Linux Virtual Delivery Agent 2204

Contents

Linux Virtual Delivery Agent 2204 5

Novedades 5

Problemas resueltos 6

Problemas conocidos 7

Avisos legales de terceros 9

Elementos retirados 9

Requisitos del sistema 11

Información general de la instalación 15

Instalación rápida con Easy Install (recomendado) 15

Instalar Linux Virtual Delivery Agent para Amazon Linux 2, CentOS y RHEL manualmente 36

Instalar Linux Virtual Delivery Agent para SUSE manualmente 73

Instalar Linux Virtual Delivery Agent para Ubuntu manualmente 102

Instalar Linux Virtual Delivery Agent para Debian manualmente 134

Crear Linux VDA en Citrix DaaS Standard para Azure 164

Utilice Machine Creation Services (MCS) para crear máquinas virtuales Linux 168

Usar Citrix Provisioning para crear máquinas virtuales Linux 195

Configurar Delivery Controllers para XenDesktop 7.6 y versiones anteriores 196

Parámetros de servidor LDAP y de directivas 197

Configuración 198

Administración 199

Customer Experience Improvement Program (CEIP) de Citrix 199

HDX Insight 204

Integración en Citrix Telemetry Service 205

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualización automática de Linux VDA para Citrix DaaS Standard para Azure **209**

Métricas de sesión de Linux y Linux VM **213**

Recopilación de registros **222**

Remedo de sesiones **226**

El demonio del servicio de supervisión **232**

Herramientas y utilidades **235**

Otros **240**

Compatibilidad con la aplicación Citrix Workspace para HTML5 **240**

Crear un entorno virtual Python3 **241**

Integrar NIS en Active Directory **243**

IPv6 **249**

LDAPS **251**

Xauthority **255**

Autenticación **258**

Autenticación de inicio de sesión Single Sign-On de dos saltos **259**

Servicio de autenticación federada **261**

Autenticación sin SSO **270**

Tarjetas inteligentes **271**

Sesiones sin autenticar de usuarios anónimos **282**

Archivo **284**

Copiar y pegar archivos **284**

Transferencia de archivos **285**

Gráficos **290**

Configuración y ajuste de gráficos **291**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pantalla compartida de HDX **302**

Tarjetas gráficas que no son de GPU virtuales **311**

Marca de agua en sesiones basada en texto **313**

Presentación progresiva de Thinwire **314**

Teclado **316**

Editor de métodos de entrada (IME) de cliente **317**

Sincronización de la interfaz de usuario IME del cliente **318**

Sincronización de la distribución de teclado dinámico **322**

Teclado en pantalla **326**

Compatibilidad para entrada de texto en varios idiomas **329**

Contenido multimedia **331**

Funciones de audio **331**

Redirección de contenido de explorador web **332**

Compresión de vídeo de cámara web HDX **338**

VDA no unidos a ningún dominio **344**

Lista de directivas disponibles **346**

Impresión **371**

Prácticas recomendadas de impresión **371**

Impresión de PDF **378**

Acceso con Remote PC **379**

La función de persistencia **392**

Transporte adaptable **393**

Iniciar sesión con un directorio de inicio temporal **396**

Publicar aplicaciones **398**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Rendezvous V1 **399**

Rendezvous V2 **402**

Sesiones de usuario seguras mediante DTLS **406**

Sesiones de usuario seguras mediante TLS **406**

Fiabilidad de la sesión **410**

Redirección de USB **413**

Virtual Channel SDK (experimental) **421**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux Virtual Delivery Agent 2204

August 9, 2022

> **Importante:**
>
> La estrategia de ciclos de vida para las versiones Current Release (CR) y las versiones Long Term Service (LTSR) del producto se describe en Hitos del ciclo de vida.

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

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

Novedades

July 6, 2022

Novedades en la versión 2204

La versión 2204 de Linux VDA ofrece estas mejoras y funciones nuevas:

Codificación por hardware extendida a códec selectivo

Anteriormente disponible solo para toda la pantalla, la codificación por hardware H.264 ahora admite el uso selectivo para áreas en cambio constante. Esta funcionalidad reduce la carga de CPU en la compresión de vídeo con ayuda de hardware y mejora la calidad de la imagen y el número de fotogramas por segundo (FPS). Para obtener información sobre cómo habilitar esta función, consulte Configuración y ajuste preciso de gráficos.

Compatibilidad con inicio de sesión con un directorio de inicio temporal

A partir de esta versión, puede especificar un directorio de inicio temporal para los casos en los que el punto de montaje de Linux VDA falle. Al especificarse un directorio de inicio temporal, se muestra un mensaje durante el inicio de sesión cuando el punto de montaje falla. Los datos del usuario se

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

almacenan en el directorio de inicio temporal. Para obtener más información, consulte Iniciar sesión con un directorio de inicio temporal.

Compatibilidad con proxies SOCKS5 para el tráfico HDX con Rendezvous

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

Compatibilidad con proxy transparente para Rendezvous

Ahora se admite un proxy HTTP transparente con Rendezvous. Si utiliza un proxy transparente en la red, no se requiere configuración adicional en el VDA.

Compatibilidad con el escritorio GNOME Classic

Esta versión incorpora GNOME Classic como opción de escritorio que puede especificarse con `CTX_XDL_DESKTOP _ENVIRONMENT` en ctxsetup.sh. Para obtener más información, consulte el artículo sobre la instalación del VDA Linux GNOME Classic basado en su distribución.

Agrupación de botones en la barra de tareas de aplicaciones

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

Novedades en versiones anteriores

Para conocer las nuevas funciones incluidas en las versiones publicadas después de 1912 LTSR y hasta 2203 LTSR, consulte Historial de novedades.

Problemas resueltos

July 6, 2022

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 2203 LTSR:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Al cerrar sesión e iniciarla de nuevo en una sesión de Linux VDA con Ubuntu, es posible que las extensiones de escritorio de GNOME no se conserven. [CVADHELP-19038].
- Al intentar abrir un menú contextual o un cuadro de diálogo, la operación puede fallar cuando se utiliza una instancia publicada de la aplicación Mozilla Firefox en modo integrado. El problema se produce cuando se usa la aplicación Citrix Workspace para Windows con el valor de TWISeamlessFlag establecido en 8 (valor predeterminado). El menú aparece y, a continuación, desaparece rápidamente. Para habilitar la corrección, ejecute el siguiente comando en Linux VDA:

  ```
  sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
     CurrentControlSet\Control\Citrix\TWI" -t   "REG_DWORD" -v "
     SeamlessFlags" -d "0x00000008" --force
  <!--NeedCopy-->
  ```

  [CVADHELP-18648]
- Linux VDA puede dejar de responder o entrar en un interbloqueo. El problema se debe al aumento del uso del ancho de banda o a una mala conexión de red. [CVADHELP-19037]
- Al intentar cerrar una sesión de escritorio desde Desktop Viewer, puede mostrarse una pantalla gris indefinidamente. El problema ocurre cuando el servicio AutoFS está habilitado para las carpetas de almacenamiento NFS. [CVADHELP-19384]
- Al intentar iniciar una sesión de Linux VDA, es posible que la sesión se cierre de manera imprevista y se muestre una pantalla gris. [CVADHELP-19556]

Problemas conocidos

July 14, 2023

Se han identificado los problemas siguientes en esta versión:

- Linux VDA no admite el cifrado SecureICA. Al habilitar SecureICA en Linux VDA, se produce un error en el inicio de la sesión.
- En una sesión de escritorio de GNOME, los intentos de cambiar la distribución del teclado pueden fallar. [CVADHELP-15639]
- 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]
- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[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]
- 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]
- 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

Avisos legales de terceros

December 12, 2022

Linux Virtual Delivery Agent versión 2204 (descarga en PDF)

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

Elementos retirados

July 8, 2022

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 soporte técnico de la vida útil del producto, consulte el artículo Política de soporte técnico del ciclo de vida del producto.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
Compatibilidad con RHEL 8.1, RHEL 8.3	2203	2206
Compatibilidad con RHEL 7.8, CentOS 7.8	2203	2204
Compatibilidad con CentOS 8.x	2110	2201
Compatibilidad con SUSE 12.5	2109	2204
Compatibilidad con Ubuntu 16.04	2109	2203
Compatibilidad con RHEL 7.7, CentOS 7.7	2006	2009
Compatibilidad con SUSE 12.3	2006	2006
Compatibilidad con RHEL 6.10, CentOS 6.10	2003	2003
Compatibilidad con RHEL 6.9, CentOS 6.9	1909	1909
Compatibilidad con RHEL 7.5, CentOS 7.5	1903	1903
Compatibilidad con RHEL 7.4, CentOS 7.4	1811	1811
Compatibilidad con RHEL 6.8, CentOS 6.8	1811	1811
Se admite en RHEL 7.3, CentOS 7.3	7.18	7.18
Compatibilidad con RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos del sistema

October 31, 2022

La versión Current Release de Linux VDA va a la par con Citrix Virtual Apps and Desktops. También es retrocompatible con versiones anteriores de Citrix Virtual Apps and Desktops que aún no han alcanzado el final de su vida útil. Para obtener más información acerca de la vida útil de los productos Citrix y para determinar cuándo deja Citrix de ofrecer 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. Cualquier comunidad de Delivery Controllers puede hacer de intermediaria tanto para escritorios Windows como para escritorios Linux.

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

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.

Distribuciones de Linux

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.

- Amazon Linux
  - Amazon Linux 2
- CentOS Linux
  - CentOS 7.9
- Debian Linux
  - Debian 10.9
- Red Hat Enterprise Linux
  - Workstation 8.4
  - Workstation 8.3

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Workstation 8.2
  - Workstation 8.1
  - Workstation 7.9
  - Server 8.4
  - Server 8.3
  - Server 8.2
  - Server 8.1
  - Server 7.9
- SUSE Linux Enterprise:
  - Server 15 Service Pack 3
  - Server 15 Service Pack 2
- Ubuntu Linux
  - Ubuntu Desktop 20.04
  - Ubuntu Server 20.04
  - Ubuntu Desktop 18.04
  - Ubuntu Server 18.04
  - Ubuntu Live Server 18.04

> **Nota:**
>
> El proyecto CentOS se centra ahora en CentOS Stream. CentOS Linux 8, como recompilación de RHEL 8, termina a finales de 2021. A partir de esa fecha, continúa CentOS Stream, sirviendo como rama ascendente (de desarrollo) de Red Hat Enterprise Linux (RHEL). Para obtener más información, consulte https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux.

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	Escritorio compatible
Amazon Linux 2	1.20	MATE, GNOME, GNOME Classic
Debian 10.9	1.20	MATE, GNOME, GNOME Classic
RHEL 8.4, RHEL 8.3, RHEL 8.2, RHEL 8.1	= 1.20.8	MATE, GNOME, GNOME Classic, KDE
RHEL 7.9, CentOS 7.9	1.20	MATE, GNOME, GNOME Classic, KDE

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Distribución de Linux	Versión de Xorg	Escritorio compatible
SUSE 15.3, SUSE 15.2	1.20	MATE, GNOME, GNOME Classic
Ubuntu 20.04	1.20	MATE, GNOME, GNOME Classic
Ubuntu 18.04	1.19	MATE, GNOME, GNOME Classic

> **Sugerencia:**
>
> No utilice `HWE kernel` ni `HWE Xorg` en Ubuntu.
>
> Debe instalarse al menos un escritorio. Con los scripts ctxinstall.sh o ctxsetup.sh, puede especificar el entorno de escritorio GNOME o MATE que se utilizará en las sesiones.
> El formato del nombre de usuario debe cumplir con las reglas de sintaxis de `systemd` del administrador de pantallas actual. Para obtener más información sobre la sintaxis de los nombres de usuario de `systemd`, consulte User/Group Name Syntax.

Plataformas de host y entornos de virtualización compatibles

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

> **Nota:**
>
> En todos los casos, la arquitectura de procesador admitida es x86-64.
>
> Desde Citrix Virtual Apps and Desktops 7 2003 hasta Citrix Virtual Apps and Desktops 7 2112, el alojamiento de Linux VDA en Microsoft Azure, AWS y GCP solo era posible con Citrix DaaS (antes, Virtual Apps and Desktops Service). A partir de la versión 2203, puede alojar Linux VDA en estas nubes públicas tanto con Citrix DaaS como con Citrix Virtual Apps and Desktops. Para agregar las conexiones de host de estas nubes públicas a su implementación de Citrix Virtual Apps and Desktops, necesita una licencia de derechos híbridos. Para obtener información sobre la licencia de derechos híbridos, consulte Transición e intercambios (TTU) con derechos híbridos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paquetes de integración de Active Directory

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

	Winbind	SSSD	Centrify	PBIS	Quest
Amazon Linux 2	Sí	Sí	Sí	Sí	No
Debian 10.9	Sí	Sí	Sí	Sí	No
RHEL 8.4	Sí	Sí	Sí	Sí	No
RHEL 8.3	Sí	Sí	Sí	Sí	No
RHEL 8.2	Sí	Sí	Sí	Sí	No
RHEL 8.1	Sí	Sí	Sí	Sí	No
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y versiones posteriores)
SUSE 15.3	Sí	Sí	Sí	Sí	No
SUSE 15.2	Sí	Sí	Sí	Sí	No
Ubuntu 20.04	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y versiones posteriores)
Ubuntu 18.04	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y versiones posteriores)

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 estos hipervisores:

- Citrix Hypervisor
- Hipervisor VMware vSphere
- Nutanix AHV

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

> **Nota:**
>
> Los hipervisores son compatibles con algunas distribuciones de Linux.
> Para usar HDX 3D Pro para Amazon Linux 2, se recomienda instalar el controlador NVIDIA 470.

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. Por ahora, Linux VDA admite hasta vGPU 13. Para obtener más información, consulte NVIDIA Virtual GPU Software Supported GPUs.

Información general de la instalación

July 6, 2022

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
- Crear Linux VDA unidos y no unidos a un dominio en Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure)
- Usar Citrix Provisioning para crear máquinas virtuales Linux
- Configurar Delivery Controllers para XenDesktop 7.6 y versiones anteriores

Instalación rápida con Easy Install (recomendado)

August 11, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.
> - Para crear VDA no unidos a ningún dominio, debe usar Machine Creation Services (MCS). Para obtener más información, consulte Utilice Machine Creation Services (MCS) para crear máquinas virtuales Linux.
> - Para obtener información sobre las funciones disponibles para los VDA que no están unidos a ningún dominio, vaya a VDA que no están unidos a ningún dominio.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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:

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

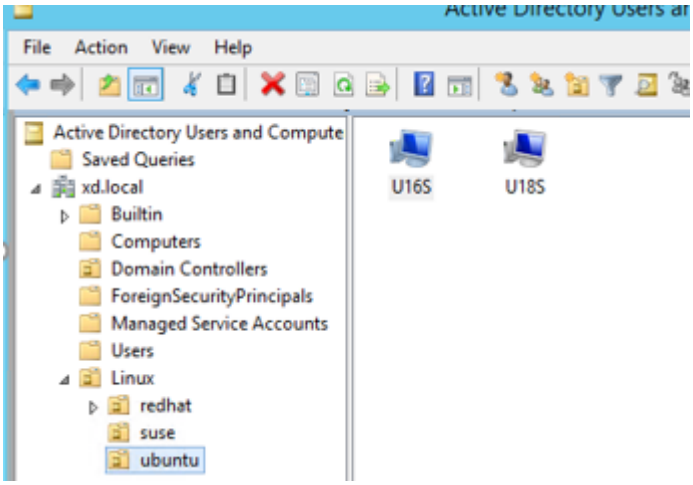
  Este problema es exclusivo de Centrify y su configuración. Para resolver este problema, haga lo siguiente:

  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**.

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

  1. Asegúrese de que la unidad organizativa específica existe en el controlador de dominio.

     La siguiente captura de pantalla le sirve de ejemplo de unidad organizativa.

  2. Cree el archivo /tmp/ctxinstall.conf en el VDA.
  3. Agregue la línea ou=\<su unidad organizativa\> al archivo /tmp/ctxinstall.conf.

     Los valores de unidad organizativa varían con los diferentes métodos de AD. Consulte la siguiente tabla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SO	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	`ou="Linux/amazon"`	`ou="Linux/amazon"`	`ou="XD.LOCAL/Linux/amazon"`	`ou="Linux/amazon"`
Debian	`ou="Linux/debian"`	`ou="Linux/debian"`	`ou="XD.LOCAL/Linux/debian"`	`ou="Linux/debian"`
RHEL 8	`ou="OU=redhat,OU=Linux"`	`ou="OU=redhat,OU=Linux"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
RHEL 7	`ou="Linux/redhat"`	`ou="Linux/redhat"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
SUSE	`ou="Linux/suse"`	`ou="Linux/suse"`	`ou="XD.LOCAL/Linux/suse"`	`ou="Linux/suse"`
Ubuntu	`ou="Linux/ubuntu"`	`ou="Linux/ubuntu"`	`ou="XD.LOCAL/Linux/ubuntu"`	`ou="Linux/ubuntu"`

- 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.
  - Centrify 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 Centrify como el método para unirse a un dominio, el script ctxinstall.sh requiere el paquete de Centrify. ctxinstall.sh puede obtener el paquete de Centrify de dos formas:
  - Easy Install ayuda a descargar el paquete de Centrify desde Internet automáticamente. Las direcciones URL especificadas para cada distribución son:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

  Por ejemplo:

```
cat /tmp/ctxinstall.conf
set  " centrifypkgpath=/home/mydir "
ls  -ls  /home/mydir
    9548 -r-xr-xr-x. 1 root root  9776688 May 13  2016
       adcheck-rhel4-x86_64
    4140 -r--r--r--. 1 root root  4236714 Apr 21  2016
   centrifyda-3.3.1-rhel4-x86_64.rpm
    33492 -r--r--r--. 1 root root 34292673 May 13  2016
   centrifydc-5.3.1-rhel4-x86_64.rpm
    4 -rw-rw-r--. 1 root root     1168 Dec  1  2015
   centrifydc-install.cfg
    756 -r--r--r--. 1 root root   770991 May 13  2016
   centrifydc-ldapproxy-5.3.1-rhel4-x86_64.rpm
    268 -r--r--r--. 1 root root   271296 May 13  2016
   centrifydc-nis-5.3.1-rhel4-x86_64.rpm
    1888 -r--r--r--. 1 root root  1930084 Apr 12  2016
   centrifydc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
    124 -rw-rw-r--. 1 root root   124543 Apr 19  2016
   centrify-suite.cfg
    0 lrwxrwxrwx. 1 root root       10 Jul  9  2012 install-
   express.sh -> install.sh
    332 -r-xr-xr--. 1 root root   338292 Apr 10  2016 install
   .sh
    12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-
   notes-agent-rhel4-x86_64.txt
    4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-
   notes-da-rhel4-x86_64.txt
    4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-
   notes-nis-rhel4-x86_64.txt
    12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-
   notes-openssh-rhel4-x86_64.txt
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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:

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

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

    Debian, Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh`
  - Obtenga una versión específica del paquete PBIS 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:

```
pbisDownloadPath_RHEL="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
pbisDownloadPath_Ubuntu="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
```

Paso 2: Prepare el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Haga estos cambios en función de la plataforma de hipervisor que se use. No se requieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix Hypervisor

Cuando está habilitada la función de sincronización horaria de Citrix Hypervisor en cada VM de Linux paravirtualizada, hay problemas con NTP y Citrix Hypervisor. Ambos intentan gestionar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, compruebe que el reloj del sistema de cada invitado de Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

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 habilitada desde la máquina virtual de Linux:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -

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

Este comando devuelve 0 o 1:

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

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

Si está habilitada, inhabilite la función de sincronización horaria escribiendo 1 en el archivo:

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

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

```
su -

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

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

Desde el sistema operativo de administración:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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

Cuando la función de sincronización horaria de VMware está habilitada en cada VM de Linux paravirtualizada, hay problemas con el protocolo NTP y el hipervisor. Ambos 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: Instale .NET Runtime 6.0 como requisito previo

Antes de instalar Linux VDA, instale .NET Runtime 6.0 conforme a las instrucciones de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de .NET Runtime. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para distribuciones RHEL y CentOS:

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

Para distribuciones Ubuntu/Debian:

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

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

Para las distribuciones SUSE:

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

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

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.

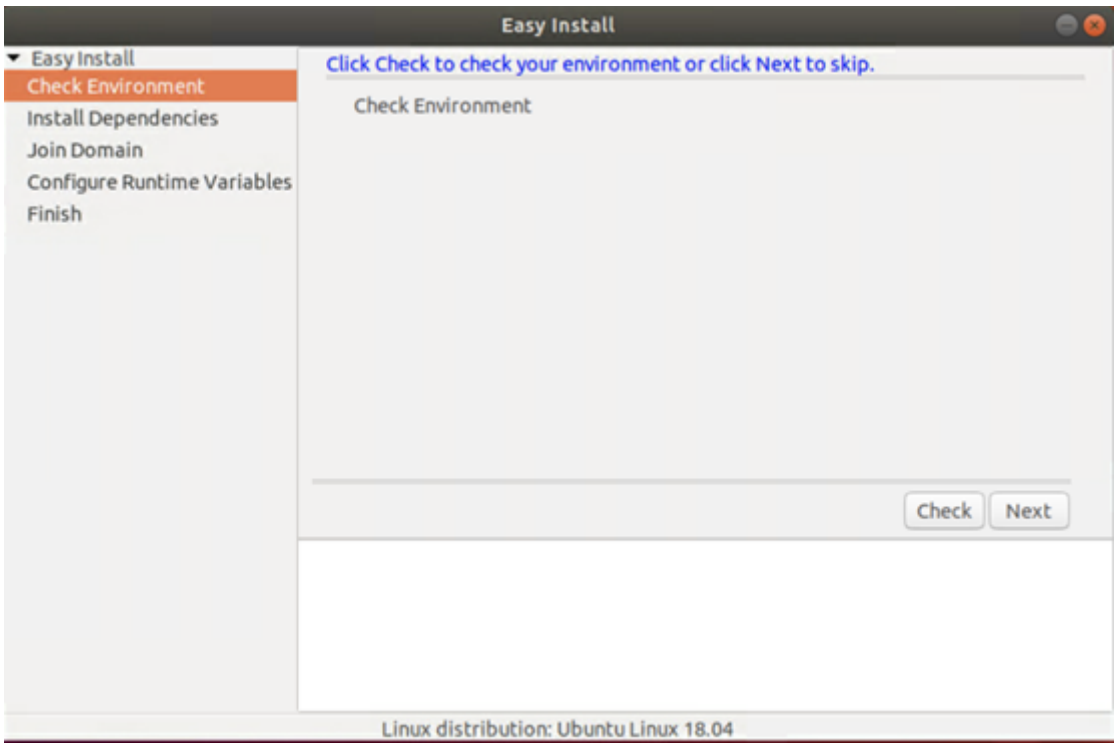
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Antes de configurar el entorno en tiempo de ejecución, asegúrese de que la configuración regional `en_US.UTF-8` esté instalada 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`. Para Debian, modifique el archivo `/etc/locale.gen` quitando la marca de comentario de la línea `# en_US.UTF-8 UTF-8` y, a continuación, ejecute el comando `sudo locale-gen`.

Modo interactivo:

Hay dos formas de utilizar Easy Install en modo interactivo:

- Ejecute el comando `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` y escriba el parámetro correspondiente en cada mensaje de la interfaz de línea de comandos.
- Ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio del VDA y, a continuación, siga las instrucciones de la GUI de Easy Install.



La GUI de Easy Install le guía a través de estas operaciones:

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

Modo silencioso:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Virtual Desktop se inician después del arranque de la máquina.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N**: Los servicios de Linux Virtual Desktop requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema de Linux Virtual Desktop.
- **CTX_XDL_HDX_3D_PRO = Y | N**: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. Si se selecciona HDX 3D Pro, el VDA se configura para el modo de escritorios VDI (sesión única); es decir, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N**: Indica si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos alojados. Para entornos HDX 3D Pro, establézcalo en Y.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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, establézcalo 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 Runtime 6.0 para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se va a utilizar en las sesiones. Si deja la variable sin especificar, se utilizará el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de la variable como **mate**.

  También puede cambiar el entorno de escritorio del usuario de una sesión de destino mediante estos pasos:

  1. Cree un archivo `.xsession` o `.Xclients` en el directorio **$HOME/<nombre de usuario\>** del VDA. Si utiliza Amazon Linux 2, cree un archivo `.Xclients`. Si usa otras distribuciones, cree un archivo `.xsession`.
  2. Modifique el archivo `.xsession` o `.Xclients` para especificar un entorno de escritorio basado en distribuciones.
     - **Para escritorios MATE en Amazon Linux 2, Debian, RHEL 8, SUSE 15 y Ubuntu**

```
MSESSION="$(type -p mate-session)"
if [ -n "$MSESSION" ]; then
  exec mate-session
fi
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Para escritorios GNOME Classic en Amazon Linux 2, CentOS, Debian, RHEL, SUSE 15 y Ubuntu**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- **Para escritorios GNOME en Amazon Linux 2, CentOS, Debian, RHEL, SUSE 15 y Ubuntu**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

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

- **CTX_XDL_START_SERVICE=Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración.
- **CTX_XDL_TELEMETRY_SOCKET_PORT**: El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT**: El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Si 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 Runtime 6.0.

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

```
export CTX_EASYINSTALL_HOSTNAME=host-name

export CTX_EASYINSTALL_DNS=ip-address-of-dns

export CTX_EASYINSTALL_NTPS=address-of-ntps

export CTX_EASYINSTALL_DOMAIN=domain-name

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify |
    pbis

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y | N

export CTX_XDL_ADD_FIREWALL_RULES=Y | N

export CTX_XDL_HDX_3D_PRO=Y | N

export CTX_XDL_VDI_MODE=Y | N

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

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

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

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y | N

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--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:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

Paso 8: Ejecute XDPing

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

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--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:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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

Comprobar el estado de Linux VDA:

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

```
sudo /sbin/service ctxvda status

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

Paso 10: Cree catálogos 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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 grupos 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 2203.

Solución de problemas

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Falla el proceso de unirse a un dominio mediante SSSD

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

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

/var/log/xdl/vda.log:

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

/var/log/messages:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 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:

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

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

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

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

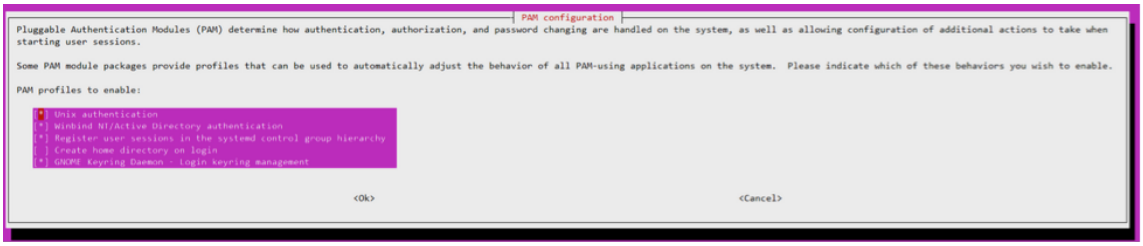
> **Sugerencia:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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):

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

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

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

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

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

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

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

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

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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 Amazon Linux 2, CentOS y RHEL manualmente

September 25, 2023

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paso 1: Prepare la distribución de Linux para la instalación de 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 cerciorarse de que el nombre de host de la máquina se notifique correctamente, cambie el archivo **/etc/hostname** para que solo contenga el nombre de host de la máquina.

```
hostname
```

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

Para asegurarse de que se notifiquen correctamente el nombre de dominio DNS y el nombre de dominio completo de la máquina (FQDN), cambie esta 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. 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

Paso 1f: Configure la sincronización horaria

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

Un entorno predeterminado RHEL 8 o RHEL 7 utiliza el demonio Chrony (`chronyd`) para la sincronización del reloj.

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

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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

Guarde los cambios y reinicie el demonio de Chrony:

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

Paso 1g: Instale OpenJDK 11

Linux VDA requiere la presencia de OpenJDK 11.

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

  ```
  amazon-linux-extras install java-openjdk11
  <!--NeedCopy-->
  ```

Confirme la versión correcta:

```
sudo yum info java-11-openjdk
<!--NeedCopy-->
```

El OpenJDK previamente empaquetado puede ser una versión anterior. Actualice la versión a OpenJDK 11:

```
sudo yum -y update java-11-openjdk
<!--NeedCopy-->
```

Paso 1h: Instale PostgreSQL

Linux VDA requiere PostgreSQL. Los siguientes comandos instalan PostgreSQL desde el paquete de Linux VDA (PostgreSQL 9 para Amazon Linux 2, RHEL 7 y CentOS 7, y PostgreSQL 10 para RHEL 8).

```
sudo yum -y install postgresql-server

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

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

Paso 1i: Inicie PostgreSQL

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

```
sudo systemctl enable postgresql

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

Compruebe la versión de PostgreSQL con:

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

(solo RHEL 7) Compruebe que se ha definido el directorio de datos mediante la utilidad de línea de comandos **psql**:

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

Paso 2: Prepare el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Haga estos cambios en función de la plataforma de hipervisor que se use. No se requieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix Hypervisor

Cuando está habilitada la función de sincronización horaria de Citrix Hypervisor en cada VM de Linux paravirtualizada, hay problemas con NTP y Citrix Hypervisor. Ambos intentan gestionar 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.

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 habilitada desde la máquina virtual de Linux:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -

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

Este comando devuelve 0 o 1:

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

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

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

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

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

```
su -

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

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

Desde el sistema operativo de administración:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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

Cuando la función de sincronización horaria de VMware está habilitada en cada VM de Linux paravirtualizada, hay problemas con el protocolo NTP y el hipervisor. Ambos 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
- 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

Instale o actualice los paquetes requeridos:

Para RHEL 8:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Para Amazon Linux 2, CentOS 7 y RHEL 7:

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

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

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

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

1. Ejecute este comando.

   Para RHEL 8:

   ```
   sudo authselect select winbind with-mkhomedir --force
   <!--NeedCopy-->
   ```

   Para Amazon Linux 2 y RHEL 7:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 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
   winbind offline logon = no
   ```

3. (solo RHEL 8) Abra **/etc/krb5.conf** y agregue entradas bajo las secciones `[libdefaults]`, `[realms]` y `[domain_realm]`:

   En la sección `[libdefaults]`:

   ```
   default_ccache_name = FILE:/tmp/krb5cc_%{ uid }
   default_realm = REALM
   dns_lookup_kdc = true
   ```

   En la sección `[realms]`:

   ```
   REALM = {
   kdc = fqdn-of-domain-controller
   }
   ```

   En la sección `[domain_realm]`:

   ```
   realm = REALM
   .realm = REALM
   ```

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:

Para RHEL 8:

```
sudo realm join -U user --client-software=winbind REALM
<!--NeedCopy-->
```

Para Amazon Linux 2 y RHEL 7:

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Compruebe que no haya puntos y comas al principio de cada parámetro. Estos cambios requieren reiniciar el demonio de Winbind:

```
sudo /sbin/service winbind restart
<!--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:

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

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

Examine los datos de la cuenta de la máquina:

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

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

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

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

Para 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.

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

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

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

Salga de la sesión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
exit
<!--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:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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

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

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

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

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

Salga de la sesión.

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

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

Centrify DirectControl

Unirse a un dominio de Windows Con el agente Centrify DirectControl instalado, una la máquina Linux al dominio de Active Directory mediante el comando `adjoin` de Centrify:

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 (VDA con Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para comprobar si hay una máquina Linux unida a Centrify en el dominio:

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

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

Para obtener información de diagnóstico y sistema más completa:

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

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

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

Continúe con el Paso 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. Habilitar SSSD
4. Verificar la configuración de Kerberos
5. Verificar la autenticación de usuario

Unirse al dominio y crear un keytab de host SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo de sistema keytab. En su lugar, puede usar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`adcli`, `realmd` o `Samba`.

En esta sección se describe el enfoque de `Samba` para Amazon Linux 2 y RHEL 7 y el enfoque de `adcli` para RHEL 8. Para `realmd`, consulte la documentación de RHEL o CentOS. Debe seguir estos pasos para configurar SSSD.

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

  Instale o actualice los paquetes requeridos:

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

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

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

  > **Nota:**
  >
  > Los parámetros de este artículo están pensados para el modelo de bosque y dominio únicos. Configure Kerberos en función de su infraestructura de AD.

  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
  winbind offline logon = no
  ```

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

- **Adcli (RHEL 8):**

  Instale o actualice los paquetes requeridos:

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

  Configure la máquina para la autenticación Kerberos y Samba:

  ```
  sudo authselect select sssd with-mkhomedir --force
  <!--NeedCopy-->
  ```

  Abra **/etc/krb5.conf** y agregue las entradas bajo las secciones [realms] y [domain_realm].

  En la sección [realms]:

  ```
  REALM = {
  kdc = fqdn-of-domain-controller
  }
  ```

  En la sección [domain_realm]:

  ```
  realm = REALM
  .realm = REALM
  ```

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

  ```
  sudo realm join REALM -U user
  <!--NeedCopy-->
  ```

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

Configurar SSSD Configurar SSSD consta de los siguientes pasos:

- Instale el paquete **sssd-ad** en Linux VDA ejecutando el comando `sudo yum -y install sssd`.
- 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** para RHEL 7 (se pueden agregar opciones adicionales, según sea necesario):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

# Should be specified as the lower-case version of the long version of the Active Directory domain.
ad_domain = ad.example.com

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

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

(Solo RHEL 8)

Abra **/etc/sssd/sssd.conf** y agregue estas entradas en la sección [domain/ad.example.com]:

```
ad_gpo_access_control = permissive
full_name_format = %2$s\\%1$s
fallback_homedir = /home/%d/%u
# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
```

Establezca la pertenencia y los permisos de archivos en sssd.conf:

```
chown root:root /etc/sssd/sssd.conf
chmod 0600 /etc/sssd/sssd.conf
restorecon /etc/sssd/sssd.conf
```

Habilitar SSSD Para RHEL 8:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ejecute los siguientes comandos para habilitar SSSD:

```
sudo systemctl restart sssd
sudo systemctl enable sssd.service
sudo chkconfig sssd on
<!--NeedCopy-->
```

Para Amazon Linux 2, CentOS 7 y RHEL 7:

Use `authconfig` para habilitar SSSD. Instale **oddjob-mkhomedir** para que la creación del directorio de inicio sea compatible con SELinux:

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

sudo service sssd start

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

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

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

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

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

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

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

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

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

```
sudo getent passwd DOMAIN\username
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--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.

```
sudo ssh localhost  – l DOMAIN\username

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

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

```
ls /tmp/krb5cc_{
 uid }

<!--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.

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

PBIS

Descargar el paquete PBIS requerido Para CentOS 7 y RHEL 7, por ejemplo:

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

Para Amazon Linux 2 y RHEL 8, por ejemplo:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
    pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Convertir el script de instalación de PBIS en ejecutable Para CentOS 7 y RHEL 7, por ejemplo:

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

Para Amazon Linux 2 y RHEL 8, por ejemplo:

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

Ejecutar el script de instalación de PBIS Para CentOS 7 y RHEL 7, por ejemplo:

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

Para Amazon Linux 2 y RHEL 8, por ejemplo:

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--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:

```
/opt/pbis/bin/domainjoin-cli join domain-name user
<!--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 (VDA con Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para comprobar si hay una máquina Linux unida a PBIS en el dominio:

```
/opt/pbis/bin/domainjoin-cli query
<!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

```
ssh localhost -l domain\user

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

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

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

Salga de la sesión.

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

Paso 4: Instale .NET Runtime 6.0 como requisito previo

Antes de instalar Linux VDA, instale .NET Runtime 6.0 conforme a las instrucciones de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de .NET Runtime. 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 de 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

   ```
   sudo /sbin/service ctxvda stop

   sudo /sbin/service ctxhdx stop
   <!--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:

   ```
   sudo rpm -e XenDesktopVDA
   <!--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. Descargar 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 de Linux VDA correspondiente a su distribución Linux.

3. Instalación de Linux VDA

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

     Para Amazon Linux 2:

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

     Para RHEL 8:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para RHEL 7 y CentOS 7:

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

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

Para Amazon Linux 2:

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

Para RHEL 8:

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

Para RHEL 7 y CentOS 7:

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

Lista de dependencias RPM para RHEL 8:

```
qt5-qtbase >= 5.5~

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python2 >= 2.7~

postgresql-jdbc >= 42.2.3

postgresql-server >= 10.6

java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.8.0

policycoreutils-python-utils >= 2.9

python3-policycoreutils >= 2.9

dbus >= 1.12.8

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

motif >= 2.3.4

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 2.2

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7
<!--NeedCopy-->
```

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

```
qt5-qtbase >= 5.5~

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

gperftools-libs >= 2.4

nss-tools >= 3.44.0

postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

motif >= 2.3.4

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
56
57  foomatic-filters >= 4.0.9
58
59  openldap >= 2.4
60
61  cyrus-sasl >= 2.1
62
63  cyrus-sasl-gssapi >= 2.1
64
65  libxml2 >= 2.9
66
67  python-requests >= 2.6.0
68
69  gperftools-libs >= 2.4
70
71  rpmlib(FileDigests) <= 4.6.0-1
72
73  rpmlib(PayloadFilesHavePrefix) <= 4.0-1
74
75  pmlib(CompressedFileNames) <= 3.0.4-1
76
77  rpmlib(PayloadIsXz) <= 5.2-1
78  <!--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.
>
> 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 la versión de una instalación existente desde las dos versiones anteriores y desde una versión LTSR.

> **Nota:**
>
> La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de iniciar una actualización, haga copia de seguridad de los archivos.

- Para actualizar el software con Yum:

  Para Amazon Linux 2:

  ```
  1  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
  2  <!--NeedCopy-->
  ```

  Para RHEL 8:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Para RHEL 7 y CentOS 7:

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

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

  Para Amazon Linux 2:

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

  Para RHEL 8:

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

  Para RHEL 7 y CentOS 7:

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

> **Nota:**
>
> Si utiliza RHEL 7, complete los pasos siguientes después de ejecutar los comandos de actualización anteriores:
>
> 1. ejecute `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "DotNetRuntimePath"-d "/opt/rh/rh-dotnet31/root/usr/bin/"--force` para establecer la ruta de ejecución de .NET correcta.
> 2. Reinicie el servicio `ctxvda`.
>
> **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.

> **Nota:**
>
> Para usar HDX 3D Pro para Amazon Linux 2, se recomienda instalar el controlador NVIDIA 470.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Para obtener más información, consulte Requisitos del sistema.

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
- Nutanix AHV

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:

```
yum install gcc

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

systemctl set-default multi-user.target
<!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
nvidia-smi

+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Establezca la configuración correcta para la tarjeta:

`etc/X11/ctx-nvidia.sh`

Para aprovechar las capacidades de varios monitores y altas resoluciones, necesitará una licencia válida de NVIDIA. Para aplicar la licencia, siga la documentación del producto de “GRID Licensing Guide.pdf - DU-07757-001 de septiembre de 2015 (en inglés)”.

Paso 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:

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

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 que hacen un uso intensivo de gráficos. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 los puertos 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. 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 Runtime 6.0 para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se va a utilizar en las sesiones. Si deja la variable sin especificar, se utilizará el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de la variable como **mate**.

  También puede cambiar el entorno de escritorio del usuario de una sesión de destino mediante estos pasos:

  1. Cree un archivo `.xsession` o `.Xclients` en el directorio **$HOME/<nombre de usuario\>** del VDA. Si utiliza Amazon Linux 2, cree un archivo `.Xclients`. Si usa otras distribuciones, cree un archivo `.xsession`.
  2. Modifique el archivo `.xsession` o `.Xclients` para especificar un entorno de escritorio basado en distribuciones.

     - **Para escritorios MATE en Amazon Linux 2 y RHEL 8**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
MSESSION="$(type -p mate-session)"
if [ -n "$MSESSION" ]; then
  exec mate-session
fi
```

- **Para escritorios GNOME Classic en Amazon Linux 2, CentOS y RHEL**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- **Para escritorios GNOME en Amazon Linux 2, CentOS y RHEL**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

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

- **CTX_XDL_START_SERVICE=Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT**: El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT**: El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

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

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
      none>'
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--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|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_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Quitar cambios de configuración

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

Consulte la ayuda de este script antes de continuar:

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

Para quitar los cambios de configuración:

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

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

Registros de configuración

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

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

Paso 9: Ejecute XDPing

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

Paso 10: Ejecute Linux VDA

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxhdx start

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

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

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

> **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:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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

Comprobar el estado de Linux VDA:

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

```
sudo /sbin/service ctxvda status

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

Paso 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 2203.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instalar Linux Virtual Delivery Agent para SUSE manualmente

February 12, 2024

> **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:

```
su -

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

Para iniciar la herramienta YaST de interfaz gráfica:

```
su -

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

Paso 1b: Configure la red

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

Configurar el nombre de host y el sistema de nombres de dominio (DNS)

1. Inicie la herramienta YaST de interfaz gráfica.
2. Seleccione **System** y, luego, **Network Settings**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Abra la ficha **Hostname/DNS**.
4. Seleccione la opción **no** para **Set Hostname via DHCP**.
5. Seleccione la opción **Use Custom Policy** para **Modify DNS Configuration**.
6. Modifique lo siguiente para que refleje su propia configuración de red:
   - **Static Hostname**: Agregue el nombre de host 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.
7. Cambie esta 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 <FQDN of the VDA> <hostname of the VDA> localhost
   ```

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

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

Paso 1c: Configure el servicio NTP

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

Para SUSE 15.3 y SUSE 15.2:

1. Inicie la herramienta YaST de interfaz gráfica.
2. Seleccione **Network Services** y, a continuación, **NTP Configuration**.
3. En la sección **Start NTP Daemon**, seleccione **Now and on Boot**.
4. Seleccione **Dynamic** para **Configuration Source**.
5. Agregue servidores NTP según sea necesario. Por regla general, el servicio NTP se aloja en el controlador de dominio de Active Directory.
6. Elimine o comente esta línea en /etc/chrony.conf si existe.

   ```
   include /etc/chrony.d/*.conf
   ```

   Después de modificar chrony.conf, reinicie el servicio `chronyd`.

   ```
   sudo systemctl restart chronyd.service
   <!--NeedCopy-->
   ```

Paso 1d: Instale paquetes dependientes de Linux VDA

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

- Postgresql13-server 13 o una versión posterior

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- OpenJDK 11
- Open Motif Runtime Environment 2.3.1 o una versión posterior
- Cups 1.6.0 o una versión posterior
- ImageMagick 6.8 o una versión posterior

Agregar repositorios Puede obtener la mayoría de los paquetes necesarios, excepto ImageMagick, de los repositorios oficiales. Para obtener los paquetes de ImageMagick, habilite el repositorio `sle-module-desktop-applications` mediante YaST o este comando:

```
SUSEConnect -p sle-module-desktop-applications/<version number>/
x86_64
```

Instalar el cliente Kerberos Instale el cliente Kerberos para la autenticación mutua entre el 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 11 Linux VDA requiere la presencia de OpenJDK 11.

Para instalar OpenJDK 11, ejecute el siguiente comando:

```
1 sudo zypper install java-11-openjdk
2 <!--NeedCopy-->
```

Instalar PostgreSQL Para instalar `Postgresql`, ejecute estos comandos:

```
1 sudo zypper install postgresql-server
2
3 sudo zypper install postgresql-jdbc
4 <!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Haga estos cambios en función de la plataforma de hipervisor que se use. 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 función de sincronización horaria de Citrix Hypervisor en cada VM de Linux paravirtualizada, hay problemas con NTP y Citrix Hypervisor. Ambos intentan gestionar 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.

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 habilitada desde la máquina virtual de Linux:

```
su -

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

Este comando devuelve 0 o 1:

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

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

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

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

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de reiniciar, compruebe que la configuración es correcta:

```
su -

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

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

Desde el sistema operativo de administración:

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

> **Nota:**
>
> Este método difiere de 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 la función de sincronización horaria de VMware está habilitada en cada VM de Linux paravirtualizada, hay problemas con el protocolo NTP y el hipervisor. Ambos intentan sincronizar 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.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

Siga las instrucciones en función del método elegido.

> **Nota:**
>
> Es posible que no se puedan iniciar sesiones cuando se usa el mismo nombre de usuario para la cuenta local en el Linux VDA y para 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. Inicie YaST, seleccione **Network Services** y, a continuación, **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 **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 le solicita que instale algunos paquetes, haga clic en **Install**.
4. Si se encuentra un controlador de dominio, se le pregunta si quiere unirse al dominio. Haga clic en **Sí**.
5. Cuando se le solicite, introduzca las credenciales de un usuario de dominio con permisos para agregar máquinas al dominio y haga clic en **OK**.
6. Reinicie los servicios manualmente o reinicie la máquina. Le recomendamos que reinicie la máquina:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -
reboot
<!--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.

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

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

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

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

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

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

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

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

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

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

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

Examine los datos de la cuenta de la máquina:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

Compruebe que el módulo PAM de Winbind esté configurado correctamente. Para hacerlo, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

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

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

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

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

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

Salga de la sesión.

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

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

Servicio de autenticación Quest

Configurar Quest en el controlador de dominio Se asume que se ha instalado y configurado el software de Quest en los controladores de dominio, 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Configurar Quest en Linux VDA

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

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

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

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

Configurar PAM y NSS Para habilitar los inicios de sesión del usuario de dominio mediante HDX y otros servicios como su, ssh o RDP, configure PAM y NSS de forma manual:

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

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

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

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. En cambio, si la máquina no está unida a ningún dominio, aparece el siguiente error:

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

Verificar la autenticación de usuario Verifique que Quest pueda autenticar a los usuarios del dominio mediante PAM. Para hacerlo, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

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

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

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

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

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

Salga de la sesión.

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
sudo adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

El parámetro **user** es un usuario de dominio de Active Directory con permisos para unir máquinas 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:

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

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo  – diag
<!--NeedCopy-->
```

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

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

SSSD

Si utiliza SSSD en SUSE, 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 SUSE, siga estos pasos:

1. Unirse al dominio y crear keytabs de host

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Configurar PAM para SSSD
3. Configurar SSSD
4. Habilitar SSSD
5. Verificar la pertenencia al dominio
6. Verificar la configuración de Kerberos
7. Verificar la autenticación de usuario

Unirse al dominio y crear un keytab de host SSSD no proporciona funciones de cliente de Active Directory para unirse al dominio y administrar el archivo de sistema keytab. Puede usar el enfoque de Samba en su lugar. Complete los siguientes pasos antes de configurar SSSD.

1. Detenga e inhabilite el demonio de caché para el servicio de nombres (NSCD).

```
sudo systemctl stop nscd
sudo systemctl disable nscd
<!--NeedCopy-->
```

2. Compruebe el nombre del host y la sincronización horaria de Chrony.

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

3. Instale o actualice los paquetes requeridos:

```
sudo zypper install samba-client sssd-ad
<!--NeedCopy-->
```

4. Modifique el archivo `/etc/krb5.conf` como usuario root para permitir que la utilidad `kinit` se comunique con el dominio de destino. Agregue estas entradas bajo las secciones **[libdefaults]**, **[realms]** y **[domain_realm]**:

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. Estos parámetros están pensados para el modelo de bosque y dominio únicos.

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[realms]

    REALM = {


        kdc = fqdn-of-domain-controller

        default_domain = realm

        admin_server = fqdn-of-domain-controller
     }

[domain_realm]

    .realm = REALM
<!--NeedCopy-->
```

realm es el nombre del territorio Kerberos, como ejemplo.com. **REALM** es el nombre del territorio Kerberos en mayúsculas, como EJEMPLO.COM.

5. Modifique `/etc/samba/smb.conf` como usuario root para permitir que la utilidad **net** se comunique con el dominio de destino. Agregue estas entradas bajo la sección **[global]**:

```
[global]
    workgroup = domain

    client signing = yes

    client use spnego = yes

    kerberos method = secrets and keytab

    realm = REALM

    security = ADS
<!--NeedCopy-->
```

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

6. Modifique las entradas **passwd** y **group** en el archivo `/etc/nsswitch.conf` para hacer referencia a SSSD al resolver usuarios y grupos.

```
passwd: compat sss

group: compat sss
<!--NeedCopy-->
```

7. Utilice el cliente Kerberos configurado para autenticarse en el dominio de destino como administrador.

```
kinit administrator
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Utilice la utilidad `net` para unir el sistema al dominio y generar un archivo keytab del sistema.

```
net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
    administrator
<!--NeedCopy-->
```

Configurar PAM para SSSD Antes de configurar PAM para SSSD, instale o actualice los paquetes necesarios.

```
sudo zypper install sssd sssd-ad
<!--NeedCopy-->
```

Configure el módulo PAM para la autenticación de usuarios a través de SSSD y cree directorios de inicio para los inicios de sesión de usuario.

```
sudo pam-config --add  --sss
sudo pam-config --add --mkhomedir
<!--NeedCopy-->
```

Configurar SSSD

1. Modifique el archivo `/etc/sssd/sssd.conf` como usuario root para permitir que el demonio SSSD se comunique con el dominio de destino. A continuación, se ofrece un ejemplo de configuración de `sssd.conf` (se pueden agregar opciones adicionales, según sea necesario):

```
[sssd]
    config_file_version = 2
    services = nss,pam
    domains = domain-dns-name

[domain/domain-dns-name]
    id_provider = ad
    auth_provider = ad
    access_provider = ad
    ad_domain = domain-dns-name
    ad_server = fqdn-of-domain-controller
    ldap_id_mapping = true
    ldap_schema = ad

# Kerberos settings
    krb5_ccachedir = /tmp
    krb5_ccname_template = FILE:%d/krb5cc_%U

# Comment out if the users have the shell and home dir set on the
   AD side

    fallback_homedir = /home/%d/%u
    default_shell = /bin/bash

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
# Uncomment and adjust if the default principal SHORTNAME$@REALM
    is not available

# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM

    ad_gpo_access_control = permissive

<!--NeedCopy-->
```

domain-dns-name es el nombre de dominio DNS, como example.com.

> **Nota:**
>
> **ldap_id_mapping** tiene el valor true, de forma que el propio SSSD se ocupa de asignar los SID de Windows a UID de Unix. De lo contrario, Active Directory debe poder proporcionar extensiones POSIX. **ad_gpo_access_control** está establecido en **permissive** para evitar un error de inicio de sesión no válido con las sesiones de Linux. Consulte las páginas man de `sssd.conf` y `sssd-ad`.

2. Establezca la pertenencia y los permisos de archivos en `sssd.conf`:

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

Habilitar SSSD Ejecute los siguientes comandos para habilitar e iniciar el demonio SSSD cuando se inicie el sistema:

```
sudo systemctl enable sssd
sudo systemctl start sssd
<!--NeedCopy-->
```

Verificar la pertenencia al dominio

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

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Muestra la lista de las claves disponibles para las distintas combinaciones de nombres principales y conjuntos de cifrado.

Ejecute el comando `kinit` de Kerberos para autenticar la máquina en el controlador de dominio con estas claves:

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

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

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

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

Verificar la autenticación de usuario 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.

```
ssh localhost -l domain\username

id -u

klist

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

PBIS

Descargar el paquete PBIS requerido Por ejemplo:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
    pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

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

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

Ejecutar el script de instalación de PBIS Por ejemplo:

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

Unirse a un 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:

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

El parámetro **user** es un usuario de dominio con permisos para agregar máquinas 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 (VDA con Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para comprobar si hay una máquina Linux unida a PBIS en el dominio:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Verifique que PBIS pueda autenticar a los usuarios del dominio mediante PAM. Para hacerlo, inicie sesión en Linux VDA con una cuenta de usuario de dominio que no se haya utilizado antes.

```
ssh localhost -l domain\user

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

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

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

Salga de la sesión.

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

Paso 4: Instale .NET Runtime 6.0 como requisito previo

Antes de instalar Linux VDA, instale .NET Runtime 6.0 conforme a las instrucciones de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de .NET Runtime. 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 de Linux VDA correspondiente a su distribución Linux.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--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:

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

> **Importante:**
>
> Se admite la actualización desde las dos últimas versiones.
>
> **Nota:**
>
> Puede encontrar los componentes instalados en **/opt/Citrix/VDA/**.
>
> Para ejecutar un comando, se necesita la ruta completa. 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:

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

> **Nota:**
>
> La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de iniciar una actualización, haga copia de seguridad de los archivos.

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

Lista de dependencias de RPM para SUSE 15:

```
postgresql >= 13

postgresql-server >= 13

postgresql-jdbc >= 9.4

java-11-openjdk >= 11

ImageMagick >= 7.0

dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

motif >= 2.3.4

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4

cups >= 2.2

cups-filters >= 1.25
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
38
39 libxml2-2 >= 2.9
40
41 libmspack0 >= 0.6
42
43 ibus >= 1.5
44
45 libtcmalloc4 >= 2.5
46
47 libcap-progs >= 2.26
48
49 mozilla-nss-tools >= 3.53.1
50
51 libpython2_7-1_0 >= 2.7
52 <!--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
- Nutanix AHV

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 que el script realice cambios, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

Configuración automatizada

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

Las variables de entorno admitidas son:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N**: Linux VDA permite especificar un nombre de Delivery Controller mediante un registro CNAME de DNS. Se establece en N de forma predeterminada.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'**: Linux VDA necesita una lista de nombres de dominio completo de Delivery Controllers, separados por espacios, para registrarse en un Delivery Controller. Se debe especificar al menos un FQDN o alias de CNAME.
- **CTX_XDL_VDA_PORT=port-number**: Linux VDA se comunica con los Delivery Controllers a través de un puerto TCP/IP. Este es el puerto 80 de forma predeterminada.
- **CTX_XDL_REGISTER_SERVICE=Y | N**: Los servicios de Linux VDA 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 VDA requieren que se permitan las conexiones de red entrantes a través del firewall del sistema. Puede abrir automáticamente los puertos necesarios (de forma predeterminada, los puertos 80 y 1494) en el firewall del sistema para 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 1 –Samba Winbind
  - 2 –Servicio de autenticación Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD

- **CTX_XDL_HDX_3D_PRO = Y | N**: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. Si se selecciona HDX 3D Pro, 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 los puertos 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. 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 Runtime 6.0 para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se va a utilizar en las sesiones. Si deja la vari-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

able sin especificar, se utilizará el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de la variable como **mate**.

También puede cambiar el entorno de escritorio del usuario de una sesión de destino mediante estos pasos:

1. Cree un archivo `.xsession` en el directorio **$HOME/<nombre de usuario\>** del VDA.
2. Modifique el archivo `.xsession` para especificar un entorno de escritorio basado en distribuciones.
   - **Para escritorios MATE en SUSE 15**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

   - **Para escritorios GNOME Classic en SUSE 15**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

   - **Para escritorios GNOME en SUSE 15**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     ```

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

- **CTX_XDL_START_SERVICE=Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT**: El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT**: El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--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`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Paso 9: Ejecute XDPing

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

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:

```
sudo /sbin/service ctxhdx start

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

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

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

> **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:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comprobar el estado de Linux VDA:

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

```
sudo /sbin/service ctxvda status

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

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

Paso 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Los grupos y usuarios de AD que seleccione deben estar correctamente configurados para poder iniciar sesión en las máquinas de Linux VDA.
- 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 2203.

Instalar Linux Virtual Delivery Agent para Ubuntu manualmente

July 6, 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 cerciorarse de 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 notifican 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A:

```
hosts: files dns
```

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

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

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

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

Instalar Chrony:

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

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

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

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

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

Guarde los cambios y reinicie el demonio de Chrony:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Paso 1h: Instale OpenJDK 11

Linux VDA requiere la presencia de OpenJDK 11.

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

```
sudo apt-get install -y openjdk-11-jdk
<!--NeedCopy-->
```

Paso 1i: Instale PostgreSQL

Linux VDA requiere PostgreSQL 9.x en Ubuntu:

```
sudo apt-get install -y postgresql

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

Paso 1j: Instale Motif

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

Paso 1k: Instale otros paquetes

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

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

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

sudo apt-get install -y krb5-user

sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Paso 2: Prepare el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Haga estos cambios en función de la plataforma de hipervisor que se use. No se re-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

quieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix Hypervisor

Cuando está habilitada la función de sincronización horaria de Citrix Hypervisor en cada VM de Linux paravirtualizada, hay problemas con NTP y Citrix Hypervisor. Ambos intentan gestionar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, compruebe que el reloj del sistema de cada invitado de Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

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 habilitada desde la máquina virtual de Linux:

```
su -

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

Este comando devuelve 0 o 1:

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

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

Si está habilitada, inhabilite la función de sincronización horaria escribiendo 1 en el archivo:

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

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

```
su -

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

Este comando devuelve el valor 1.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 cerciorarse de que el reloj del sistema no se desincroniza, 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

Cuando la función de sincronización horaria de VMware está habilitada en cada VM de Linux paravirtualizada, hay problemas con el protocolo NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, compruebe que el reloj del sistema de cada invitado de Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host.

Si ejecuta un kernel Linux paravirtualizado con VMware Tools instalado:

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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

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

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

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

> **Nota:**
>
> Compruebe que el script `winbind` se encuentra en `/etc/init.d`.

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

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. Estos parámetros están pensados para el modelo de bosque y dominio únicos.

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como **ejemplo.com**. **REALM** es el nombre del territorio Kerberos en mayúsculas, como **EJEMPLO.COM**.

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

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

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Reiniciar `winbind`

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

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

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

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

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

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

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

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

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

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

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

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

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

Los nombres de máquina y territorio deben especificarse en mayúsculas. Debe anteponerse la barra diagonal inversa (\) al signo de dólar ($) para evitar la sustitución del shell. En algunos entornos, el nombre de dominio DNS difiere del nombre del territorio Kerberos. Compruebe que se usa el nombre

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

del territorio Kerberos. Si la operación de este comando se realiza correctamente, no aparece ningún resultado.

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

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

Examine los datos de la cuenta de la máquina:

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

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

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

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

Para 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.

```
ssh localhost -l domain\username

id -u
<!--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**:

```
ls /tmp/krb5cc_uid
<!--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:

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

Salga de la sesión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
exit
<!--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.

Servicio de autenticación Quest

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

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

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

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

Configurar Quest en Linux VDA

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

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

```
SELINUX=disabled
```

Este cambio requiere un reinicio de la máquina:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

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

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. En cambio, si la máquina no está unida a ningún dominio, aparece el siguiente error:

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

Verificar la autenticación de usuario Para 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.

```
ssh localhost -l domain\username

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

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

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

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

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

Salga de la sesión.

```
exit
<!--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:

```
su -
adjoin -w -V -u user domain-name
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

El parámetro **user** es un usuario de dominio de Active Directory con permisos para unir equipos al dominio de Active Directory. El parámetro **domain-name** es el nombre del dominio al que se unirá la máquina Linux.

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

```
su -

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

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

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

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

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

SSSD

Configurar Kerberos Ejecute el siguiente comando para instalar Kerberos:

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

Para configurar Kerberos, abra **/etc/krb5.conf** como root y establezca los parámetros:

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. Estos parámetros están pensados para el modelo de bosque y dominio únicos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

El parámetro `domain-dns-name` en este contexto es el nombre de dominio DNS, como ejemplo.com. *REALM* es el nombre del territorio Kerberos en mayúsculas, como EJEMPLO.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. En su lugar, puede usar `adcli`, `realmd` o `Samba`.

> **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`.

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

2. Únase al dominio con `adcli`.

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

   ```
   su -

   rm -rf /etc/krb5.keytab

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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

   En el caso de máquinas con Ubuntu 18.04, ejecute el comando `sudo klist -ket` para asegurarse de que se haya creado el archivo keytab del sistema.

   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.

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

2. Configure Samba.

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

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
```

   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.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Configurar SSSD **Instalar o actualizar los paquetes requeridos:**

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

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

Si los paquetes ya están instalados, se recomienda actualizarlos:

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

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

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

```
[sssd]

services = nss, pam

config_file_version = 2

domains = domain-dns-name

[domain/domain-dns-name]

id_provider = ad

access_provider = ad

auth_provider = krb5

krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
krb5_renew_interval = 1h
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
# This ldap_id_mapping setting is also the default value
ldap_id_mapping = true
override_homedir = /home/%d/%u
default_shell = /bin/bash
ad_gpo_map_remote_interactive = +ctxhdx
```

> **Nota:**
>
> ldap_id_mapping 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.
>
> El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como ejemplo.com. **REALM** es el nombre del territorio Kerberos en mayúsculas, como EJEMPLO.COM. No es necesario configurar el nombre de dominio NetBIOS.
>
> Para obtener 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 este comando y compruebe que las opciones **SSS authentication** y **Create home directory on login** están seleccionadas:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA (VDA con 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, compruebe que el archivo del sistema keytab se ha creado y contiene claves válidas:

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

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

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

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

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

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

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.

```
ssh localhost -l domain\username

id -u

klist
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 (VDA con Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para comprobar si hay una máquina Linux unida a PBIS en el dominio:

```
/opt/pbis/bin/domainjoin-cli query
<!--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.

```
sudo ssh localhost -l domain\user

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

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

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

Salga de la sesión.

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

Paso 4: Instale .NET Runtime 6.0 como requisito previo

Antes de instalar Linux VDA, instale .NET Runtime 6.0 conforme a las instrucciones de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar su ruta de runtime.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 20.04:

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

Para Ubuntu 18.04:

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

Lista de dependencias de Debian para Ubuntu 20.04:

```
libqt5widgets5 >= 5.7~

ibus >= 1.5

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

postgresql >= 12

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

libgoogle-perftools4 >= 2.7~

libpython2.7 >= 2.7~
<!--NeedCopy-->
```

Lista de dependencias de Debian para Ubuntu 18.04:

```
libqt5widgets5 >= 5.7~

libmspack0 >= 0.6

ibus >= 1.5

libnss3-tools >= 2:3.35

postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

openjdk-11-jdk >= 11

gtk3-nocsd >=3

imagemagick >= 8:6.8.9.9

ufw >= 0.35

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

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

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~

xserver-xorg-core >= 2:1.18

xserver-xorg-core << 2:1.19

x11vnc>=0.9.13

python-websockify >= 0.6.1
<!--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.

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

> **Nota:**
>
> La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de iniciar una actualización, haga copia de seguridad de los archivos.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- VMware ESX
- Nutanix AHV

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

1. Asegúrese de que la 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:

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

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

Configuración automatizada

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

Las variables de entorno admitidas son:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N**: Linux VDA permite especificar un nombre de Delivery Controller mediante un registro CNAME de DNS. Se establece en N de forma predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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 –Servicio de autenticación Quest
  - 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 los puertos de LDAP. Por ejemplo, ad1.miempresa.com:389. Esta variable está establecida en **<none>** de forma predeterminada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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=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 `AD Group Policy`. 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 `AD Group Policy`. 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 Runtime 6.0 para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se va a utilizar en las sesiones. Si deja la variable sin especificar, se utilizará el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de la variable como **mate**.

  También puede cambiar el entorno de escritorio del usuario de una sesión de destino mediante estos pasos:

  1. Cree un archivo `.xsession` en el directorio **$HOME/<nombre de usuario\>** del VDA.
  2. Modifique el archivo `.xsession` para especificar un entorno de escritorio basado en distribuciones.

     - **Para escritorios MATE**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Para escritorios GNOME Classic**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

     - **Para escritorios GNOME**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3   exec gnome-session
4   fi
```

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

- **CTX_XDL_START_SERVICE=Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT**: El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT**: El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

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

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

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

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Para quitar los cambios de configuración:

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

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

Registros de configuración

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

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

Desinstalar el software de Linux VDA

Para comprobar si Linux VDA está instalado y para ver la versión del paquete instalado:

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

Para ver información más detallada:

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

Para desinstalar el software de Linux VDA:

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> La información en esta sección no cubre la eliminación de paquetes dependientes incluido el de PostgreSQL.

Paso 9: Ejecute XDPing

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

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:

```
sudo systemctl start ctxhdx

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

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda

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

> **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:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Comprobar el estado de Linux VDA:

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

```
sudo systemctl status ctxvda

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

Paso 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 2203.

Instalar Linux Virtual Delivery Agent para Debian manualmente

July 8, 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 Debian 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 cerciorarse de 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 notifican 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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. 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:

```
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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

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

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

Instalar Chrony:

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

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

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

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

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

Guarde los cambios y reinicie el demonio de Chrony:

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

Paso 1h: Instale los paquetes

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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Paso 1i: Agregue el repositorio `oldstable`

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

Paso 1j: Instale PostgreSQL

Linux VDA requiere PostgreSQL versión 11 en Debian:

```
sudo apt-get install -y postgresql

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

Paso 2: Prepare el hipervisor

Se necesitan algunos cambios cuando se ejecuta Linux VDA como una máquina virtual en un hipervisor admitido. Haga estos cambios en función de la plataforma de hipervisor que se use. No se requieren cambios si se está ejecutando la máquina Linux sin sistema operativo.

Corregir la sincronización horaria en Citrix Hypervisor

Cuando está habilitada la función de sincronización horaria de Citrix Hypervisor en cada VM de Linux paravirtualizada, hay problemas con NTP y Citrix Hypervisor. Ambos intentan gestionar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, compruebe que el reloj del sistema de cada invitado de Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host. No se requieren cambios en el modo HVM.

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 habilitada desde la máquina virtual de Linux:

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

Este comando devuelve 0 o 1:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 está habilitada, inhabilite la función de sincronización horaria escribiendo 1 en el archivo:

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

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Corregir la sincronización horaria en ESX y ESXi

Cuando la función de sincronización horaria de VMware está habilitada en cada VM de Linux paravirtualizada, hay problemas con el protocolo NTP y el hipervisor. Ambos intentan sincronizar el reloj del sistema. Para evitar la desincronización del reloj respecto a los demás servidores, el reloj del sistema de cada invitado Linux debe sincronizarse con NTP. Por eso, es necesario inhabilitar la sincronización horaria del host.

Si ejecuta un kernel Linux paravirtualizado con VMware Tools instalado:

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

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

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

> **Nota:**
>
> Compruebe que el script `winbind` se encuentra en `/etc/init.d`.

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

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. Estos parámetros están pensados para el modelo de bosque y dominio únicos.

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como **ejemplo.com**. **REALM** es el nombre del territorio Kerberos en mayúsculas, como **EJEMPLO.COM**.

Configurar la autenticación de Winbind Abra **/etc/samba/smb.conf** y configure los parámetros siguientes:

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

WORKGROUP es el primer campo 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: systemd winbind
group: systemd winbind
```

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

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

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

Reiniciar Winbind

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

Examine los datos de la cuenta de la máquina:

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Para 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.

```
ssh localhost -l domain\username

id -u
<!--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**:

```
ls /tmp/krb5cc_uid
<!--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:

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

Salga de la sesión.

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Servicio de autenticación Quest

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

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

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

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

Configurar Quest en Linux VDA

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

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

```
SELINUX=disabled
```

Este cambio requiere un reinicio de la máquina:

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

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

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

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

Si la máquina está unida a un dominio, este comando devuelve el nombre del dominio. En cambio, si la máquina no está unida a ningún dominio, aparece el siguiente error:

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

```
ssh localhost -l domain\username

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

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

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

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

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

Salga de la sesión.

```
exit
<!--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:

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

El parámetro **user** es un usuario de dominio de Active Directory con permisos para unir equipos al dominio de Active Directory. El parámetro **domain-name** es el nombre del dominio al que se unirá la máquina Linux.

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

```
su -

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

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

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

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

SSSD

Configurar Kerberos Ejecute el siguiente comando para instalar Kerberos:

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

Para configurar Kerberos, abra **/etc/krb5.conf** como root y establezca los parámetros:

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. Estos parámetros están pensados para el modelo de bosque y dominio únicos.

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[domain_realm]

domain-dns-name = *REALM*

.*domain-dns-name* = *REALM*

El parámetro domain-dns-name en este contexto es el nombre de dominio DNS, como ejemplo.com. *REALM* es el nombre del territorio Kerberos en mayúsculas, como EJEMPLO.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. En su lugar, puede usar adcli, realmd o Samba.

> **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.

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

2. Únase al dominio con adcli.

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

   ```
   su -

   rm -rf /etc/krb5.keytab

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

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

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

3. Compruebe el archivo keytab del sistema.

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

1. Instale el paquete.

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

2. Configure Samba.

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

   ```
   [global]

   workgroup = WORKGROUP

   security = ADS

   realm = REALM

   client signing = yes

   client use spnego = yes

   kerberos method = secrets and keytab
   ```

   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.

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

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

Configurar SSSD Instalar o actualizar los paquetes requeridos:

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

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

Si los paquetes ya están instalados, se recomienda actualizarlos:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

```
[sssd]

services = nss, pam

config_file_version = 2

domains = domain-dns-name

[domain/domain-dns-name]

id_provider = ad

access_provider = ad

auth_provider = krb5

krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true

override_homedir = /home/%d/%u

default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> ldap_id_mapping tiene el valor **true**, de forma que el propio SSSD se ocupa de asignar los SID de Windows a UID de Unix. De lo contrario, `Active Directory` debe poder proporcionar extensiones POSIX. El `ctxhdx` de servicio PAM se agrega a ad_gpo_map_remote_interactive.
>
> El parámetro **domain-dns-name** en este contexto es el nombre de dominio DNS, como ejemplo.com. **REALM** es el nombre del territorio Kerberos en mayúsculas, como EJEMPLO.COM. No es necesario configurar el nombre de dominio NetBIOS.
>
> Para obtener 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:

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--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:

```
sudo systemctl start sssd

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

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

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

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA (VDA con 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

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

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

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

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

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.

```
ssh localhost -l domain\username

id -u

klist

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

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

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

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

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

Ejecutar el script de instalación de PBIS Por ejemplo:

```
sudo sh pbis-open-8.8.0.506.linux.x86_64.deb.sh
<!--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:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--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 (VDA con Windows y Linux) tengan un objeto de equipo en `Active Directory`. Para comprobar si hay una máquina Linux unida a PBIS en el dominio:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

```
sudo ssh localhost -l domain\user

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

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

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

Salga de la sesión.

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

Continúe con el Paso 6: Instale Linux VDA después de la verificación de unión al dominio.

Paso 4: Instale .NET Runtime 6.0 como requisito previo

Antes de instalar Linux VDA, instale .NET Runtime 6.0 conforme a las instrucciones de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Después de instalar .NET Runtime 6.0, ejecute el comando **which dotnet** para encontrar su ruta de runtime.

En función del resultado del comando, establezca la ruta binaria de .NET Runtime. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paso 6: Instale Linux VDA

Paso 6a: Instale Linux VDA

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

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

Lista de dependencias de Debian para Debian 10.9:

```
libqt5widgets5          >= 5.5~
ibus                    >= 1.5
postgresql              >= 11
libpostgresql-jdbc-java >= 42.2
openjdk-11-jdk           >= 11
imagemagick             >= 8:6.9.10
ufw                     >= 0.36
desktop-base            >= 10.0.2
libxrandr2              >= 2:1.5.1
libxtst6                >= 2:1.2.3
libxm4                  >= 2.3.8
util-linux              >= 2.33
gtk3-nocsd              >= 3
bash                    >= 5.0
findutils               >= 4.6.0
sed                     >= 4.7
cups                    >= 2.2
ghostscript             >= 9.27~
libmspack0              >= 0.10
libgoogle-perftools4    >= 2.7~
libpython2.7            >= 2.7~
libsasl2-modules-gssapi-mit >= 2.1.~
<!--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.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La actualización de una instalación existente sobrescribe los archivos de configuración en /etc/xdl. Antes de iniciar una actualización, haga copia de seguridad de los archivos.

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
- Nutanix AHV

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:

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

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 –Servicio de autenticación Quest
  - 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 los puertos 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=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. 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 Runtime 6.0 para admitir el nuevo servicio de agente intermediario (`ctxvda`). La ruta predeterminada es /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Especifica el entorno de escritorio GNOME, GNOME Classic o MATE que se va a utilizar en las sesiones. Si deja la variable sin especificar, se utilizará el escritorio instalado actualmente en el VDA. Sin embargo, si el escritorio instalado actualmente es MATE, debe establecer el valor de la variable como **mate**.

  También puede cambiar el entorno de escritorio del usuario de una sesión de destino mediante estos pasos:

  1. Cree un archivo `.xsession` en el directorio **$HOME/<nombre de usuario\>** del VDA.
  2. Modifique el archivo `.xsession` para especificar un entorno de escritorio basado en distribuciones.

     - **Para escritorios MATE**

```
MSESSION="$(type -p mate-session)"
if [ -n "$MSESSION" ]; then
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  exec mate-session
fi
```

- **Para escritorios GNOME Classic**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- **Para escritorios GNOME**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

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

- **CTX_XDL_START_SERVICE=Y | N**: Indica si los servicios de Linux VDA se inician cuando se complete su configuración. Se establece en Y de forma predeterminada.
- **CTX_XDL_TELEMETRY_SOCKET_PORT**: El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT**: El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

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

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
   none>'
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--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|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_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Quitar cambios de configuración

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

Consulte la ayuda de este script antes de continuar:

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

Para quitar los cambios de configuración:

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

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

Registros de configuración

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

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

Desinstalar el software de Linux VDA

Para comprobar si Linux VDA está instalado y para ver la versión del paquete instalado:

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

Para ver información más detallada:

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

Para desinstalar el software de Linux VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Paso 9: Ejecute XDPing

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

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:

```
sudo systemctl start ctxhdx

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

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> `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:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

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

Comprobar el estado de Linux VDA:

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

```
sudo systemctl status ctxvda

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

Paso 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:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 2203.

Crear Linux VDA en Citrix DaaS Standard para Azure

June 14, 2023

En Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure), puede crear tanto Linux VDA unidos a un dominio como Linux VDA no unidos a un dominio para entregar aplicaciones y escritorios virtuales a cualquier dispositivo desde Microsoft Azure. Para obtener más información, consulte Citrix DaaS Standard para Azure.

Distribuciones compatibles de Linux

Las siguientes distribuciones de Linux admiten esta funcionalidad:

- RHEL 8.3
- RHEL 8.2
- Ubuntu 20.04
- Ubuntu 18.04

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pasos

Para crear VDA Linux en Citrix DaaS Standard para Azure, siga estos pasos:

1. Prepare una imagen maestra en Azure:

   > **Nota:**
   >
   > También puede utilizar la función Autoactualización de Linux VDA para programar actualizaciones automáticas de software. Para hacerlo, agregue líneas de comandos al archivo etc/xdl/mcs/mcs_local_setting.reg de la imagen maestra.
   > Por ejemplo, puede agregar las siguientes líneas de comandos:

   ```
   create -k "HKLM\System\CurrentControlSet\Control\Citrix\
       SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" –
       force

   create -k "HKLM\System\CurrentControlSet\Control\Citrix\
       SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately"
         – force

   create -k "HKLM\System\CurrentControlSet\Control\Citrix\
       SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-
       Url>" – force

   create -k "HKLM\System\CurrentControlSet\Control\Citrix\
       SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-
       Certificate-Path-of-PortalAzureCom>" --force
   <!--NeedCopy-->
   ```

   a) En Azure, cree una máquina virtual Linux de una distribución compatible.

   b) Instale un entorno de escritorio en la máquina virtual de Linux si fuera necesario.

   c) En la máquina virtual, instale .NET Runtime 6.0 conforme a las instrucciones de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

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

   e) (Solo para Ubuntu) Apunte `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf`, en lugar de apuntar a `/run/systemd/resolve/stub-resolv.conf`:

   ```
   unlink /etc/resolv.conf

   ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
   <!--NeedCopy-->
   ```

   f) Instale el paquete de Linux VDA.

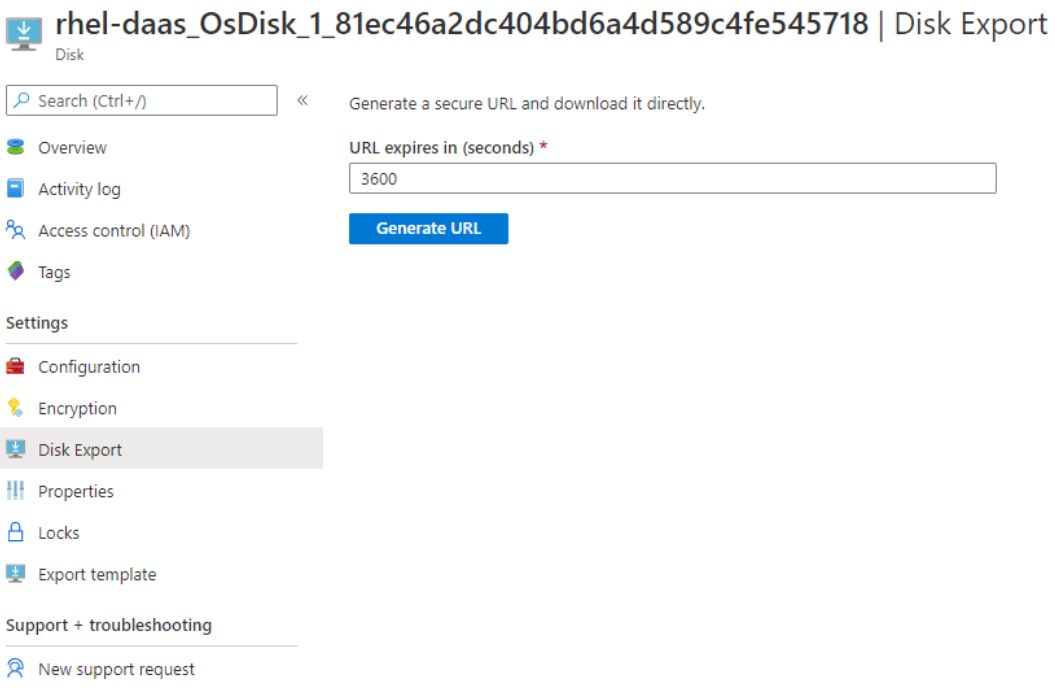
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

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

i) En Azure, detenga (o desasigne) la máquina virtual. Haga clic en **Exportación de disco** para generar una dirección URL SAS para el archivo de disco duro virtual (VHD) que pueda utilizar como imagen maestra para crear otras máquinas virtuales.



j) (Opcional) Configure la directiva de grupo en la imagen maestra. Puede utilizar la herramienta `ctxreg` para configurar la directiva de grupo. Por ejemplo, el comando siguiente habilita la directiva **Crear automáticamente una impresora universal de PDF** para la impresión de PDF.

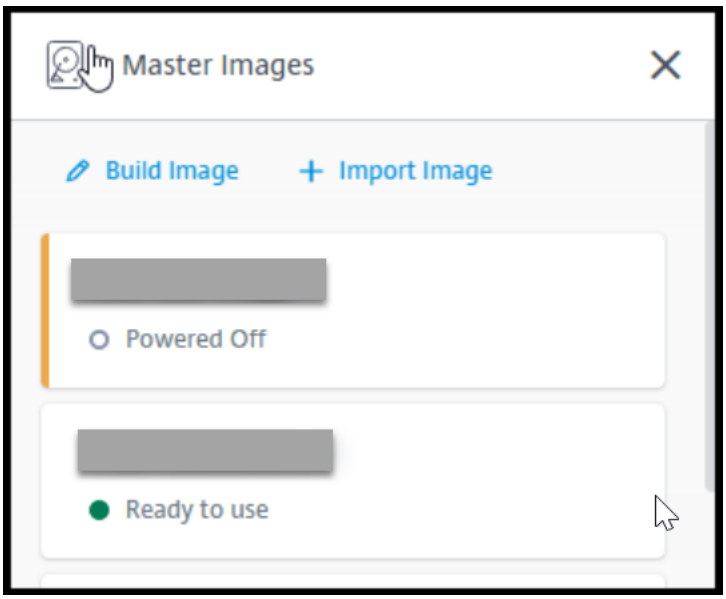
```
1    /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
        GroupPolicy\Defaults\PrintingPolicies" -t "REG_DWORD" -v
         "AutoCreatePDFPrinter" -d "0x00000001" –force
2    <!--NeedCopy-->
```

2. Importe la imagen maestra desde Azure.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

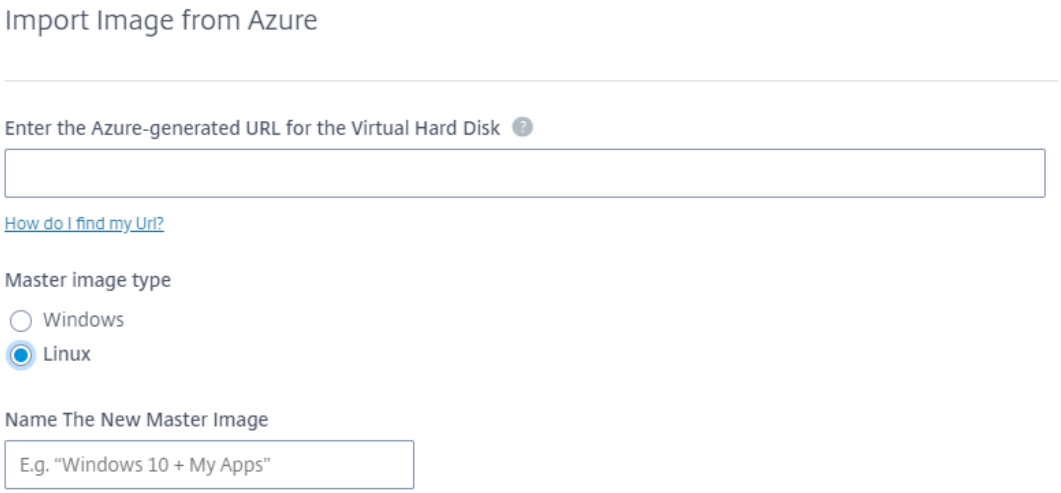
a) En el panel de mandos Administrar, expanda **Imágenes maestras** a la derecha. La pantalla muestra las imágenes maestras que proporciona Citrix y las imágenes que ha creado e importado.

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



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

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



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Cree un catálogo de máquinas.

   Acceda al panel Administrar y haga clic en **Crear catálogo**. Al crear el catálogo de máquinas, elija la imagen maestra que creó anteriormente.

   > **Nota:**
   >
   > No se puede acceder a la VM utilizada como imagen maestra a través de SSH o RDP. Para acceder a la VM, use la consola de serie en Azure Portal.

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

January 9, 2024

Distribuciones compatibles

	Winbind	SSSD	Centrify	PBIS
Debian 10.9	Sí	Sí	No	Sí
RHEL 8.4, RHEL 8.3, RHEL 8.2, RHEL 8.1	Sí	No	Sí	Sí
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí	Sí
SUSE 15.3, SUSE 15.2	Sí	Sí	No	Sí
Ubuntu 20.04, Ubuntu 18.04	Sí	Sí	No	Sí

Hipervisores compatibles

- AWS
- Citrix Hypervisor
- GCP
- Microsoft Azure
- Nutanix AHV
- VMware vSphere

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Usar MCS para crear máquinas virtuales Linux

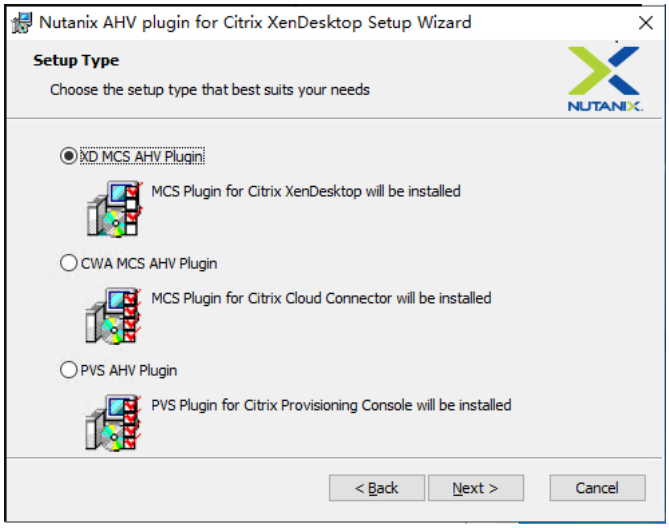
> **Nota:**
>
> Desde Citrix Virtual Apps and Desktops 7 2003 hasta Citrix Virtual Apps and Desktops 7 2112, el alojamiento de Linux VDA en Microsoft Azure, AWS y GCP solo era posible con Citrix DaaS (antes, Virtual Apps and Desktops Service). A partir de la versión 2203, puede alojar Linux VDA en estas nubes públicas tanto con Citrix DaaS como con Citrix Virtual Apps and Desktops. Para agregar las conexiones de host de estas nubes públicas a su implementación de Citrix Virtual Apps and Desktops, necesita una licencia de derechos híbridos. Para obtener información sobre la licencia de derechos híbridos, consulte Transición e intercambios (TTU) con derechos híbridos.
>
> No se permite usar servidores bare metal con MCS para crear máquinas virtuales.
>
> Si utiliza PBIS o Centrify para unir máquinas creadas con MCS a dominios de Windows, complete las siguientes tareas:
>
> - En la máquina de plantilla, configure la ruta de descarga del paquete PBIS o Centrify en el archivo `/etc/xdl/mcs/mcs.conf` o instale el paquete PBIS o Centrify directamente.
> - Antes de ejecutar `/opt/Citrix/VDA/sbin/deploymcs.sh`, cree una unidad organizativa (OU) que tenga permisos de escritura y restablecimiento de contraseña para todas sus máquinas subordinadas creadas por MCS.
> - Antes de reiniciar las máquinas creadas por MCS tras finalizar la ejecución de `/opt/Citrix/VDA/sbin/deploymcs.sh`, ejecute `klist -li 0x3e4 purge` en el Delivery Controller o en Citrix Cloud Connector, según la implementación.

(Solo para Nutanix) Paso 1: Instale y registre el plug-in de Nutanix AHV

Obtenga el paquete del plug-in de Nutanix AHV de Nutanix. Instale y registre el plug-in en el entorno de Citrix Virtual Apps and Desktops. Para obtener más información, consulte la guía de instalación de plug-ins MCS de Nutanix Acropolis, disponible en el portal de asistencia de Nutanix.

Paso 1a: Instale y registre el plug-in de Nutanix AHV para Delivery Controllers locales Después de instalar Citrix Virtual Apps and Desktops, seleccione e instale el **plug-in XD MCS AHV** en sus Delivery Controllers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Paso 1b: Instale y registre el plug-in de Nutanix AHV para Delivery Controllers en la nube Seleccione e instale el **plug-in CWA MCS AHV** en sus Citrix Cloud Connectors. Instale el plug-in en todos los Citrix Cloud Connectors registrados con el arrendatario de Citrix Cloud. Debe registrar los Citrix Cloud Connectors incluso cuando atienden una ubicación de recursos sin AHV.

Paso 1c: Complete los siguientes pasos después de instalar el plug-in

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

  > **Consejo:**
  >
  > Le recomendamos que detenga y reinicie Citrix Host Service, Citrix Broker Service y Machine Creation Service cuando instale o actualice el plug-in de Nutanix AHV.

Paso 2: Cree una conexión de alojamiento

En esta sección se explica cómo crear una conexión de alojamiento con Azure, AWS, GCP, Nutanix AHV y VMware vSphere:

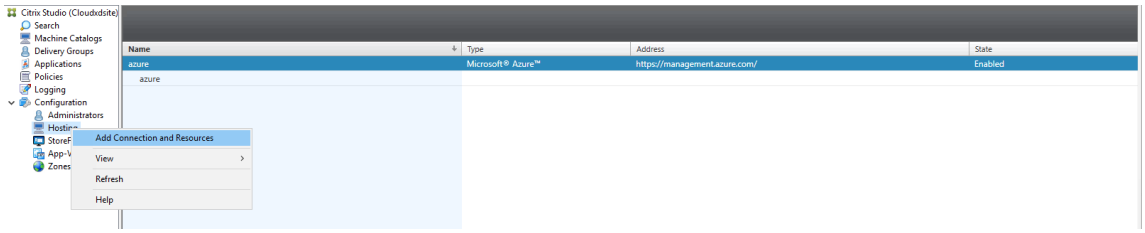
- Crear una conexión de alojamiento con Azure en Citrix Studio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

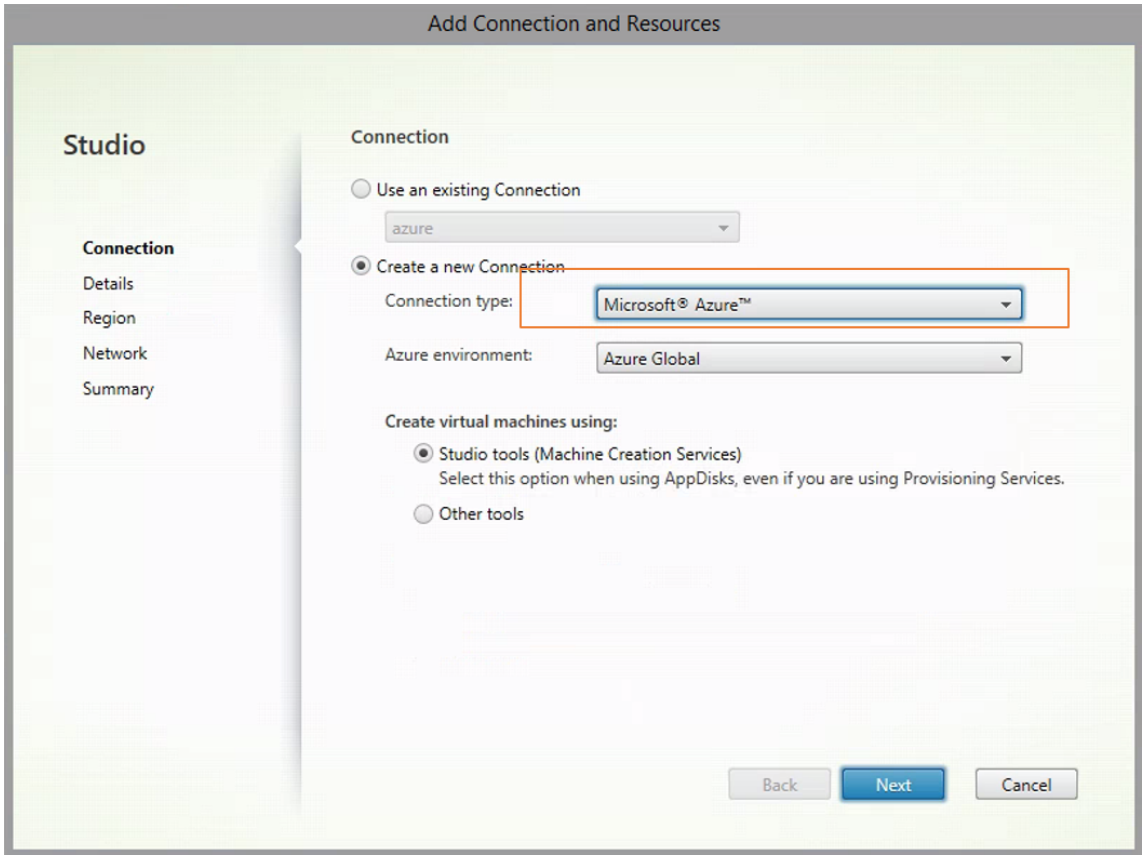
- Crear una conexión de alojamiento con AWS en Citrix Studio
- Crear una conexión de alojamiento con GCP en Citrix Studio
- Crear una conexión de alojamiento con Nutanix en Citrix Studio
- Crear una conexión de alojamiento con VMware en Citrix Studio

Crear una conexión de alojamiento con Azure en Citrix Studio

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

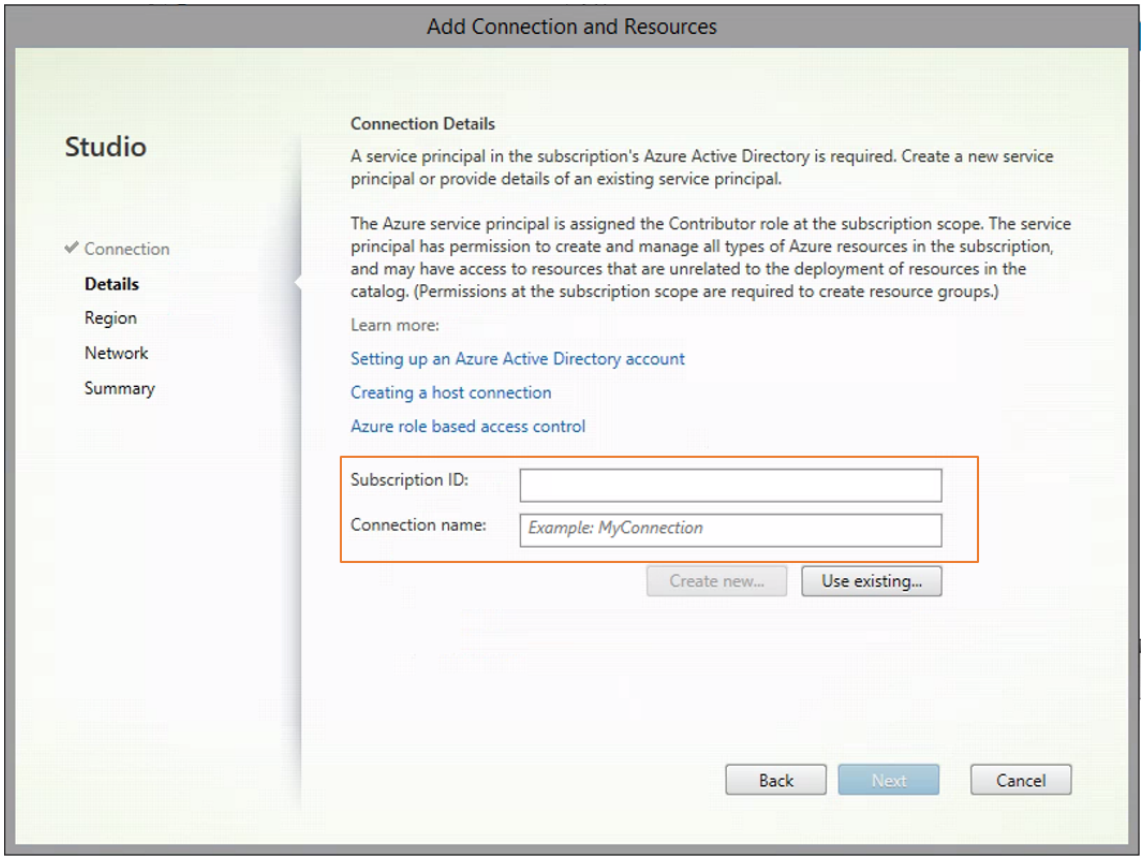


2. Elija Microsoft Azure como el tipo de conexión.

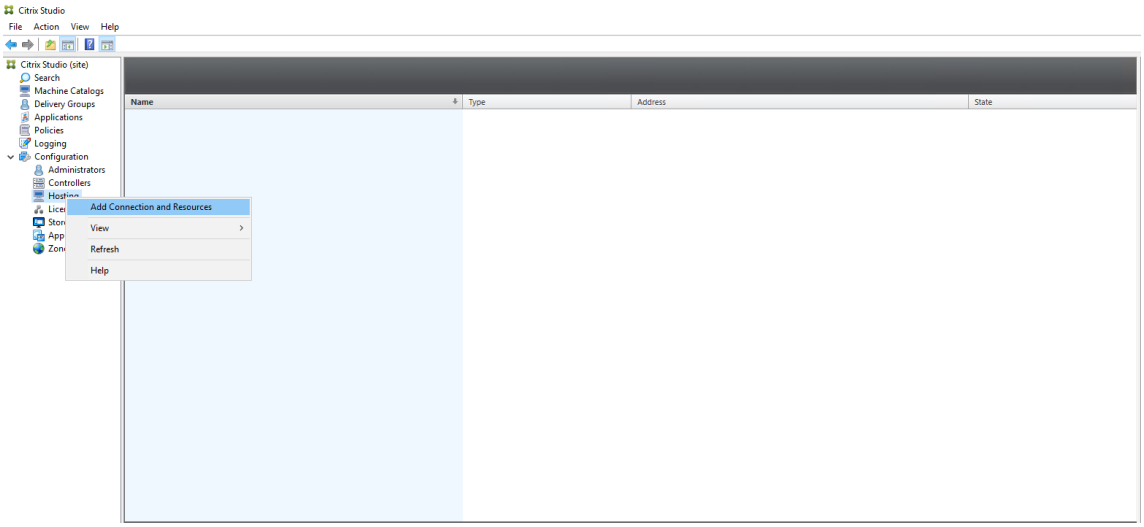


3. Escriba el ID de suscripción de su cuenta de Azure y el nombre de su conexión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



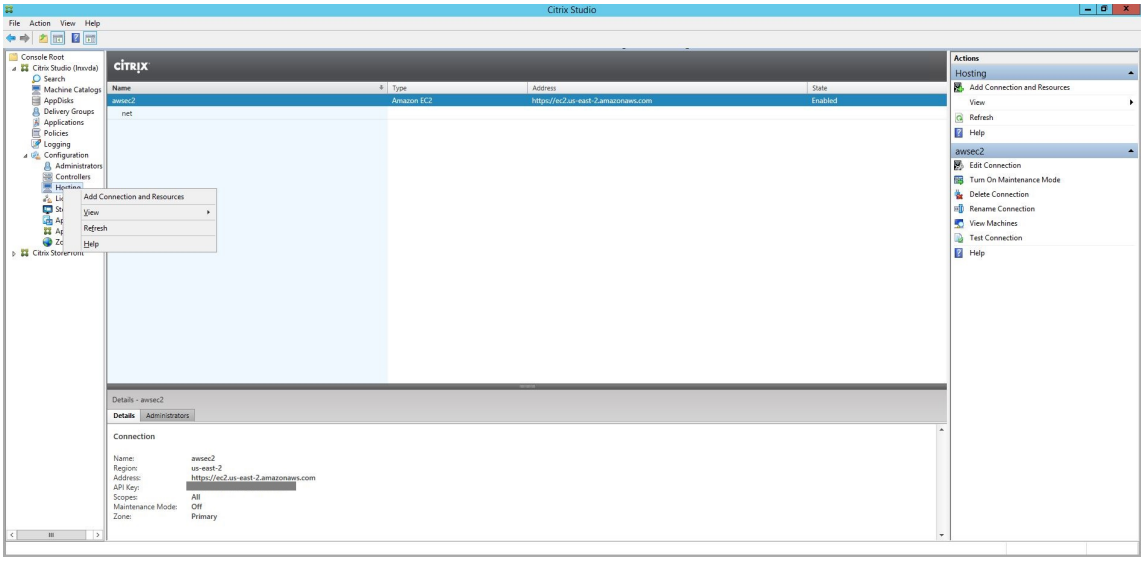
Aparece una nueva conexión en el panel de alojamiento.



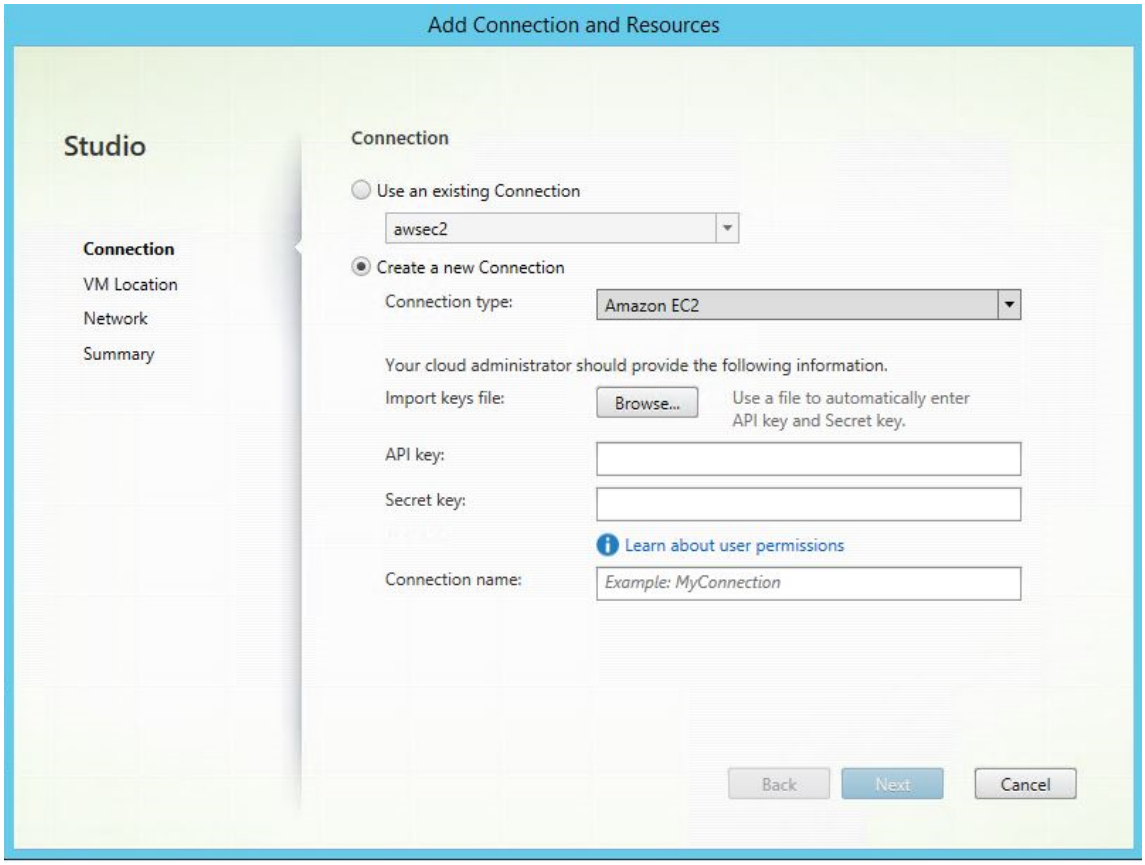
Crear una conexión de alojamiento con AWS en Citrix Studio

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

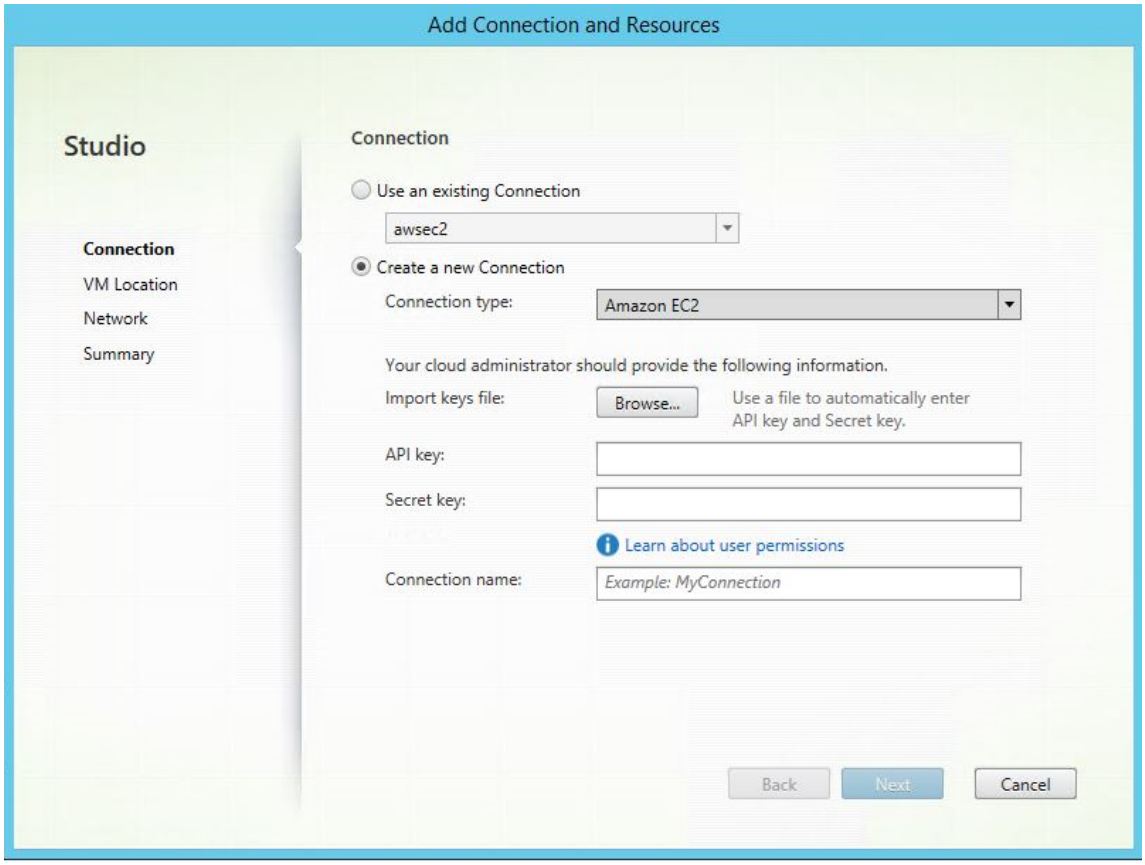


2. Elija **Amazon EC2** como tipo de conexión.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

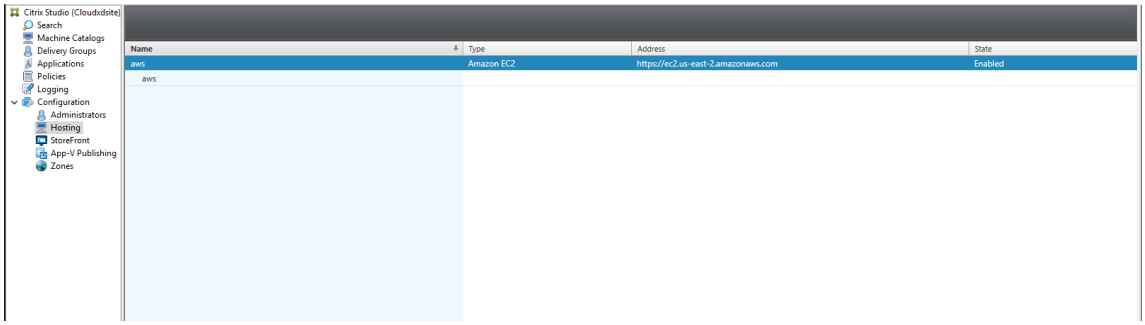


La **clave API** es el ID de la clave de acceso y la **clave secreta** es la clave de acceso secreta. Se las considera un par de claves de acceso. Si pierde su clave de acceso secreta, puede eliminar la clave de acceso y crear otra. Para crear una clave de acceso, haga lo siguiente:

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

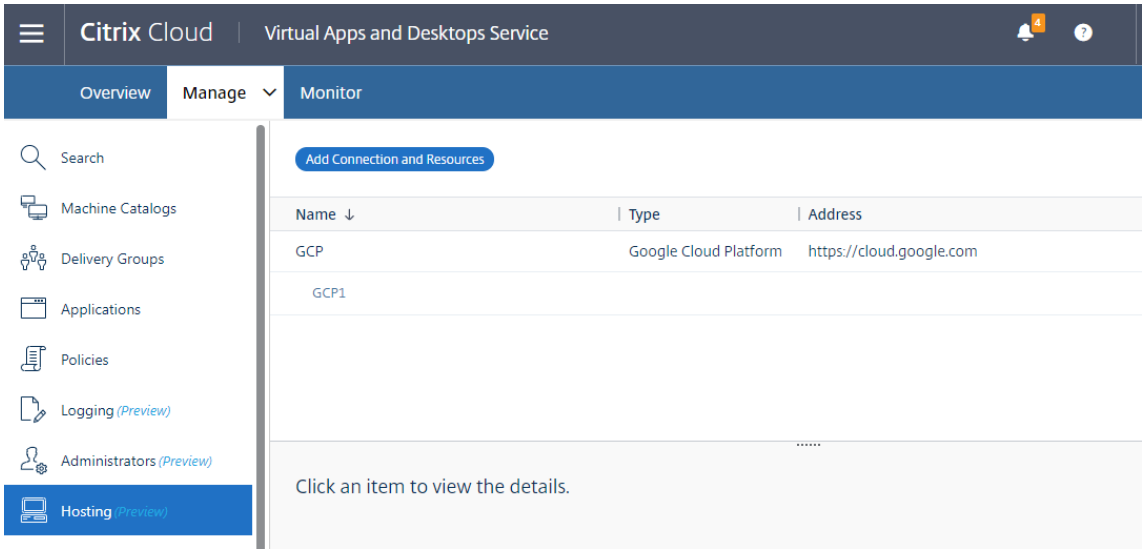
Aparece una nueva conexión en el panel de alojamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



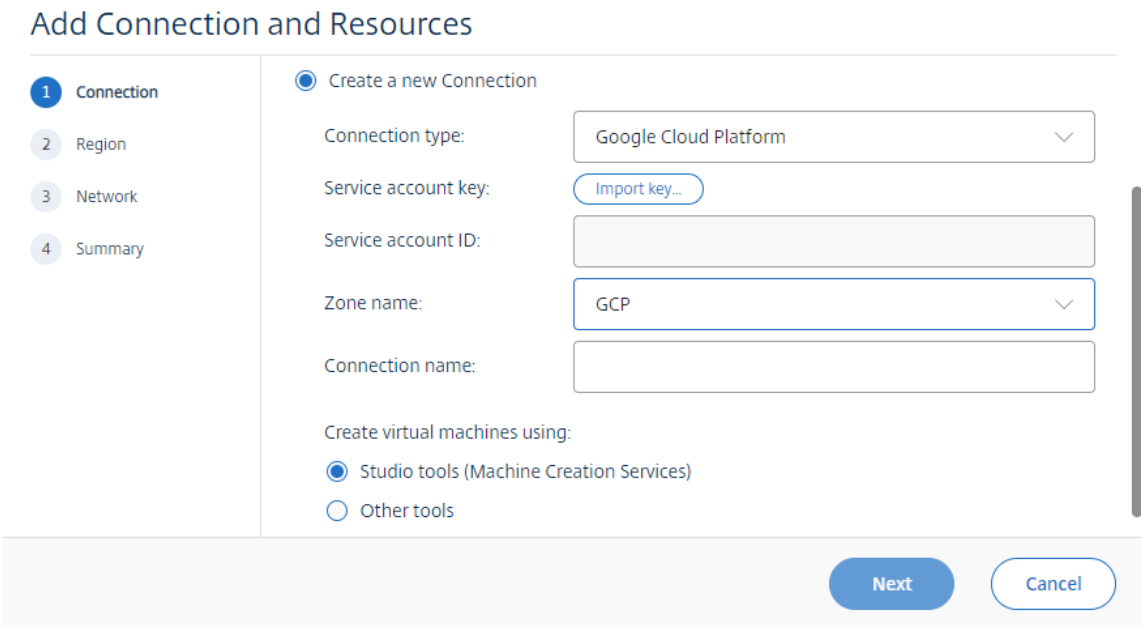
Crear una conexión de alojamiento con GCP en Citrix Studio Configure su entorno de GCP conforme a los entornos de virtualización de Google Cloud Platform y, a continuación, siga estos pasos para crear una conexión de alojamiento con GCP.

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

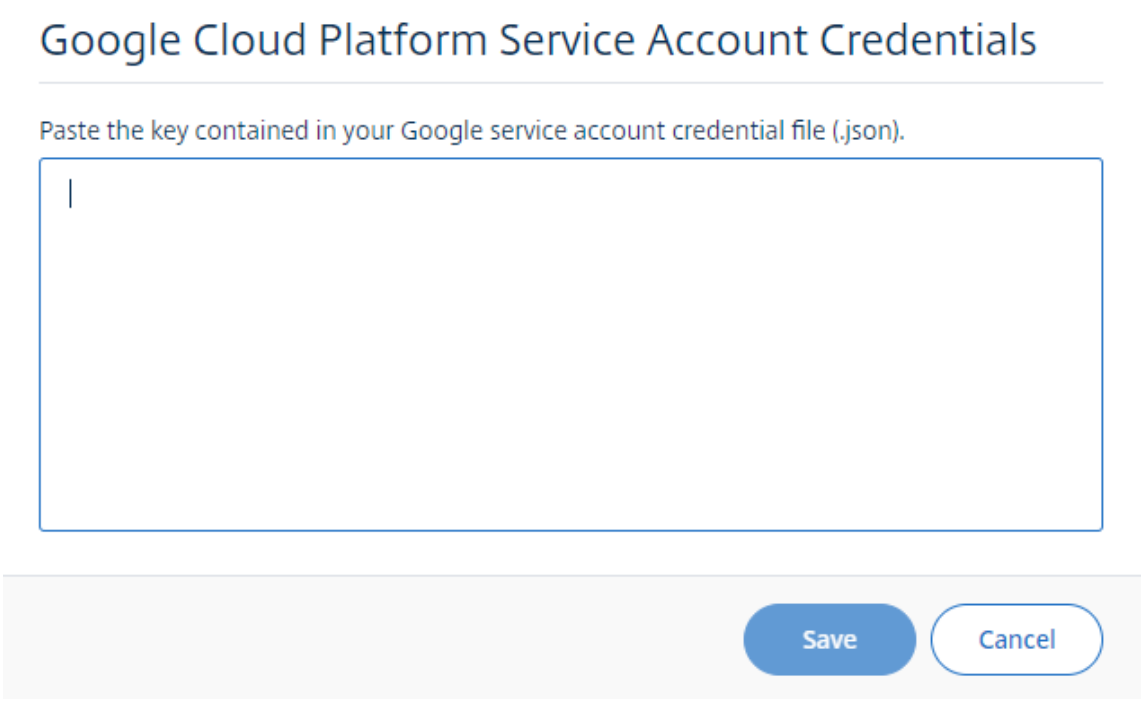


2. Seleccione **Google Cloud Platform** como el tipo de conexión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

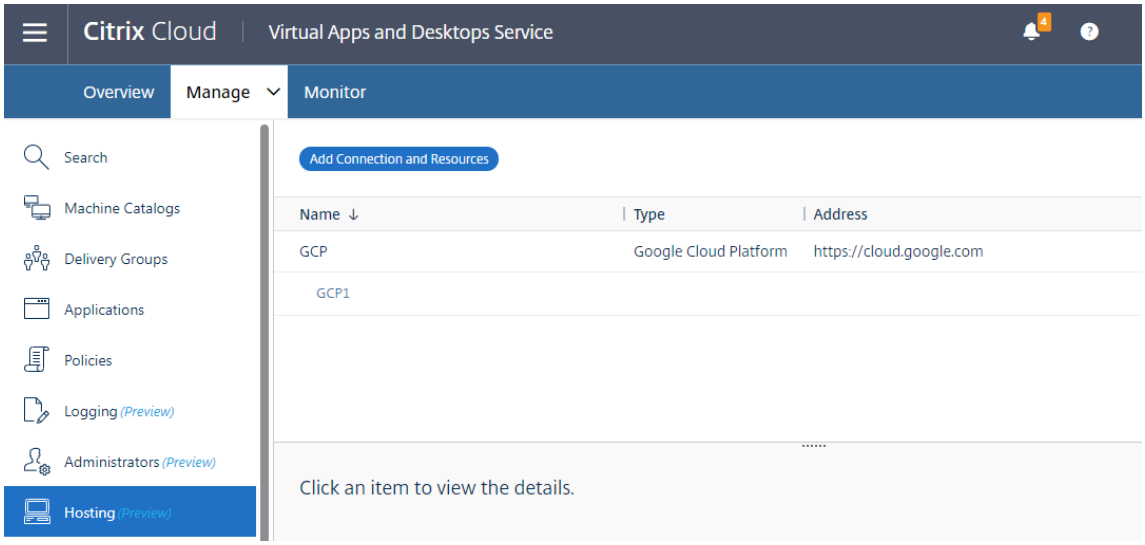


3. Importe la clave de cuenta de servicio de su cuenta de GCP e introduzca el nombre de conexión.



Aparece una nueva conexión en el panel de alojamiento.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

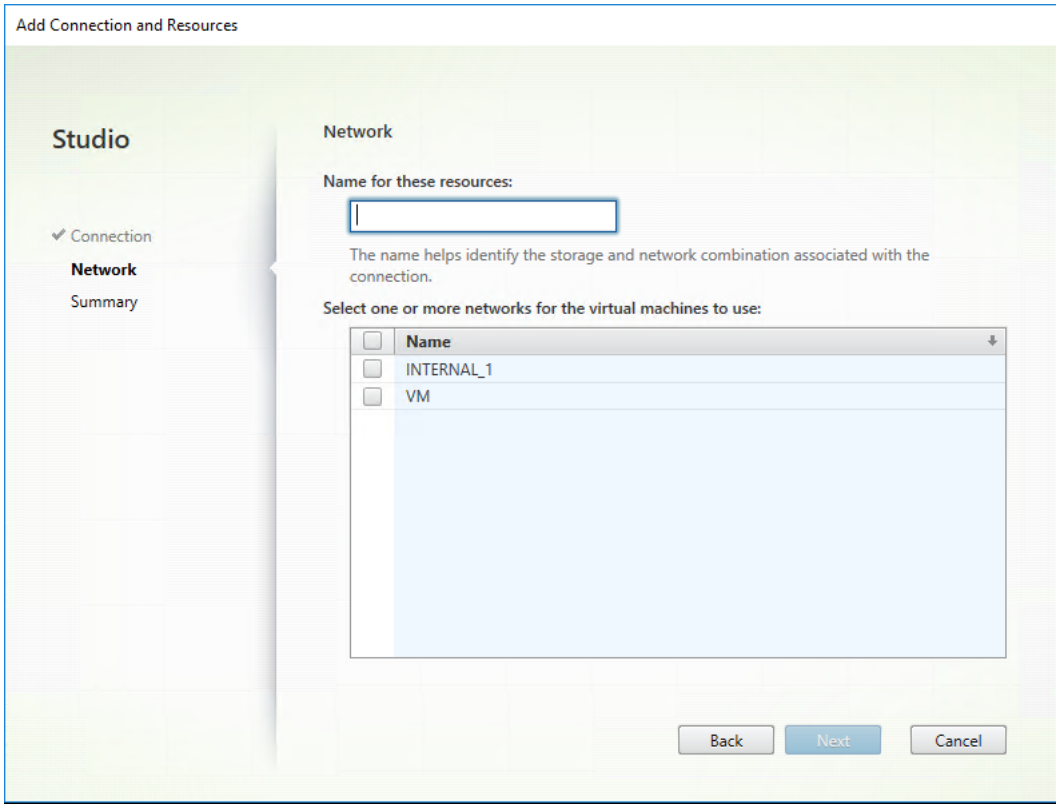


Crear una conexión de alojamiento con Nutanix en Citrix Studio

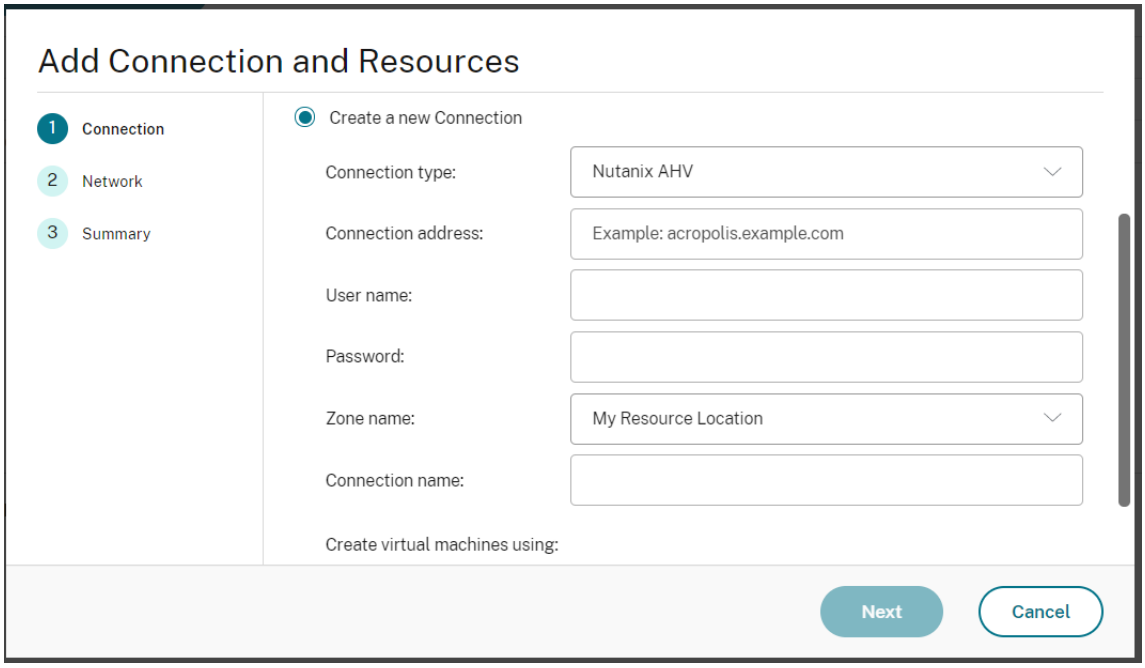
1. Para Delivery Controllers locales, elija **Configuración > Alojamiento > Agregar conexión y recursos** en la instancia de Citrix Studio local. En el caso de Delivery Controllers en la nube, elija **Administrar > Alojamiento > Agregar conexión y recursos** en la consola web de Studio en Citrix Cloud para crear una conexión al hipervisor Nutanix.
2. En el asistente **Agregar conexión y recursos**, seleccione el tipo de conexión Nutanix AHV en la página **Conexión** y luego especifique la dirección y las credenciales del hipervisor, y un nombre para la conexión. En la página **Red**, seleccione una red para la unidad de alojamiento.

   Por ejemplo, en Citrix Studio local:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

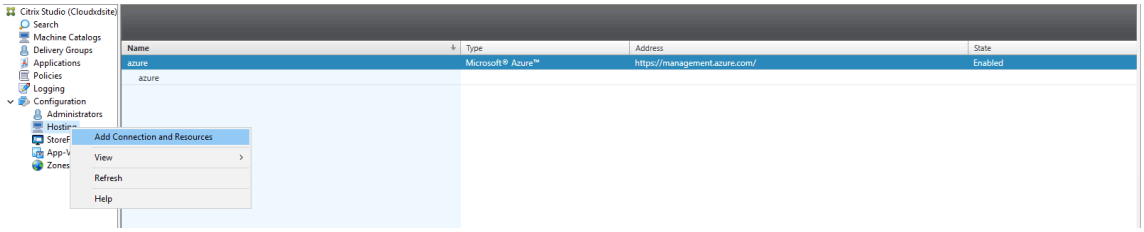


3. En la página **Red**, seleccione una red para la unidad de alojamiento.

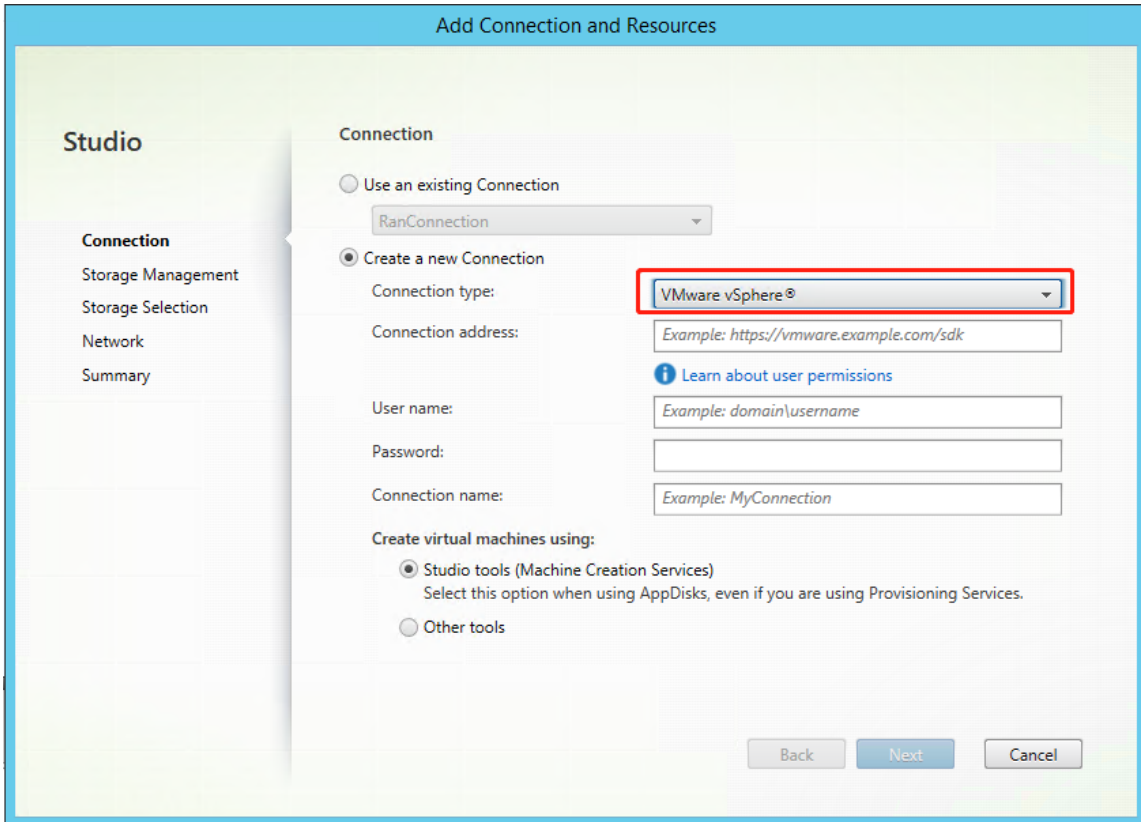
Crear una conexión de alojamiento con VMware en Citrix Studio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

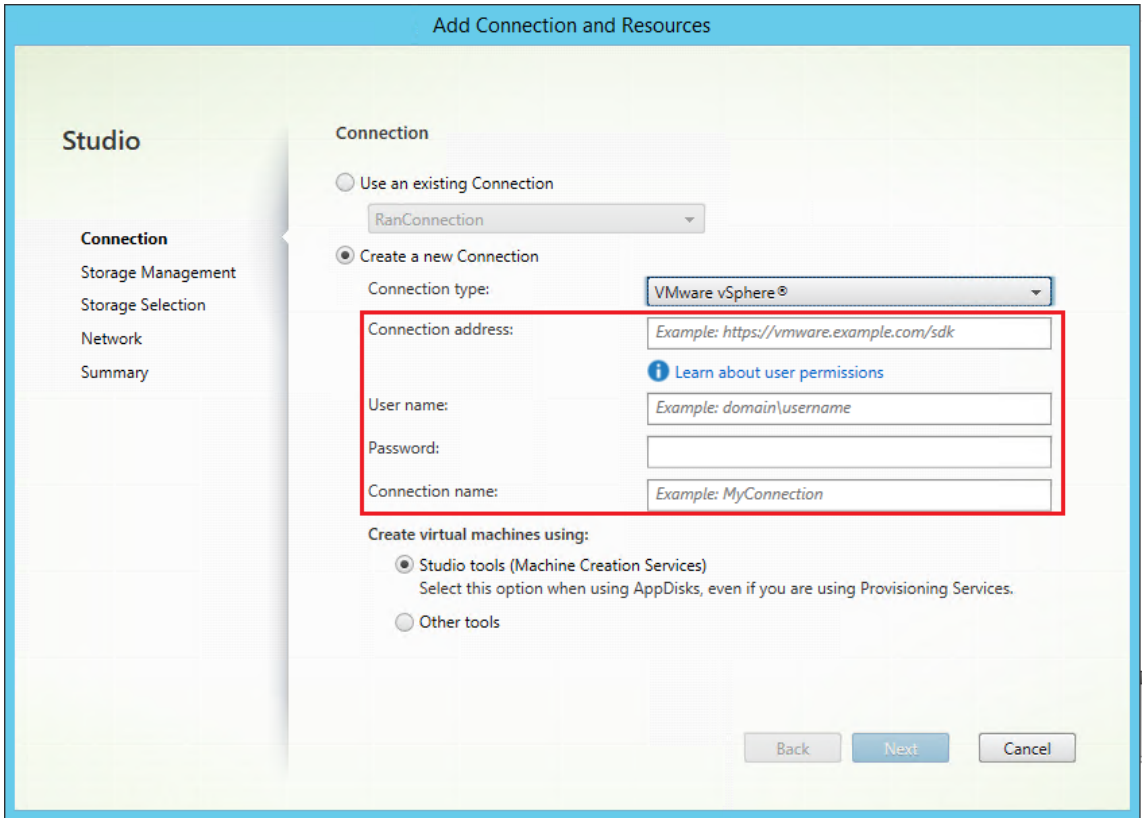


3. Elija VMware vSphere como tipo de conexión.

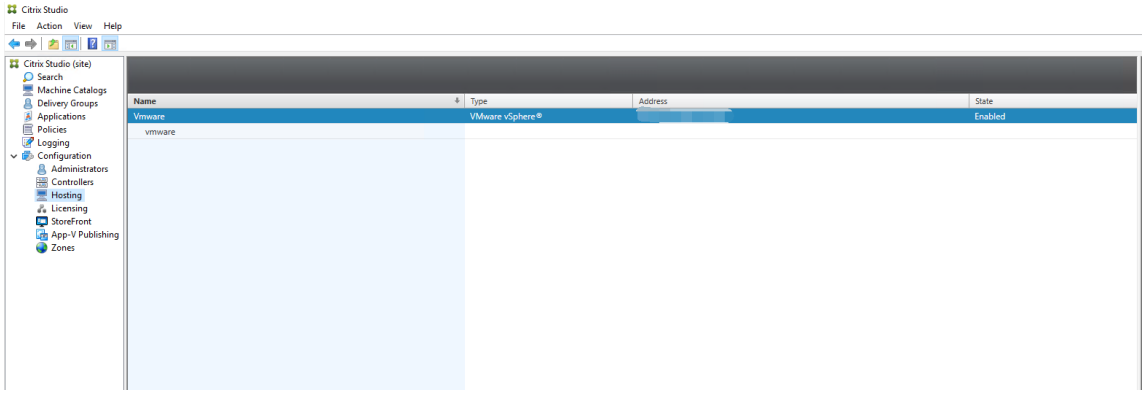


4. Escriba la dirección de conexión (la URL de vCenter Server) de la cuenta de VMware, el nombre de usuario y la contraseña, y el nombre de la conexión.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Aparece una nueva conexión en el panel de alojamiento.



Paso 3: Prepare una imagen maestra

(Solo para Citrix Hypervisor) Paso 3a: Instale Citrix VM Tools Instale Citrix VM Tools en la VM de plantilla para que cada VM use la CLI xe o XenCenter. El rendimiento de la VM puede ser lento, a menos que instale 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`).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

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

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

   Para RHEL/CentOS:

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

   Para Ubuntu/Debian:

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

   Para SUSE:

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

(Para Azure, AWS y GCP) Paso 3b: Configure cloud-init para Ubuntu 18.04

1. Para asegurarse de que el nombre de host de un VDA persiste cuando se reinicia o se detiene una máquina virtual, ejecute este comando:

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

   Compruebe que estas líneas se encuentran en la sección **system_info** del archivo /etc/cloud/-cloud.cfg:

```
system_info:
   network:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        renderers: ['netplan', 'eni', 'sysconfig']
<!--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).

     ```
     users:
     - default
     <!--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:

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

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

Paso 3c: 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 Runtime 6.0.

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

Para RHEL/CentOS:

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

Para Ubuntu/Debian:

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para SUSE:

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

Paso 3d: Habilite repositorios para instalar el paquete tdb-tools **Para el servidor de RHEL 7:**

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

Para la estación de trabajo de RHEL 7:

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

Paso 3e: (en RHEL y CentOS) Instale el repositorio EPEL que puede ofrecer ntfs-3g Instale el repositorio EPEL en RHEL 8, RHEL 7 y CentOS 7 para que la ejecución posterior de `deploymcs.sh` instale el paquete ntfs-3g disponible en el repositorio EPEL. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en https://docs.fedoraproject.org/en-US/epel/.

Paso 3f: (en SUSE) Instale manualmente ntfs-3g En la plataforma SUSE, 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:

   ```
   sudo zypper install gcc
   sudo zypper install make
   <!--NeedCopy-->
   ```

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

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

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

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

5. Instale ntfs-3g:

   ```
   ./configure
   make
   make install
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Paso 3g: Modifique los archivos de configuración de MCS

1. Cambie variables en `/etc/xdl/mcs/mcs.conf`.

   - **Para supuestos sin unión a ningún dominio**

     Para supuestos sin unión a ningún dominio, puede dejar las variables de `/etc/xdl/mcs/mcs.conf` sin especificar o cambiar las siguientes variables si es necesario:

     `DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
     `DESKTOP_ENVIRONMENT`= **gnome | mate **
     `VDA_PORT`=**port-number**
     `REGISTER_SERVICE`=**Y | N**
     `ADD_FIREWALL_RULES`=**Y | N**
     `HDX_3D_PRO`=**Y | N**
     `VDI_MODE`=**Y | N**
     `SITE_NAME`=**dns-site-name | '<none>'**
     `SEARCH_BASE`=**search-base-set | '<none>'**
     `START_SERVICE`=**Y | N**
     `TELEMETRY_SOCKET_PORT`=**port-number**
     `TELEMETRY_PORT`=**port-number**

     > **Sugerencia:**
     >
     > La variable `AD_INTEGRATION` de `/etc/xdl/mcs/mcs.conf` está establecida en `Winbind` de forma predeterminada. El valor predeterminado no afecta a los supuestos sin unión a ningún dominio.

   - **Para supuestos con unión a un dominio**

     Cambie variables en `/etc/xdl/mcs/mcs.conf`. El archivo de configuración `mcs.conf` ofrece variables para configurar MCS y Linux VDA. A continuación, dispone de las variables que puede configurar según sea necesario:

     - `Use_Existing_Configurations_Of_Current_VDA`: Determina si se deben usar los archivos de configuración existentes relacionados con AD (/etc/krb5.conf, /etc/sssd.conf y /etc/samba/smb.conf) del VDA que se está ejecutando 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 las plantillas de configuración de la imagen maestra determinan los archivos de configuración de las máquinas creadas por MCS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `dns`: Establece la dirección IP de cada servidor DNS. Puede configurar hasta cuatro servidores DNS.
- `NTP_SERVER`: Establece la dirección IP de su servidor NTP. A menos que se especifique lo contrario, es la dirección IP de su controlador de dominio.
- `WORKGROUP`: establece el nombre del grupo de trabajo en el nombre NetBIOS (distingue mayúsculas y minúsculas) que configuró en AD. De lo contrario, MCS utiliza la parte del nombre de dominio que sigue inmediatamente al nombre de host de la máquina como nombre del grupo de trabajo. Por ejemplo, si la cuenta de máquina es **user1.lvda.citrix.com**, MCS usa **lvda** como nombre del grupo de trabajo, mientras que **citrix** es la opción correcta. Asegúrese de configurar correctamente el nombre del grupo de trabajo.
- `AD_INTEGRATION`: Establece Winbind, SSSD, PBIS o Centrify. Para obtener una tabla de las distribuciones de Linux y los métodos de unión de dominios que admite MSC, consulte Distribuciones compatibles en este artículo.
- `CENTRIFY_DOWNLOAD_PATH`: Establece la ruta de descarga del paquete Server Suite Free (anteriormente, Centrify Express). El valor surte efecto solo cuando la variable `AD_INTEGRATION` se establece en Centrify.
- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Establece la ruta de descarga del paquete Centrify Samba. El valor surte efecto solo cuando la variable `AD_INTEGRATION` se establece en Centrify.
- `PBIS_DOWNLOAD_PATH`: Establece la ruta para descargar el paquete PBIS. El valor surte efecto solo cuando la variable `AD_INTEGRATION` se establece en PBIS.
- `UPDATE_MACHINE_PW`: Habilita o inhabilita la automatización de las actualizaciones de contraseñas de cuentas de máquina. Para obtener más información, consulte Automatizar la actualización de las contraseñas de cuentas de máquina.
- Estas variables de configuración de Linux VDA:

  `DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
  `DESKTOP_ENVIRONMENT`= **gnome | mate **
  `SUPPORT_DDC_AS_CNAME`=**Y | N**
  `VDA_PORT`=**port-number**
  `REGISTER_SERVICE`=**Y | N**
  `ADD_FIREWALL_RULES`=**Y | N**
  `HDX_3D_PRO`=**Y | N**
  `VDI_MODE`=**Y | N**
  `SITE_NAME`=**dns-site-name | '<none>'**
  `LDAP_LIST`='**list-ldap-servers**'| '**<none>**'

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SEARCH_BASE=**search-base-set | '<none>'**
FAS_LIST=**'list-fas-servers'| '<none>'**
START_SERVICE=**Y | N**
TELEMETRY_SOCKET_PORT=**port-number**
TELEMETRY_PORT=**port-number**

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
#!/bin/bash

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


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

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

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

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

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

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


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


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


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

#########################Linux VDA Configuration################################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
SUPPORT_DDC_AS_CNAME=N
VDA_PORT=80
REGISTER_SERVICE=Y
ADD_FIREWALL_RULES=Y
HDX_3D_PRO=N
VDI_MODE=Y
SITE_NAME='<none>'
LDAP_LIST="dc1.example.com"
SEARCH_BASE="DC=example,DC=com"
FAS_LIST='<none>'
START_SERVICE=Y
TELEMETRY_SOCKET_PORT=7503
TELEMETRY_PORT=7502
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Ejecute /opt/Citrix/VDA/sbin/deploymcs.sh.
3. 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:

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

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

Paso 3h: Cree una imagen maestra

1. Ejecute /opt/Citrix/VDA/sbin/deploymcs.sh.
2. (si utiliza un VDA que se está ejecutando como máquina virtual de plantilla, omita este paso). 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/sssd/sssd.conf relevantes 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/sssd.conf.tmpl, /etc/xdl/mcs/sssd_krb5.conf.tmpl y /etc/xdl/mcs/sssd_smb.conf.tmpl.

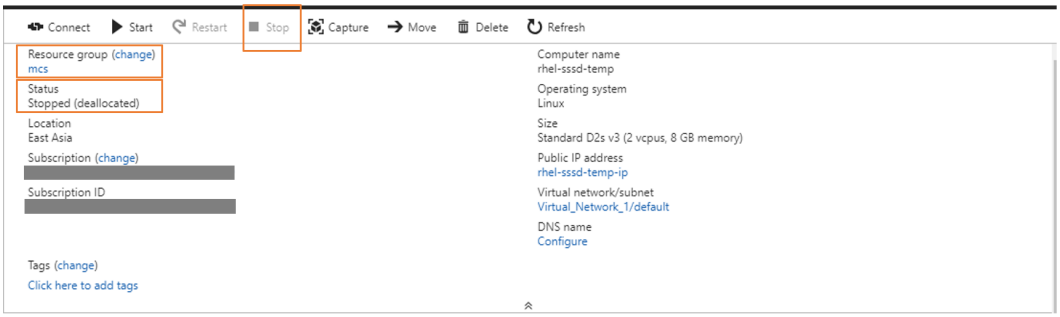
   Para los usuarios de Centrify, actualice las plantillas /etc/xdl/mcs/centrify_krb5.conf.tmpl y /etc/xdl/mcs/centrify_smb.conf.tmpl.

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

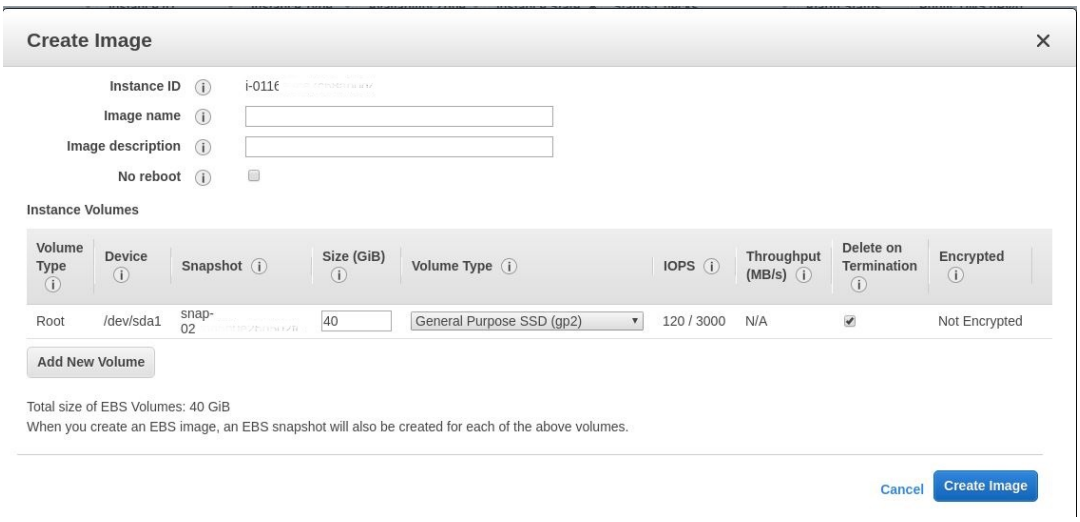
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Cree y asigne un nombre a una instantánea de su imagen maestra en función de la nube pública que utilice.

   - **(Para Citrix Hypervisor, GCP y VMware vSphere)** Instale aplicaciones en la máquina virtual de plantilla y apague la máquina virtual de plantilla. Cree y nombre la instantánea de su imagen maestra.
   - **(Para Azure)** 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.



   - **(Para AWS)** 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**. 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**.



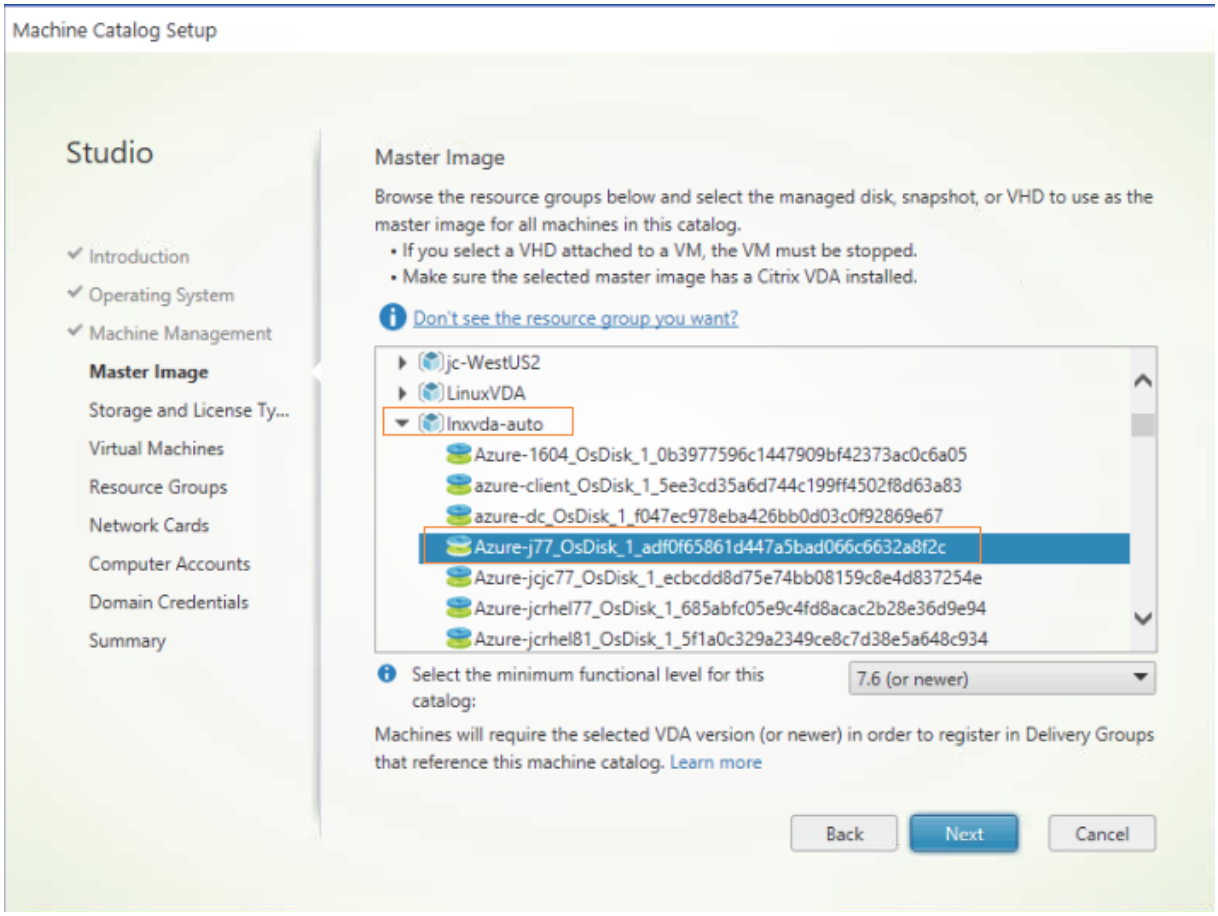
   - **(Para Nutanix)** En Nutanix AHV, apague la máquina virtual de plantilla. Cree y nombre la instantánea de su imagen maestra.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

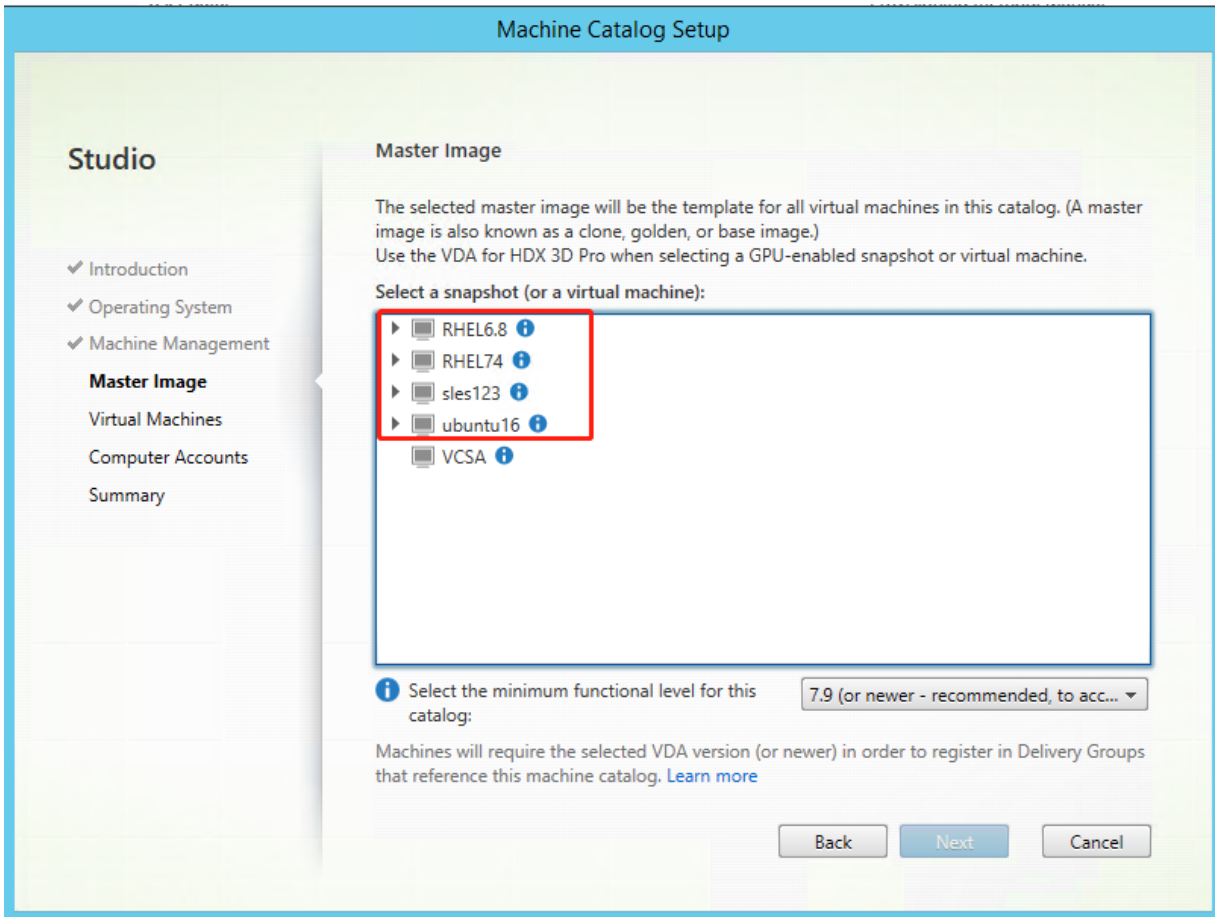
> **Nota:**
>
> Los nombres de instantánea de Acropolis deben incluir el prefijo `XD_` para poder utilizarse en Citrix Virtual Apps and Desktops. Utilice la consola de Acropolis para cambiar el nombre de las instantáneas, si es necesario. Después de cambiar el nombre de una instantánea, reinicie el asistente **Crear catálogo** para obtener una lista actualizada.

Paso 4: 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. A continuación, se muestran algunos ejemplos:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



En la página **Contenedor** exclusiva de Nutanix, seleccione el contenedor que especificó anteriormente para la VM de plantilla. En la página **Imagen maestra**, seleccione la instantánea de la imagen. En la página **Máquinas virtuales**, compruebe la cantidad de unidades CPU virtuales y la cantidad de núcleos por cada CPU virtual.

> **Nota:**
>
> Si el proceso de creación del catálogo de máquinas en el Delivery Controller lleva mucho tiempo, vaya a Nutanix Prism y encienda manualmente la máquina con el prefijo **Preparation**. Este enfoque ayuda a continuar el proceso de creación.

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

Paso 5: 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Usar MCS para actualizar Linux VDA

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

1. Asegúrese de instalar .NET Runtime 6.0 antes de actualizar Linux VDA a la versión Current Release.
2. Actualice su Linux VDA en la plantilla de máquina:

> **Nota:**
>
> También puede utilizar la función Autoactualización de Linux VDA para programar actualizaciones automáticas de software. Para hacer esto, agregue líneas de comandos al archivo etc/xdl/mcs/mcs_local_setting.reg de la máquina de plantilla.
> Por ejemplo, puede agregar las siguientes líneas de comandos:

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" –
    force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately"
     – force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-
    Url>" – force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-
    Certificate-Path-of-PortalAzureCom>" --force
<!--NeedCopy-->
```

Para RHEL 7 y CentOS 7:

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

Para RHEL 8:

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

Para SUSE:

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

Para Ubuntu 18.04:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Para Ubuntu 20.04:

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

3. Modifique /etc/xdl/mcs/mcs.conf y /etc/xdl/mcs/mcs_local_setting.reg.
4. Tome una nueva instantánea.
5. En Citrix Studio, seleccione la nueva instantánea para actualizar su catálogo de máquinas. Espere a que se reinicie cada máquina. No reinicie ninguna máquina manualmente.

Automatizar la actualización de las contraseñas de cuenta de máquina

Las contraseñas de cuenta de máquina caducan, de forma predeterminada, al cabo de 30 días de la creación del catálogo de máquinas. Para evitar que las contraseñas caduquen y automatizar la actualización de las contraseñas de cuenta de máquina, haga lo siguiente:

1. Agregue la siguiente entrada a /etc/xdl/mcs/mcs.conf antes de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh.

   ```
   UPDATE_MACHINE_PW="enabled"
   ```

2. Después de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh., abra /etc/cron.d/mcs_update_password_cronjob para establecer la hora y la frecuencia de actualización. En la configuración predeterminada, las contraseñas de las cuentas de máquina se actualizan semanalmente a las 2:30 a. m. del domingo.

Después de actualizar cada contraseña de cuenta de máquina, la caché de tíquets del Delivery Controller deja de ser válida y puede aparecer el siguiente error en /var/log/xdl/jproxy.log:

```
[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred.
 Error: Failure unspecified at GSS-API level (Mechanism level:
Checksum failed)
```

Para eliminar el error, borre la caché de tíquets periódicamente. Puede programar una tarea de limpieza de caché en todos los Delivery Controllers o en el controlador de dominio.

Habilitar FAS en máquinas virtuales creadas por MCS

Puede habilitar Servicio de autenticación federada en máquinas virtuales creadas con MCS que se ejecuten en las distribuciones siguientes:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Winbind	SSSD	Centrify	PBIS
RHEL 8	Sí	No	No	Sí
RHEL 7, CentOS 7	Sí	Sí	No	Sí
Ubuntu 20.04	Sí	No	No	No
Ubuntu 18.04	Sí	No	No	No
Debian 10.9	Sí	No	No	No
SUSE 15.3	Sí	No	No	No
SUSE 15.2	Sí	No	No	No

Habilitar FAS al preparar una imagen maestra en la máquina virtual de plantilla

1. Importe el certificado raíz de la CA.

```
sudo cp root.pem /etc/pki/CA/certs/
<!--NeedCopy-->
```

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

> **Nota:**
>
> Establezca todas las variables necesarias en `/etc/xdl/mcs/mcs.conf`, puesto que se invocan al iniciarse la máquina virtual.

   a) Establezca el valor de `Use_Existing_Configurations_Of_Current_VDA` en Y.
   b) Establezca la variable `FAS_LIST` en la dirección del servidor de FAS o en varias direcciones de servidor de FAS. Separe las direcciones con puntos y comas, y acótelas con comillas simples. Por ejemplo, `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`.
   c) Establezca las otras variables según sea necesario, como `VDI_MODE`.

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

Habilitar FAS en una máquina virtual creada por MCS

Si FAS no se habilitó en la máquina de la plantilla como se describió anteriormente, puede habilitar FAS en cada máquina virtual creada por MCS.

Para habilitar FAS en una máquina virtual creada por MCS, haga lo siguiente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Configure variables en /etc/xdl/mcs/mcs.conf.

   > **Nota:**
   >
   > Establezca todas las variables necesarias en `/etc/xdl/mcs/mcs.conf`, puesto que se invocan al iniciarse la máquina virtual.

   a) Establezca el valor de `Use_Existing_Configurations_Of_Current_VDA` en Y.
   b) Establezca la variable `FAS_LIST` en la dirección del servidor FAS.
   c) Establezca las otras variables según sea necesario, como `VDI_MODE`.

2. Importe el certificado raíz de la CA.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   <!--NeedCopy-->
   ```

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

Usar Citrix Provisioning para crear máquinas virtuales Linux

September 5, 2022

En este artículo se proporciona información sobre los dispositivos de destino para el streaming de Linux. Con esta funcionalidad, puede aprovisionar escritorios virtuales Linux directamente en el entorno de Citrix Virtual Apps and Desktops.

Se admiten las siguientes distribuciones de Linux:

- Ubuntu 18.04
- Ubuntu 20.04
- RHEL 8.4
- RHEL 8.3
- RHEL 7.9
- SUSE 15.2
- SUSE 15.3

> **Importante:**
>
> - Le recomendamos usar el paquete de instalación de la versión Current Release, disponible en el ejecutable de Citrix Provisioning, `Citrix_Provisioning_2203.iso`. Utilice el paquete basado en su distribución Linux. Se requiere Citrix Provisioning Server 2109 o una versión posterior para utilizar la versión 2109 del agente de streaming de Linux y versiones posteriores.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - Al usar Citrix Provisioning para distribuir dispositivos de destino Linux por streaming, cree una partición de arranque independiente en la única imagen de disco compartido para que los dispositivos aprovisionados puedan arrancar según lo previsto.
> - No dé formato a las particiones con `btrfs`. GRUB2 tiene un problema intrínseco para encontrar particiones btrfs. GRUB es un cargador de arranque múltiple cuyas siglas corresponden a GRand Unified Bootloader.

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

Configurar Delivery Controllers para XenDesktop 7.6 y versiones anteriores

July 6, 2022

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

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**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
.\Update-BrokerServiceConfig.ps1
<!--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:
>
> ```
> Set-ExecutionPolicy Unrestricted
> <!--NeedCopy-->
> ```

El script **Update-BrokerServiceConfig.ps1** actualiza el archivo de configuración del servicio de broker con nuevos puntos finales WCF que necesita Linux VDA y después reinicia el servicio del broker. El script determina automáticamente la ubicación del archivo de configuración del servicio del broker. Se crea una copia de seguridad del archivo de configuración original en el mismo directorio con la extensión **.prelinux**.

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

Comprobación de la configuración del Delivery Controller

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

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

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

Parámetros de servidor LDAP y de directivas

September 5, 2022

Configuración de directivas en Citrix Studio

Para configurar directivas en Citrix Studio, lleve a cabo lo siguiente:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

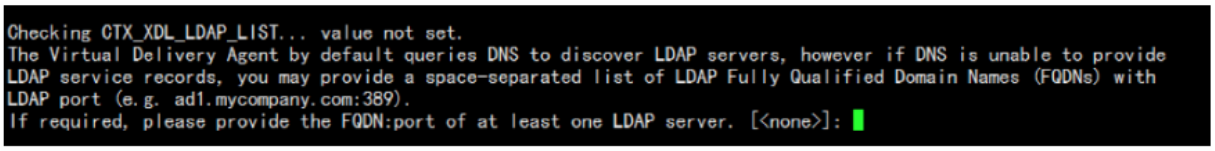
Configuración del servidor LDAP en el VDA

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. La configuración es necesaria para que el servicio de directiva realice una búsqueda LDAP en esos entornos.

Después de instalar el paquete de Linux VDA, ejecute el comando:

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

Escriba todos los servidores LDAP en este formato: lista de nombres de dominio completos (FQDN) de LDAP, separados por espacios, con el puerto de LDAP (p. ej.: ad1.miempresa.com:389 ad2.miempresa.com:389).



También puede ejecutar el comando **ctxreg** para escribir este parámetro directamente en el Registro:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -t "REG_SZ" -v "ListOfLDAPServers" -d "ad1.
   mycompany.com:389 ad2.mycomany.com:389" --force
<!--NeedCopy-->
```

Configuración

July 6, 2022

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Administración

July 6, 2022

Esta sección contiene estos temas:

- CEIP
- HDX Insight
- Integración en Citrix Telemetry Service
- Actualización automática de Linux VDA para Citrix DaaS Standard para Azure
- Métricas de sesión de Linux y Linux VM
- Recopilación de registros
- Remedo de sesiones
- El demonio del servicio de supervisión
- Herramientas y utilidades
- Otros
  - Compatibilidad con la aplicación Citrix Workspace para HTML5
  - Crear un entorno virtual Python3
  - Integrar NIS en Active Directory
  - IPv6
  - LDAPS
  - **Xauthority**

Customer Experience Improvement Program (CEIP) de Citrix

July 6, 2022

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. De forma predeterminada, la disponibilidad general está inhabilitada.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 = 1):

Ubicación: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nombre: **GASwitch**

Valor: 1 = inhabilitado, 0 = habilitado

Si no se especifica, significa que GA está inhabilitado.

Puede ejecutar el siguiente comando en un cliente para habilitar el programa GA:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "GASwitch" -d "0"
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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\CEIP" -v "DataPersistPath" -d "your_path"
<!--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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Punto de datos	Nombre de la clave	Descripción
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 `ctxhdx` y `ctxvda`, 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
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Punto de datos	Nombre de la clave	Descripción
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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX Insight

July 6, 2022

Información general

Linux VDA admite parcialmente la función HDX Insight.

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. Todos los datos de HDX Insight se obtienen del canal virtual NSAP y se envían sin comprimir. De forma predeterminada, el canal virtual NSAP está habilitado.

Los siguientes comandos inhabilitan y habilitan el canal virtual NSAP, respectivamente:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"
     --force
2 <!--NeedCopy-->
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
     --force
2 <!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

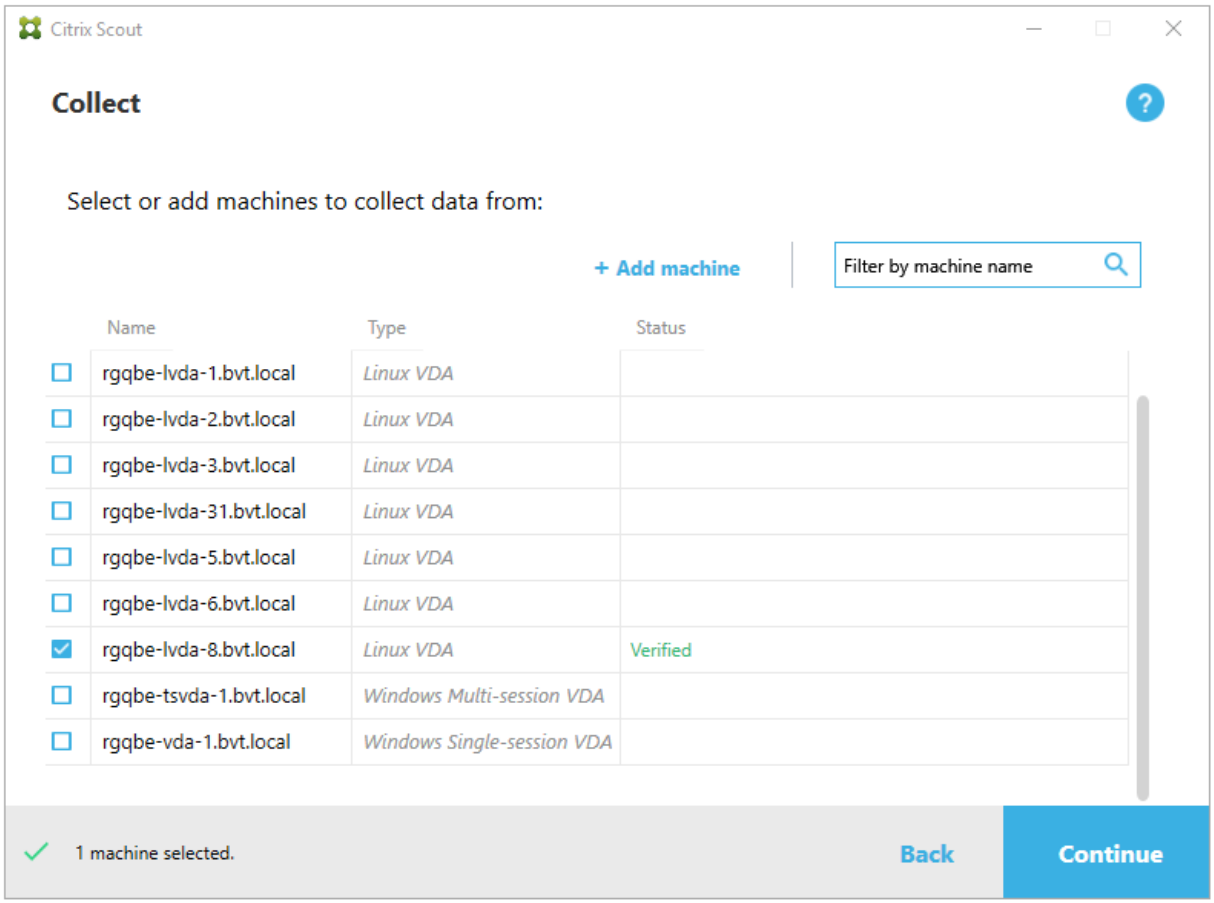
No se muestran puntos de datos de aplicaciones

Verifique que el canal virtual integrado esté habilitado y haya una aplicación integrada activa.

Integración en Citrix Telemetry Service

July 6, 2022

Con Citrix Telemetry Service (`ctxtelemetry`) integrado con el software Linux VDA, puede ejecutar Citrix Scout, que, a su vez, utiliza el script /opt/Citrix/VDA/bin/xdlcollect.sh para recopilar registros sobre Linux VDA.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Después de actualizar desde Linux VDA 1912 y versiones anteriores, debe volver a ejecutar /opt/Citrix/VDA/sbin/ctxsetup.sh para configurar las variables de Citrix Telemetry Service (`ctxtelemetry`). Para obtener más información acerca de las variables, consulte Easy Install.

Habilitar e inhabilitar Citrix Telemetry Service

- Para habilitar el servicio, ejecute el comando **sudo systemctl enable ctxtelemetry.socket**.
- Para inhabilitar el servicio, ejecute **sudo systemctl disable ctxtelemetry.socket**.

Ports

De forma predeterminada, Citrix Telemetry Service (`ctxtelemetry`) utiliza el puerto TCP/IP 7503 para escuchar a Citrix Scout. Para comunicarse con Citrix Scout, utiliza el puerto TCP/IP 7502 en el Delivery Controller.

Puede utilizar los puertos predeterminados o cambiarlos mediante las siguientes variables al instalar Linux VDA.

- **CTX_XDL_TELEMETRY_SOCKET_PORT**: El puerto de socket para escuchar a Citrix Scout. El puerto predeterminado es 7503.
- **CTX_XDL_TELEMETRY_PORT**: El puerto para comunicarse con Citrix Scout. El puerto predeterminado es 7502.

Para cambiar los puertos una vez instalado el VDA, haga lo siguiente:

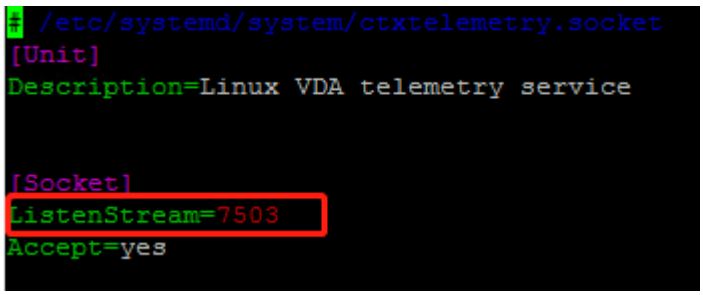
1. Para cambiar un puerto para comunicarse con Scout, ejecute el siguiente comando.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
      -t REG_DWORD
2 <!--NeedCopy-->
```

2. Para cambiar el puerto de socket para escuchar a Scout, ejecute el siguiente comando para abrir y modificar el archivo ctxtelemetry.socket.

```
1 sudo vi /etc/systemd/system/ctxtelemetry.socket
2 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Ejecute los siguientes comandos para reiniciar el puerto de socket.

```
sudo systemctl daemon-reload
sudo systemctl stop ctxtelemetry.socket
sudo systemctl start ctxtelemetry.socket
<!--NeedCopy-->
```

4. Habilite los nuevos puertos en la configuración del firewall.

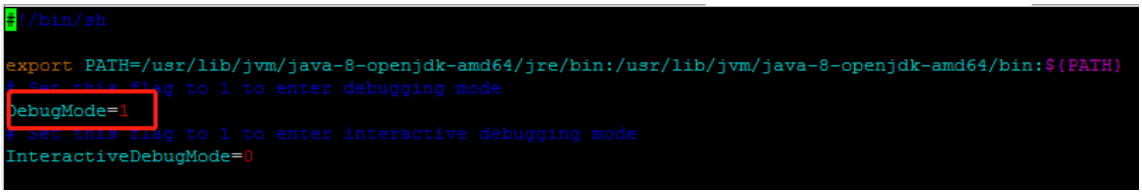
   Si está utilizando Ubuntu, por ejemplo, ejecute el comando **sudo ufw allow 7503** para habilitar el puerto 7503.

Modo de depuración

Si Citrix Telemetry Service no funciona de la manera prevista, puede habilitar el modo de depuración para determinar las causas.

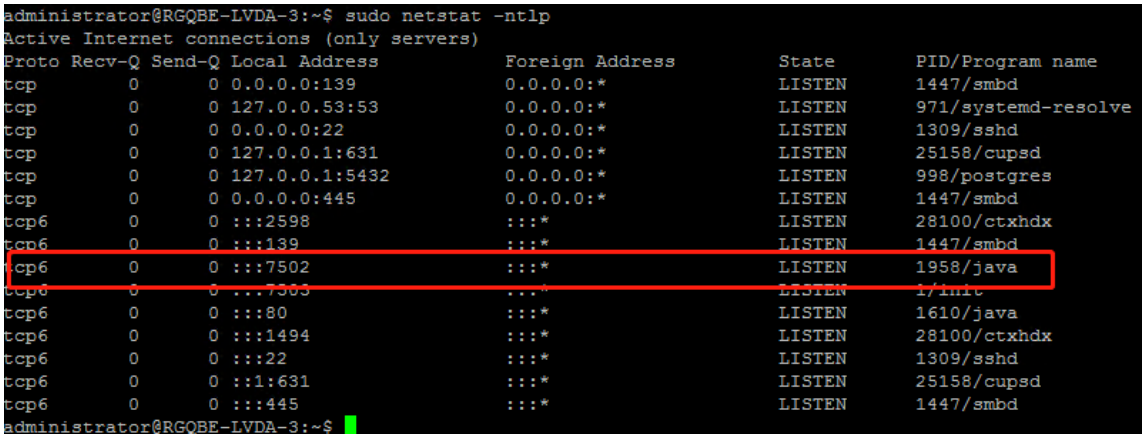
1. Para habilitar el modo de depuración, ejecute el siguiente comando para abrir el archivo `ctxtelemetry` y, a continuación, cambie el valor de DebugMode a 1.

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
<!--NeedCopy-->
```



2. Detenga manualmente Citrix Telemetry Service o espere 15 minutos para que el servicio se detenga automáticamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



En este ejemplo, puede ejecutar los siguientes comandos para detener Citrix Telemetry Service.

```
sudo netstat -ntlp
Kill -9 1958
<!--NeedCopy-->
```

3. Para reiniciar Citrix Telemetry Service, seleccione su Linux VDA en Scout y busque telemetry-debug.log en /var/log/xdl/.

Tiempo de espera del servicio

El demonio `systemd` que abre el puerto de socket se inicia de forma predeterminada y utiliza pocos recursos. Citrix Telemetry Service se detiene de forma predeterminada y solo se inicia cuando hay una solicitud de recopilación de registros de Delivery Controller. Una vez completada la recopilación de registros, el servicio espera nuevas solicitudes de recopilación durante un plazo de 15 minutos y se detiene de nuevo si no hay ninguna. Puede configurar el tiempo de espera con el siguiente comando. El valor mínimo es de 10 minutos. Si establece un valor inferior a 10 minutos, surtirá efecto el valor mínimo de 10 minutos. Después de configurar el tiempo de espera, detenga y reinicie el servicio.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -v "TelemetryServiceIdleTimeoutInMinutes" -d <
    number> -t REG_DWORD
<!--NeedCopy-->
```

Pruebas de verificación

Antes del inicio de una recopilación, se ejecutan automáticamente pruebas de verificación en cada máquina seleccionada. Estas pruebas tienen por finalidad comprobar que se cumplen los requisitos. Si la prueba de una máquina falla, Scout muestra un mensaje con acciones correctivas sugeridas. Para obtener más información acerca de las pruebas de verificación, consulte la sección Pruebas de verificación de la documentación de Citrix Scout.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Actualización automática de Linux VDA para Citrix DaaS Standard para Azure

November 21, 2023

Esta función ayuda a actualizar automáticamente el software de Linux VDA, inmediatamente o a una hora programada. Resulta útil al crear agentes Linux VDA en Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure). No tiene privilegios de administrador de las máquinas virtuales en Azure. Para obtener más información, consulte Crear agentes VDA de Linux en Citrix DaaS Standard para Azure.

Configuración

Para utilizar esta función, siga estos pasos:

Paso 1: Cargar información de actualización y nuevos paquetes VDA en el contenedor de Azure

Paso 1a: Cree un contenedor en su cuenta de almacenamiento de Azure y establezca el nivel de acceso al contenedor en **Blob (Anonymous read access for blobs only)**.

> **Nota:**
>
> Los clientes mantienen y administran exclusivamente los contenedores y blobs de Azure. Citrix no se hace responsable de ningún problema de seguridad asociado a estos. Para garantizar la seguridad de los datos y la rentabilidad, establezca el nivel de acceso al contenedor en **Private (no anonymous access)** después de cada actualización automática.

Paso 1b: Incorpore la información de actualización del VDA a un archivo JSON denominado UpdateInfo.json. Para ver un ejemplo del formato de archivo, consulte el siguiente bloque:

```
{

 "Version": "21.04.200.4",
"Distributions":[
{

"TargetOS": "RHEL7_9",
"PackageName": "",
"PackageHash": ""
 }
 ,
{

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
"TargetOS": "RHEL8_3",
"PackageName": "XenDesktopVDA-21.04.200.4-1.el8_x.x86_64.rpm",
"PackageHash": "
   a6f2aba23b84bbc3a4640294a8bb92474e0cacbab1e5ae33416c0a4473a28d73"
 }
 ,
{

"TargetOS": "UBUNTU18_04",
"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
"PackageHash": "4148
   cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"
 }
 ,
{

"TargetOS": "UBUNTU20_04",
"PackageName": "",
"PackageHash": ""
 }

]
 }

<!--NeedCopy-->
```

Donde, **"Version"** indica la nueva versión del VDA y **"Distributions"** es una matriz de objetos de actualización. Cada objeto contiene tres elementos:

- **"TargetOS"**: Debe ser "RHEL7_9"(para RHEL 7, CentOS 7 y Amazon Linux 2), "RHEL8_3" , "UBUNTU18_04"o "UBUNTU20_04". `ctxmonitorservice` No reconoce ninguna otra distribución.
- **"PackageName"**: Nombre completo del paquete VDA de la versión especificada.
- **"PackageHash"**: Valor SHA-256 que se calcula mediante el comando `shasum -a 256 <pkgname>`.

Paso 1c: Cargue el archivo JSON y la nueva versión de paquetes Linux VDA en su contenedor de Azure.

Paso 2: Habilitar la función de autoactualización en la imagen maestra o en cada VDA

De forma predeterminada, la autoactualización está inhabilitada. Si crea agentes Linux VDA en Citrix DaaS Standard para Azure, la habilitación de funciones debe realizarse en la imagen maestra. De lo contrario, habilite la función en cada VDA de destino directamente.

Para habilitar la autoactualización, ejecute comandos similares a los siguientes para modificar la clave de registro en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "
   Immediately" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-
   Container-Url>" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local
   -Certificate-Path-of-PortalAzureCom>" --force
<!--NeedCopy-->
```

En la tabla siguiente, se describen los parámetros de Registro.

Parámetro de Registro	Descripción
fEnabled	Este parámetro es obligatorio. De forma predeterminada, el valor es 0, lo que significa que la autoactualización está inhabilitada. Puede establecerlo en 1 para habilitar la actualización automática.
URL	Este parámetro es obligatorio. Establece la URL del contenedor de Azure para obtener la información de actualización y los nuevos paquetes de VDA.
ScheduledTime	Este parámetro es obligatorio. Puede establecerlo en **Immediately** o **NextStart**. **Immediately** significa ejecutar la actualización inmediatamente después de descargar los paquetes del VDA. Esta opción es adecuada cuando la velocidad de descarga es alta y la actualización es urgente. Al mismo tiempo, puede afectar negativamente a la experiencia de usuario si hay sesiones en directo al descargar el paquete. **NextStart** significa ejecutar la actualización tras el siguiente inicio de `ctxmonitorservice`. Esta opción es adecuada cuando la velocidad de descarga no es alta y la actualización no es urgente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Parámetro de Registro	Descripción
CaCertificate	Este parámetro es opcional. Establece la ruta completa de un certificado PEM para verificar la URL del contenedor de Azure. Para los blobs de Azure, puede ser el certificado de portal.azure.com que se obtiene del explorador web y luego se convierte a PEM. Por motivos de seguridad, le recomendamos agregar este parámetro de Registro, aunque solo se admite en Ubuntu. En RHEL, falla la vinculación de algunas bibliotecas NSS para el comando `curl`. Asegúrese de establecer los privilegios mínimos del certificado.

Cuando `ctxmonitorservice` se reinicia, consulta primero **Url** para obtener el archivo UpdateInfo.json y recupera la versión de actualización del archivo JSON. A continuación, `ctxmonitorservice` compara la versión de actualización con la versión actual. Si la versión actual es anterior, el servicio descarga la nueva versión del paquete VDA de Azure y la guarda localmente. Después de eso, ejecuta una actualización según la configuración de **ScheduledTime**. En el caso de una implementación local, puede reiniciar `ctxmonitorservice` directamente para desencadenar la actualización. Sin embargo, en Citrix DaaS Standard para Azure, donde no tiene privilegios de administrador para las máquinas virtuales, solo se puede reiniciar `ctxmonitorservice` después de reiniciar la máquina VDA. Si falla una actualización, el VDA revierte a la versión existente.

> **Nota:**
>
> - Los parámetros de Registro configurados en la imagen maestra no se pueden modificar.
> - Si todas las máquinas virtuales de un entorno descargan un paquete al mismo tiempo, la red local se puede congestionar.
> - Si tanto la actualización como la reversión fallan, se pierden los datos del usuario.
> - Si una actualización falla pero la reversión se realiza correctamente, los usuarios de la misma red pueden tener versiones de Linux VDA diferentes. Esta no es una situación ideal.
> - Una actualización normalmente tarda varios minutos en completarse. No hay ningún indicador de estado en Citrix Studio.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métricas de sesión de Linux y Linux VM

December 12, 2022

En la siguiente tabla, se muestran algunas métricas disponibles para máquinas virtuales Linux y sesiones de Linux.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Mín. versión de VDA requerida	Descripción	Observaciones
Métrica	Mín. versión de VDA requerida	Descripción	Observaciones
Duración de inicio de sesión	2109	Es una medida del proceso entre el momento en que un usuario se conecta desde la aplicación Citrix Workspace y el momento en que la sesión está lista para usarse. Para ver la métrica de una sesión, vaya a la ficha Supervisar de Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure). Supervisar está disponible como la consola de Director para supervisar y solucionar problemas de implementación de las versiones Current Release y LTSR de Citrix Virtual Apps and Desktops. En la ficha Supervisar, haga clic en **Ver tendencia histórica** en la sección **Promedio de duración de inicio de sesión**. En la página **Rendimiento de inicio de sesión**, establezca las condiciones de filtro y haga clic en **Aplicar** para ver las métricas.	Disponible solo en Supervisar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Mín. versión de VDA requerida	Descripción	Observaciones
Recuento de reconexiones automáticas de sesiones	2109	Para ver la cantidad de reconexiones automáticas en una sesión, acceda a la vista **Tendencias**. Establezca las condiciones y haga clic en **Aplicar** para reducir los resultados de la búsqueda. La columna **Recuento de reconexiones automáticas de sesiones** muestra la cantidad de reconexiones automáticas en una sesión. La reconexión automática se habilita cuando las directivas de **fiabilidad de la sesión** o de **reconexión automática del cliente** están activas. Para obtener más información acerca de la reconexión de sesiones, consulte Sesiones. Para obtener más información, consulte Configuraciones de directiva de Reconexión automática de clientes y Configuraciones de directiva de Fiabilidad de la sesión	Disponible tanto en Citrix Director como en Supervisar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Mín. versión de VDA requerida	Descripción	Observaciones
Tiempo de inactividad	2103	Para acceder a esta métrica, abra la página **Todas las sesiones** seleccionando **Filtros > Sesiones > Todas las sesiones**.	Disponible tanto en Citrix Director como en Supervisar.
Métricas de una VM de Linux	2103	Estas métricas están disponibles para las máquinas virtuales de Linux: la cantidad de núcleos de CPU, el tamaño de la memoria, la capacidad del disco duro y la utilización actual e histórica de la CPU y de la memoria	Disponible tanto en Citrix Director como en Supervisar.
Protocolo	1909	El protocolo de transporte de una sesión de Linux aparece como UDP o TCP en el panel **Detalles de la sesión**.	Disponible tanto en Citrix Director como en Supervisar.

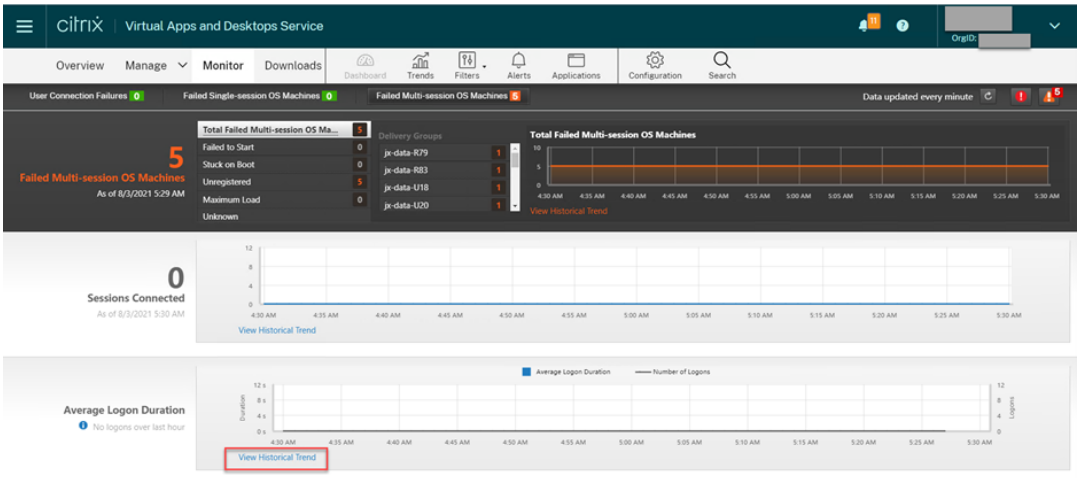
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Métrica	Mín. versión de VDA requerida	Descripción	Observaciones
RTT de ICA	1903	El tiempo de retorno (RTT) de ICA es el tiempo transcurrido desde que se pulsa una tecla hasta que aparece la respuesta en el dispositivo de punto final. Para obtener las métricas de RTT de ICA, cree las directivas **Cálculo del tiempo de retorno ICA** e **Intervalo de cálculo del tiempo de retorno ICA** en Citrix Studio.	Disponible tanto en Citrix Director como en Supervisar.

Ejemplos sobre cómo acceder a las distintas métricas de Citrix Director y Supervisar

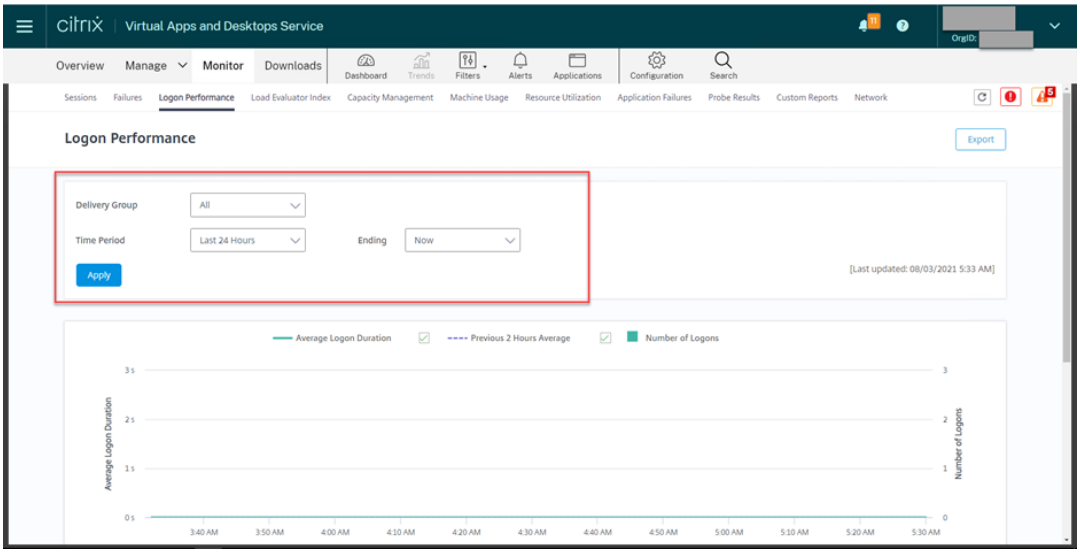
- Duración de inicio de sesión

  1. En la ficha Supervisar de Citrix DaaS, haga clic en **Ver tendencia histórica**, en la sección **Promedio de duración de inicio de sesión**.

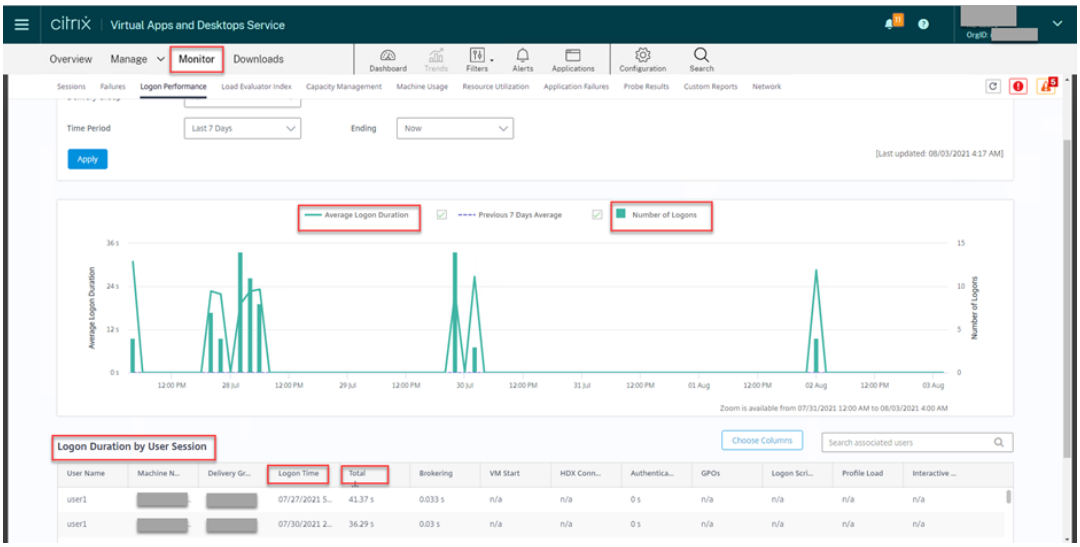


  2. En la página **Rendimiento de inicio de sesión**, establezca las condiciones de filtro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Para ver las métricas de duración de los inicios de sesión, haga clic en **Aplicar**.



- La cantidad de núcleos de CPU, tamaño de memoria, capacidad de disco duro y utilización actual e histórica de CPU y memoria de una VM Linux

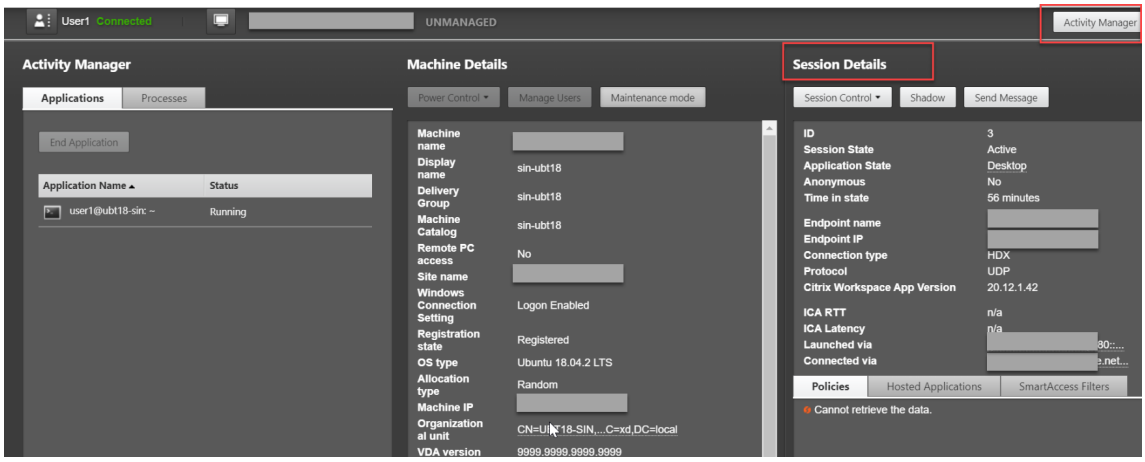
  Para acceder a las métricas de una máquina virtual Linux, busque la máquina virtual en Citrix Director o Supervisar y compruebe el panel **Detalles de la máquina**. Por ejemplo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- RTT de ICA, protocolo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

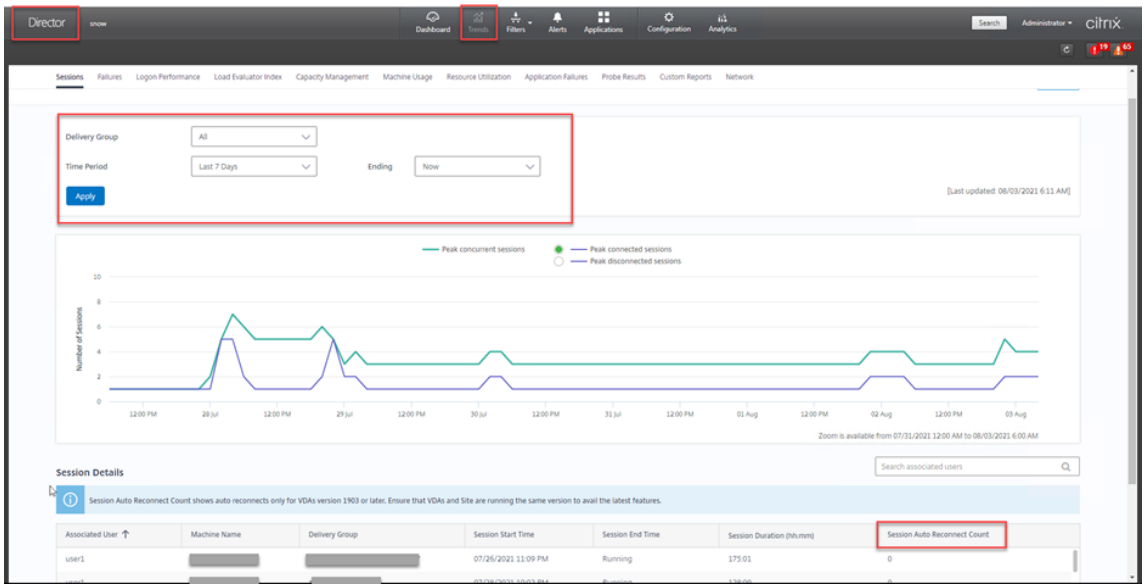
Para ver las métricas de una sesión de Linux, abra la página **Todas las sesiones** seleccionando **Filtros > Sesiones > Todas las sesiones**, o acceda al panel **Detalles de la sesión**. Para acceder al panel **Detalles de la sesión**, abra la página **Todas las Sesiones** y haga clic en una sesión de destino para acceder a su vista **Administrador de actividades**. Por ejemplo:



- Recuento de reconexiones automáticas de sesiones

  Para ver la cantidad de reconexiones automáticas en una sesión, acceda a la vista **Tendencias**. Establezca las condiciones y haga clic en **Aplicar** para reducir los resultados de la búsqueda.

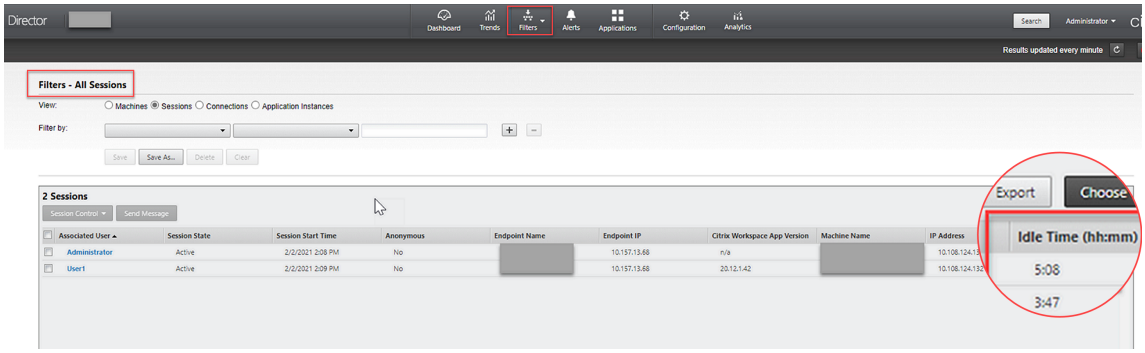
  La columna **Recuento de reconexiones automáticas de sesiones** muestra la cantidad de reconexiones automáticas en una sesión. Por ejemplo:



- Tiempo de inactividad

  Por ejemplo:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Recopilación de registros

July 6, 2022

Información general

Recopilar registros y reproducir problemas ralentiza los diagnósticos y degrada la experiencia del usuario. La recopilación de registros está habilitada para Linux VDA de forma predeterminada.

Configuración

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.

El demonio ctxlogd

Todos los demás servicios que se rastrean dependen del demonio `ctxlogd`. Puede detener el demonio `ctxlogd` si no quiere rastrear Linux VDA.

La utilidad setlog

La recopilación de registros 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`:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
setlog help
<!--NeedCopy-->
```

Valores De forma predeterminada, la ruta de salida **Log Output Path** está establecida en **/var/log/xdl/hdx.log**, el tamaño máximo **Max Log Size** está establecido en 200 MB, y puede guardar dos archivos antiguos de registro como máximo en **Log Output Path**.

Ver los valores actuales de `setlog`:

```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
<!--NeedCopy-->
```

Ver o establecer un solo valor de `setlog`:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

Por ejemplo:

```
setlog value log_size 100
<!--NeedCopy-->
```

Niveles De forma predeterminada, 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:

```
setlog levels
<!--NeedCopy-->
```

Para configurar los niveles de registro (incluidos Disable, Inherited, Verbose, Information, Warnings, Errors y Fatal Errors), ejecute el siguiente comando:

```
setlog level <class> [<level>]
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nivel de registro	Parámetro de comando (no se distingue entre mayúsculas y minúsculas)
Inhabilitado	none
Heredado	inherit
Detallado	verbose
Información	info
Advertencia	warning
Errores	error
Errores irrecuperables	fatal

La variable **<class>** especifica un componente de Linux VDA. Para cubrir todos los componentes, establézcalos todos. Por ejemplo:

```
setlog level all error
<!--NeedCopy-->
```

Marcas De forma predeterminada, las marcas se configuran como se muestra a continuación:

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ver las marcas actuales:

```
setlog flags
<!--NeedCopy-->
```

Ver o establecer una sola marca de registro:

```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

Restaurar valores predeterminados Revertir todos los niveles, las marcas y los valores a los parámetros predeterminados:

```
setlog default
<!--NeedCopy-->
```

> **Importante:**
>
> El servicio `ctxlogd` se configura desde el archivo **/var/xdl/.ctxlog**, que solo puede crear el usuario root. Los demás usuarios no tienen el permiso de escritura en este archivo. Se recomienda que los usuarios root no otorguen permisos de escritura a otros usuarios. No seguir esta premisa puede derivar en una configuración arbitraria o malintencionada de `ctxlogd`, que puede afectar al rendimiento del servidor y, por lo tanto, a la experiencia del usuario.

Solución de problemas

El demonio `ctxlogd` falla y el servicio `ctxlogd` no se puede reiniciar si falta el archivo **/var/xdl/.ctxlog** (por ejemplo, si se ha eliminado por accidente).

/var/log/messages:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
    configuration file.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
    =exited, status=1/FAILURE

Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
<!--NeedCopy-->
```

Para resolver este problema, ejecute `setlog` como usuario root para volver a crear el archivo **/var/xdl/.ctxlog**. A continuación, reinicie el servicio `ctxlogd`, del que dependen los demás servicios.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Remedo de sesiones

July 6, 2022

El remedo de sesiones permite a los administradores de dominio ver las sesiones ICA de los usuarios en una red de intranet. La función utiliza noVNC para conectarse a las sesiones ICA.

> **Nota:**
>
> Para usar la función, utilice `Citrix Director` 7.16 o una versión posterior.

Instalación y configuración

Dependencias

Se requieren dos dependencias nuevas, `python-websockify` y `x11vnc`, para el remedo de sesiones. Instale `python-websockify` y `x11vnc` de forma manual después de instalar Linux VDA.

Para RHEL 7.x y Amazon Linux 2:

Ejecute este comando para instalar `python-websockify` y `x11vnc` (la versión 0.9.13 de `x11vnc` o una posterior):

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

Para resolver `python-websockify` y `x11vnc`, habilite los repositorios Extra Packages for Enterprise Linux (EPEL) y RPM opcionales en RHEL 7.x:

- EPEL

  El repositorio EPEL es necesario para `x11vnc`. Ejecute este comando para habilitar el repositorio de EPEL:

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  <!--NeedCopy-->
  ```

- RPM opcionales

  Ejecute este comando para habilitar el repositorio opcional de `RPMs` para instalar algunos paquetes de dependencias de `x11vnc`:

  ```
  subscription-manager repos --enable rhel-7-server-optional-rpms --enable rhel-7-server-extras-rpms
  <!--NeedCopy-->
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para RHEL 8.x:

Ejecute este comando para instalar `python-websockify` y `x11vnc` (la versión 0.9.13 de `x11vnc` o una posterior).

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

Para resolver `x11vnc`, habilite los repositorios EPEL y CodeReady Linux Builder:

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

subscription-manager repos --enable "codeready-builder  -for-rhel-8-x86_64-rpms"
<!--NeedCopy-->
```

Para Ubuntu:

Ejecute este comando para instalar `python-websockify` y `x11vnc` (la versión 0.9.13 de `x11vnc` o una posterior):

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

Para SUSE:

Ejecute este comando para instalar `python-websockify` y `x11vnc` (la versión 0.9.13 de `x11vnc` o una posterior):

```
sudo pip3 install websockify
sudo zipper install x11vnc
<!--NeedCopy-->
```

Para Debian:

Ejecute este comando para instalar `python-websockify` y `x11vnc` (la versión 0.9.13 de `x11vnc` o una posterior):

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--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 con `Citrix Director`. Por lo tanto, la cantidad de sesiones ICA que puede remedar simultáneamente se limita a 99. Compruebe

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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	Habilita o inhabilita la función de 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, el registro "ShadowingUseSSL"mencionado anteriormente determina si se selecciona `ws://` o `wss://`. De forma predeterminada, se elige `ws://`. Sin embargo, por razones de seguridad, se recomienda usar `wss://` e instalar certificados en cada cliente de 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. En su lugar, puede usar un certificado comodín para todo el dominio. En ese caso, debe conocer al menos el nombre de dominio.

También se requiere un certificado raíz para cada cliente de Citrix Director que se comunique con Linux VDA. Los certificados de raíz están disponibles en las mismas CA que emiten los certificados de servidor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Puede instalar certificados de servidor y cliente de las siguientes entidades de certificación:

- Una entidad de certificación incluida en el sistema operativo
- Una entidad de certificación empresarial (una entidad que su organización pone a su disposición)
- Una entidad de certificación no incluida en el sistema operativo

Consulte con el 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 de 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.

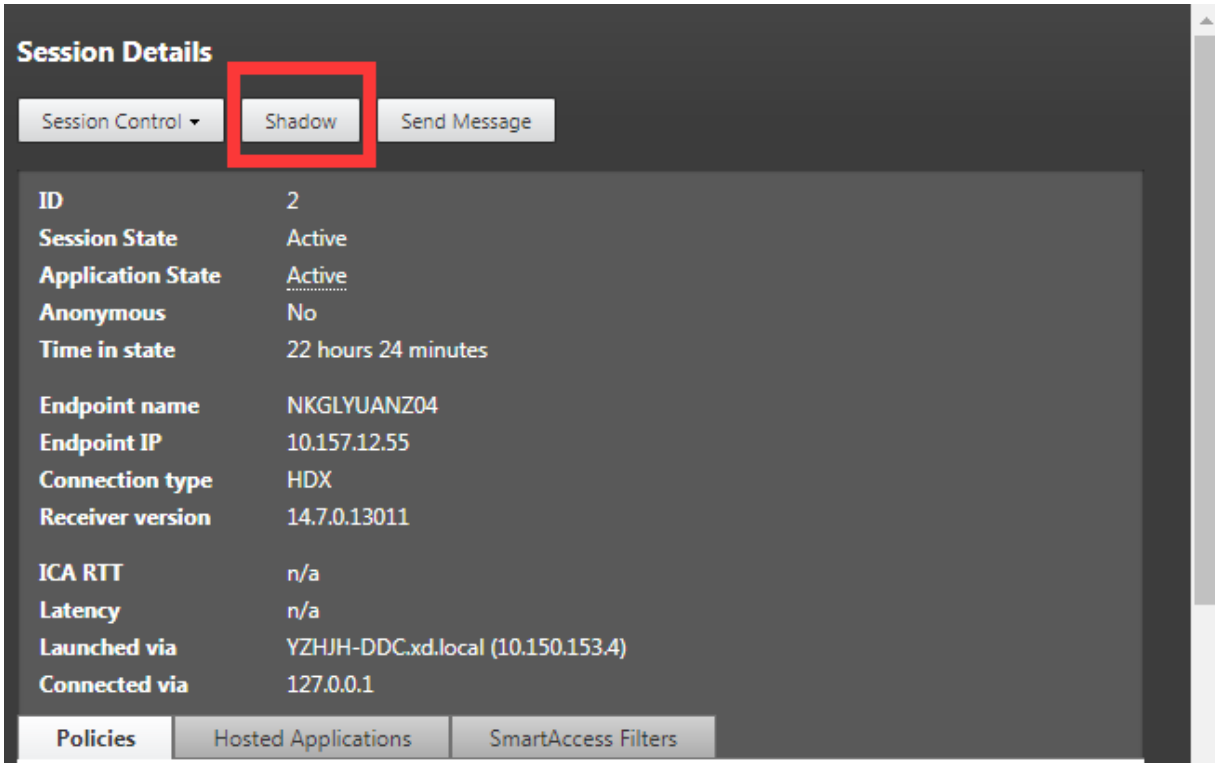
Instalar un certificado raíz en cada cliente de Citrix Director El remedo se sesiones usa el mismo almacén de certificados (basado en el registro del sistema) que IIS, de modo que se puede instalar certificados con IIS o el complemento de certificados de Microsoft Management Console (MMC). Cuando reciba 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.*"(* indica el formato, como shadowingcert.pem o 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`.

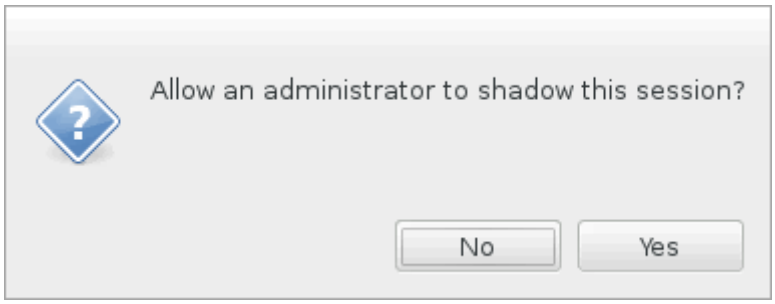
Uso

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Una vez inicializada la conexión, aparece una confirmación en el cliente de la sesión ICA (no en el cliente de `Citrix Director`) con el fin de 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 sesiones. Por ejemplo, si el administrador B envía una solicitud de remedo para una sesión que remeda el administrador A, la confirmación para obtener el permiso del usuario aparece de nuevo en el dispositivo del usuario. Si el usuario la acepta, la conexión de remedo del administrador A se detiene y se crea otra conexión de remedo para el administrador B. Si un administrador envía otra solicitud de remedo para la misma sesión, también se puede crear otra conexión de remedo.
- Para usar el remedo de sesiones, instale `Citrix Director` 7.16 o una versión posterior.
- Un cliente de `Citrix Director` utiliza un FQDN, en lugar de una dirección IP, para conectarse al servidor de Linux VDA de destino. Por lo tanto, el cliente de `Citrix Director` debe poder resolver el FQDN del servidor de Linux VDA.

Solución de problemas

Si se produce un error en el remedo de sesiones, realice la depuración de errores tanto en el cliente de `Citrix Director` como en Linux VDA.

En el cliente de 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 aparece la confirmación para obtener el permiso del usuario, pero falla la creación de la conexión, haga ping al FQDN del VDA manualmente para comprobar que `Citrix Director` puede resolver el FQDN. Si hay problemas 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"
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Abra /etc/xdl/log4j.xml, busque la parte com.citrix.dmc, y cambie “info”por “trace”, tal como se muestra a continuación:

```
<!-- Broker Agent Plugin - Director VDA plugin Logger -->

 <logger name="com.citrix.dmc">

   <level value="trace"/>

 </logger>
<!--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 remedo 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 y que se encuentran en la ruta adecuada.
3. Compruebe que haya suficientes puertos entre 6001 y 6099 para las nuevas solicitudes de remedo de sesiones.

El demonio del servicio de supervisión

July 6, 2022

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**, en **/opt/Citrix/VDA/sbin**, con privilegios de administrador.

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.

```
service ctxmonitorservice restart
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

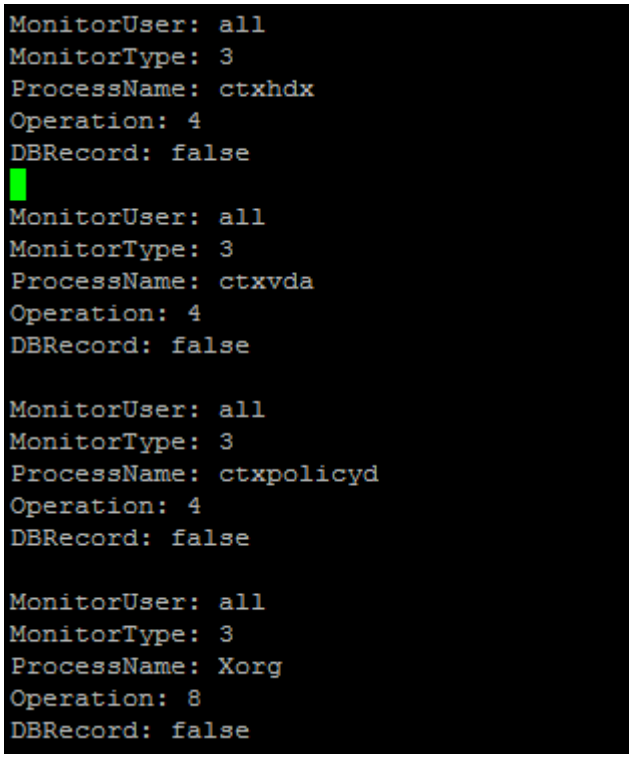
- **scanningpolicy.conf**

  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.



  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)

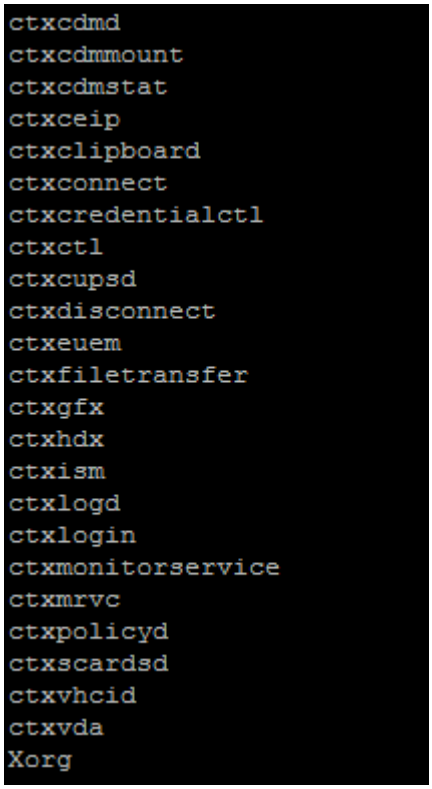
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - **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 = borra 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.



> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Herramientas y utilidades

May 4, 2023

Utilidad de consulta de datos de la sesión

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

- **Ancho de banda de entrada en la sesión**
- **Ancho de banda de salida en la sesión**
- **Velocidad saliente en la sesión**
- **Latencia - Último registro**
- **Tiempo de ida y vuelta**
- **Ancho de banda saliente de Thinwire**
- **Ancho de banda saliente de audio**
- **Ancho de banda saliente de la impresora**
- **Ancho de banda entrante de la unidad**
- **Ancho de banda saliente de la unidad**

El script Bash de xdlcollect

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. El script `xdlcollect` de Bash puede preguntarle si quiere cargar 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

XDPing

La herramienta **XDPing** de Linux es una aplicación de la línea de comandos. Automatiza el proceso de comprobación de problemas de configuración comunes en un entorno de Linux VDA.

La herramienta **XDPing** de Linux realiza más de 150 pruebas individuales en el sistema, que se clasifican en líneas generales de la siguiente manera:

- Comprobar si se cumplen los requisitos del sistema Linux VDA
- Identificar y mostrar información de la máquina, incluidas las distribuciones Linux
- Comprobar la compatibilidad con el kernel de Linux
- Comprobar si hay problemas conocidos de distribución de Linux que puedan afectar al funcionamiento de Linux VDA
- Comprobar el modo de seguridad mejorada de Linux (SELinux) y la compatibilidad
- Identificar interfaces de red y comprobar los parámetros de red
- Comprobar la partición de almacenamiento y el espacio disponible en disco
- Comprobar la configuración del host de la máquina y del nombre de dominio
- Comprobar la configuración DNS y realizar pruebas de búsqueda
- Identificar los hipervisores subyacentes y comprobar la configuración de máquina virtual. Compatibilidad con:
  - Citrix Hypervisor
  - Microsoft HyperV
  - VMware vSphere
- Comprobar la configuración de hora y si la sincronización horaria es operativa
- Comprobar si el servicio PostgreSQL está configurado y es operativo
- Comprobar si el firewall está habilitado y los puertos necesarios están abiertos
- Comprobar la configuración de Kerberos y realizar pruebas de autenticación
- Comprobar el entorno de búsqueda LDAP para el motor del servicio de directivas de grupo
- Compruebe si la integración de Active Directory está configurada correctamente y la máquina actual está unida al dominio. Compatibilidad con:
  - Samba Winbind
  - Quest Authentication Services de Dell
  - Centrify DirectControl
  - SSSD
- Comprobar la integridad del objeto de equipo Linux en Active Directory
- Comprobar la configuración del módulo de autenticación conectable (PAM)
- Comprobar el patrón de volcado principal
- Comprobar si están instalados los paquetes que requiere Linux VDA
- Identificar el paquete Linux VDA y verificar la integridad de la instalación

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Comprobar la integridad de la base de datos del Registro PostgreSQL
- Comprobar si los servicios Linux VDA están configurados correctamente y son operativos
- Comprobar la integridad de la configuración de VDA y HDX
- Sondear cada Delivery Controller configurado para comprobar que Broker Service es accesible, operativo y receptivo
- Comprobar si la máquina está registrada en la comunidad del Delivery Controller
- Comprobar el estado de cada sesión HDX activa o desconectada
- Analizar los archivos de registros en busca de errores y advertencias relacionados con Linux VDA
- Comprobar si la versión de Xorg es válida

Usar la herramienta XDPing de Linux

> **Nota:**
>
> La ejecución de ctxsetup.sh no instala **XDPing**. Puede ejecutar `sudo /opt/Citrix/VDA/bin/xdping` para instalar **XDPing**.
> Este comando también crea un entorno virtual de Python3 que se requiere para **XDPing**. Si este comando no logra crear un entorno virtual Python3, créelo manualmente a partir de las instrucciones indicadas en Crear un entorno virtual Python3.
>
> Para solucionar los errores de conexión SSL que pueden surgir al utilizar la herramienta pip, considere agregar los siguientes hosts de confianza al archivo /etc/pip.conf:
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

XDPing viene con el único ejecutable llamado `xdping` que se ejecuta desde el shell de comandos.

Para mostrar las opciones de la línea de comandos, utilice la opción `-h`:

```
1 sudo /opt/Citrix/VDA/bin/xdping -h
2 <!--NeedCopy-->
```

Para ejecutar el conjunto completo de pruebas, ejecute `xdping` sin ninguna opción de línea de comandos:

```
1 sudo /opt/Citrix/VDA/bin/xdping
2 <!--NeedCopy-->
```

Para comprobar el entorno antes de instalar el paquete Linux VDA, ejecute las pruebas `pre-flight`:

```
1 sudo /opt/Citrix/VDA/bin/xdping --preflight
2 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

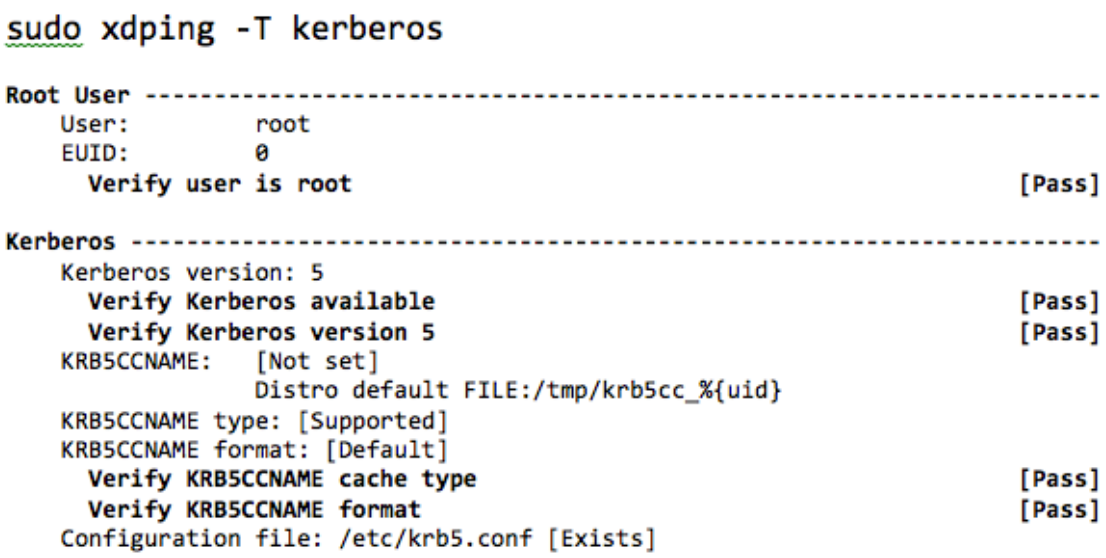
Para ejecutar solo categorías de prueba específicas, por ejemplo, las pruebas de hora y Kerberos, utilice la opción -T:

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
<!--NeedCopy-->
```

Para sondear un Controller de XenDesktop concreto:

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
<!--NeedCopy-->
```

Resultado de ejemplo A continuación, se muestra un ejemplo de resultados de la ejecución de la prueba Kerberos:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  Verify Kerberos configuration file found                              [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                                      [Pass]
  Verify default realm set                                              [Pass]
  Verify default realm in upper-case                                    [Pass]
  Verify default realm not EXAMPLE.COM                                  [Pass]
  Verify default realm domain mappings                                  [Pass]
  Verify default realm master KDC configured                            [Pass]
  Verify Kerberos weak crypto disabled                                  [Pass]
  Verify Kerberos clock skew setting                                    [Pass]
Default ccache: [Not set]
               Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                            [Pass]
  Verify default credential cache format                                [Pass]
UPN system key [MYVDA1$@          ]: [MISSING]
SPN system key [host/m                  l]: [Exists]
  Verify Kerberos system keys for UPN exist                            [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.

      Verify Kerberos system keys for SPN exist                          [Pass]
    Kerberos login: [FAILED AUTHENTICATION]
                    Keytab contains no suitable keys for MYVDA1$@
                    while getting initial credentials
      Verify KDC authentication                                         [ERROR]
      Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
      from the KDC authentication service for the machine account UPN
      MYVDA1$@          . Check that the Kerberos configuration is
      valid and the keys in the system keytab are current.


Summary ------------------------------------------------------------------------
  The following tests did not pass:
      Verify Kerberos system keys for UPN exist                         [ERROR]
      Verify KDC authentication                                         [ERROR]
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Otros

July 6, 2022

Esta sección contiene estos temas:

- Compatibilidad con la aplicación Citrix Workspace para HTML5
- Crear un entorno virtual Python3
- Integrar NIS en Active Directory
- IPv6
- LDAPS
- **Xauthority**

Compatibilidad con la aplicación Citrix Workspace para HTML5

July 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Crear un entorno virtual Python3

November 21, 2023

Si se está conectando a la red, la ejecución de los comandos `sudo /opt/Citrix/VDA/bin/xdping` o `/opt/Citrix/VDA/sbin/enable_ldaps.sh` puede crear un entorno virtual Python3. Sin embargo, si los comandos no logran crear un entorno virtual de Python3, puede crearlo manualmente incluso sin una conexión de red. En este artículo, se indican los requisitos previos y los pasos para crear un entorno virtual Python3 sin conexión de red.

Requisitos previos

- Debe tener privilegios administrativos para acceder al directorio `/opt/Citrix/VDA/sbin/ctxpython3`.
- Dispone de los archivos wheel de los paquetes `Python3`. Puede descargar los archivos wheel desde https://pypi.org/.

Crear un entorno virtual Python3

Complete estos pasos para crear un entorno virtual Python3:

1. Instale las dependencias de Python3.

   Para RHEL:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
yum -y install python36-devel krb5-devel gcc
<!--NeedCopy-->
```

> **Nota:**
>
> Es posible que tenga que habilitar un repositorio en particular para instalar algunas dependencias. Para RHEL 7, ejecute el comando `subscription-manager repos --enable rhel-7-server-optional-rpms`. Para RHEL 8, ejecute el comando `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms`.

Para Ubuntu, Debian:

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
<!--NeedCopy-->
```

Para SUSE:

```
zypper -i -n install python3-devel python3-setuptools krb5-devel gcc libffi48-devel
<!--NeedCopy-->
```

2. Cree un entorno virtual Python3.

> **Nota:**
>
> Para solucionar los errores de conexión SSL que pueden surgir al utilizar la herramienta pip, considere agregar los siguientes hosts de confianza al archivo /etc/pip.conf:
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

Para RHEL, Ubuntu, Debian:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

Para SUSE:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install setuptools==40.6.2
<!--NeedCopy-->
```

3. Instale las dependencias de LDAPS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para RHEL, Ubuntu, Debian:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
    cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
    ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
    pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
    termcolor==1.1.0
<!--NeedCopy-->
```

Para SUSE:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install
    cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
    ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
    pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
    termcolor==1.1.0
<!--NeedCopy-->
```

4. Instale las dependencias de XDPing.

Para RHEL, Ubuntu, Debian:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
    cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
    ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
    pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
    termcolor==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /
    opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
<!--NeedCopy-->
```

Para SUSE:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install
    cffi==1.14.2 cryptography==3.1 decorator==4.4.2 gssapi==1.6.2
    ldap3==2.8.1 netifaces==0.10.9 pg8000==1.17.0 psutil==5.8.0
    pyasn1==0.4.8 pycparser==2.20 scramp==1.2.0 six==1.15.0
    termcolor==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install /
    opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
<!--NeedCopy-->
```

Integrar NIS en Active Directory

July 6, 2022

En este tema, se describe cómo integrar NIS con Windows Active Directory (AD) en Linux VDA mediante

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, en lugar de Active Directory, como un proveedor de UID y GID, es necesario que la información de cuenta (la combinación de nombre de usuario y contraseña) sea la misma en AD y 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.

Integrar NIS con AD

Para integrar NIS con AD, siga estos pasos:

Paso1: Agregar el Linux VDA como cliente NIS

Configure el cliente NIS:

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

Establezca el dominio NIS:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

Configure NIS con `authconfig`:

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
   nis.domain --enablemkhomedir --update
<!--NeedCopy-->
```

nis.domain representa el nombre de dominio del servidor NIS. **server.nis.domain** es el nombre de host del servidor NIS, que puede ser también la dirección IP del servidor NIS.

Configure los servicios de NIS:

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

Compruebe que la configuración de NIS es correcta:

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

Valide que la información de la cuenta esté disponible desde el servidor NIS:

```
getent passwd nisaccount
<!--NeedCopy-->
```

> **Nota:**
>
> El valor de **nisaccount** representa la verdadera cuenta de NIS en el servidor NIS. Compruebe que el GID, el UID, el directorio principal y el shell de inicio de sesión están configurados correctamente.

Paso 2: 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

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

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

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

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

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

```
kerberos method = secrets and keytab
winbind offline logon = no
```

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:

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

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

Paso 3: Configurar SSSD

Configurar SSSD consta de los siguientes pasos:

- Instalar los paquetes **sssd-ad** y **sssd-proxy** en la máquina cliente Linux.
- Realice cambios de configuración en varios archivos (por ejemplo, **sssd.conf**).
- Inicie el **servicio sssd**.

/etc/sssd/sssd.conf A continuación, se ofrece un ejemplo de configuración de **sssd.conf** (se pueden agregar opciones adicionales, según sea necesario):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[sssd]
config_file_version = 2
domains = EXAMPLE
services = nss, pam

[domain/EXAMPLE]
# Uncomment if you need offline logins
# cache_credentials = true
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = ad

# Should be specified as the long version of the Active Directory domain.
ad_domain = EXAMPLE.COM

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
<!--NeedCopy-->
```

Reemplace **ad.domain.com**, **server.ad.example.com** por el valor correspondiente. Para obtener más información, consulte **sssd-ad**(5) - Linux man page.

Establezca la pertenencia y los permisos de archivos en **sssd.conf**:

```
chown root:root /etc/sssd/sssd.conf
chmod 0600 /etc/sssd/sssd.conf
restorecon /etc/sssd/sssd.conf
```

Paso 4: Configurar NSS/PAM

RHEL/CentOS:

Use **authconfig** para habilitar SSSD. Instale **oddjob-mkhomedir** para que la creación del directorio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de inicio sea compatible con SELinux:

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

sudo systemctl start sssd

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

> **Sugerencia:**
>
> Al configurar Linux VDA, tenga en cuenta que, para SSSD, no hay ninguna configuración especial para el cliente Linux VDA. Para soluciones adicionales en el script **ctxsetup.sh**, use el valor predeterminado.

Paso 5: Verificar la configuración de Kerberos

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

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

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

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

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

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

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

Paso 5: Verificar la autenticación del usuario

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

```
sudo getent passwd DOMAIN\username
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

El parámetro **DOMAIN** indica la versión corta del nombre de dominio. Si se necesita otro formato de inicio de sesión, compruébelo primero con el comando **getent**.

Los formatos de inicio de sesión admitidos son:

- Nombre de inicio de sesión de nivel inferior: `DOMAIN\username`
- UPN: `username@domain.com`
- Formato del sufijo NetBIOS: `username@DOMAIN`

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

```
sudo ssh localhost  – l DOMAIN\username

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

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

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

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

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

IPv6

July 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

LDAPS

March 11, 2024

LDAPS es la versión segura del Protocolo ligero de acceso a directorios (LDAP) en la que las comunicaciones LDAP se cifran mediante TLS/SSL.

De forma predeterminada, las comunicaciones LDAP entre las aplicaciones de cliente y de servidor no están cifradas. 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 un 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/inhabilitar LDAPS en Linux VDA
- Configurar LDAPS para plataformas de terceros
- Configurar SSSD
- Configurar Winbind
- Configurar Centrify
- Configurar Quest

> **Nota:**
>
> Puede ejecutar el siguiente comando para establecer un ciclo de supervisión para los servidores LDAP. El valor predeterminado es 15 minutos. Establézcalo en 10 minutos, como mínimo.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "
     REG_DWORD" -d "0x0000000f" --force
2 <!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Sugerencia:**
>
> 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.

Si dispone de una jerarquía de entidades de certificación multicapa, 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.

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 en Linux VDA, ejecute el siguiente script (habiendo iniciado una sesión como administrador):

La sintaxis del comando es la siguiente:

- Habilitar LDAP por SSL/TLS con el certificado de CA raíz suministrado:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- Habilite LDAP por SSL/TLS con vinculación de canales:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
<!--NeedCopy-->
```

> **Nota:**
>
> El certificado de CA raíz para la vinculación de canales debe estar en formato PEM. Si habilitar LDAPS no crea correctamente un entorno virtual Python3, créelo manualmente a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> partir de las instrucciones indicadas en Crear un entorno virtual Python3.
>
> Para solucionar los errores de conexión SSL que pueden surgir al utilizar la herramienta pip, considere agregar los siguientes hosts de confianza al archivo /etc/pip.conf:
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

- Recurrir a LDAP sin SSL/TLS

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

El almacén de claves de Java dedicado para LDAPS reside en **/etc/xdl/.keystore**. Las claves de Registro afectadas incluyen:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
<!--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 el puerto 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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 actualizó las claves relacionadas con LDAPS 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. En general, debería admitir la mayoría de los tipos de Java Keytool disponibles. Si no aparece en la lista de compatibilidad, puede convertir el tipo. Recomendamos el formato PEM con codificación base64 si encuentra algún problema de formato del certificado.

- **No se puede ver el certificado de CA raíz con el parámetro de Keytool -list**

  Al habilitar LDAPS ejecutando `/opt/Citrix/VDA/sbin/enable_ldaps.sh`, el certificado se importa a /etc/xdl/.keystore y la contraseña se establece para proteger el almacén de claves. Si olvida la contraseña, puede volver a ejecutar el script para crear un almacén de claves.

Xauthority

July 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA admite los entornos que utilizan la funcionalidad de pantalla X11 (incluidos `xterm` y `gvim`) para la comunicación remota interactiva. Esta función proporciona un mecanismo de seguridad necesario para proteger la comunicación entre XClient y XServer.

Existen dos métodos para garantizar este permiso para la comunicación segura:

- **Xhost**. De forma predeterminada, Xhost solo permite al XClient de localhost la comunicación con XServer. Si elige permitir el acceso a XServer a un XClient remoto, el comando Xhost tiene que ser ejecutado para conceder permiso a esa máquina concreta. O bien, puede usar **xhost +** para permitir que cualquier XClient se conecte a XServer.
- **Xauthority**. El archivo `.Xauthority` se encuentra en el directorio principal de cada usuario. Se usa para almacenar credenciales en las cookies utilizadas por xauth para la autenticación de XServer. Una vez que una instancia de XServer (Xorg) se ha iniciado, la cookie se usa para autenticar las conexiones específicas a esa pantalla concreta.

Funcionamiento

Cuando se inicia Xorg, se pasa un archivo `.Xauthority` a Xorg. Este archivo `.Xauthority` contiene los siguientes elementos:

- Número de pantalla
- Protocolo de solicitud remota
- Número de cookie

Puede examinar este archivo mediante el comando `xauth`. Por ejemplo:

```
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1
     fb228d1b695729242616c5908f11624b
<!--NeedCopy-->
```

Si **XClient** se conecta de forma remota a Xorg, deben cumplirse dos requisitos previos:

- Definir la variable de entorno **DISPLAY** con el valor del XServer remoto.
- Obtener el archivo `.Xauthority` que contiene uno de los números de cookie en Xorg.

Configurar Xauthority

Para habilitar **Xauthority** en Linux VDA para la pantalla X11 remota, deben crearse dos claves de Registro:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
    XauthEnabled" -d "0x00000001" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
     -d "0x00000001" --force
<!--NeedCopy-->
```

Después de habilitar **Xauthority**, pase el archivo `.Xauthority` a **XClient** manualmente o mediante el montaje de un directorio particular (home) compartido:

- Pasar el archivo `.Xauthority` a XClient manualmente

  Después de iniciar una sesión ICA, el Linux VDA genera el archivo `.Xauthority` para el XClient y almacena el archivo en el directorio home del usuario de inicio de sesión. Puede copiar este archivo `.Xauthority` en la máquina XClient remota y establecer las variables de entorno **DISPLAY** y **XAUTHORITY**. `DISPLAY` es el número de pantalla almacenado en el archivo `.Xauthority` y `XAUTHORITY` es la ruta de archivo de **Xauthority**. Por ejemplo, fíjese en el comando siguiente:

  ```
  export DISPLAY={
  Display number stored in the Xauthority file }


  export XAUTHORITY={
  the file path of .Xauthority }

  <!--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 montando 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 home 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

   ```
   ps aux | grep -i xorg
   <!--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:

   ```
   /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

   Muestre las cookies mediante el comando **Xauth**:

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   <!--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 y el número de pantalla del escritorio publicado.

   Ejecute, por ejemplo, el siguiente comando en la máquina XClient:

   ```
   telnet 10.158.11.11 6160
   <!--NeedCopy-->
   ```

   El número de puerto es la suma de 6000 + \<número de pantalla\>.

   Si se produce un error en la operación de Telnet, el firewall puede estar bloqueando la solicitud.

Autenticación

July 6, 2022

Esta sección contiene estos temas:

- Autenticación de inicio de sesión Single Sign-On de dos saltos
- Servicio de autenticación federada
- Credenciales de los inicios de sesiones

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Tarjetas inteligentes
- Sesiones sin autenticar

Autenticación de inicio de sesión Single Sign-On de dos saltos

July 6, 2022

Se pueden inyectar 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:

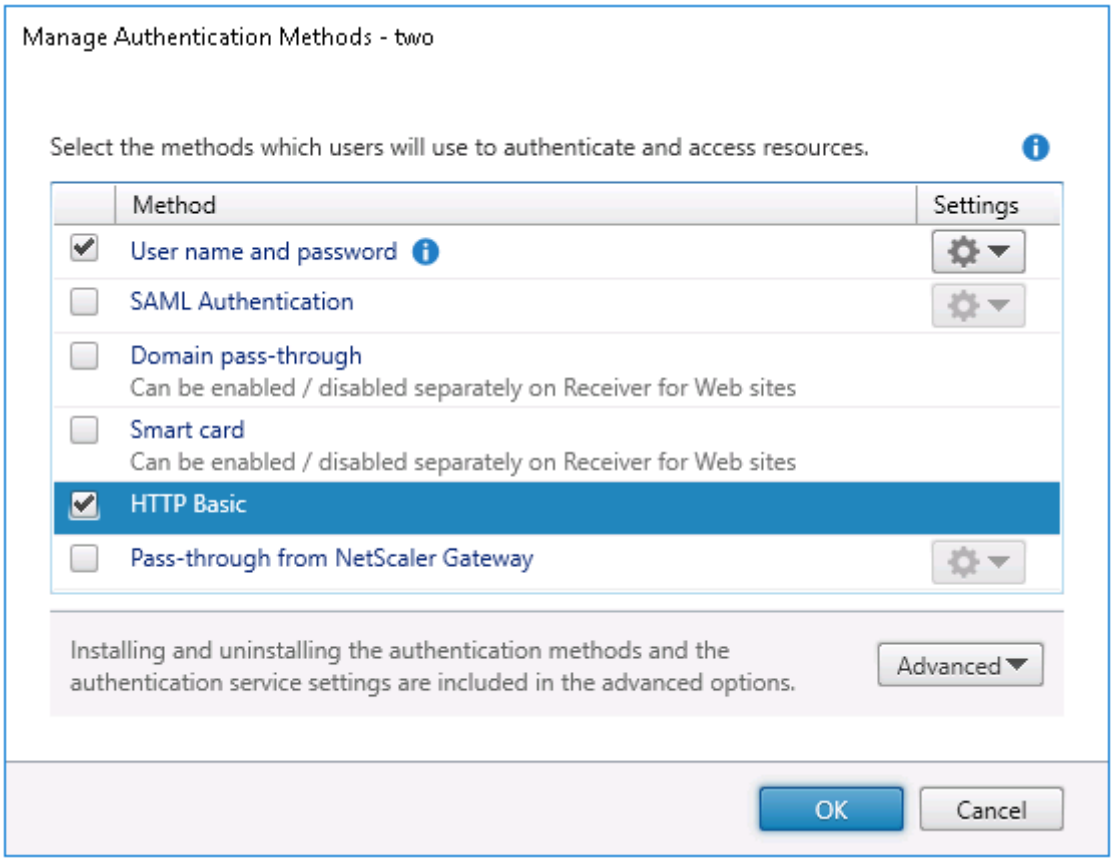
1. En el Linux VDA, instale la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Agregue la siguiente clave al archivo de configuración de AuthManager ($ICAROOT/config/AuthManConfig.xml) para permitir la autenticación HTTP básica:

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
<!--NeedCopy-->
```

4. Ejecute los siguientes comandos para instalar el certificado raíz en el directorio especificado.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/
$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
<!--NeedCopy-->
```

5. Ejecute el siguiente comando para habilitar la función:

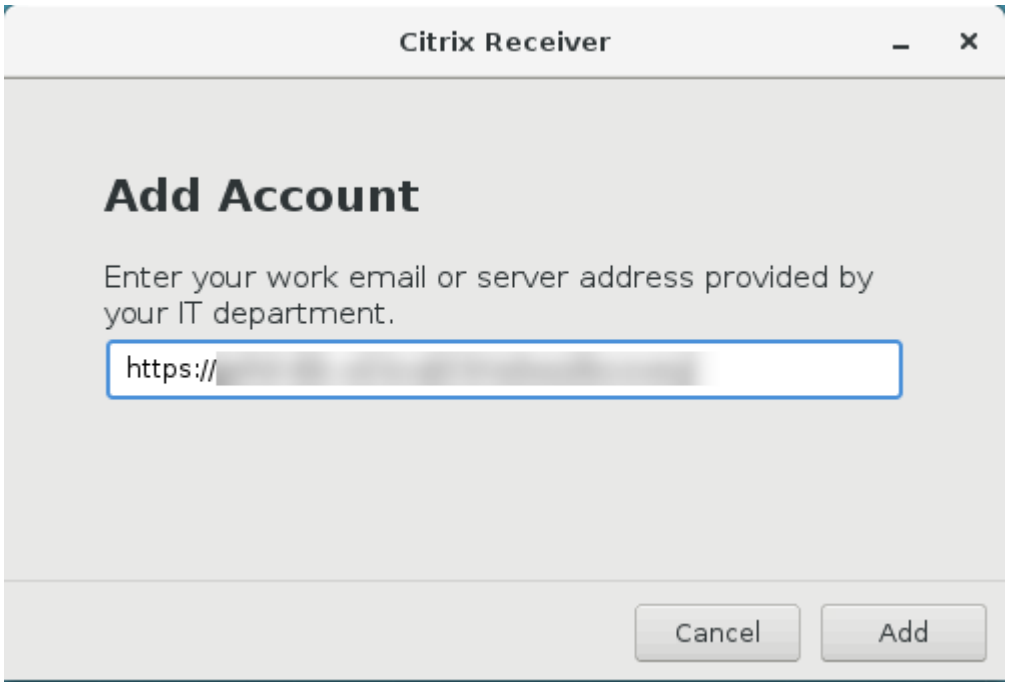
```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
<!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Se le pedirá una cuenta de almacén cuando inicie la aplicación Citrix Workspace por primera vez. Más tarde, la sesión se iniciará automáticamente en el almacén que especificó anteriormente.

> **Nota:**
>
> introduzca una URL HTTPS como su cuenta de almacén.



Servicio de autenticación federada

June 14, 2023

Puede usar el Servicio de autenticación federada (FAS) para autenticar a los usuarios que inician sesión en un VDA de Linux. El VDA de Linux utiliza el mismo entorno de Windows que el VDA de Windows para la funcionalidad de inicio de sesión con FAS. Para obtener información sobre cómo configurar el entorno Windows para FAS, consulte Servicio de autenticación federada. Este artículo proporciona información adicional específica de Linux VDA.

> **Nota:**
>
> Linux VDA no admite la directiva **In-session Behavior** (Comportamiento durante la sesión).
>
> Linux VDA usa conexiones cortas para la transmisión de datos con servidores de FAS.
>
> Linux VDA se comunica con los servidores de FAS únicamente a través del puerto 80.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configurar FAS en Linux VDA

Compatibilidad con FAS en RHEL 8

FAS depende del módulo pam_krb5, que se ha retirado en RHEL 8. Para usar FAS en RHEL 8, genere el módulo pam_krb5 de la siguiente manera:

1. Descargue el código fuente pam_krb5-2.4.8-6 del siguiente sitio web:

   https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Genere e instale el módulo pam_krb5 en RHEL 8.

```
yum install make gcc krb5-devel pam-devel autoconf libtool
rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
tar xvzf pam_krb5-2.4.8.tar.gz
cd pam_krb5-2.4.8
./configure --prefix=/usr
make
make install
<!--NeedCopy-->
```

3. Compruebe que pam_krb5.so existe en /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

Configurar servidores FAS

Para usar FAS en una instalación nueva de Linux VDA, escriba el FQDN de cada servidor de FAS cuando ejecute 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 el orden de las direcciones de servidor.

Para actualizar la versión de una instalación Linux VDA existente, puede ejecutar `ctxsetup.sh` de nuevo y configurar los servidores de FAS. O puede ejecutar los siguientes comandos para configurar los servidores FAS y reiniciar el servicio `ctxvda` para que los cambios surtan efecto.

```
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

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Para actualizar los servidores FAS mediante `ctxreg`, ejecute los siguientes comandos:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
   VirtualDesktopAgent\Authentication\UserCredentialService" -v "
   Addresses" -d "<Your-FAS-Server-List>"

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

Instalación de certificados

Para verificar los certificados de los usuarios, instale el certificado raíz de CA y todos los certificados intermedios en el VDA. Por ejemplo, para instalar el certificado raíz de CA, 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.

```
sudo openssl x509 -inform der -in root.cer -out root.pem
<!--NeedCopy-->
```

Luego, instale el certificado raíz de CA en el directorio `openssl` ejecutando un comando similar al siguiente:

```
sudo cp root.pem /etc/pki/CA/certs/
<!--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.

Ejecutar ctxfascfg.sh

Ejecute el script ctxfascfg.sh para configurar FAS:

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

Se agregan variables de entorno para que `ctxfascfg.sh` pueda ejecutarse en modo silencioso:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis**: 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_CERT_PATH =<certificate path>**: Especifica la ruta completa donde se almacenan el certificado raíz y todos los certificados intermedios.
- **CTX_FAS_KDC_HOSTNAME**: Especifica el nombre de host del Centro de distribución de claves (KDC) cuando selecciona PBIS.
- **CTX_FAS_PKINIT_KDC_HOSTNAME**: Especifica el nombre de host de KDC PKINIT, que es igual a CTX_FAS_KDC_HOSTNAME a menos que se especifique lo contrario.

Elija el método apropiado de integración en Active Directory y escriba la ruta apropiada a los certificados (por ejemplo, `/etc/pki/CA/certs/`).

El script instala los paquetes krb5-pkinit y pam_krb5, y establece los archivos de configuración relevantes.

Limitación

- FAS admite plataformas Linux y métodos de integración de AD limitados. Consulte la siguiente matriz:

	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	Sí	Sí	Sí	Sí
RHEL 8.4	Sí	Sí	Sí	Sí
RHEL 8.3	Sí	Sí	Sí	Sí
RHEL 8.2	Sí	Sí	Sí	Sí
RHEL 8.1	Sí	Sí	Sí	Sí
RHEL 7.9 / CentOS 7.9	Sí	Sí	Sí	Sí
SLES 15.3	Sí	No	Sí	No
SLES 15.2	Sí	No	Sí	No
Ubuntu 20.04	Sí	No	Sí	No
Ubuntu 18.04	Sí	No	Sí	No

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 y que puedan iniciarse sesiones que no sean de 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.

Consulte **/var/log/xdl/hdx.log** y busque el registro de errores similar al siguiente:

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon Type] Federated Authentication Logon.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start connect to server 0

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed to connect: Connection refused.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed to connect to server [0], please confirm if fas service list is well configurated in condb

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit, 43

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed to validate fas credential

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate: failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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>.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
<!--NeedCopy-->
```

Si la configuración existente no es correcta, siga el anterior paso Configurar servidores FAS para definirla nuevamente.

Configuración incorrecta del certificado 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:

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: entry

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
   current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: entry

2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
    for response...

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query
   to server success

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: exit

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    input size 1888

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
    cache certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: exit, 0

2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
   pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
<!--NeedCopy-->
```

Solución Compruebe que se ha configurado correctamente en `/etc/krb5.conf` la ruta completa que almacena el certificado de CA raíz y todos los certificados intermedios. La ruta completa será parecida a esta:

```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

 }

<!--NeedCopy-->
```

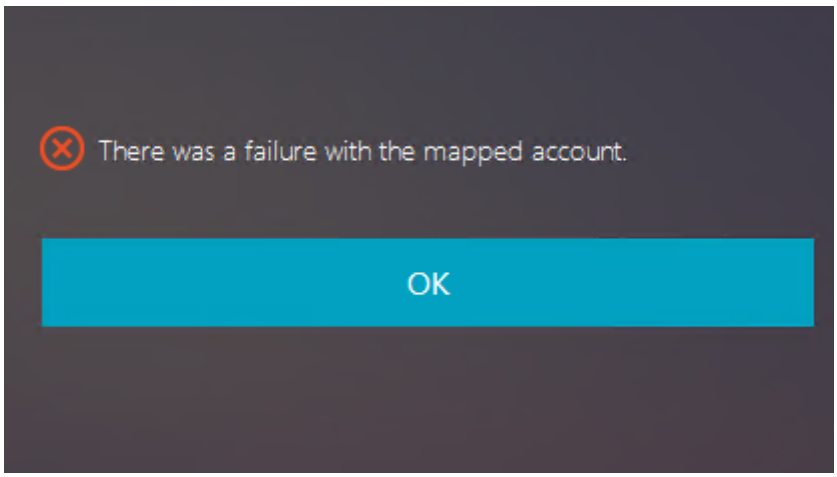
Si la configuración existente no es correcta, siga el paso anterior Instalar certificados para definirla nuevamente.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

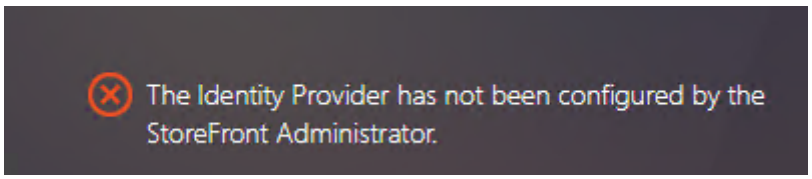


Este error indica que el usuario de ADFS se ha verificado correctamente, pero no hay ningún usuario sombra configurado en AD.

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 problema se produce cuando el almacén FAS está configurado para utilizar la autenticación 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.

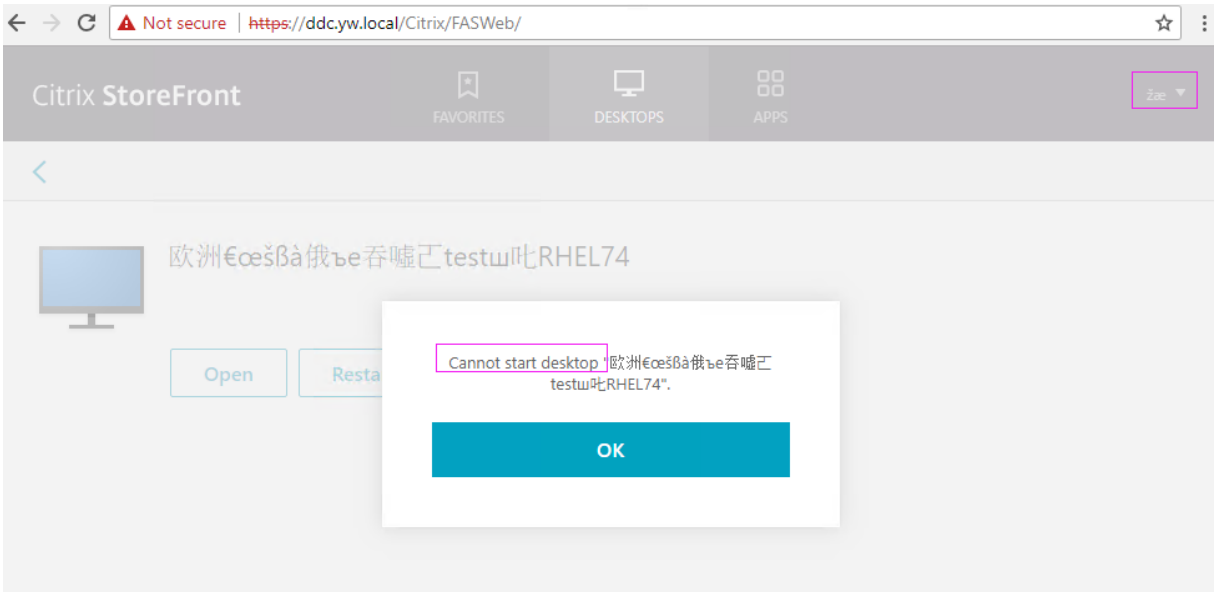
Información relacionada

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Problema conocido

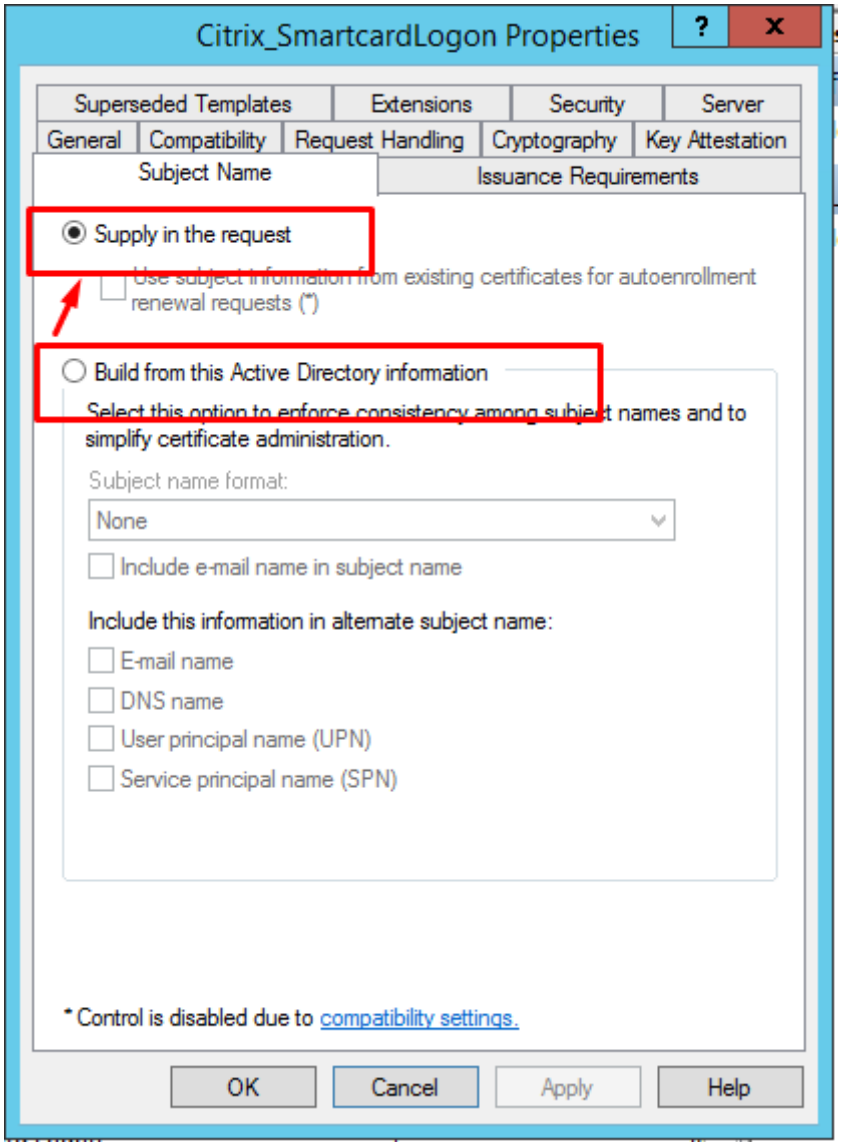
Cuando se usa FAS, puede que fallen los inicios de una sesión de aplicación o escritorio publicados si se usan caracteres que no sean en inglés.



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**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Autenticación sin SSO

August 8, 2022

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Con la función habilitada, se le solicitarán credenciales al iniciar sesiones. Esta función es compatible con estas distribuciones:

- RHEL 8.4
- RHEL 7.9 / CentOS 7.9
- Debian 10.9
- SUSE 15.3
- SUSE 15.2

Tarjetas inteligentes

July 6, 2022

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 y autenticarse en un sitio web.

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.

> **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.

Requisitos previos

La disponibilidad de la autenticación PassThrough con tarjeta inteligente depende de estas condiciones:

- Linux VDA se instala en una de estas distribuciones:
  - RHEL 8
  - RHEL 7/CentOS 7
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Debian 10.9

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Después de completar la instalación del VDA, compruebe que el VDA se puede registrar en el Delivery Controller y que puede abrir las sesiones de escritorio de Linux publicadas con las credenciales de Windows.

- Se utilizan tarjetas inteligentes compatibles con OpenSC. Para obtener más información, consulte Comprobar que OpenSC admite la tarjeta inteligente.
- Se usa la aplicación Citrix Workspace para Windows.

Comprobar que OpenSC admite la tarjeta inteligente

OpenSC es un controlador de tarjeta inteligente muy utilizado en RHEL 7.4 y versiones posteriores. Como reemplazo totalmente compatible de CoolKey, OpenSC admite muchos tipos de tarjetas inteligentes (consulte Soporte para tarjetas inteligentes en 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 OpenSC admite YubiKey 4.

Si su organización necesita una tarjeta inteligente más avanzada, prepare una máquina física con una distribución de Linux compatible y el paquete OpenSC instalado. Para obtener información sobre la instalación de OpenSC, consulte Instalar el controlador de tarjeta inteligente. Inserte su tarjeta inteligente y ejecute el siguiente comando para verificar que OpenSC la admite:

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuración

Preparar un certificado raíz

Un certificado raíz se utiliza para verificar el certificado que se encuentra en la tarjeta inteligente. Siga estos pasos para descargar e instalar un certificado raíz.

1. Obtenga un certificado raíz en formato PEM, generalmente desde su servidor de CA.

   Puede ejecutar un comando similar al siguiente para convertir un archivo DER (*.crt, *.cer, *.der) a PEM. En el siguiente ejemplo de comando, **certnew.cer** es un archivo DER.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   <!--NeedCopy-->
   ```

2. Instale el certificado raíz en el directorio `openssl`. El archivo **certnew.pem** se usa como ejemplo.

   ```
   cp certnew.pem <path where you install the root certificate>
   <!--NeedCopy-->
   ```

   Para crear una ruta donde instalar el certificado raíz, ejecute `sudo mdkir -p <path where you install the root certificate>`.

Crear el módulo pam_krb5 en RHEL 8

La autenticación con tarjeta inteligente depende del módulo pam_krb5, que se ha retirado en RHEL 8. Para utilizar la autenticación con tarjeta inteligente en RHEL 8, genere el módulo pam_krb5 de la siguiente manera:

1. Descargue el código fuente de pam_krb5-2.4.8-6 desde https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.
2. Genere e instale el módulo pam_krb5 en RHEL 8.

   ```
   yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-
       tools
   yum install gcc krb5-devel pam-devel autoconf libtool
   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
   tar xvzf pam_krb5-2.4.8.tar.gz
   cd pam_krb5-2.4.8
   ./configure --prefix=/usr
   make
   make install
   <!--NeedCopy-->
   ```

3. Compruebe que pam_krb5.so existe en /usr/lib64/security/.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

Configurar el entorno de tarjeta inteligente

Puede utilizar el script ctxsmartlogon.sh para configurar el entorno de tarjetas inteligentes o puede completar la configuración manualmente.

(Opción 1) 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.

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--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.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

También puede inhabilitar las tarjetas inteligentes ejecutando el script ctxsmartlogon.sh:

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--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.
```

(Opción 2) Configurar manualmente el entorno de la tarjeta inteligente 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 continuar al siguiente paso, compruebe que todos los componentes estén correctamente configurados, que la clave privada y el certificado de usuario se hayan descargado en la tarjeta inteligente y que pueda iniciar sesión correctamente 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:

RHEL 7/CentOS 7, RHEL 8:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
<!--NeedCopy-->
```

Ubuntu 20.04, Ubuntu 18.04, Debian 10.9:

```
apt-get install -y libpcsclite1 libccid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instale el controlador de tarjeta inteligente OpenSC es un controlador de tarjeta inteligente muy utilizado. Si OpenSC no está instalado, ejecute el siguiente comando para instalarlo:

RHEL 7/CentOS 7, RHEL 8:

```
yum install opensc
<!--NeedCopy-->
```

Ubuntu 20.04, Ubuntu 18.04, Debian 10.9:

```
apt-get install -y opensc
<!--NeedCopy-->
```

Instalar los módulos PAM para la autenticación con tarjeta inteligente Ejecute el siguiente comando para instalar los módulos pam_krb5 y krb5-pkinit.

RHEL 7/CentOS 7:

```
yum install pam_krb5 krb5-pkinit
<!--NeedCopy-->
```

RHEL 8:

```
yum install krb5-pkinit
<!--NeedCopy-->
```

Ubuntu 20.04, Ubuntu 18.04:

```
apt-get install libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

Debian 10.9:

```
apt-get install -y libpam-krb5 krb5-pkinit
<!--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:

```
authconfig --enablekrb5 --update
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:
>
> *[relación-operador] componente-regla ...*
>
> 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:

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM

    auth_to_local = RULE:[1:$1@$0]

    pkinit_anchors = FILE:<path where you install the root certificate
       >/certnew.pem

    pkinit_kdc_hostname = KDC.EXAMPLE.COM

    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature

    pkinit_eku_checking = kpServerAuth

  }

<!--NeedCopy-->
```

El archivo de configuración se parece a esto después de agregar la información sobre PKINIT.

```
CTXDEV.LOCAL = {
    kdc = ctx-ad.ctxdev.local
    auth_to_local = RULE:[1:$1@$0]
    pkinit_kdc_hostname = ctx-ad.ctxdev.local
    pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

Configurar la autenticación PAM Los archivos de configuración PAM indican los módulos que se usan para la autenticación PAM. Para agregar pam_krb5 como un módulo de autenticación, agregue

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

la siguiente línea al archivo **/etc/pam.d/smartcard-auth**:

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options
=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.
so
```

El archivo de configuración se parece al siguiente después de la modificación, si se utiliza SSSD.

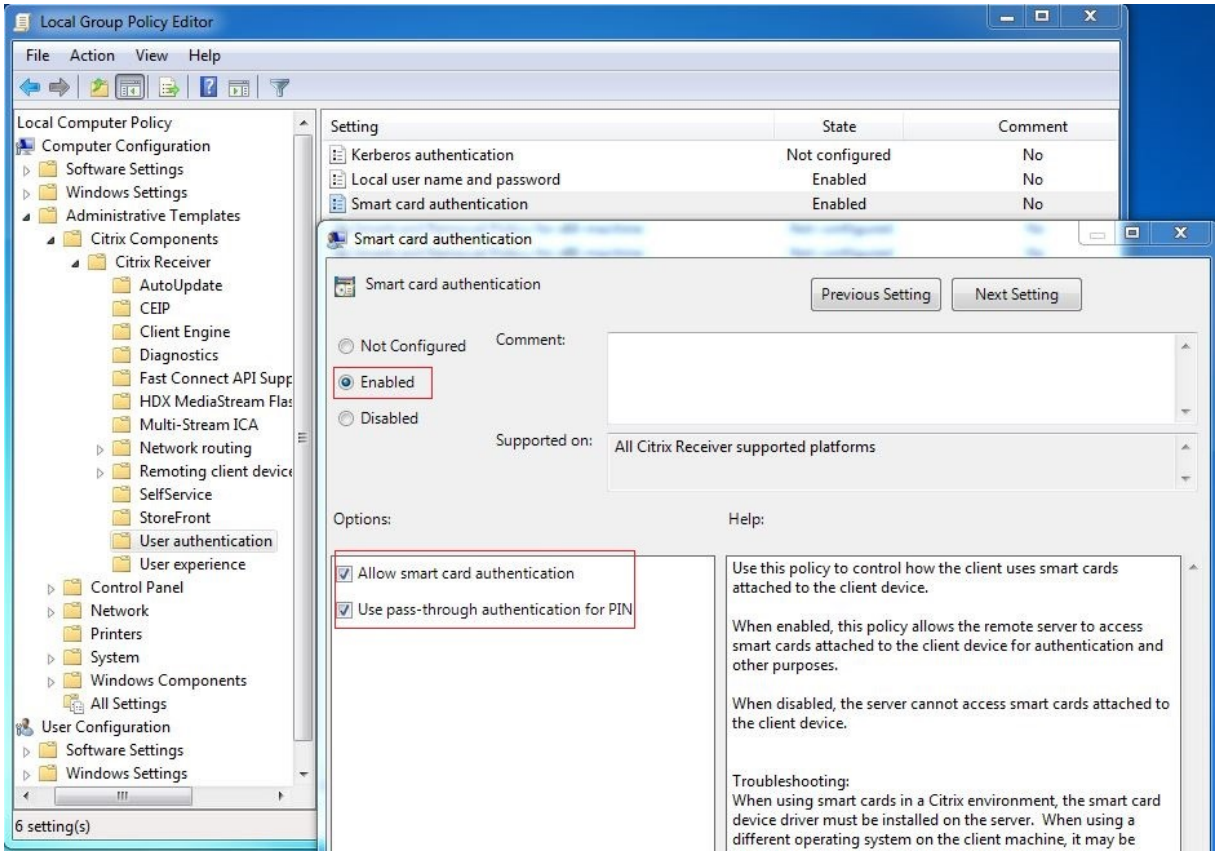
```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
account     required      pam_permit.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
#session     optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```

(Opcional) 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

```
[WFClient]
SmartCardCryptographicRedirection=On
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

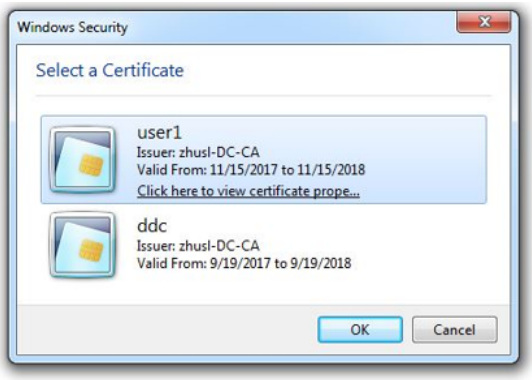
Inhabilitar el inicio de sesión con tarjeta inteligente rápida en el cliente Para inhabilitar el inicio de sesión con tarjeta inteligente rápida en el cliente, quite el parámetro **SmartCardCryptographicRedirection** del archivo default.ica del sitio StoreFront asociado.

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.

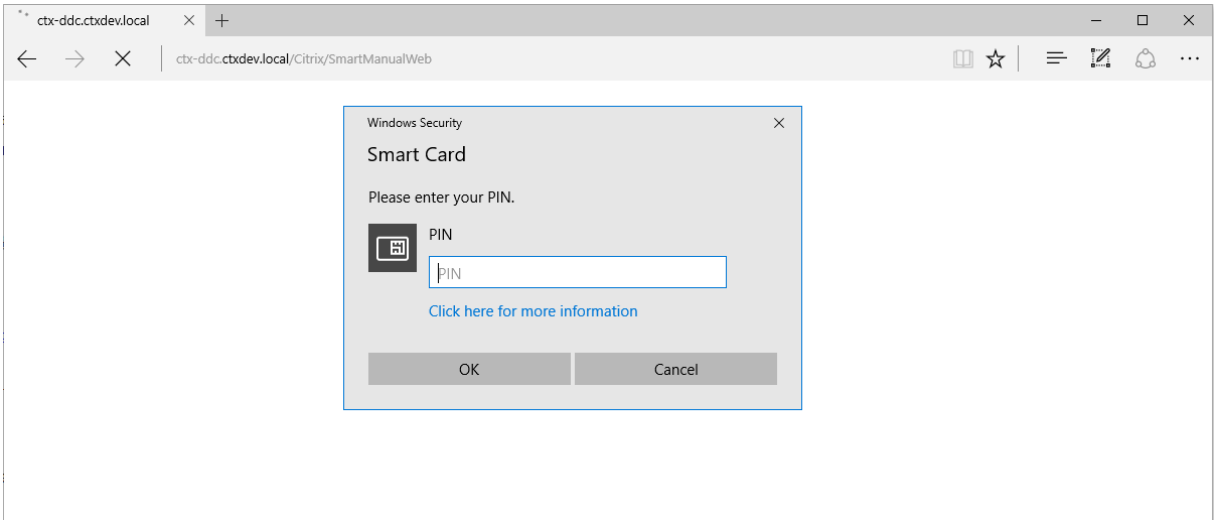
- En el caso de inicio SSO, inicia sesión automáticamente en StoreFront con el PIN y el certificado de la tarjeta inteligente guardados en la caché. Al iniciar una sesión de escritorio virtual Linux en StoreFront, el PIN se pasa al Linux VDA para la autenticación con tarjeta inteligente.
- En el caso 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

Actualmente, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Compatibilidad con otras tarjetas inteligentes y la biblioteca PKCS#11

Aunque solo figura la tarjeta inteligente OpenSC en su lista de compatibilidad, puede intentar utilizar otras tarjetas inteligentes y la biblioteca PKCS#11, ya que 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 `opensc-pkcs11.so` instancias con su biblioteca PKCS#11 .
2. Para establecer la ruta de su biblioteca PKCS#11 al Registro, ejecute el siguiente comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
   PKCS11LibPath" -d "PATH"
<!--NeedCopy-->
```

   donde **PATH** apunta a su biblioteca PKCS#11, como /usr/lib64/pkcs11/opensc-pkcs11.so
3. Inhabilite el inicio de sesión con tarjeta inteligente rápida en el cliente.

Sesiones sin autenticar de usuarios anónimos

September 25, 2023

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 **ncsd** 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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Establezca la variable de la memoria caché de **passwd** en **no** si está habilitado y, a continuación, reinicie el servicio **ncsd**. Es posible que tenga que volver a instalar Linux VDA después de cambiar esta configuración.

- **El botón de pantalla de bloqueo aparece con KDE en una sesión no autenticada**.

El menú y el botón de la pantalla de bloqueo están inhabilitados de forma predeterminada en una sesión no autenticada. Sin embargo, pueden aparecer en KDE. En KDE, para inhabilitar el menú y el botón de la pantalla de bloqueo de un usuario concreto, agregue las siguientes líneas al archivo de configuración **$Home/.kde/share/config/kdeglobals**. Por ejemplo:

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

Sin embargo, si el parámetro `KDE Action Restrictions` está configurado como inmutable en un archivo `kdeglobals` global como, por ejemplo, `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals`, la configuración del usuario no surte 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 la página KDE System Administration/Kiosk/Keys.

Archivo

July 6, 2022

Esta sección contiene estos temas:

- Copiar y pegar archivos
- Transferencia de archivos

Copiar y pegar archivos

July 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Los usuarios pueden copiar y pegar archivos entre una sesión y un cliente local mediante el menú contextual o los atajos de teclado. Esta función requiere Citrix Virtual Apps and Desktops 2006 o una versión posterior y la aplicación Citrix Workspace 1903 o una versión posterior para Windows.

Para copiar y pegar archivos correctamente, asegúrese de que:

- La cantidad de archivos no sea mayor que 20.
- El tamaño máximo de archivo no supere 200 MB.

Plataformas compatibles

La función de copiar y pegar archivos está disponible para:

- RHEL 7.9
- Ubuntu 18.04
- Debian 10

Directivas relevantes

Las siguientes directivas del portapapeles son relevantes para configurar la función. Para obtener más información acerca de las directivas del portapapeles, consulte Lista de directivas disponibles.

- Redirección del portapapeles del cliente
- Modo de actualización de la selección del portapapeles
- Modo de actualización de la selección primaria

> **Nota:**
>
> Para inhabilitar la función para copiar y pegar archivos, establezca la directiva **Redirección del portapapeles del cliente** en **Prohibida** en Citrix Studio.

Limitaciones

- No se admite la función de cortar contenido. Las solicitudes para cortar contenido se tratan como copias.
- No se admite la función de arrastrar y colocar contenido.
- No se admite la copia de directorios.

Transferencia de archivos

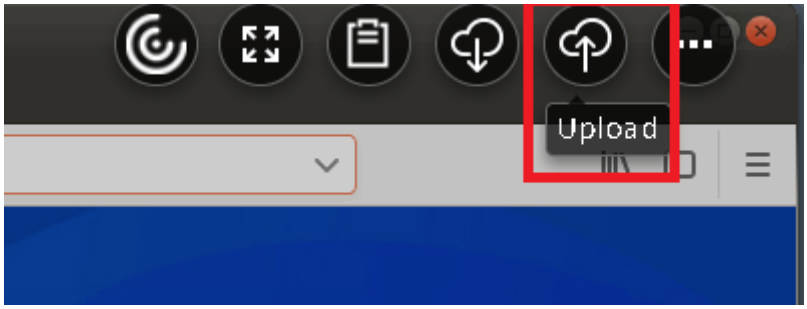
July 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 los escritorios y aplicaciones virtuales mediante la aplicación Citrix Workspace para HTML5 y para Chrome.

> **Nota:**
>
> La transferencia de archivos está disponible para la aplicación Citrix Workspace para HTML5 y para Chrome.

Dentro de las sesiones de escritorio y aplicación publicadas, la transferencia de archivos permite la carga y descarga de archivos entre Linux VDA y el dispositivo cliente. Para cargar archivos desde el dispositivo cliente en Linux VDA, haga clic en el icono **Cargar** de la barra de herramientas de la aplicación Citrix Workspace y seleccione el archivo deseado en los cuadros de diálogo de archivos. Para descargar archivos desde Linux VDA en el dispositivo cliente, haga clic en el icono **Descargar**. Puede agregar archivos durante la carga o descarga. Puede transferir hasta 100 archivos a la vez.



> **Nota:**
>
> Para cargar y descargar archivos entre Linux VDA y el dispositivo cliente, habilite la barra de herramientas de la aplicación Citrix Workspace.
> Puede utilizar una versión de la aplicación Citrix Workspace que le permita arrastrar y colocar archivos.

La descarga automática es una mejora para la transferencia de archivos. Los archivos que descargue o transfiera al directorio **Guardar en mi dispositivo** del VDA se transfieren automáticamente al dispositivo cliente.

> **Nota:**
>
> La descarga automática requiere que las directivas **Permitir transferencia de archivos entre escritorio y cliente** y **Descargar archivos desde el escritorio** se establezcan en **Permitido**.

Estos son algunos casos de uso para la descarga automática:

- Descargar archivos en **Guardar en mi dispositivo**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

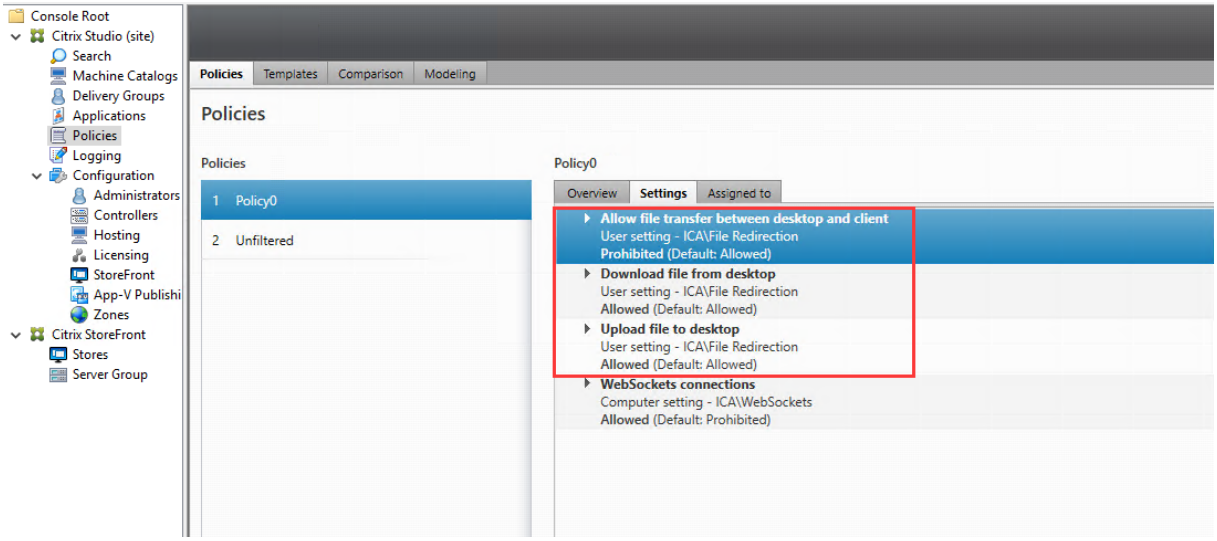
En las sesiones publicadas de aplicaciones de escritorio y explorador web, los archivos que descargue de sitios web se pueden guardar en el directorio **Guardar en mi dispositivo** del VDA para transferirlos automáticamente al dispositivo cliente. Para posibilitar la descarga automática, establezca el directorio de descargas predeterminado del explorador web de la sesión en **Guardar en mi dispositivo** y establezca un directorio de descargas local en el explorador web que ejecute la aplicación Citrix Workspace para HTML5 o para Chrome.

- Transferir archivos a, o copiarlos en, **Guardar en mi dispositivo**

  En las sesiones de escritorio publicadas, elija los archivos de destino y transfiéralos a, o cópielos en, el directorio **Guardar en mi dispositivo**, de manera que estén disponibles en el dispositivo cliente.

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.

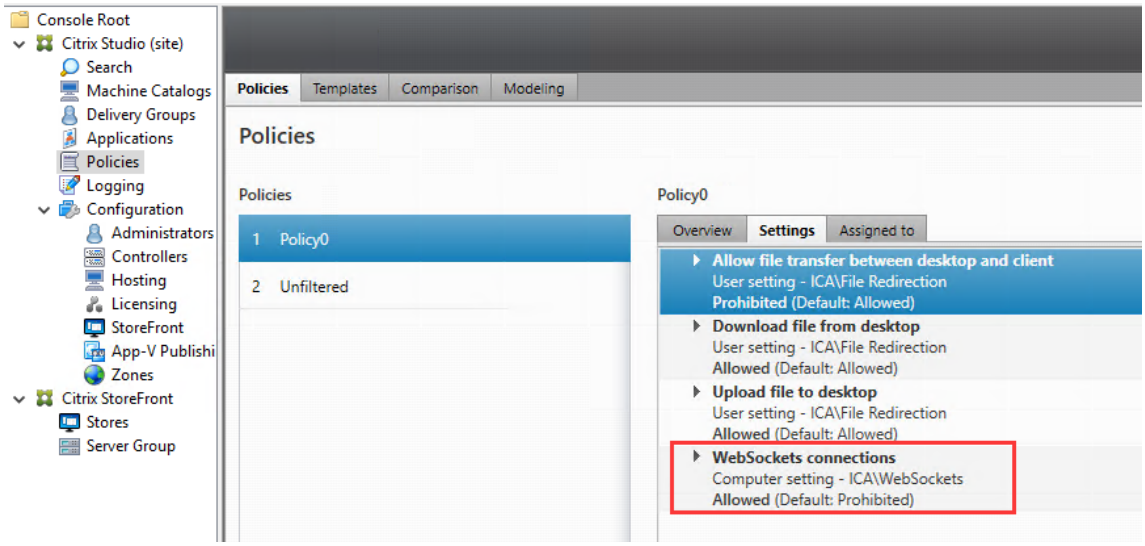
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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

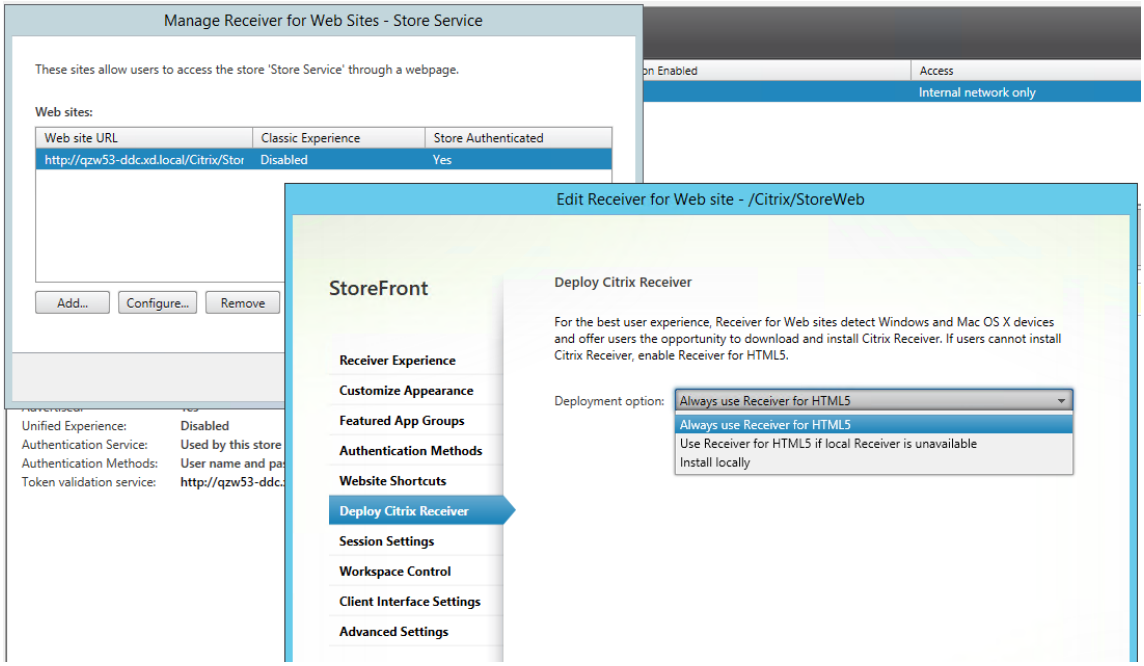
Para utilizar la función de transferencia de archivos a través de la aplicación Citrix Workspace para HTML5:

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Inicie una sesión de un escritorio virtual o de una aplicación de explorador web. Realice una o más transferencias de archivos entre Linux VDA y su dispositivo cliente.

Para utilizar la función de transferencia de archivos a través de la aplicación Citrix Workspace para Chrome:

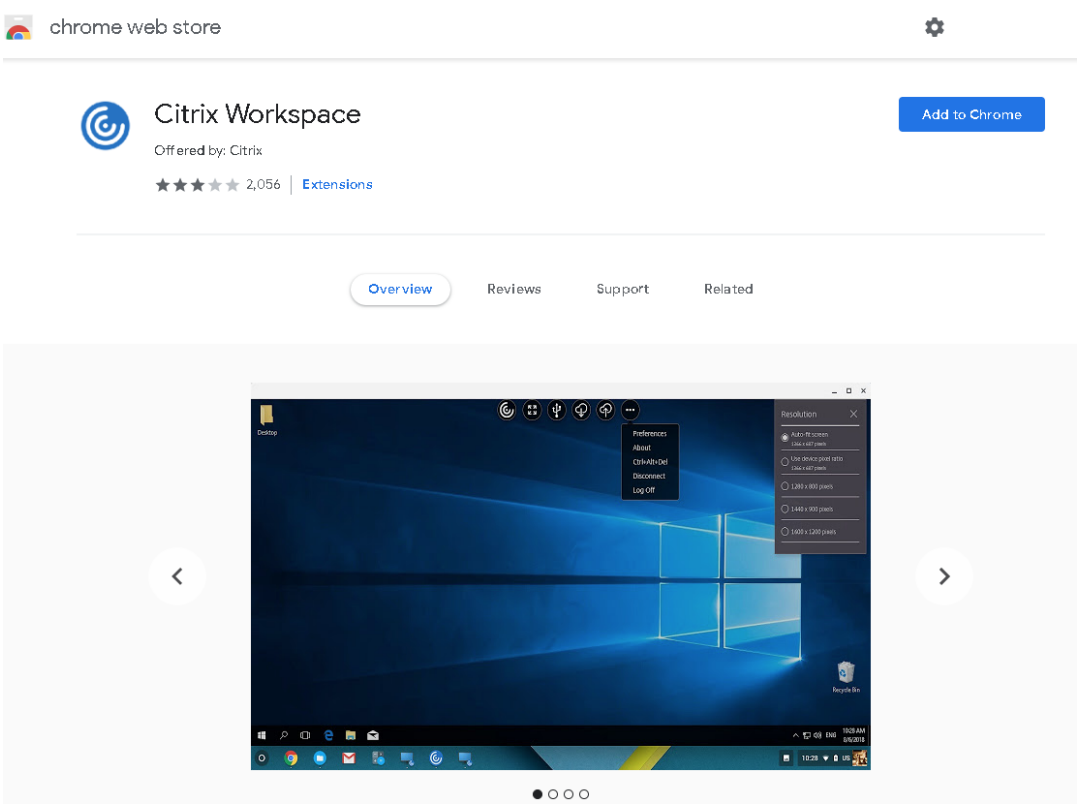
1. Habilite la transferencia de archivos mediante las directivas de transferencia de archivos que descritas anteriormente.
2. Adquiera la aplicación Citrix Workspace desde la tienda Chrome Web Store.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Haga clic en **Añadir a Chrome** para agregar la aplicación Citrix Workspace a Google Chrome.

3. Haga clic en la aplicación Citrix Workspace para Chrome en la página Aplicaciones 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 escritorio o aplicación virtuales. Realice una o más transferencias de archivos entre Linux VDA y su dispositivo cliente.

Gráficos

July 6, 2022

Esta sección contiene estos temas:

- Configuración y ajuste preciso de gráficos
- Pantalla compartida de HDX
- Gráficos 3D sin cuadrícula

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Marca de agua en sesiones basada en texto
- Presentación progresiva de Thinwire

Configuración y ajuste de gráficos

November 21, 2023

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

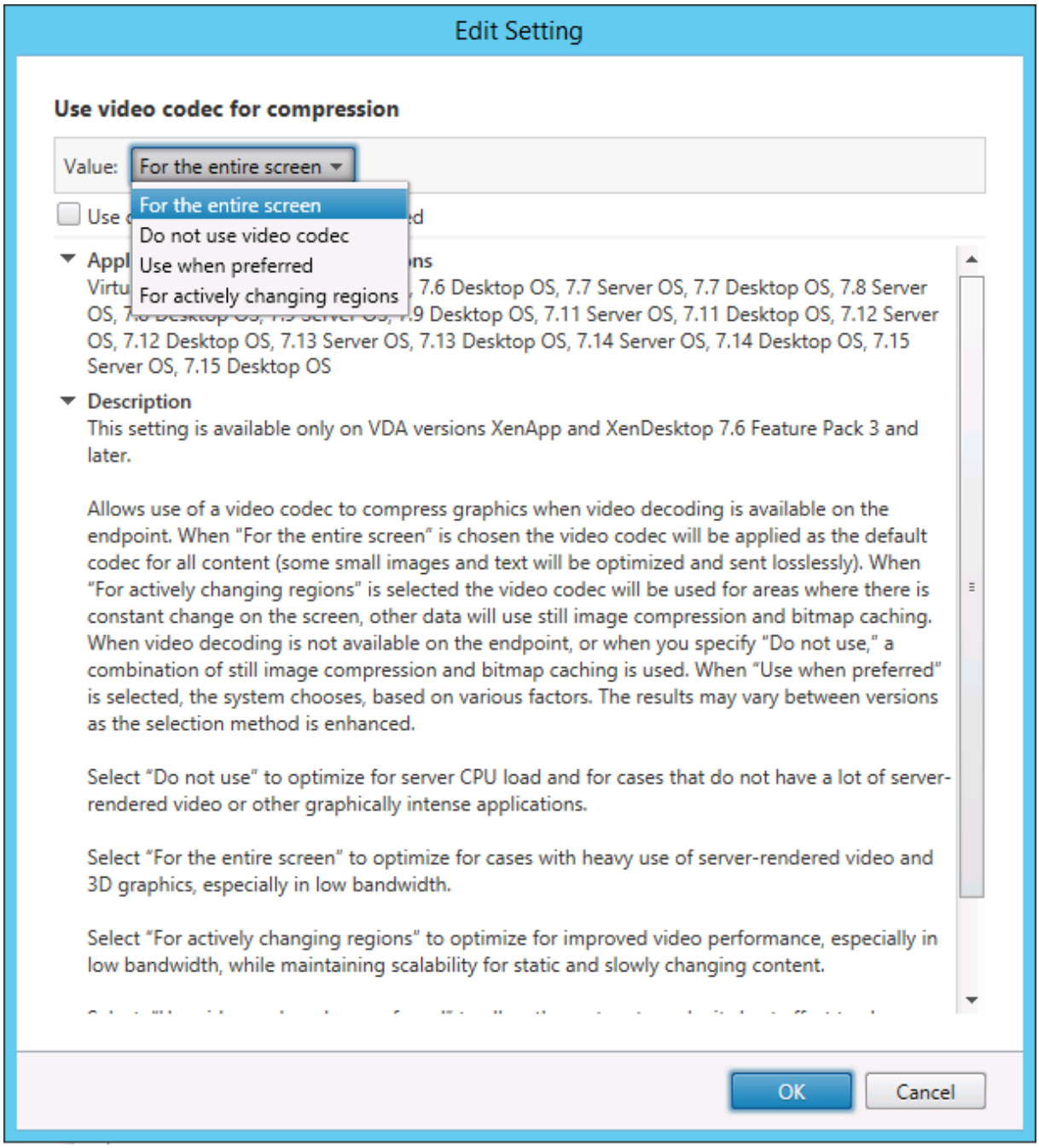
Thinwire es la tecnología de pantallas remotas que se utiliza en Linux Virtual Delivery Agent. Esta tecnología permite que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí.

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. Esto garantiza que 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**. La tecnología de pantalla adaptable de Thinwire identifica imágenes en movimiento (vídeo, 3D en movimiento). Utiliza H.264 solo en aquella parte de la pantalla donde se mueva la imagen. El 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. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

de gráficos. Para habilitar la codificación por hardware H.264 para esta funcionalidad, consulte Uso selectivo del códec de hardware H.264 para áreas en cambio constante.



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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Calidad visual**

Procesamiento paralelo

Thinwire puede mejorar la cantidad de fotogramas por segundo (FPS) al paralelizar ciertas tareas, con la sobrecarga de un consumo general de CPU ligeramente mayor. Esta función está inhabilitada de forma predeterminada. Para habilitar esta función, ejecute este comando en el VDA:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   ParallelProcessing" -d "0x00000001" --force
<!--NeedCopy-->
```

Uso selectivo del códec de hardware H.264 para áreas en cambio constante

A partir de la versión 2204, Linux VDA admite el uso selectivo del códec de hardware H.264 para áreas en cambio constante. Esta funcionalidad reduce la carga de CPU en la compresión de vídeo con ayuda de hardware y mejora la calidad de la imagen y el número de fotogramas por segundo (FPS). Para habilitar esta funcionalidad, haga lo siguiente:

1. Habilite la directiva **Usar codificación por hardware para códec de vídeo**.
2. Habilite la directiva **Usar códec de vídeo para compresión** y seleccione **Para áreas en cambio constante**.

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.

Los siguientes clientes admiten Selective H.264:

- Citrix Receiver para Windows 4.9 a 4.12
- Citrix Receiver para Linux 13.5 a 13.10
- Aplicación Citrix Workspace para Windows 1808 y versiones posteriores
- Aplicación Citrix Workspace 1808 para Linux y versiones posteriores

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 4.10 a 4.12
- Aplicación Citrix Workspace para Windows 1808 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 las sesiones recurren 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**.

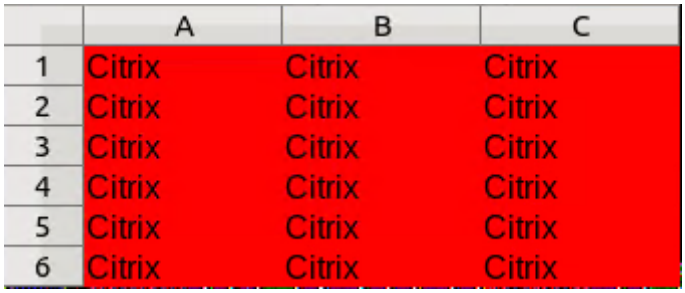
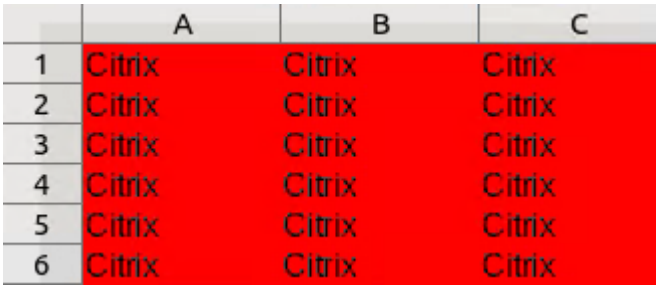
Para habilitar la codificación por hardware H.265 en su dispositivo cliente, consulte Codificación de vídeo H.265.

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 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, o 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

YUV444	YUV420
	

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 los fotogramas codificados en consecuencia. 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    MaxBitRatePercent" -d "100" --force
<!--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.

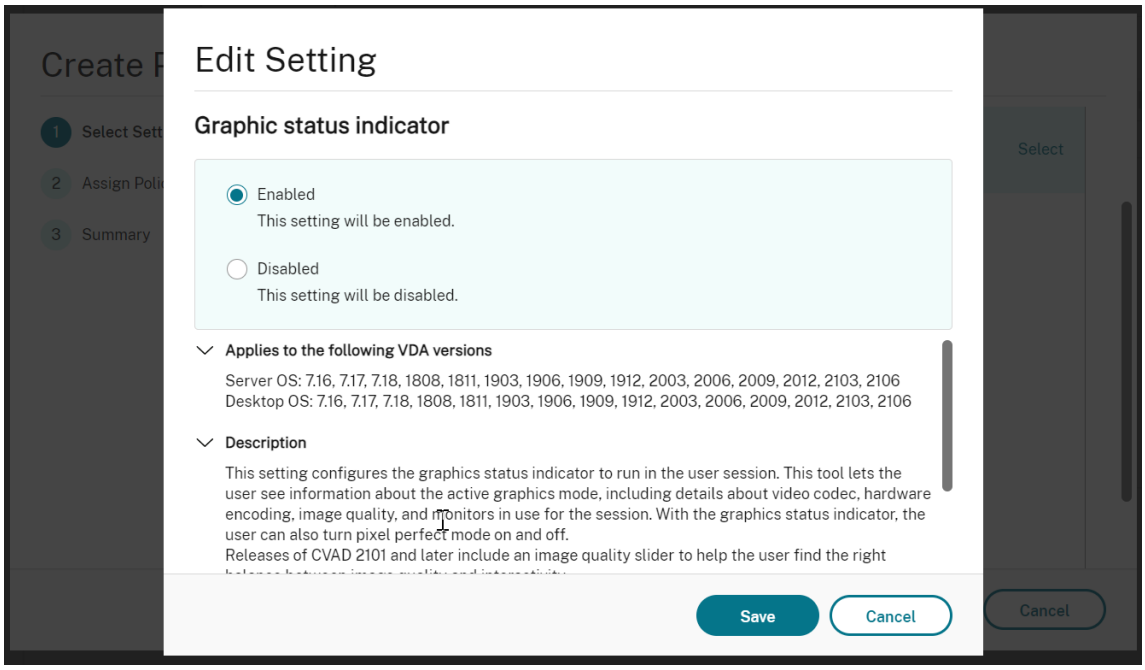
Para obtener información sobre la configuración de la compatibilidad con varios monitores en Linux VDA, consulte CTX220128.

Control deslizante de calidad gráfica

Hemos incluido un control deslizante de calidad gráfica en la herramienta Indicador de estado de gráficos que se ejecuta en las sesiones virtuales de Linux. El control deslizante ayuda a encontrar un buen equilibrio entre calidad de imagen e interactividad.

Para utilizar el control deslizante, siga estos pasos:

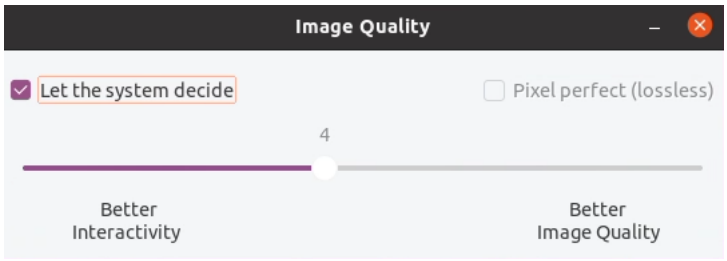
1. Habilite la directiva **Indicador de estado de gráficos** en Citrix Studio.



2. Abra el terminal y ejecute el comando `ctxslider`. Aparecerá la interfaz de usuario del control deslizante.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Si ha establecido la directiva **Calidad visual** en **Siempre sin pérdida** o **Gradual sin pérdida**, no se muestra la interfaz de usuario del control deslizante.



Ahora están disponibles las siguientes opciones:

- Para cambiar la calidad de la imagen, mueva el control deslizante. El control deslizante admite un intervalo de 0 a 9.
- Para utilizar la configuración definida por el sistema, seleccione **Dejar que el sistema decida**.
- Para cambiar al modo sin pérdida, selecciona **Píxel perfecto**.

Solución de problemas

Compruebe el modo de gráficos en uso

Ejecute este comando para comprobar qué modo de gráficos se está utilizando (**0** significa TW+; **1** significa códec de vídeo para la pantalla entera):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
<!--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 este comando para comprobar si H.264 se está utilizando (**0** significa que no se usa; **1** significa que sí se usa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 este comando para comprobar si H.265 en pantalla completa se está utilizando (**0** significa que no se usa; **1** significa que sí se usa):

```
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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 este comando (**0** significa que no se usa; **1** significa que sí se usa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
<!--NeedCopy-->
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

Otra forma de averiguarlo es usar el comando **nvidia-smi**. Los resultados son similares a lo siguiente si se utiliza la codificación por hardware:

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28         |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
                     N/A |
| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|

|    0      2164  C+G   /usr/local/bin/ctxgfx
   106MiB |
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
|    0      2187    G   Xorg
    85MiB |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Compruebe si el controlador de gráficos NVIDIA GRID se ha instalado correctamente

Para verificar si el controlador de gráficos NVIDIA GRID se ha instalado correctamente, ejecute **nvidia-smi**. El resultado es similar a:

```
+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70         |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  Tesla M60           Off  | 0000:00:05.0     Off |
                    Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|

|  No running processes found
                                    |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Establezca la configuración correcta para la tarjeta:

`etc/X11/ctx-nvidia.sh`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
[root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
   disable_vnc=1
<!--NeedCopy-->
```

Para versiones de Citrix Hypervisor anteriores a 8.1:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
<!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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)`'.

Pantalla compartida de HDX

July 6, 2022

Información general

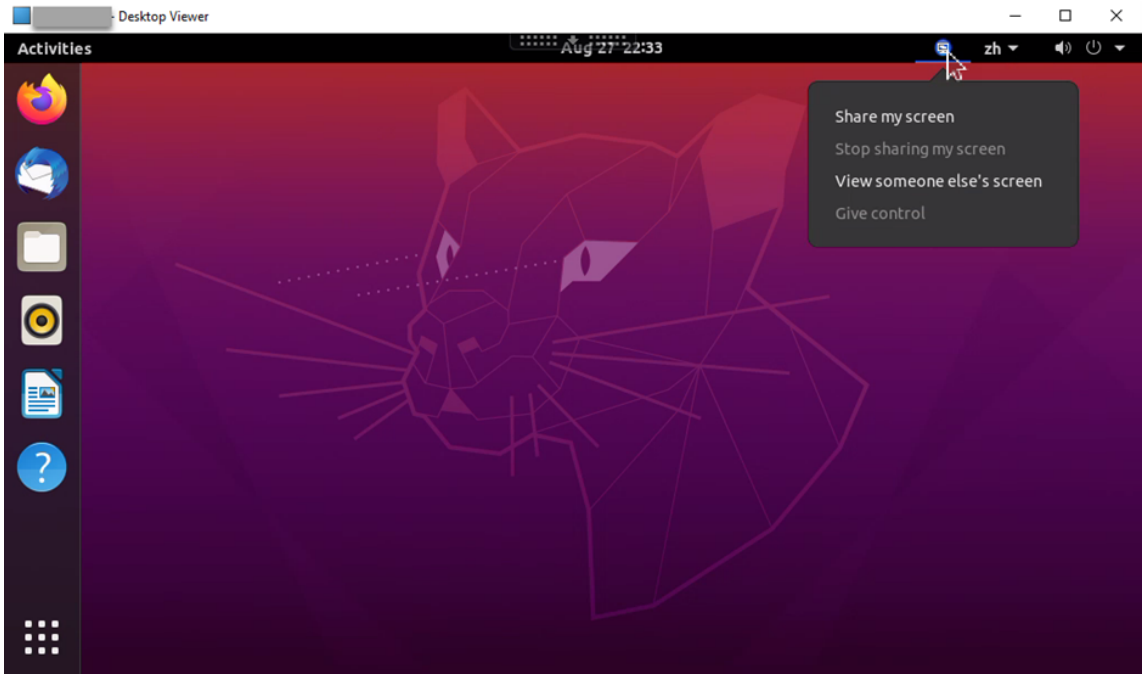
Linux VDA le permite compartir la pantalla de su escritorio virtual con usuarios de una sesión en otros escritorios virtuales.

El siguiente ejemplo le guiará a través del procedimiento de compartir una pantalla y ver la pantalla de otro usuario.

Para compartir una pantalla:

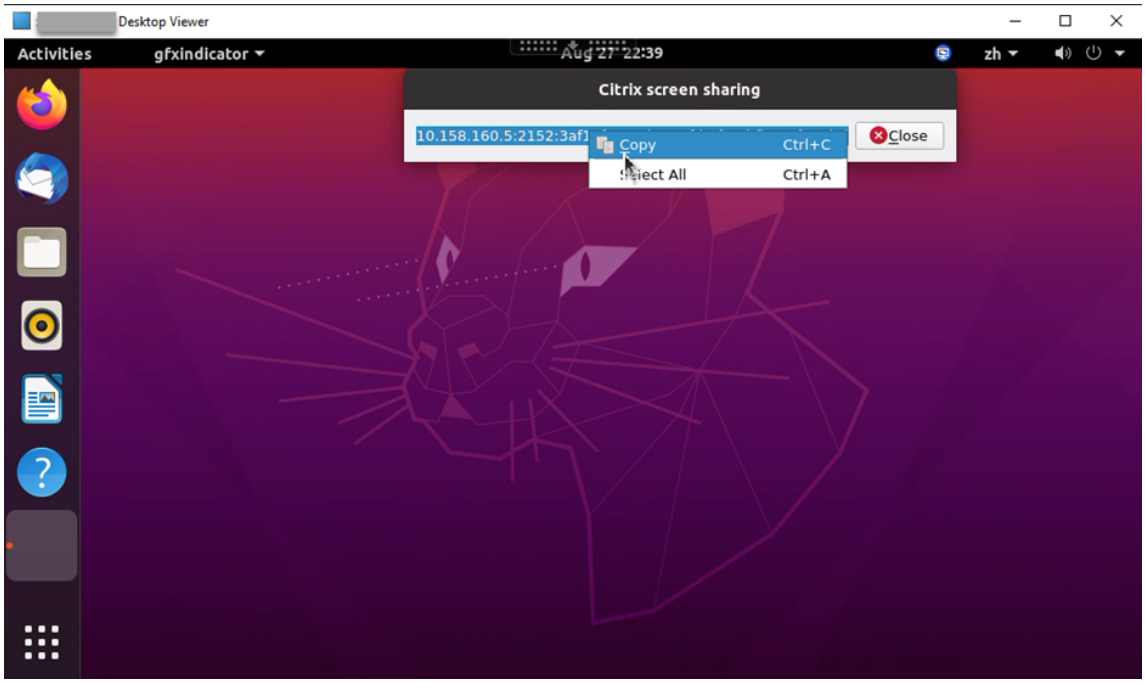
1. En el área de notificaciones de su escritorio virtual, haga clic en el icono de **compartir pantalla** y seleccione **Compartir mi pantalla**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Haga clic en **Copiar y Cerrar**.

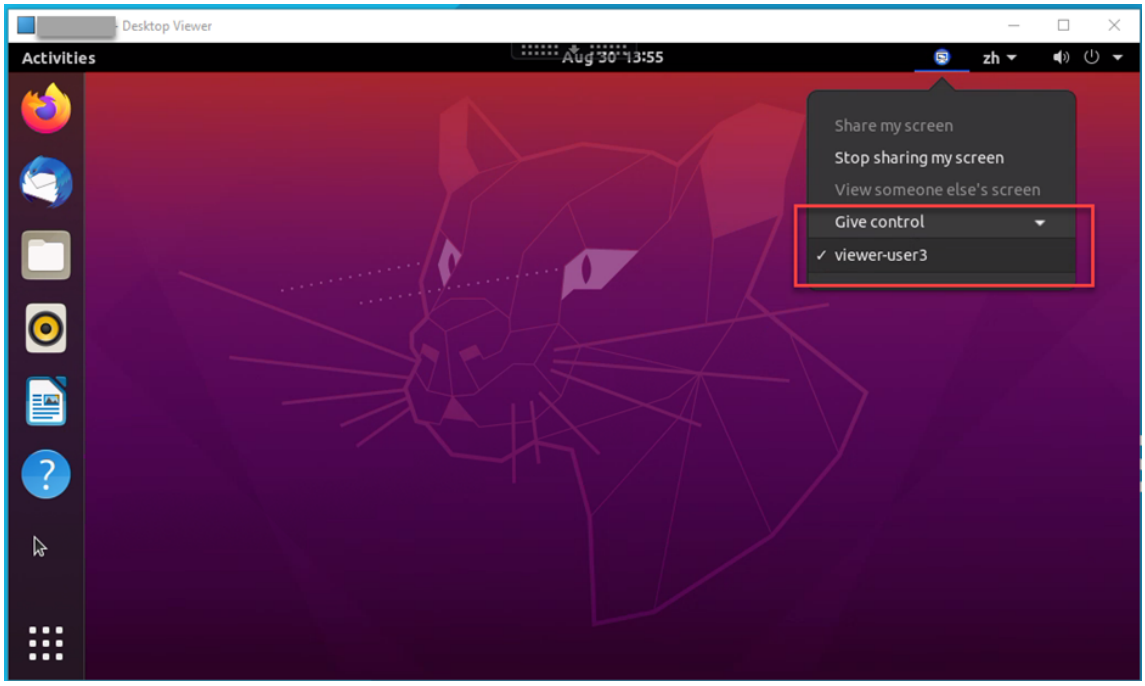
   El código actual para compartir pantalla persiste hasta que detenga y reinicie el uso compartido de la pantalla.



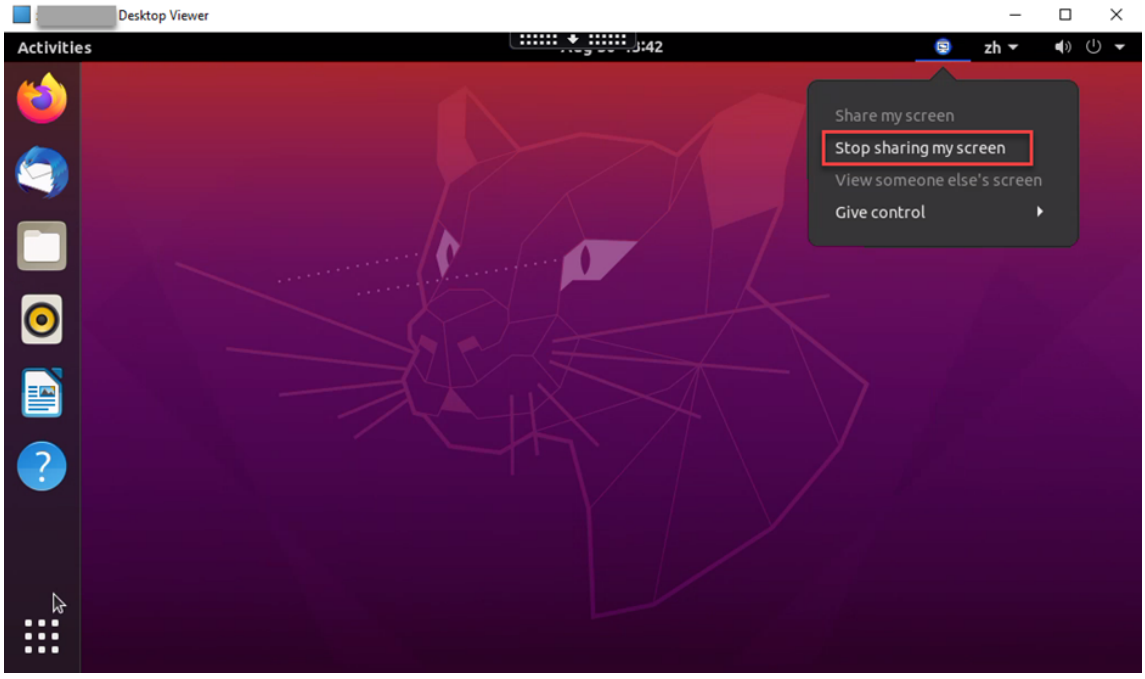
> **Sugerencia:**
>
> Mientras comparte la pantalla, hay un borde rojo a su alrededor, lo que indica que la pantalla se está compartiendo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Comparta el código copiado con los usuarios de la sesión de otros escritorios virtuales con los que quiera compartir la pantalla.
4. Para permitir que un participante controle la pantalla, seleccione **Dar control** y, a continuación, el nombre del participante. Para dejar de dar control, borre el nombre del participante.



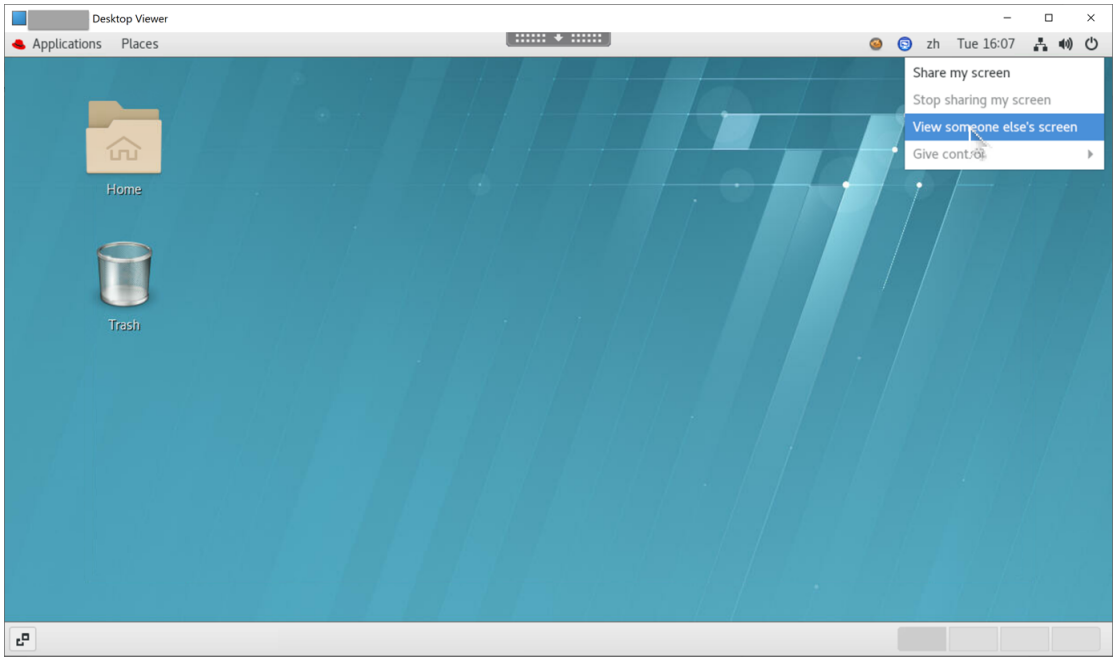
5. Para dejar de compartir la pantalla, seleccione **Dejar de compartir mi pantalla**.



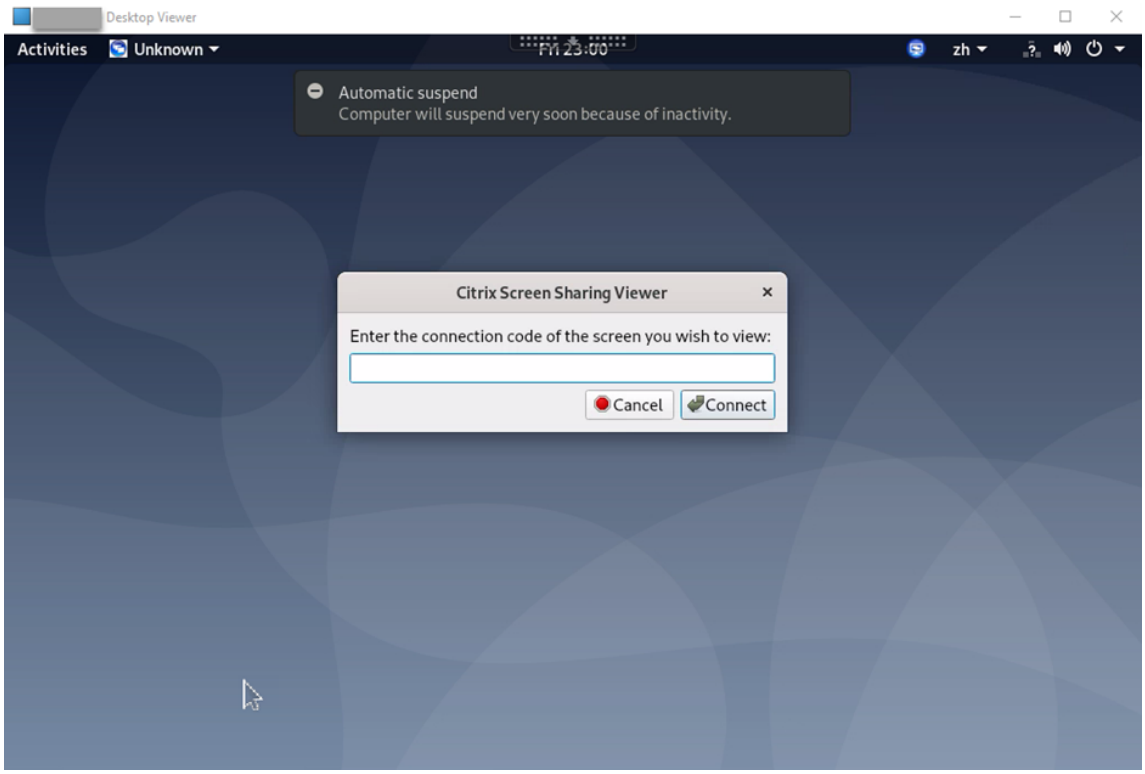
Para ver la pantalla de otro participante:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. En el área de notificaciones de su escritorio virtual, haga clic en el icono de **pantalla compartida** y seleccione **Ver la pantalla de otra persona**.

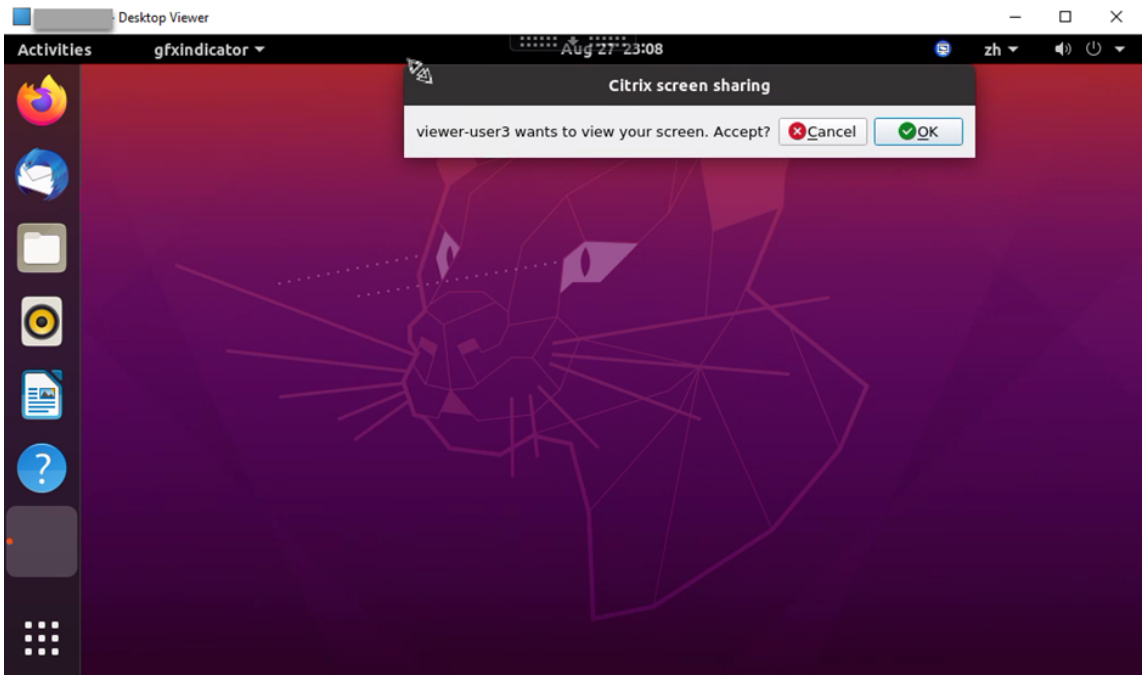


2. Introduzca el código de conexión de la pantalla que quiere ver y, a continuación, haga clic en **Conectar**.



3. Espere a que el usuario que comparte la pantalla acepte su solicitud. Por ejemplo:

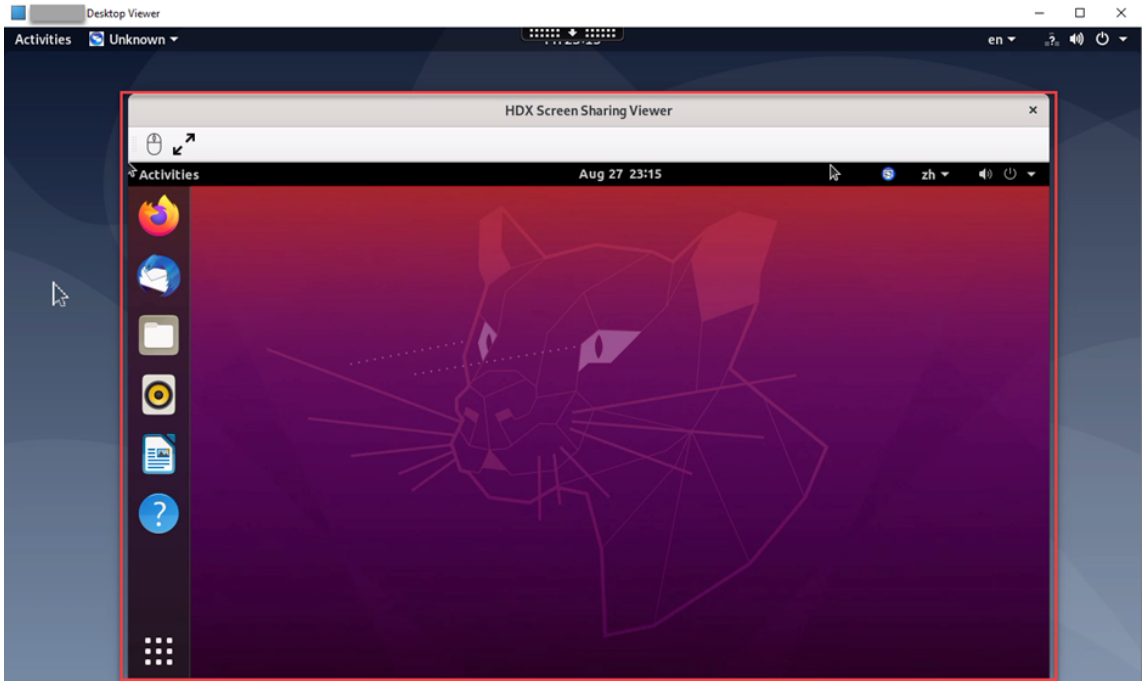
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Sugerencia:**
>
> - En el lado del usuario que comparte la pantalla, el sistema Linux envía una notificación de su solicitud.
> - Si dicho usuario no acepta su solicitud en 30 segundos, la solicitud caduca y aparece un mensaje.

4. Una vez que el usuario que comparte la pantalla haya aceptado su solicitud tras hacer clic en **Aceptar**, la pantalla compartida aparecerá en Desktop Viewer. Se conecta como espectador con un nombre de usuario asignado automáticamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

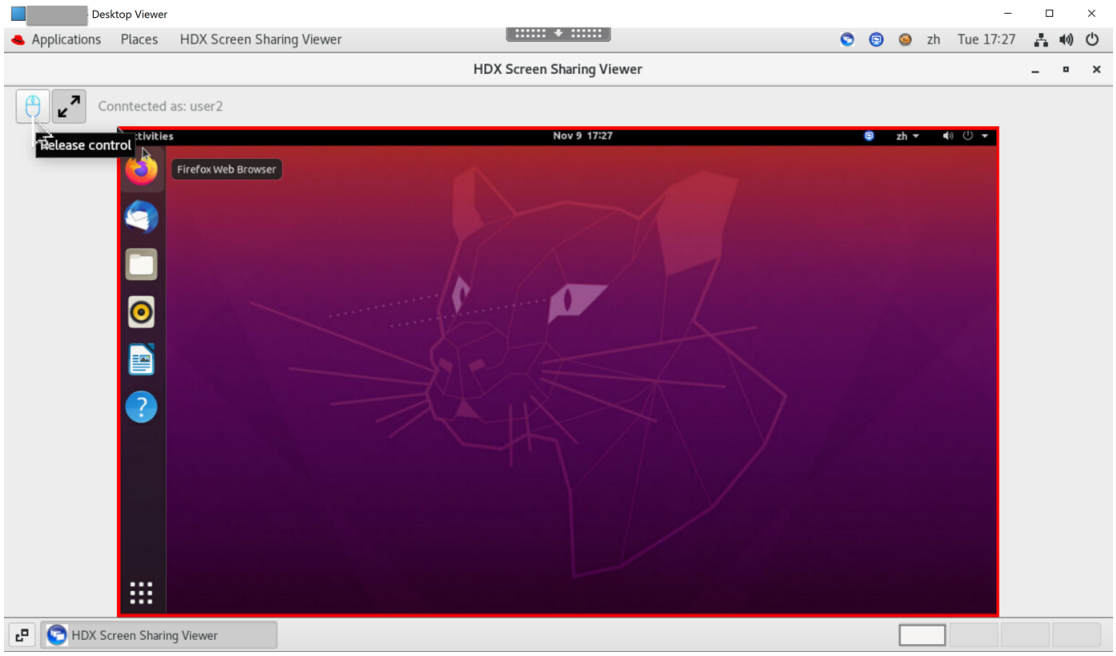


5. Para solicitar el control sobre la pantalla compartida, haga clic en el icono del mouse situado en la esquina superior izquierda.

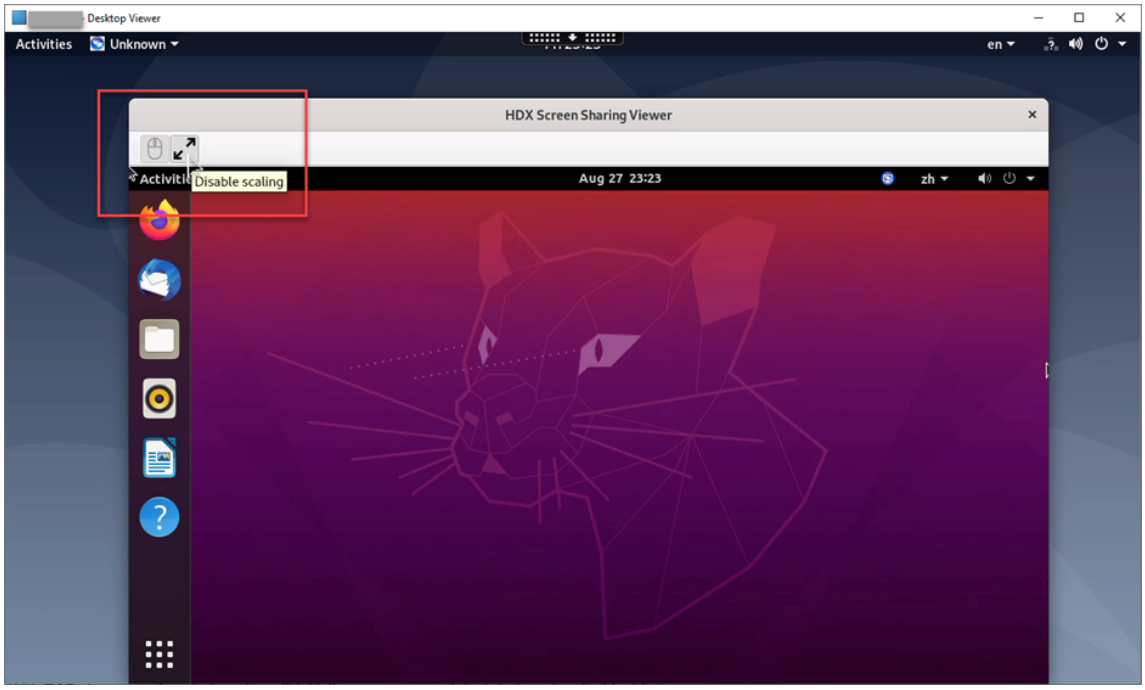
   > **Sugerencia:**
   >
   > - Si el usuario que comparte la pantalla no acepta su solicitud en 30 segundos, la solicitud caduca.
   > - Solo un espectador tiene permiso para controlar una pantalla compartida.

   Haga clic de nuevo en el icono del mouse para liberar el control de la pantalla compartida.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Para inhabilitar el escalado de pantalla o escalar al tamaño de la ventana, haga clic en el icono situado junto al icono del mouse.



Configuración

La función de uso compartido de pantalla está inhabilitada de forma predeterminada. Para habilitarla, complete los siguientes parámetros:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

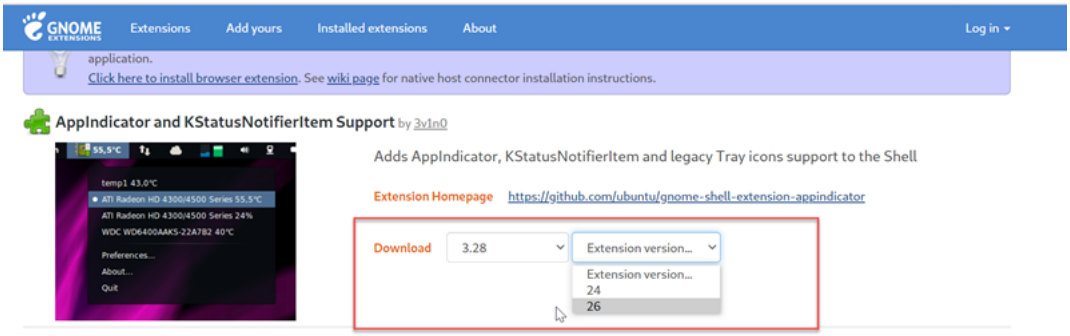
1. Habilite la directiva de indicador de estado de gráficos en Citrix Studio.
2. Para Citrix Virtual Apps and Desktops 2112 y versiones posteriores, habilite la directiva **Uso compartido de la pantalla** en Citrix Studio.
3. (Opcional) Para Citrix Virtual Apps and Desktops 2109 y versiones anteriores, habilite el uso compartido de la pantalla en Linux VDA mediante este comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -v "
   EnableScreenSharing" -d "0x00000001"
<!--NeedCopy-->
```

4. Permita los puertos 52525-52625 en su firewall.
5. (Opcional) Si utiliza RHEL 8.x o SUSE 15.x instalado con GNOME, instale una extensión compatible para el shell de GNOME a fin de habilitar la compatibilidad con AppIndicator:

   a) Ejecute el comando `gnome-shell --version` para comprobar la versión del shell de GNOME.

   b) Descargue una extensión compatible para el shell GNOME desde https://extensions.gnome.org/extension/615/appindicator-support . Por ejemplo, si la versión de shell es 3.28, puede seleccionar 24 o 26 para la versión de la extensión.



   c) Extraiga el paquete descargado. Compruebe que el valor **"uuid"** del archivo **metadata.json** del paquete está establecido en **appindicatorsupport@rgcjonas.gmail.com**.

   d) Ejecute el comando `mv` para mover el directorio **appindicatorsupport@rgcjonas.gmail.com** a la ubicación `/usr/share/gnome-shell/extensions/`.

   e) Ejecute el comando `chmod a+r metadata.json` para hacer el archivo **metadata.json** legible para otros usuarios.

> **Sugerencia:**
>
> De forma predeterminada, el archivo **metadata.json** del directorio **appindicatorsupport@rgcjonas.gmail.com** solo puede leerlo el usuario root. Para habilitar el uso compartido de pantalla, haga el archivo **metadata.json** legible también para

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> otros usuarios.

f) Instale GNOME Tweaks.

g) En el entorno de escritorio, pulse las teclas `Alt`+`F2`, `r` y `Enter` en secuencia o ejecute el comando `killall -SIGQUIT gnome-shell` para volver a cargar el shell de GNOME.

h) En el entorno de escritorio, ejecute GNOME Tweaks y, a continuación, habilite **KStatusNotifierItem/AppIndicator Support** en la herramienta Tweaks.

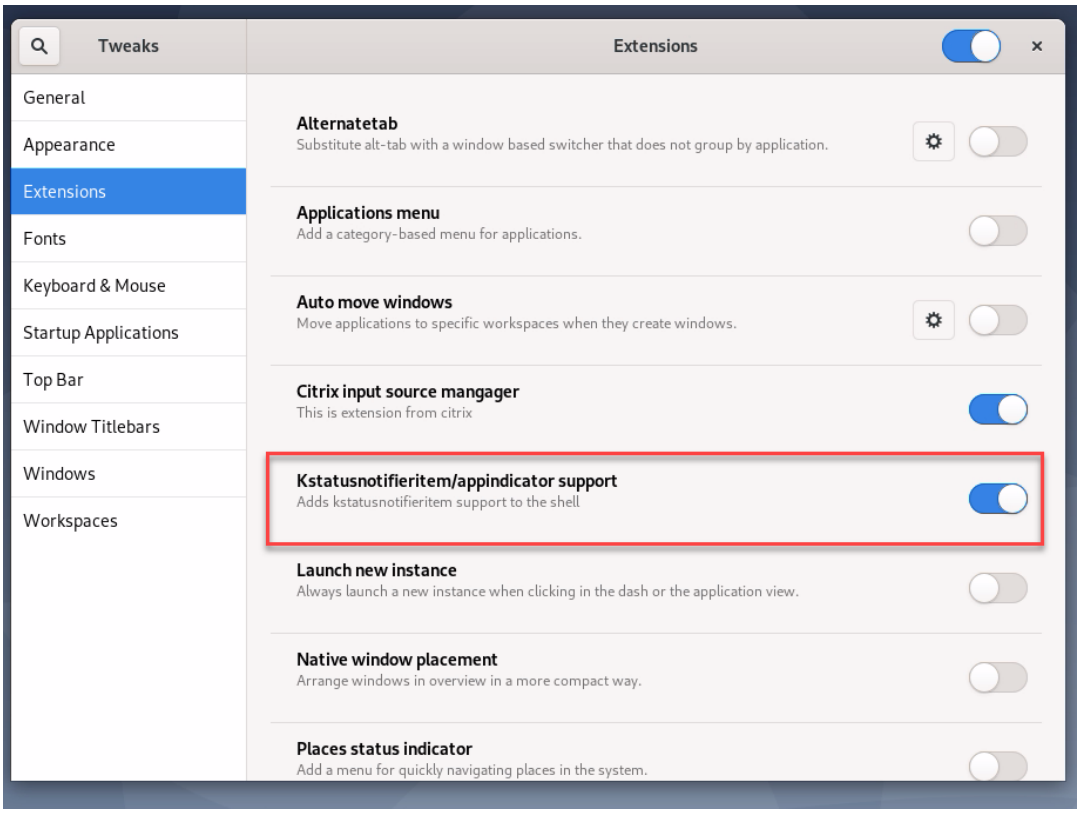
6. (Opcional) Si utiliza Debian 10 instalado con GNOME, complete los siguientes pasos para instalar y habilitar los iconos de la bandeja del sistema de GNOME:

a) Ejecute el comando `sudo apt install gnome-shell-extension-appindicator`. Puede que tenga que cerrar la sesión y reiniciarla para que GNOME vea la extensión.

b) Busque Tweaks en la pantalla **Activities**.

c) Seleccione **Extensions** en la herramienta Tweaks.

d) Habilite **Kstatusnotifieritem/appindicator support**.



Consideraciones

- La función de uso compartido de pantalla no es compatible con el códec de vídeo H.265.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- La función de uso compartido de pantalla no está disponible para las sesiones de aplicación.
- Los usuarios de sesiones de escritorio pueden, de forma predeterminada, compartir la pantalla de sus sesiones con hasta 10 usuarios. El máximo de usuarios se puede configurar mediante `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-v "ScreenSharingViewerMaxNum"-d <hex_value>`. Al alcanzar el máximo, aparece un mensaje cuando los usuarios intentan aceptar solicitudes de conexión adicionales.

Tarjetas gráficas que no son de GPU virtuales

March 11, 2024

Las tarjetas gráficas que no son de GPU virtuales se refieren a tarjetas gráficas que no admiten la solución de GPU virtual (vGPU) de NVIDIA. Este artículo proporciona información sobre el uso de tarjetas gráficas que no son de GPU virtuales.

Requisitos previos

Para usar tarjetas gráficas que no sean de GPU virtuales, 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

Modificar los archivos de configuración de Xorg

Para tarjetas gráficas NVIDIA Si utiliza un controlador NVIDIA, los archivos de configuración se instalan y se configuran automáticamente.

Para otras tarjetas gráficas Debe modificar los cuatro archivos de configuración de las plantillas que se instalaron en `/etc/X11/`:

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 proporcionada por el fabricante de tarjetas para obtener información sobre la configuración. Se puede generar un archivo de configuración nativo. Verifique que su tarjeta funciona en un entorno local con el archivo de configuración nativo cuando no está ejecutando una sesión 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 gráficos que no son de GPU virtuales

La función de gráficos que no son de GPU virtuales está inhabilitada de forma predeterminada. Puede ejecutar el siguiente comando para habilitarla estableciendo el valor de 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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Marca de agua en sesiones basada en texto

July 6, 2022

Las marcas de agua de la sesión basadas en texto ayudan a disuadir del robo de datos y rastrear los datos robados. La información rastreable aparece en los escritorios de sesiones como un elemento de disuasión para quienes usan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto. La capa de texto se muestra en la pantalla de toda la sesión sin cambiar el contenido del documento original.

> **Importante:**
>
> La marca de agua basada en texto de la sesión no es una función de seguridad. Esta solución no impide por completo el robo de datos, pero ofrece cierto nivel de disuasión frente al robo de datos y rastreabilidad de los datos robados. No garantizamos la rastreabilidad completa de la información cuando se utiliza esta funcionalidad. Sin embargo, le recomendamos que combine esta funcionalidad con otras soluciones de seguridad, según corresponda.

La marca de agua de la sesión es texto y se aplica a la sesión que se entrega al usuario. La marca de agua de la sesión contiene información para rastrear datos robados. La información más importante es la identidad del usuario que inició la sesión en la que se realizó la captura de la pantalla. Para rastrear la filtración de datos de manera más efectiva, incluya otra información (como la hora de conexión y la dirección del protocolo de Internet del servidor o del cliente).

Para ajustar la experiencia del usuario, use las configuraciones de directiva de Marca de agua para definir la ubicación y la apariencia de la marca de agua en la pantalla.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Limitaciones

- Las marcas de agua de sesión no se admiten en las sesiones en las que se utiliza la redirección de contenido del explorador. Para utilizar la funcionalidad de marca de agua de sesión, asegúrese de que la redirección de contenido del explorador esté inhabilitada.
- No se admite la marca de agua de la sesión, y esta no aparece si la sesión se ejecuta en modos de aceleración de hardware en pantalla completa, con codificación H.264 o H.265, con los controladores NVIDIA antiguos. (En este caso, NvCaptureType se establece en 2 en el registro).
- Las marcas de agua no son visibles para el remedo de sesiones.
- Si se presiona la tecla Imprimir pantalla, la pantalla capturada en el lado del VDA no incluirá las marcas de agua. Le recomendamos que tome las medidas oportunas para evitar que se copien las imágenes capturadas.

Presentación progresiva de Thinwire

July 6, 2022

La interactividad de la sesión puede degradarse en conexiones de latencia baja o poco ancho de banda. Por ejemplo, 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 a un modo de actualización progresiva de forma predeterminada en cualquiera de los siguientes casos:

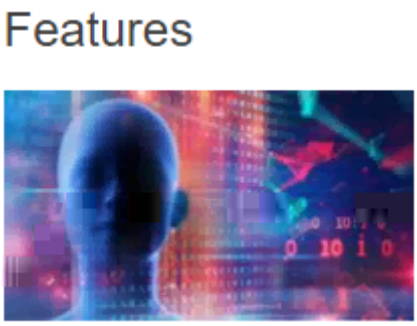
- El ancho de banda disponible es inferior a 2 Mbps.
- La latencia de red supera los 200 ms.

En este modo:

Por ejemplo, en el siguiente gráfico, donde el modo de actualización progresiva está activo, las letras **F** y **e** tienen artefactos azules, y la imagen está muy comprimida. Este 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplay" -d "<value>" --force
<!--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:

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
<!--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

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SOFTWARE
    \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplayLatencyThreshold" -d "<value>" --force
<!--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.

Teclado

July 6, 2022

Esta sección contiene estos temas:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- IME del cliente
- Sincronización de la interfaz de usuario IME del cliente
- Sincronización de la distribución de teclado dinámico
- Teclado en pantalla
- Compatibilidad para entrada de texto en varios idiomas

Editor de métodos de entrada (IME) de cliente

July 6, 2022

Información general

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.

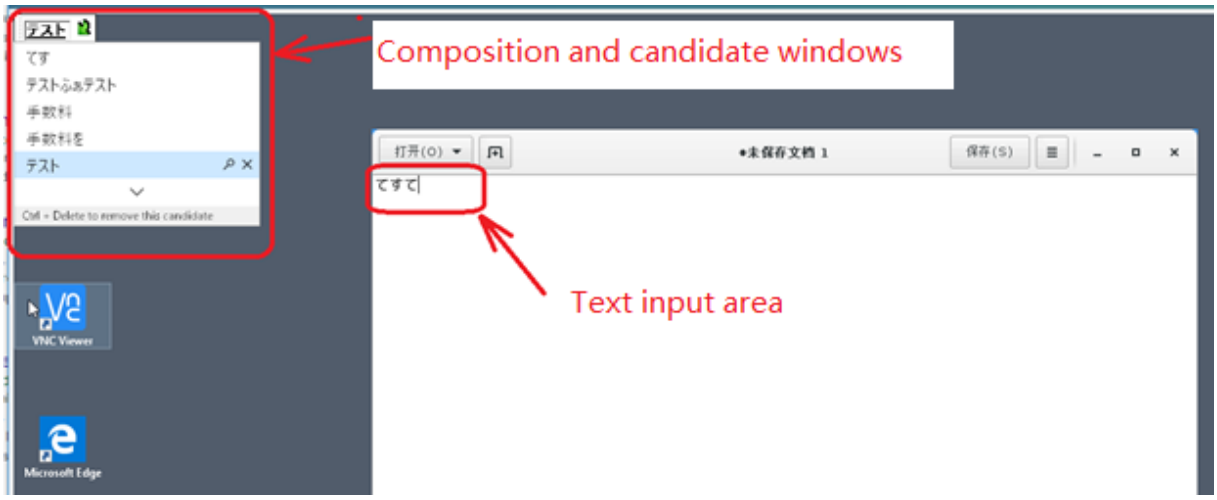
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sincronización de la interfaz de usuario IME del cliente

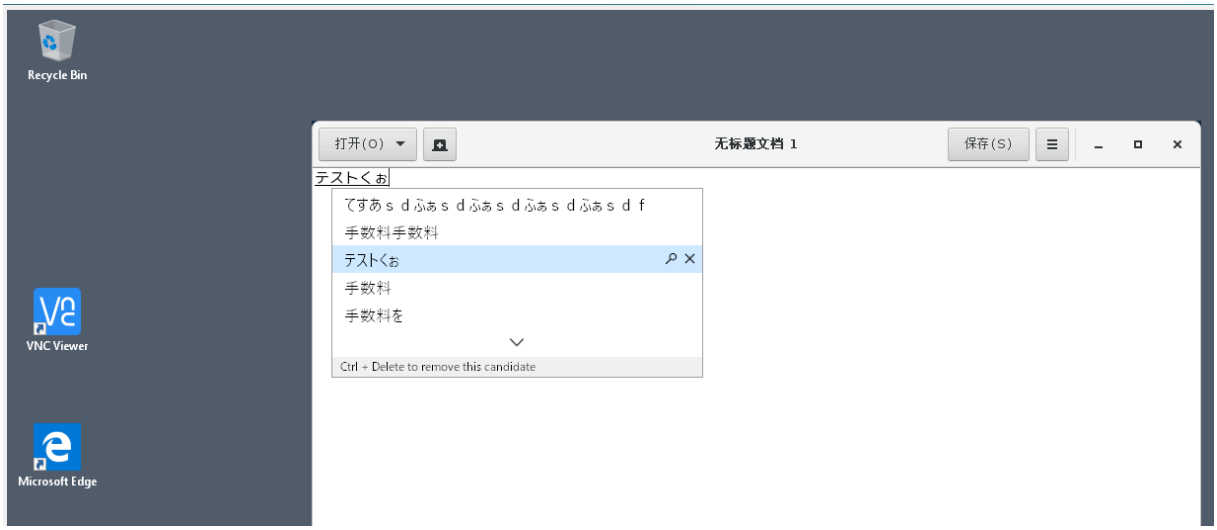
July 6, 2022

Información general

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:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Requisitos previos para utilizar la función

1. Habilite Intelligent Input Bus (`IBus`) en Linux VDA. Para obtener información sobre cómo habilitar `IBus` en un sistema operativo Linux, consulte la documentación del proveedor del sistema operativo. Por ejemplo:
   - Ubuntu: https://help.ubuntu.com/community/ibus
   - CentOS, RHEL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods
   - Debian: https://wiki.debian.org/I18n/ibus
   - SUSE: https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang
2. La función se instala automáticamente, pero debe habilitarla para poder usarla.

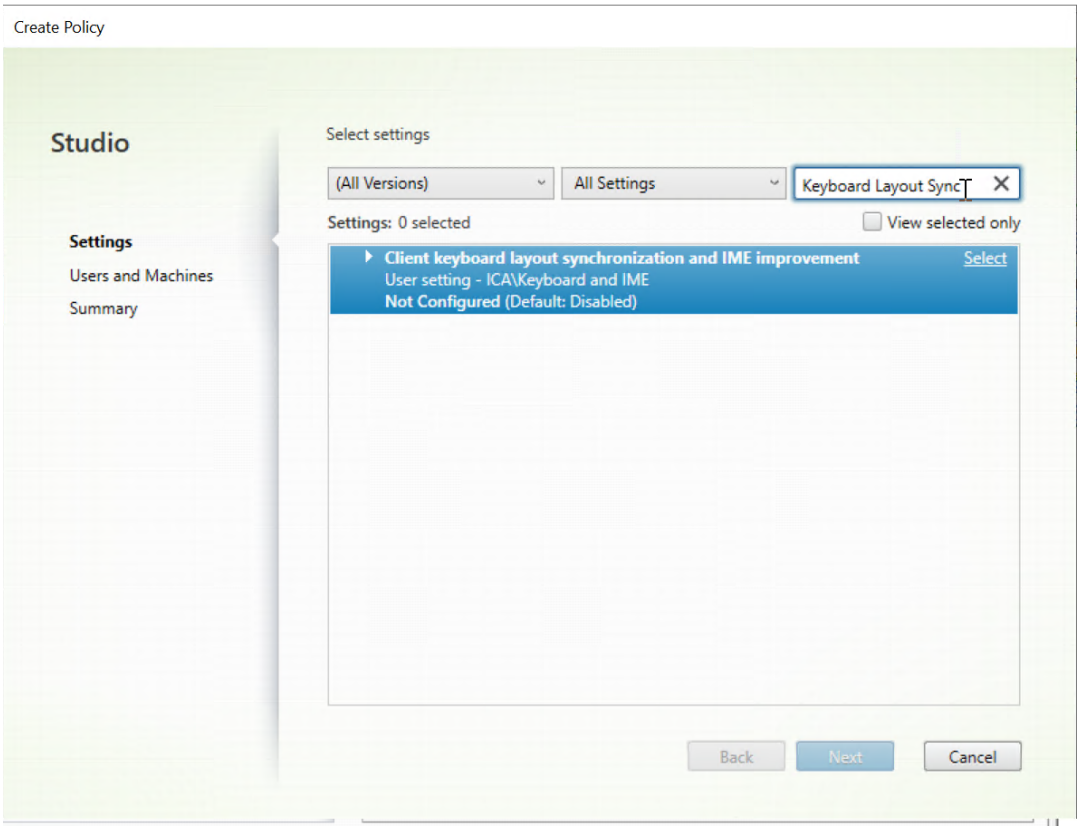
Habilitar e inhabilitar la función

La función de sincronización de la interfaz de usuario del IME del cliente está inhabilitada de forma predeterminada. Para habilitar o inhabilitar la función, establezca la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** o modifique el Registro por medio de la utilidad `ctxreg`.

> **Nota:**
>
> La directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** tiene prioridad sobre la configuración del Registro y se puede aplicar a los objetos de usuario y máquina especificados o a todos los objetos del sitio. La configuración del Registro en un Linux VDA específico se aplica a todas las sesiones de ese VDA.

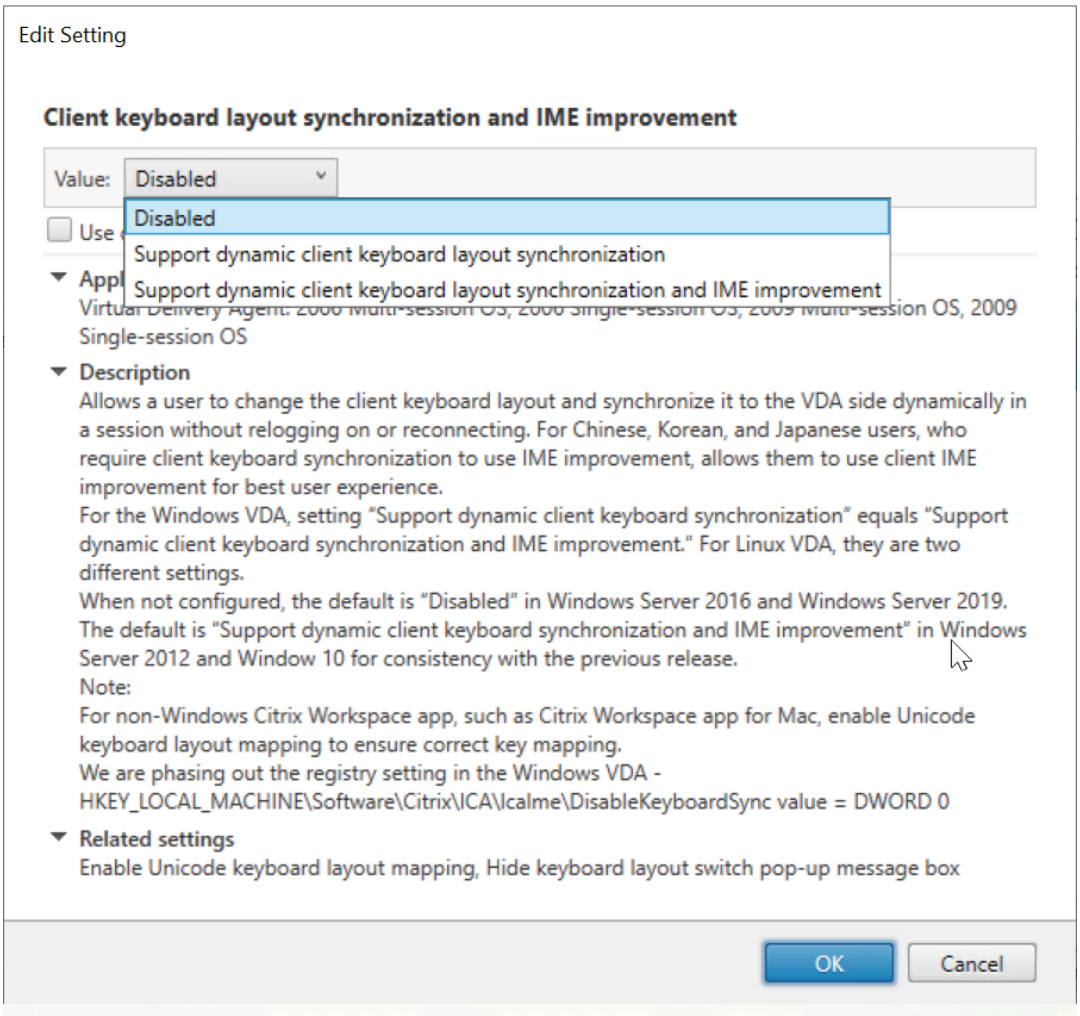
- Establezca la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** para habilitar o inhabilitar la función de sincronización de la interfaz de usuario del IME del cliente:
  1. En Studio, haga clic con el botón secundario en **Directivas** y seleccione **Crear directiva**.
  2. Busque la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Haga clic en **Seleccionar** junto al nombre de la directiva.
4. Establezca la directiva.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hay tres opciones disponibles:

- **Inhabilitado**: Inhabilita la sincronización dinámica de la distribución del teclado y la sincronización de la interfaz de usuario del IME del cliente.
- **Compatibilidad con sincronización dinámica de la distribución del teclado del cliente**: Habilita la sincronización dinámica de la distribución del teclado, independientemente del valor DWORD de la clave de Registro **SyncKeyboardLayout** en `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Compatibilidad con sincronización dinámica de la distribución del teclado del cliente**: Habilita la sincronización dinámica de la distribución del teclado y la sincronización de la interfaz de usuario del IME del cliente, independientemente de los valores DWORD de las claves del Registro **SyncKeyboardLayout** y **SyncClientIME** en `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Modifique el Registro por medio de la utilidad `ctxreg` para habilitar o inhabilitar la función de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sincronización de la interfaz de usuario del IME del cliente:

Para habilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v  "
   SyncClientIME" -d "0x00000001"
<!--NeedCopy-->
```

Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncClientIME" -d "0x00000000"
<!--NeedCopy-->
```

Sincronización de la distribución de teclado dinámico

July 6, 2022

Anteriormente, las distribuciones del teclado en Linux VDA y en el dispositivo cliente tenían que ser los mismos. Podrían surgir problemas de asignación de teclas, por ejemplo, cuando la distribución del teclado cambiaba del inglés al francés en el dispositivo cliente, pero no en el VDA.

Para resolver el problema, Citrix sincroniza 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.

> **Nota:**
>
> La aplicación Citrix Workspace para HTML5 no admite la función de sincronización dinámica de la distribución del teclado.

Configuración

La función de sincronización dinámica de la distribución del teclado está inhabilitada de forma predeterminada. Para habilitar o inhabilitar la función, establezca la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** o modifique el Registro por medio de la utilidad `ctxreg`.

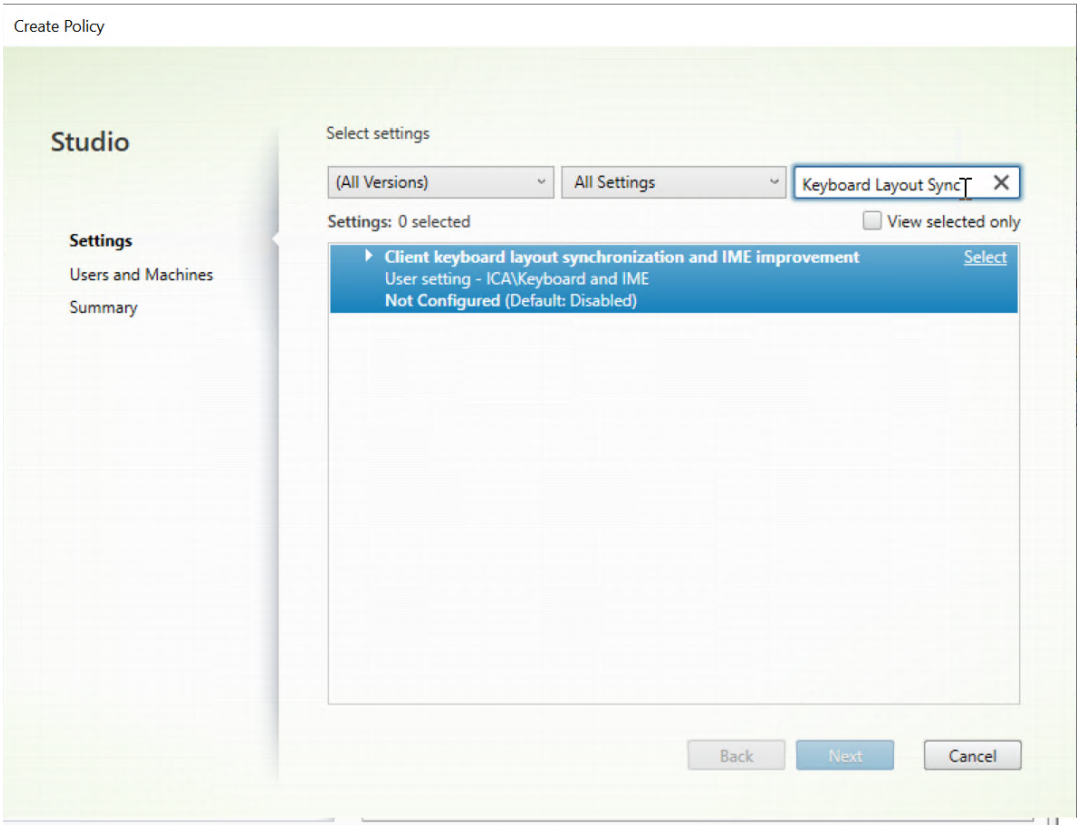
> **Nota:**
>
> La directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** tiene prioridad sobre la configuración del Registro y se puede aplicar a los objetos de usuario y máquina

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> especificados o a todos los objetos del sitio. La configuración del Registro en un Linux VDA específico se aplica a todas las sesiones de ese VDA.

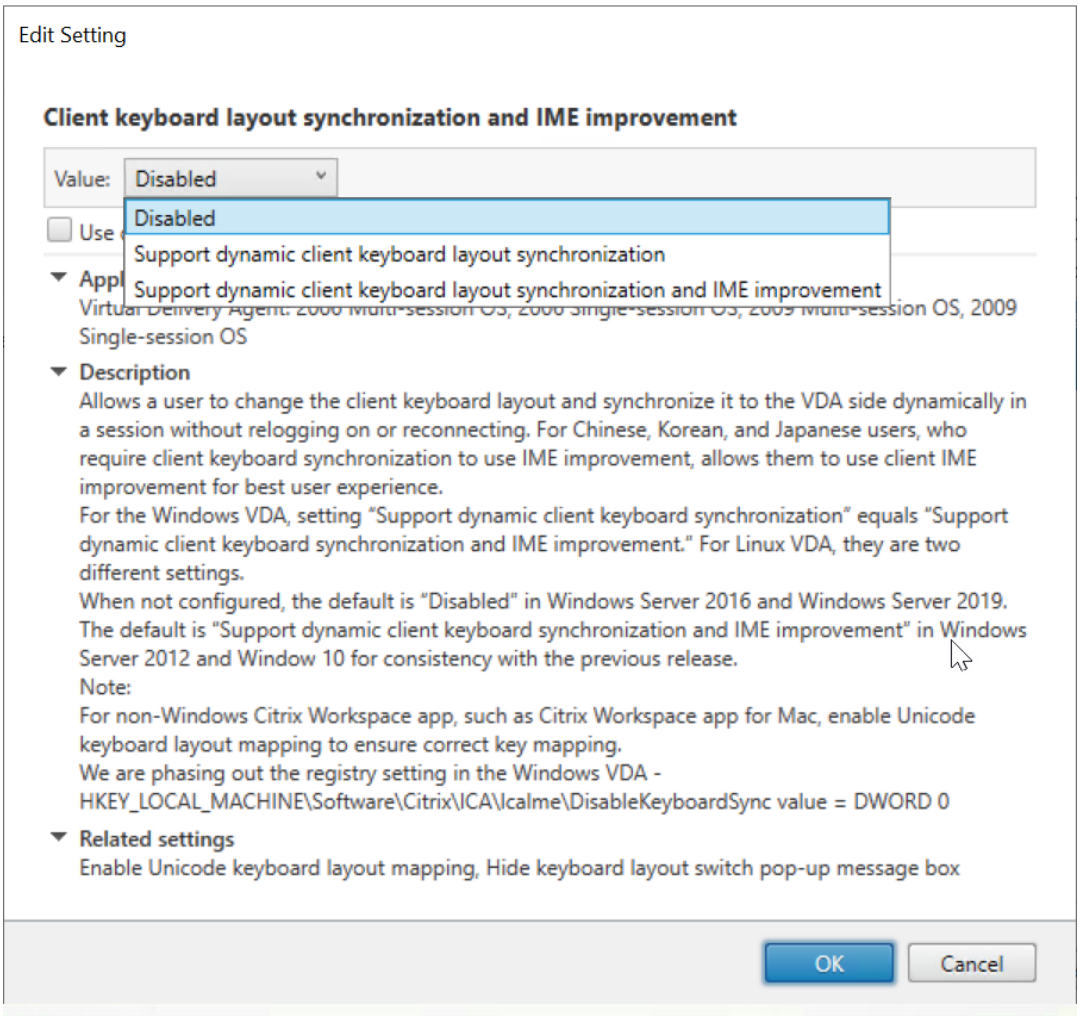
- Establezca la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** para habilitar o inhabilitar la función de sincronización dinámica de la distribución del teclado:

  1. En Studio, haga clic con el botón secundario en **Directivas** y seleccione **Crear directiva**.
  2. Busque la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME**.



  3. Haga clic en **Seleccionar** junto al nombre de la directiva.
  4. Establezca la directiva.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hay tres opciones disponibles:

- **Inhabilitado**: Inhabilita la sincronización dinámica de la distribución del teclado y la sincronización de la interfaz de usuario del IME del cliente.
- **Compatibilidad con sincronización dinámica de la distribución del teclado del cliente**: Habilita la sincronización dinámica de la distribución del teclado, independientemente del valor DWORD de la clave de Registro **SyncKeyboardLayout** en `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Compatibilidad con sincronización dinámica de la distribución del teclado del cliente**: Habilita la sincronización dinámica de la distribución del teclado y la sincronización de la interfaz de usuario del IME del cliente, independientemente de los valores DWORD de las claves del Registro **SyncKeyboardLayout** y **SyncClientIME** en `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Modifique el Registro por medio de la utilidad `ctxreg` para habilitar o inhabilitar la función de

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

sincronización de la interfaz de usuario del IME del cliente:

Para habilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncKeyboardLayout" -d "0x00000001"
<!--NeedCopy-->
```

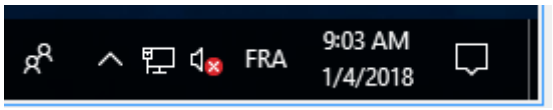
Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncKeyboardLayout" -d "0x00000000"
<!--NeedCopy-->
```

Uso

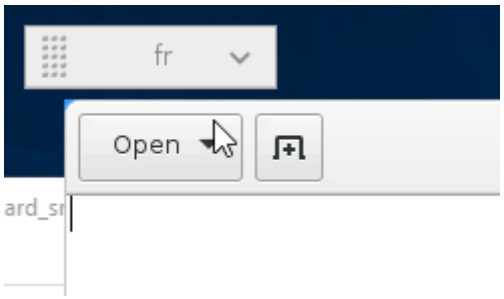
Con esta función habilitada, cuando la distribución del teclado cambia en el dispositivo cliente durante una sesión, también cambia la distribución del teclado de la sesión.

Por ejemplo, si cambia la distribución del teclado en un dispositivo cliente a francés (FR):

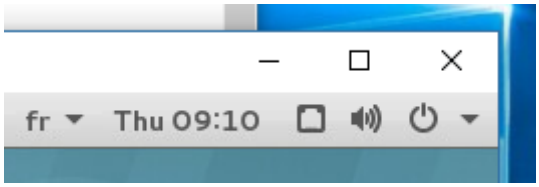


La distribución del teclado de la sesión de Linux VDA también cambia a “fr”.

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:



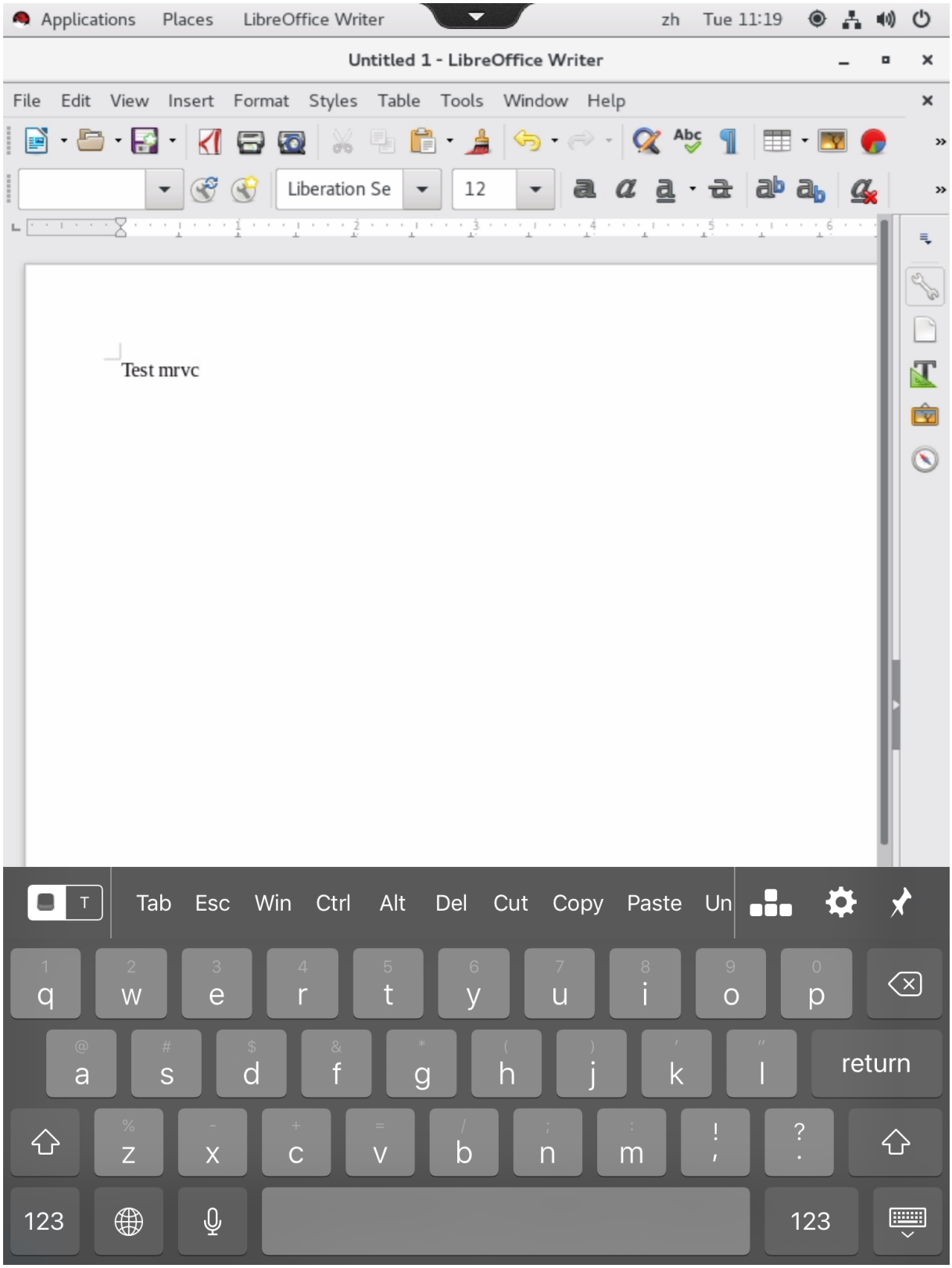
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Teclado en pantalla

September 5, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> La función está disponible para RHEL 7.9, RHEL 8.1, RHEL 8.2, RHEL 8.3, SUSE 15.3, SUSE 15.2, Ubuntu 18.04 y Ubuntu 20.04. 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:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v "
   Enabled" -d "0x00000001"
<!--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:

```
echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
<!--NeedCopy-->
```

Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
<!--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 volver a mostrar el teclado en pantalla después de ocultarlo manualmente, haga clic en un campo que no sea de entrada de texto y, luego, haga clic de nuevo en el campo de entrada actual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

Compatibilidad para entrada de texto en varios idiomas

July 6, 2022

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-->
```

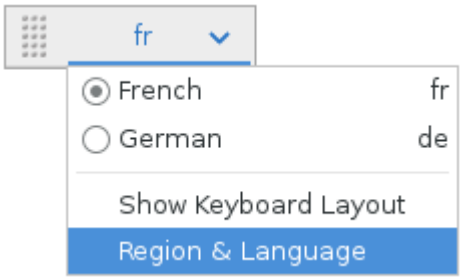
Para inhabilitar esta función, ejecute el comando:

```
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.

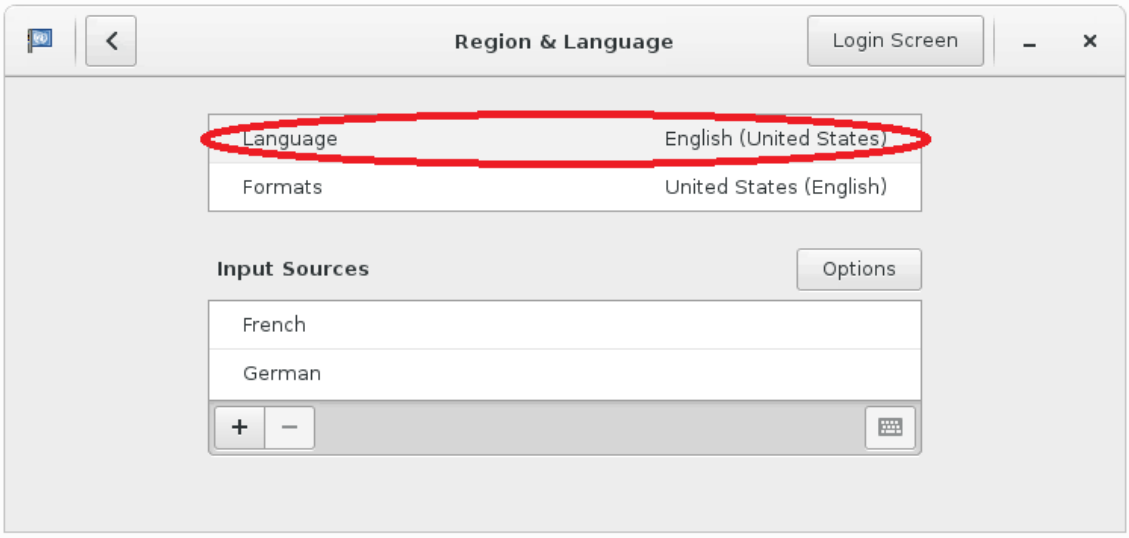
1. Habilite la función.
2. Acceda a una aplicación publicada que acepte la entrada de texto. Aparece una barra de idioma en la sesión, junto a la aplicación.
3. En el menú desplegable, seleccione **Region & Language** (Región e idioma) para agregar el idioma pertinente (origen de entrada).



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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Contenido multimedia

July 6, 2022

Esta sección contiene estos temas:

- Funciones de audio
- Redirección de contenido de explorador web
- Compresión de vídeo de cámara web HDX

Funciones de audio

July 6, 2022

Audio adaptable

El audio adaptable está habilitado de forma predeterminada. Admite estos clientes de la aplicación Citrix Workspace:

- Aplicación Citrix Workspace para Windows: 2109 y versiones posteriores
- Aplicación Citrix Workspace para Linux: 2109 y versiones posteriores
- Aplicación Citrix Workspace para Mac: 2109 y versiones posteriores

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El audio adaptable recurre al audio antiguo al utilizar un cliente que no está en la lista.

Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en los VDA. El audio adaptable ajusta dinámicamente la velocidad de bits de muestreo de audio en función de las condiciones de la red para ofrecer una experiencia de audio superior.

En esta tabla se muestra una comparación entre el audio adaptable y el audio antiguo:

Audio adaptable	Audio antiguo
Frecuencia máxima de muestreo de audio: 48 kHz	Frecuencia máxima de muestreo de audio: 8 kHz
Canal estéreo	Canal mono

> **Sugerencia:**
>
> Use PulseAudio 13.99 o una versión posterior en RHEL 8.x.
>
> Utilice PulseAudio 14.2 o una versión posterior en SUSE 15.3 y PulseAudio 13.0 o una versión posterior en SUSE 15.2.

Redirección de contenido de explorador web

July 6, 2022

Información general

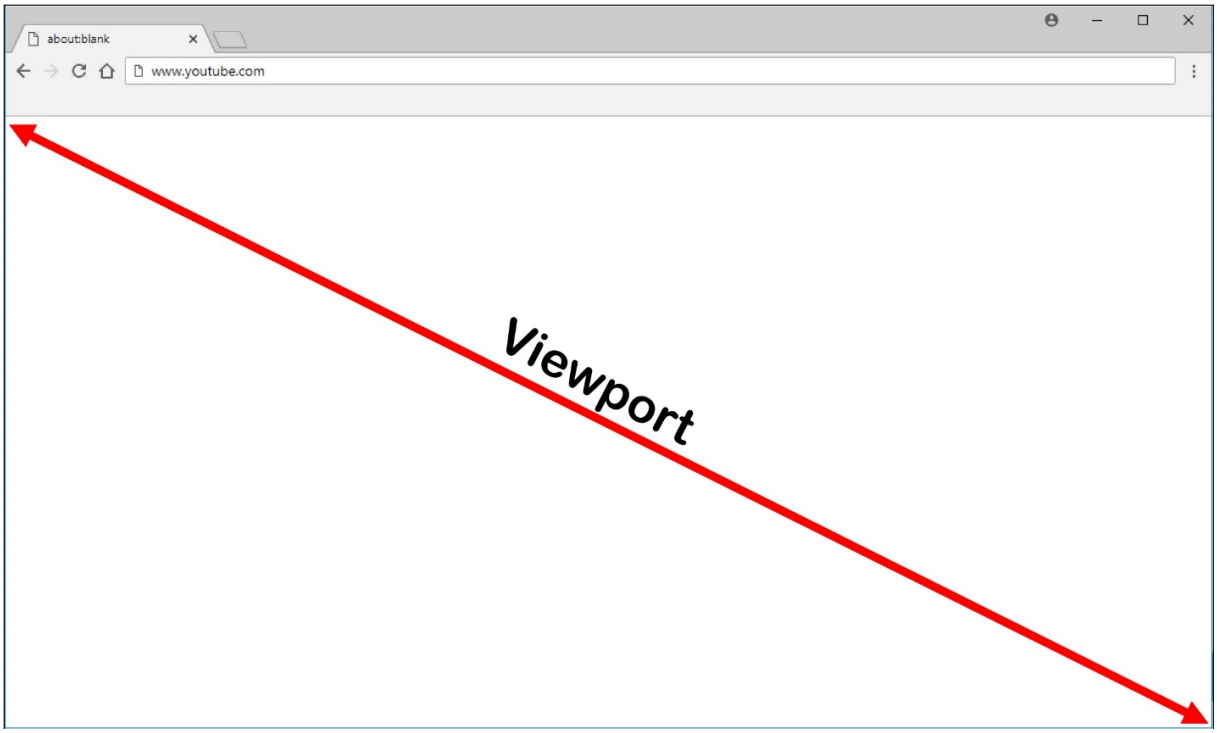
Linux VDA admite la redirección de contenido del explorador en Google Chrome. La redirección de contenido del explorador ofrece la posibilidad de generar páginas web incluidas en la lista de permitidos en el lado del cliente. Esta función utiliza la aplicación Citrix Workspace para crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

> **Nota:**
>
> Mediante una lista de permitidos, puede especificar qué páginas web se redirigen al lado del cliente. A la inversa, mediante una lista de bloqueados, puede especificar qué páginas web no se redirigen al lado del cliente.

Este motor web de distribución superpuesta se ejecuta en el cliente, en lugar de ejecutarse en el VDA, y utiliza la CPU, la GPU, la memoria RAM y la red del cliente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solo se redirige la ventanilla del explorador web. La ventanilla es el área rectangular del explorador web donde aparece el contenido. La ventanilla no incluye elementos como la barra de direcciones, la barra de favoritos ni la barra de estado. Esos elementos siguen ejecutándose en el explorador del VDA.



Requisitos del sistema

Cliente Windows:

- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores

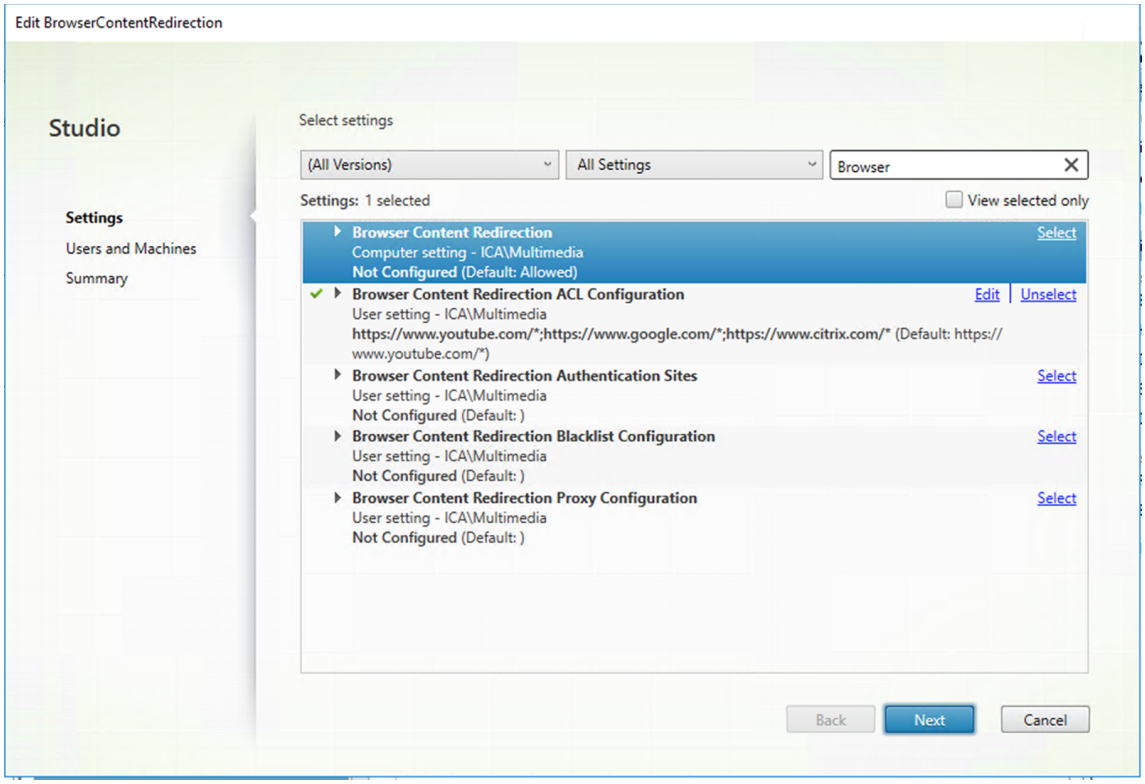
Linux VDA:

- Sistema operativo del VDA: Ubuntu 20.04, Ubuntu 18.04, RHEL 8.2, RHEL 8.1
- Explorador en el VDA: Google Chrome v66 o una versión posterior con la extensión de redirección de contenido de explorador Citrix agregada

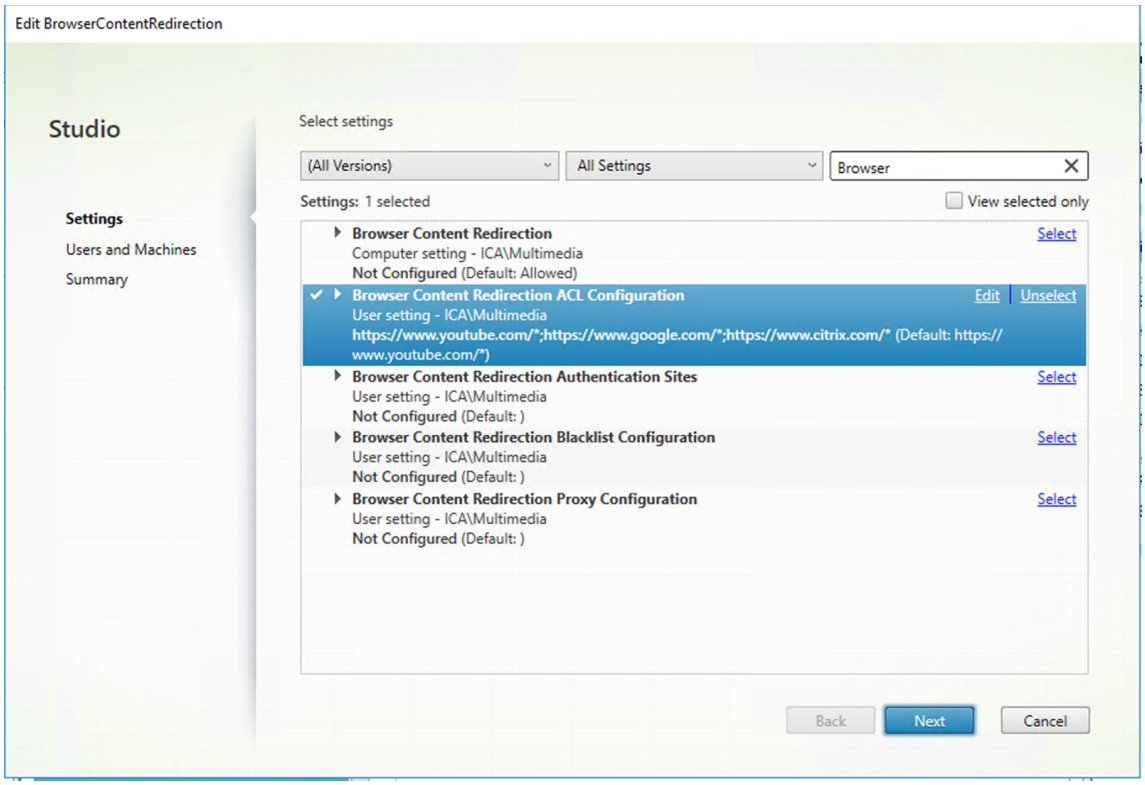
Configurar la redirección de contenido de explorador

1. En Citrix Studio, configure directivas para especificar una lista de direcciones URL permitidas y una lista de direcciones URL bloqueadas para la redirección de contenido del explorador. La redirección de contenido del explorador web está **permitida** de forma predeterminada.

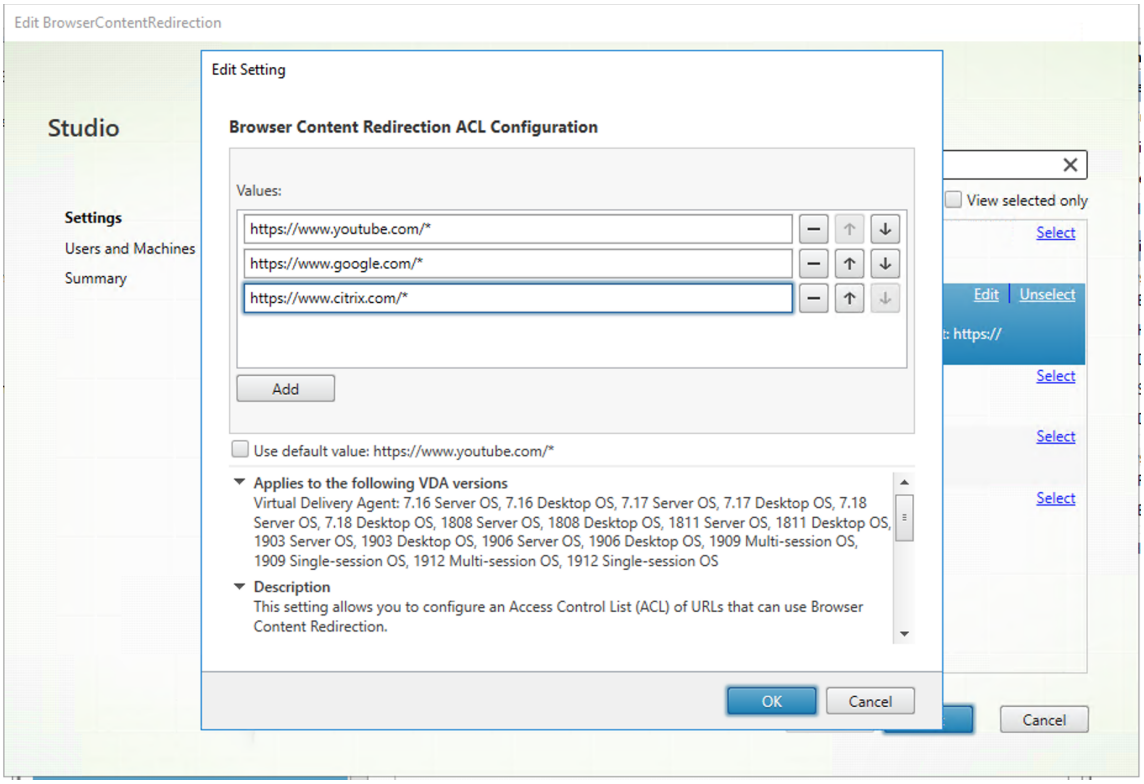
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



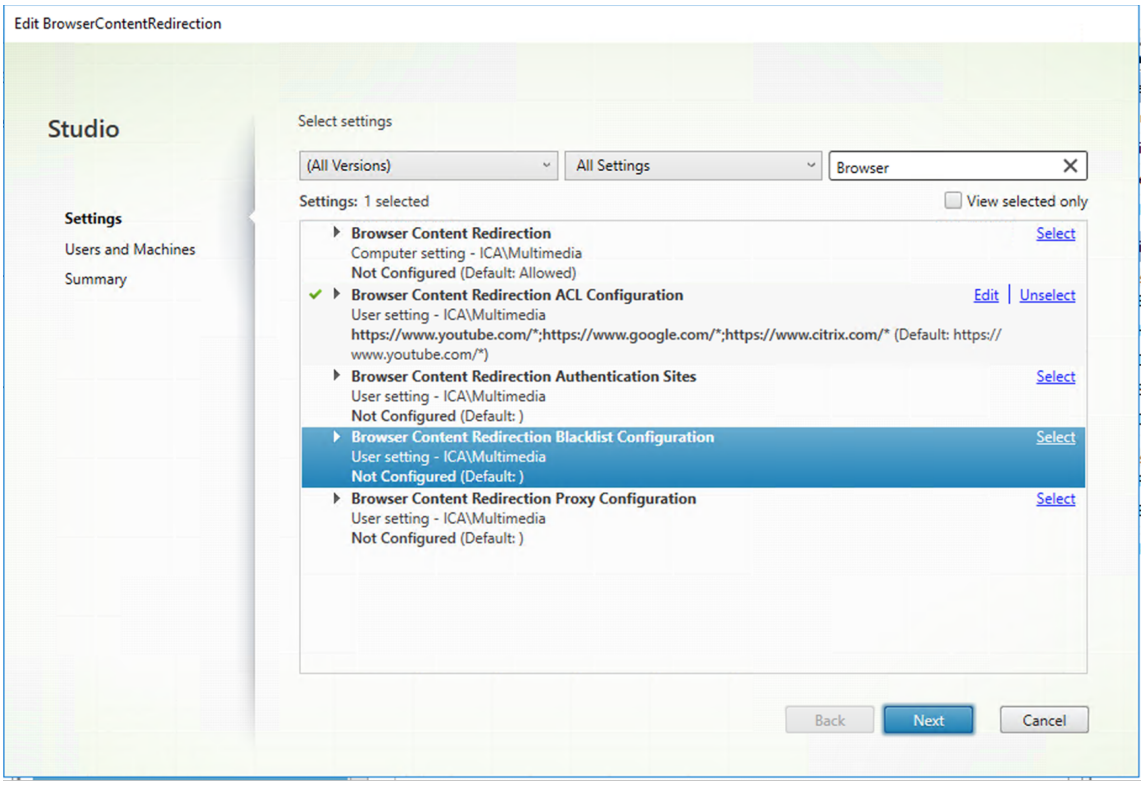
El parámetro **Configuración de lista ACL para redirección de contenido del explorador web** especifica una lista de direcciones URL que pueden utilizar la redirección de contenido de explorador.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



El parámetro **Configuración de lista de bloqueados para la redirección de contenido del explorador web** especifica una lista de direcciones URL que no pueden utilizar la redirección de contenido de explorador.

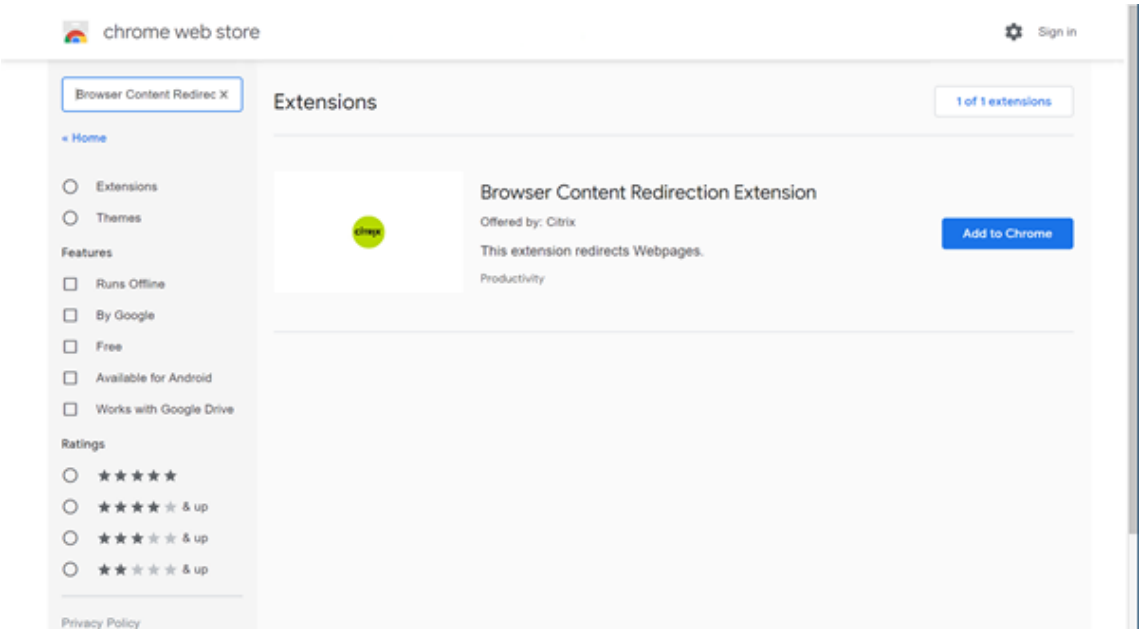


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Linux VDA actualmente no admite la opción **Configuración de proxy para redirección de contenido del explorador web**.

2. Haga clic en **Añadir a Chrome** en el VDA para agregar la extensión de redirección de contenido de explorador Citrix desde Chrome Web Store. Esto ayuda al explorador del VDA a detectar si una URL (de destino) pertenece a una lista de permitidos o una lista de bloqueados.

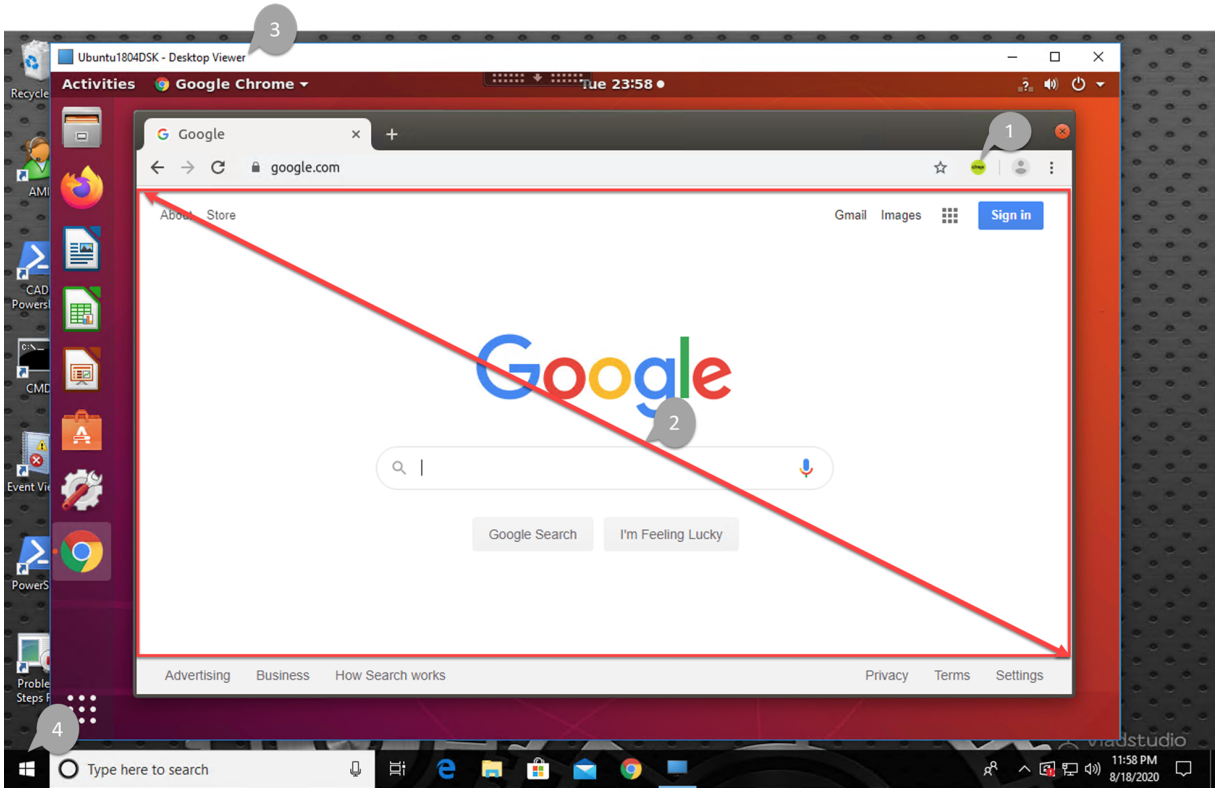
   > **Importante:**
   >
   > La extensión no es necesaria en el cliente. Agréguela solo al VDA.
   >
   > Las extensiones de Chrome se instalan basándose en el usuario. No es necesario actualizar una imagen maestra para agregar o eliminar una extensión.



Si se encuentra una coincidencia con una URL en una lista de permitidos (por ejemplo, `https://www.mycompany.com/`) y no hay ninguna en una lista de bloqueados, un canal virtual (CTXCSB) indica a la aplicación Citrix Workspace que se requiere una redirección y transmite la URL. La aplicación Citrix Workspace crea una instancia de motor de generación local y muestra el sitio web.

La aplicación Citrix Workspace introduce el sitio web en el área de contenido del explorador web que tenga el escritorio virtual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Icono de la extensión de redirección de contenido de explorador web Citrix

   El color del icono de la extensión especifica el estado de la extensión de Chrome. Puede ser uno de estos tres colores:

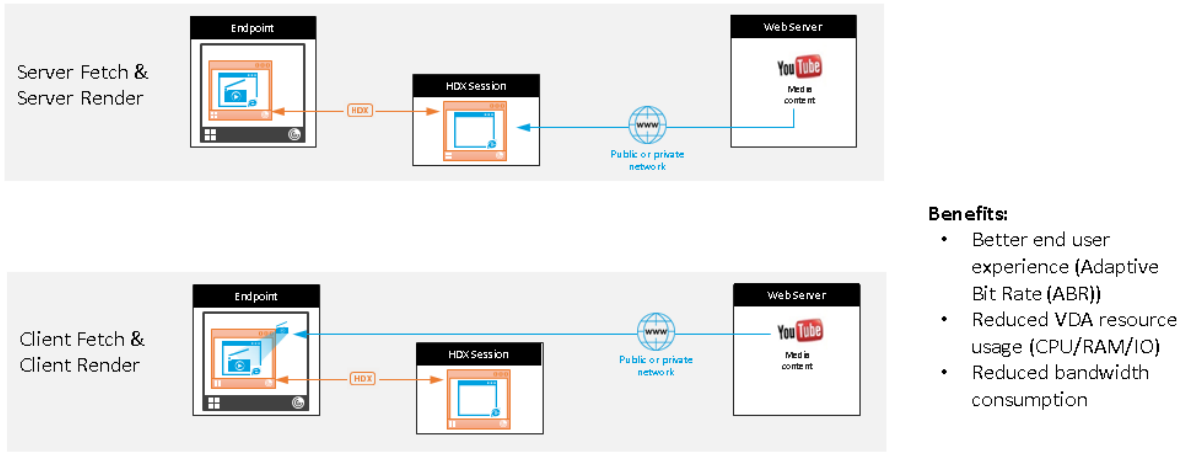
   - Verde: Activo y conectado
   - Gris: No activo/inactivo en la ficha actual
   - Rojo: No funciona

2. Ventanilla generada en el cliente o integrada en el escritorio virtual
3. Linux VDA
4. Cliente Windows

Supuestos de redirección

La aplicación Citrix Workspace obtiene el contenido de estas maneras:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Obtención en el servidor y generación en el servidor:** No hay redirección porque el sitio no consta en la lista de permitidos o la redirección ha fallado. Se recurre a la generación de la página web en el VDA y se usa Thinwire para generar remotamente los gráficos. Se usan directivas para controlar el comportamiento cuando se recurre al mecanismo alternativo. Este supuesto provoca un alto consumo de CPU, RAM y ancho de banda en el VDA.
- **Obtención en el cliente y generación en el cliente:** Como la aplicación Citrix Workspace se comunica directamente con el servidor web, requiere acceso a Internet. En este supuesto, no se consume la red, la CPU ni la memoria RAM del sitio de Citrix Virtual Apps and Desktops.

Mecanismo alternativo

La redirección de cliente puede fallar a veces. Por ejemplo, si la máquina cliente no tiene acceso directo a Internet, el VDA puede recibir una respuesta de error. En tales casos, el explorador presente en el VDA puede volver a cargar la página web y generarla en el servidor.

Compresión de vídeo de cámara web HDX

March 27, 2023

Información general

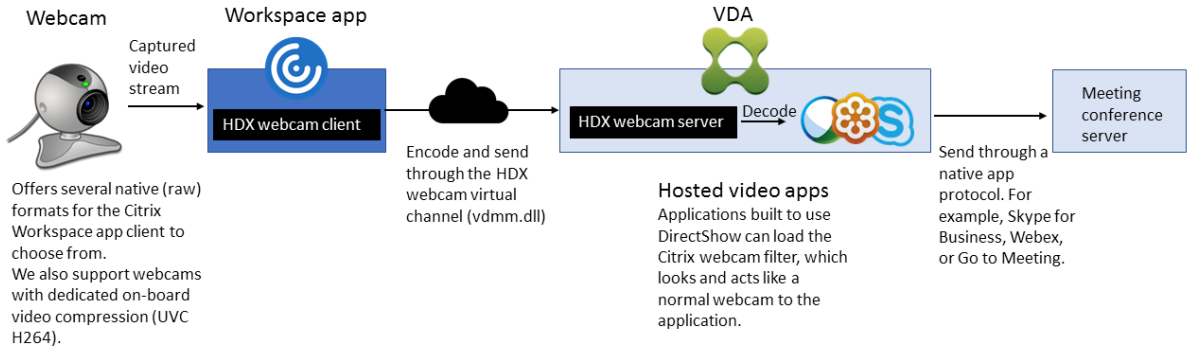
Los usuarios de aplicaciones de videoconferencia que se ejecutan en sesiones de Linux VDA ahora pueden usar sus cámaras web con compresión de vídeo HDX. Esta función está habilitada de manera

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

predeterminada. Se recomienda usar la compresión de vídeo de cámaras web de HDX siempre que sea posible.

La compresión de vídeo de cámaras web de HDX también se llama modo de cámara web **optimizado**. Este tipo de compresión de vídeo por cámara web envía el vídeo en H.264 directamente a la aplicación de videoconferencias de la sesión virtual. La compresión de vídeo de cámaras web de HDX utiliza la tecnología de framework multimedia que forma parte del sistema operativo cliente para interceptar el vídeo de los dispositivos de captura, transcodificarlo y comprimirlo. Los fabricantes de los dispositivos de captura suministran controladores que complementan la arquitectura de streaming del kernel del sistema operativo.

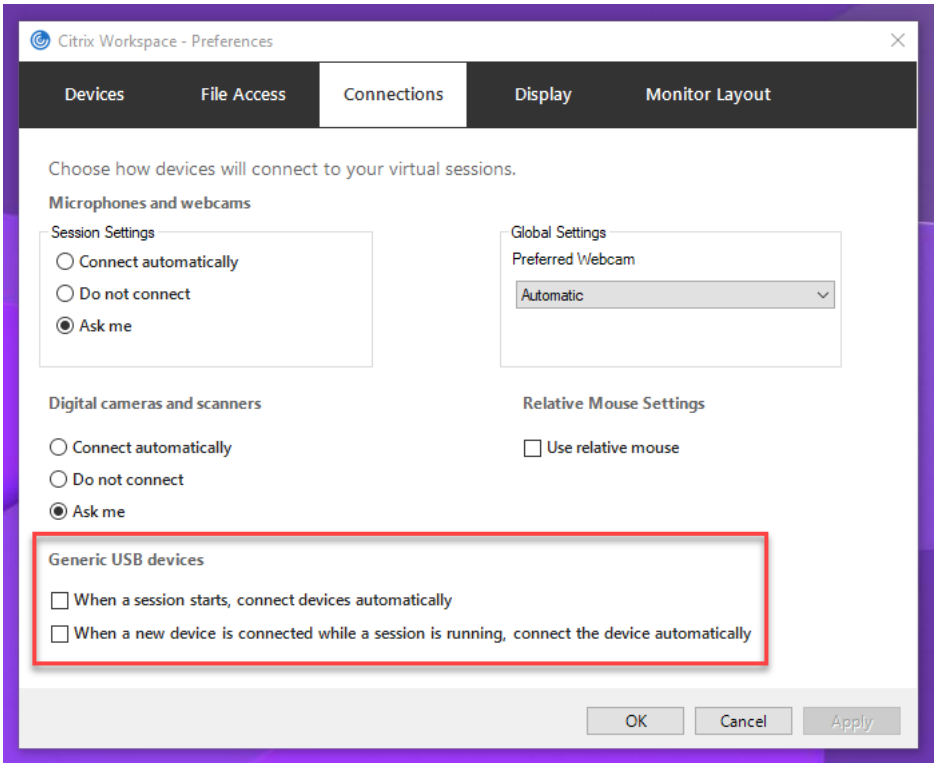
El cliente gestiona la comunicación con la cámara web. El cliente envía el vídeo solo al servidor que puede mostrarlo correctamente. El servidor no trata directamente con la cámara web, pero su integración le ofrece la misma experiencia en el escritorio que un tratamiento directo. La aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mejor capacidad de recuperación en conexiones WAN.



Nota:

- Esta función solo admite vídeos H.264 del cliente de la aplicación Citrix Workspace.
- La resolución de cámara web admitida oscila entre 48x32 y 1920x1080.
- No elija **Dispositivos USB genéricos** en la barra de herramientas de la aplicación Citrix Workspace cuando utilice una cámara web. De lo contrario, podrían ocurrir problemas imprevistos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Distribuciones compatibles de Linux

- RHEL 8.4
- RHEL 8.3
- RHEL 7.9 / CentOS 7.9
- Ubuntu 20.04
- Ubuntu 18.04
- Debian 10
- SUSE 15.3
- SUSE 15.2

Aplicación Citrix Workspace compatible

La compresión de vídeo de cámaras web de HDX admite las siguientes versiones de la aplicación Citrix Workspace:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Plataforma	Procesador
Aplicación Citrix Workspace para Windows	La aplicación Citrix Workspace para Windows admite la compresión de vídeo de cámara web para aplicaciones de 32 y 64 bits en XenApp y XenDesktop 7.17 y versiones posteriores. En versiones anteriores, la aplicación Citrix Workspace para Windows solo es compatible con aplicaciones de 32 bits.
Aplicación Citrix Workspace para Chrome	Debido a que algunos dispositivos Chromebook ARM no son compatibles con la codificación H.264, solo las aplicaciones de 32 bits pueden utilizar la compresión de vídeo de cámaras web de HDX optimizada.

Cámaras web probadas por completo

Las distintas cámaras web ofrecen diferentes velocidades de fotogramas y tienen diferentes niveles de brillo y contraste. Citrix utiliza las siguientes cámaras web para la validación inicial de funciones:

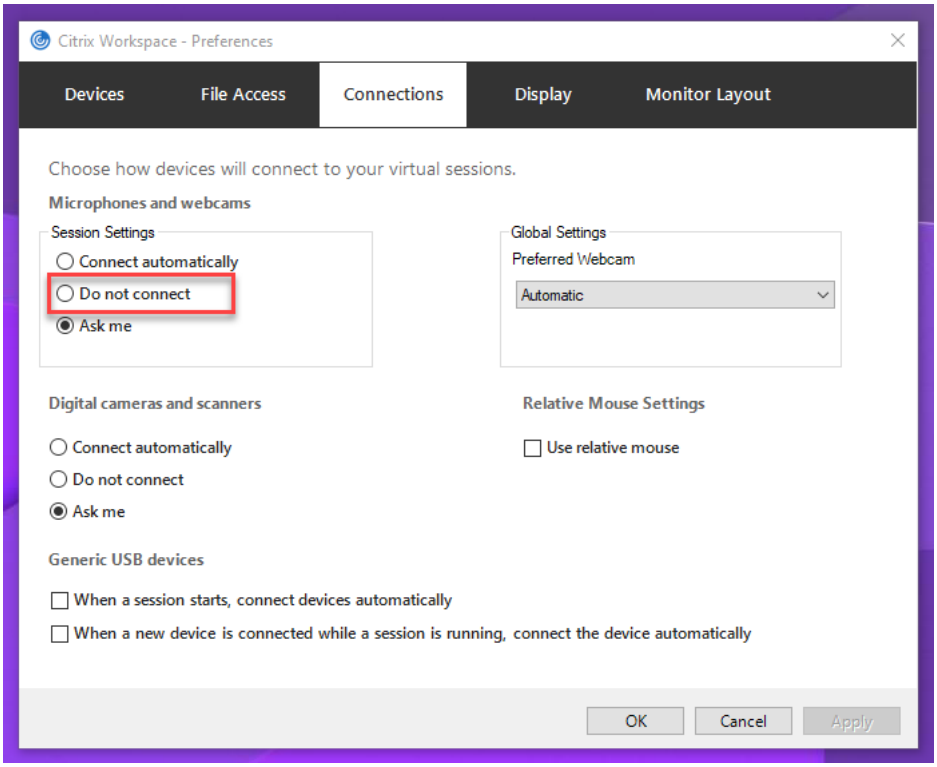
- Cámara web Logitech HD C270
- Cámara web Logitech C930e
- Microsoft-LifeCam-HD3000

Configuración

Esta función está habilitada de manera predeterminada. Para utilizarla, complete la siguiente verificación y configuración:

> **Consejo:**
>
> Los usuarios de la aplicación Citrix Workspace pueden ignorar la configuración predeterminada. Para ello, deben elegir la opción **No conectar** en **Micrófonos y cámaras web** de Desktop Viewer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Una vez completada la instalación del VDA, compruebe que este puede registrarse en el Delivery Controller y que las sesiones de escritorio de Linux publicadas se puedan iniciar correctamente con credenciales de Windows.
2. Compruebe que el VDA tiene acceso a Internet y ejecute el comando `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` para completar la configuración de la cámara web. Si el VDA no tiene acceso a Internet, vaya al paso 3.

   Si el VDA se implementa en Debian 10, asegúrese de que se ejecuta en la última versión del kernel. De lo contrario, ejecute los siguientes comandos para actualizar a la última versión del kernel:

   ```
   sudo apt-get update
   sudo apt-get dist-upgrade
   sudo reboot
   <!--NeedCopy-->
   ```

   Si el VDA se implementa en SUSE 15.3, SUSE 15.2 o SUSE 12.5, ejecute estos comandos para actualizarse a la versión más reciente del kernel y reiniciarlo:

   ```
   zypper up kernel-default
   reboot
   <!--NeedCopy-->
   ```

   El script ctxwcamcfg.sh ayuda a:

   a) Instalar los programas `kernel-devel` y DKMS (Dynamic Kernel Module Support) en el

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA.

- `kernel-devel` se utiliza para crear un módulo de kernel de cámara web virtual de la versión correspondiente.
- DKMS se utiliza para administrar dinámicamente el módulo de kernel de cámara web virtual.

> **Nota:**
>
> Al instalar los programas anteriores en RHEL y CentOS, el script `ctxwcamcfg.sh` instala y habilita los siguientes repositorios en el VDA:
>
> - Extra Packages for Enterprise Linux (EPEL)
> - RPM Fusion

b) Descargue el código abierto `v4l2loopback` desde https://github.com/umlaeute/v4l2loopback y utilice DKMS para administrar `v4l2loopback`.
`v4l2loopback` es un módulo de kernel que permite crear dispositivos de bucle invertido V4L2.

c) Ejecute el comando `sudo service ctxwcamsd restart`. El servicio de cámara web de Linux VDA (`ctxwcamsd`) reinicia y carga el módulo de kernel `v4l2loopback` para la función de compresión de vídeo de las cámaras web de HDX.

3. Si el VDA no tiene acceso a Internet, genere el módulo de kernel v4l2loopback en otra máquina y, a continuación, cópielo en el VDA.

a) Prepare una máquina de compilación que tenga acceso a Internet y la misma versión de kernel con el VDA. El comando `uname -r` ayuda a encontrar versiones de kernel.

b) En la máquina de compilación, ejecute el comando `sudo mkdir -p /var/xdl`.

c) Copie `/var/xdl/configure_*` desde el VDA a la máquina de compilación en `/var/xdl/`.

d) En la máquina de compilación, ejecute el comando `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` para generar el módulo de kernel. Si el comando se ejecuta correctamente, crea un archivo v4l2loopback.ko bajo la ruta `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/`. Ignore los errores que puedan producirse al ejecutar el script ctxwcamcfg.sh.

e) Copie v4l2loopback.ko desde la máquina de compilación en el VDA y colóquelo en `/opt/Citrix/VDA/lib64/` .

f) En el VDA, ejecute el comando `sudo service ctxwcamsd restart` para reiniciar el servicio de cámara web y cargar el módulo de kernel v4l2loopback.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA no unidos a ningún dominio

July 8, 2022

Introducción a la configuración

Los VDA que no están unidos a un dominio solo son compatibles con Citrix DaaS. Para crear VDA no unidos a ningún dominio en Citrix DaaS, debe usar Machine Creation Services (MCS). Los pasos abreviados son:

1. Cree una imagen maestra en una VM de plantilla en la que también instale el paquete de VDA. Puede usar una sola imagen con la que crear VDA tanto unidos a un dominio como no unidos a ningún dominio.
2. Use la imagen maestra para crear un catálogo de máquinas. Seleccione MCS como método de implementación de máquinas y seleccione **No unido a un dominio** como identidad para las máquinas que se crearán en el catálogo.

Para obtener más información, consulte Utilice Machine Creation Services (MCS) para crear máquinas virtuales Linux e Identidades de las máquinas.

Funciones disponibles para VDA que no están unidos a ningún dominio

Crear usuarios locales con atributos especificados en VDA que no están unidos a ningún dominio

Al abrir una sesión alojada en un VDA que no está unido a ningún dominio, el VDA crea automáticamente un usuario local con atributos predeterminados. El VDA crea el usuario local en función del nombre de usuario que utilizó para iniciar sesión en la aplicación Citrix Workspace. También puede especificar atributos de usuario, como el identificador de usuario (UID), el identificador de grupo (GID), el directorio principal y el shell de inicio de sesión del usuario. Para utilizar esta función, siga estos pasos:

1. Ejecute el siguiente comando para habilitar la función:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
     CreateWithUidGid" -d "0x00000001" --force
2 <!--NeedCopy-->
```

2. Especifique estos atributos en el script `/var/xdl/getuidgid.sh` de la ruta de instalación del VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Atributo	Obligatorio u opcional	Descripción
uid	Si son necesarias	El identificador de usuario (UID) es un número asignado por Linux a cada usuario del sistema. Determina a qué recursos del sistema puede acceder el usuario.
gid	Si son necesarias	El identificador de grupo (GID) es un número que se utiliza para representar un grupo específico.
homedir	Opcional	El directorio principal de Linux es un directorio de un usuario en particular.
shell	Opcional	El shell de inicio de sesión es un shell que se le da a un usuario al iniciar sesión en su cuenta de usuario.

A continuación se muestra un ejemplo del script getuidgid.sh:

> **Nota:**
>
> Asegúrese de que los atributos especificados en el script sean válidos.

```
#!/bin/bash

################################################################################

#
# Script de Citrix Virtual Apps and Desktops para Linux: Obtener el uid y el gid del usuario
#
# Copyright (c) Citrix Systems, Inc. Todos los derechos reservados.
#

export LC_ALL="en_US.UTF-8"

function get_uid_gid_for_user()
{

echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
echo "shell:/bin/sh"
 }


get_uid_gid_for_user $1<!--NeedCopy-->
```

Lista de directivas disponibles

September 5, 2022

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	Booleano	ICA/Control de zona horaria	Usar zona horaria del servidor
Cálculo del tiempo de retorno ICA	IcaRoundTripCheckEnabled	Entero	ICA/Supervisión de usuario final	Inhabilitado (1)

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Intervalo de cálculo del tiempo de retorno ICA	IcaRoundTripCheckEnSub	EquipoClave	ICA/Sesión de usuario final	15
Cálculo del tiempo de retorno ICA para conexiones inactivas	IcaRoundTripCheckEnSub	EquipoClave	ICA/Sesión de usuario final	Habilitado (0)
Límite de ancho de banda global de la sesión	LimitOverallBw	UlBw	ICA\Ancho de banda	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Límite de ancho de banda de redirección de sonido	LimitAudioBw	UsBw	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de sonido	LimitAudioBwPct	UsBwPct	ICA\Ancho de banda	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Límite de ancho de banda de redirección de dispositivos USB del cliente	LimitUSBBwUsuario	Entero	ICA\Ancho de banda	0
Porcentaje de ancho de banda de redirección de dispositivos USB del cliente	LimitUSBBwPorcentaje	Entero	ICA\Ancho de banda	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Límite de ancho de banda de redirección del portapapeles	LimitClipboardBW	DWORD	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección del portapapeles	LimitClipboardBWPercent	DWORD	ICA\Ancho de banda	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Límite de ancho de banda de redirección de archivos	LimitCdmBw	DWORD	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de archivos	LimitCdmBwPercent	DWORD	ICA\Ancho de banda	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Límite de ancho de banda de redirección de impresoras	LimitPrinterBandwidth	DWORD	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de impresoras	LimitPrinterBandwidthPercent	DWORD	ICA\Ancho de banda	0
Conexiones con WebSockets	AcceptWebSocketsConnections	DWORD	ICA\WebSockets	Permitida

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Número de puerto de WebSockets	WebSocketsPort	Equipo	ICA\WebSockets	8008
Lista de servidores de origen de WebSockets de confianza	WSTrustedOriginServerList	Equipo	ICA\WebSockets	*
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Número de puerto de escucha ICA	IcaListenerPortNumber	Equipo	ICA	1494
Transporte adaptable HDX	HDXoverUDP	Equipo	ICA	Preferido (2)
Conexiones de fiabilidad de la sesión	AcceptSessionReliability	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%

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
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 s
Reconexión automática de clientes	AllowAutoClientReconnect	Usuario	ICA/Reconexión automática de clientes	Permitido (1)
Redirección de audio del cliente	AllowAudioRedirection	Usuario	Audio	Permitido (1)
Redirección de impresoras del cliente	AllowPrinterRedir	Usuario	Impresión	Permitido (1)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Crear automáticamente la impresora universal de PDF	AutoCreateUniversalPrinter	DWORD	Impresión	Inhabilitado (0)
Asignación y compatibilidad de controladores de impresora	DriverMappingList	Lista	Impresión	`'Microsoft XPS Document Writer *, Deny ; Send to Microsoft OneNote *, Deny '`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado					
Redirección del portapapeles del cliente	AllowClipboardRedirection	Usuario	Portapapeles	Permitido (1)					
Redirección de dispositivos USB del cliente	AllowUSBRedirection	Usuario	USB	Prohibido (0)					
Reglas de redirección de dispositivos USB del cliente	USBDeviceRules	Usuario	USB	“	**Reglas de redirección de dispositivos USB del cliente**	USBDeviceRules	Usuario	USB	“\0” ”
Compresión de imágenes en movimiento	MovingImageCompression	Usuario	Thinwire Graphics	Habilitado (1)					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Usar codificación por hardware para códec de vídeo	UseHardwareEncoding	Usuario	Thinwire	Habilitado (1)
Permitir compresión sin pérdida visual	AllowVisualLoss	Usuario	ThinWire	Inhabilitado (0)
Optimizar para cargas de trabajo de gráficos 3D	OptimizeFor3dWorkload	Usuario	Thinwire	Inhabilitado (0)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Profundidad de color preferida para gráficos simples	PreferredColorDepth	ColorDepth	Thinwire	24 bits por píxel (1)
Calidad de audio	SoundQuality	Usuario	Audio	Alto – Sonido de alta definición (2)
Redirección de micrófonos del cliente	AllowMicrophoneRedir	Usuario	Audio	Permitido (1)
Número máximo de sesiones	MaximumSessionsPerServer	Equipo	Administración de carga	250

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Tolerancia de inicios de sesión simultáneos	ConcurrentLogonsTolerance	Equipo	Administración de carga	2
Habilitar actualización automática de Controllers	EnableAutoUpdateOfControllers	Equipo	Parámetros de Virtual Delivery Agent	Permitido (1)
Modo de actualización de la selección del portapapeles	ClipboardSelectionUpdateMode	Equipo	Portapapeles	Modo

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Modo de actualización de la selección primaria	PrimarySelectionUpdateMode	Usuario	Portapapeles	1
Calidad máxima de Speex	MaxSpeexQuality	Usuario	Audio	5
Conectar automáticamente las unidades del cliente	AutoConnectDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Habilitado (1)
Unidades ópticas del cliente	AllowCdromDrive	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Unidades fijas del cliente	AllowFixedDrives	UseDrive	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades de disco flexible del cliente	AllowFloppyDrives	UseDrive	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades de red del cliente	AllowNetworkDrives	UseDrive	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Redirección de unidades del cliente	AllowDriveRedir	UseRedir	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Acceso de lectura solamente a unidades del cliente	ReadOnlyMappedDrive	Usuario	Redirección de archivos/Asignación de unidades del cliente	Inhabilitado (0)
Presentación automática del teclado	AllowAutoKeyboardPopup	Usuario	VDA	Inhabilitado (0)
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Cargar archivos al escritorio	AllowFileUpload	Usuario	Transferencia de archivos	Se permite
Temporizador de sesión inactiva	EnableSessionIdleTimer	Usuario	Temporizador de sesión	Habilitado (1)
Intervalo de temporizador de sesiones inactivas	SessionIdleTimerInterval	Usuario	Temporizador de sesión	1440 minutos
Temporizador de sesiones desconectadas	EnableSessionDisconnectTimer	Usuario	Temporizador de sesión	Habilitado (0)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predeterminado
Intervalo de temporizador de sesiones desconectadas	SessionDisconnectTimerInterval	Usuario	Temporizador de sesión	1440 minutos

> **Nota:**
>
> Solo Virtual Delivery Agent (VDA) de Windows admite sonido a través del protocolo UDP. Linux VDA no lo hace. Para obtener más información, consulte Transporte de sonido en tiempo real sobre UDP.

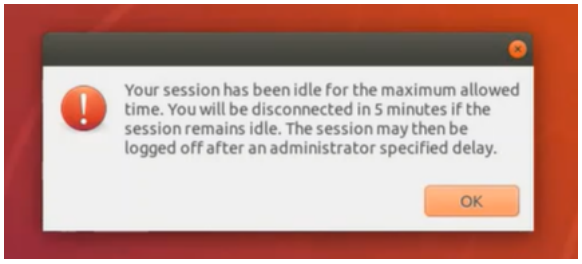
Puede usar los siguientes parámetros de directiva Citrix para configurar temporizadores de conexión de sesión en Citrix Studio:

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

Al actualizar estos parámetros de directiva, compruebe que son coherentes en toda la implementación.

Aparecerá un mensaje de advertencia cuando caduque el límite de tiempo para las sesiones inactivas. La siguiente captura de pantalla sirve de ejemplo. Al pulsar **Aceptar**, se cierra el mensaje de advertencia pero no se puede mantener la sesión activa. Para mantener la sesión activa, proporcione una entrada de usuario, de manera que se restablezca el temporizador de inactividad.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Se pueden configurar las siguientes directivas en la versión 7.12 de Citrix Studio o versiones posteriores.

- MaxSpeexQuality

  Valor (entero): [0–10]

  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]

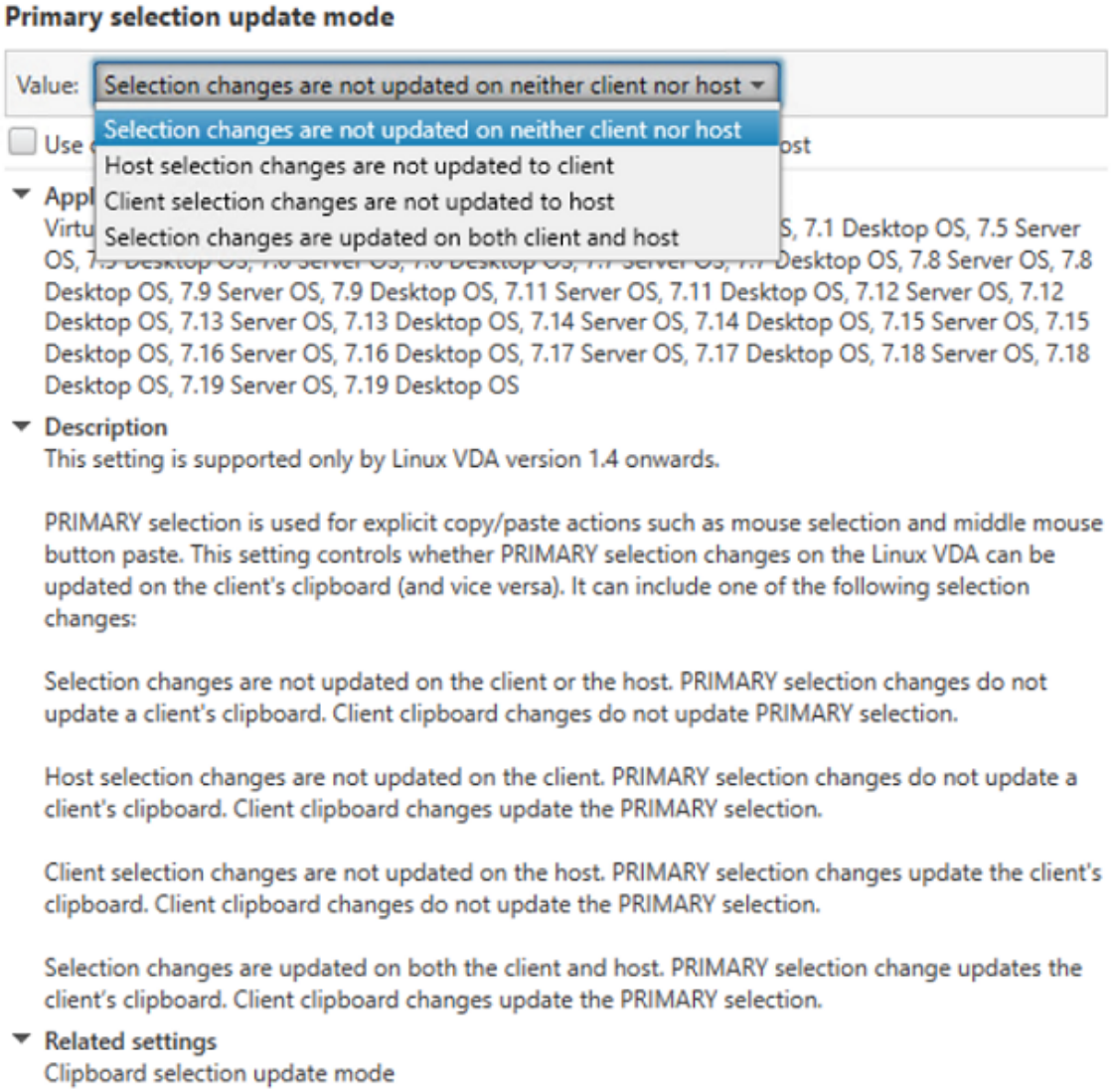
  Valor predeterminado: 3

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 y el cliente pueden actualizar el portapapeles de cada uno entre sí. Hay cuatro opciones de valores:



- **Los cambios de selección no se actualizan ni en el cliente ni en el host**
  Los cambios realizados con la selección principal en Linux VDA no actualizan el portapapeles en el cliente. Los cambios realizados con la selección principal en el cliente no actualizan el portapapeles en Linux VDA.
- **Los cambios de selección en el host no se actualizan en el cliente**
  Los cambios realizados con la selección principal en Linux VDA no actualizan el portapape-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

les 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]

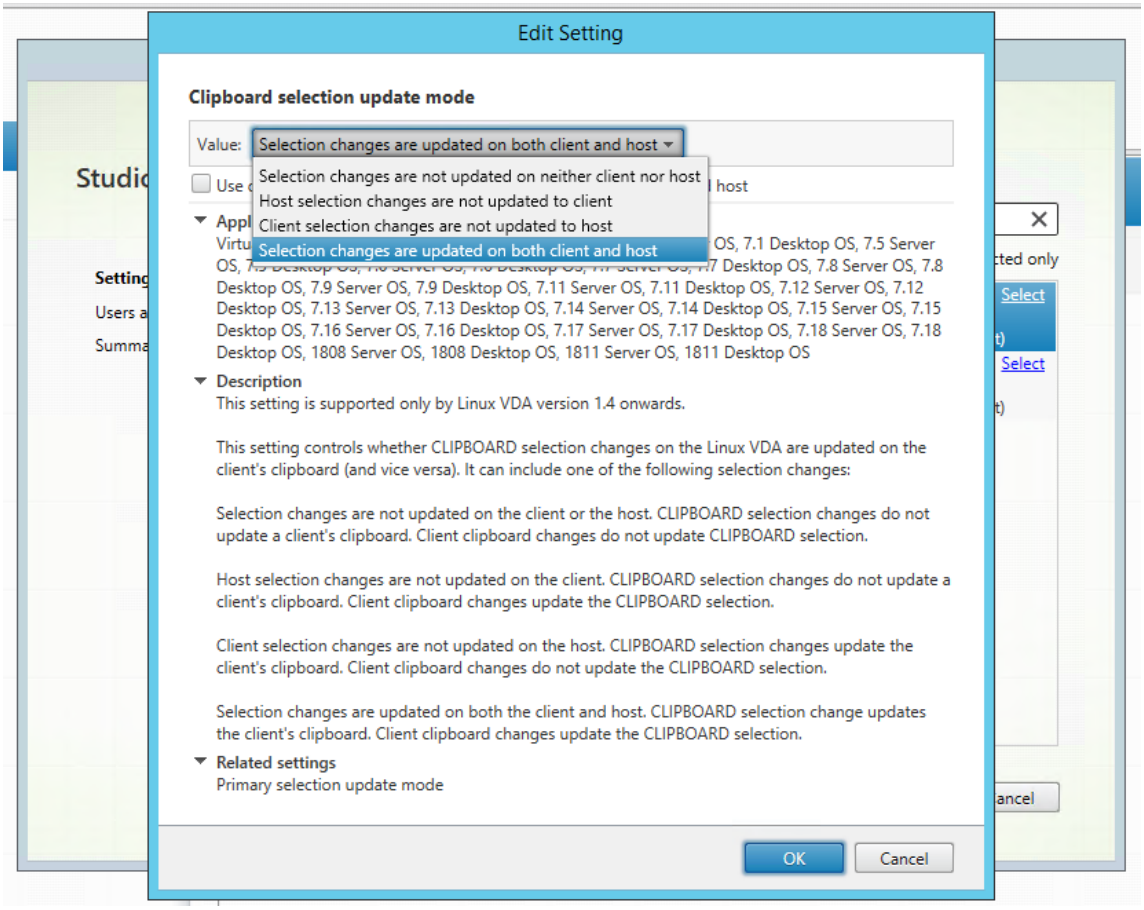
  Valor predeterminado: 3

  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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> Linux VDA admite tanto la selección del portapapeles como la selección primaria. Para controlar los comportamientos de las funciones copiar y pegar entre Linux VDA y el cliente, se recomienda que configure el modo de actualización de selección de portapapeles y el modo de actualización de selección principal con el mismo valor.

Impresión

July 6, 2022

Esta sección contiene estos temas:

- Prácticas recomendadas de impresión
- Impresión de PDF

Prácticas recomendadas de impresión

September 5, 2022

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:

```
sudo yum  –y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

Configuración

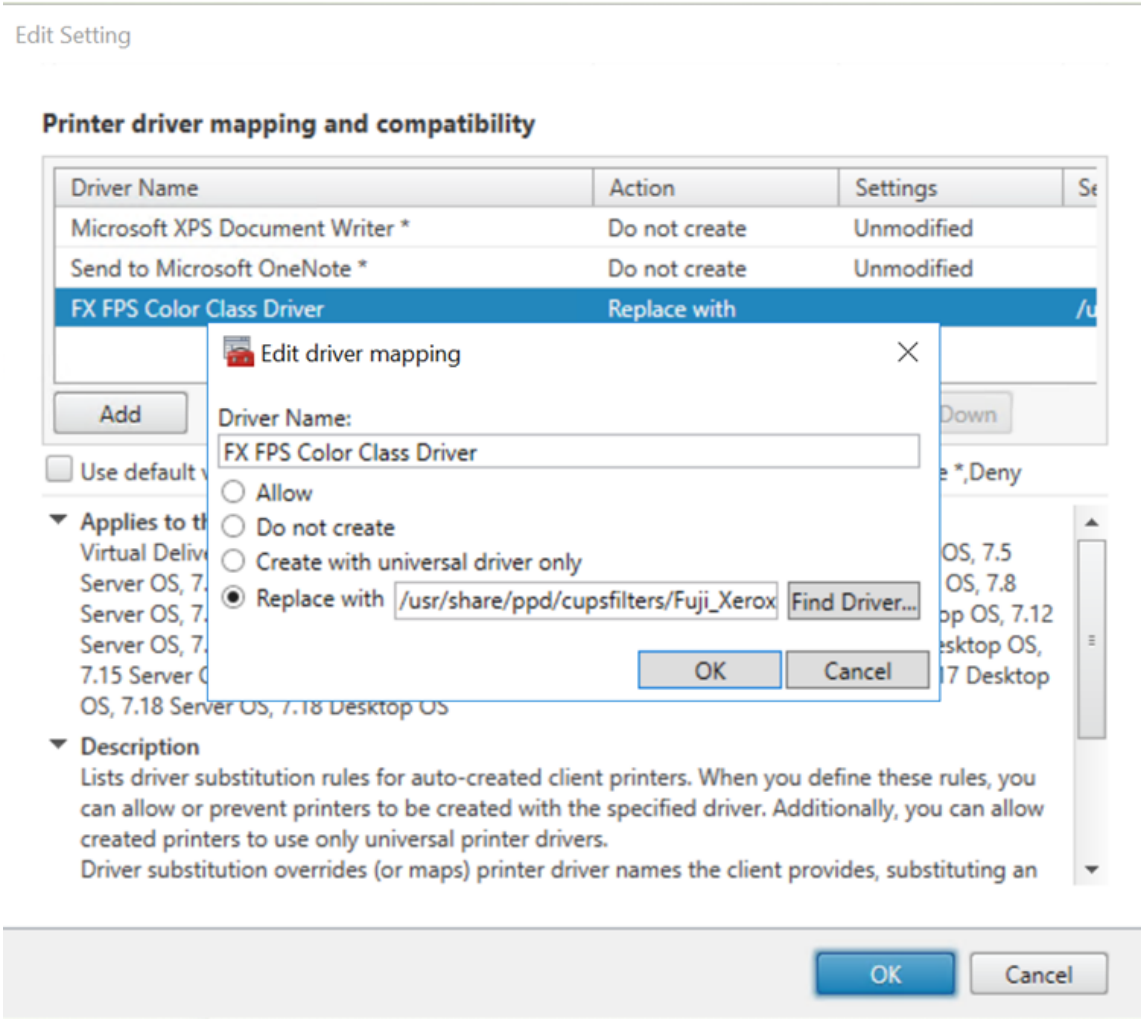
Existen tres tipos de controlador de impresora universal suministrados por Citrix (postscript, pcl5 y pcl6). Sin embargo, es posible que el controlador de impresora universal no sea compatible con la

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Nota:**
>
> - Solo se admiten archivos de controlador PPD.
> - No se admiten otras opciones de la directiva **Asignación y compatibilidad de controladores 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
service ctxcups status
<!--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**:

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
<!--NeedCopy-->
```

> **Nota:**
>
> Esta configuración 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 **~/.CtxlpProfile$CLIENT_NAME**:

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
<!--NeedCopy-->
```

> **Importante:**
>
> El campo **printername** contiene el nombre de la impresora actual predeterminada del cliente. Es un valor de solo lectura. No debe modificarlo.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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**:

```
lpinfo -m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

<!--NeedCopy-->
```

  A continuación, puede configurar el modelo para que coincida con la impresora:

```
model=xerox/ph3115.ppd.gz
<!--NeedCopy-->
```

- Si el controlador de impresora universal no es compatible con la impresora cliente, configure la ruta al archivo PPD del controlador nativo de la impresora. El valor de **ppdpath** es la ruta absoluta al archivo del controlador nativo de la impresora.

  Por ejemplo, hay un controlador **PPD** en /home/tester/NATIVE_PRINTER_DRIVER.ppd:

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
<!--NeedCopy-->
```

- Existen tres tipos de controlador de impresora universal suministrados por Citrix (postscript, pcl5 y pcl6). Puede configurar el tipo de controlador 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:

```
drivertype=pcl5
<!--NeedCopy-->
```

El tamaño de la salida es cero

Pruebe diferentes tipos de impresoras. Asimismo, pruebe una impresora virtual (como CutePDF y PDFCreator) para averiguar si el problema está relacionado con el controlador de la impresora.

El trabajo de impresión depende del controlador de impresora establecido en la impresora predeterminada del cliente. Es importante identificar el tipo de controlador activo actual. Si la impresora

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

   ```
   deletespoolfile=no
   <!--NeedCopy-->
   ```

4. Cierre la sesión y vuelva a iniciarla para cargar los cambios de configuración.
5. Imprima el documento para reproducir el problema. Después de imprimir, habrá un archivo de cola de impresión guardado en **/var/spool/cups-ctx/$logon_user/$spool_file**.
6. Compruebe si la cola de impresión está vacía. Un archivo de cola de impresión vacío representa un problema. Póngase en contacto con la asistencia de Citrix (y facilite el registro de impresión) para obtener más información.
7. Si la cola de impresión no es cero, copie el archivo al cliente. El archivo de cola de impresión depende del tipo de controlador de impresora establecido en la impresora predeterminada del cliente. Si el controlador de la impresora asignada (nativa) es PostScript, el archivo de cola de impresión se puede abrir directamente en el sistema operativo Linux. Compruebe que el contenido sea correcto.

   Si el archivo de cola de impresión es PCL o si el sistema operativo del cliente es Windows, copie el archivo de cola de impresión al cliente e imprímalo 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:

      ```
      localhost:631
      <!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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-->
```

Impresión de PDF

July 6, 2022

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Acceso con Remote PC

July 6, 2022

Información general

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. 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.

Consideraciones

Estas consideraciones son específicas de Linux VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- En máquinas físicas, utilice Linux VDA solo en modo no 3D. Debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no puede oscurecerse por completo cuando el modo HDX 3D está habilitado. Mostrar esta pantalla representa un riesgo potencial para la seguridad.
- Con máquinas Linux físicas, utilice catálogos de máquinas de tipo SO de sesión única.
- La asignación automática de usuarios no está disponible para máquinas Linux. Con la asignación automática de usuarios, los usuarios se asignan automáticamente a sus máquinas cuando inician sesión localmente en los equipos. Este inicio de sesión se produce sin intervención del administrador. La aplicación Citrix Workspace del 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.

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:

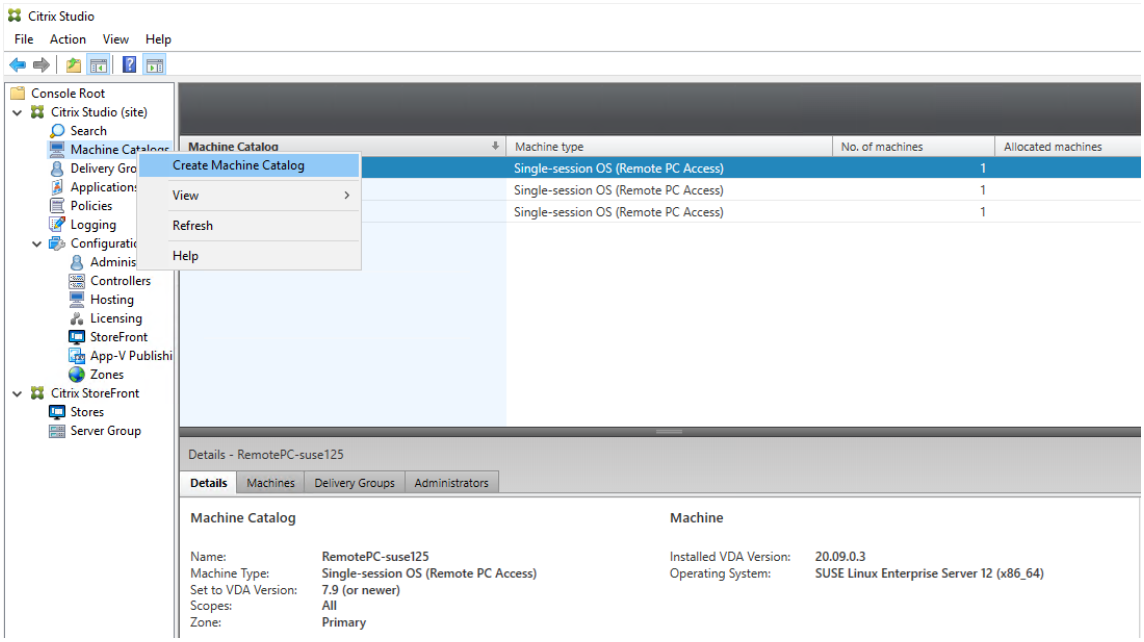
Paso 1 - Instalar Linux VDA en los equipos de destino

Se recomienda utilizar Easy Install para instalar Linux VDA. Durante la instalación, establezca el valor de la variable `CTX_XDL_VDI_MODE` en `Y`.

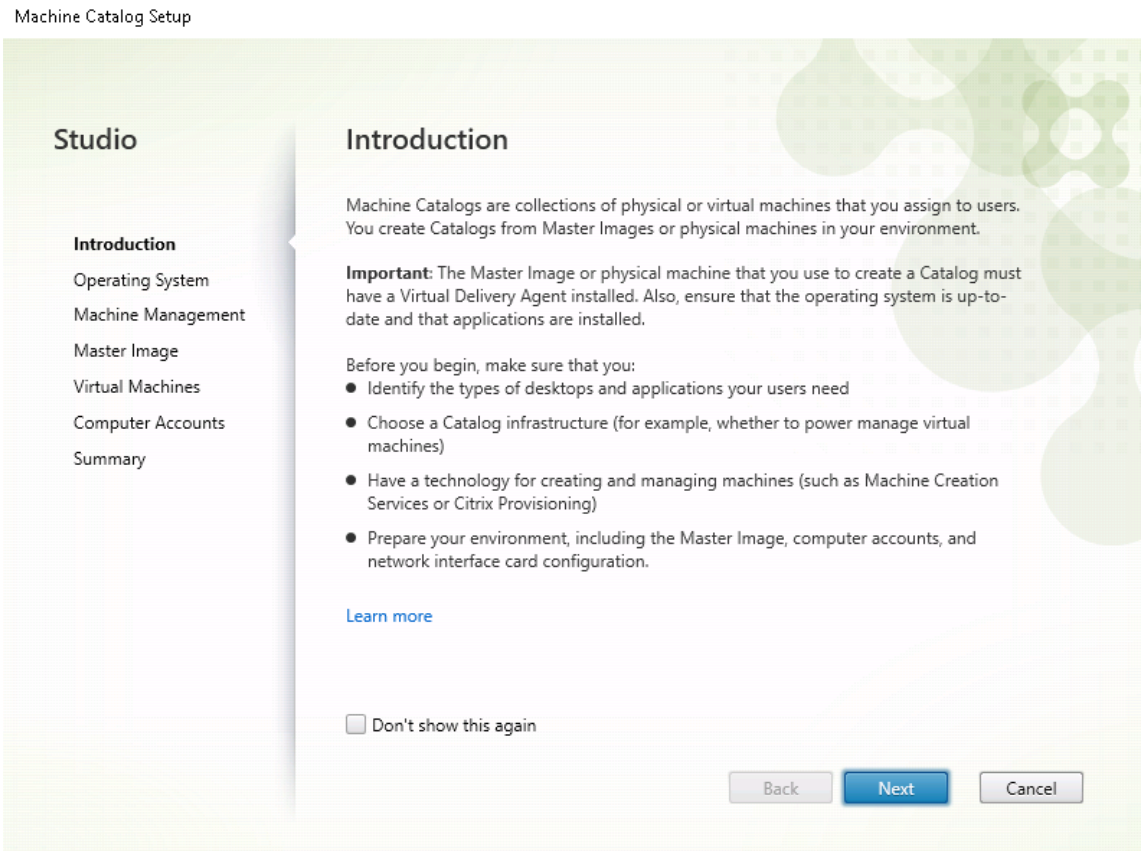
Paso 2 - Crear un catálogo de máquinas de tipo Acceso con Remote PC

1. En Citrix Studio, haga clic con el botón secundario en **Catálogos de máquinas** y seleccione **Crear catálogo de máquinas** en el menú contextual.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

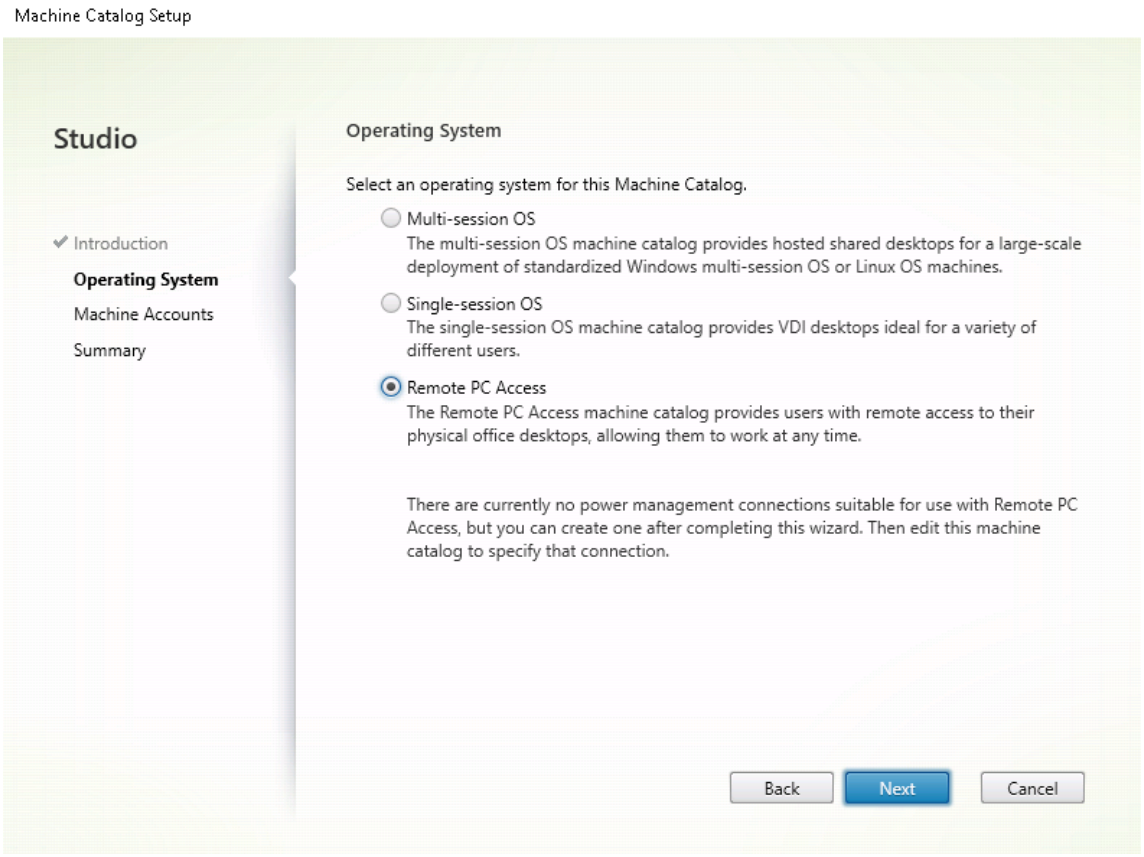


2. En la página **Introducción**, haga clic en **Siguiente**.



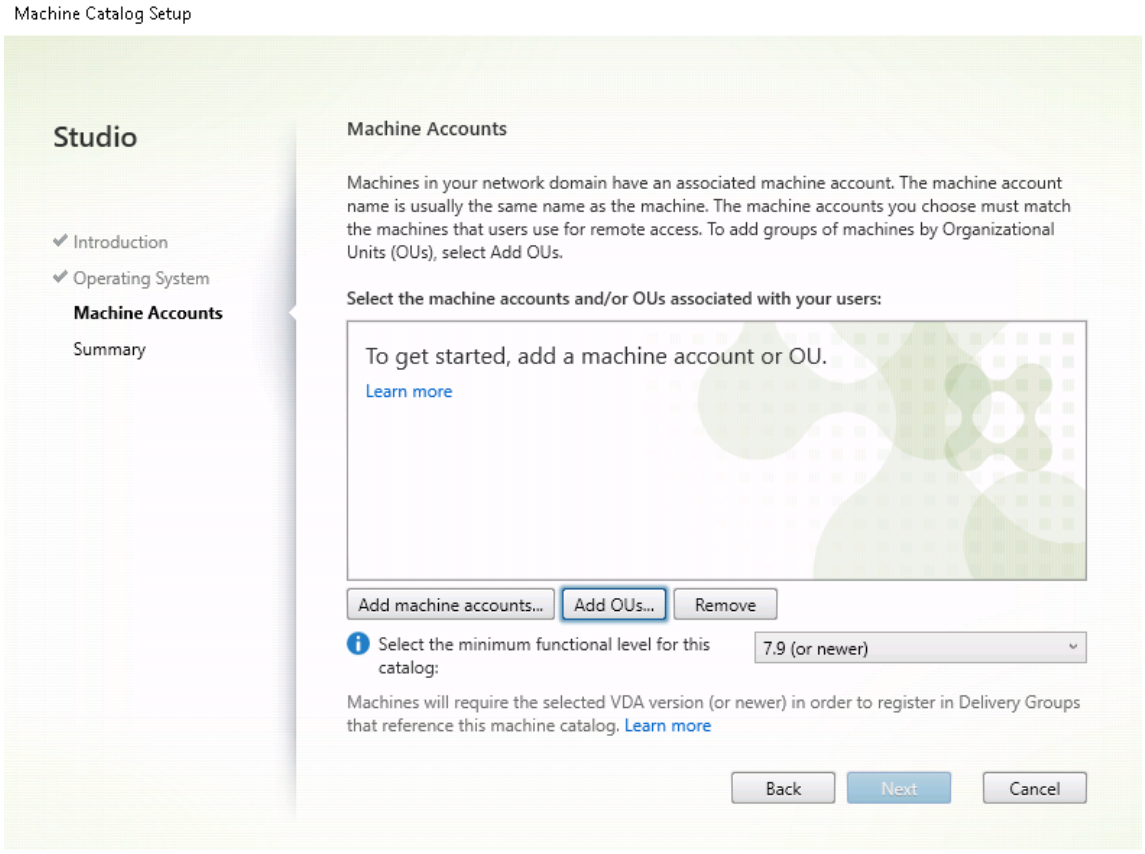
3. En la página **Sistema operativo**, seleccione **Acceso con Remote PC**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



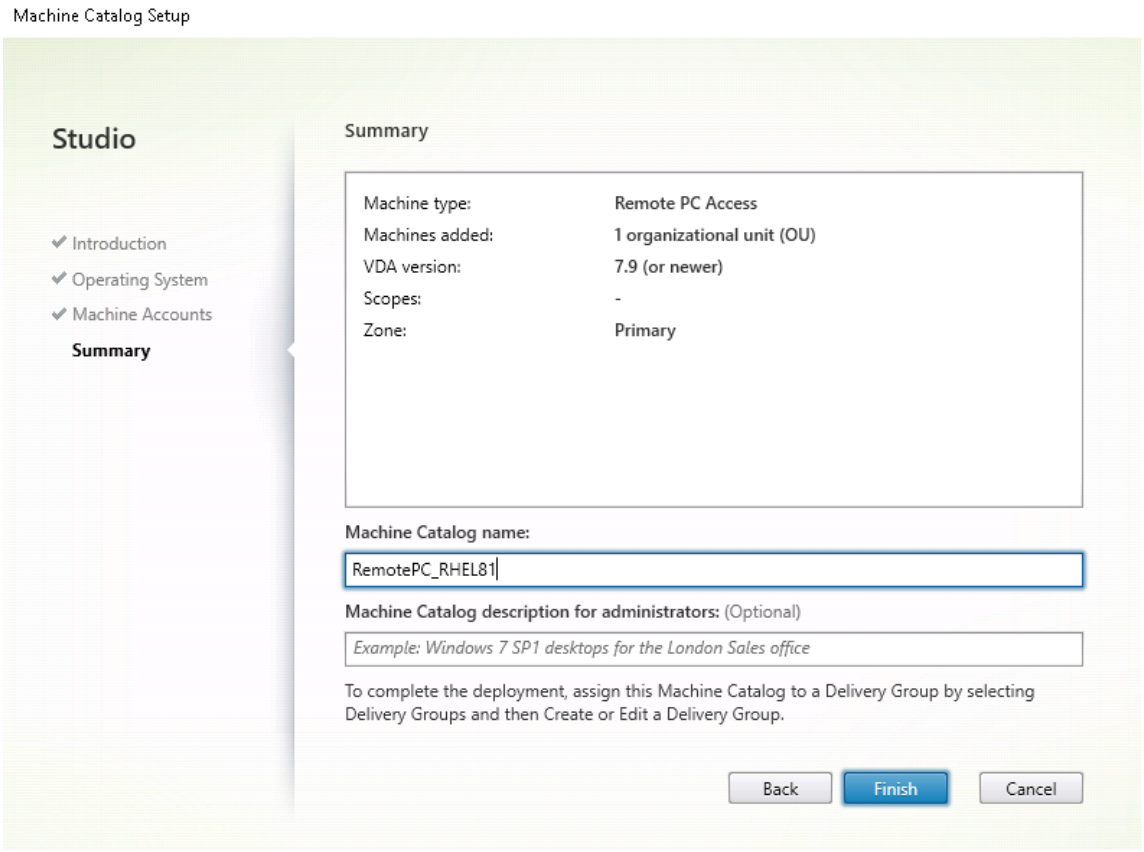
4. Haga clic en **Agregar unidades organizativas** para seleccionar las unidades organizativas que contendrán los equipos de destino o haga clic en **Agregar cuentas de máquina** para agregar máquinas individuales al catálogo de máquinas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

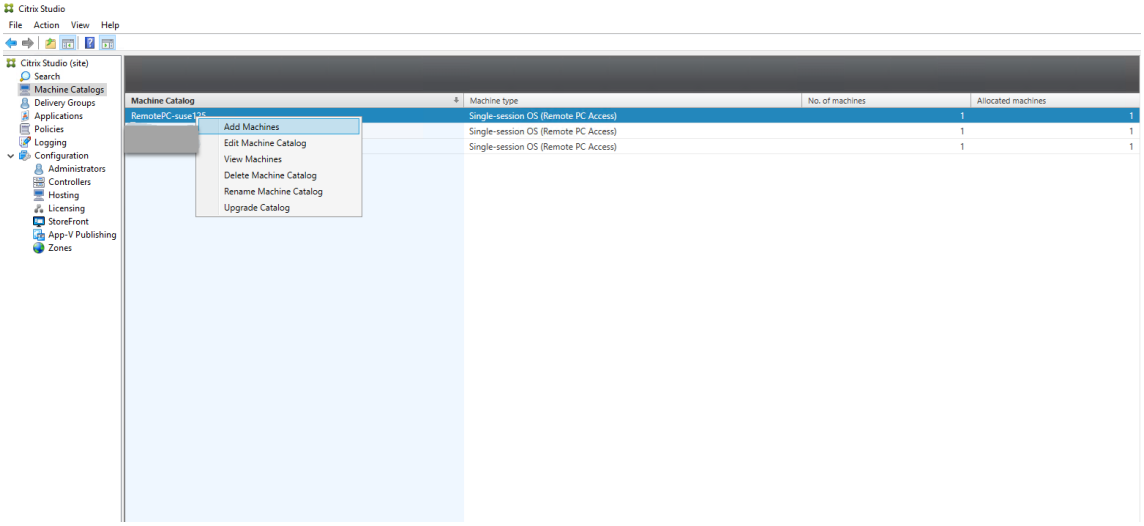


5. Asigne un nombre al catálogo de máquinas.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



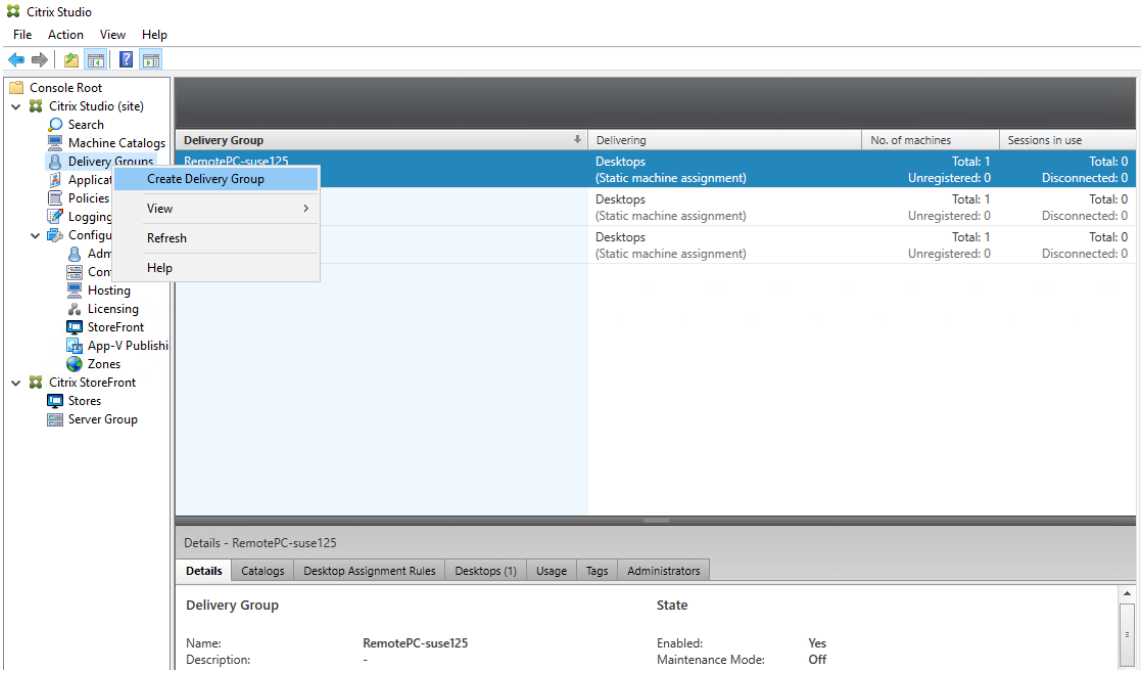
6. (Opcional) Haga clic con el botón secundario en el catálogo de máquinas para realizar las operaciones relevantes.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

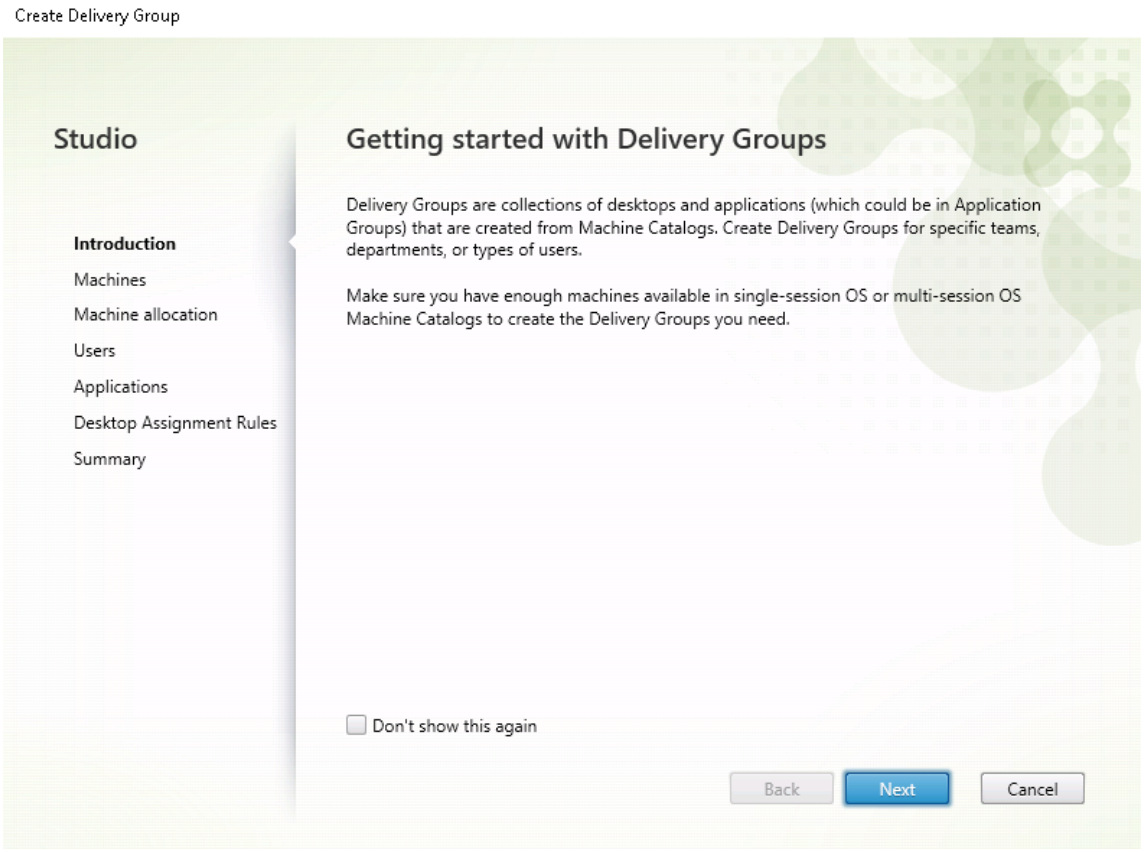
Paso 3 - Crear un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso

1. En Citrix Studio, haga clic con el botón secundario en **Grupos de entrega** y seleccione **Crear grupo de entrega** en el menú contextual.



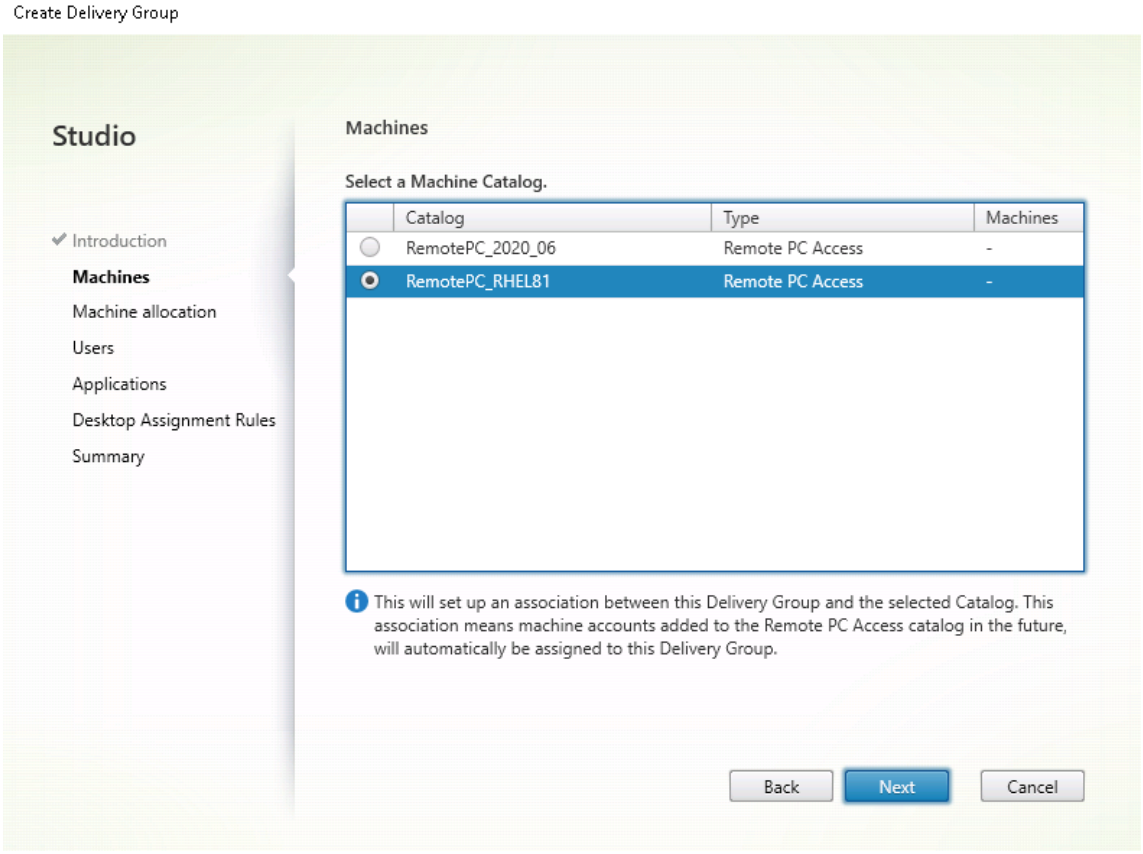
2. Haga clic en **Siguiente** en la página **Introducción a los grupos de entrega**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



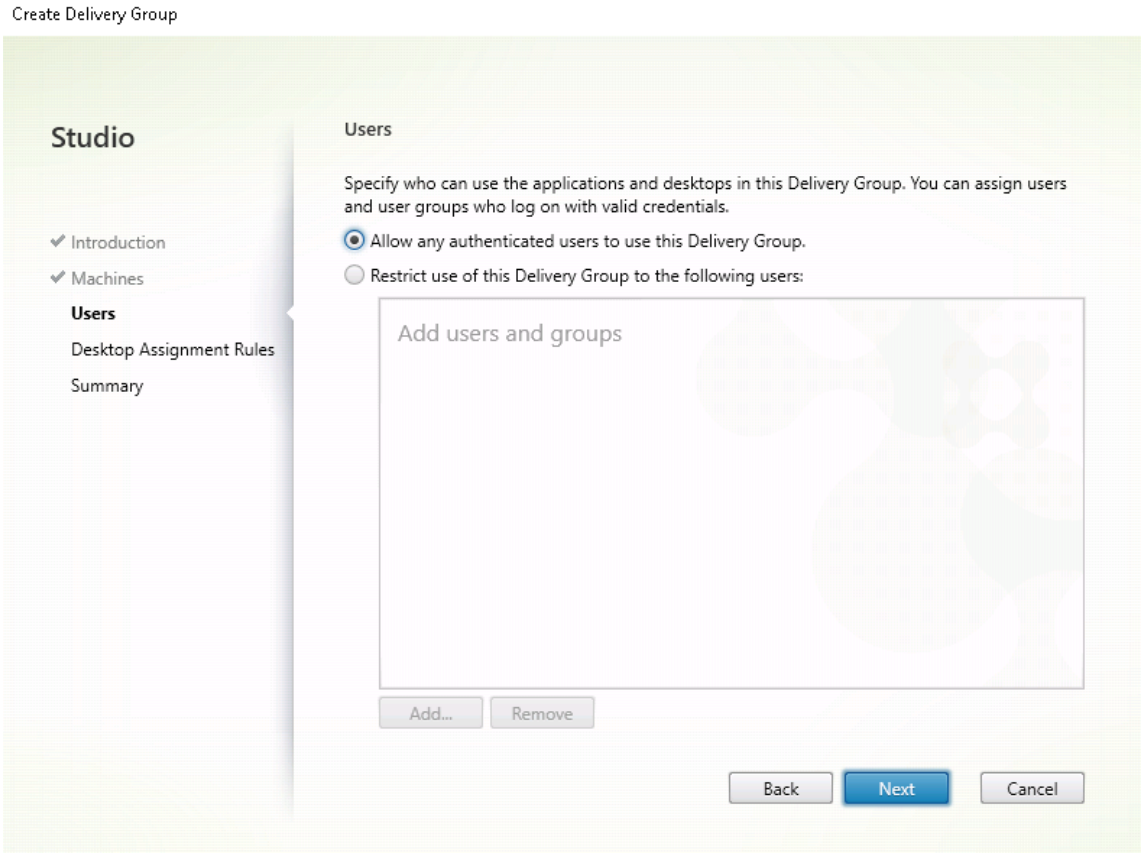
3. Seleccione el catálogo de máquinas creado en el paso 2 para asociarlo al grupo de entrega.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wake on LAN

La función de acceso con Remote PC admite Wake on LAN, el cual ofrece a los usuarios la capacidad de encender equipos físicos de forma remota. Esta función permite a los usuarios mantener apagados sus equipos de oficina cuando no estén en uso, lo que reduce los costes de energía. También permite el acceso remoto cuando una máquina se ha apagado inadvertidamente.

Con la función Wake on LAN, los Magic Packets se envían directamente desde el VDA a la subred en la que reside el equipo cuando se lo indica el Delivery Controller. Esto permite que la función no requiera dependencias de componentes de infraestructura adicionales ni soluciones de terceros para la entrega de Magic Packets.

La función Wake on LAN difiere de la función Wake on LAN que se basa en una versión de SCCM antigua. Para obtener información sobre Wake on LAN basada en SCCM, consulte Función Wake on LAN integrada en SCCM.

Requisitos del sistema

A continuación, se indican los requisitos del sistema para usar la función Wake on LAN:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Plano de control:
  - Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 2012 o una versión posterior
- PC físicos:
  - VDA 2012 o una versión posterior
  - Wake on LAN (WOL) habilitado en el BIOS y en la tarjeta de interfaz de red

Configurar Wake on LAN

Actualmente, la configuración de Wake on LAN integrada solo es compatible cuando se utiliza PowerShell.

Para configurar Wake on LAN:

1. Cree el catálogo de máquinas de acceso con Remote PC si aún no tiene uno.
2. Cree la conexión de host Wake on LAN si aún no tiene una.

   > **Nota:**
   >
   > Para utilizar la función Wake on LAN, si tiene una conexión de host del tipo "Microsoft Configuration Manager Wake on LAN", cree otra conexión de host.

3. Obtenga el identificador único de la conexión de host Wake on LAN.
4. Asocie la conexión de host Wake on LAN a un catálogo de máquinas.

   Para crear la conexión de host Wake on LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
            -Name $connectionName `
            -HypervisorAddress "N/A" `
            -UserName "woluser" `
            -Password "wolpwd" `
            -ConnectionType Custom `
            -PluginId VdaWOLMachineManagerFactory `
            -CustomProperties "<CustomProperties></
               CustomProperties>" `
            -Persist

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -
        HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

Cuando la conexión de host esté lista, ejecute los siguientes comandos para obtener el identificador único de la conexión de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>
    "
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Después de obtener el identificador único de la conexión, ejecute los siguientes comandos para asociar la conexión al catálogo de máquinas de acceso con Remote PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

5. Habilite Wake on LAN en el BIOS y en la tarjeta de interfaz de red en cada máquina virtual del catálogo de máquinas.

   Nota: El método para habilitar Wake on LAN varía según las diferentes configuraciones de la máquina.

   - Para habilitar Wake on LAN en el BIOS:
     a) Acceda al BIOS y habilite la funcionalidad Wake on LAN.
        El método para acceder al BIOS depende del fabricante de la placa base y del proveedor de BIOS que haya seleccionado el fabricante.
     b) Guarde la configuración y reinicie la máquina.
   - Para habilitar Wake on LAN en la tarjeta de interfaz de red:
     a) Ejecute el comando `sudo ethtool <NIC>` para comprobar si su tarjeta de interfaz de red admite Magic Packets.
        `<NIC>` es el nombre de dispositivo de su tarjeta de interfaz de red, por ejemplo, `eth0`.
        El comando `sudo ethtool <NIC>` proporciona información acerca de las capacidades de su tarjeta de interfaz de red:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Si la información contiene una línea similar a `Supports Wake-on: <letters>`, donde `<letters>` contiene la letra `g`, la tarjeta de interfaz de red admite el método Wake on LAN con Magic Packet.
- Si la información contiene una línea similar a `Wake-on: <letters>`, donde `<letters>` contiene la letra `g` y no contiene la letra `d`, se habilitará el método Wake on LAN con Magic Packet. Sin embargo, si `<letters>` contiene la letra `d`, indica que la función Wake on LAN está inhabilitada. En este caso, habilite Wake on LAN ejecutando el comando `sudo ethtool -s <NIC> wol g`.

b) En la mayoría de las distribuciones, el comando `sudo ethtool -s <NIC> wol g` es necesario después de cada inicio. Para establecer esta opción de forma persistente, siga los pasos que se indican a continuación, en función de sus distribuciones:

Ubuntu:

Agregue la línea `up ethtool -s <NIC> wol g` al archivo de configuración de interfaz `/etc/network/interfaces`. Por ejemplo:

```
# ifupdown has been replaced by netplan(5) on this system.
    See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
# sudo apt install ifupdown
auto eth0
iface eth0 inet static
           address 10.0.0.1
           netmask 255.255.240.0
           gateway 10.0.0.1
           up ethtool -s eth0 wol g
<!--NeedCopy-->
```

RHEL/SUSE:

Agregue este parámetro `ETHTOOL_OPTS` al archivo de configuración de interfaz `/etc/sysconfig/network-scripts/ifcfg-<NIC>`:

```
ETHTOOL_OPTS="-s ${
 DEVICE }
  wol g"
<!--NeedCopy-->
```

Consideraciones sobre el diseño

Cuando planee usar Wake on LAN con acceso con Remote PC, tenga en cuenta lo siguiente:

- Varios catálogos de máquinas pueden utilizar la misma conexión de host Wake on LAN.
- Para que un equipo reactive otro equipo, ambos deben estar en la misma subred y utilizar la misma conexión de host Wake on LAN. No importa si los equipos están en los mismos catálogos de máquinas o en catálogos diferentes.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Las conexiones de host se asignan a zonas específicas. Si la implementación contiene más de una zona, debe disponer de una conexión de host Wake on LAN en cada zona. Lo mismo es aplicable a los catálogos de máquinas.
- Los Magic Packets se transmiten mediante la dirección de difusión global 255.255.255.255. Asegúrese de que la dirección no esté bloqueada.
- Debe haber al menos un equipo encendido en la subred por cada conexión Wake on LAN para poder activar máquinas en esa subred.

Consideraciones operativas

A continuación, se incluyen consideraciones para uso de la función Wake on LAN:

- El VDA debe registrarse al menos una vez antes de que el PC pueda activarse mediante la función Wake on LAN integrada.
- Wake on LAN solo se puede utilizar para activar PC. No admite otras acciones de energía, como reinicio o apagado.
- Después de crear la conexión Wake on LAN, es visible en Studio. Sin embargo, no se admite la modificación de sus propiedades dentro de Studio.
- Los Magic Packets se envían de una de dos maneras:
  - Cuando un usuario intenta iniciar una sesión en su PC y el VDA no está registrado
  - Cuando un administrador envía manualmente un comando de encendido desde Studio o PowerShell
- Dado que el Delivery Controller no conoce el estado de energía de un equipo, Studio muestra **No compatible** con el estado de alimentación. El Delivery Controller utiliza el estado del registro del VDA para determinar si un equipo está encendido o apagado.

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.

La función de persistencia

July 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Esta sección contiene estos temas:

- Transporte adaptable
- Iniciar sesión con un directorio de inicio temporal
- Publicar aplicaciones
- Fiabilidad de la sesión
- Rendezvous V1
- Rendezvous V2
- Sesiones de usuario seguras mediante TLS
- Sesiones de usuario seguras mediante DTLS

Transporte adaptable

July 6, 2022

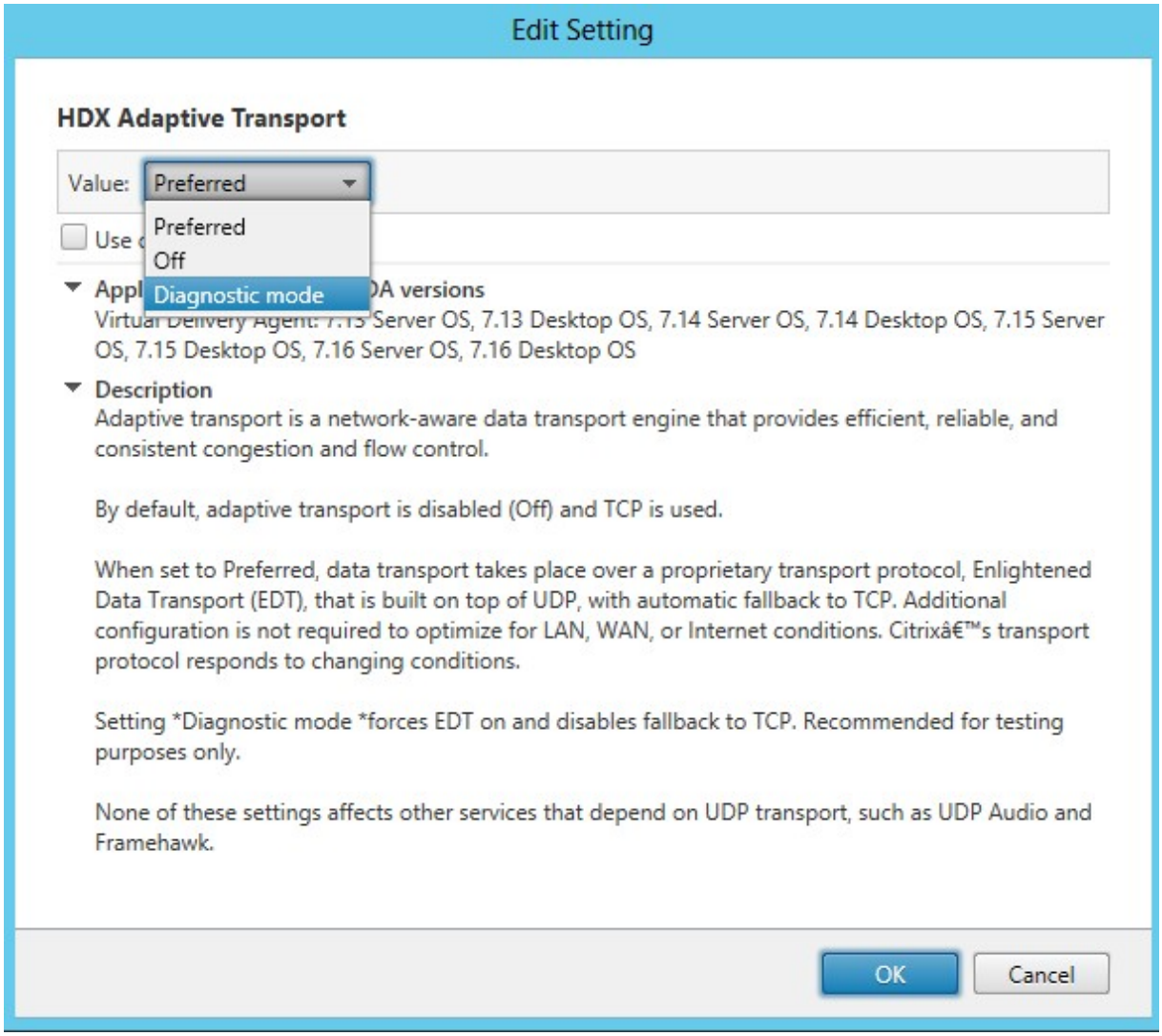
El transporte adaptable es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops. Es más rápido, más escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones de Internet y WAN difíciles de largo recorrido. Para obtener más información sobre el transporte adaptable, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Inhabilitar el transporte adaptable

Para inhabilitar el transporte adaptable, **desactive** la **directiva de transporte adaptable HDX** en Citrix Studio.

Comprobar si el transporte adaptable está habilitado

Ejecute este comando para comprobar si los agentes de escucha UDP están en ejecución.

```
netstat -an | grep "1494|2598"
<!--NeedCopy-->
```

En situaciones habituales, el resultado es similar a este:

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
udp        0      0 :::1494                 :::*
<!--NeedCopy-->
```

Detección de MTU en EDT

EDT determina automáticamente la unidad de transmisión máxima (MTU) al establecer una sesión. Al hacerlo, se evita la fragmentación de paquetes de EDT que podría provocar una degradación del rendimiento o un error al establecer una sesión.

Requisitos mínimos:

- Linux VDA 2012
- Aplicación Citrix Workspace 1911 para Windows
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Fiabilidad de la sesión debe estar habilitada

Si utiliza plataformas de cliente o versiones que no admiten esta función, puede configurar una unidad de transmisión máxima de EDT personalizada adecuada para su entorno. Para obtener más información, consulte el artículo CTX231821 de Knowledge Center.

> **ADVERTENCIA:**
>
> Si modifica el Registro de forma incorrecta, pueden ocurrir problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del **Editor del Registro** puedan resolverse. Si utiliza el **Editor del Registro**, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Habilitar o inhabilitar la detección de MTU en EDT en el VDA

La detección de MTU en EDT está inhabilitada de forma predeterminada.

- Para habilitar la detección de MTU en EDT, establezca la clave `MtuDiscovery` del Registro con el siguiente comando, reinicie el VDA y espere a que el VDA se registre:

  ```
  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet
  \Control\Terminal Server\Wds\icawd"-t "REG_DWORD"-v "MtuDiscovery
  "-d "0x00000001"--force
  ```

- Para inhabilitar la detección de MTU en EDT, elimine el valor `MtuDiscovery` del Registro.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Controlar la detección de MTU en EDT en el cliente

Puede controlar la detección de MTU en EDT selectivamente en el cliente agregando el parámetro `MtuDiscovery` en el archivo ICA. Para inhabilitar la función, establezca lo siguiente en la sección `Application`:

```
MtuDiscovery=Off
```

Para volver a habilitar la función, quite el parámetro `MtuDiscovery` del archivo ICA.

> **IMPORTANTE:**
>
> Para que este parámetro del archivo ICA funcione, habilite la detección de MTU en EDT en el VDA. Si la detección de MTU en EDT no está habilitada en el VDA, el parámetro del archivo ICA no surte ningún efecto.

Iniciar sesión con un directorio de inicio temporal

July 6, 2022

Puede especificar un directorio de inicio temporal para los casos en los que el punto de montaje de Linux VDA falle. Al especificarse un directorio de inicio temporal, se muestra un mensaje durante el inicio de sesión cuando el punto de montaje falla. Los datos del usuario se almacenan en el directorio de inicio temporal.

En la siguiente tabla se describen las claves de Registro que sirven de ayuda en la configuración del directorio de inicio.

Clave del Registro	Descripción	Comando
`LogNoHome`	Controla si los usuarios pueden conectarse a sesiones sin un directorio de inicio. El valor predeterminado es 1 y significa sí. Si el valor se establece en 0, se inhabilita la conexión a sesiones sin un directorio de inicio.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Clave del Registro	Descripción	Comando
HomeMountPoint	Establece un punto de montaje local en Linux VDA. Por ejemplo, si el punto de montaje es /mnt/home, el directorio de inicio de un usuario es /mnt/home/domain/<user_name>. Asegúrese de que el punto de montaje sea el mismo que el directorio de inicio del usuario de su entorno.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "<A directory where the NFS share is to be mounted>"--force
TempHomeDirectoryPath	Establece un directorio de inicio temporal en Linux VDA en caso de que el punto de montaje falle. El valor predeterminado es /tmp. La clave de Registro depende de HomeMountPoint. Solo surte efecto cuando el sistema detecta que el punto de montaje no está disponible. Un directorio de inicio temporal para un usuario es /tmp/domain/user_id.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "</tmp by default>"--force
RemoveHomeOnLogoff	Controla si deben eliminarse los directorios de inicio temporales cuando los usuarios cierran sesión. 1 significa sí. 0 significa no.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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).

> **Nota:**
>
> - Cuando configure grupos de entrega, compruebe que el tipo de entrega está establecido en **Escritorio y aplicaciones** o **Aplicaciones**.
> - 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, se recomienda crear grupos de entrega separados para entregar escritorios y aplicaciones.
> - 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

En una sesión de aplicación, solo los accesos directos específicos de la aplicación funcionan según lo previsto.

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.
- 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.

Rendezvous V1

July 6, 2022

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

Hay dos tipos de tráfico que se deben tener en cuenta: 1) el tráfico de control para el registro de VDA y la intermediación de sesiones; 2) el tráfico de sesiones HDX.

Rendezvous V1 permite que el tráfico de sesiones HDX omita los Cloud Connectors, pero aun así requiere que los Cloud Connectors hagan de intermediario de todo el tráfico de control para el registro de VDA y la intermediación de sesiones.

Requisitos

- Acceda al entorno mediante Citrix Workspace y Citrix Gateway Service.
- Plano de control: Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).
- Linux VDA 2112 o una versión posterior
  - 2112 es la versión la mínima necesaria para los proxies HTTP no transparentes.
  - 2204 es la versión mínima necesaria para los proxies transparentes y SOCKS5.
- Habilite el protocolo Rendezvous en la directiva de Citrix. Para obtener más información, consulte Configuración de directiva del protocolo Rendezvous.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Los agentes VDA deben tener acceso a `https://*.nssvc.net`, incluidos todos los subdominios. Si no puede incluir en la lista de permitidos todos los subdominios de esa manera, use `https://*.c.nssvc.net` y `https://*.g.nssvc.net` en su lugar. Para obtener más información, consulte la sección Requisitos de la conectividad a Internet de la documentación de Citrix Cloud (en Virtual Apps and Desktops Service) y el artículo CTX270584 de Knowledge Center.
- Los Cloud Connectors deben obtener los FQDN de los VDA al hacer de intermediarios en una sesión. Para lograr este objetivo, habilite la resolución DNS para el sitio: En el SDK de PowerShell remoto de Citrix DaaS, ejecute el comando `Set-BrokerSite -DnsResolutionEnabled $true`. Para obtener más información sobre el SDK de PowerShell remoto de Citrix DaaS, consulte SDK y API.

Configuración de proxy

Se pueden establecer conexiones Rendezvous a través de proxies HTTP y SOCKS5 en el VDA.

Consideraciones sobre servidores proxy

Tenga en cuenta lo siguiente al usar servidores proxy con Rendezvous:

- Se admiten proxies HTTP no transparentes y proxies SOCKS5.
- No se admite el descifrado y la inspección de paquetes. Configure una excepción para que el tráfico ICA entre el VDA y Gateway Service no se intercepte, descifre o inspeccione. De lo contrario, la conexión se interrumpe.
- Los proxies HTTP admiten la autenticación por máquina mediante protocolos de autenticación Negotiate y Kerberos. Cuando se conecta al servidor proxy, el esquema de autenticación Negotiate selecciona automáticamente el protocolo Kerberos. Kerberos es el único esquema que admite Linux VDA.

  > **Nota:**
  >
  > Para utilizar Kerberos, debe crear el nombre principal de servicio (SPN) para el servidor proxy y asociarlo a la cuenta de Active Directory del proxy. El VDA genera el SPN en el formato `HTTP/<proxyURL>` al establecer una sesión, donde la URL del proxy se obtiene de la configuración de directiva de **proxy Rendezvous**. Si no crea un SPN, se produce un error en la autenticación.

- Actualmente, no se admite la autenticación con un proxy SOCKS5. Si utiliza un proxy SOCKS5 , deberá configurar una excepción para que el tráfico destinado a las direcciones de Gateway Service (especificadas en los requisitos) pueda omitir la autenticación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como el protocolo de transporte para ICA.

Proxy transparente

Se admite un proxy HTTP transparente con Rendezvous. Si utiliza un proxy transparente en la red, no se requiere configuración adicional en el VDA.

Proxy no transparente

Al utilizar un proxy no transparente en la red, configure el parámetro Configuración del proxy Rendezvous. Cuando la configuración está habilitada, especifique la dirección de proxy HTTP o SOCKS5 para que el VDA sepa qué proxy usar. Por ejemplo:

- Dirección de proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`

Comprobación de Rendezvous

Si cumple todos los requisitos, siga estos pasos para comprobar si se utiliza Rendezvous:

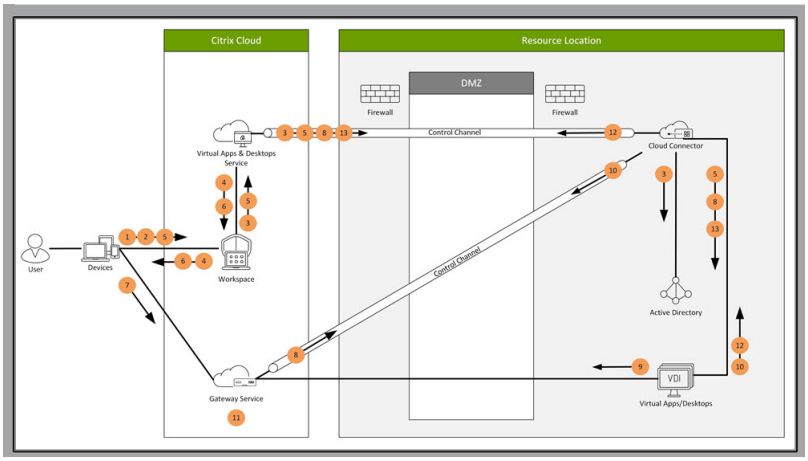
1. Inicie un terminal en el VDA.
2. Ejecute `/opt/Citrix/VDA/bin/ctxquery -f iP`.
3. Los PROTOCOLOS DE TRANSPORTE en uso indican el tipo de conexión:
    - TCP Rendezvous: TCP - TLS - CGP - ICA
    - EDT Rendezvous: UDP - DTLS - CGP - ICA
    - Proxy a través de Cloud Connector: TCP - PROXY - SSL - CGP - ICA o UDP - PROXY - DTLS - CGP - ICA

> **Sugerencia:**
>
> Si el VDA no puede acceder directamente a Citrix Gateway Service con Rendezvous habilitado, el VDA recurre al Cloud Connector para hacer de intermediario con la sesión HDX.

Cómo funciona Rendezvous

Este diagrama es una descripción general del flujo de conexión de Rendezvous.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Siga los pasos para entender el flujo.

1. Vaya a Citrix Workspace.
2. Introduzca las credenciales en Citrix Workspace.
3. Si utiliza Active Directory de manera local, Citrix DaaS autentica las credenciales con Active Directory mediante el canal del Cloud Connector.
4. Citrix Workspace muestra los recursos enumerados de Citrix DaaS.
5. Seleccione recursos de Citrix Workspace. Citrix DaaS envía un mensaje al VDA con el fin de prepararse para una sesión entrante.
6. Citrix Workspace envía un archivo ICA al dispositivo de punto final que contiene un tíquet de STA generado por Citrix Cloud.
7. El dispositivo de punto final se conecta a Citrix Gateway Service y proporciona el tíquet para conectarse al VDA, tras lo cual Citrix Cloud valida el tíquet.
8. Citrix Gateway Service envía información de la conexión al Cloud Connector. El Cloud Connector determina si la conexión es una conexión con Rendezvous y envía la información al VDA.
9. El VDA establece una conexión directa con Citrix Gateway Service.
10. Si no es posible establecer una conexión directa entre el VDA y Citrix Gateway Service, el VDA emplea el Cloud Connector como intermediario.
11. Citrix Gateway Servicio establece una conexión entre el dispositivo de punto final y el VDA.
12. El VDA verifica su licencia con Citrix DaaS a través del Cloud Connector.
13. Citrix DaaS envía directivas de sesión al VDA a través del Cloud Connector. Esas directivas se aplican.

Rendezvous V2

October 3, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Hay dos tipos de tráfico que se deben tener en cuenta: 1) el tráfico de control para el registro de VDA y la intermediación de sesiones; 2) el tráfico de sesiones HDX.

Rendezvous V1 permite que el tráfico de sesiones HDX omita los Cloud Connectors, pero aun así requiere que los Cloud Connectors hagan de intermediario de todo el tráfico de control para el registro de VDA y la intermediación de sesiones.

Las máquinas unidas a un dominio de AD estándar y las máquinas no unidas a ningún dominio pueden usar Rendezvous V2 con Linux VDA de sesión única y multisesión. En el caso de máquinas que no estén unidas a ningún dominio, Rendezvous V2 permite que tanto el tráfico HDX como el tráfico de control omitan los Cloud Connectors.

Requisitos

Los requisitos para usar Rendezvous V2 son:

- Acceso al entorno mediante Citrix Workspace y Citrix Gateway Service.
- Plano de control: Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).
- Versión 2201 de VDA o una posterior.
  - 2204 es la versión mínima necesaria para los proxies HTTP y SOCKS5.
- Habilite el protocolo Rendezvous en la directiva de Citrix. Para obtener más información, consulte Configuración de directiva del protocolo Rendezvous.
- Los agentes VDA deben tener acceso a `https://*.nssvc.net`, incluidos todos los subdominios. Si no puede incluir en la lista de permitidos todos los subdominios de esa manera, use `https://*.c.nssvc.net` y `https://*.g.nssvc.net` en su lugar. Para obtener más información, consulte la sección Requisitos de la conectividad a Internet de la documentación de Citrix Cloud (en Virtual Apps and Desktops Service) y el artículo CTX270584 de Knowledge Center.
- Los VDA deben poder conectarse a las direcciones mencionadas anteriormente:
  - En TCP 443, para Rendezvous con TCP.
  - En UDP 443, para Rendezvous con EDT.

Configuración de proxy

El VDA admite la conexión a través de proxy tanto para el tráfico de control como para el tráfico de sesiones HDX cuando se usa Rendezvous. Los requisitos y consideraciones para ambos tipos de tráfico son diferentes, así que revíselos detenidamente.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Consideraciones sobre el proxy de tráfico

- Solo se admiten proxies HTTP.
- No se admite el descifrado y la inspección de paquetes. Configure una excepción para que el tráfico de control entre el VDA y el plano de control de Citrix Cloud no se intercepte, descifre ni inspeccione. De lo contrario, la conexión falla.
- No se admite la autenticación de proxy.
- Para configurar un proxy para controlar el tráfico, modifique el Registro de la siguiente manera:

```
1  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
       VirtualDesktopAgent" -t "REG_SZ" -v "ProxySettings" -d "http
       ://<URL or IP>:<port>" --force
2  <!--NeedCopy-->
```

Consideraciones sobre el proxy de tráfico HDX

- Se admiten los proxies HTTP y SOCKS5.
- EDT solo se puede usar con proxies SOCKS5.
- Para configurar un proxy para el tráfico HDX, utilice el parámetro de directiva Configuración del proxy de Rendezvous.
- No se admite el descifrado y la inspección de paquetes. Configure una excepción para que el tráfico HDX entre el VDA y el plano de control de Citrix Cloud no se intercepte, descifre ni inspeccione. De lo contrario, la conexión falla.
- Los proxies HTTP admiten la autenticación por máquina mediante protocolos de autenticación Negotiate y Kerberos. Cuando se conecta al servidor proxy, el esquema de autenticación Negotiate selecciona automáticamente el protocolo Kerberos. Kerberos es el único esquema que admite Linux VDA.

  > **Nota:**
  >
  > Para utilizar Kerberos, debe crear el nombre principal de servicio (SPN) para el servidor proxy y asociarlo a la cuenta de Active Directory del proxy. El VDA genera el SPN en el formato `HTTP/<proxyURL>` al establecer una sesión, donde la URL del proxy se obtiene de la configuración de directiva de **proxy Rendezvous**. Si no crea un SPN, se produce un error en la autenticación.

- Actualmente, no se admite la autenticación con un proxy SOCKS5. Si utiliza un proxy SOCKS5 , deberá configurar una excepción para que el tráfico destinado a las direcciones de Gateway Service (especificadas en los requisitos) pueda omitir la autenticación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como el protocolo de transporte para ICA.

Proxy transparente

Se admite un proxy HTTP transparente con Rendezvous. Si utiliza un proxy transparente en la red, no se requiere configuración adicional en el VDA.

Cómo configurar Rendezvous V2

A continuación, se muestran los pasos necesarios para configurar Rendezvous en su entorno:

1. Compruebe que se cumplen todos los requisitos.
2. Una vez instalado el VDA, ejecute este comando para establecer la clave de Registro requerida:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "GctRegistration" -d "0
     x00000001" --force
2 <!--NeedCopy-->
```

3. Reinicie la máquina del VDA.
4. Cree una directiva de Citrix o modifique una existente:
   - Establezca el parámetro Protocolo Rendezvous en **Permitido**.
   - Asegúrese de que los filtros de directivas de Citrix estén configurados correctamente. La directiva se aplica a las máquinas que necesitan habilitar Rendezvous.
   - Compruebe que la directiva de Citrix tenga la prioridad correcta para que no sobrescriba a otra.

Comprobación de Rendezvous

Para comprobar si una sesión utiliza el protocolo Rendezvous, ejecute el comando `/opt/Citrix/VDA/bin/ctxquery -f iP` en el terminal.

Los protocolos de transporte en uso indican el tipo de conexión:

- TCP Rendezvous: TCP - TLS - CGP - ICA
- EDT Rendezvous: UDP - DTLS - CGP - ICA
- Proxy a través de Cloud Connector: TCP - PROXY - SSL - CGP - ICA o UDP - PROXY - DTLS - CGP - ICA

Si Rendezvous V2 se está usando, la versión del protocolo muestra 2.0.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Sugerencia:**
>
> Si el VDA no puede acceder directamente a Citrix Gateway Service con Rendezvous habilitado, el VDA recurre al Cloud Connector para hacer de intermediario con la sesión HDX.

Sesiones de usuario seguras mediante DTLS

July 6, 2022

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, use la herramienta `enable_vdassl.sh` en **/opt/Citrix/VDA/sbin** para habilitar (o inhabilitar) el cifrado SSL. 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` mediante la herramienta `enable_vdassl.sh`.

Sesiones de usuario seguras mediante TLS

July 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, instale certificados y habilite el cifrado TLS en el Linux VDA y el Delivery Controller (el Controller).

Instalar certificados en Linux VDA

Obtenga certificados de servidor en formato PEM y certificados raíz en formato CRT. Un certificado de servidor contiene estas secciones:

- Certificado
- Clave privada no cifrada
- Certificados intermedios (opcional)

Un ejemplo de certificado de servidor:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
-----BEGIN CERTIFICATE-----
MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL
MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE
ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G
A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTTOdxcivbIOLOF66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9
t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEwl3YxM6COyBf7L6psrsCDNnBPlq8TJH
4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8yOw
gZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB
AD5axBYHwIxJCJzNt2zdXnbp2O0yUToWElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68
Vel8u1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbuOIjOtr3pkxAe
b6CFJtNLudHUrwF6lOrB72zbyz3PiIx+HEwt1jOj8z4K
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
R+MaDyF1HmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea
FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSxOYb/lAdck/
FXzU0tqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1kRZjIN5uz
Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri9O+OoEPxclvvp5ne8QOzUpshbjFEPbOC
ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
fIenmTrfZ+Wo4DaKg+8ar2OvOnKFOHFAmDECQQDEwRlH6cE3WyCfN1u942M9XkhR
GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
h5eEmxSZS50TvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
EjAQBgNVBAgTCUNhbWJyawRnZTESMBAGA1UEBxMJQ2FtYm9lcmSlMRQwEgYDVQQK
EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKVZmF7Uj7uOnvO3Qwdfi0nr3QkNH2DXpWrZ
Zh8cI9Vv+UFRUiC6oB7izLtBMFn3fOUP7i2CfkHN3ZGJ17p89pdyjket1MslVeJw
acOqrYvD+fNNSvJjunTbaCywVtALjmFSfMHeZJXVSckrpEhnk0nkMS16tcrya/K/
osSlzvI3AgMBAAGjgcwwgckwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU85kN1EPJ
OcVhcOss1slseDQwGsIwgZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQw
GsKha6RpMGcxCzAJBgNVBAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNV
BAcTCUNhbWJvdXJuZTEUMBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNh
MDAxLmNpdHJpdGUubmV0ggkAy8nC8dcB32EwDQYJKoZIhvcNAQEFBQADgYEAIZ4Z
gXLLXf12RNqh/awtSbd41Ugv8BIKAsg5zhNAiTiXbzz8Cl3ec53Fb6nigMWc5Tli
UNCLXwnxRUiD4O0tESLX9ACUNH3I94yxOgujkSOSBni21jjZTvfBB32Rmr5DByJg
UmKORn/hdqMlcqpe5wO6as6+HN4WUOi+hEtUMME=
-----END CERTIFICATE-----
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Habilitar el cifrado TLS

Habilitar el cifrado TLS en Linux VDA En Linux VDA, use el script `enable_vdassl.sh` del directorio **/opt/Citrix/VDA/sbin** para habilitar (o inhabilitar) el cifrado TLS. Para obtener información acerca de las opciones disponibles en el script, ejecute el comando `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help`.

```
root@lxu1804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used, If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
       -Certificate <CERT-FILE>
       Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
       is currently supported, that is PEM.

       -RootCertificate <ROOT-CERT-FILE>
       Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path, The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

       -SSLPort <SSL-PORT-NUMBER>
       Specify an SSL port number. Unless otherwise specified, the default port 443 used.

       -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
       Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

       -SSLCipherSuite <GOV|COM|ALL>
       Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem"
       Enable Linux VDA SSL using Certificate cert001.pem.

       enable-vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
       Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -SSLPort 445
       Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
       Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

Sugerencia: 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`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

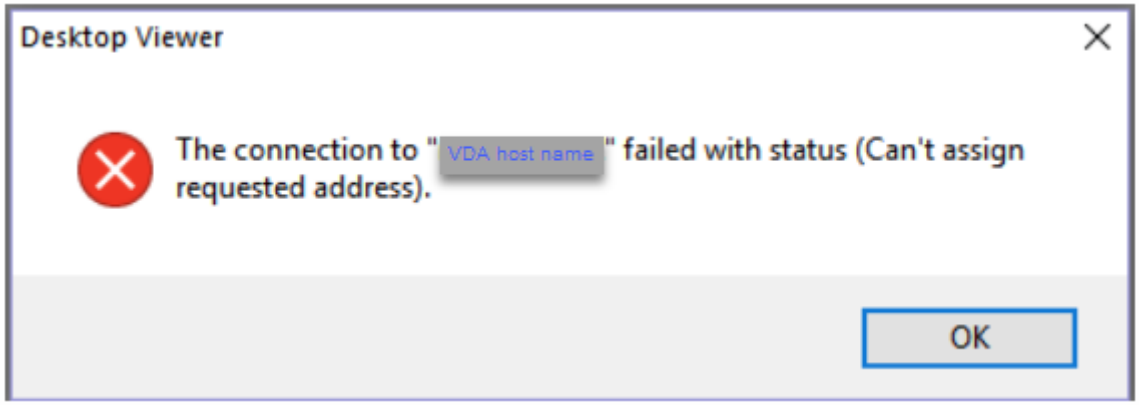
> **Nota:**
>
> Para asegurarse de que solo los nombres de dominio completos de los VDA están contenidos en el archivo de una sesión ICA, también puede ejecutar el comando `Set-BrokerSite –DnsResolutionEnabled $true`. Este comando habilita la resolución DNS. Si inhabilita la resolución DNS, el archivo 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 "No se puede asignar la dirección solicitada"en la aplicación Citrix Workspace para Windows al intentar acceder a una sesión de escritorio publicado:



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`.

Fiabilidad de la sesión

July 6, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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).

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\WinStations\cgp" -v "PortNumber"
    -d "2599"
<!--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**

Cuando no hay actividad (por ejemplo, no se mueve el mouse ni se actualiza la pantalla) en una sesión, se envían mensajes de Keep Alive entre Linux VDA y el cliente. 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).

```
/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).

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\XTEConfig" -t "REG_DWORD" -v "CgpClientToServerKeepAlive"
    -d "10" --force
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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).

   ```
   netstat -an | grep 2598
   <!--NeedCopy-->
   ```

   Si no hay ningún agente de escucha TCP en el puerto de la fiabilidad de la sesión, habilítelo con este comando.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
      CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
      fEnableWinStation" -d "0x00000001"
   <!--NeedCopy-->
   ```

Redirección de USB

September 5, 2022

Los dispositivos USB se comparten entre la aplicación Citrix Workspace y el escritorio de Linux VDA. Cuando un dispositivo USB se redirige al escritorio, puede usar ese dispositivo como si estuviera conectado localmente.

> **Consejo:**
>
> Se recomienda utilizar redirección USB cuando la latencia de red es inferior a 100 milisegundos. No utilice redirección USB cuando la latencia de red sea superior a 200 milisegundos.

La redirección USB incluye tres áreas principales de funcionalidad:

- Implementación de proyectos de código abierto (VHCI)
- Servicio VHCI
- Servicio USB

VHCI de código abierto:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 actúa como un módulo que administra la virtualización y las transferencias de datos en el dispositivo USB.

Cómo funciona la redirección USB

Por lo general, si un dispositivo USB se redirige correctamente a Linux VDA, se crean uno o varios nodos de dispositivos en la ruta /dev del sistema. Sin embargo, hay veces en que el dispositivo redirigido no puede utilizarse para una sesión activa de Linux VDA. Los dispositivos USB necesitan los controladores pertinentes para poder funcionar correctamente; algunos dispositivos requieren incluso controladores especiales. Por eso, si no se proporcionan los controladores adecuados, los dispositivos USB redirigidos resultan inaccesibles para una sesión activa de Linux VDA. Para garantizar la conectividad del dispositivo USB, instale los controladores y configure el sistema correctamente.

Linux VDA admite una lista de dispositivos USB que se redirigen correctamente a y desde el cliente.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
SanDisk SDCZ80 flash drive	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. 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 redirección USB

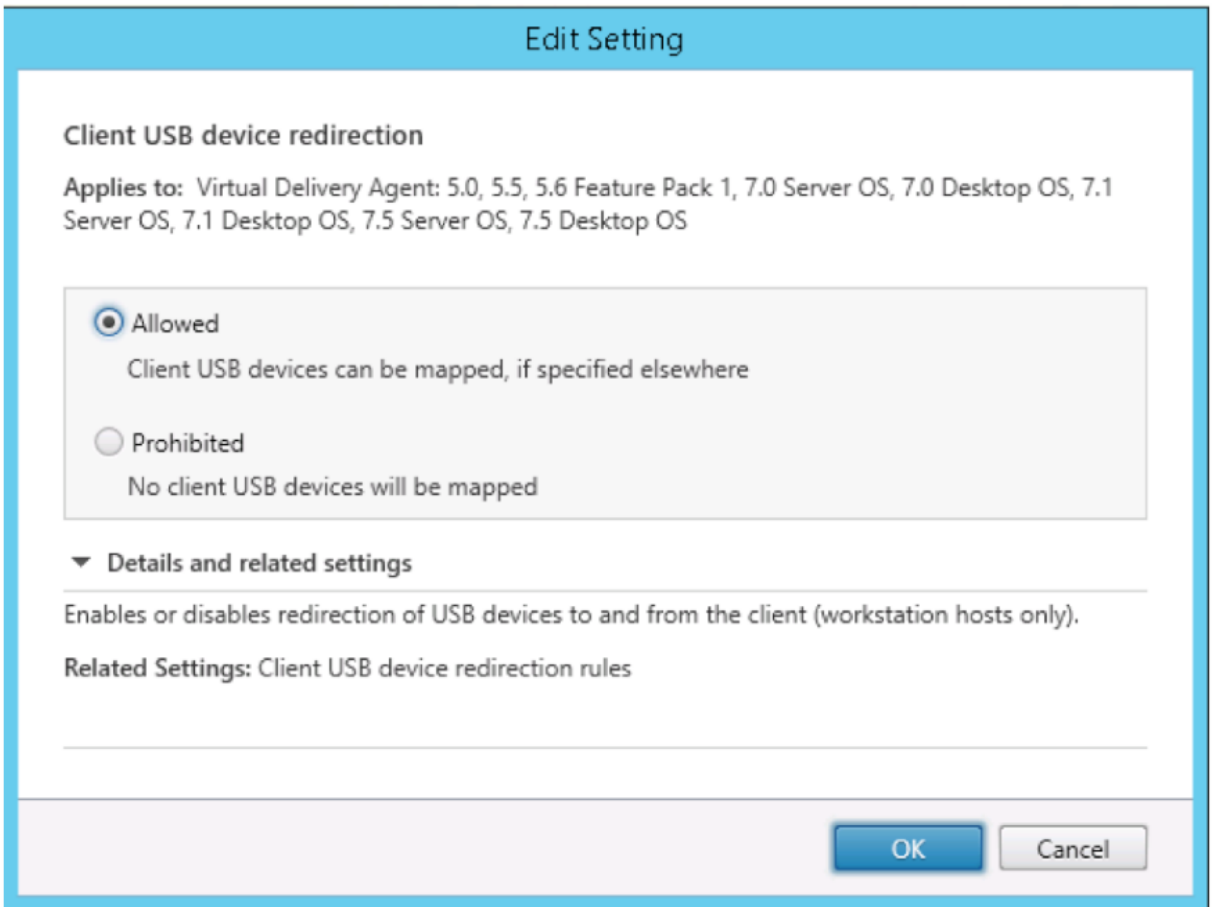
En Citrix Studio, habilite (o inhabilite) la redirección de dispositivos USB desde y hacia el cliente (solo para hosts de estación de trabajo).

En el diálogo **Modificar configuración**:

1. Seleccione la opción **Permitido**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Haga clic en **Aceptar**.



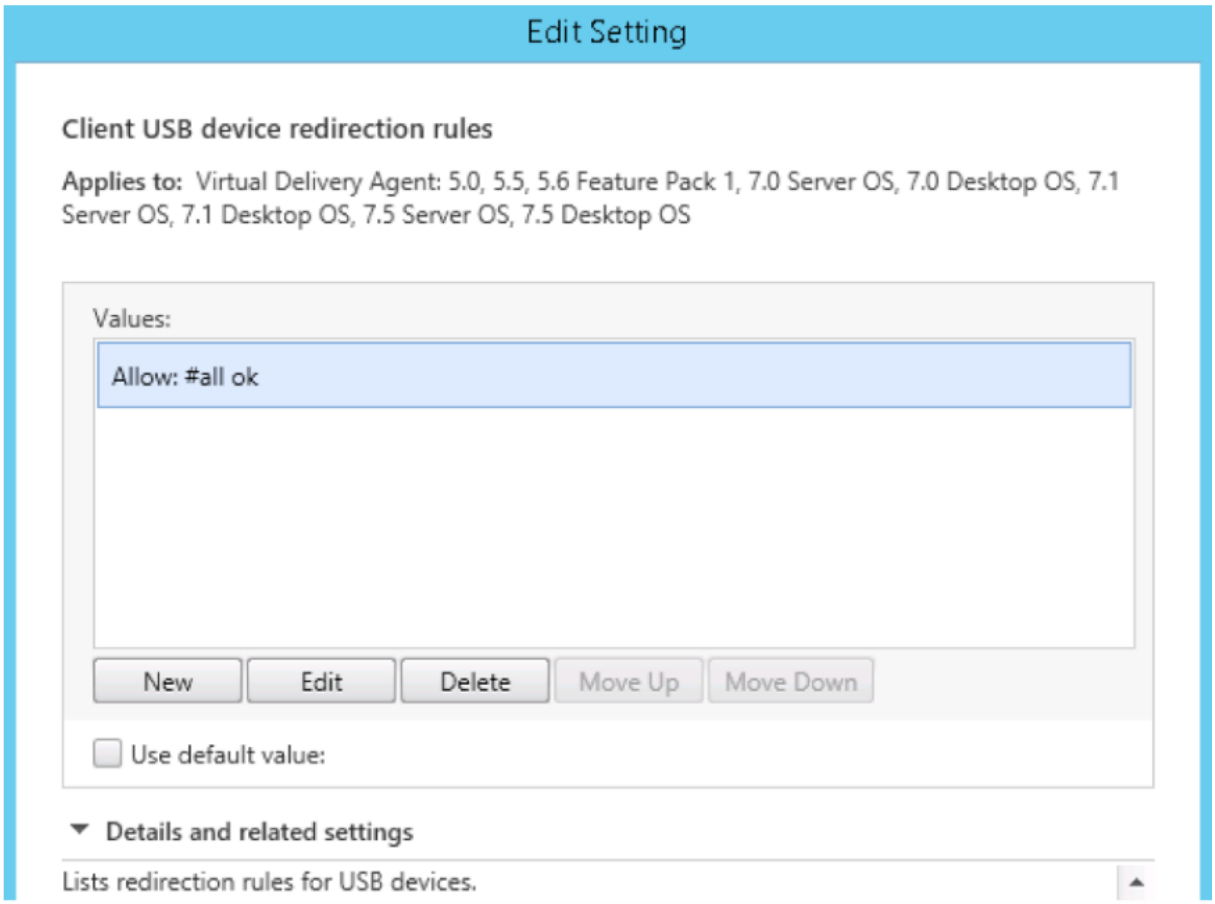
Configurar reglas de redirección USB

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Para obtener más información sobre la configuración de la redirección de USB genérico, consulte Citrix Generic USB Redirection Configuration Guide.

Compilación del módulo de kernel VHCI

La redirección USB depende de los módulos de kernel VHCI (`usb-vhci-hcd.ko` y `usb-vhci-iocif.ko`). Esos módulos forman parte de la distribución de Linux VDA (como parte del paquete RPM). Se compilan en función de los kernels de la distribución oficial de Linux y se indican en la siguiente tabla:

Distribución compatible de Linux	Versión de kernel
RHEL 8.x	4.18.0-240
RHEL 7.9, CentOS 7.9	3.10.0-1160
Ubuntu 20.04	5.4.0-81
Ubuntu 18.04	4.15.0-154
Debian 10	4.19.0-17

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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:

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
<!--NeedCopy-->
```

Si el comando se ejecuta correctamente, el módulo del kernel se ha cargado correctamente y la versión es coherente con la instalada por Citrix.

Si el comando se ejecuta con errores, significa que el kernel no es coherente con el módulo de Citrix y se debe volver a generar.

Recompilación del módulo de kernel VHCI

Si el módulo de kernel no corresponde a la versión de Citrix, lleve a cabo lo siguiente:

1. Descargue el código fuente de LVDA desde el sitio de descargas de Citrix. Seleccione el archivo de la sección "**Linux Virtual Delivery Agent (orígenes)**".
2. Extraiga el archivo **citrix-linux-vda-sources.zip**. Vaya a **linux-vda-sources/vhci-hcd-1.15.zip** y extraiga los archivos de origen VHCI con el comando `unzip vhci-hcd-1.15.zip`.
3. Asegúrese de que tiene instalado el paquete Linux VDA y, a continuación, ejecute cualquiera de los siguientes comandos:

   - `sudo bash ctxusbcfg.sh dkms`

     Este comando le permite utilizar el programa Dynamic Kernel Module Support (DKMS) para administrar los módulos del kernel VHCI. DKMS no está disponible para SUSE.

     > **Nota:**
     >
     > El comando `sudo bash ctxusbcfg.sh dkms` instala los programas `kernel-devel` y `DKMS` en el VDA. Al instalar los programas en RHEL y CentOS, el comando instala y habilita el repositorio Extra Packages for Enterprise Linux (EPEL) en el VDA.
     >
     > Es posible que DKMS no compile los módulos del kernel de VHCI (`usb-vhci-hcd.ko` y `usb-vhci-iocif.ko`) cuando tiene lugar una actualización importante del kernel, por ejemplo, de la versión 4.x.y a la versión 5.x.y. Si el DKMS falla, vuelva a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ejecutar `sudo bash ctxusbcfg.sh dkms`.

- `sudo bash ctxusbcfg.sh build`

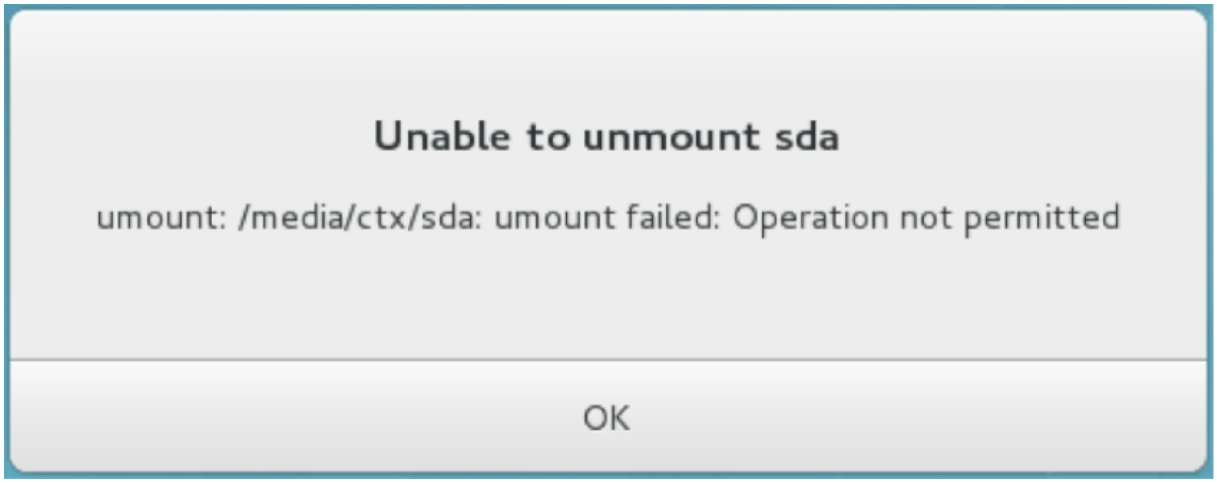
  Este comando compila e instala los módulos del núcleo VHCI sin la opción DKMS.

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

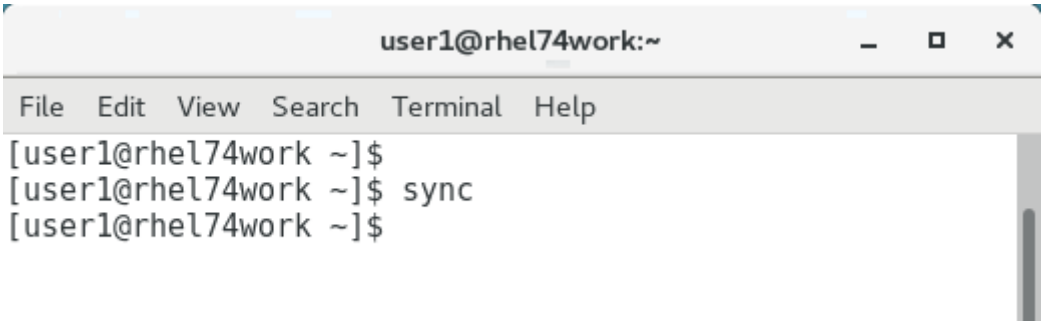
Linux VDA administra todos los discos USB redirigidos desde la aplicación Citrix Workspace bajo el privilegio administrativo para asegurarse de que solo el propietario pueda acceder al dispositivo redirigido. Como resultado, puede desmontar el dispositivo solo con el privilegio administrativo.



Se pierde el archivo cuando se detiene la redirección del disco USB

Si deja de redirigir un disco USB inmediatamente mediante la barra de herramientas de la aplicación Citrix Workspace, los archivos que modificó o creó en el disco se pueden 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.

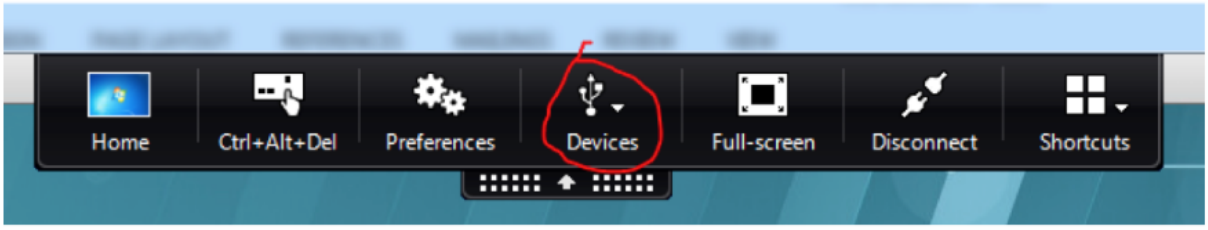
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



No hay ningún dispositivo en la barra de herramientas de la aplicación Citrix Workspace

En algunos casos, es posible que no vea 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 Cómo configurar la redirección automática de dispositivos USB.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

El dispositivo USB se redirige correctamente, pero no lo puedo usar en mi sesión

Normalmente, 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. 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 correctamente. 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. Es posible que no sea el caso para dispositivos que no consten en la lista de los dispositivos admitidos.

Virtual Channel SDK (experimental)

July 6, 2022

Con Virtual Channel Software Development Kit (SDK) para Linux VDA, puede escribir aplicaciones del lado del servidor para que se ejecuten en el VDA. Para obtener más información, consulte la documentación de Citrix Virtual Channel SDK para Linux VDA.

Citrix Virtual Channel SDK para Linux VDA está disponible para su descarga desde la página de descargas de Citrix Virtual Apps and Desktops. Expanda la versión adecuada de Citrix Virtual Apps and Desktops y haga clic en **Components** para seleccionar la descarga de Linux VDA.

© 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).