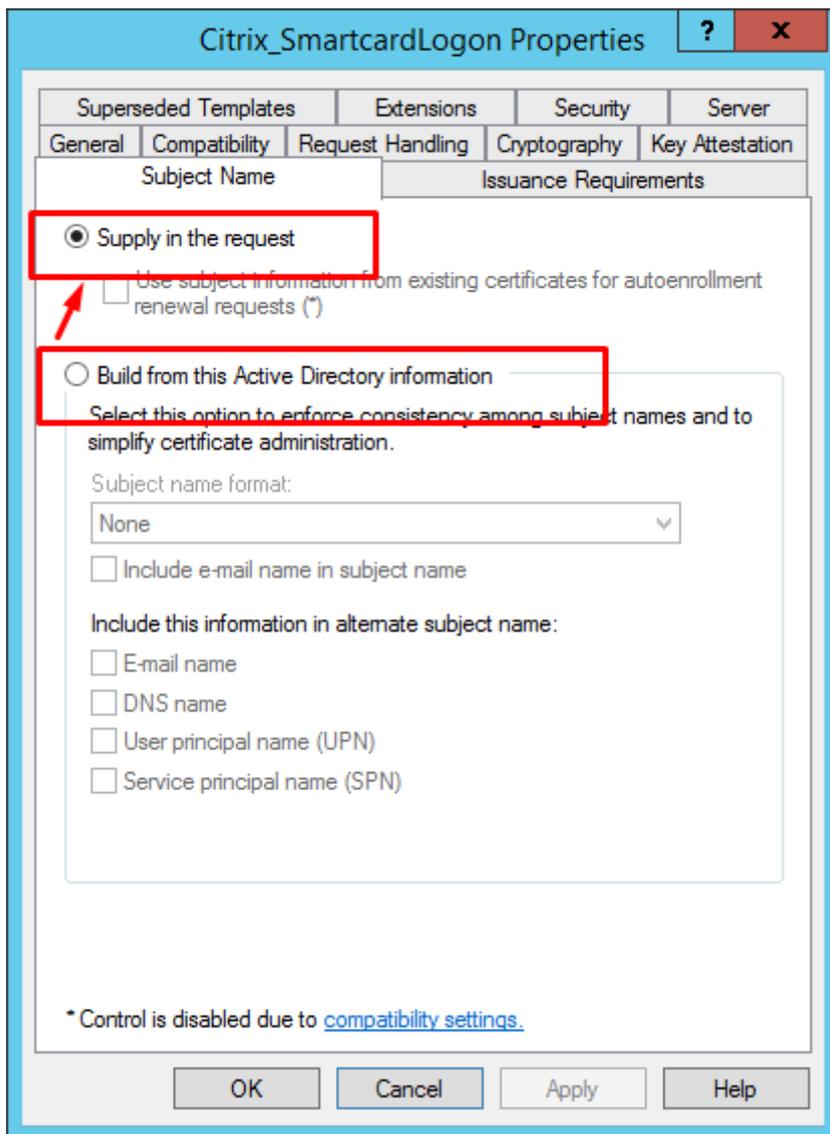
## Problema conocido

Cuando se usa FAS, puede que fallen los inicios de una sesión de aplicación o escritorio publicados si se usan caracteres que no sean en inglés.



## Solución temporal

En la herramienta de CA, haga clic con el botón secundario en **Manage Templates** para cambiar la plantilla **Citrix\_SmartcardLogon** de **Build from this Active Directory information** a **Supply in the request**:





© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).