Linux Virtual Delivery Agent 2301

Contents

Linux Virtual Delivery Agent 2301 5

Novedades 5

Problemas resueltos 6

Problemas conocidos 7

Avisos legales de terceros 10

Elementos retirados 10

Requisitos del sistema 12

Información general de la instalación 17

Crear VDA unidos a un dominio mediante Easy Install 17

Crear Linux VDA no unidos a ningún dominio 40

Crear Linux VDA con Machine Creation Services (MCS) 54

Crear Linux VDA mediante Citrix Provisioning 80

Crear Linux VDA en Citrix DaaS Standard para Azure 81

Instalar Linux VDA manualmente 87

Instalar Linux VDA en Amazon Linux 2, CentOS, RHEL y Rocky Linux manualmente 87

Instalar Linux VDA en SUSE manualmente 126

Instalar Linux VDA en Ubuntu manualmente 155

Instalar Linux VDA en Debian manualmente 188

Configurar 218

Administración 218

Customer Experience Improvement Program (CEIP) de Citrix 219

HDX Insight 223

Integración en Citrix Telemetry Service 224

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

Autoactualización de Linux VDA a través de Azure 228

Métricas de máquinas virtuales y sesiones de Linux 232

Recopilación de registros 241

Remedo de sesiones 244

El demonio del servicio de supervisión 253

Herramientas y utilidades 255

Otros 260

Compatibilidad con la aplicación Citrix Workspace para HTML5 260

Crear un entorno virtual Python3 261

Integrar NIS en Active Directory 263

IPv6 269

LDAPS 270

Xauthority 275

Autenticación 278

Autenticación con Azure Active Directory 278

Autenticación Single Sign-On de doble salto 283

Servicio de autenticación federada 285

Autenticación sin SSO 295

Tarjetas inteligentes 296

Sesiones sin autenticar de usuarios anónimos 307

Archivo 309

Copiar y pegar archivos 309

Transferencia de archivos 310

Gráficos 315

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

Escalado automático de PPP 316

Pantalla de estado de la batería del cliente 317

Configuración y ajuste de gráficos 321

Pantalla compartida de HDX 334

GPU no virtualizadas 343

Marca de agua de la sesión 345

Presentación progresiva de Thinwire 352

Redirección de contenido general 354

Asignación de unidades del cliente 355

Redirección de dispositivos USB 356

Teclado 365

Editor de métodos de entrada (IME) de cliente 365

Sincronización de la interfaz de usuario IME del cliente 366

Sincronización de la distribución de teclado dinámico 370

Teclado en pantalla 374

Compatibilidad para entrada de texto en varios idiomas 377

Contenido multimedia 379

Funciones de audio 379

Redirección de contenido del explorador web 380

Compresión de vídeo de cámara web HDX 386

Linux VDA no unidos a ningún dominio 391

Lista de directivas disponibles 394

Impresión 420

Prácticas recomendadas de impresión 420

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

Impresión de PDF 427

Acceso con Remote PC 428

La función de persistencia 442

Transporte adaptable 443

Fondos y mensajes en pancartas personalizados en las pantallas de inicio de sesión 446

Entornos de escritorio personalizados por los usuarios de las sesiones 447

Iniciar sesión con un directorio de inicio temporal 448

Publicar aplicaciones 450

Rendezvous V1 451

Rendezvous V2 454

Sesiones de usuario seguras mediante DTLS 458

Sesiones de usuario seguras mediante TLS 458

Fiabilidad de la sesión 462

Grabación de sesiones (experimental) 465

Virtual Channel SDK (experimental) 467

Wayland (experimental) 467

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

Linux Virtual Delivery Agent 2301

March 27, 2023

> **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 (VM) Linux, configure el Delivery Controller y use Citrix Studio para poner los escritorios y las aplicaciones a disposición de los usuarios.

Novedades

March 27, 2023

Novedades en la versión 2301

La versión 2301 de Linux VDA ofrece estas mejoras y funciones nuevas:

Compatibilidad con RHEL 8.7, Rocky Linux 8.7 y SUSE 15.4

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

> **Nota:**
>
> SUSE 15.3 se ha retirado a partir de esta versión. Para ejecutar Linux VDA en SUSE 15.4, haga una nueva instalación del VDA.

Compatibilidad con Wayland (experimental)

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

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

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

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

Asignación de unidades del cliente y redirección de carpetas de cliente de forma dinámica

Anteriormente, las unidades conectadas al cliente después de iniciar una sesión no estaban asignadas a esa sesión. Para poder acceder a esas unidades en la sesión, era necesario desconectar la sesión y volver a conectarla. A partir de esta versión, las unidades conectadas al cliente en cualquier momento durante una sesión se pueden asignar automáticamente. Además, esta versión presenta la redirección de carpetas del cliente, que permite redirigir una parte personalizada de una unidad local del cliente a la sesión de forma dinámica. Para obtener más información, consulte Asignación de unidades del cliente.

Novedades en versiones anteriores

Para conocer las nuevas funciones incluidas en las versiones publicadas después de 1912 LTSR y hasta 2212 CR, consulte Historial de novedades.

Problemas resueltos

March 27, 2023

Se han resuelto estos problemas desde Linux Virtual Delivery Agent 2212:

- Al intentar iniciar una sesión de Linux VDA puede aparecer una pantalla gris, que hace que la sesión se desconecte. [CVADHELP-21079]
- Los VDA pueden perder la conectividad con el dominio si no se puede restablecer la contraseña de la cuenta de máquina. [CVADHELP-21803]
- Al intentar iniciar una sesión de Linux VDA, el proceso puede fallar, incluso cuando el VDA tiene el estado registrado. [CVADHELP-21832]
- Es posible que las sesiones de usuario tarden mucho en cerrarse (hasta 60 segundos). [CVADHELP-21899]

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

Problemas conocidos

August 8, 2023

Se han identificado los problemas siguientes en esta versión:

- Cuando HDX 3D Pro está habilitado, las sesiones en los monitores extendidos se oscurecen y solo el monitor principal las muestra correctamente. Para resolver el problema, abra un terminal en el VDA y ejecute estos comandos según sea necesario:

  - Para monitores dobles, ejecute:

    ```
    #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP""
        /etc/X11/ctx-nvidia-2.conf
    ```

  - Para monitores triples, ejecute:

    ```
    #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP,
       DFP"" /etc/X11/ctx-nvidia-3.conf
    ```

  - Para monitores cuádruples, ejecute:

    ```
    #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP,
       DFP, DFP"" /etc/X11/ctx-nvidia-4.conf
    ```

  [LNXVDA-15259]

- Es posible que se produzca un error en el registro de VDA debido a esta excepción de LDAP producida en **/var/log/xdl/jproxy.log**:

  ```
  javax.naming.NamingException: LDAP response read timed out,
     timeout used: 10000 ms.
  ```

  Para solucionar este problema, lleve a cabo los pasos siguientes:

  - Cambie el valor del tiempo de espera de LDAP. Por ejemplo, cambie el valor del tiempo de espera de LDAP a 60 s con este comando:

    ```
    ctxreg create -k "HKLM\Software\Citrix\GroupPolicy\Defaults"
       -t "REG_DWORD" -v "LDAPTimeout" -d "0x000EA60" --force
    ```

  - Acelere las consultas de LDAP mediante la configuración de una base de búsqueda. Puede establecer una base de búsqueda con la variable CTX_XDL_SEARCH_BASE de ctxsetup.sh o con este comando:

    ```
    ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -
       t "REG_SZ" -v "LDAPComputerSearchBase" -d "<specify a
       search base instead of the root of the domain to improve
       search performance>" --force
    ```

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

[CVADHELP-20895]

- Microsoft publicó las actualizaciones acumulativas KB5019966 y KB5019964 para Windows 10 en noviembre de 2022. Las actualizaciones crean errores en la unión y el registro de dominios. Para solucionar este problema, consulte el artículo CTX474888 de Knowledge Center.
- Con el tipo de cifrado **RC4_HMAC_MD5** autorizado para Kerberos, es posible que Linux VDA no se registre en el Controller y aparezca el siguiente mensaje de error:

  Error: Failure unspecified at GSS-API level (Mechanism level: Encryption type RC4 with HMAC is not supported/enabled)

  Para resolver este problema, inhabilite **RC4_HMAC_MD5** de forma global en su dominio de Active Directory (*o de forma específica en una unidad organizativa*) o permita tipos de cifrado débiles en el Linux VDA. A continuación, borre los tíquets de Kerberos almacenados en la caché del Controller y del Citrix Cloud Connector mediante el comando **klist -li 0x3e4 purge** y reinicie el Linux VDA.

  Para inhabilitar **RC4_HMAC_MD5** de forma global en su dominio de Active Directory, siga estos pasos:

  1. Abra la Consola de administración de directivas de grupo.
  2. Busque el dominio de destino y, a continuación, seleccione **Directiva predeterminada de dominio**.
  3. Haga clic con el botón secundario en **Directiva predeterminada de dominio** y seleccione **Modificar**. Se abrirá el Editor de administración de directivas de grupo.
  4. Seleccione **Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad**.
  5. Haga doble clic en **Seguridad de red: Configurar tipos de cifrado permitidos para Kerberos**.
  6. Desactive las casillas de verificación **DES_CBC_CRC**, **DES_CBC_MD5** y **RC4_HMAC_MD5** y seleccione **AES128_HMAC_SHA1**, **AES256_HMAC_SHA1** y **Tipos de cifrado futuros**.

  Para permitir tipos de cifrado débiles en Linux VDA, siga estos pasos:

  > **Nota:**
  >
  > Los tipos de cifrado débiles vuelve su implementación vulnerable a los ataques.

  1. Abra el archivo /etc/krb5.conf en el Linux VDA.
  2. Agregue este parámetro en la sección **[libdefaults]**:

     ```
     allow_weak_crypto= TRUE
     ```

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

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

- 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. [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

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

el Broker no pueda establecer un contexto de seguridad en la devolución al VDA. El síntoma habitual de este problema es que falla el registro del VDA.

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

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

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

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

March 27, 2023

Linux Virtual Delivery Agent versión 2301 (descarga en PDF)

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

Elementos retirados

March 28, 2023

Los anuncios de este artículo ofrecen un adelanto de las plataformas, los productos y las funciones de Citrix que se están retirando progresivamente, de modo que pueda tomar a tiempo las decisiones

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

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 sobre el ciclo de vida útil de los productos, consulte el artículo Product Lifecycle Support Policy.

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
Soporte para Ubuntu 18.04	2212	2305
Compatibilidad con SUSE 15.3	2210	2301
Compatibilidad con Debian 10.9	2206	2210
Compatibilidad con SUSE 15.2	2206	2209
Se admite en RHEL 8.2	2206	2209
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

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

Elemento	Retirada anunciada en	Eliminado en
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

Requisitos del sistema

March 27, 2023

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:

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

> **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 11.3
- Red Hat Enterprise Linux
  - Workstation 9.0
  - Workstation 8.7
  - Workstation 8.6
  - Workstation 8.4
  - Workstation 7.9
  - Server 9.0
  - Server 8.7
  - Server 8.6
  - Server 8.4
  - Server 7.9
- Rocky Linux 9.0
- Rocky Linux 8.7
- Rocky Linux 8.6
- SUSE Linux Enterprise:
  - Server 15 Service Pack 4
- Ubuntu Linux
  - Ubuntu Desktop 22.04
  - Ubuntu Server 22.04
  - Ubuntu Desktop 20.04
  - Ubuntu Server 20.04
  - Ubuntu Desktop 18.04
  - Ubuntu Server 18.04
  - Ubuntu Live Server 18.04

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

> **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 11.3	1.20	MATE, GNOME, GNOME Classic, KDE
RHEL 9.0, Rocky Linux 9.0	1.20	GNOME
RHEL 8.7/8.6/8.4	1.20	MATE, GNOME, GNOME Classic
RHEL 7.9, CentOS 7.9	1.20	MATE, GNOME, GNOME Classic, KDE
Rocky Linux 8.7/8.6	1.20	MATE, GNOME, GNOME Classic, KDE
SUSE 15.4	1.20	MATE, GNOME, GNOME Classic
Ubuntu 22.04	1.21	MATE, GNOME, GNOME Classic, KDE
Ubuntu 20.04	1.20	MATE, GNOME, GNOME Classic, KDE
Ubuntu 18.04	1.19	MATE, GNOME, GNOME Classic, KDE

> **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.

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

Plataformas de host y entornos de virtualización compatibles

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

> **Nota:**
>
> En todos los casos, la arquitectura de procesador admitida es x86-64.
>
> Desde Citrix Virtual Apps and Desktops 7 2003 hasta 2112, el alojamiento de Linux VDA en Microsoft Azure, AWS y GCP solo era posible con Citrix DaaS (antes, Citrix 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.

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 11.3	Sí	Sí	Sí	Sí	No
RHEL 9.0	Sí	Sí	No	No	No
RHEL 8.7/8.6/8.4	Sí	Sí	Sí	Sí	No
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y versiones posteriores)
Rocky Linux 9.0	Sí	Sí	No	No	No

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

	Winbind	SSSD	Centrify	PBIS	Quest
Rocky Linux 8.7/8.6	Sí	Sí	No	No	No
SUSE 15.4	Sí	Sí	Sí	Sí	No
Ubuntu 22.04/20.04/18.04	Sí	Sí	Sí	Sí	Sí (Quest v4.1 y versiones posteriores)

HDX 3D Pro

HDX 3D Pro de Citrix Virtual Apps and Desktops le permite 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
- 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 14. Para obtener más información, consulte NVIDIA Virtual GPU Software Supported GPUs.

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

Información general de la instalación

March 27, 2023

Esta sección le guía a través de los siguientes procedimientos:

- Crear VDA unidos a un dominio mediante Easy Install
- Crear Linux VDA no unidos a ningún dominio mediante MCS
- Crear Linux VDA mediante MCS
- Crear Linux VDA mediante Citrix Provisioning
- Crear Linux VDA en Citrix DaaS Standard para Azure
- Instalar Linux VDA manualmente
  - Instalar Linux VDA en Amazon Linux 2, CentOS, RHEL y Rocky Linux manualmente
  - Instalar Linux VDA en SUSE manualmente
  - Instalar Linux VDA en Ubuntu manualmente
  - Instalar Linux VDA en Debian manualmente

Crear VDA unidos a un dominio mediante Easy Install

August 20, 2024

> **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 Crear Linux VDA no unidos a ningún dominio.
> - 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.

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

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 iniciar una sesión, compruebe que se instalan los entornos de escritorio y el sistema X Window están instalados.

Consideraciones

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

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

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

  Registro:

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

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

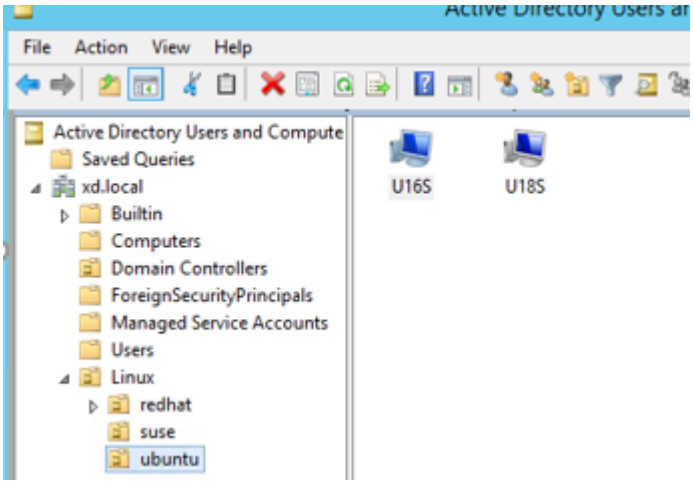
  a. Abra **Herramientas administrativas** en el controlador del dominio.
  b. Seleccione **Sitios y servicios de Active Directory**.
  c. Agregue una dirección de subred adecuada para **Subredes**.

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

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

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. Esta tabla refleja los nombres de unidades organizativos de ejemplo de la captura de pantalla anterior. Puede usar los nombres que quiera para las unidades organizativas de su organización.

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 9.0, Rocky Linux 9.0	`ou="OU=redhat,OU=Linux"`	`ou="OU=redhat,OU=Linux"`	N/D	N/D
RHEL 8.x, Rocky Linux 8.x	`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"`

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

SO	Winbind	SSSD	Centrify	PBIS
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 es compatible con 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:

    Amazon Linux 2/RHEL: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz

    CentOS: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz

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

    Ubuntu/Debian: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-deb9-x86_64.tgz
  - Obtenga el paquete 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.

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

Por ejemplo:

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

- Si elige PBIS como 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. Por ejemplo, estas son las direcciones URL especificadas para cada distribución:

    Amazon Linux 2, CentOS 7, RHEL 8, RHEL 7, SUSE 15.4: `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/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh`
  - Obtenga una versión específica del paquete PBIS desde Internet. Para hacerlo, cambie las líneas “pbisDownloadRelease”y “pbisDownloadExpectedSHA256”del archivo /opt/Citrix/VDA/sbin/ctxinstall.sh.

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

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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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:

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

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:

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

```
su -

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux 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

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**.

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

Paso 3: Instale .NET Runtime 6.0

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

1. Vaya a la página de descargas de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Haga clic en **Componentes** para descargar el paquete de Linux VDA que corresponda a su distribución de Linux y la clave pública GPG que puede usar para comprobar la integridad del paquete de Linux VDA.

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

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

     ```
     rpmkeys --import <path to the public key>
     rpm --checksig --verbose <path to the Linux VDA package>
     ```

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

     ```
     sudo apt-get install dpkg-sig
     gpg --import <path to the public key>
     dpkg-sig --verify <path to the Linux VDA package>
     ```

Paso 5: Instale el paquete de Linux VDA

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

Para las distribuciones de Amazon Linux 2, CentOS, RHEL y Rocky Linux:

> **Nota:**
>
> - En el caso de RHEL y CentOS, debe instalar el repositorio EPEL para poder instalar Linux VDA correctamente. Para obtener información sobre cómo instalar EPEL, consulte las in-

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

> strucciones en https://docs.fedoraproject.org/en-US/epel/.
>
> - Antes de instalar Linux VDA en RHEL 9.0 y Rocky Linux 9.0, actualice el paquete **libsepol** a la versión 3.4 o posterior.

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

> **Nota:**
>
> Tras instalar Linux VDA en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, es posible que se pierda la conexión Ethernet y que no se pueda acceder a Linux VDA después de reiniciar la máquina virtual. Para solucionar el problema, ejecute estos comandos antes de reiniciar la máquina virtual:
>
> ```
> nmcli dev connect eth0
> service NetworkManager restart
> ```

Para distribuciones Ubuntu/Debian:

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

> **Nota:**
>
> - Para instalar las dependencias necesarias para una distribución Debian 11.3, agregue la línea `deb http://deb.debian.org/debian/ bullseye main` al archivo /etc/apt/sources.list.
> - Para Ubuntu 20.04 en GCP, inhabilite RDNS. Para ello, agregue la línea **rdns = false** en **[libdefaults]** en /etc/krb5.conf.

Para las distribuciones SUSE:

1. Para SUSE 15.4 en AWS, Azure y GCP, asegúrese de que:
   - Está utilizando **libstdc++6** versión 12 o posterior.
   - El parámetro **Default_WM** de **/etc/sysconfig/windowmanager** está configurado en **"gnome"**.
2. Ejecute el siguiente comando para instalar Linux VDA:

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

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.

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

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: Especifique una base de datos que se utilizará

Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA.

Para ello, modifique `etc/xdl/db.conf` antes de ejecutar `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` o `/opt/Citrix/VDA/bin/easyinstall`.

> **Nota:**
>
> - Le recomendamos utilizar SQLite solo para el modo VDI.
> - Para Easy Install y MCS, puede cambiar entre SQLite y PostgreSQL sin tener que instalarlos manualmente. A menos que se especifique lo contrario mediante `/etc/xdl/db.conf`, Linux VDA usa PostgreSQL de forma predeterminada.
> - También puede utilizar `/etc/xdl/db.conf` para configurar el número de puerto de PostgreSQL.

Paso 8: 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.

> **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`.

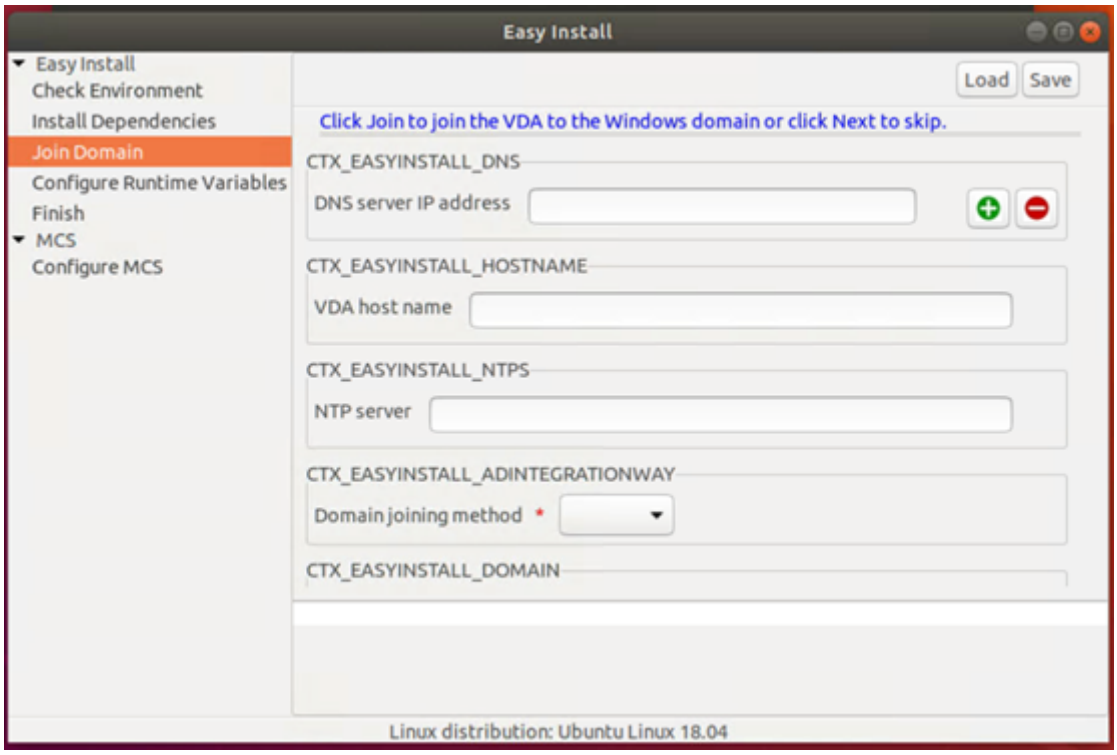
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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

> **Sugerencia:**
>
> Haga clic en **Save** para guardar los parámetros de las variables en un archivo local en la ruta que especifique. Haga clic en **Load** para cargar los parámetros de las variables desde

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

> el archivo que especifique. Para obtener información sobre la configuración de variables de MCS, consulte el Paso 3: Prepare una imagen maestra.

Modo silencioso:

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

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

El script ctxsetup.sh utiliza las siguientes variables:

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

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

- **CTX_XDL_VDI_MODE=Y | N**: Indica si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos alojados. Para entornos HDX 3D Pro, establézcalo en Y.
- **CTX_XDL_SITE_NAME=dns-name**: Linux VDA detecta los servidores LDAP mediante DNS. Para limitar los resultados de búsqueda de DNS a un sitio local, especifique un nombre de sitio DNS. Si no es necesario, establézcalo en **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'**: Linux VDA consulta a DNS para detectar servidores LDAP. Sin embargo, si el DNS no puede proporcionar registros del servicio LDAP, se puede suministrar una lista de nombres FQDN de LDAP, separados por espacios, con los puertos de LDAP. Por ejemplo, ad1.miempresa.com:389 ad2.miempresa.com:3268 ad3.miempresa.com:3268. Si especifica el número de puerto de LDAP como 389, Linux VDA consulta a cada servidor LDAP del dominio especificado en modo de sondeo. Si hay una cantidad "x"de directivas y una cantidad "y"de servidores LDAP, Linux VDA realiza el total de consultas X multiplicado por Y. Si el tiempo de sondeo supera el umbral, los inicios de sesión pueden fallar. Para habilitar las consultas LDAP más rápidas, habilite **Catálogo global** en un controlador de dominio y especifique 3268 como número de puerto LDAP correspondiente. 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). 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. Para comunicarse correctamente con los servidores FAS, añada un número de puerto coherente con el especificado en los servidores FAS, por ejemplo, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **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` 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**

     ```
     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
     exec gnome-session
     fi
     ```

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

A partir de la versión 2209, los usuarios de las sesiones pueden personalizar sus entornos de escritorio. Para habilitar esta función, debe instalar con antelación en el VDA entornos de escritorio que se puedan cambiar. Para obtener más información, consulte Entornos de escritorio personalizados por usuarios de las sesiones.

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

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

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

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 | '<
```

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

```
    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
```

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 \

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
```

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

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

Iniciar Linux VDA:

Para iniciar los servicios de Linux VDA:

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

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

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
```

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

Paso 11: Cree catálogos de máquinas

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 grupos de entrega

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.

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

> **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 2212.

Paso 13: 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.

Para RHEL 7 y CentOS 7:

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

Para RHEL 8 y Rocky Linux 8:

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

Para RHEL 9.0 y Rocky Linux 9.0:

> **Nota:**
>
> Antes de actualizar Linux VDA en RHEL 9.0 y Rocky Linux 9.0, actualice el paquete **libsepol** a la versión 3.4 o posterior.

```
sudo rpm -U XenDesktopVDA-<version>.el9x.x86_64.rpm
```

Para SUSE:

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

Para Ubuntu 18.04:

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

Para Ubuntu 20.04:

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

Para Ubuntu 22.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

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

Solución de problemas

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

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.
```

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

/var/log/messages:

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

Para solucionar este problema:

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

Las sesiones de escritorio en Ubuntu muestran una pantalla gris

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

Para solucionar este problema:

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

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

/var/log/xdl/hdx.log:

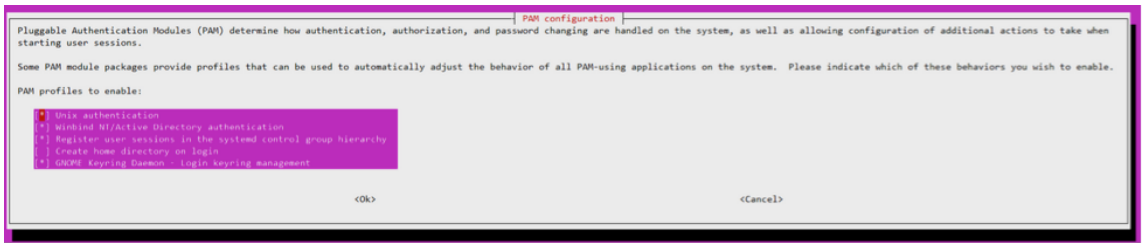
```
2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
    failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)

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.
```

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

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

Para solucionar este problema:

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



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

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

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

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

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

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

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

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

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

O 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.

```

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

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

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

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

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

Algunos grupos o módulos no 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:

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

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

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

If you want to allow polyinstantiation to enabled

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

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

```

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

    Do

       setsebool -P polyinstantiation_enabled 1

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

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

Then you should report this as a bug.

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

      Do

       allow this access for now by executing:

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

# semodule -i mypol.pp
```

Para solucionar este problema:

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

   SELINUX=disabled

2. Reinicie el VDA.

Crear Linux VDA no unidos a ningún dominio

March 27, 2023

En este artículo se explica el uso de Machine Creation Services (MCS) para crear Linux VDA no unidos a ningún dominio en Citrix DaaS.

> **Importante:**
>
> - Los VDA que no están unidos a ningún dominio son compatibles con Citrix DaaS.
> - Su plano de control debe implementarse a través de Citrix DaaS.
> - Puede implementar VDA que no estén unidos a un dominio en una nube pública o en un centro de datos local. El plano de control de Citrix DaaS administra los VDA que no están unidos a un dominio.

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

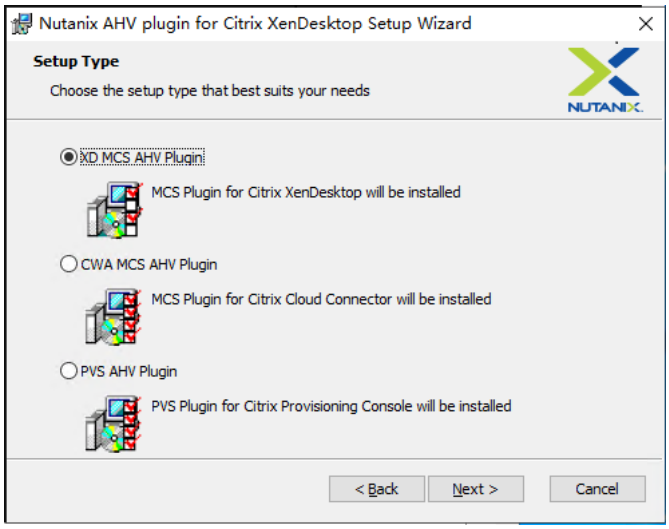
  - Puede configurar Rendezvous V2 para omitir los Citrix Cloud Connectors. De lo contrario, debe instalar Cloud Connectors para conectar VDA a su plano de control.
- Para crear VDA que no estén unidos a ningún dominio, debe usar MCS.
  - MCS no es compatible con servidores bare metal.
- Las siguientes funciones están disponibles para los Linux VDA que no están unidos a ningún dominio
  - Crear usuarios locales con atributos especificados en VDA que no están unidos a ningún dominio
  - Autenticación sin SSO
  - Autenticación con Azure Active Directory
  - Rendezvous V2

(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 host

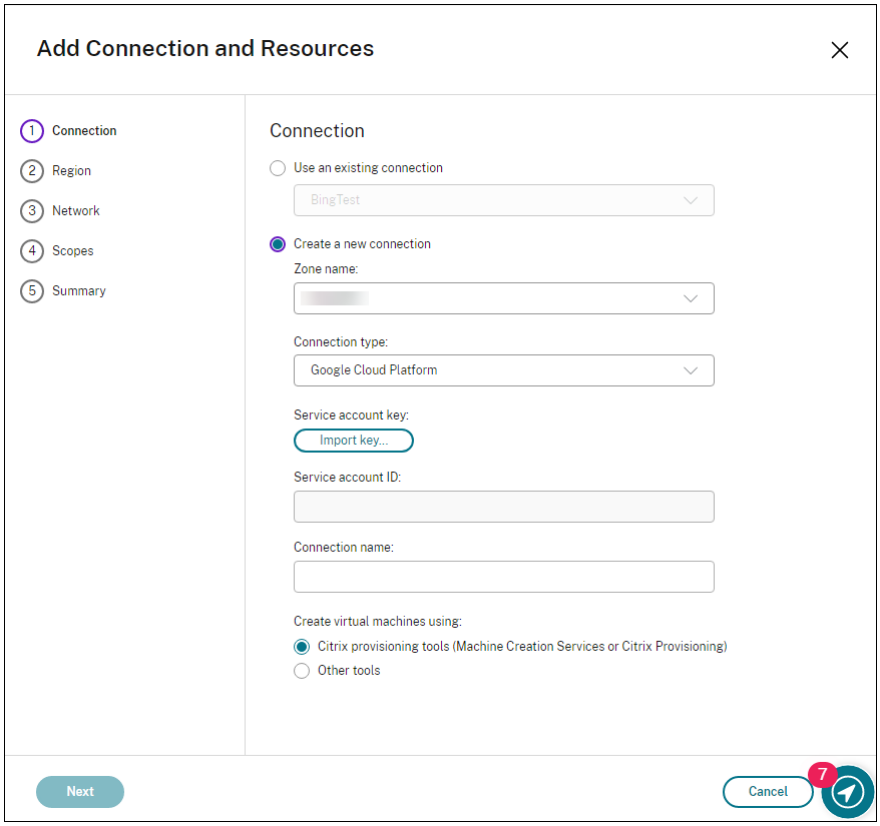
Los hosts son hipervisores o servicios de la nube que se utilizan en las ubicaciones de recursos. Este paso le permite especificar la información que utiliza DaaS para comunicarse con las máquinas virtuales de un host. La información detallada incluye la ubicación del recurso, el tipo de host, las credenciales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

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

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

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

Paso 2a: Conexión



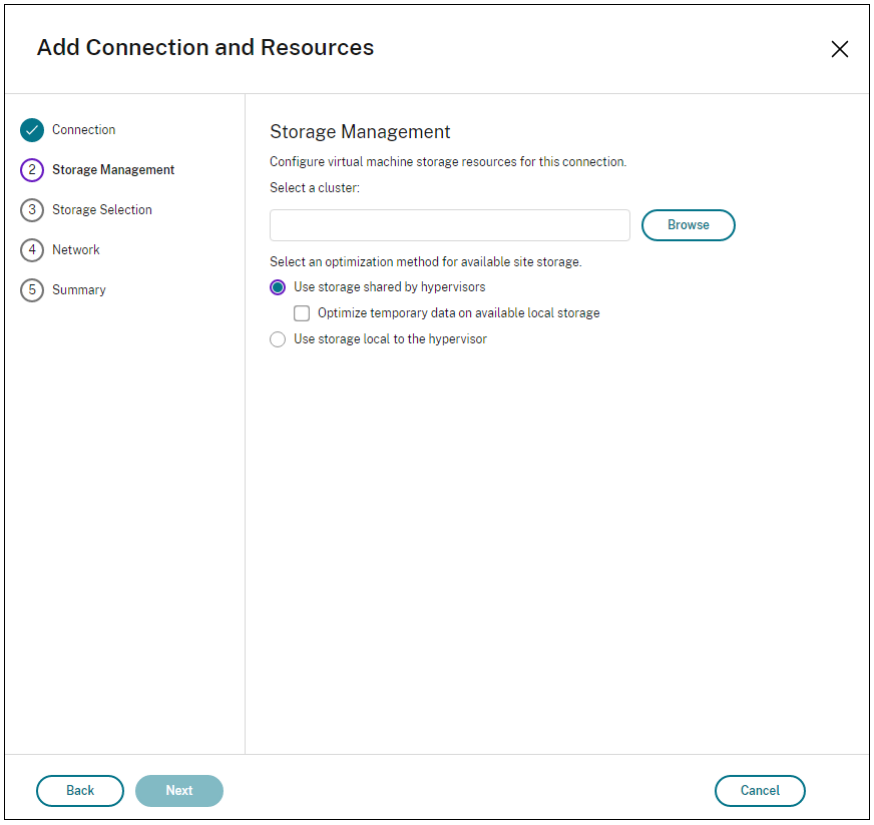
En la página **Conexión**:

- Para crear una conexión, seleccione **Crear una conexión**. Para crear una conexión basada en la misma configuración de host que una conexión existente, seleccione **Usar una conexión existente** y, a continuación, seleccione la conexión correspondiente.
- Seleccione una zona en el campo **Nombre de zona**. Las opciones son todas las ubicaciones de recursos que configuró.
- Seleccione un hipervisor o servicio de la nube en el campo **Tipo de conexión**. Las opciones son hipervisores y servicios de la nube que tienen sus plug-ins instalados correctamente en la zona.
  Como alternativa, puede usar el comando `Get-HypHypervisorPlugin -ZoneUid` de PowerShell para obtener la lista de plug-ins de hipervisor disponibles con la zona seleccionada.
- Escriba un nombre para la conexión. Este nombre aparece en la pantalla **Administrar**.
- Elija la herramienta para crear máquinas virtuales: Machine Creation Services o Citrix Provisioning.

La información de la página **Conexión** varía según el host (tipo de conexión) que se utiliza. Por ejemplo, cuando se usa Azure Resource Manager, puede utilizar una entidad de servicio existente o crear otra.

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

Paso 2b: Administración del almacenamiento



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

Si está configurando una conexión con un host de Hyper-V o VMware, busque y seleccione el nombre del clúster. Otros tipos de conexión no requieren un nombre de clúster.

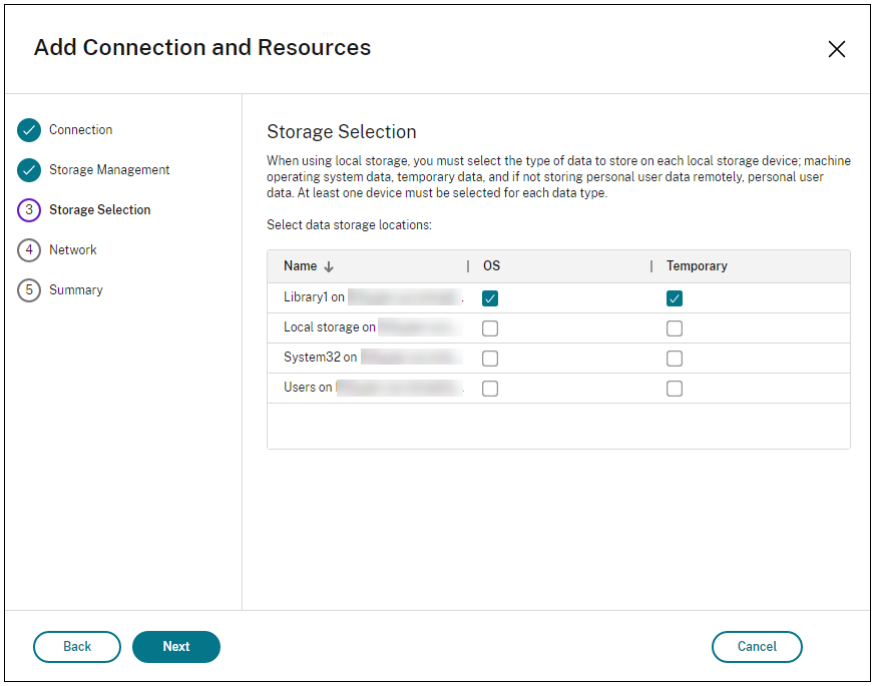
Seleccione un método de administración del almacenamiento: puede ser almacenamiento compartido por los hipervisores o almacenamiento local en cada hipervisor.

- Si elige el almacenamiento compartido por los hipervisores, indique si quiere conservar los datos temporales en almacenamiento local disponible (puede especificar tamaños de almacenamiento temporal no predeterminados en los catálogos de máquinas que usen esta conexión). **Excepción:** Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite crear discos de caché de datos temporales en el almacenamiento local. Al intentar configurar esa administración de almacenamiento en la consola **Administrar**, el proceso falla.

Si usa almacenamiento compartido en una agrupación de Citrix Hypervisor, indique si quiere usar IntelliCache para reducir la carga en el dispositivo de almacenamiento compartido. Consulte Entornos de virtualización de Citrix Hypervisor.

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

Paso 2c: Selección del almacenamiento



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

Seleccione al menos un dispositivo de almacenamiento en el host para cada tipo de datos. El método de administración de almacenamiento seleccionado en la página anterior afecta a qué tipos de datos estarán disponibles para seleccionar en esta página. Es necesario seleccionar al menos un dispositivo de almacenamiento para cada tipo de datos admitido antes de pasar a la página siguiente del asistente.

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

Se mostrará la cantidad de dispositivos de almacenamiento seleccionados en ese momento (en el gráfico "1 storage device selected"). Al pasar el puntero sobre ese texto, aparecen los nombres de los dispositivos seleccionados (a menos que no haya ninguno configurado).

1. Seleccione **Seleccionar** para cambiar los dispositivos de almacenamiento que quiere usar.
2. En el cuadro de diálogo **Seleccionar almacenamiento**, seleccione o deje sin seleccionar las casillas de cada dispositivo de almacenamiento y, a continuación, seleccione **Aceptar**.

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

Paso 2d: Región

(aparece solamente para algunos tipos de host). La selección de región indica dónde se implementarán las máquinas virtuales. Preferiblemente, elija una región cercana a donde los usuarios acceden a sus aplicaciones.

Paso 2e: Red

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

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

Paso 2f: Resumen

Revise lo que ha seleccionado y si quiere hacer cambios, vuelva a las páginas anteriores del asistente. Una vez revisado, seleccione **Finalizar**.

Recuerde: Si guarda los datos temporales localmente, puede configurar valores no predeterminados para el almacenamiento de datos temporales cuando cree el catálogo que contendrá las máquinas que usen esta conexión.

> **Nota:**
>
> El ámbito no se muestra a los administradores de acceso total. Para obtener más información, consulte Administradores, roles y ámbitos.

Para obtener más información, consulte Crear y administrar conexiones.

Paso 3: Prepare una imagen maestra

> **Sugerencia:**
>
> Puede usar una sola imagen con la que crear VDA tanto unidos a un dominio como no unidos a ningún dominio.

(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:

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

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

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

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

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

   Para RHEL/CentOS/Rocky Linux:

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

   Para Ubuntu/Debian:

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

   Para SUSE:

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

3. 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
```

   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']
```

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
     ```

   - 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
     ```

     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/Rocky Linux:

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

> **Nota:**
>
> En el caso de RHEL y CentOS, debe instalar el repositorio EPEL para poder instalar Linux VDA y ejecutar `deploymcs.sh` correctamente. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en https://docs.fedoraproject.org/en-US/epel/.
>
> - Tras instalar Linux VDA en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, es posible que

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

> se pierda la conexión Ethernet y que no se pueda acceder a Linux VDA después de reiniciar la máquina virtual. Para solucionar el problema, ejecute estos comandos antes de reiniciar la máquina virtual:
>
> ```
> nmcli dev connect eth0
> service NetworkManager restart
> ```

Para Ubuntu/Debian:

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

apt-get install -f
```

Para SUSE:

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

Paso 3d: Habilite repositorios para instalar el paquete tdb-tools (solo para RHEL 7)

Para el servidor de RHEL 7:

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

Para la estación de trabajo de RHEL 7:

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

Paso 3e: (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
   ```

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

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

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

   ```
   sudo cd ntfs-3g_ntfsprogs-<package version>
   ```

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

5. Instale ntfs-3g:

```
./configure
make
make install
```

Paso 3f: Especifique una base de datos que se utilizará

Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh` Omita este paso si se trata de una instalación nueva.
2. Modifique `/etc/xdl/db.conf` antes de ejecutar `deploymcs.sh`.

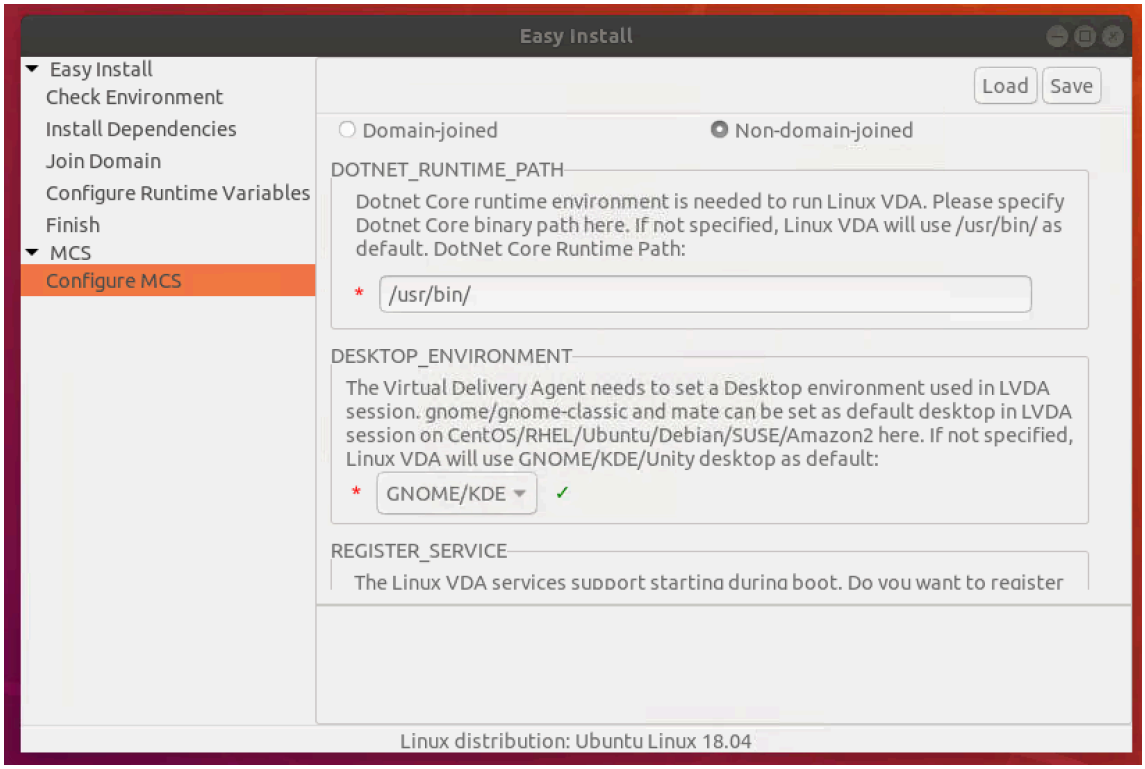
> **Nota:**
>
> - Le recomendamos utilizar SQLite solo para el modo VDI.
> - Para Easy Install y MCS, puede cambiar entre SQLite y PostgreSQL sin tener que instalarlos manualmente. A menos que se especifique lo contrario mediante `/etc/xdl/db.conf`, Linux VDA usa PostgreSQL de forma predeterminada.
> - También puede utilizar `/etc/xdl/db.conf` para configurar el número de puerto de PostgreSQL.

Paso 3g: Configure las variables de MCS

Hay dos formas de configurar variables de MCS:

- Modificar el archivo `/etc/xdl/mcs/mcs.conf`.
- Utilizar la interfaz gráfica de usuario de Easy Install. Para usar la GUI de Easy Install, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su Linux VDA.

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



> **Sugerencia:**
>
> Haga clic en **Save** para guardar los parámetros de las variables en un archivo local en la ruta que especifique. Haga clic en **Load** para cargar los parámetros de las variables desde el archivo que especifique.

Estas son variables de MCS que puede configurar para casos no unidos a ningún dominio: Puede utilizar los valores predeterminados de las variables o personalizar las variables según sea necesario (opcional):

`DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
`DESKTOP_ENVIRONMENT`= **gnome | mate **
`REGISTER_SERVICE`=**Y | N**
`ADD_FIREWALL_RULES`=**Y | N**
`VDI_MODE`=**Y | N**
`START_SERVICE`=**Y | N**

Paso 3h: Escriba o actualice los valores del Registro para MCS (opcional)

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.

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

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

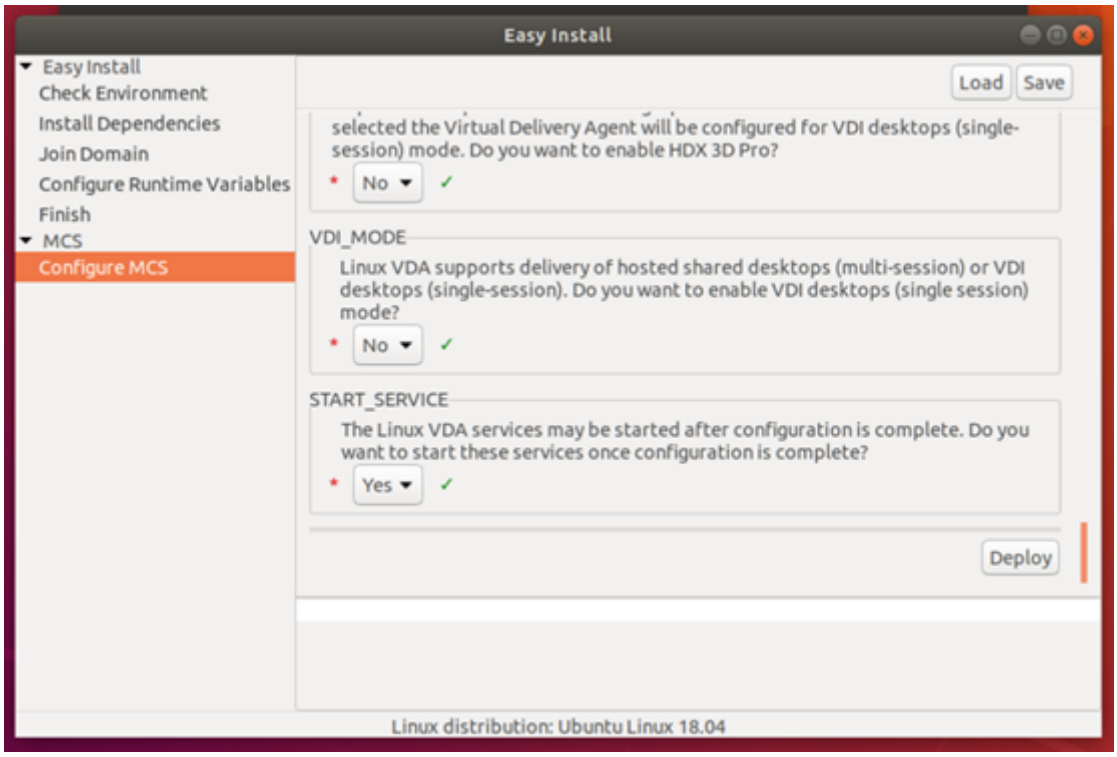
Por ejemplo, puede agregar las siguientes líneas de comando al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar un archivo del Registro, respectivamente:

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

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

Paso 3i: Cree una imagen maestra

1. Si configura variables de MCS mediante la modificación de `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura variables de MCS mediante la GUI, haga clic en **Deploy**.

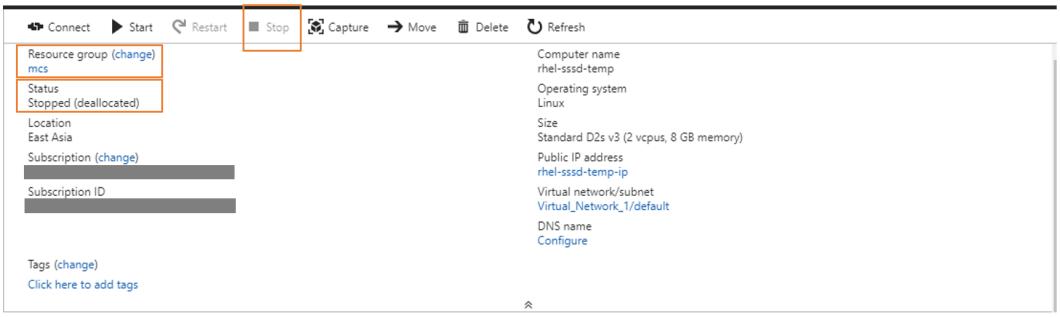


   Tras hacer clic en **Deploy** en la GUI, las variables que defina en la GUI supeditarán las variables que haya establecido en el archivo `/etc/xdl/mcs/mcs.conf`.

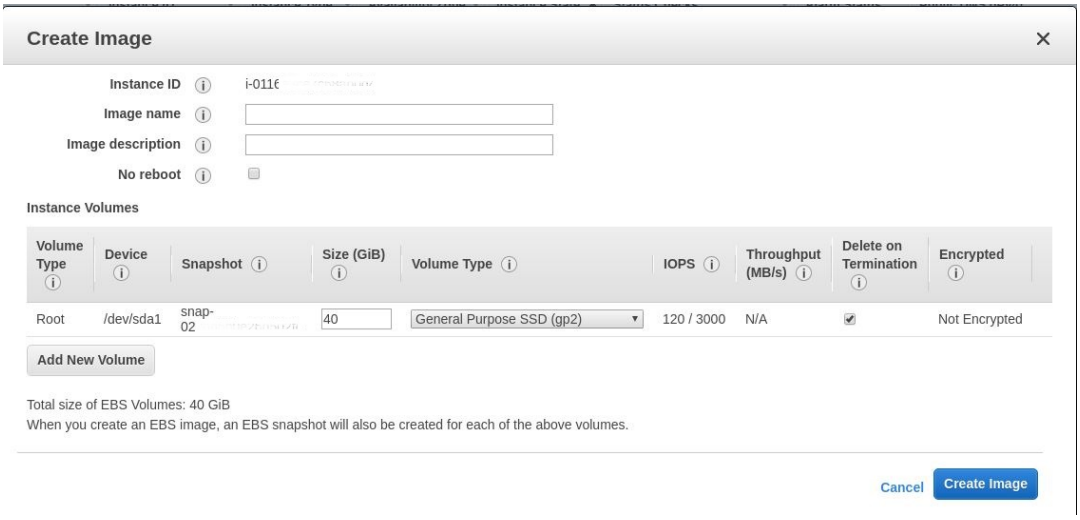
2. Cree y asigne un nombre a una instantánea de su imagen maestra en función de la nube pública que utilice.

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

- **(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.

> **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 cam-

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

> biar 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

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
3. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.
4. El asistente le guiará para crear un catálogo de máquinas.

   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. Seleccione MCS como método de implementación de máquinas y seleccione **No unido a un dominio** como identidad para las máquinas que se crearán en el catálogo.

   Realice otras tareas de configuración según sea necesario. Para obtener más información, consulte Crear catálogos de máquinas.

> **Nota:**
>
> 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.

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.

Crear Linux VDA con Machine Creation Services (MCS)

January 9, 2024

Con MCS, puede crear VDA tanto unidos a un dominio como no unidos a ningún dominio.

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

> **Importante:**
>
> Estos son cambios importantes a partir de la versión 2212:
>
> - La variable **AD_INTEGRATION** del archivo /etc/xdl/mcs/mcs.conf o de la GUI de Easy Install ya no tiene un valor predeterminado. Debe establecer un valor donde sea necesario. Para obtener más información, consulte la sección Paso 3h: Configure variables de MCS de este artículo.
> - El valor válido de la entrada **UPDATE_MACHINE_PW** de /etc/xdl/mcs/mcs.conf ya no es **enabled** ni **disabled**, sino que es **Y** o **N**. Para obtener más información, consulte la sección Automatizar la actualización de las contraseñas de cuentas de máquina de este artículo.

Distribuciones compatibles

	Winbind	SSSD	Centrify	PBIS
Debian 11.3	Sí	Sí	No	Sí
RHEL 9.0	Sí	No	No	No
RHEL 8.7/8.6/8.4	Sí	No	Sí	Sí
Rocky Linux 9.0	Sí	No	No	No
Rocky Linux 8.7/8.6	Sí	No	No	No
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí	Sí
SUSE 15.4	Sí	Sí	No	Sí
Ubuntu 22.04, 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

Consideraciones

- 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.
- Citrix usa las siguientes versiones de Centrify para la validación inicial de funciones en las distribuciones de Linux relevantes:

Distribución de Linux	Versión de Centrify
RHEL 7/8	5.8.0
SUSE	5.7.1
Debian, Ubuntu	5.6.1

  El uso de otras versiones de Centrify puede provocar errores. No utilice Centrify para unir una máquina de plantilla a un dominio.

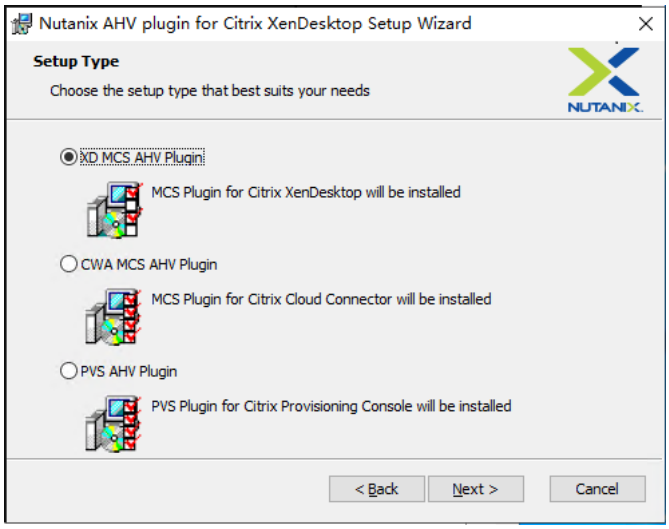
- Si utiliza PBIS o Centrify para unir máquinas creadas con MCS a dominios de Windows, complete las siguientes tareas:
  - En la máquina de plantilla, configure la ruta de descarga del paquete PBIS o Centrify en el archivo `/etc/xdl/mcs/mcs.conf` o instale el paquete PBIS o Centrify directamente.
  - Antes de ejecutar `/opt/Citrix/VDA/sbin/deploymcs.sh`, cree una unidad organizativa (OU) que tenga permisos de escritura y 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.

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

(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.



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.

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

> **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 host

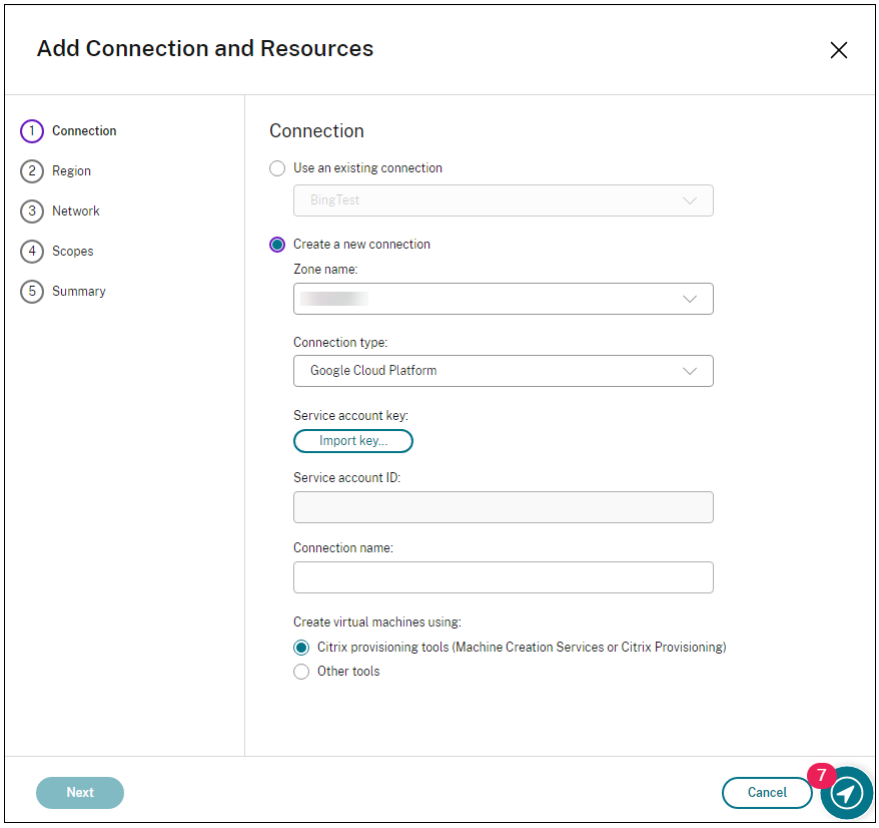
En esta sección se explica cómo crear una conexión de host con Azure, AWS, GCP, Nutanix AHV y VMware vSphere:

- Crear una conexión de host con Azure en Citrix Studio
- Crear una conexión de host con AWS en Citrix Studio
- Crear una conexión de host con GCP en Citrix Studio
- Crear una conexión de host con Nutanix en Citrix Studio
- Crear una conexión de host con VMware en Citrix Studio

Crear una conexión de host con Azure en Citrix Studio

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
3. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
4. Seleccione **Agregar conexión y recursos** en la barra de acciones.

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

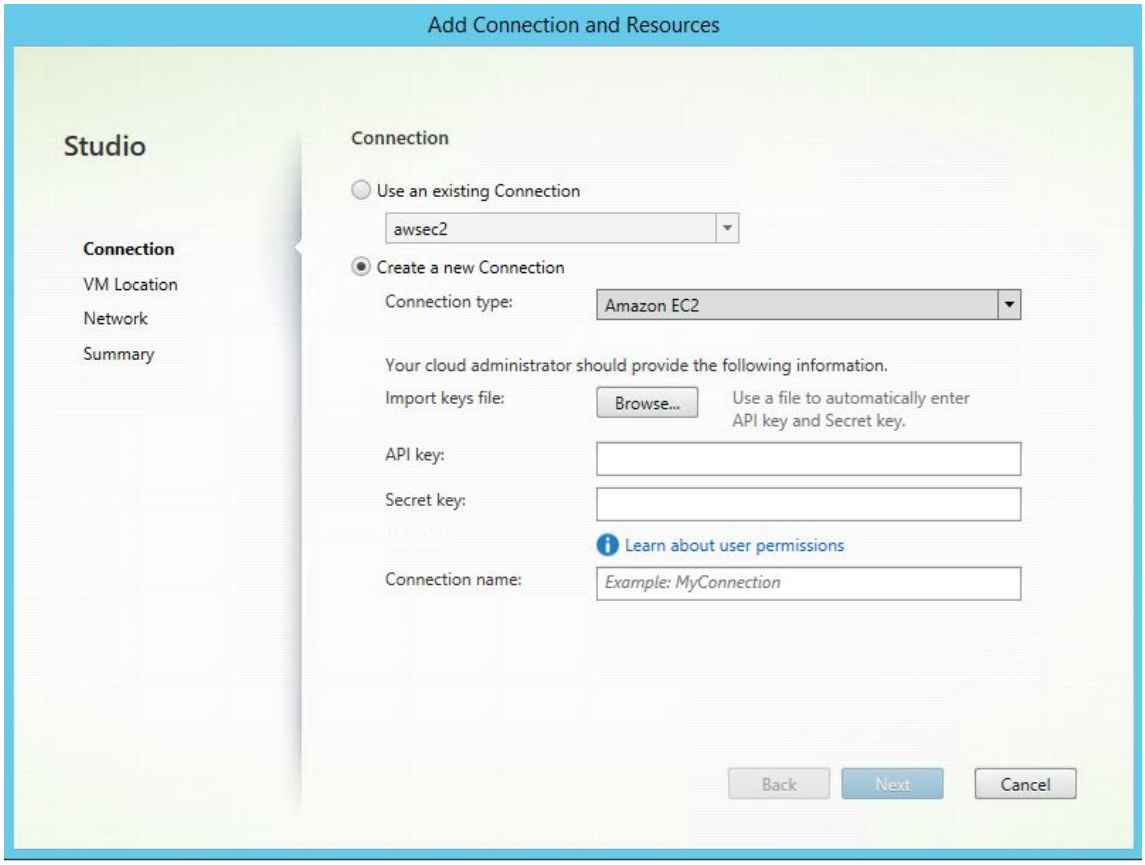


5. Seleccione el tipo de conexión Microsoft Azure.
6. El asistente le guiará a través de las páginas. El contenido específico de cada página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte el Paso 2: Cree una conexión de host en el artículo Crear Linux VDA no unidos a ningún dominio.

Crear una conexión de host con AWS en Citrix Studio

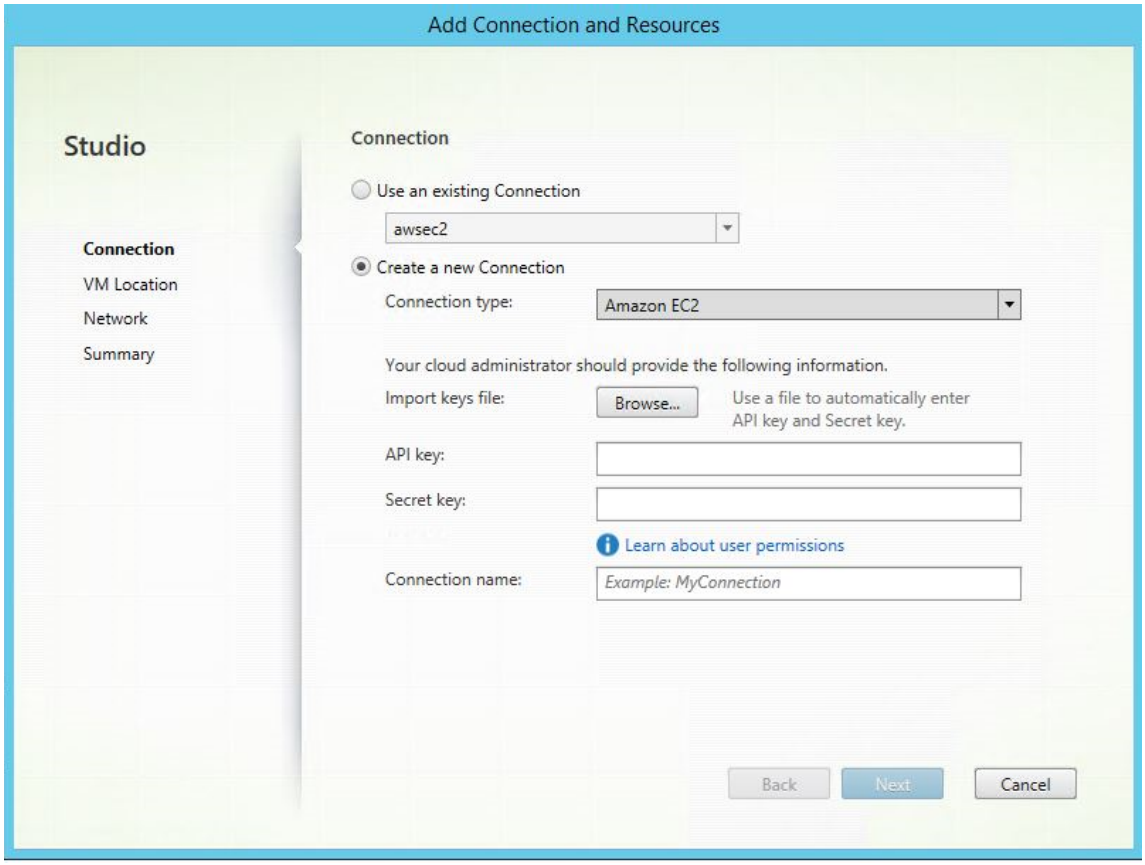
1. En Citrix Studio, elija **Configuración** > **Alojamiento** > **Agregar conexión y recursos**.
2. Elija **Amazon EC2** como tipo de conexión.

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



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.

4. El asistente le guiará a través de las páginas. El contenido específico de cada página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**.

Crear una conexión de host 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 host con GCP.

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

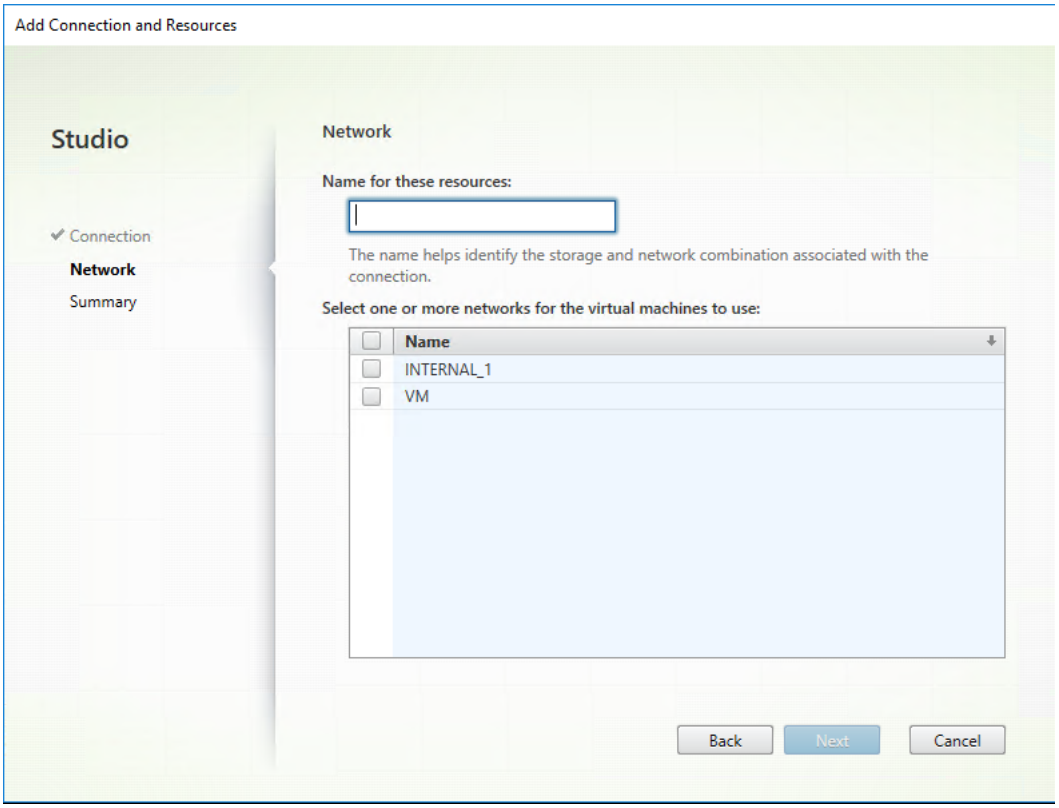
1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
3. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
4. Seleccione **Agregar conexión y recursos** en la barra de acciones.
5. Seleccione **Google Cloud Platform** como tipo de conexión.
6. Importe la clave de cuenta de servicio de su cuenta de GCP e introduzca el nombre de conexión.
7. El asistente le guiará a través de las páginas. El contenido específico de cada página depende del tipo de conexión seleccionado. Después de completar cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**. Para obtener más información, consulte el Paso 2: Cree una conexión de host en el artículo Crear Linux VDA no unidos a ningún dominio.

Crear una conexión de host 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.

   Por ejemplo, en Citrix Studio local:

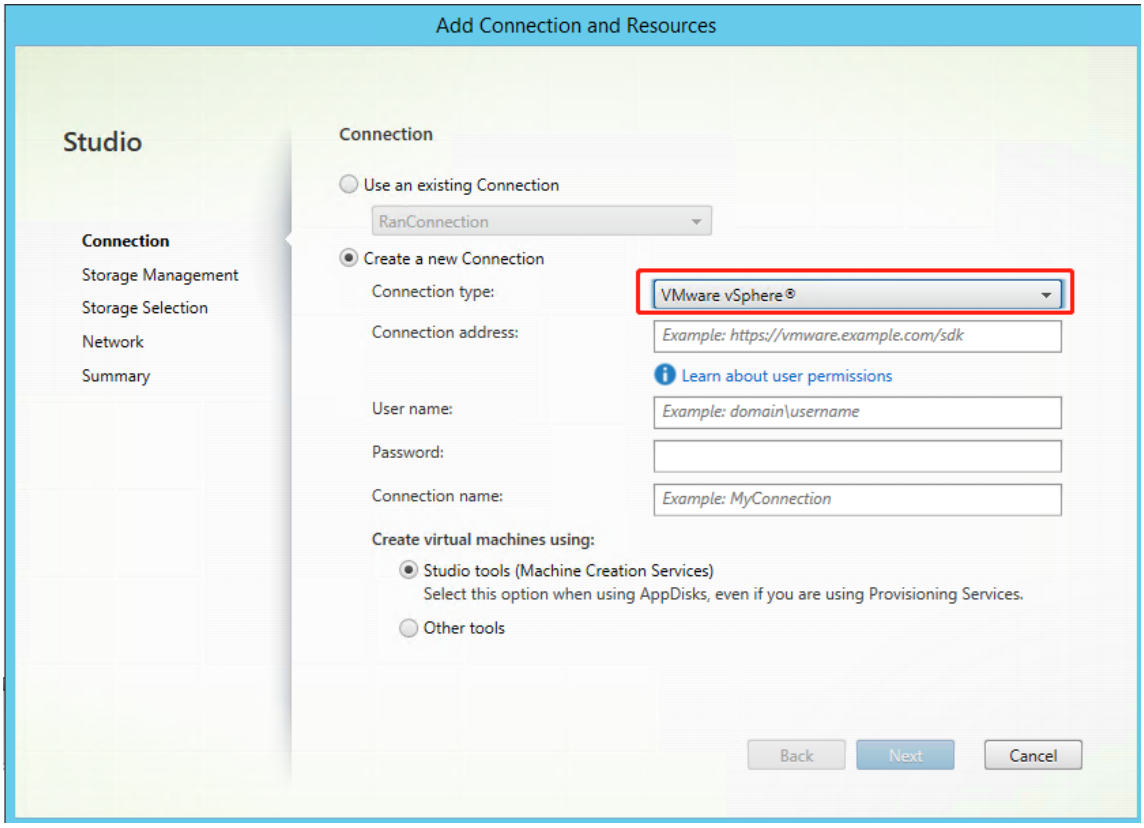
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Crear una conexión de host con VMware en Citrix Studio

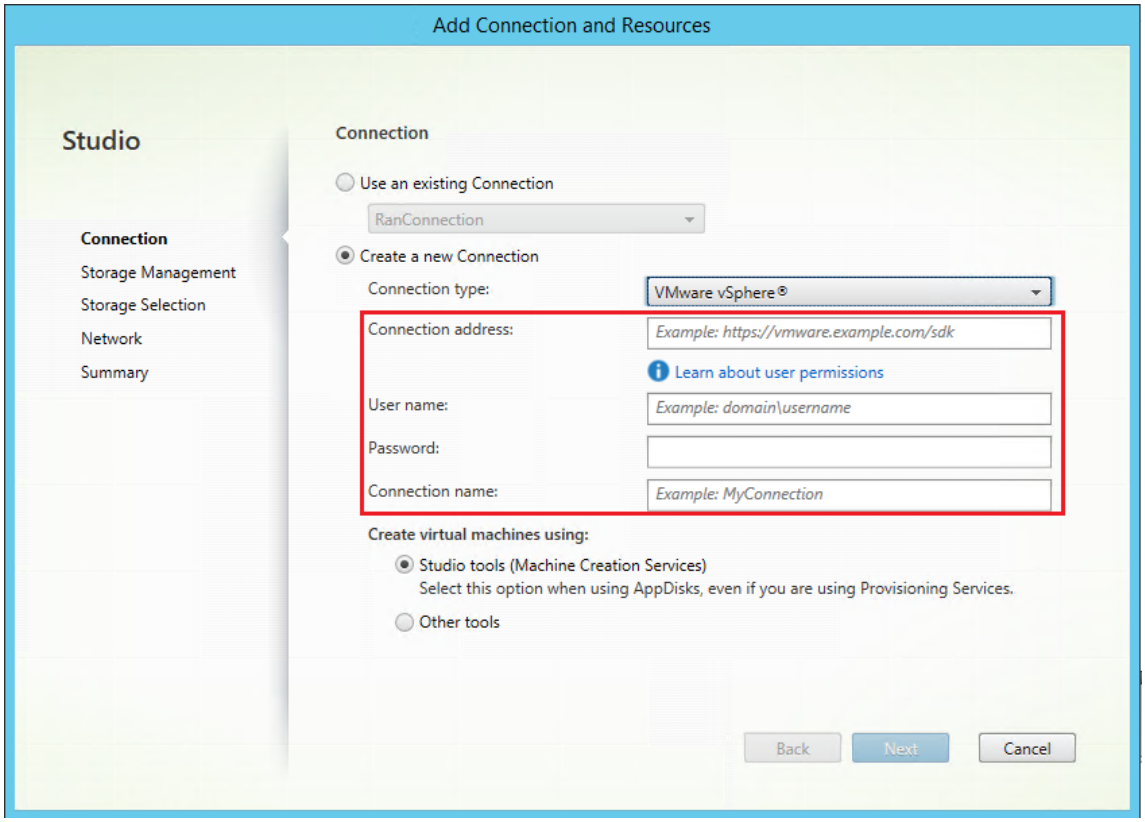
1. Instale vCenter Server en el entorno vSphere. Para obtener más información, consulte VMware vSphere.
2. En Citrix Studio, elija **Configuración > Alojamiento > Agregar conexión y recursos**.
3. Elija VMware vSphere como tipo de conexión.

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



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.



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`).
- 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
```

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

   Para RHEL/CentOS/Rocky Linux:

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

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

```
3  _all.rpm
```

Para Ubuntu/Debian:

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

Para SUSE:

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

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

Paso 3b: Verifique las configuraciones de SUSE 15.4 en AWS, Azure y GCP Para SUSE 15.4 en AWS, Azure y GCP, asegúrese de que:

- Está utilizando **libstdc++6** versión 12 o posterior.
- El parámetro **Default_WM** de **/etc/sysconfig/windowmanager** está configurado en "**gnome**".

Paso 3c: Configure cloud-init para Ubuntu 18.04 en Azure, AWS y GCP

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:

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

Compruebe que estas líneas se encuentran en la sección **system_info** del archivo /etc/cloud/-cloud.cfg:

```
1 system_info:
2    network:
3        renderers: ['netplan', 'eni', 'sysconfig']
```

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).

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

```
users:
- default
```

- 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
  ```

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

Paso 3d: Inhabilite RDNS para Ubuntu 20.04 en GCP En la máquina virtual de la plantilla, agregue la línea **rdns = false** en **[libdefaults]** en /etc/krb5.conf.

Paso 3e: 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/Rocky Linux:

> **Nota:**
>
> - En el caso de RHEL y CentOS, debe instalar el repositorio EPEL para poder instalar Linux VDA y ejecutar `deploymcs.sh` correctamente. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en https://docs.fedoraproject.org/en-US/epel/.
> - Antes de instalar Linux VDA en RHEL 9.0 y Rocky Linux 9.0, actualice el paquete **libsepol** a la versión 3.4 o posterior.

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

Para Ubuntu/Debian:

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

apt-get install -f
```

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

Para SUSE:

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

Paso 3f: Habilite repositorios para instalar el paquete tdb-tools (solo para RHEL 7) **Para el servidor de RHEL 7:**

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

Para la estación de trabajo de RHEL 7:

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

Paso 3g: (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
   ```

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

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

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

   ```
   sudo cd ntfs-3g_ntfsprogs-<package version>
   ```

5. Instale ntfs-3g:

   ```
   ./configure
   make
   make install
   ```

Paso 3h: Especifique una base de datos que se utilizará Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

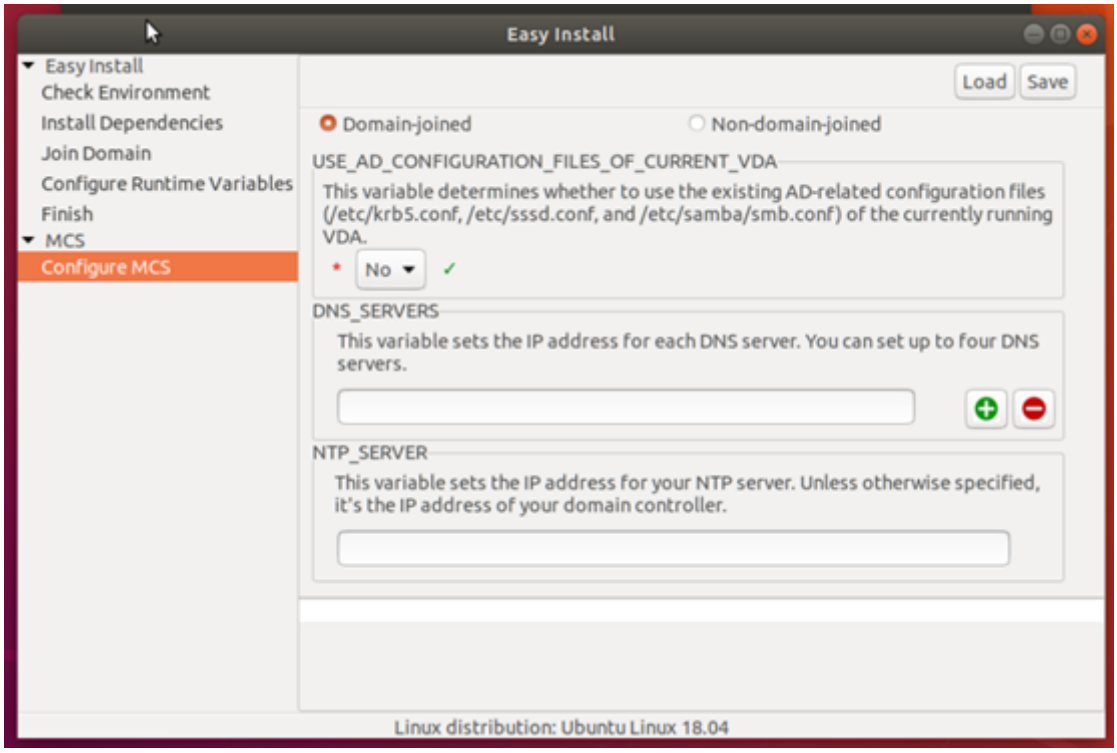
1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.
2. Modifique `/etc/xdl/db.conf` antes de ejecutar `deploymcs.sh`.

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

> **Nota:**
>
> - Le recomendamos utilizar SQLite solo para el modo VDI.
> - Para Easy Install y MCS, puede cambiar entre SQLite y PostgreSQL sin tener que instalarlos manualmente. A menos que se especifique lo contrario mediante `/etc/xdl/db.conf`, Linux VDA usa PostgreSQL de forma predeterminada.
> - También puede utilizar `/etc/xdl/db.conf` para configurar el número de puerto de PostgreSQL.

Paso 3i: Configure las variables de MCS Hay dos formas de configurar variables de MCS:

- Modifique el archivo `/etc/xdl/mcs/mcs.conf`.
- Utilizar la interfaz gráfica de usuario de Easy Install. Para usar la GUI de Easy Install, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su Linux VDA.



> **Sugerencia:**
>
> Haga clic en **Save** para guardar los parámetros de las variables en un archivo local en la ruta que especifique. Haga clic en **Load** para cargar los parámetros de las variables desde el archivo que especifique.

Estas son variables de MCS que puede configurar para casos no unidos a ningún dominio y casos unidos a un dominio:

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

- **Para supuestos sin unión a ningún dominio**

  Puede utilizar los valores predeterminados de las variables o personalizar las variables según sea necesario (opcional):

  `DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
  `DESKTOP_ENVIRONMENT`= **gnome | mate **
  `REGISTER_SERVICE`=**Y | N**
  `ADD_FIREWALL_RULES`=**Y | N**
  `VDI_MODE`=**Y | N**
  `START_SERVICE`=**Y | N**

- **Para supuestos con unión a un dominio**

  - `Use_AD_Configuration_Files_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.
  - `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.

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

- `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.
- 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>‘**
  `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**

Paso 3j: Escriba o actualice los valores del Registro para MCS En la máquina de la plantilla, agregue líneas de comandos al archivo `/etc/xdl/mcs/mcs_local_setting.reg` para escribir o actualizar los valores del Registro según sea necesario. Esta acción evita la pérdida de datos y configuraciones cada vez que se reinicia una máquina aprovisionada con MCS.

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

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

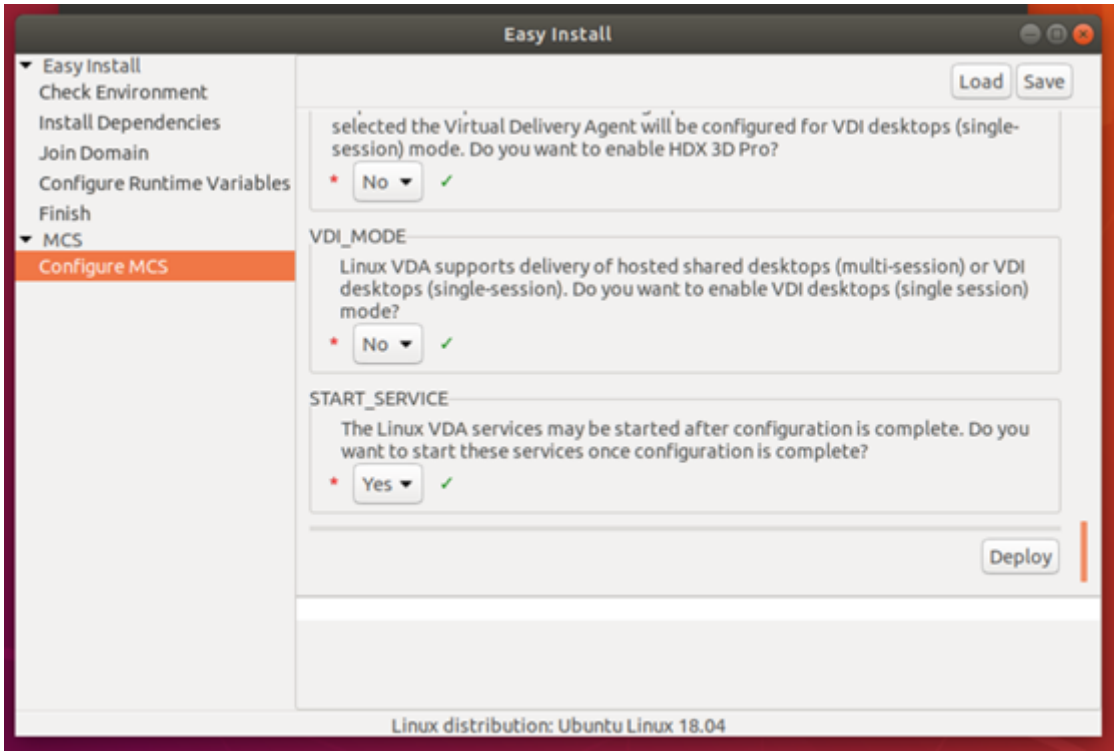
```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels
    \Clipboard\ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0
    x00000003" --force
```

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

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

Paso 3k: Cree una imagen maestra

1. Si configura variables de MCS mediante la modificación de `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura variables de MCS mediante la GUI, haga clic en **Deploy**.



   Tras hacer clic en **Deploy** en la GUI, las variables que defina en la GUI supeditarán las variables que haya establecido en el archivo `/etc/xdl/mcs/mcs.conf`.

2. (si utiliza un VDA que se está ejecutando como máquina virtual de plantilla o la máquina no está unida a ningún dominio, 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/ad_join/winbind_krb5.conf.tmpl` y `/etc/xdl/ad_join/winbind_smb.conf.tmpl`.

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

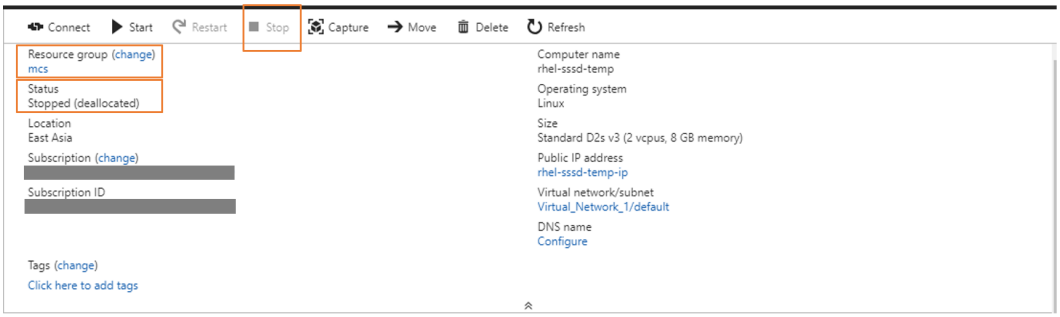
   Para los usuarios de Centrify, actualice las plantillas `/etc/xdl/ad_join/centrify_krb5.conf.tmpl` y `/etc/xdl/ad_join/centrify_smb.conf.tmpl`.

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

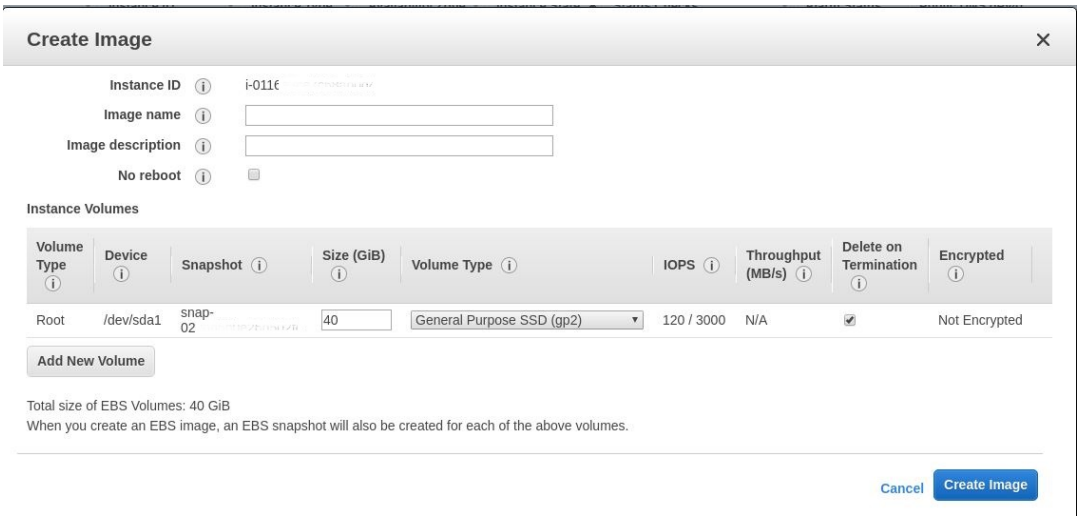
> **Nota:**
>
> Mantenga el formato utilizado en los archivos de plantilla y utilice variables como $WORKGROUP, $REALM, $realm, ${new_hostname} y $AD_FQDN.

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**.



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

- **(Para Nutanix)** En Nutanix AHV, apague la máquina virtual de plantilla. Cree y nombre la instantánea de su imagen maestra.

  > **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.

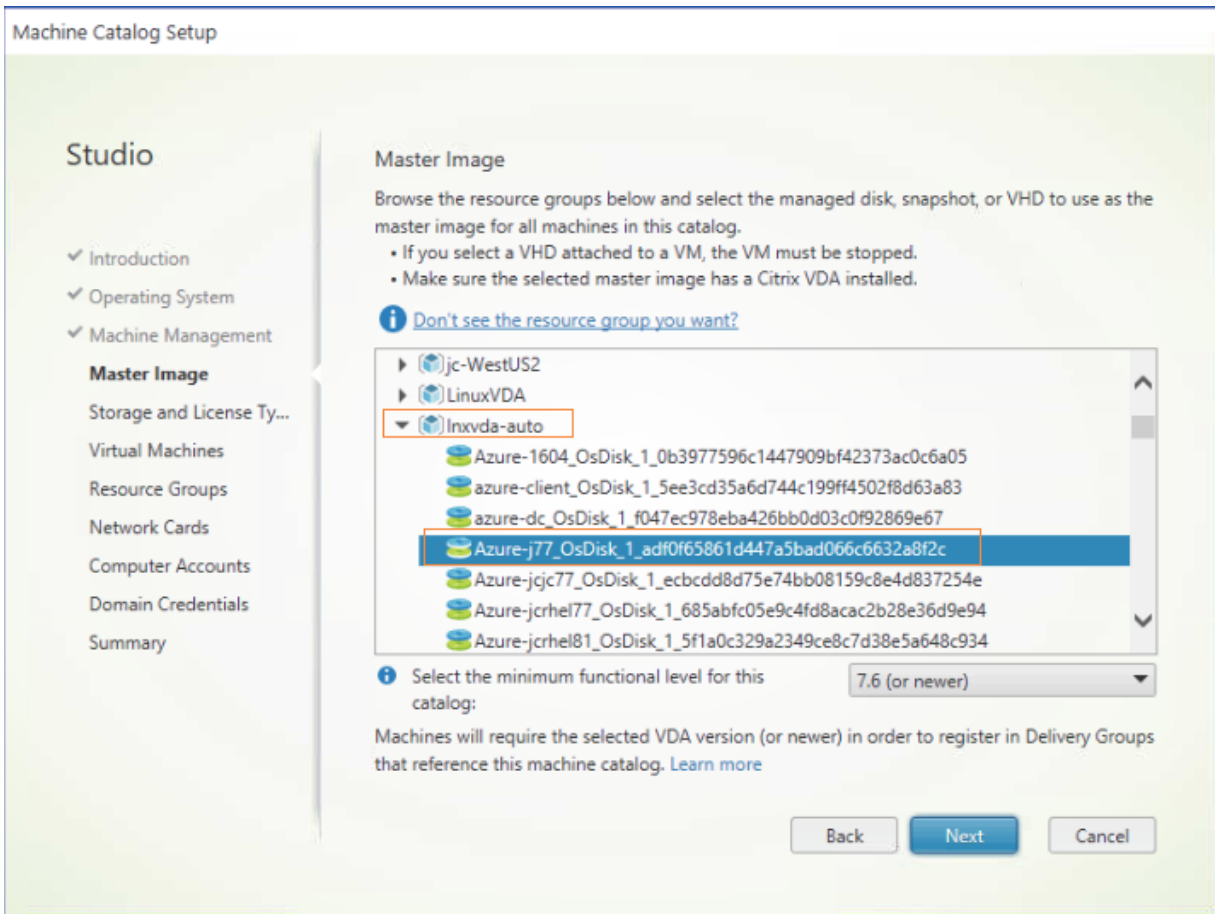
(Para GCP) Paso 3l: Configure la conexión Ethernet en RHEL 8.x/9.x y Rocky Linux 8.x/9.x Tras instalar Linux VDA en RHEL 8.x/9.x y Rocky Linux 8.x/9.x alojados en GCP, es posible que se pierda la conexión Ethernet y que no se pueda acceder a Linux VDA después de reiniciar la máquina virtual. Para solucionar el problema, ejecute estos comandos antes de reiniciar la máquina virtual:

```
nmcli dev connect eth0
service NetworkManager restart
```

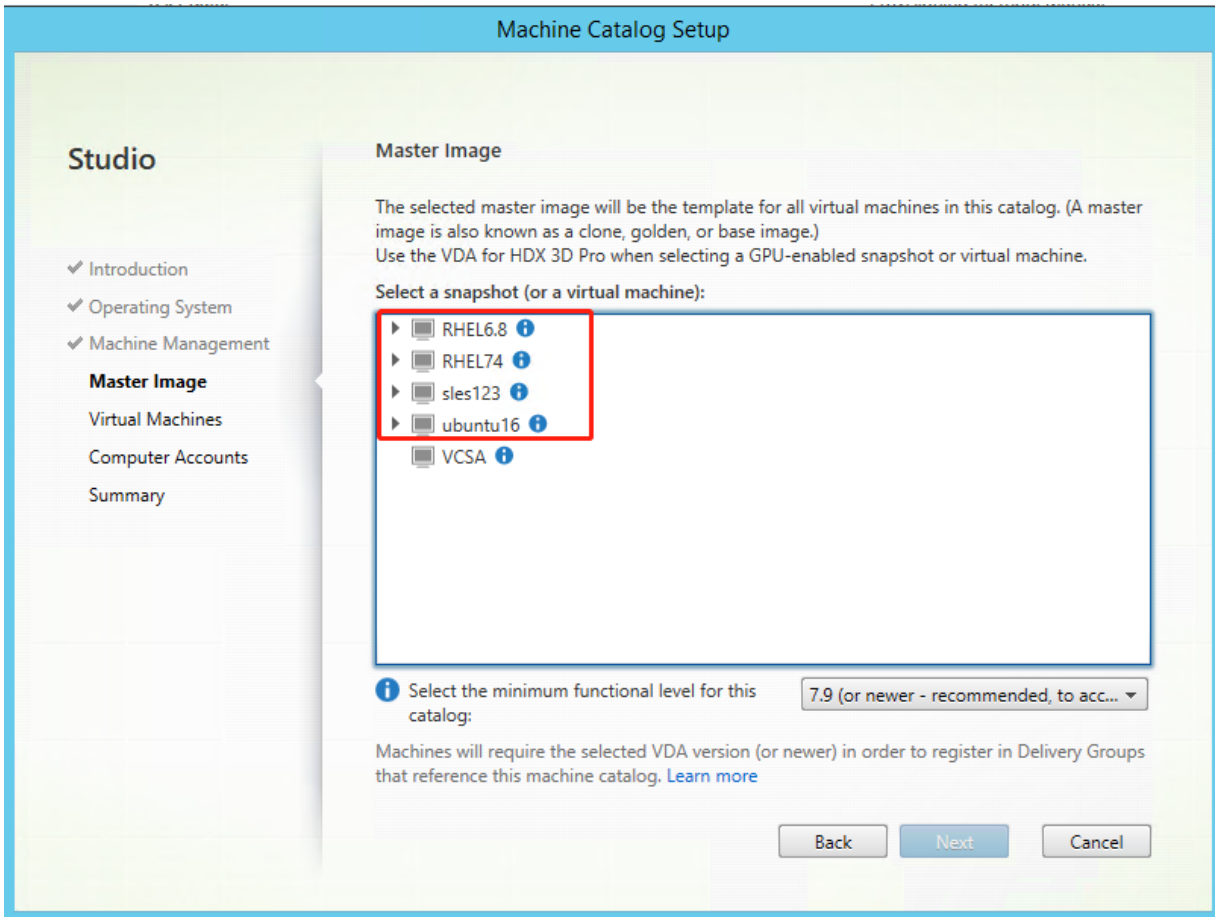
Paso 4: Cree un catálogo de máquinas

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.



© 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 la versión de Linux VDA

Para usar MCS para actualizar la versión de 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
```

Para RHEL 7 y CentOS 7:

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

Para RHEL 8.x y Rocky Linux 8.x:

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

Para RHEL 9.0 y Rocky Linux 9.0:

> **Nota:**
>
> Antes de actualizar Linux VDA en RHEL 9.0 y Rocky Linux 9.0, actualice el paquete **libsepol** a la versión 3.4 o posterior.

```
sudo rpm -U XenDesktopVDA-<version>.el9x.x86_64.rpm
```

Para SUSE:

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

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

Para Ubuntu 18.04:

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

Para Ubuntu 20.04:

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

Para Ubuntu 22.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

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="Y"
   ```

2. Después de ejecutar /opt/Citrix/VDA/sbin/deploymcs.sh., abra /etc/cron.d/mcs_update_password_cronjob para establecer la hora y la frecuencia de actualización. 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.

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

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:

	Winbind	SSSD	Centrify	PBIS
RHEL 9.0	Sí	No	No	No
RHEL 8.x	Sí	No	No	Sí
Rocky Linux 9.0	Sí	No	No	No
Rocky Linux 8.x	Sí	No	No	No
RHEL 7, CentOS 7	Sí	Sí	No	Sí
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Sí	No	No	No
Debian 11.3	Sí	No	No	No
SUSE 15.4	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/
```

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_AD_Configuration_Files_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`.

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

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:

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_AD_Configuration_Files_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/
   ```

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

Crear Linux VDA mediante Citrix Provisioning

March 27, 2023

Puede crear VDA unidos a un dominio mediante Citrix Provisioning.

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 22.04
- Ubuntu 20.04
- Ubuntu 18.04
- RHEL 8.6
- Rocky Linux 8.6
- RHEL 8.4
- RHEL 7.9

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

> **Importante:**
>
> - Le recomendamos que utilice el paquete de instalación más reciente de Citrix Provisioning. 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.
> - Cuando use 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.

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 9.0
- RHEL 8.7
- RHEL 8.6
- RHEL 8.4
- Rocky Linux 9.0
- Rocky Linux 8.7
- Rocky Linux 8.6
- SUSE 15.4
- Ubuntu 22.04

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

- Ubuntu 20.04
- Ubuntu 18.04

Paso 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
> ```

1. En Azure, cree una máquina virtual Linux de una distribución compatible.
2. Instale un entorno de escritorio en la máquina virtual de Linux si fuera necesario.
3. 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.
4. (Solo para Ubuntu) Agregue la línea `source /etc/network/interfaces.d/*` al archivo `/etc/network/interfaces`.
5. (Solo para Ubuntu) Apunte `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf`, en lugar de apuntar a `/run/systemd/resolve/stub-resolv.conf`:

   ```
   unlink /etc/resolv.conf

   ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

6. Instale el paquete de Linux VDA.
7. Especifique la base de datos que se utilizará.

   Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

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

a) Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh` Omita este paso si se trata de una instalación nueva.

b) Modifique `/etc/xdl/db.conf` antes de ejecutar `deploymcs.sh`.

> **Nota:**
>
> - Le recomendamos utilizar SQLite solo para el modo VDI.
> - Para Easy Install y MCS, puede cambiar entre SQLite y PostgreSQL sin tener que instalarlos manualmente. A menos que se especifique lo contrario mediante `/etc/xdl/db.conf`, Linux VDA usa PostgreSQL de forma predeterminada.
> - También puede utilizar `/etc/xdl/db.conf` para configurar el número de puerto de PostgreSQL.

8. Cambie las variables de MCS.

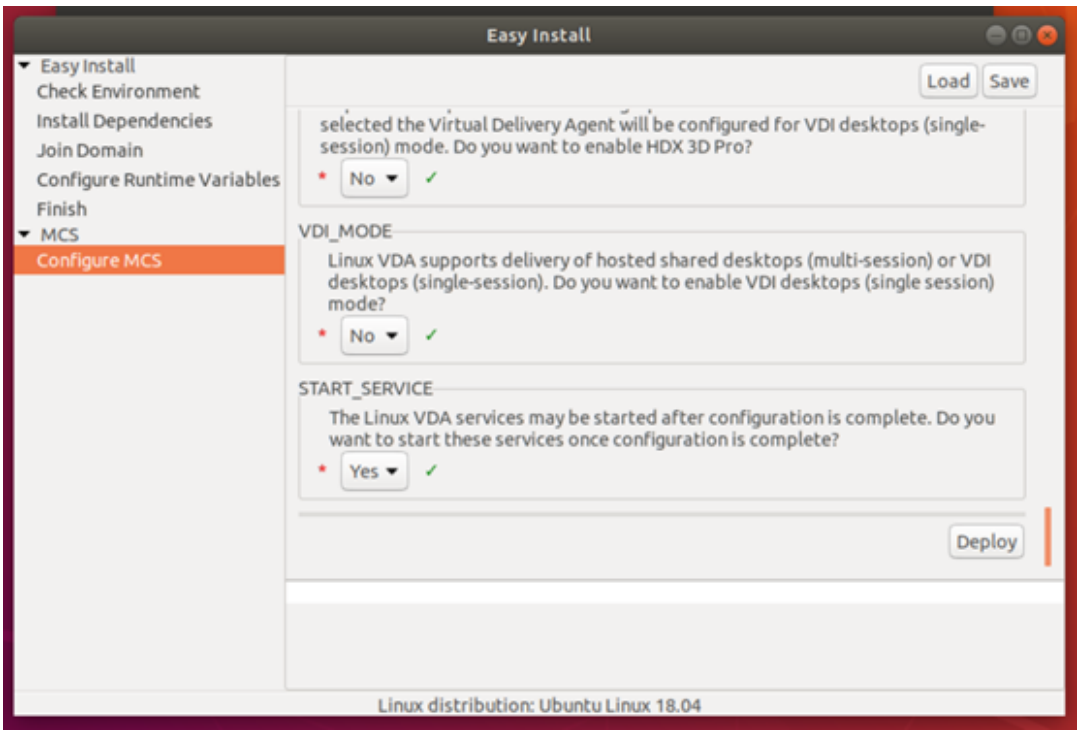
   Hay dos formas de configurar variables de MCS:

   - Modificar el archivo `/etc/xdl/mcs/mcs.conf`.
   - Utilizar la interfaz gráfica de usuario de Easy Install. Para usar la GUI de Easy Install, ejecute el comando `/opt/Citrix/VDA/bin/easyinstall` en el entorno de escritorio de su 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`.

     Si configura variables de MCS mediante la modificación de `/etc/xdl/mcs/mcs.conf`, ejecute `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si configura variables de MCS mediante la GUI, haga clic en **Deploy**.

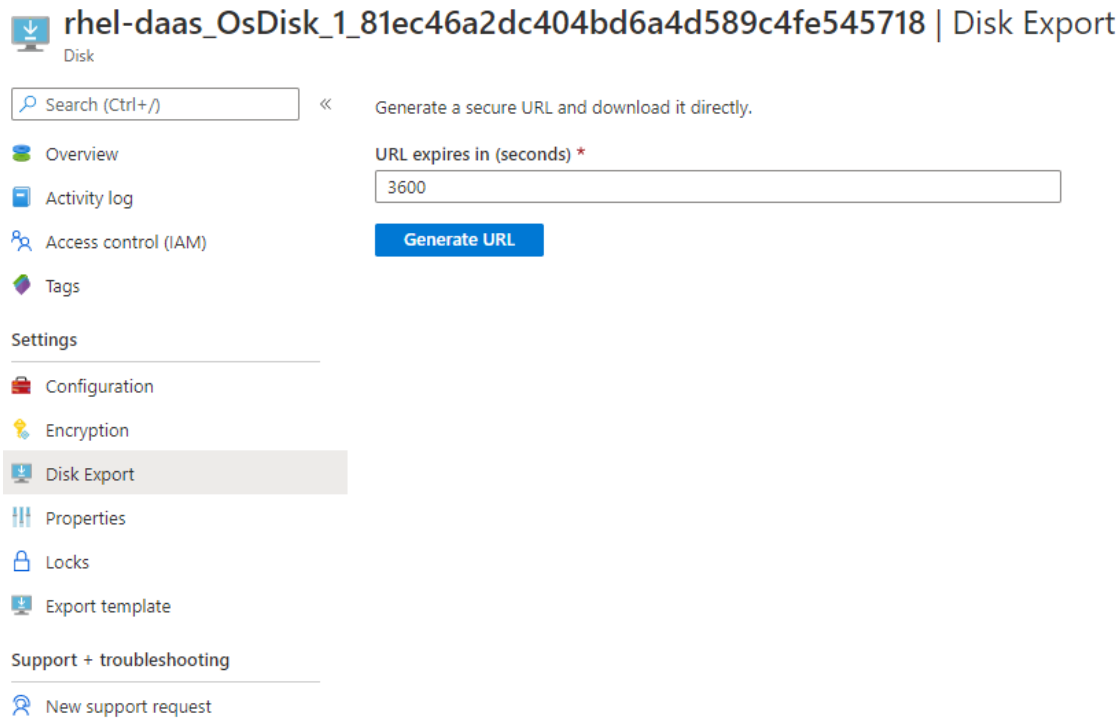
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Tras hacer clic en **Deploy** en la GUI, las variables que defina en la GUI supeditarán las variables que haya establecido en el archivo `/etc/xdl/mcs/mcs.conf`.

9. 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.

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



10. (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.

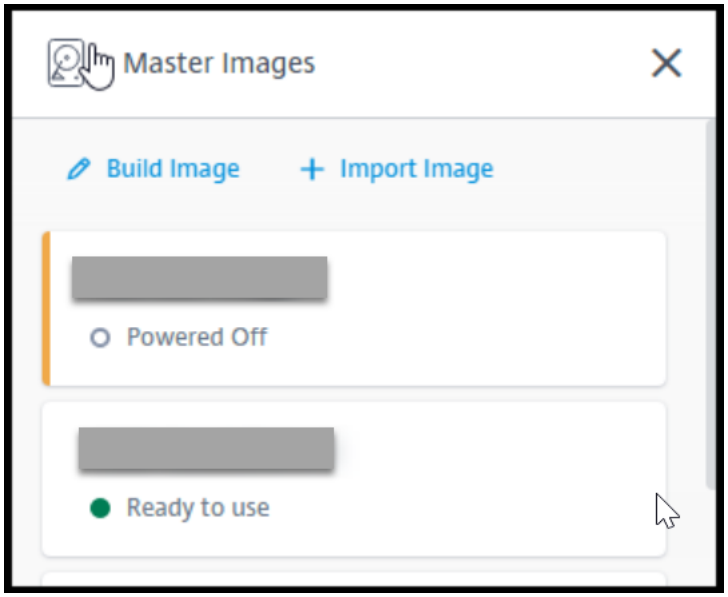
```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    GroupPolicy\Defaults\PrintingPolicies" -t "REG_DWORD" -v "
    AutoCreatePDFPrinter" -d "0x00000001" – force
```

Paso 2: Importe la imagen maestra desde Azure

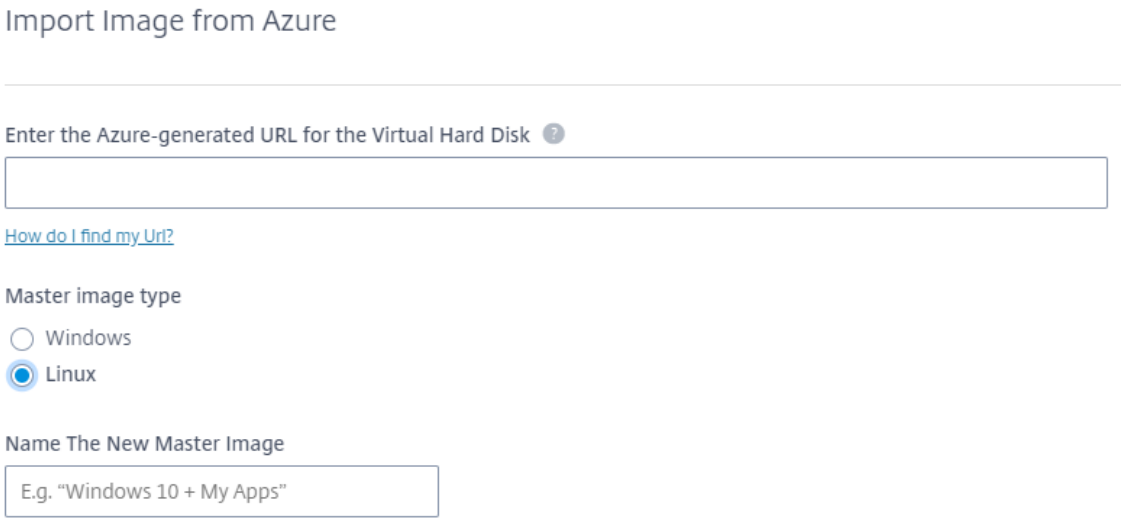
1. En el panel de mandos Administrar, expanda **Imágenes maestras** a la derecha. La pantalla muestra las imágenes maestras que proporciona Citrix y las imágenes que ha creado e importado.

> **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**.

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



2. Haga clic en **Importar imagen**.
3. Escriba la dirección URL SAS del archivo VHD que generó en Azure. Seleccione **Linux** para el tipo de imagen maestra.



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

Paso 3: 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.

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

> **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.

Instalar Linux VDA manualmente

March 27, 2023

Puede instalar Linux VDA en las siguientes distribuciones Linux de forma manual:

- Amazon Linux 2, CentOS, RHEL y Rocky Linux
- SUSE
- Ubuntu
- Debian

Instalar Linux VDA en Amazon Linux 2, CentOS, RHEL y Rocky Linux manualmente

August 20, 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 información de configuración y la máquina Linux

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.

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

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:

```
1 hostname
```

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
```

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

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

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
```

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 (VM) 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 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

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 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
```

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

Paso 1g: Instale PulseAudio (solo para RHEL 9.0 y Rocky Linux 9.0)

Ejecute este comando para instalar **pulseaudio**:

```
sudo yum -y install pulseaudio --allowerasing
```

Abra `/etc/pulse/client.conf` y agregue esta entrada:

```
autospawn = yes
```

Paso 1h: Instale OpenJDK 11

Linux VDA requiere la presencia de OpenJDK 11.

- Si utiliza CentOS, RHEL o Rocky Linux, 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
  ```

Confirme la versión correcta:

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

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

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

Paso 1i: Instale y especifique la base de datos que se utilizará

Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para las instalaciones manuales, debe instalar SQLite y PostgreSQL manualmente antes de poder cambiar entre ellas.

En esta sección se describe cómo instalar las bases de datos PostgreSQL y SQLite y cómo especificar la base de datos que se utilizará.

> **Nota:**
>
> Le recomendamos utilizar SQLite solo para el modo VDI.

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

Instalar PostgreSQL El Linux VDA requiere PostgreSQL:

- PostgreSQL 9 para Amazon Linux 2, RHEL 7 y CentOS 7
- PostgreSQL 10 para RHEL 8.x y Rocky Linux 8.x
- PostgreSQL 13 para RHEL 9.0 y Rocky Linux 9.0

Ejecute estos comandos para instalar PostgreSQL:

```
sudo yum -y install postgresql-server

sudo yum -y install postgresql-jdbc
```

Para RHEL 8.x y RHEL 9.0, ejecute este comando para instalar `libpq` para PostgreSQL:

```
sudo yum -y install libpq
```

Ejecute este comando para inicializar la base de datos. Los archivos de base de datos se crean en **/var/lib/pgsql/data**.

```
sudo postgresql-setup initdb
```

Ejecute estos comandos para iniciar PostgreSQL al iniciar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql

sudo systemctl start postgresql
```

Compruebe la versión de PostgreSQL con:

```
psql --version
```

(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'
```

Instalar SQLite Ejecute este comando para instalar SQLite:

```
sudo yum -y install sqlite
```

Especificar la base de datos que se utilizará Tras instalar SQLite, PostgreSQL o ambos, puede especificar una base de datos que utilizar al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.

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

2. Modifique `/etc/xdl/db.conf` para especificar la base de datos que se utilizará.
3. Ejecute `ctxsetup.sh`.

> **Nota:**
>
> También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

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:

```
su -

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

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
```

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

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

```
xen.independent_wallclock = 1
```

Para comprobar los cambios, reinicie el sistema:

```
su -

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux 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

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**.

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

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

Hay estos métodos disponibles 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.x/9.0 y Rocky Linux 8.x/9.0:

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

Para Amazon Linux 2, CentOS 7 y RHEL 7:

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

Habilitar el demonio 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
```

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

1. Ejecute este comando:

   Para RHEL 8.x/9.0 y Rocky Linux 8.x/9.0:

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

   Para Amazon Linux 2, CentOS 7 y RHEL 7:

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

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

Donde **REALM** es el nombre del 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.

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 para RHEL 8.x/9.0 y Rocky Linux 8.x/9.0) 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.

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

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.x/9.0 y Rocky Linux 8.x/9.0:

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

Para Amazon Linux 2 y RHEL 7:

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

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

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

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

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

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

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

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

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

Para RHEL 9.0 y Rocky Linux 9.0, ejecute estos comandos para evitar que `pam_winbind` cambie la propiedad del directorio raíz y para resolver el problema de SELinux con Winbind:

```
usermod -d /nonexistent nobody

ausearch -c 'winbindd' --raw | audit2allow -M my-winbindd -p /etc/
    selinux/targeted/policy/policy.*

semodule -X 300 -i my-winbindd.pp
```

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

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA (tanto Windows como 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
```

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

```
sudo net ads info
```

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

```
sudo klist -ke
```

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
```

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
```

Examine los datos de la cuenta de la máquina:

```
sudo net ads status
```

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
```

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.

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

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
```

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

```
klist
```

Salga de la sesión.

```
exit
```

Se puede realizar una prueba similar iniciando sesión directamente en la consola 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.

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

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
```

> **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
```

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
```

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

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

El 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.

© 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
```

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
```

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
```

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
```

Salga de la sesión.

```
exit
```

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
```

© 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 (tanto Windows como Linux) tengan un objeto de equipo en Active Directory. Para comprobar si hay una máquina Linux unida a Centrify en el dominio:

```
su -
adinfo
```

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all
adinfo -diag
```

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

```
adinfo --test
```

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 **adcli**, **realmd** o **Samba**.

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

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
  ```

  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
  ```

  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
  ```

  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.

- **Adcli (RHEL 8.x/9.0 y Rocky Linux 8.x/9.0):**

  Instale o actualice los paquetes requeridos:

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

  Configure la máquina para la autenticación Kerberos y **Samba**:

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

  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
  ```

  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 para RHEL 8.x/9.0 y Rocky Linux 8.x/9.0)
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.x/9.0 y Rocky Linux 8.x/9.0:**

© 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
```

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
```

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

```
sudo klist -ke
```

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
```

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
```

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
```

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:

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

- 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
```

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 }
```

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
```

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

PBIS

Descargar el paquete PBIS requerido

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

Convertir el script de instalación de PBIS en ejecutable

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

Ejecutar el script de instalación de PBIS

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

Unirse al dominio de Windows 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
```

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 **/opt/pbis/bin/config LoginShellTemplate/bin/bash**.

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA (tanto Windows como 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
```

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.

```
ssh localhost -l domain\user

id -u
```

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
```

Salga de la sesión.

```
exit
```

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

Paso 4: Instale .NET Runtime 6.0

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

1. Vaya a la página de descargas de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Haga clic en **Componentes** para descargar el paquete de Linux VDA que corresponda a su distribución de Linux y la clave pública GPG que puede usar para comprobar la integridad del paquete de Linux VDA.

   Para verificar la integridad del paquete de Linux VDA, importe la clave pública a la base de datos RPM y ejecute estos comandos:

   ```
   ```
   rpmkeys --import <path to the public key>
   rpm --checksig --verbose <path to the Linux VDA package>
   ```
   ```

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.

Paso 6a: Realice 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
   ```

   > **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
   ```

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

> **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

   > **Nota:**
   >
   > - En el caso CentOS, RHEL y Rocky Linux, debe instalar el repositorio EPEL para poder instalar Linux VDA correctamente. Para obtener información sobre cómo instalar EPEL, consulte las instrucciones en https://docs.fedoraproject.org/en-US/epel/.
   > - Antes de instalar Linux VDA en RHEL 9.0 y Rocky Linux 9.0, actualice el paquete **libsepol** a la versión 3.4 o posterior.

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

     Para Amazon Linux 2:

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

     Para RHEL 9.0 y Rocky Linux 9.0:

     ```
     sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
     ```

     Para RHEL 8.x y Rocky Linux 8.x:

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

     Para RHEL 7 y CentOS 7:

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

   - 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
     ```

     RHEL 9.0 y Rocky Linux 9.0:

     ```
     sudo rpm -i XenDesktopVDA-<version>.el9_x.x86_64.rpm
     ```

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

Para RHEL 8.x y Rocky Linux 8.x:

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

Para RHEL 7 y CentOS 7:

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

Lista de dependencias de RPM para RHEL 9.0 y Rocky Linux 9.0:

```
java-11-openjdk >= 11

 icoutils >= 0.32

 firewalld >= 0.6.3

 policycoreutils-python >= 2.8.9

 policycoreutils-python-utils >= 2.8

 python3-policycoreutils >= 2.8

 dbus >= 1.12.8

 dbus-common >= 1.12.8

 dbus-daemon >= 1.12.8

 dbus-tools >= 1.12.8

 dbus-x11 >= 1.12.8

 xorg-x11-server-utils >= 7.7

 xorg-x11-xinit >= 1.3.4

 libXpm >= 3.5.12

 libXrandr >= 1.5.1

 libXtst >= 1.2.3

 pam >= 1.3.1

 util-linux >= 2.32.1

 util-linux-user >= 2.32.1

 xorg-x11-utils >= 7.5

 bash >= 4.3

 findutils >= 4.6
```

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

```

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7

krb5-workstation >= 1.13

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9
```

Lista de dependencias de RPM para RHEL 8.x y Rocky Linux 8.x:

```
java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

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

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7

krb5-workstation >= 1.13

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4
```

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

```

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9
```

Lista de dependencias de RPM para CentOS 7 y RHEL 7:

```
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

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.

```
foomatic-filters >= 4.0.9

libxml2 >= 2.9

libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qt5-qtbase >= 5.5~

imlib2 >= 1.4.5
```

Lista de dependencias de RPM para Amazon Linux 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

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2
```

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

```
30
31  findutils >= 4.5
32
33  gawk >= 4.0
34
35  sed >= 4.2
36
37  cups >= 1.6.0
38
39  foomatic-filters >= 4.0.9
40
41  libxml2 >= 2.9
42
43  libmspack >= 0.5
44
45  ibus >= 1.5
46
47  cyrus-sasl-gssapi >= 2.1
48
49  gperftools-libs >= 2.4
50
51  nss-tools >= 3.44.0
52
53  qt5-qtbase >= 5.5~
54
55  qrencode-libs >= 3.4.1
56
57  imlib2 >= 1.4.5
```

> **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.

Paso 6b: Actualice la versión de una instalación existente (opcional)

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.
> - Antes de actualizar Linux VDA en RHEL 9.0 y Rocky Linux 9.0, actualice el paquete **libsepol**

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

> a la versión 3.4 o posterior.

- Para actualizar el software con Yum:

  Para Amazon Linux 2:

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

  Para RHEL 9.0 y Rocky Linux 9.0:

```
sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

  Para RHEL 8.x y Rocky Linux 8.x:

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

  Para RHEL 7 y CentOS 7:

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

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

  Para Amazon Linux 2:

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

  Para RHEL 9.0 y Rocky Linux 9.0:

```
sudo rpm -U XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

  Para RHEL 8.x y Rocky Linux 8.x:

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

  Para RHEL 7 y CentOS 7:

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

> **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:**

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

> 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. 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
```

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

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

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

© 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 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 |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**: Determina si configurar la máquina a partir de un modelo de entrega de escritorios dedicados (VDI) o un modelo de entrega de escritorios compartidos aloja-

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

dos. 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 ad2.miempresa.com:3268 ad3.miempresa.com:3268. Si especifica el número de puerto de LDAP como 389, Linux VDA consulta a cada servidor LDAP del dominio especificado en modo de sondeo. Si hay una cantidad "x"de directivas y una cantidad "y"de servidores LDAP, Linux VDA realiza el total de consultas X multiplicado por Y. Si el tiempo de sondeo supera el umbral, los inicios de sesión pueden fallar. Para habilitar las consultas LDAP más rápidas, habilite **Catálogo global** en un controlador de dominio y especifique 3268 como número de puerto LDAP correspondiente. 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. Para comunicarse correctamente con los servidores de FAS, agregue un número de puerto coherente con el especificado en los servidores de FAS. Por ejemplo: CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **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**.

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

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.
   - **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
     exec gnome-session
     fi
     ```

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

A partir de la versión 2209, los usuarios de las sesiones pueden personalizar sus entornos de escritorio. Para habilitar esta función, debe instalar con antelación en el VDA entornos de escritorio que se puedan cambiar. Para obtener más información, consulte Entornos de escritorio personalizados por usuarios de las sesiones.

- **CTX_XDL_START_SERVICE=Y | N**: Determina si los servicios de Linux VDA se inician cuando se complete su configuración. El valor predeterminado es Y.
- **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:

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

```
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
```

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 \
```

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

```
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
```

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
```

Para quitar los cambios de configuración:

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

> **Importante:**
>
> Este script elimina todos los datos de configuración de la base de datos y 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**.

© 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
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

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

Comprobar el estado de Linux VDA:

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

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

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
```

Paso 11: Cree catálogos de máquinas

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:**
>
> Cuando una de nuevo una máquina eliminada al dominio de Active Directory, quite la máquina de su catálogo de máquinas y agréguela de nuevo ahí.

Paso 12: Cree grupos de entrega

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.

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

- 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 2212.

Instalar Linux VDA en SUSE manualmente

August 20, 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 información de configuración y la máquina Linux

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
```

Para iniciar la herramienta YaST de interfaz gráfica:

```
su -

yast2 &
```

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,

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

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**.
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.
>
> **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.

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

```
hostname
```

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
```

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

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

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
```

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 (VM) 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 15.4:

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
   ```

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

Paso 1d: Instale paquetes dependientes de Linux VDA

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

- 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
```

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
```

Instalar y especificar la base de datos que se utilizará Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para las instalaciones manuales, debe instalar SQLite y PostgreSQL manualmente antes de poder cambiar entre ellas.

En esta sección se describe cómo instalar las bases de datos PostgreSQL y SQLite y cómo especificar la base de datos que se utilizará.

> **Nota:**
>
> Le recomendamos utilizar SQLite solo para el modo VDI.

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

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

```
sudo zypper install postgresql-server

sudo zypper install postgresql-jdbc
```

Ejecute estos comandos para iniciar PostgreSQL al iniciar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql

sudo systemctl restart postgresql
```

Instalar SQLite Para SUSE, ejecute este comando para instalar SQLite:

```
sudo zypper install sqlite3
```

Especificar la base de datos que se utilizará Tras instalar SQLite, PostgreSQL o ambos, puede especificar una base de datos que utilizar al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.
2. Modifique `/etc/xdl/db.conf` para especificar la base de datos que se utilizará.
3. Ejecute `ctxsetup.sh`.

> **Nota:**
>
> También puede utilizar `/etc/xdl/db.conf` para configurar el número de puerto de PostgreSQL.

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

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.

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

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
```

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
```

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
```

Después de reiniciar, compruebe que la configuración es correcta:

```
su -

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

Este comando devuelve el valor 1.

Corregir la sincronización horaria en Microsoft Hyper-V

Las máquinas virtuales Linux 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.

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

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**.

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

Hay estos métodos disponibles para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- 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.

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

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:

```
su -
reboot
```

Verificar la pertenencia al dominio El Delivery Controller requiere que todas las máquinas VDA (tanto Windows como 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
```

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

```
sudo net ads info
```

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

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

```
sudo klist -ke
```

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
```

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
```

Examine los datos de la cuenta de la máquina:

```
sudo net ads status
```

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
```

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
```

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
```

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:

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

```
klist
```

Salga de la sesión.

```
exit
```

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:

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
```

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.

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

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
```

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

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

El 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.

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
```

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
```

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
```

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
```

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

Salga de la sesión.

```
exit
```

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

Centrify DirectControl

Unirse al dominio de Windows Con el Agente Centrify DirectControl instalado, una la máquina Linux al dominio de Active Directory mediante el comando **adjoin** de Centrify:

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

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

```
sudo adinfo
```

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo – diag
```

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

```
adinfo --test
```

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.

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

Para configurar SSSD en SUSE, siga estos pasos:

1. Unirse al dominio y crear keytabs de host
2. Configurar PAM para SSSD
3. Configurar SSSD
4. Habilitar SSSD
5. Verificar la pertenencia al dominio
6. Verificar la configuración de Kerberos
7. Verificar la autenticación de usuario

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 el enfoque de **Samba**. 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
```

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

```
hostname
hostname -f
chronyc traking
```

3. Instale o actualice los paquetes requeridos:

```
sudo zypper install samba-client sssd-ad
```

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
```

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
```

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
```

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

```
kinit administrator
```

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

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

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

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

```
sudo zypper install sssd sssd-ad
```

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

```
sudo pam-config --add  --sss
sudo pam-config --add --mkhomedir
```

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

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

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

```

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

```
28      ad_gpo_access_control = permissive
```

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`:

```
1  sudo chmod 0600 /etc/sssd/sssd.conf
```

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

```
1  sudo systemctl enable sssd
2  sudo systemctl start sssd
```

Verificar la pertenencia al dominio

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

```
1  sudo net ads testjoin
```

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

```
1  sudo net ads info
```

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

```
1  sudo klist -ke
```

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:

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

```
sudo kinit -k MACHINE$@REALM
```

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
```

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
```

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
```

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
```

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

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

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

Ejecutar el script de instalación de PBIS Por ejemplo:

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

Unirse a un dominio de Windows 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
```

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
```

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
```

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
```

Salga de la sesión.

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

```
exit
```

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

Paso 4: Instale .NET Runtime 6.0

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

1. Vaya a la página de descargas de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Haga clic en **Componentes** para descargar el paquete de Linux VDA que corresponda a su distribución de Linux y la clave pública GPG que puede usar para comprobar la integridad del paquete de Linux VDA.

   Para verificar la integridad del paquete de Linux VDA mediante la clave pública, importe la clave pública a la base de datos RPM y ejecute estos comandos:

   ```
   rpmkeys --import <path to the public key>
   rpm --checksig --verbose <path to the Linux VDA package>
   ```

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
   ```

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

> **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
```

> **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
```

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

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

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
```

Lista de dependencias de RPM para SUSE 15:

```
java-11-openjdk >= 11

```

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

```
ImageMagick >= 7.0

dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4

cups >= 2.2

cups-filters >= 1.25

libxml2-2 >= 2.9

libmspack0 >= 0.6

ibus >= 1.5

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1

libpython3_6m1_0 >= 3.6~

libQt5Widgets5 >= 5.12

libqrencode4 >= 4.0.0

libImlib2-1 >= 1.4.10
```

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

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

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.

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
```

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

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.

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

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 VDA. Se establece en Y de forma predeterminada.
- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4**: Linux VDA requiere parámetros de configuración Kerberos para autenticarse en los Delivery Controllers. La configuración de Kerberos se determina a partir de la herramienta de integración de Active Directory instalada y configurada en el sistema. Especifique el método admitido de integración de Active Directory que se va a utilizar:
  - 1 –Samba Winbind
  - 2 –Servicio de autenticación Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N**: Linux VDA admite HDX 3D Pro, un conjunto de tecnologías para la aceleración de la GPU que se ha diseñado para optimizar la virtualización de aplicaciones con gráficos sofisticados. Si se selecciona HDX 3D Pro, 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.

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

- **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 ad2.miempresa.com:3268 ad3.miempresa.com:3268. Si especifica el número de puerto de LDAP como 389, Linux VDA consulta a cada servidor LDAP del dominio especificado en modo de sondeo. Si hay una cantidad "x"de directivas y una cantidad "y"de servidores LDAP, Linux VDA realiza el total de consultas X multiplicado por Y. Si el tiempo de sondeo supera el umbral, los inicios de sesión pueden fallar. Para habilitar las consultas LDAP más rápidas, habilite **Catálogo global** en un controlador de dominio y especifique 3268 como número de puerto LDAP correspondiente. 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. Para comunicarse correctamente con los servidores FAS, añada un número de puerto coherente con el especificado en los servidores FAS, por ejemplo, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **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.

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

– **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.

A partir de la versión 2209, los usuarios de las sesiones pueden personalizar sus entornos de escritorio. Para habilitar esta función, debe instalar con antelación en el VDA entornos de escritorio que se puedan cambiar. Para obtener más información, consulte Entornos de escritorio personalizados por usuarios de las sesiones.

- **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

```

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

```
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
```

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 \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

```

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

```
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
```

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 /usr/local/sbin/ctxcleanup.sh --help
```

Para quitar los cambios de configuración:

```
sudo /usr/local/sbin/ctxcleanup.sh
```

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

Registros de configuración

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

`/tmp/xdl.configure.log`

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

Paso 9: Ejecute XDPing

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.

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

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
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

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

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
```

Paso 11: Cree catálogos de máquinas

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 grupos de entrega

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 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 2212.

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

Instalar Linux VDA en Ubuntu manualmente

August 20, 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 información de configuración y la máquina Linux

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
```

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.

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

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

Paso 1d: Compruebe el nombre de host

Compruebe que el nombre de host está definido correctamente:

```
hostname
```

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

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

```
hostname -f
```

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
```

Para:

```
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

```

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

```
nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
```

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 (VM) puede causar problemas de reloj sesgado. Por este motivo, se recomienda sincronizar la hora con un servicio remoto de sincronización horaria.

Instale Chrony:

```
apt-get install chrony
```

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
```

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
```

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

Paso 1i: Instale y especifique la base de datos que se utilizará

Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para las instalaciones manuales, debe instalar SQLite y PostgreSQL manualmente antes de poder cambiar entre ellas.

En esta sección se describe cómo instalar las bases de datos PostgreSQL y SQLite y cómo especificar la base de datos que se utilizará.

> **Nota:**
>
> Le recomendamos utilizar SQLite solo para el modo VDI.

Instalar PostgreSQL Ejecute estos comandos para instalar PostgreSQL:

```
sudo apt-get install -y postgresql

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

Ejecute estos comandos para iniciar PostgreSQL al iniciar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql

sudo systemctl restart postgresql
```

Instalar SQLite Para Ubuntu, ejecute este comando para instalar SQLite:

```
sudo apt-get install -y sqlite3
```

Especificar la base de datos que se utilizará Tras instalar SQLite, PostgreSQL o ambos, puede especificar una base de datos que utilizar al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.
2. Modifique `/etc/xdl/db.conf` para especificar la base de datos que se utilizará.
3. Ejecute `ctxsetup.sh`.

> **Nota:**
>
> También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

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

Paso 1j: Instale Motif

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

Paso 1k: Instale otros paquetes

Para Ubuntu 22.04:

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.5-0
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
```

Para Ubuntu 20.04, Ubuntu 18.04:

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.4-2
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
```

Paso 2: 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
```

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

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
```

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
```

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 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.

© 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, 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 Linux al dominio de Windows

Hay estos métodos disponibles para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- 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
```

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
```

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

> **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 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
```

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

```
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
```

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

Reiniciar winbind

```
1 sudo systemctl restart winbind
```

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:

```
1 sudo pam-auth-update
```

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

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

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

```
1 sudo net ads testjoin
```

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

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

```
sudo net ads info
```

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

```
sudo klist -ke
```

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
```

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
```

Examine los datos de la cuenta de la máquina:

```
sudo net ads status
```

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
```

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
```

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

> **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
```

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
```

Salga de la sesión.

```
exit
```

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.

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

> **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
```

> **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
```

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
```

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

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

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

El usuario es 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
```

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
```

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
```

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
```

Salga de la sesión.

```
exit
```

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:

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

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
```

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo --diag
```

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

```
adinfo --test
```

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
```

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

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

> 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.

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 sobre **adcli** y **Samba**.

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

1. Instale **adcli**.

```
sudo apt-get install adcli
```

2. Únase al dominio con **adcli**.

   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
```

© 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. Verifique la pertenencia al dominio.

   Para máquinas con Ubuntu 22.04 y Ubuntu 20.04, ejecute el comando `adcli testjoin` para comprobar si las máquinas están unidas al dominio.

   Para una máquina con Ubuntu 18.04, ejecute el comando `sudo klist -ket`. La capacidad de la herramienta **adcli** es limitada. La herramienta no proporciona una forma de comprobar si una máquina se ha unido al dominio. La mejor opción es 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.

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

1. Instale el paquete.

```
sudo apt-get install samba krb5-user
```

2. Configure **Samba**.

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

© 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
```

Si los paquetes ya están instalados, se recomienda actualizarlos:

```
sudo apt-get install --only-upgrade sssd
```

> **Nota:**
>
> De forma predeterminada, el proceso de instalación en Ubuntu configura automáticamente **nsswitch.conf** y el módulo de 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
```

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

```
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
```

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
```

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
```

© 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 el Linux VDA, compruebe que el archivo del sistema keytab se haya creado y contenga claves válidas:

```
sudo klist -ke
```

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
```

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
```

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
```

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

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
```

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

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
    /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

Convertir el script de instalación de PBIS en ejecutable

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

Ejecutar el script de instalación de PBIS

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

Unirse al dominio de Windows 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
```

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
```

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.

```
sudo ssh localhost -l domain\user

id -u
```

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
```

Salga de la sesión.

```
exit
```

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

Paso 4: Instale .NET Runtime 6.0

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

1. Vaya a la página de descargas de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Haga clic en **Componentes** para descargar el paquete de Linux VDA que corresponda a su distribución de Linux y la clave pública GPG que puede usar para comprobar la integridad del paquete de Linux VDA.

   Para verificar la integridad del paquete de Linux VDA mediante la clave pública, importe la clave pública a la base de datos DEB y ejecute estos comandos:

   ```
   ```
   sudo apt-get install dpkg-sig
   gpg --import <path to the public key>
   dpkg-sig --verify <path to the Linux VDA package>
   ```
   ```

© 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:

Para Ubuntu 22.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

Para Ubuntu 20.04:

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

> **Nota:**
>
> Para Ubuntu 20.04 en GCP, inhabilite RDNS. Para ello, agregue la línea **rdns = false** en **[libdefaults]** en /etc/krb5.conf.

Para Ubuntu 18.04:

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

Lista de dependencias de Debian para Ubuntu 22.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.11

libgtkmm-3.0-1v5 >= 3.24.5

ufw >= 0.36

ubuntu-desktop >= 1.481

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.37

gtk3-nocsd >= 3

bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4
```

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

```

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.9~

libpython3.10 >= 3.10~

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

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

libimlib2 >= 1.7.4
```

Lista de dependencias de Debian para Ubuntu 20.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.2

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

ibus >= 1.5

```

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

```
libgoogle-perftools4 >= 2.7~

libpython3.8 >= 3.8~

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

libnss3-tools >= 2:3.49

libqt5widgets5 >= 5.7~

libqrencode4 >= 4.0.0

libimlib2 >= 1.6.1
```

Lista de dependencias de Debian para Ubuntu 18.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.8.9.9

ufw >= 0.35

libgtkmm-3.0-1v5 >= 3.22.2

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

gtk3-nocsd >= 3

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libmspack0 >= 0.6

ibus >= 1.5

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

libgoogle-perftools4 >= 2.4~

libpython3.6 >= 3.6~
```

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

```
38
39 libnss3-tools >= 2:3.35
40
41 libqt5widgets5 >= 5.7~
42
43 libqrencode3 >= 3.4.4
44
45 libimlib2 >= 1.4.10
```

> **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 la versión de una instalación existente desde las dos versiones anteriores y desde una versión LTSR.

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

> **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.

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

Paso 8: Configure Linux VDA

Después de instalar el paquete, debe configurar el 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
```

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

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 VDA 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 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 VDA. Se establece en Y de forma predeterminada.

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

- **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 ad2.miempresa.com:3268 ad3.miempresa.com:3268. Si especifica el número de puerto de LDAP como 389, Linux VDA consulta a cada servidor LDAP del dominio especificado en modo de sondeo. Si hay una cantidad "x"de directivas y una cantidad "y"de servidores LDAP, Linux VDA realiza el total de consultas X multiplicado por Y. Si el tiempo de sondeo supera el umbral, los inicios de sesión pueden fallar. Para habilitar las consultas LDAP más rápidas, habilite **Catálogo global** en un controlador de dominio y especifique 3268 como número de puerto LDAP correspondiente. 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 fed-

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

erada (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. Para comunicarse correctamente con los servidores FAS, añada un número de puerto coherente con el especificado en los servidores FAS, por ejemplo, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.

- **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
exec gnome-session
fi
```

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

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

A partir de la versión 2209, los usuarios de las sesiones pueden personalizar sus entornos de escritorio. Para habilitar esta función, debe instalar con antelación en el VDA entornos de escritorio que se puedan cambiar. Para obtener más información, consulte Entornos de escritorio personalizados por usuarios de las sesiones.

- **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
```

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

```
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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
```

Para quitar los cambios de configuración:

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

> **Importante:**
>
> Este script elimina todos los datos de configuración de la base de datos y 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
```

Para ver información más detallada:

```
apt-cache show xendesktopvda
```

Para desinstalar el software de Linux VDA:

```
dpkg -r xendesktopvda
```

> **Nota:**
>
> La desinstalación del software de 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.

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

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
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
```

> **Nota:**
>
> Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando `service ctxmonitorservice stop` para detener el demonio del servicio de 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
```

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
```

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

Paso 11: Cree catálogos de máquinas

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 grupos de entrega

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 2212.

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

Instalar Linux VDA en Debian manualmente

August 20, 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 información de configuración y la máquina Linux

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:

```
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:**

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

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

Paso 1d: Compruebe el nombre de host

Compruebe que el nombre de host está definido correctamente:

```
hostname
```

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

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

```
hostname -f
```

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
```

Para:

```
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
```

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

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

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 (VM) puede causar problemas de reloj sesgado. Por este motivo, se recomienda sincronizar la hora con un servicio remoto de sincronización horaria.

Instale Chrony:

```
apt-get install chrony
```

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
```

Paso 1h: Instale los paquetes

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

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

Paso 1i: Agregue repositorios para instalar las dependencias necesarias

Para Debian 11.3, agregue la línea `deb http://deb.debian.org/debian/ bullseye main` al archivo /etc/apt/sources.list.

Paso 1j: Instale y especifique una base de datos que se utilizará

Como función experimental, puede utilizar SQLite además de PostgreSQL. También puede cambiar entre SQLite y PostgreSQL al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux

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

VDA. Para las instalaciones manuales, debe instalar SQLite y PostgreSQL manualmente antes de poder cambiar entre ellas.

En esta sección se describe cómo instalar las bases de datos PostgreSQL y SQLite y cómo especificar la base de datos que se utilizará.

> **Nota:**
>
> Le recomendamos utilizar SQLite solo para el modo VDI.

Instalar PostgreSQL Ejecute estos comandos para instalar PostgreSQL:

```
sudo apt-get install -y postgresql

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

Ejecute estos comandos para iniciar PostgreSQL al iniciar la máquina o inmediatamente, respectivamente:

```
sudo systemctl enable postgresql

sudo systemctl start postgresql
```

Instalar SQLite Para Debian, ejecute este comando para instalar SQLite:

```
sudo apt-get install -y sqlite3
```

Especificar la base de datos que se utilizará Tras instalar SQLite, PostgreSQL o ambos, puede especificar una base de datos que utilizar al modificar `/etc/xdl/db.conf` después de instalar el paquete de Linux VDA. Para ello, siga estos pasos:

1. Ejecute `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omita este paso si se trata de una instalación nueva.
2. Modifique `/etc/xdl/db.conf` para especificar la base de datos que se utilizará.
3. Ejecute `ctxsetup.sh`.

> **Nota:**
>
> También puede usar **/etc/xdl/db.conf** para configurar el número de puerto de PostgreSQL.

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.

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

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
```

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
```

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
```

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:

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

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, 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 Linux al dominio de Windows

Hay estos métodos disponibles para agregar máquinas Linux al dominio de Active Directory (AD):

- Samba Winbind
- 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.

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

Samba Winbind

Instalar o actualizar los paquetes requeridos

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-
    config krb5-locales krb5-user
```

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
```

> **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**.

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

Configurar la autenticación de Winbind 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: 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:

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

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

Reiniciar Winbind

```
1 sudo systemctl restart winbind
```

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

```
1 sudo pam-auth-update
```

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

> **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
```

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

```
sudo net ads info
```

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

```
sudo klist -ke
```

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
```

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
```

Examine los datos de la cuenta de la máquina:

```
sudo net ads status
```

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
```

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
```

> **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
```

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
```

Salga de la sesión.

```
exit
```

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`.

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

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
```

> **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
```

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.

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

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
```

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

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

El usuario es 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
```

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
```

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
```

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

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

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

Salga de la sesión.

```
exit
```

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
```

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
```

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

Para obtener información de diagnóstico y sistema más completa:

```
adinfo --sysinfo all

adinfo --diag
```

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

```
adinfo --test
```

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.

SSSD

Configurar Kerberos Ejecute el siguiente comando para instalar Kerberos:

```
sudo apt-get install krb5-user
```

Para configurar Kerberos, abra **/etc/krb5.conf** como root y establezca los parámetros:

> **Nota:**
>
> Configure Kerberos en función de su infraestructura de AD. 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.

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 sobre **adcli** y **Samba**.

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

1. Instale **adcli**.

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

```
sudo apt-get install adcli
```

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
```

   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.

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

1. Instale el paquete.

```
sudo apt-get install samba krb5-user
```

2. Configure **Samba**.

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

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

3. Únase al dominio con **Samba**.

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

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

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

Configurar SSSD **Instalar o actualizar los paquetes requeridos:**

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

```
1 sudo apt-get install sssd
```

Si los paquetes ya están instalados, se recomienda actualizarlos:

```
1 sudo apt-get install --only-upgrade sssd
```

> **Nota:**
>
> De forma predeterminada, el proceso de instalación en Ubuntu configura automáticamente **nsswitch.conf** y el módulo de 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
```

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

```
krb5_renewable_lifetime = 14d
# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours
krb5_renew_interval = 1h
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
# This ldap_id_mapping setting is also the default value
ldap_id_mapping = true
override_homedir = /home/%d/%u
default_shell = /bin/bash
ad_gpo_map_remote_interactive = +ctxhdx
```

> **Nota:**
>
> ldap_id_mapping 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:

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
```

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
```

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

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

```
sudo pam-auth-update
```

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 el Linux VDA, compruebe que el archivo del sistema keytab se haya creado y contenga claves válidas:

```
sudo klist -ke
```

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
```

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
```

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

```

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

```
klist

exit
```

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
```

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

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
    /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

Convertir el script de instalación de PBIS en ejecutable

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

Ejecutar el script de instalación de PBIS

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

Unirse al dominio de Windows 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
```

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
```

© 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
```

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
```

Salga de la sesión.

```
exit
```

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

Paso 4: Instale .NET Runtime 6.0

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

1. Vaya a la página de descargas de Citrix Virtual Apps and Desktops.
2. Expanda la versión adecuada de Citrix Virtual Apps and Desktops.
3. Haga clic en **Componentes** para descargar el paquete de Linux VDA que corresponda a su distribución de Linux y la clave pública GPG que puede usar para comprobar la integridad del paquete de Linux VDA.

   Para verificar la integridad del paquete de Linux VDA, importe la clave pública a la base de datos DEB y ejecute estos comandos:

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

```
```
sudo apt-get install dpkg-sig
gpg --import <path to the public key>
dpkg-sig --verify <path to the Linux VDA package>
```
```

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
```

Lista de dependencias para Debian 11.3:

```
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 >= 9.53~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

```

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

```
35 libpython3.9 >= 3.9~
36
37 libsasl2-modules-gssapi-mit >= 2.1.~
38
39 libqt5widgets5 >= 5.5~
40
41 mutter >= 3.38.6~
42
43 libqrencode4 >= 4.0.0
44
45 libimlib2 >= 1.5.1
```

> **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 la versión de una instalación existente desde las dos versiones anteriores y desde una versión LTSR.

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

> **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.

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

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 el 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
```

Configuración con preguntas

Ejecute una configuración manual con preguntas para el usuario:

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

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 VDA se inician después del arranque de la máquina. Se establece en Y de forma predeterminada.

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

- **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 VDA. 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 ad2.miempresa.com:3268 ad3.miempresa.com:3268. Si especifica el número de puerto de LDAP como 389, Linux VDA consulta a cada servidor LDAP del dominio especificado en modo de sondeo. Si hay una cantidad "x"de directivas y una cantidad "y"de servidores LDAP, Linux VDA realiza el total de consultas X multiplicado por Y. Si el tiempo de sondeo supera el umbral, los inicios de sesión pueden fallar. Para habilitar las consultas LDAP más rápidas, habilite **Catálogo global** en un controlador de dominio y especifique 3268 como número de puerto LDAP correspondiente. 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,

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

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. Para comunicarse correctamente con los servidores FAS, añada un número de puerto coherente con el especificado en los servidores FAS, por ejemplo, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **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**

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

```
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.

A partir de la versión 2209, los usuarios de las sesiones pueden personalizar sus entornos de escritorio. Para habilitar esta función, debe instalar con antelación en el VDA entornos de escritorio que se puedan cambiar. Para obtener más información, consulte Entornos de escritorio personalizados por usuarios de las sesiones.

- **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>'
```

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

```

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
```

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
```

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

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
```

Para quitar los cambios de configuración:

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

> **Importante:**
>
> Este script elimina todos los datos de configuración de la base de datos y 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
```

Para ver información más detallada:

```
apt-cache show xendesktopvda
```

Para desinstalar el software de Linux VDA:

```
dpkg -r xendesktopvda
```

> **Nota:**
>
> La desinstalación del software de 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
```

Detener Linux VDA:

Para detener los servicios de Linux VDA:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
```

> **Nota:**
>
> Antes de detener los servicios `ctxvda` y `ctxhdx`, ejecute el comando `service ctxmonitorservice stop` para detener el demonio del servicio de 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
```

Comprobar el estado de Linux VDA:

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

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

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
```

Paso 11: Cree catálogos de máquinas

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 grupos de entrega

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.

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

- 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 2212.

Configurar

March 27, 2023

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

Administración

May 4, 2023

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 máquinas virtuales y sesiones de Linux
- 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

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

- LDAPS
- **Xauthority**

Customer Experience Improvement Program (CEIP) de Citrix

March 27, 2023

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.

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:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

- **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.

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

Puede ejecutar el siguiente comando en un cliente para habilitar el programa GA:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\CEIP" -v "GASwitch" -d "0"
```

- **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:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\CEIP" -v "DataPersistPath" -d "your_path"
```

Si la ruta configurada no existe o no se puede acceder a ella, los datos se guardan en la ruta predeterminada.

Datos 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

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

Punto de datos	Nombre de la clave	Descripción
Método de LVDA instalado	install_method	Cadena de texto que indica que el paquete de Linux VDA se instala mediante MCS, PVS, Easy Install, o instalación manual.
HDX 3D Pro habilitado o no	**hdx_3d_pro**	Cadena de texto que indica si HDX 3D Pro está habilitado en la máquina
Modo VDI habilitado o no	**vdi_mode**	Cadena de texto que indica si el modo VDI está habilitado
Configuración regional del sistema	**system_locale**	Cadena de texto que indica la configuración regional de esta máquina
Último reinicio de los servicios principales de LVDA	**ctxhdx ctxvda**	La fecha y hora a la que se reiniciaron por última vez los servicios `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

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

Punto de datos	Nombre de la clave	Descripción
Tipo de recurso	**resource_type**	Cadena de texto que indica el tipo de sesión iniciada: escritorio o <appname>
Tiempo de sesión activa	**active_session_time**	Se utiliza para guardar los tiempos de sesión activa. Una sesión puede tener varios periodos activos, porque la sesión puede desconectarse o reconectarse.
Duración de sesión	**session_duration_time**	Utilizado para guardar la duración de la sesión desde que se inicia la sesión hasta que se cierra
Tipo de cliente Receiver	**receiver_type**	Número entero que indica el tipo de aplicación Citrix Workspace utilizada para iniciar la sesión
Versión de cliente de Receiver	**receiver_version**	Cadena de texto que indica la versión de la aplicación Citrix Workspace utilizada para lanzar la sesión
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

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

Punto de datos	Nombre de la clave	Descripción
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

HDX Insight

August 20, 2024

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:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"
    --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
    --force
```

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

Solución de problemas

No se muestran los puntos de datos

Puede haber dos motivos:

- HDX Insight no está configurado correctamente.

  Por ejemplo, AppFlow no está habilitado en Citrix ADC o se ha configurado una instancia de Citrix ADC incorrecta en Citrix ADM.

- El canal virtual de control de ICA no se ha iniciado en Linux VDA.

  ```
  ps aux | grep -i ctxctl
  ```

  Si no se está ejecutando `ctxctl`, póngase en contacto con el administrador para notificar un fallo a Citrix.

No se muestran puntos de datos de aplicaciones

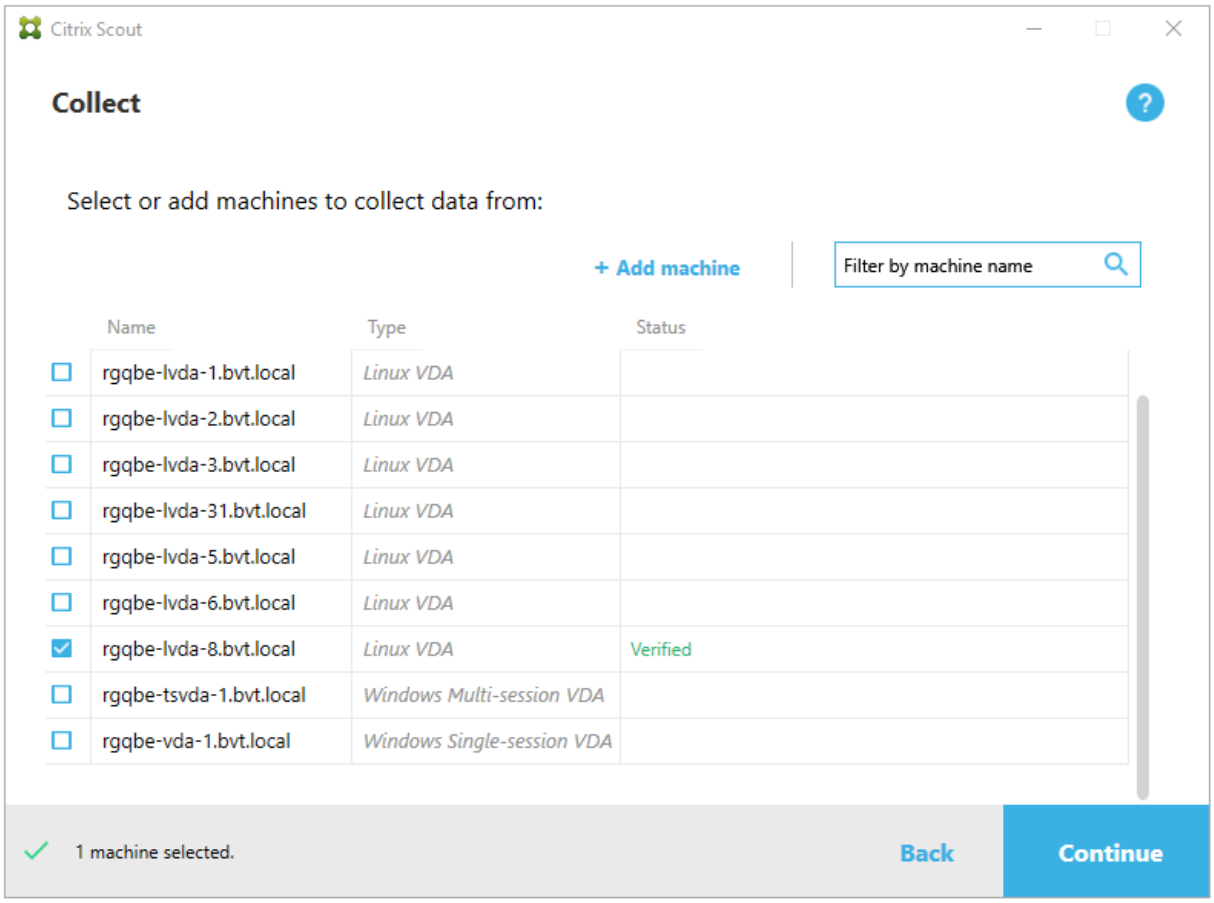
Verifique que el canal virtual integrado esté habilitado y haya una aplicación integrada activa.

Integración en Citrix Telemetry Service

March 27, 2023

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 sobre las variables, consulte Crear VDA unidos a un dominio mediante 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**.

Puertos

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.

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

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.

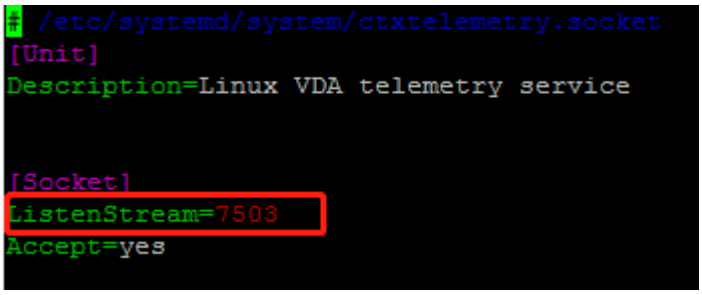
Para cambiar los puertos una vez instalado el VDA, haga lo siguiente:

1. Para cambiar un puerto para comunicarse con Scout, ejecute el siguiente comando.

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
     -t REG_DWORD
```

2. Para cambiar el puerto de socket para escuchar a Scout, ejecute el siguiente comando para abrir y modificar el archivo ctxtelemetry.socket.

```
sudo vi /etc/systemd/system/ctxtelemetry.socket
```



3. Ejecute los siguientes comandos para reiniciar el puerto de socket.

```
sudo systemctl daemon-reload
sudo systemctl stop ctxtelemetry.socket
sudo systemctl start ctxtelemetry.socket
```

4. Habilite los nuevos puertos en la configuración del firewall.

   Si 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.

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

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
```

```
#!/bin/sh

export PATH=/usr/lib/jvm/java-8-openjdk-amd64/jre/bin:/usr/lib/jvm/java-8-openjdk-amd64/bin:${PATH}
# Set this flag to 1 to enter debugging mode
DebugMode=1
# Set this flag to 1 to enter interactive debugging mode
InteractiveDebugMode=0
```

2. Detenga manualmente Citrix Telemetry Service o espere 15 minutos para que el servicio se detenga automáticamente.

```
administrator@RGQBE-LVDA-3:~$ sudo netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1447/smbd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      971/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1309/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      25158/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      998/postgres
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1447/smbd
tcp6       0      0 :::2598                 :::*                    LISTEN      28100/ctxhdx
tcp6       0      0 :::139                  :::*                    LISTEN      1447/smbd
tcp6       0      0 :::7502                 :::*                    LISTEN      1958/java
tcp6       0      0 :::7503                 :::*                    LISTEN      1/init
tcp6       0      0 :::80                   :::*                    LISTEN      1610/java
tcp6       0      0 :::1494                 :::*                    LISTEN      28100/ctxhdx
tcp6       0      0 :::22                   :::*                    LISTEN      1309/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      25158/cupsd
tcp6       0      0 :::445                  :::*                    LISTEN      1447/smbd
administrator@RGQBE-LVDA-3:~$
```

En este ejemplo, puede ejecutar los siguientes comandos para detener Citrix Telemetry Service.

```
sudo netstat -ntlp
Kill -9 1958
```

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
```

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

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.

Autoactualización de Linux VDA a través de Azure

May 30, 2024

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 necesita 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: Cargue la 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:

```
1 {
2
```

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

```
3   "Version": "21.04.200.4",
4  "Distributions":[
5  {
6
7  "TargetOS": "RHEL7_9",
8  "PackageName": "",
9  "PackageHash": ""
10  }
11  ,
12 {
13
14 "TargetOS": "UBUNTU18_04",
15 "PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
16 "PackageHash": "4148
      cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"
17  }
18  ,
19 {
20
21 "TargetOS": "UBUNTU20_04",
22 "PackageName": "",
23 "PackageHash": ""
24  }
25
26 ]
27  }
```

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), “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: Habilite 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 "0x00000001" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
```

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 máquinas virtuales y sesiones de Linux

March 27, 2023

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.

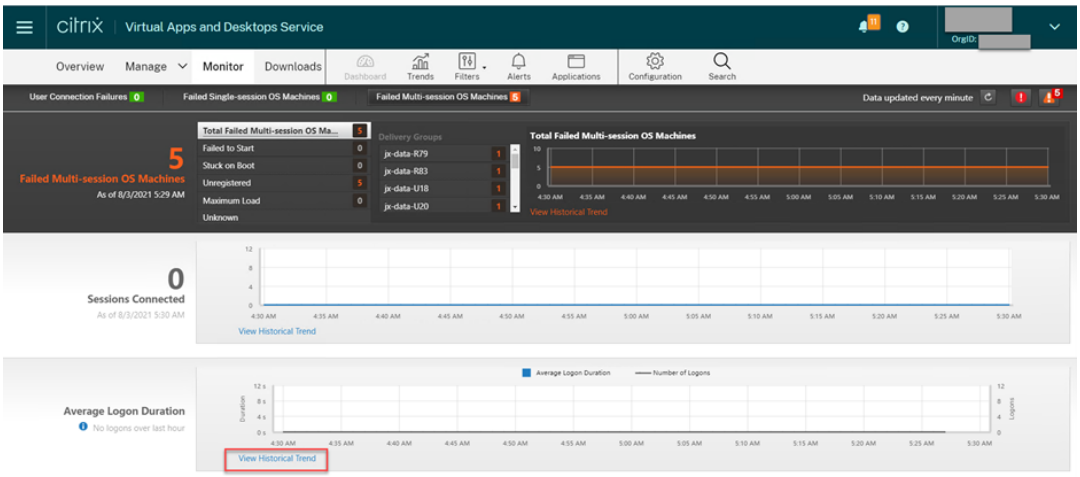
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

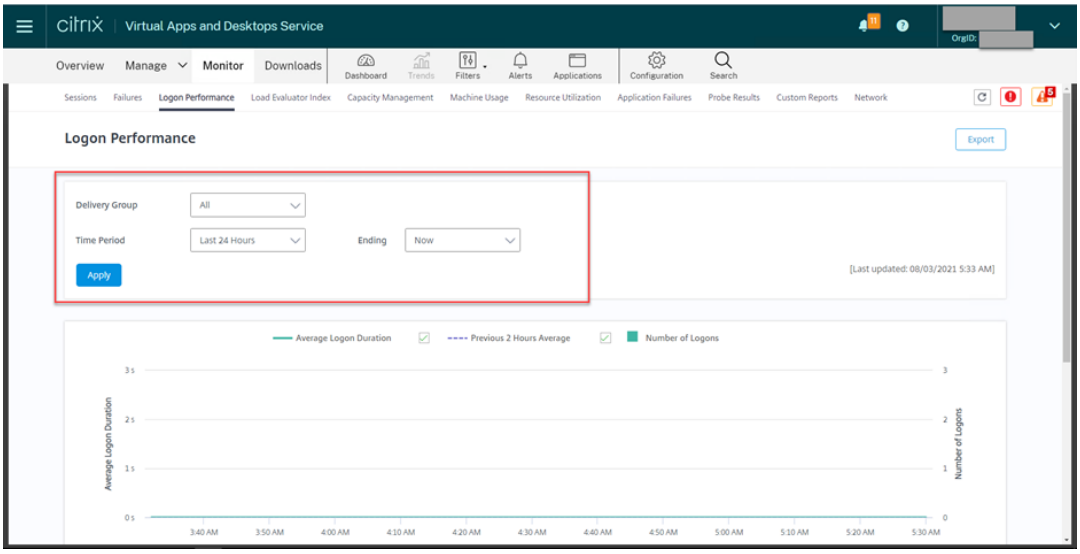
- Duración de inicio de sesión

  1. En la ficha Supervisar de Citrix DaaS, haga clic en **Ver tendencia histórica**, en la sección **Promedio de duración de inicio de sesión**.

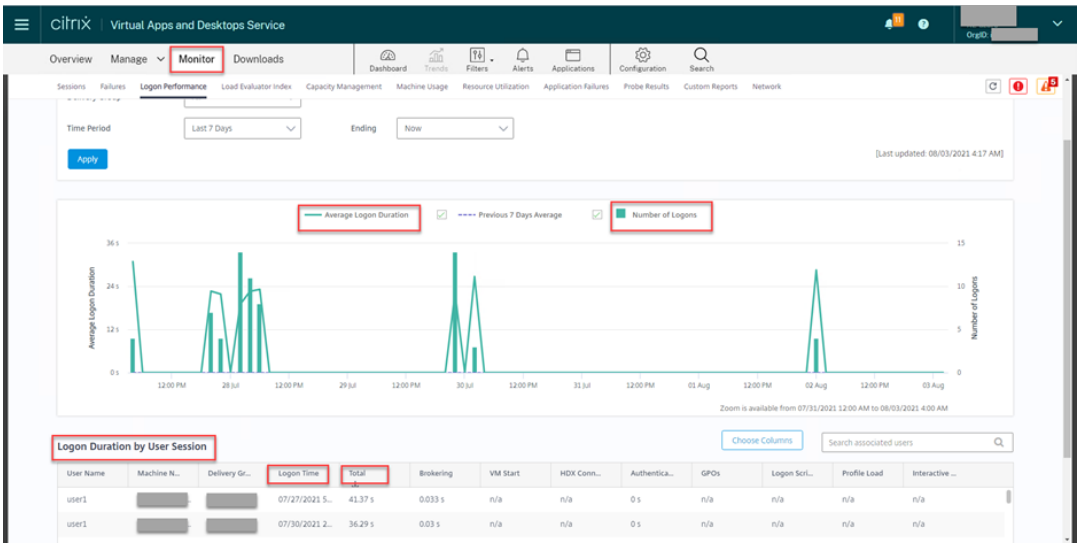


  2. En la página **Rendimiento de inicio de sesión**, establezca las condiciones de filtro.

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



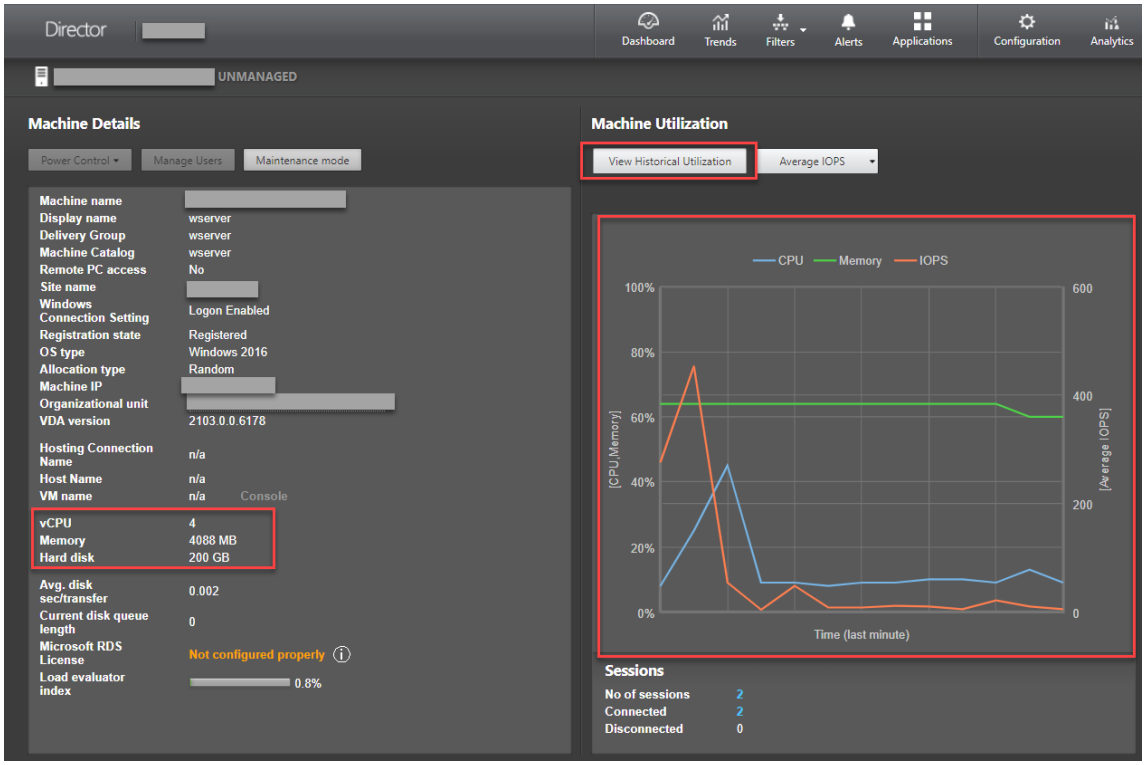
3. Para ver las métricas de duración de los inicios de sesión, haga clic en **Aplicar**.

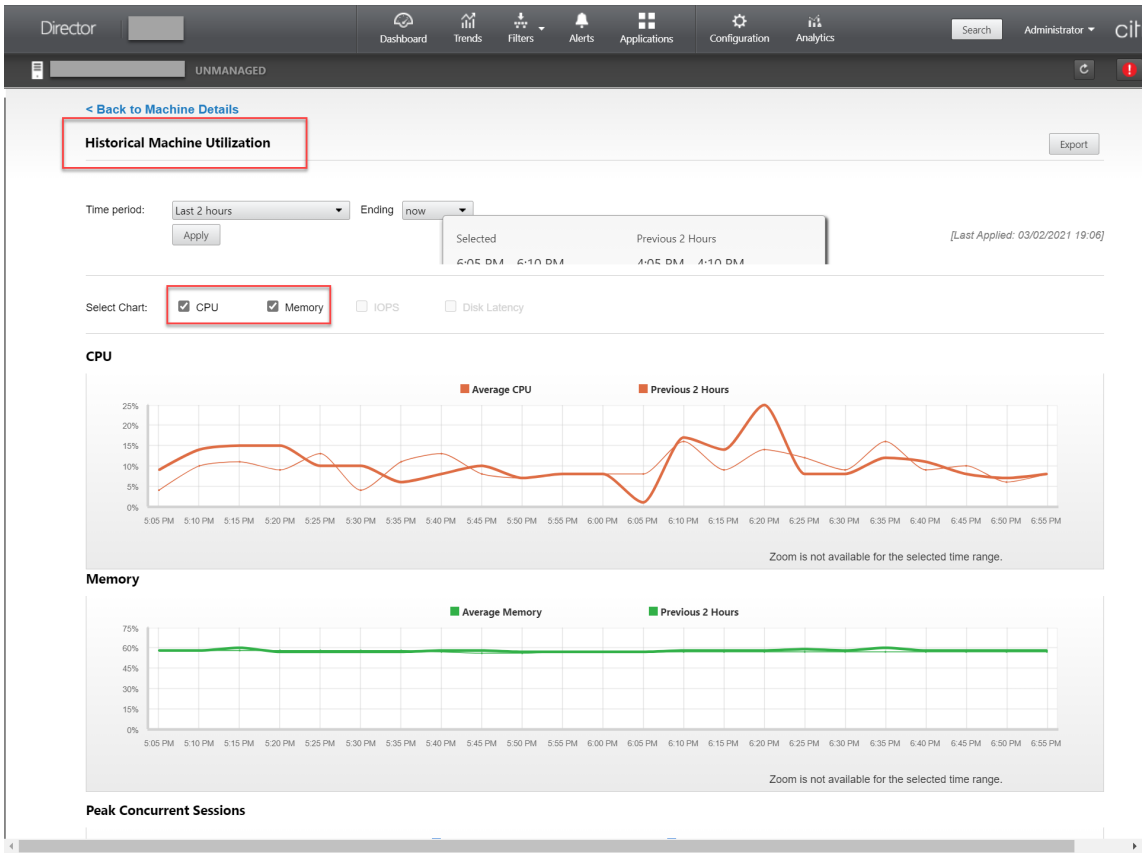


- La cantidad de núcleos de CPU, tamaño de memoria, capacidad de disco duro y utilización actual e histórica de CPU y memoria de una VM Linux

  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.

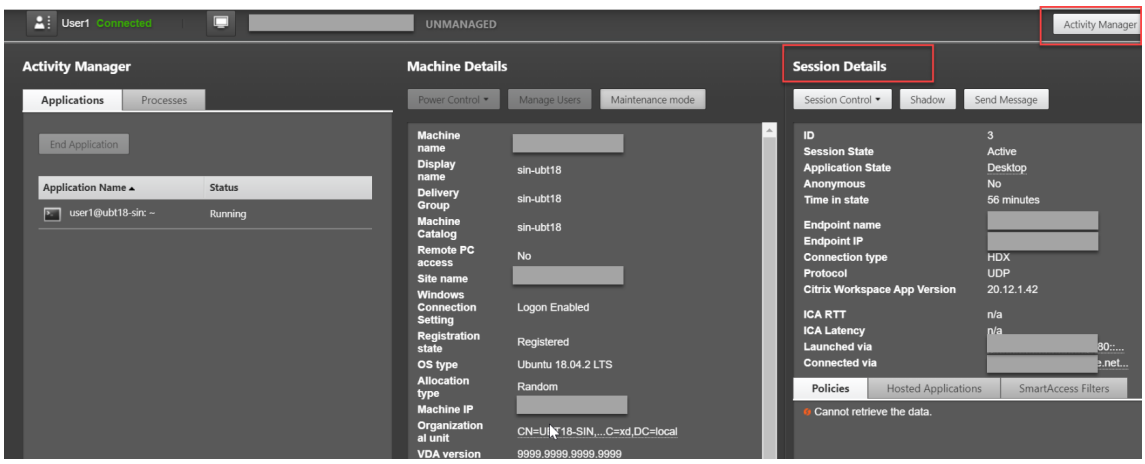




- RTT de ICA, protocolo

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

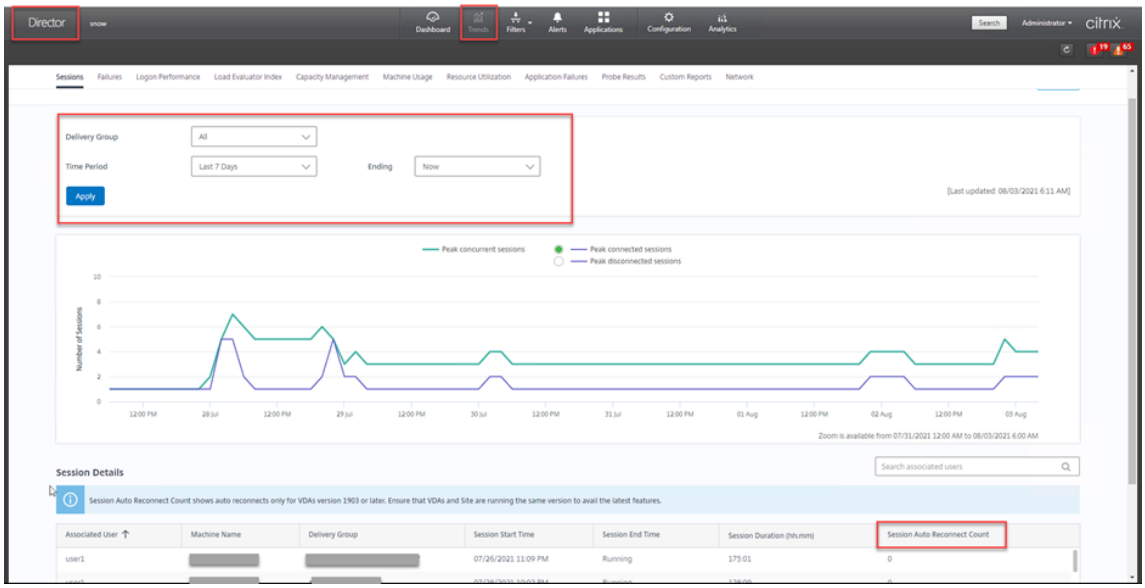
Para ver las métricas de una sesión de Linux, abra la página **Todas las sesiones** seleccionando **Filtros > Sesiones > Todas las sesiones**, o acceda al panel **Detalles de la sesión**. Para acceder al panel **Detalles de la sesión**, abra la página **Todas las Sesiones** y haga clic en una sesión 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.

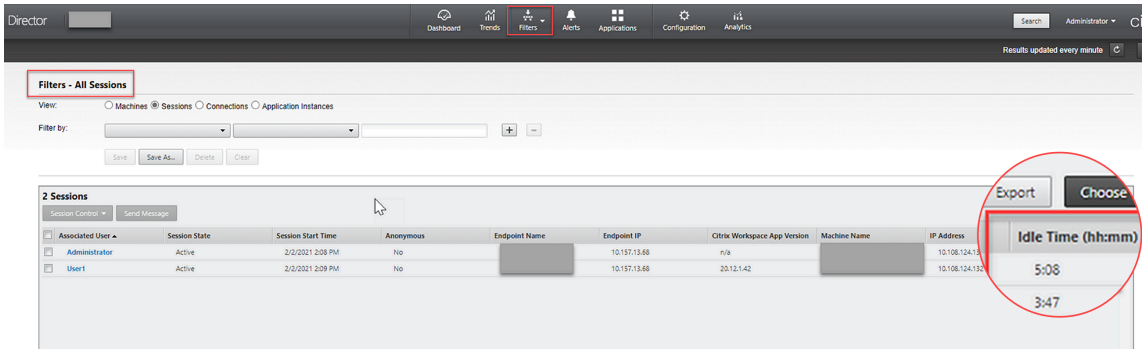
  La columna **Recuento de reconexiones automáticas de sesiones** muestra la cantidad de reconexiones automáticas en una sesión. Por ejemplo:



- Tiempo de inactividad

  Por ejemplo:

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



Recopilación de registros

March 27, 2023

Información general

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`:

```
setlog help
```

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

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
```

Ver o establecer un solo valor de `setlog`:

```
setlog value <name> [<value>]
```

Por ejemplo:

```
setlog value log_size 100
```

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
```

Para configurar los niveles de registro (incluidos Disable, Inherited, Verbose, Information, Warnings, Errors y Fatal Errors), ejecute el siguiente comando:

```
setlog level <class> [<level>]
```

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

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

Nivel de registro	Parámetro de comando (no se distingue entre mayúsculas y minúsculas)
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
```

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
```

Ver las marcas actuales:

```
setlog flags
```

Ver o establecer una sola marca de registro:

```
setlog flag <flag> [<state>]
```

Restaurar valores predeterminados Revertir todos los niveles, las marcas y los valores a los parámetros predeterminados:

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

```
setlog default
```

> **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.
```

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.

Remedo de sesiones

September 23, 2024

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` versión 7.16 o posterior.

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

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
```

(Para RHEL 7.x) Para resolver `python-websockify` y `x11vnc`, habilite los repositorios Extra Packages for Enterprise Linux (EPEL) y RPM opcionales:

- 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
  ```

- 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
  ```

Para RHEL 8.x/9.0 y Rocky Linux 8.x/9.0:

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
```

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"
```

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

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
```

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 zypper install x11vnc
```

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
```

Puerto

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 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)

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

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:

```
/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://`.

Para habilitar SSL, ejecute el comando siguiente:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -v "ShadowingUseSSL" -d "0x00000001"
```

Obtener certificados SSL raíz y de servidor Los certificados deben estar firmados por una entidad de confianza llamada Entidad de certificación (CA).

Se necesita un certificado de servidor (clave incluida) por cada servidor Linux VDA donde quiera configurar SSL. Un certificado de servidor identifica a un equipo concreto, de modo que necesita el nombre de dominio completo (FQDN) de cada servidor. Para mayor comodidad, considere la posibilidad de usar un certificado comodín para todo el 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.

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:

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

- 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.
- Chrome ha dejado de aceptar certificados SSL autofirmados por considerarlos inseguros. El error `NET::ERR_CERT_COMMON_NAME_INVALID` se produce porque el certificado generado carece del campo SAN (subjectAltName). Para resolver este problema, proporcione un certificado con atributos extendidos (extensiones X509 v3) que incluyan el campo SAN.

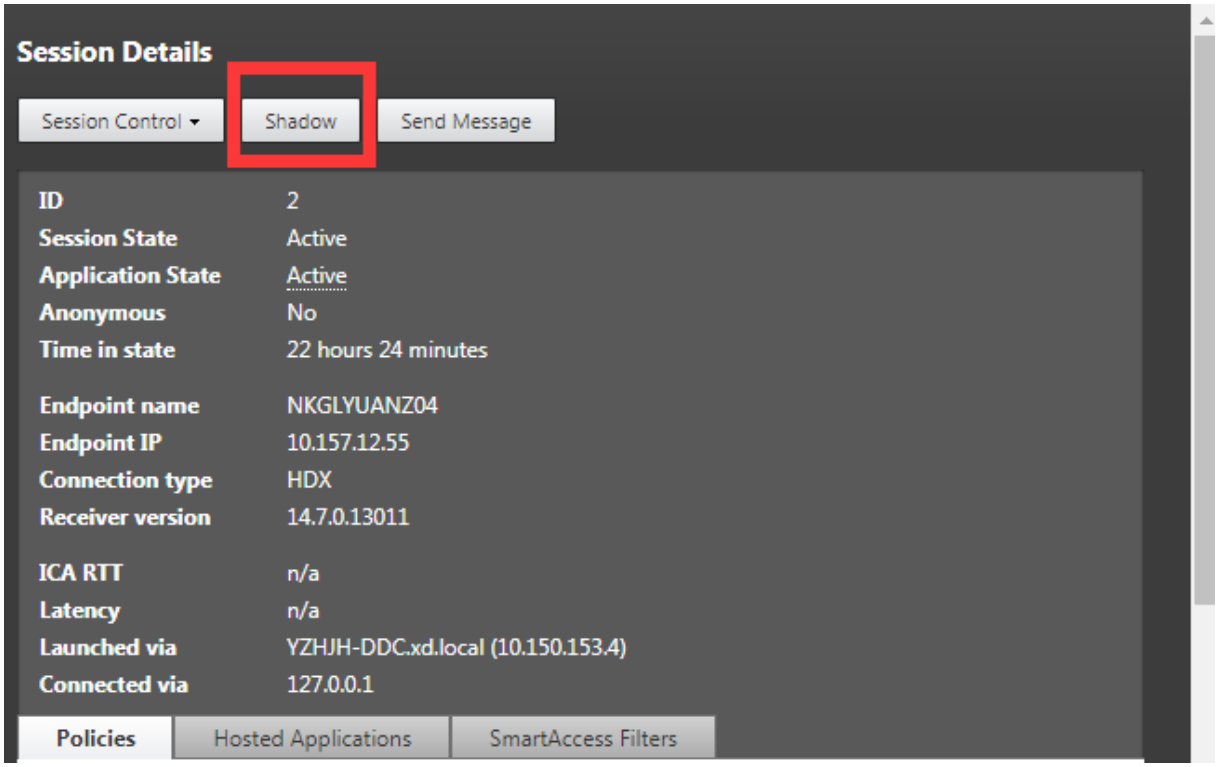
Instalar un certificado raíz en cada cliente de Citrix Director El remedo se sesiones usa el mismo almacén de certificados (basado en el registro del sistema) que IIS, de modo que se puede instalar certificados con IIS o el complemento de certificados de Microsoft Management Console (MMC). Cuando reciba 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`.

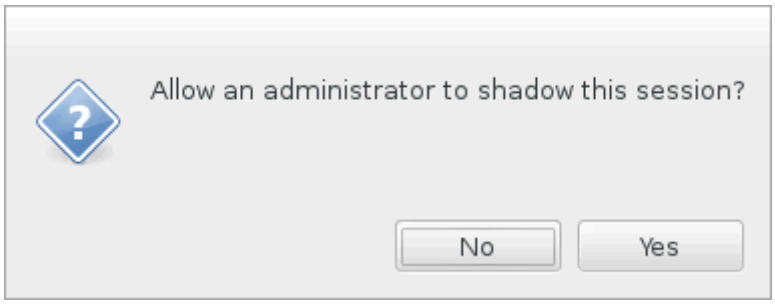
Uso

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

1. Revise el archivo `/var/log/xdl/vda.log` en busca de pistas.
2. Modifique el archivo `/var/xdl/sessionshadowing.sh` y cambie la variable “logFile” para especificar un archivo de registro que pueda rastrearse en busca de pistas durante el seguimiento de la sesión con Director.
3. Además, puede verificar manualmente si sus certificados funcionan correctamente con la conexión noVNC:

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

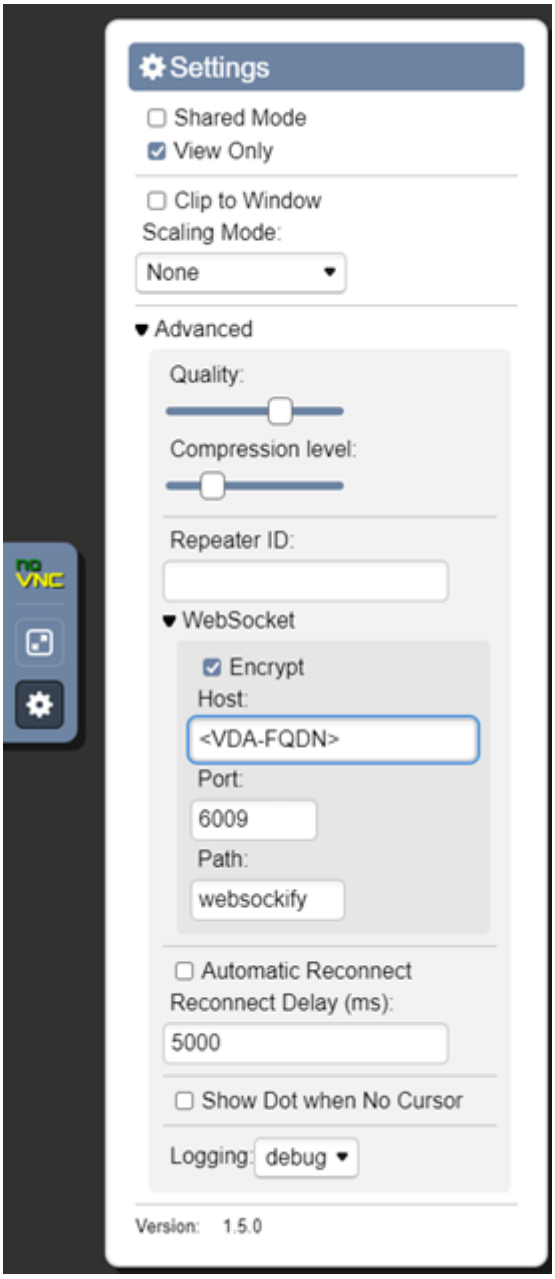
a) Ejecute **ps aux | grep xorg** para buscar el número mostrado de Xorg de la sesión actual <display-num>, por ejemplo, :3.

b) Ejecute el siguiente comando para iniciar un servidor x11vnc y esperar a que se produzca una conexión entrante.

```
1 runuser -l "ctxsrvr" -s /bin/bash -c "websockify <port> -v --
    cert  /etc/xdl/shadowingssl/shadowingcert.pem --key  /etc/
    xdl/shadowingssl/shadowingkey.key -- x11vnc  -viewonly  -
    shared -passwd <passwd> -rfbport <port> -display <display-
    num> -many -o /var/log/xdl/x11vnc.log"
```

c) Intente conectarse mediante noVNC para verificar el modo SSL de la siguiente manera. Introduzca el FQDN y el número de puerto del VDA. En este ejemplo, el número de puerto es 6009.

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



d) Resuelva los errores que Websockify imprima sobre el VDA o que notifique el explorador del cliente.

Puntos de control clave durante el establecimiento de la conexión:

i. Compruebe si hay alguna limitación de firewall que impida que el remedo de sesiones abra el puerto.

ii. 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.

iii. Compruebe que haya suficientes puertos entre 6001 y 6099 para las nuevas solici-

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

tudes de remedo de sesiones.

iv. Compruebe que "netstat" esté instalado porque lo requiere `/var/xdl/sessionshadowing.sh`.

v. Ejecute `openssl x509 -in shadowingcert.pem -text -noout` para verificar que los certificados estén configurados correctamente, prestando especial atención a los campos CN y SAN.

vi. En RHEL 8, es posible que haya un problema en el que `rebind.so` no se pueda encontrar. Para resolver este problema, ejecute el siguiente comando:

```
ln -s /usr/bin/rebind.so /usr/local/bin/rebind.so
```

El demonio del servicio de supervisión

March 27, 2023

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
```

- **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)

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

  - AutoRepair: true/false (“true”de forma predeterminada)
  - MultBalance: false
  - ReportAlarm: false

- **rulesets.conf**

  Este archivo de configuración especifica los servicios que se van a supervisar. Hay cuatro servicios supervisados de forma predeterminada, tal y como se muestra en la siguiente captura de pantalla.

```
MonitorUser: all
MonitorType: 3
ProcessName: ctxhdx
Operation: 4
DBRecord: false

MonitorUser: all
MonitorType: 3
ProcessName: ctxvda
Operation: 4
DBRecord: false

MonitorUser: all
MonitorType: 3
ProcessName: ctxpolicyd
Operation: 4
DBRecord: false

MonitorUser: all
MonitorType: 3
ProcessName: Xorg
Operation: 8
DBRecord: false
```

  Para configurar cada servicio que se deba supervisar, defina los siguientes campos.

  - **MonitorUser**: all
  - **MonitorType**: 3
  - **ProcessName**: <> (el nombre del proceso no se puede dejar vacío y debe coincidir exactamente)
  - **Operación**: 1/2/4/8 (1 = detiene el servicio cuando se detectan excepciones; 2 = finaliza el servicio cuando se detectan excepciones; 4 = reinicia el servicio; 8 = borra los residuos de los procesos Xorg)
  - **DBRecord**: false

- **whitelist.conf**

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

Los servicios especificados en el archivo **rulesets.conf** también deben configurarse en el archivo **whitelist.conf**. La configuración de la lista de permitidos es un filtro secundario por seguridad.

Para configurar la lista de permitidos, incluya solamente los nombres de los procesos (que deben coincidir exactamente) en el archivo **whitelist.conf**. La siguiente captura de pantalla le sirve de ejemplo.

```
ctxcdmd
ctxcdmmount
ctxcdmstat
ctxceip
ctxclipboard
ctxconnect
ctxcredentialctl
ctxctl
ctxcupsd
ctxdisconnect
ctxeuem
ctxfiletransfer
ctxgfx
ctxhdx
ctxism
ctxlogd
ctxlogin
ctxmonitorservice
ctxmrvc
ctxpolicyd
ctxscardsd
ctxvhcid
ctxvda
Xorg
```

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

Herramientas y utilidades

May 4, 2023

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

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.

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

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

- 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
- 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

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

- 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`:

```
sudo /opt/Citrix/VDA/bin/xdping -h
```

Para ejecutar el conjunto completo de pruebas, ejecute `xdping` sin ninguna opción de línea de comandos:

```
sudo /opt/Citrix/VDA/bin/xdping
```

Para comprobar el entorno antes de instalar el paquete Linux VDA, ejecute las pruebas `pre-flight`:

```
sudo /opt/Citrix/VDA/bin/xdping --preflight
```

Para ejecutar solo categorías de prueba específicas, por ejemplo, las pruebas de hora y Kerberos, utilice la opción `-T`:

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
```

Para sondear un Controller de XenDesktop concreto:

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
```

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.

```
sudo xdping -T kerberos

Root User ------------------------------------------------------------------
    User:         root
    EUID:         0
      Verify user is root                                                [Pass]

Kerberos -------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                          [Pass]
      Verify Kerberos version 5                                          [Pass]
    KRB5CCNAME:    [Not set]
                   Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                       [Pass]
      Verify KRB5CCNAME format                                           [Pass]
    Configuration file: /etc/krb5.conf [Exists]


  Verify Kerberos configuration file found                              [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                                      [Pass]
  Verify default realm set                                              [Pass]
  Verify default realm in upper-case                                    [Pass]
  Verify default realm not EXAMPLE.COM                                  [Pass]
  Verify default realm domain mappings                                  [Pass]
  Verify default realm master KDC configured                            [Pass]
  Verify Kerberos weak crypto disabled                                  [Pass]
  Verify Kerberos clock skew setting                                    [Pass]
Default ccache: [Not set]
                Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                            [Pass]
  Verify default credential cache format                                [Pass]
UPN system key [MYVDA1$@[redacted]]: [MISSING]
SPN system key [host/[redacted]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.
```

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

```
        Verify Kerberos system keys for SPN exist                        [Pass]
      Kerberos login: [FAILED AUTHENTICATION]
                      Keytab contains no suitable keys for MYVDA1$@[redacted]
                      while getting initial credentials
        Verify KDC authentication                                       [ERROR]
        Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
        from the KDC authentication service for the machine account UPN
        MYVDA1$@[redacted]. Check that the Kerberos configuration is
        valid and the keys in the system keytab are current.


Summary ----------------------------------------------------------------------
  The following tests did not pass:
      Verify Kerberos system keys for UPN exist                         [ERROR]
      Verify KDC authentication                                         [ERROR]
```

Otros

May 4, 2023

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

March 27, 2023

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.

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

Habilite esta función

Esta función está inhabilitada de forma predeterminada. Para habilitarla, haga lo siguiente:

1. En Citrix StoreFront, habilite la aplicación Citrix Workspace para HTML5.

   Para ver información detallada sobre el procedimiento, consulte el Paso 1 del artículo CTX208163 de Knowledge Center.

2. Habilite las conexiones de WebSocket.

   a) En Citrix Studio, establezca la directiva **Conexiones de WebSockets** en **Permitida**.

      También puede configurar las otras directivas de WebSocket. Para obtener una lista completa de las directivas de WebSocket, consulte Configuraciones de directivas de WebSockets.

   b) En el VDA, reinicie el servicio `ctxvda` y el servicio `ctxhdx`, en este orden, para que el parámetro surta efecto.

   c) En el VDA, ejecute el siguiente comando para comprobar si la escucha de WebSocket sigue ejecutándose.

      ```
      netstat -an | grep 8008
      ```

      Cuando se está ejecutando la escucha de WebSocket, el resultado del comando se parece a lo siguiente:

      ```
      tcp 0 0 :::8008 :::* LISTEN
      ```

   Nota: También puede habilitar el cifrado TLS para proteger las conexiones WebSocket. Para obtener información sobre cómo habilitar el cifrado TLS, consulte Proteger sesiones de usuario con TLS.

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.

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

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 Amazon Linux 2:

   ```
   yum -y install python3 python3-devel krb5-devel gcc
   ```

   Para RHEL y Rocky Linux:

   ```
   yum -y install python3-devel krb5-devel gcc
   ```

   > **Nota:**
   >
   > Es posible que tenga que habilitar un repositorio en particular para instalar algunas dependencias. Para RHEL 7, ejecute el comando `subscription-manager repos --enable rhel-7-server-optional-rpms`. Para RHEL 8, ejecute el comando `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms`.

   Para Debian, Ubuntu:

   ```
   apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
   ```

   Para SUSE:

   ```
   zypper -n install lsb-release python3-devel python3-setuptools krb5-devel gcc libffi-devel libopenssl-devel
   ```

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]`

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

```
trusted-host =
pypi.org
files.pythonhosted.org
```

Para Amazon Linux 2, Debian, RHEL, Rocky Linux y Ubuntu:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

Para SUSE:

```
sudo ln -s /usr/lib/mit/bin/krb5-config /usr/bin/krb5-config

export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin

sudo mkdir -p /usr/lib/mit/include/gssapi/

sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/
    gssapi/gssapi_ext.h

sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

3. Instale las dependencias de LDAPS.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
    upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
    cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi
    ==1.7.3 ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
```

4. Instale las dependencias de **XDPing**.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
    upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
    asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator
    ==5.1.1 gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging
    ==21.3 pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser
    ==2.21 pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor
    ==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /
    opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Integrar NIS en Active Directory

March 27, 2023

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

En este tema, se describe cómo integrar NIS con Windows Active Directory (AD) en Linux VDA mediante SSSD. Linux VDA se considera un componente de Citrix Virtual Apps and Desktops. Por eso, encaja bien en el entorno de Active Directory (AD) de Windows.

Para usar NIS, 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 de RHEL/CentOS, siga las instrucciones de Instalar Linux VDA en Amazon Linux 2, CentOS, RHEL y Rocky Linux manualmente. Para una distribución de Ubuntu, siga las instrucciones de Instalar Linux VDA en Ubuntu manualmente.

¿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
```

Establezca el dominio NIS:

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
```

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

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

```
{ 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
```

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
```

Compruebe que la configuración de NIS es correcta:

```
ypwhich
```

Valide que la información de la cuenta esté disponible desde el servidor NIS:

```
getent passwd nisaccount
```

> **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.

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:

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

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
```

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
```

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):

```
[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>[^@\\]+)$))
```

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

```
10 id_provider = proxy
11 proxy_lib_name = nis
12 auth_provider = ad
13 access_provider = ad
14
15 # Should be specified as the long version of the Active Directory
      domain.
16 ad_domain = EXAMPLE.COM
17
18 # Kerberos settings
19 krb5_ccachedir = /tmp
20 krb5_ccname_template = FILE:%d/krb5cc_%U
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
      side
26 default_shell = /bin/bash
27 fallback_homedir = /home/%d/%u
28
29 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
       available
30 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

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 de inicio sea compatible con SELinux:

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
```

> **Sugerencia:**
>
> Al configurar Linux VDA, tenga en cuenta que, para SSSD, no hay ninguna configuración espe-

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

> cial 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 haya creado y contenga claves válidas**:

```
sudo klist -ke
```

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
```

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
```

Paso 6: 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
```

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.

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

```
sudo ssh localhost – l DOMAIN\username

id -u
```

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 }
```

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

```
klist
```

IPv6

March 27, 2023

Linux VDA admite IPv6 para equipararse con Citrix Virtual Apps and Desktops. Cuando use esta función, tenga en cuenta lo siguiente:

- Para entornos de doble pila, se usa IPv4 a menos que se habilite IPv6 de forma explícita.
- Si se habilita IPv6 en un entorno de IPv4, el Linux VDA no funciona.

> **Importante:**
>
> - Todo el entorno de red debe ser IPv6, no solo el entorno para Linux VDA.
> - Centrify no admite el uso de IPv6 puro.

No se requieren tareas de configuración especiales para IPv6 cuando se instala Linux VDA.

Configurar IPv6 para Linux VDA

Antes de cambiar la configuración para Linux VDA, asegúrese de que la máquina virtual Linux ya funcionó anteriormente en una red IPv6. Hay dos claves del Registro relacionadas con la configuración IPv6:

```
" HKLM\Software\Policies\Citrix\VirtualDesktopAgent " -t " REG_DWORD "
    -v " OnlyUseIPv6ControllerRegistration "
" HKLM\Software\Policies\Citrix\VirtualDesktopAgent " -t " REG_DWORD "
    -v " ControllerRegistrationIPv6Netmask "
```

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

OnlyUseIPv6ControllerRegistration debe establecerse en 1 para que Linux VDA pueda usar IPv6:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
    OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
```

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:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "
    ControllerRegistrationIPv6Netmask " -d "{
 IPv6 netmask }
 " --force
```

Sustituya **{IPv6 netmask}** por la máscara de red real (por ejemplo, 2000::/64).

Para obtener más información sobre 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.

LDAPS

April 18, 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

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

- 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.
>
> ```
> /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "REG_DWORD" -d "0x0000000f" --force
> ```

Habilitar LDAPS en el servidor AD/LDAP

Puede habilitar el protocolo LDAP a través de SSL (LDAPS) instalando un certificado con el formato adecuado desde una entidad de certificación (CA) de Microsoft o una entidad de certificación (CA) de otro proveedor distinto de Microsoft.

> **Sugerencia:**
>
> 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.

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

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
```

- Habilite LDAP por SSL/TLS con vinculación de canales:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
```

> **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 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
```

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

```

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

```
9 HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
```

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.

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
```

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

Centrify

Centrify no admite LDAPS en el puerto 636. No obstante, sí que ofrece cifrado seguro en el puerto 389. Para obtener más información, visite el sitio de Centrify.

Quest

Quest Authentication Service no admite LDAPS en el puerto 636, pero proporciona cifrado seguro en el puerto 389 mediante un método diferente.

Solución de problemas

Pueden producirse los siguientes problemas cuando se usa esta función:

- **Disponibilidad del servicio LDAPS**

  Compruebe que la conexión de LDAPS está disponible en el servidor AD/LDAP. El puerto está en 636 de forma predeterminada.

- **El registro de Linux VDA falla cuando LDAPS está habilitado**

  Verifique si el servidor LDAP y el puerto o los puertos están configurados correctamente. Compruebe primero el certificado de CA raíz y asegúrese de que coincide con el servidor de AD/LDAP.

- **Registro incorrecto cambiado por accidente**

  Si 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**

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

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

March 27, 2023

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

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

Puede examinar este archivo mediante el comando `xauth`. Por ejemplo:

```
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1
     fb228d1b695729242616c5908f11624b
```

Si **XClient** se conecta de forma remota a Xorg, deben cumplirse dos requisitos previos:

- Definir la variable de entorno **DISPLAY** con el valor del XServer remoto.
- Obtener el archivo `.Xauthority` que contiene uno de los números de cookie en Xorg.

Configurar Xauthority

Para habilitar **Xauthority** en Linux VDA para la pantalla X11 remota, deben crearse dos claves de Registro:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
    XauthEnabled" -d "0x00000001" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
     -d "0x00000001" --force
```

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 }
  ```

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

> **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.

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
   ```

   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
   ```

   Muestre las cookies mediante el comando **Xauth**:

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   ```

2. Utilice el comando `Xauth` para mostrar las cookies contenidas en `~/.Xauthority`. Para el mismo número de pantalla, las cookies 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
   ```

   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.

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

Autenticación

March 27, 2023

Esta sección contiene estos temas:

- Autenticación con Azure Active Directory
- Autenticación Single Sign-On de doble salto
- Servicio de autenticación federada
- Autenticación sin SSO
- Tarjetas inteligentes
- Sesiones sin autenticar de usuarios anónimos

Autenticación con Azure Active Directory

March 27, 2023

> **Nota:**
>
> Esta función solo está disponible para los VDA alojados en Azure.

Según sus necesidades, puede implementar dos tipos de Linux VDA en Azure:

- Máquinas virtuales unidas a Azure AD DS. Las máquinas virtuales se unen a un dominio administrado de Azure Active Directory (AAD) Domain Services (DS). Los usuarios usan sus credenciales de dominio para iniciar sesión en las máquinas virtuales.
- Máquinas virtuales no unidas a ningún dominio. Las máquinas virtuales se integran con el servicio de identidad de AAD para proporcionar autenticación de usuario. Los usuarios usan sus credenciales de AAD para iniciar sesión en las máquinas virtuales.

Para obtener más información sobre AAD DS y AAD, consulte este artículo de Microsoft.

En este artículo se muestra cómo habilitar y configurar el servicio de identidad de AAD en los VDA no unidos a un dominio.

Distribuciones compatibles

- Ubuntu 22.04, 20.04, 18.04

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

- RHEL 8.7, 8.6, 8.4, 7.9
- SUSE 15.4

Para obtener más información, consulte este artículo de Microsoft.

Problemas conocidos y soluciones

En RHEL 7.9, el módulo de autenticación conectable (PAM) `pam_loginuid.so` no establece `loginuid` después de la autenticación de usuario en AAD. Este problema impide a los usuarios de AAD acceder a las sesiones de VDA.

Para solucionar este problema, en `/etc/pam.d/remote`, comente la línea `Session required pam_loginuid.so`. Consulte la siguiente captura de pantalla para ver un ejemplo.

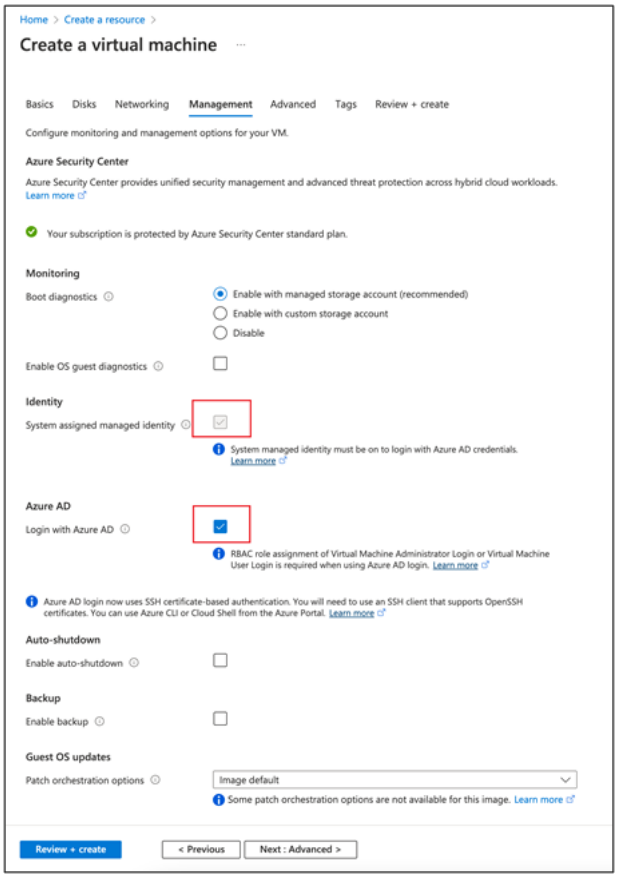
```
#%PAM-1.0
auth       substack     password-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
#session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
```

Paso 1: Cree una VM de plantilla en Azure Portal

Cree una VM de plantilla e instale la CLI de Azure en la VM.

1. En Azure Portal, cree una VM de plantilla. Seleccione **Login with Azure AD** en la ficha **Management** antes de hacer clic en **Review + create**.

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



2. Instale la CLI de Azure en la máquina virtual de plantilla.
   Para obtener más información, consulte este artículo de Microsoft.

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

Para preparar una imagen maestra, siga el **Paso 3: Prepare una imagen maestra** en Crear Linux VDA con Machine Creation Services (MCS).

Paso 3: Configure la VM de plantilla en modo no unido a un dominio

Después de crear una imagen maestra, siga estos pasos para establecer la máquina virtual en modo no unido a un dominio:

1. Ejecute el siguiente script desde el símbolo del sistema.

```
Modify /var/xdl/mcs/mcs_util.sh
```

2. Busque `function read_non_domain_joined_info()` y, a continuación, cambie el valor de `NonDomainJoined` a 2. Consulte el siguiente bloque de código para ver un ejemplo.

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

```
function read_non_domain_joined_info()
{

log "Debug: Enter read_non_domain_joined_info"
# check if websocket enabled
TrustIdentity=`cat ${
 id_disk_mnt_point }
 ${
 ad_info_file_path }
  | grep '[TrustIdentity]' | sed 's/\s//g'`
if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
NonDomainJoined=2
fi
...
 }
```

3. Guarde el cambio.
4. Apague la VM de plantilla.

Paso 4: Cree las máquinas virtuales Linux a partir de la VM de plantilla

Cuando tenga lista la VM de plantilla no unida a un dominio, siga estos pasos para crear máquinas virtuales:

1. Inicie sesión en Citrix Cloud.
2. Haga doble clic en Citrix DaaS y, a continuación, acceda a la consola de administración Configuración completa
3. En **Catálogos de máquinas**, elija usar Machine Creation Services para crear las máquinas virtuales Linux a partir de la VM de plantilla. Para obtener más información, consulte VDA no unidos a ningún dominio en la documentación de Citrix DaaS.

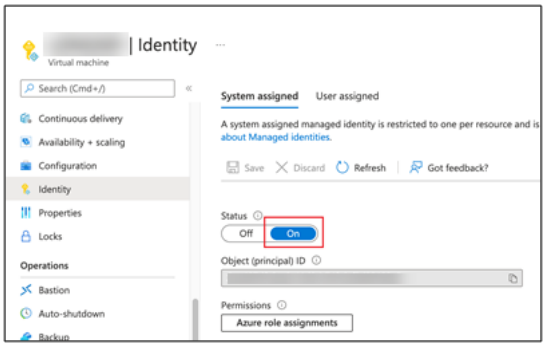
Paso 5: Asigne cuentas de usuario de AAD a las VM Linux

Después de crear las máquinas virtuales no unidas a ningún dominio, asígneles cuentas de usuario de AAD.

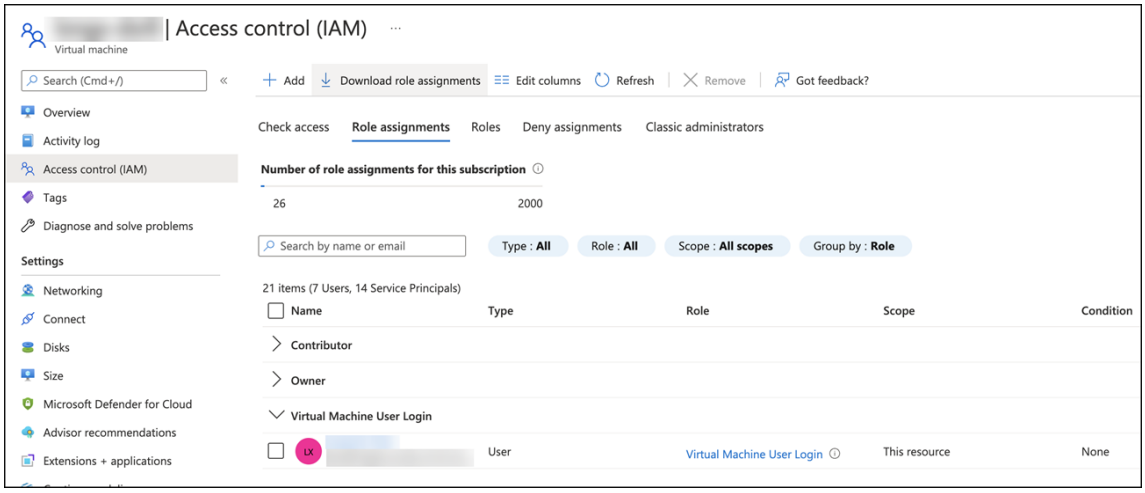
Para asignar cuentas de usuario de AAD a una VM, siga estos pasos:

1. Acceda a la VM con una cuenta de administrador.
2. En la ficha **Identify > System assigned**, habilite **System Identity**.

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



3. En la ficha **Access control (IAM) > Role assignments**, busque el área **Virtual Machine User Login** y, a continuación, agregue las cuentas de usuario de AAD según sea necesario.



Iniciar sesión en VDA no unidos a ningún dominio

Los usuarios finales de su organización pueden iniciar sesión en un VDA que no esté unido a ningún dominio de dos maneras. Estos son los pasos detallados:

1. Inicie la aplicación Workspace y, a continuación, inicie sesión en el espacio de trabajo introduciendo el nombre de usuario y la contraseña de AAD. Aparecerá la página del espacio de trabajo.

2. Haga doble clic en un escritorio no unido a un dominio. Aparecerá la página de INICIO DE SESIÓN de AAD.

   La página varía en función del modo de inicio de sesión establecido en el VDA: código de dispositivo o cuenta/contraseña de AAD. De forma predeterminada, los agentes Linux VDA autentican a los usuarios de AAD mediante el modo de inicio de sesión con código de dispositivo, como se indica a continuación. Como administrador, puede cambiar el modo de inicio de sesión a cuenta/contraseña de AAD si es necesario. Consulte la siguiente sección para conocer los pasos detallados.

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

3. Según las instrucciones que aparecen en pantalla, inicie sesión en el escritorio de una de las siguientes maneras:

   - Escanee el código QR e introduzca el código.
   - Introduzca el nombre de usuario y la contraseña de AAD.

Cambiar al modo de inicio de sesión con cuenta/contraseña de AAD

De forma predeterminada, los agentes Linux VDA autentican a los usuarios de AAD con códigos de dispositivo. Para obtener más información, consulte este artículo de Microsoft. Para cambiar el modo de inicio de sesión a *cuenta/contraseña de AAD*, siga estos pasos:

Ejecute el siguiente comando en el VDA, busque la clave `AADAcctPwdAuthEnable` y cambie su valor a `0x00000001`.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
    Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
    AADAcctPwdAuthEnable" -d "0x00000001" --force
```

> **Nota:**
>
> Este enfoque no funciona con cuentas de Microsoft ni con cuentas que tienen habilitada la autenticación de dos factores.

Autenticación Single Sign-On de doble salto

March 27, 2023

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.

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

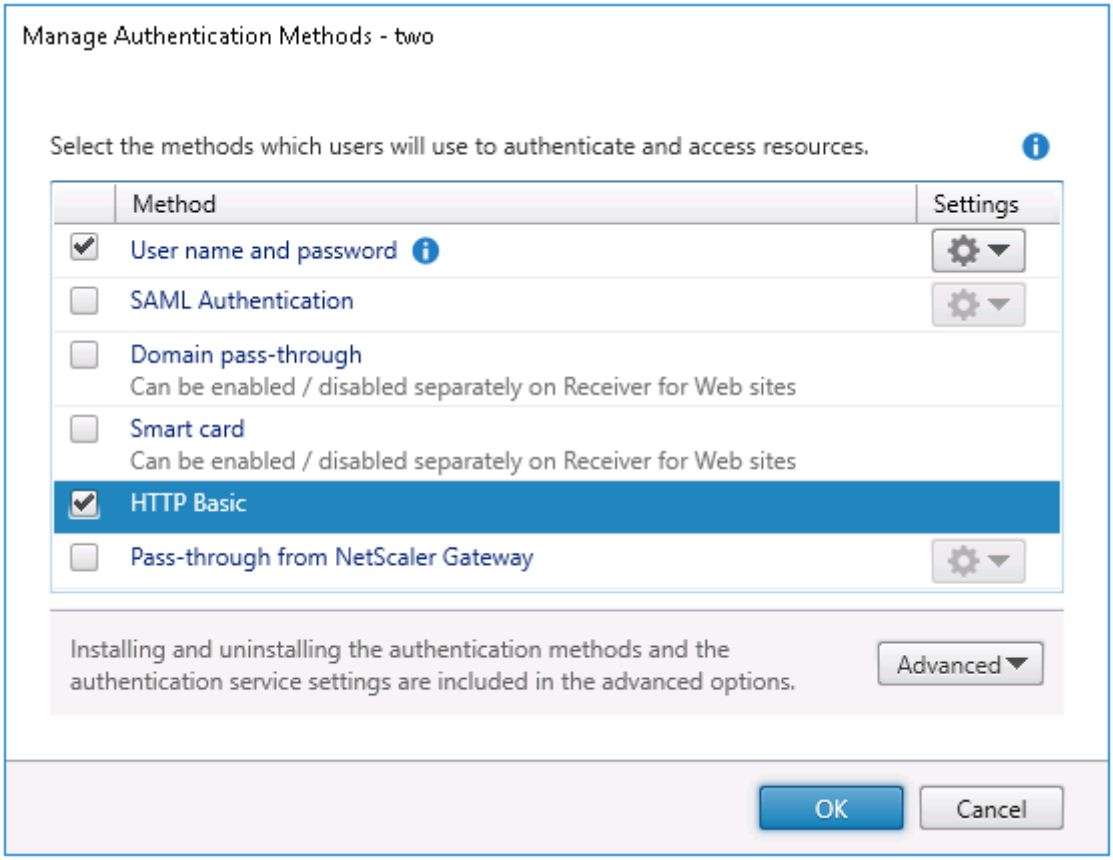
Para habilitar la funcionalidad:

1. En el Linux VDA, instale la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10.

   Descargue la aplicación Citrix Workspace o Citrix Receiver desde la página de descargas de Citrix.

   La ruta de instalación predeterminada es /opt/Citrix /ICAClient/. Si instala la aplicación en una ruta diferente, configure la variable de entorno ICAROOT para que apunte a la ruta de instalación correcta.

2. En la consola de administración de Citrix StoreFront, agregue el método de autenticación **HTTP básica** para el almacén de destino.



3. Agregue la siguiente clave al archivo de configuración de AuthManager ($ICAROOT/config/AuthManConfig.xml) para permitir la autenticación HTTP básica:

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
```

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

4. Ejecute los siguientes comandos para instalar el certificado raíz en el directorio especificado.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/
$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
```

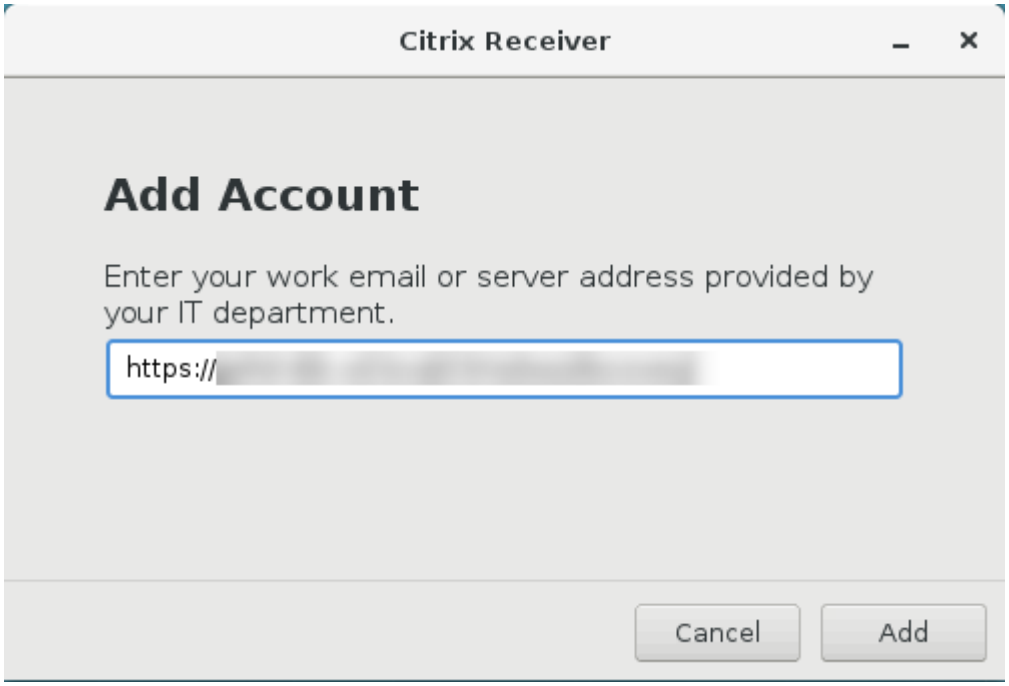
5. Ejecute el siguiente comando para habilitar la función:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
    x00000001"
```

6. Inicie una sesión de Linux Virtual Desktop y, a continuación, inicie la aplicación Citrix Workspace para Linux o Citrix Receiver para Linux 13.10 dentro de esa sesión.

   Se le pedirá una cuenta de almacén 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

February 12, 2024

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

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.
> - A partir de la versión 2206, puede personalizar el puerto de FAS en el lado de Linux VDA mediante CTX_XDL_FAS_LIST, en ctxsetup.sh. Para obtener más información, consulte el artículo sobre la instalación de Linux VDA correspondiente a su distribución.

Configurar FAS en Linux VDA

Compatibilidad de FAS con RHEL 8.x y Rocky Linux 8.x

FAS depende del módulo pam_krb5, que se retiró en RHEL 8.x y Rocky Linux 8.x. Estos pasos son necesarios si quiere utilizar FAS en máquinas con RHEL 8.x y Rocky Linux 8.x que se entregan en modo de SO multisesión. Para FAS en máquinas con RHEL 8.x y Rocky Linux 8.x entregadas en modo de SO de sesión única (VDI), puede omitir estos pasos.

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. Compile e instale el módulo pam_krb5 en RHEL 8.x y Rocky Linux 8.x.

```
yum install make gcc krb5-devel pam-devel autoconf libtool
rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
tar xvzf pam_krb5-2.4.8.tar.gz
cd pam_krb5-2.4.8
./configure --prefix=/usr
make
make install
```

3. Compruebe que pam_krb5.so existe en /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
```

Configurar servidores de 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

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

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
```

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
```

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
```

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/
```

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

> **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
```

Se agregan variables de entorno para que `ctxfascfg.sh` pueda ejecutarse en modo silencioso:

- **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. Si tiene varios Delivery Controllers, agregue los nombres de host de todos los KDC del dominio a pkinit_kdc_hostname en el archivo **/etc/krb5.conf**. Para obtener más información, consulte el artículo CTX322129 de Knowledge Center.

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.

Inhabilitar FAS

Para inhabilitar FAS en Linux VDA, quite todos los servidores de FAS de ConfDB con estos comandos:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
    " -v "Addresses" -d "" --force

service ctxjproxy restart

```

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

```
5 service ctxvda restart
```

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
Debian 11.3	Sí	Sí	Sí	Sí
RHEL 9.0	Sí	Sí	No	No
RHEL 8.7/8.6/8.4	Sí	Sí	Sí	Sí
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí	Sí
Rocky Linux 9.0	Sí	Sí	No	No
Rocky Linux 8.7/8.6	Sí	Sí	No	No
SUSE 15.4	Sí	Sí	Sí	No
Ubuntu 22.04/20.04/18.04	Sí	Sí	Sí	Sí

- FAS aún no admite la pantalla de bloqueo. Si hace clic en el botón de bloqueo en una sesión, no podrá volver a iniciar la sesión mediante FAS.
- Esta versión admite solamente las implementaciones más frecuentes del servicio FAS, que se resumen en el artículo Introducción arquitectural al Servicio de autenticación federada, y no incluye **Unión a Azure AD de Windows 10**.

Solución de problemas

Antes de solucionar problemas en FAS, compruebe que Linux VDA esté instalado y configurado correctamente 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 la habilitación del registro de seguimiento para Linux VDA, consulte el artículo CTX220130 de Knowledge Center.

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

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
```

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"
```

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.

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

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

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode: output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate: cache certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: get_logon_certificate: exit, 0

2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user: pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
```

Solución 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

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

será parecida a esta:

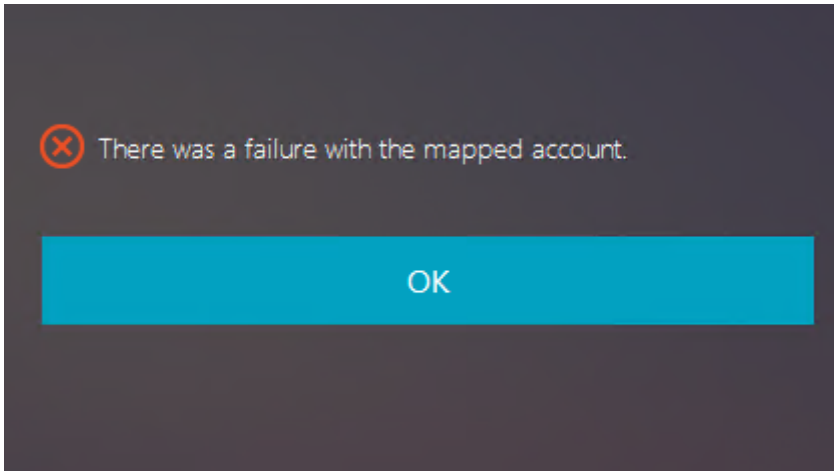
```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

 }
```

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.



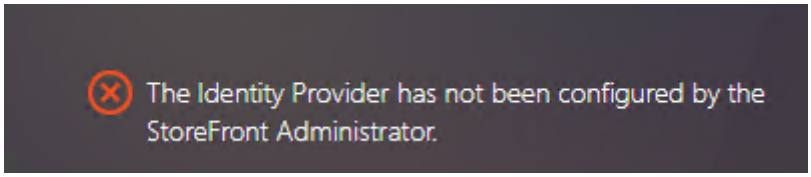
Este error indica que el usuario de ADFS se ha verificado correctamente, pero no hay ningún usuario sombra configurado en AD.

Solución Establezca la cuenta sombra en AD.

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

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.

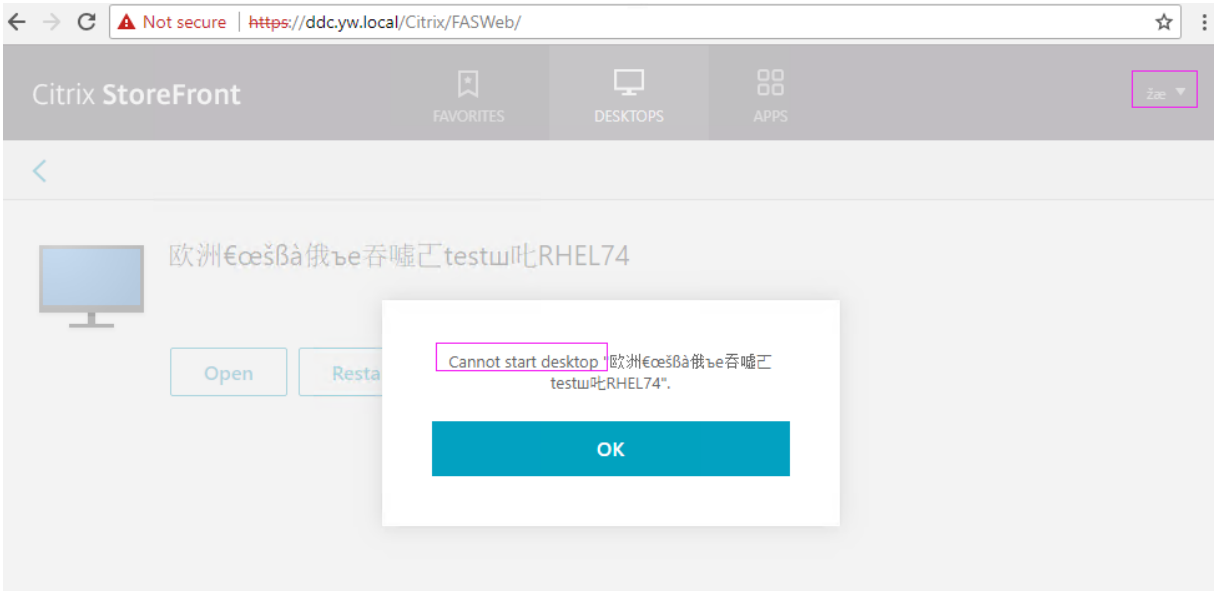
Información relacionada

- 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.

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.

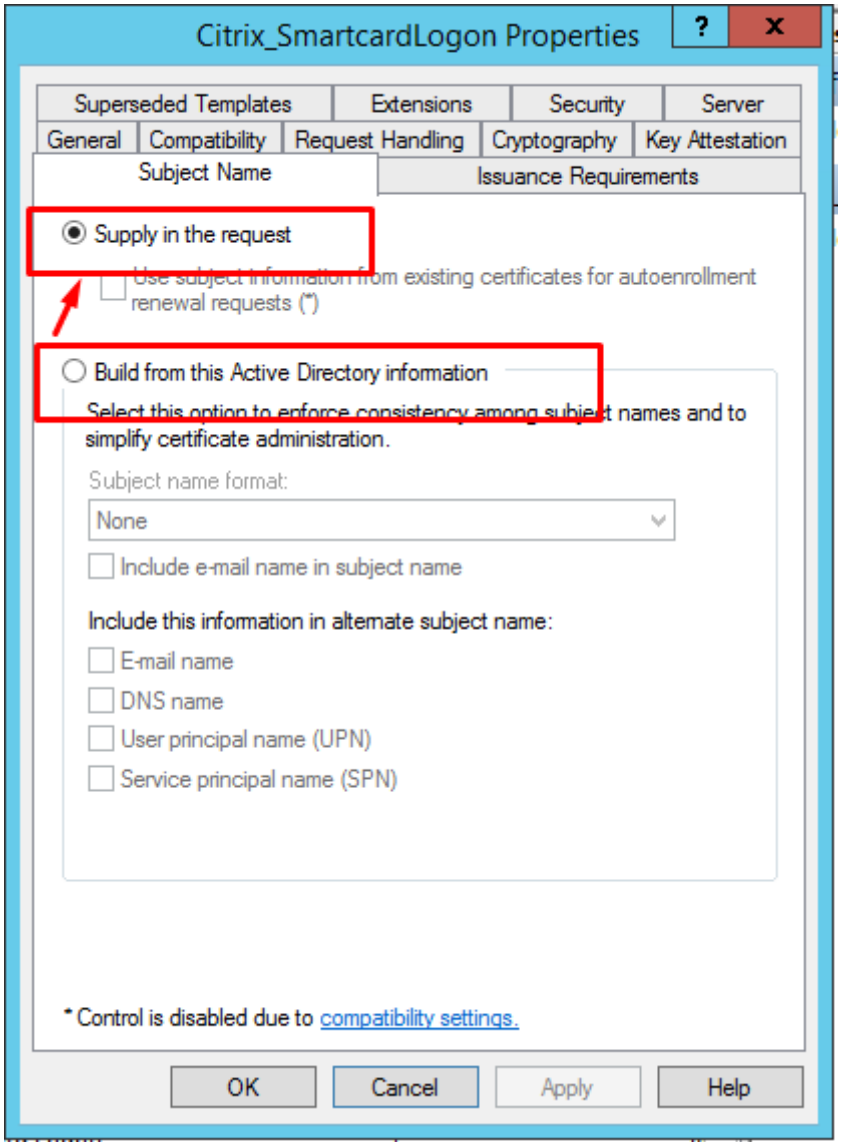
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

March 27, 2023

En este artículo, se ofrecen instrucciones sobre cómo habilitar la autenticación sin SSO en Linux VDA.

Información general

De forma predeterminada, Linux VDA tiene habilitado el inicio de sesión único (SSO). Los usuarios inician sesión en la aplicación Citrix Workspace y en las sesiones de VDA con un conjunto de creden-

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

ciales.

Para que los usuarios inicien sesión en sesiones de VDA con un conjunto diferente de credenciales, inhabilite el inicio de sesión SSO en Linux VDA. En la siguiente tabla se enumeran las combinaciones de métodos de autenticación de usuarios admitidos en supuestos sin SSO.

Aplicación Citrix Workspace	Sesión de VDA
nombre de usuario	nombre de usuario
tarjeta inteligente	nombre de usuario
nombre de usuario	tarjeta inteligente

Inhabilitar SSO

Ejecute el siguiente comando en Linux VDA:

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

Tarjetas inteligentes

March 27, 2023

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. Entre los casos de uso, se incluyen:

- Agregar una firma digital a un documento
- Cifrar o descifrar un correo electrónico
- 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.

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

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 9.0
  - RHEL 8.7/8.6/8.4
  - RHEL 7, CentOS 7
  - Rocky Linux 9.0
  - Rocky Linux 8.7/8.6
  - Ubuntu 22.04
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Debian 11.3

  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 como ejemplo para ilustrar la configuración. YubiKey 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.

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
```

© 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
   ```

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>
   ```

   Para crear una ruta donde instalar el certificado raíz, ejecute `sudo mdkir -p <path where you install the root certificate>`.

Generar el módulo pam_krb5 en RHEL 8.x y Rocky Linux 8.x

La autenticación con tarjeta inteligente depende del módulo pam_krb5, que se retiró en RHEL 8.x y Rocky Linux 8.x. Estos pasos son necesarios si quiere utilizar la autenticación con tarjeta inteligente en máquinas con RHEL 8.x y Rocky Linux 8.x que se entregan en modo de SO multisesión. Para la autenticación con tarjeta inteligente en máquinas con RHEL 8.x y Rocky Linux 8.x entregadas en modo de SO de sesión única (VDI), puede omitir estos pasos.

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. Compile e instale el módulo pam_krb5 en RHEL 8.x y Rocky Linux 8.x.

   ```
   yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-
       tools
   yum install gcc krb5-devel pam-devel autoconf libtool
   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio – div
   tar xvzf pam_krb5-2.4.8.tar.gz
   cd pam_krb5-2.4.8
   ./configure --prefix=/usr
   make
   make install
   ```

3. Compruebe que pam_krb5.so existe en /usr/lib64/security/.

   ```
   ls -l /usr/lib64/security | grep pam_krb5
   ```

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

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
```

Los resultados se asemejan a esto:

```
#*****************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*****************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

También puede inhabilitar las tarjetas inteligentes ejecutando el script ctxsmartlogon.sh:

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

Los resultados se asemejan a esto:

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

```
#*****************************************************************************
# 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, consulte el artículo CTX206156 de Knowledge Center.

Antes de ir al siguiente paso, asegúrese de que:

- Ha configurado todos los componentes correctamente.
- Ha descargado la clave privada y el certificado de usuario en la tarjeta inteligente.
- Puede iniciar sesión en el VDA con 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 9.0/8.x, Rocky Linux 9.0/8.x, RHEL 7/CentOS 7:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Debian 11.3:

```
apt-get install -y libpcsclite1 libccid
```

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 9.0/8.x, Rocky Linux 9.0/8.x, RHEL 7/CentOS 7:

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

```
yum install opensc
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Debian 11.3:

```
apt-get install -y opensc
```

Instalar los módulos PAM para la autenticación con tarjeta inteligente Ejecute el siguiente comando para instalar los módulos pam_krb5 y krb5-pkinit.

RHEL 7/CentOS 7:

```
yum install pam_krb5 krb5-pkinit
```

RHEL 9.0/8.x, Rocky Linux 9.0/8.x:

```
yum install krb5-pkinit
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04:

```
apt-get install libpam-krb5 krb5-pkinit
```

Debian 11.3:

```
apt-get install -y libpam-krb5 krb5-pkinit
```

El módulo pam_krb5 es un módulo de autenticación conectable. Las aplicaciones compatibles con PAM pueden usar pam_krb5 para comprobar las 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
```

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…**

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

> , donde **relación-operador** 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

  }
```

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 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.

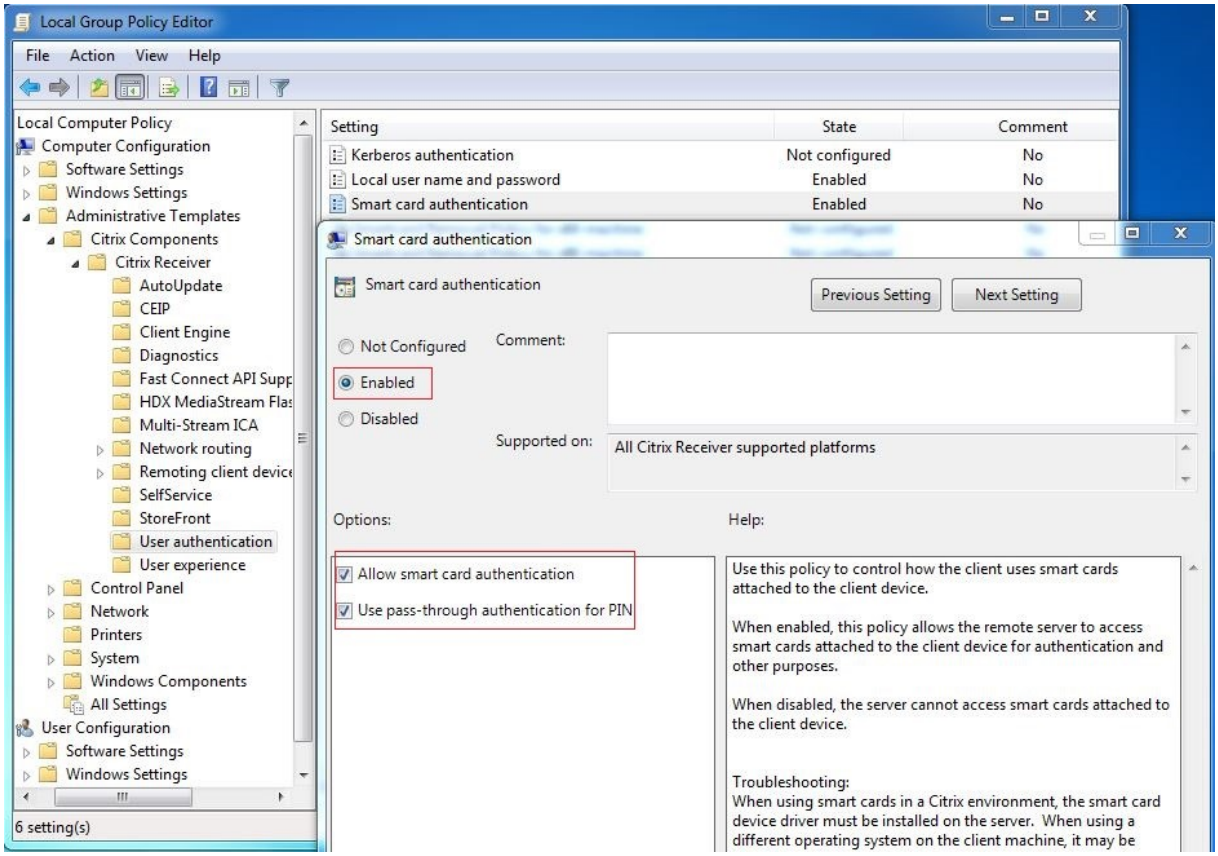
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
#%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
```

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.

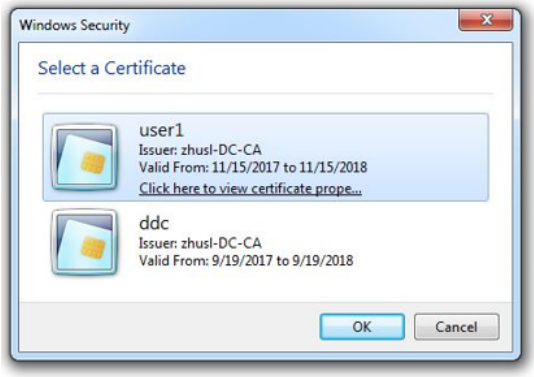
Uso

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.

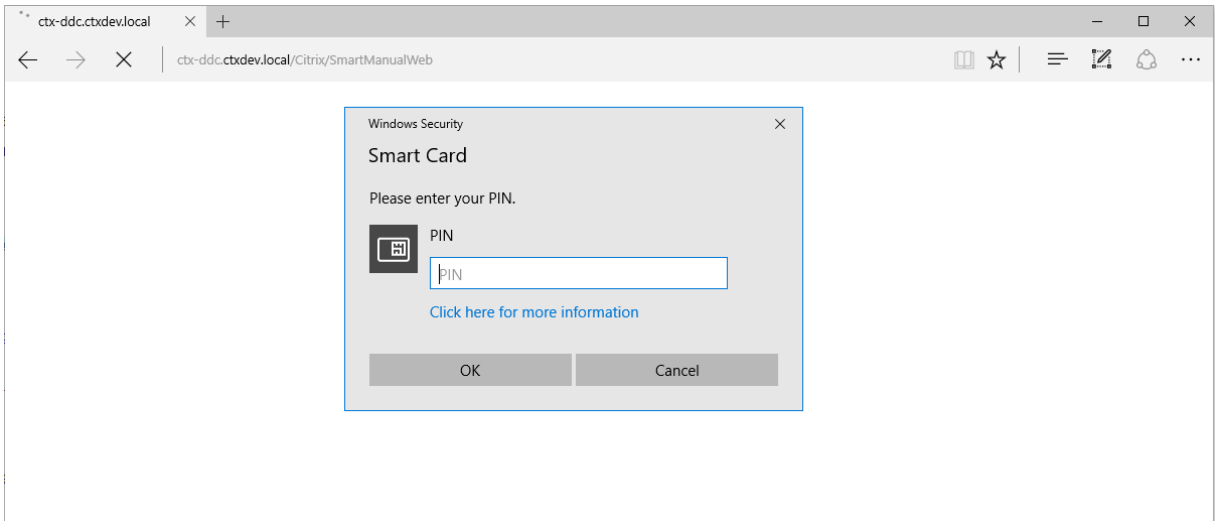
- En el caso de inicio SSO, inicia sesión automáticamente en StoreFront con el PIN y el certificado de la tarjeta inteligente guardados en la caché. Al iniciar una sesión de escritorio virtual Linux en StoreFront, el PIN se pasa al Linux VDA para la autenticación con tarjeta inteligente.
- En el caso de un inicio sin SSO, se le solicita seleccionar un certificado y escribir un PIN para iniciar sesión en StoreFront.

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



Al iniciar una sesión de escritorio virtual Linux en StoreFront, aparece este cuadro de diálogo para iniciar sesión en Linux VDA. El nombre de usuario se extrae del certificado en la tarjeta inteligente, y debe escribir el PIN nuevamente para la autenticación del inicio de sesión.

Este es el mismo comportamiento que con Windows VDA.



Reconectarse a una sesión mediante una tarjeta inteligente

Para volver a conectarse a una sesión, la tarjeta inteligente debe estar conectada al dispositivo cliente. De lo contrario, aparece una ventana gris de almacenamiento en caché en el lado del Linux VDA y se cierra rápidamente porque la reautenticación falla si la tarjeta inteligente no está conectada. No aparece ningún otro aviso en este caso para recordarle que conecte la tarjeta inteligente.

Sin embargo, en el lado de StoreFront, si una tarjeta inteligente no está conectada cuando vuelve a conectarse a una sesión, el sitio Web de StoreFront puede avisarle de la siguiente manera.

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

Limitación

Compatibilidad con distribuciones limitadas de Linux y métodos de integración de AD

- La autenticación PassThrough con tarjeta inteligente admite distribuciones limitadas de Linux y métodos de integración de AD. Consulte la siguiente matriz:

	Winbind	SSSD	Centrify
Debian 11.3	Sí	Sí	Sí
RHEL 9.0	Sí	Sí	No
RHEL 8.7/8.6/8.4	Sí	Sí	Sí
RHEL 7.9, CentOS 7.9	Sí	Sí	Sí
Rocky Linux 9.0	Sí	Sí	No
Rocky Linux 8.7/8.6	Sí	Sí	No
Ubuntu 22.04/20.04/18.04	Sí	Sí	Sí

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.

Compatibilidad con otras tarjetas inteligentes y la biblioteca PKCS#11

Citrix ofrece una solución genérica de redirección de tarjetas inteligentes. Aunque solo figura la tarjeta inteligente OpenSC en nuestra lista de compatibilidad, puede intentar utilizar otras tarjetas in-

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

teligentes y la biblioteca PKCS #11. 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"
   ```

   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

April 18, 2024

Use la información de este artículo para configurar sesiones no autenticadas. No se necesita ninguna configuración especial cuando se instala Linux VDA para usar esta función.

> **Nota:**
>
> Cuando configure sesiones no autenticadas, tenga en cuenta que la funcionalidad Preinicio de sesiones no está admitida. El preinicio de sesiones tampoco es compatible con la aplicación Citrix Workspace para Android.

Crear un almacén no autenticado

Para admitir una sesión no autenticada en Linux VDA, cree un almacén no autenticado con StoreFront.

Habilitar usuarios no autenticados en un grupo de entrega

Después de crear un almacén no autenticado, habilite usuarios no autenticados en un grupo de entrega para admitir sesiones no autenticadas. Para habilitar usuarios no autenticados en un grupo de entrega, siga las instrucciones indicadas en la documentación de Citrix Virtual Apps and Desktops.

© 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:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0x00000005
```

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:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0x00000020
```

> **Importante:**
>
> Limite la cantidad de sesiones no autenticadas. El inicio simultáneo de demasiadas sesiones puede provocar problemas en el VDA (por ejemplo, que se agote la memoria disponible).

Solución de problemas

Tenga en cuenta lo siguiente al configurar sesiones no autenticadas:

- **No se pudo iniciar sesión en una sesión no autenticada**.

Compruebe que el Registro se haya actualizado para incluir lo siguiente (establecer en 0):

```
sudo /opt/Citrix/VDA/bin/ctxreg read –k "HKLM\System\CurrentControlSet\Control\Citrix" –v MaxAnonymousUserNumber
```

Compruebe que el servicio **ncsd** se está ejecutando y está configurado para habilitar la memoria caché de **passwd**:

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

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.

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

- **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
```

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

March 27, 2023

Esta sección contiene estos temas:

- Copiar y pegar archivos
- Transferencia de archivos

Copiar y pegar archivos

March 27, 2023

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.

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

- El tamaño máximo de archivo no supere 200 MB.
- El administrador de archivos Nautilus está disponible en la máquina en la que instaló Linux VDA.

Distribuciones compatibles de Linux

La **función de copiar y pegar archivos** está disponible para todas las distribuciones de Linux compatibles con Linux VDA.

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 en el 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.
- La copia y el pegado de archivos deben hacerse de forma secuencial. Solo después de que el archivo anterior se haya copiado y pegado correctamente, se podrá copiar el siguiente archivo.

Transferencia de archivos

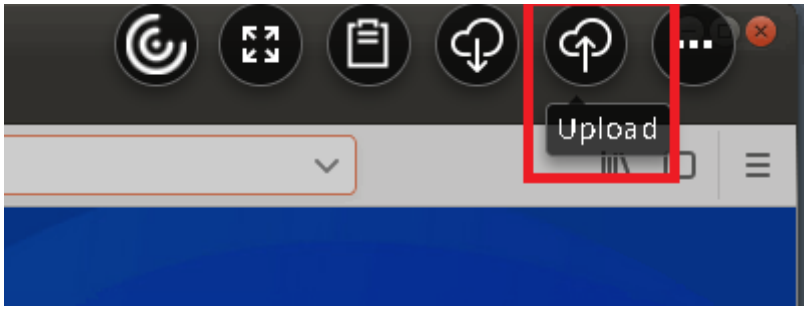
March 27, 2023

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.

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

> **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**

  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

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

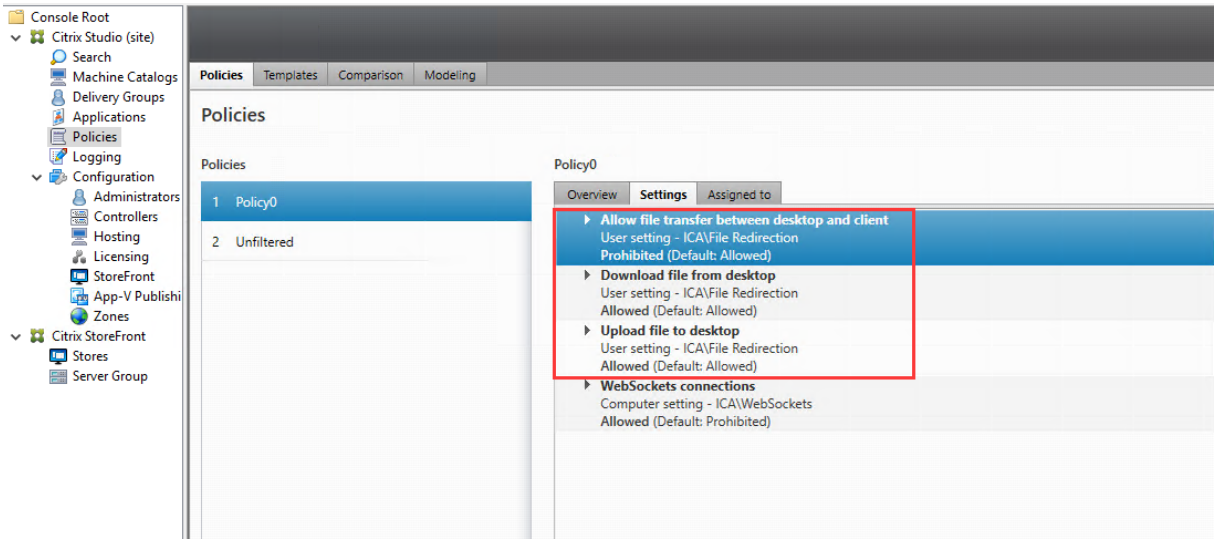
en **Guardar en mi dispositivo** y establezca un directorio de descargas local en el explorador web que ejecute la aplicación Citrix Workspace para HTML5 o para Chrome.

- 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.

> **Nota:**
>
> Para asegurarse de que las directivas **Descargar archivos desde el escritorio** y **Cargar archivos**

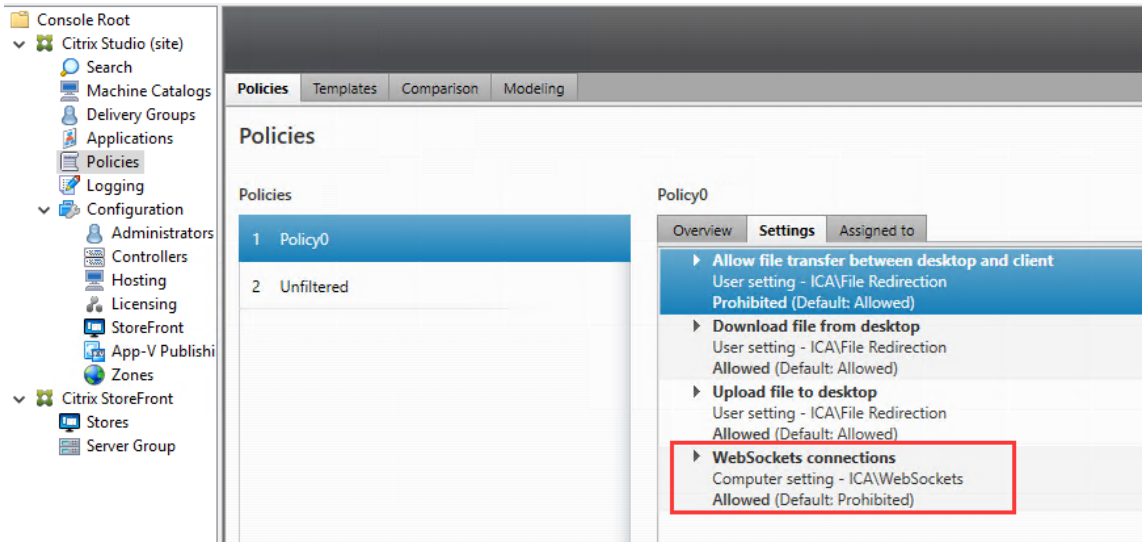
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **al escritorio** surtan efecto, establezca la directiva **Permitir transferencia de archivos entre escritorio y cliente** en **Sí**.

Uso

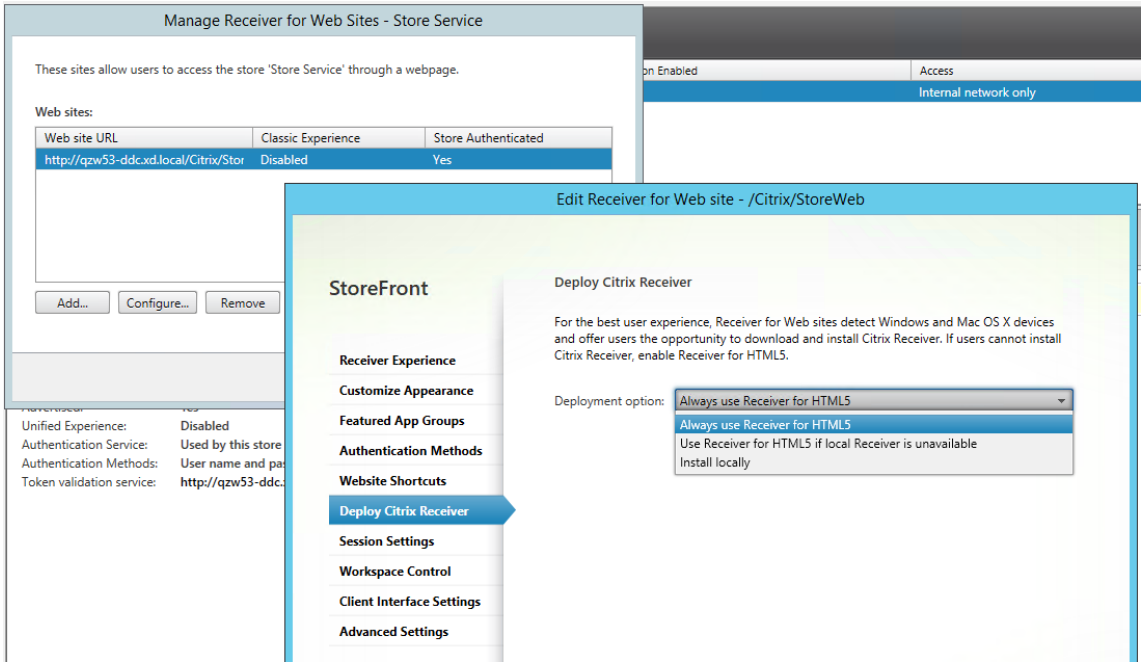
Para utilizar la función de transferencia de archivos a través de la aplicación Citrix Workspace para HTML5:

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:

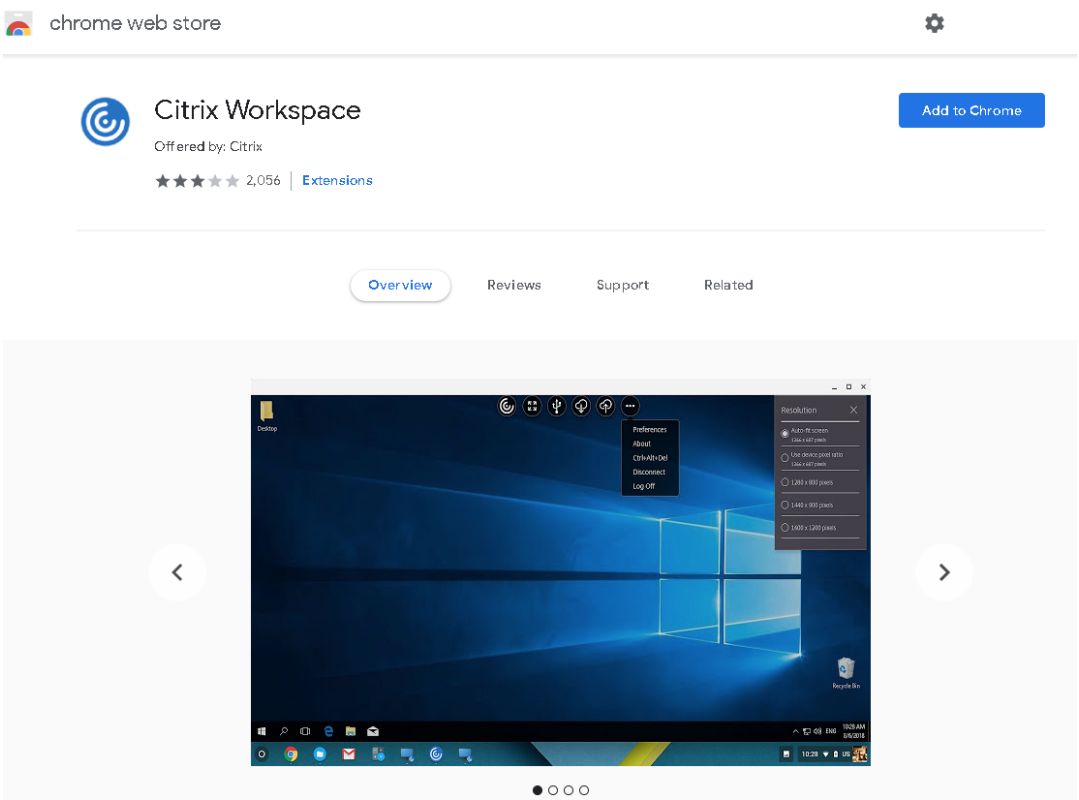
1. Habilite la transferencia de archivos mediante las directivas de transferencia de archivos que descritas anteriormente.
2. Adquiera la aplicación Citrix Workspace desde la tienda Chrome Web Store.

   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

March 27, 2023

Esta sección contiene estos temas:

- Escalado automático de PPP
- Pantalla de estado de la batería del cliente
- Configuración y ajuste de gráficos

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

- Pantalla compartida de HDX
- GPU no virtualizadas
- Marca de agua de la sesión
- Presentación progresiva de Thinwire

Escalado automático de PPP

April 18, 2024

Linux VDA admite el escalado automático de PPP. Cuando un usuario abre una sesión de aplicación o escritorio virtual, el valor de PPP de la sesión cambia automáticamente para coincidir con la configuración de PPP del lado del cliente.

A continuación, se indican algunas consideraciones relacionadas con esta función:

- La función requiere que habilite la correspondencia de PPP para Citrix Workspace. En el caso de la aplicación Citrix Workspace para Windows, asegúrese de que esté seleccionada la opción **No, usar la resolución nativa**. Para obtener más información sobre cómo configurar el escalado de PPP para la aplicación Citrix Workspace para Windows, consulte Escalado de PPP.
- Para que esta característica funcione en entornos de varios monitores, todos ellos deben tener la misma configuración de PPP. No se admiten escenarios de PPP mixtos. Si los monitores tienen diferentes configuraciones de PPP, Linux VDA aplica el valor de PPP más bajo en todas las pantallas.
- La función está habilitada para MATE, GNOME, GNOME Classic y KDE. Al usar KDE o MATE, tenga en cuenta lo siguiente:
  - Para escritorios virtuales Linux que se ejecutan en un entorno de escritorio KDE:
    * Recomendamos usar KDE Plasma 5 o una versión posterior.
    * Para cambiar la configuración de PPP en el lado del cliente mientras se ejecutan las sesiones, los usuarios deben cerrar sesión y volver a iniciarla.
  - Para escritorios virtuales Linux que se ejecutan en un entorno de escritorio MATE:
    * Solo se admiten los factores de escala de 1 y 2.
    * Para cambiar la configuración de PPP en el lado del cliente mientras se ejecutan las sesiones, los usuarios deben cerrar sesión y volver a iniciarla.
- El valor de PPP en la sesión virtual cambia automáticamente de acuerdo con la configuración de PPP del lado del cliente. Actualmente, la función solo admite factores de escala de tipo entero, por ejemplo, 100% y 200%. Si el factor de escala configurado en el lado del cliente es de tipo

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

fraccionario, el PPP de la sesión virtual cambia a un factor de escala entero de acuerdo con la siguiente tabla. Ejemplo: si el factor de escala es del 125%, el valor de PPP cambia al 100%.

Factor de escala del lado del cliente	PPP de sesión remota
Menor o igual que 174%	96 (1 x 96)
175 %–274 %	192 (2 x 96)
275 %–399 %	288 (3 x 96)
Mayor o igual que 400%	384 (4 x 96)

Pantalla de estado de la batería del cliente

March 27, 2023

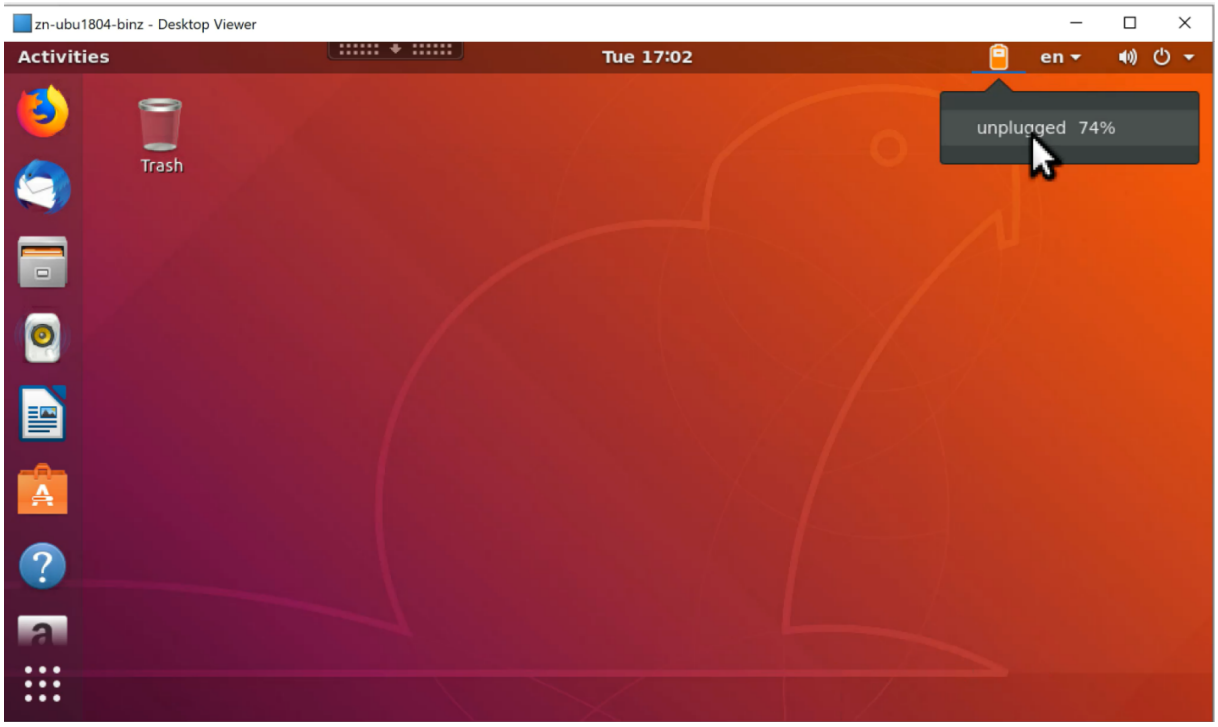
Linux VDA puede redirigir y mostrar el estado de la batería de los dispositivos cliente en los escritorios virtuales. Esta función está habilitada de forma predeterminada y disponible para las siguientes versiones de la aplicación Citrix Workspace:

- Aplicación Citrix Workspace para iOS
- Aplicación Citrix Workspace para Linux
- Aplicación Citrix Workspace para Mac (no compatible con la versión 2204.1)
- Aplicación Citrix Workspace para Windows (no compatible con la versión 2204.1)

Información general

Cuando los usuarios abren un escritorio virtual, pueden ver un icono de batería en la bandeja del sistema Linux. El icono indica el estado de la batería de sus dispositivos cliente. Para comprobar el porcentaje de duración restante, haga clic en el icono de la batería. La siguiente captura de pantalla sirve de ejemplo:

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



Los diferentes iconos de batería indican diferentes estados de esta. Para ver una descripción general, consulte la siguiente tabla:

Icono de batería	Estado de carga	Nivel de duración restante de la batería	Porcentaje de duración restante de la batería
	Cargando (se indica con un símbolo “+”)	Alto (se indica en color verde)	=80 %
	Cargando (se indica con un símbolo “+”)	Medio (se indica en color ámbar)	= 20% y < 80%
	Cargando (se indica con un símbolo “+”)	Bajo (se indica en color rojo)	< 20 %
	No cargando (se indica con un símbolo “-“)	Alto (se indica en color verde)	=80 %
	No cargando (se indica con un símbolo “-“)	Medio (se indica en color ámbar)	= 20% y < 80%

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

Icono de batería	Estado de carga	Nivel de duración restante de la batería	Porcentaje de duración restante de la batería
	No cargando (se indica con un símbolo “-“)	Bajo (se indica en color rojo)	< 20 %
	Desconocido	Desconocido	Desconocido

Configuración

La presentación del estado de la batería del cliente está habilitada por defecto.

Para inhabilitar esta función, ejecute el comando siguiente:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
    Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
```

Para habilitar esta función, ejecute el comando siguiente:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
    Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000001"
```

> **Nota:**
>
> Los comandos anteriores afectan a la función de teclado en pantalla, que comparte el canal virtual de Mobile Receiver (MRVC) con la presentación del estado de la batería del cliente.

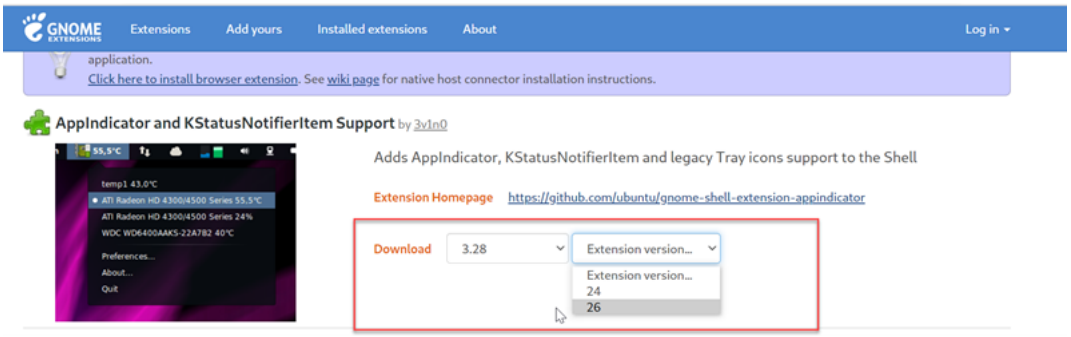
En función de su distribución, complete los siguientes pasos adicionales:

1. 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.

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



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 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.

2. Si utiliza Debian 11.3 instalado con GNOME, complete estos pasos para instalar y habilitar los iconos de la bandeja del sistema de GNOME:

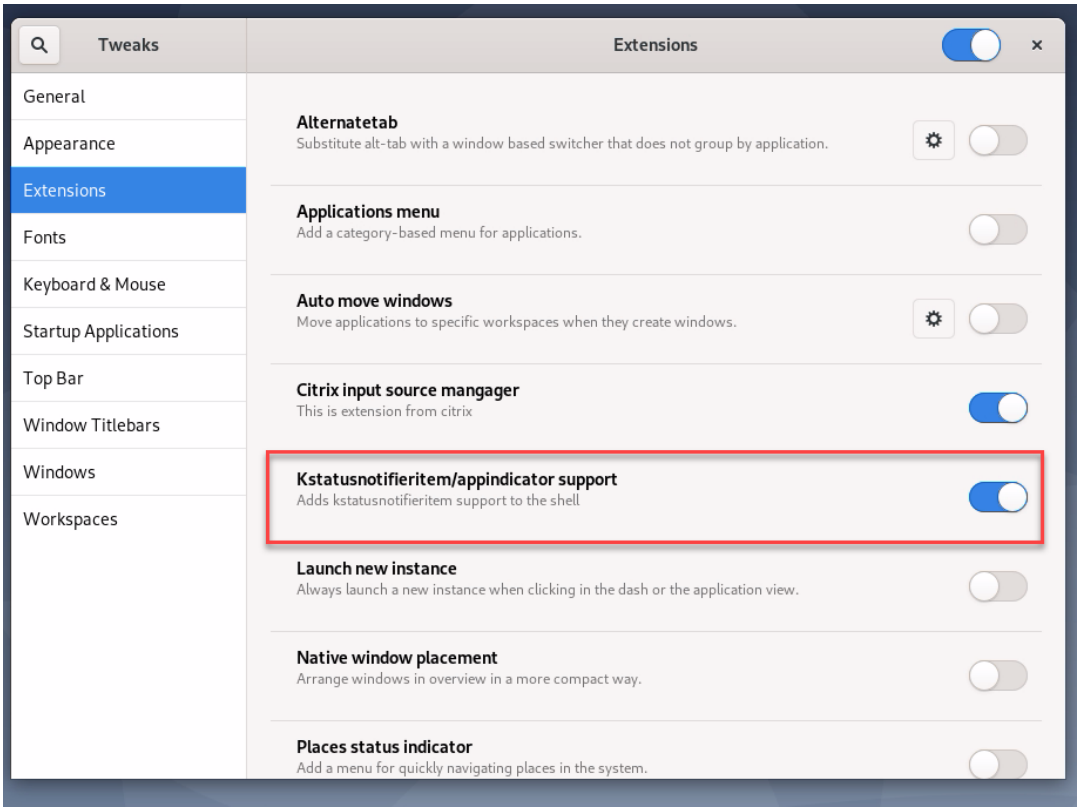
   a) Ejecute el comando `sudo apt install gnome-shell-extension-appindicator`. Puede que tenga que cerrar la sesión y reiniciarla para que GNOME vea la extensión.

   b) Busque Tweaks en la pantalla **Activities**.

   c) Seleccione **Extensions** en la herramienta Tweaks.

   d) Habilite **Kstatusnotifieritem/appindicator support**.

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



Configuración y ajuste de gráficos

April 18, 2024

En este artículo se ofrece una guía para configurar los gráficos y ajustes precisos en Linux VDA.

Para obtener más información, consulte Requisitos del sistema y la sección Información general de la instalación.

Configuración

Optimizar para cargas de trabajo de gráficos 3D

Esta configuración define los valores predeterminados que mejor se adaptan a cargas de trabajo con muchos gráficos. Habilite esta configuración para usuarios cuyas cargas de trabajo se centren en aplicaciones que hacen uso intensivo de gráficos. Aplique esta directiva solo en situaciones donde haya una GPU disponible en la sesión. Tiene prioridad cualquier otra configuración que anule explícitamente la configuración predeterminada establecida por esta directiva.

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

De forma predeterminada, la configuración **Optimizar para cargas de trabajo de gráficos 3D** está inhabilitada.

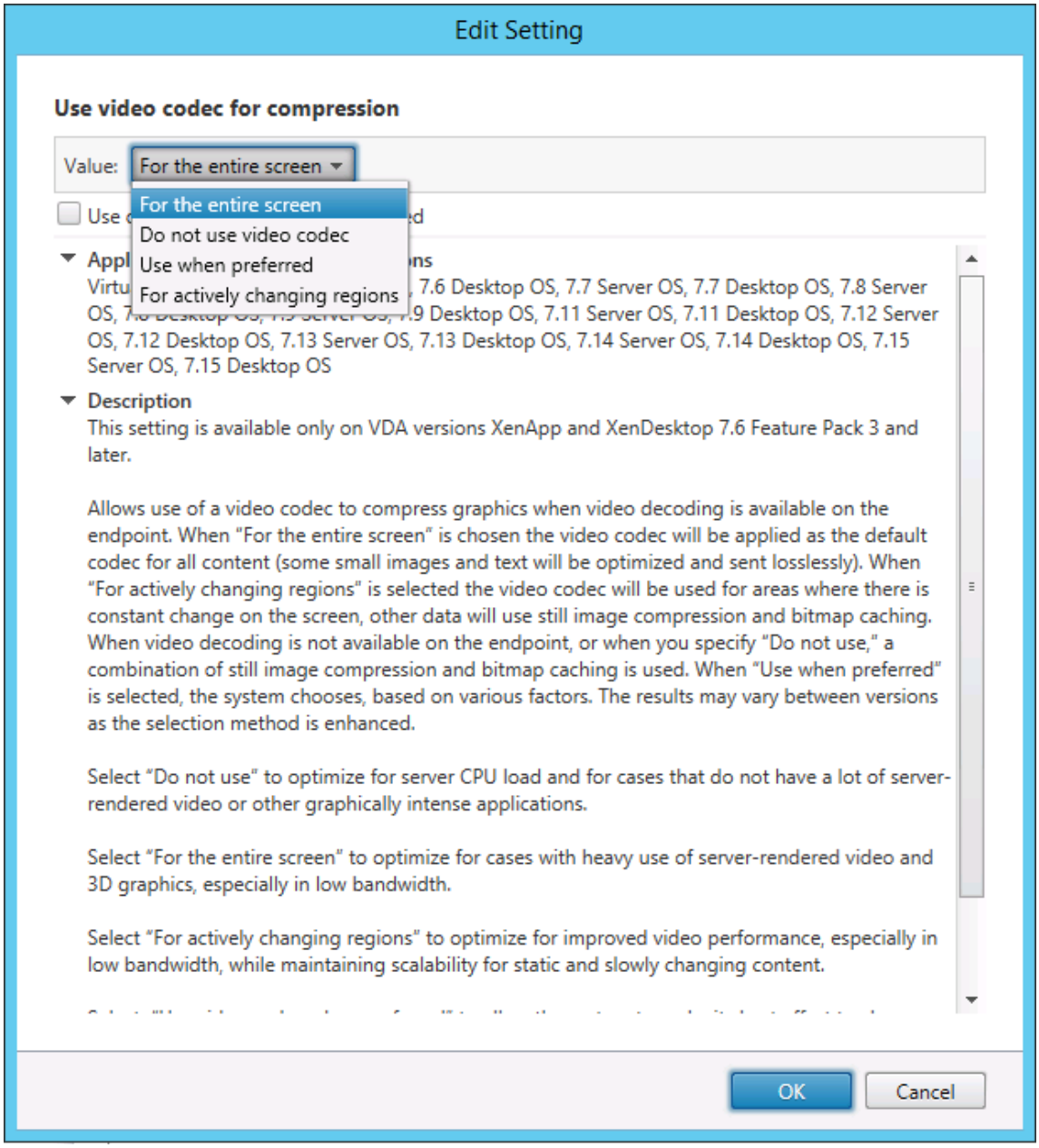
Códec de vídeo para compresión

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. La marca de agua de sesión se admite cuando se selecciona **Para la pantalla entera** o cuando se selecciona **Usar si se prefiere** y la opción Optimizar para cargas de trabajo de gráficos 3D está habilitada.
- **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, establezca la directiva **Usar códec de vídeo para compresión** en **Usar si se prefiere** (valor predeterminado) o **Para áreas en cambio constante**. Para obtener más información, consulte Configuraciones de directiva de gráficos.

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



Varias configuraciones de directiva más, incluidas las siguientes configuraciones de directiva de Presentación visual, se pueden usar para optimizar el rendimiento de la tecnología de pantallas remotas:

- **Profundidad de color preferida para gráficos simples**
- **Velocidad de fotogramas de destino**
- **Calidad visual**

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

Codificación por hardware H.264

La directiva **Usar codificación por hardware para códec de vídeo** permite el uso de aceleración de hardware de GPU, si está disponible, para comprimir los elementos en pantalla con el códec de vídeo. Si no hay hardware de GPU disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software.

La aceleración de hardware de GPU optimiza la utilización de los recursos de hardware y mejora considerablemente el rendimiento en términos de fotogramas por segundo (FPS).

A partir de la versión 2210, la aceleración de hardware de GPU abarca los siguientes modos gráficos:

- Usar si se prefiere
- Para la pantalla entera
- Para áreas en cambio constante

Permitir compresión sin pérdida visual

La directiva **Permitir compresión sin pérdida visual** permite usar compresión sin pérdida visual, en lugar de compresión sin pérdida verdadera, para los gráficos. La compresión sin pérdida visual mejora el rendimiento en mayor medida que la compresión sin pérdida verdadera, con una pérdida menor que no se nota a la vista. Este parámetro cambia el modo en que se usan los valores de la configuración **Calidad visual**.

La directiva **Permitir compresión sin pérdida visual** está inhabilitada de forma predeterminada. Para habilitar la compresión sin pérdida visual, establezca **Permitir compresión sin pérdida visual** en **Habilitado** y la directiva **Calidad visual** en **Gradual sin pérdida**.

Si la directiva **Usar códec de vídeo para compresión** está establecida en **No usar códec de vídeo**, la compresión sin pérdida visual se aplica a la codificación de imágenes estáticas. Si la directiva **Usar códec de vídeo para compresión** se establece en un modo de gráficos distinto de **No usar códec de vídeo**, la compresión sin pérdida visual se aplica a la codificación H.264.

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

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.

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

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**.

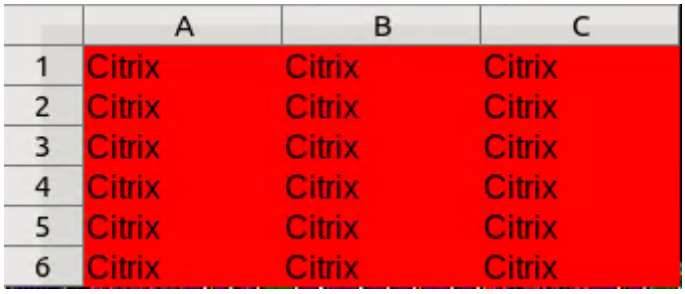
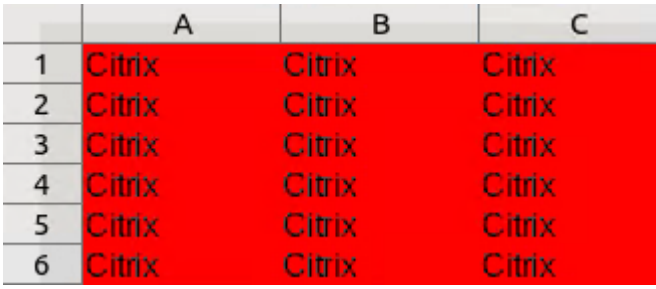
Para habilitar la codificación por hardware H.265 en su dispositivo cliente, consulte Codificación de vídeo H.265.

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**.

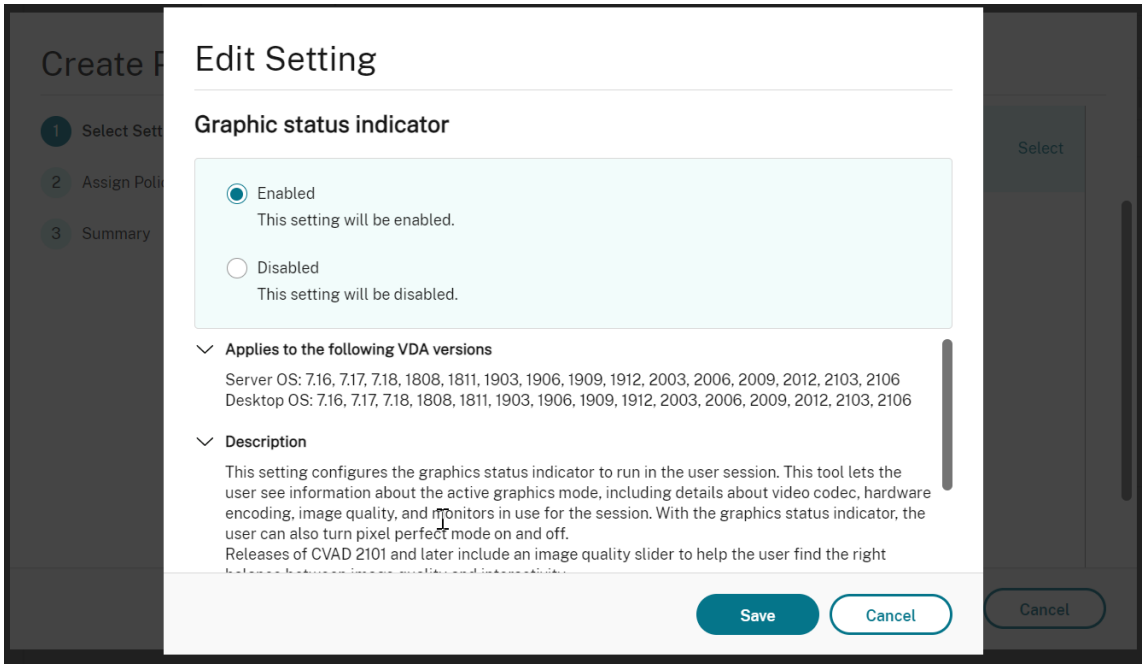
Control deslizante de calidad gráfica

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:

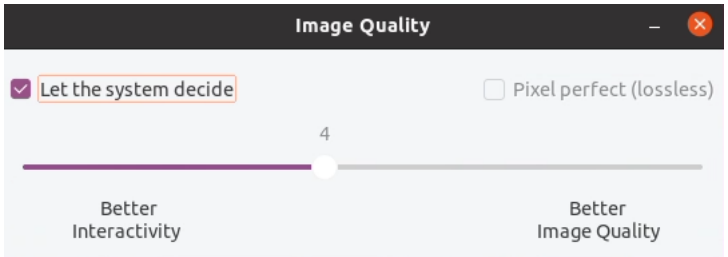
1. Habilite la directiva **Indicador de estado de gráficos** en Citrix Studio.

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



2. Abra el terminal y ejecute el comando `ctxslider`. Aparecerá la interfaz de usuario del control deslizante.

> **Nota:**
>
> Si ha establecido la directiva **Calidad visual** en **Siempre sin 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**.

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

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
```

Además de utilizar esta función, también puede ejecutar los siguientes comandos para ajustar entre nitidez y fluidez. Los parámetros **AverageBitRatePercent** y **MaxBitRatePercent** establecen el porcentaje de uso del ancho de banda. Cuanto más altos sean los valores que establezca, obtendrá mejor nitidez y fluidez. El intervalo de parámetros recomendado es de 50 a 100.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    AverageBitRatePercent" -d "90" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    MaxBitRatePercent" -d "100" --force
```

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.

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:

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

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ParallelProcessing" -d "0x00000001" --force
```

Solución de problemas

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
```

El resultado es similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

Compruebe que se utiliza H.264

Ejecute este comando para comprobar que se está utilizando H.264 (**0** significa que no se usa; **1** significa que sí se usa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

Por ejemplo, el resultado puede ser similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000000"--force
```

Compruebe que se utiliza H.265

Ejecute este comando para comprobar que se está utilizando H.265 en pantalla competa (**0** significa que no se usa; **1** significa que sí se usa):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Por ejemplo, el resultado puede ser similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H265"-d "0x00000000"--force
```

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

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.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

Por ejemplo, el resultado puede ser similar a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000000"--force
```

Compruebe que se utiliza la codificación por software YUV444

Ejecute el siguiente comando para comprobar que se está utilizando la codificación por software YUV444:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

Cuando YUV444 se está utilizando, el resultado se asemeja a:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force
```

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
```

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000000"--force
```

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--force
```

Compruebe que HDX 3D Pro esté habilitado

Ejecute los siguientes comandos para comprobar que HDX 3D Pro está habilitado:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep ProductEdition

sudo /opt/Citrix/VDA/bin/ctxreg dump | grep StackSessionMode

sudo /opt/Citrix/VDA/bin/ctxreg dump | grep 3DPro
```

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

Cuando HDX 3D Pro está habilitado, el resultado es similar al siguiente:

```
create -k "HKLM\Software\Citrix\VirtualDesktopAgent\State"-t "REG_SZ"
-v "ProductEdition"-d "<PLT or ENT>"--force
```

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\
tcp"-t "REG_DWORD"-v "StackSessionMode"-d "0x00000000"--force
```

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD
"-v "3DPro"-d "0x00000000"--force
```

Para comprobar que están cargadas las bibliotecas NVIDIA necesarias para HDX 3D Pro, ejecute el comando **nvidia-smi** en Linux VDA. El resultado es similar a:

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28         |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|
|   0  GRID K1             Off  | 0000:00:05.0     Off |
                      N/A |
| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
   Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|
|    0      2164  C+G   /usr/local/bin/ctxgfx
   106MiB |
|    0      2187    G   Xorg
    85MiB |
+-----------------------------------------------------------------------------+
```

Compruebe que se utiliza la codificación por hardware para 3D Pro

Ejecute este comando (**0** significa que no se usa; **1** significa que sí se usa):

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

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
```

Cuando se utiliza 3D Pro, el resultado se asemeja a:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

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
                                 |
+-----------------------------------------------------------------------------+
```

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
```

Para versiones de Citrix Hypervisor anteriores a 8.1:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

Los elementos emergentes de escritorio Gnome 3 son lentos cuando se inicia sesión

Esta es una limitación del inicio de sesiones en escritorios Gnome 3.

Algunas aplicaciones OpenGL o WebGL no se generan correctamente después de cambiar el tamaño de la ventana de la aplicación Citrix Workspace

Si cambia el tamaño de la ventana de la aplicación Citrix Workspace, cambiará la resolución de pantalla. El controlador propietario NVIDIA cambia algunos estados internos y puede requerir que las aplicaciones respondan adecuadamente. Por ejemplo, el elemento de la biblioteca de WebGL **lightgl.js** puede generar el error **Rendering to this texture is not supported (incomplete frame buffer)**.

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

Pantalla compartida de HDX

March 27, 2023

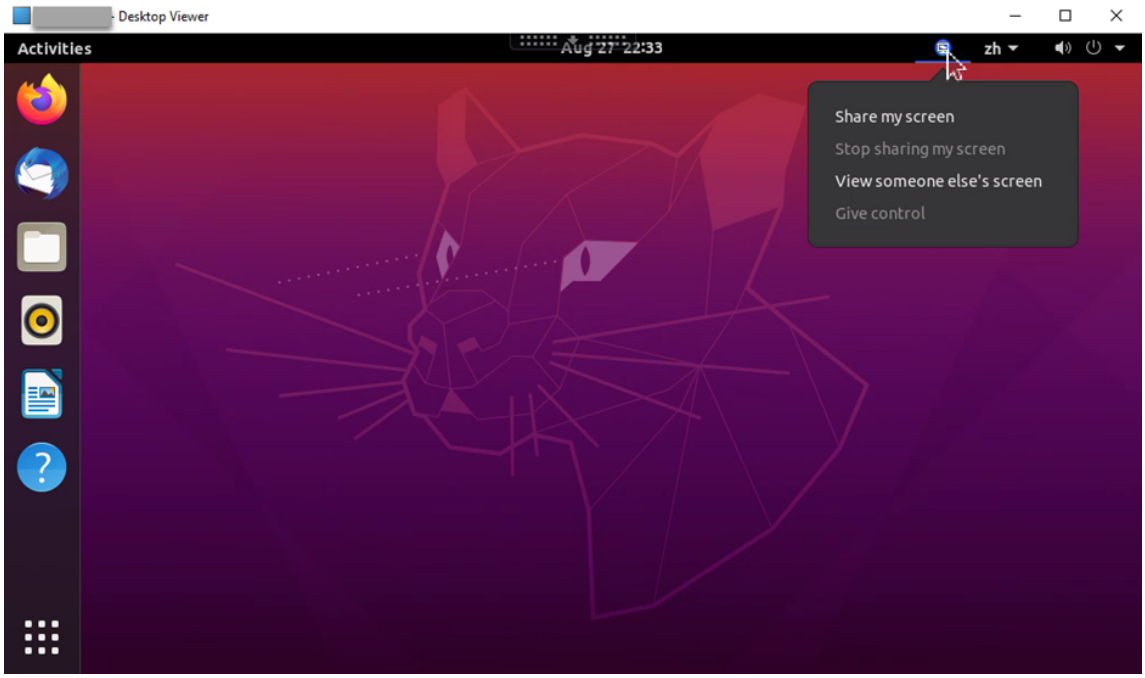
Información general

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:

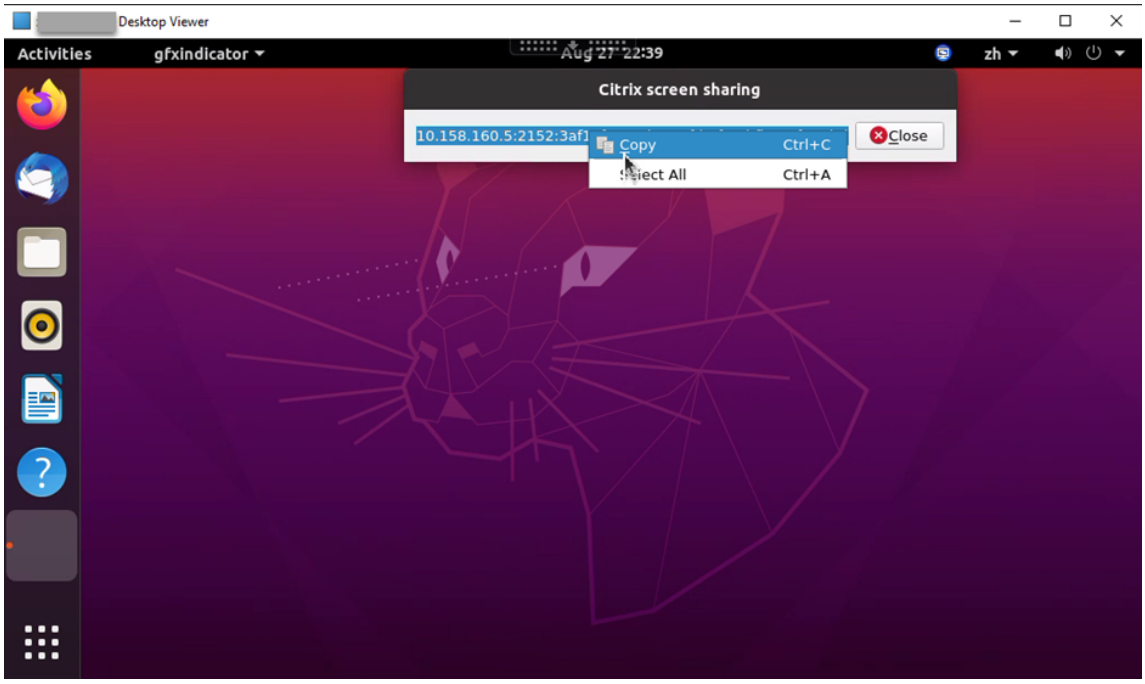
1. En el área de notificaciones de su escritorio virtual, haga clic en el icono de **compartir pantalla** y seleccione **Compartir mi pantalla**.



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.

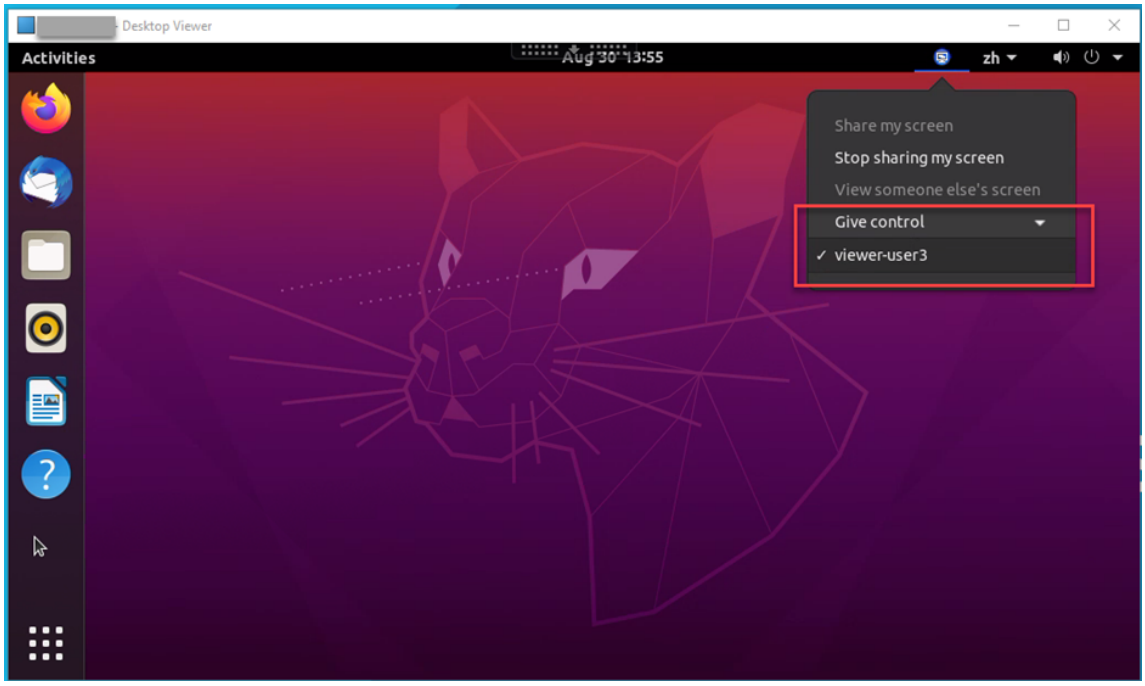
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



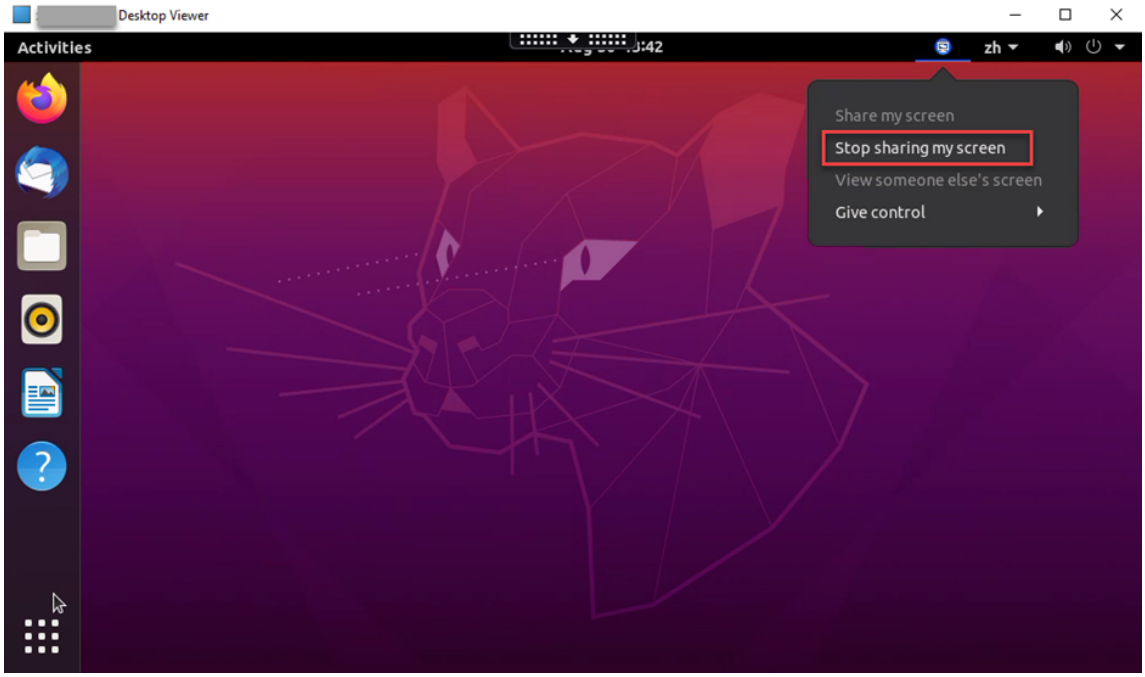
> **Sugerencia:**
>
> Mientras comparte la pantalla, hay un borde rojo a su alrededor, lo que indica que la pantalla se está compartiendo.

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.

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



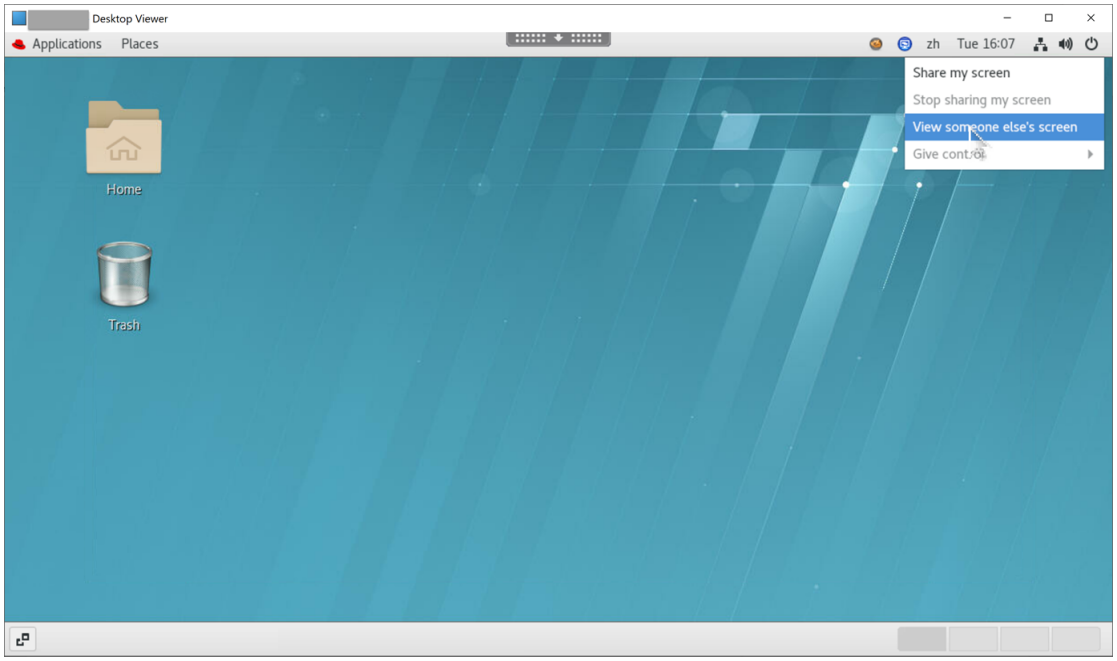
5. Para dejar de compartir la pantalla, seleccione **Dejar de compartir mi pantalla**.



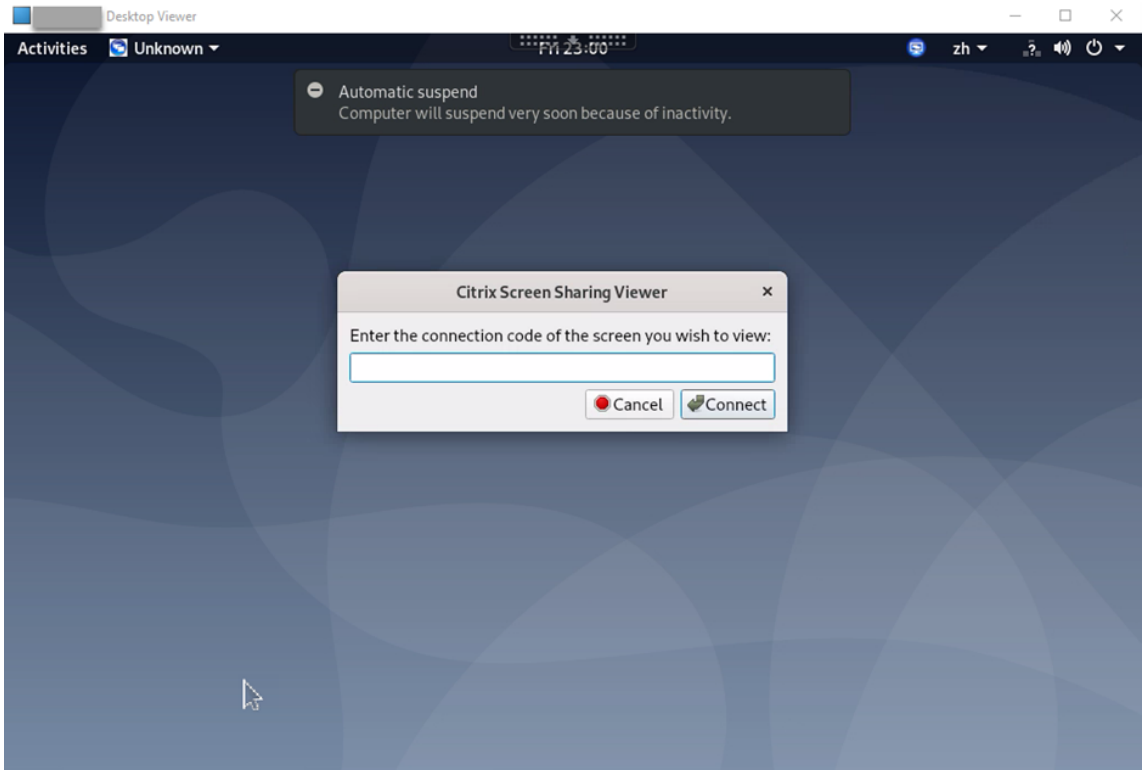
Para ver la pantalla de otro participante:

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**.

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

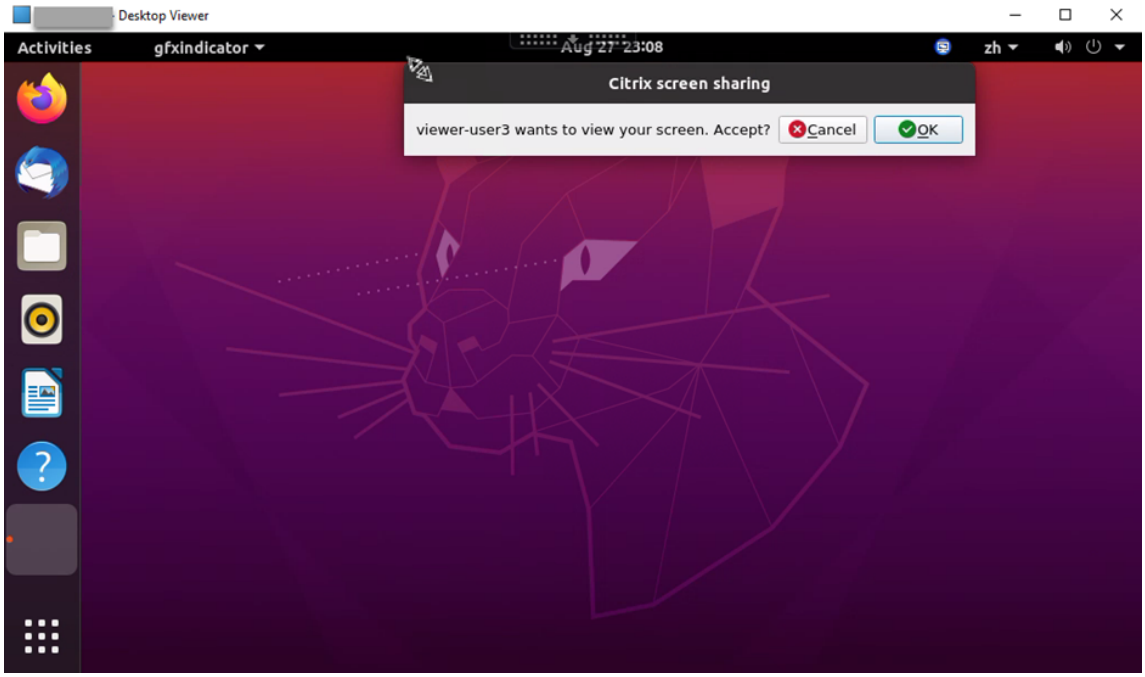


2. Introduzca el código de conexión de la pantalla que quiere ver y, a continuación, haga clic en **Conectar**.



3. Espere a que el usuario que comparte la pantalla acepte su solicitud. Por ejemplo:

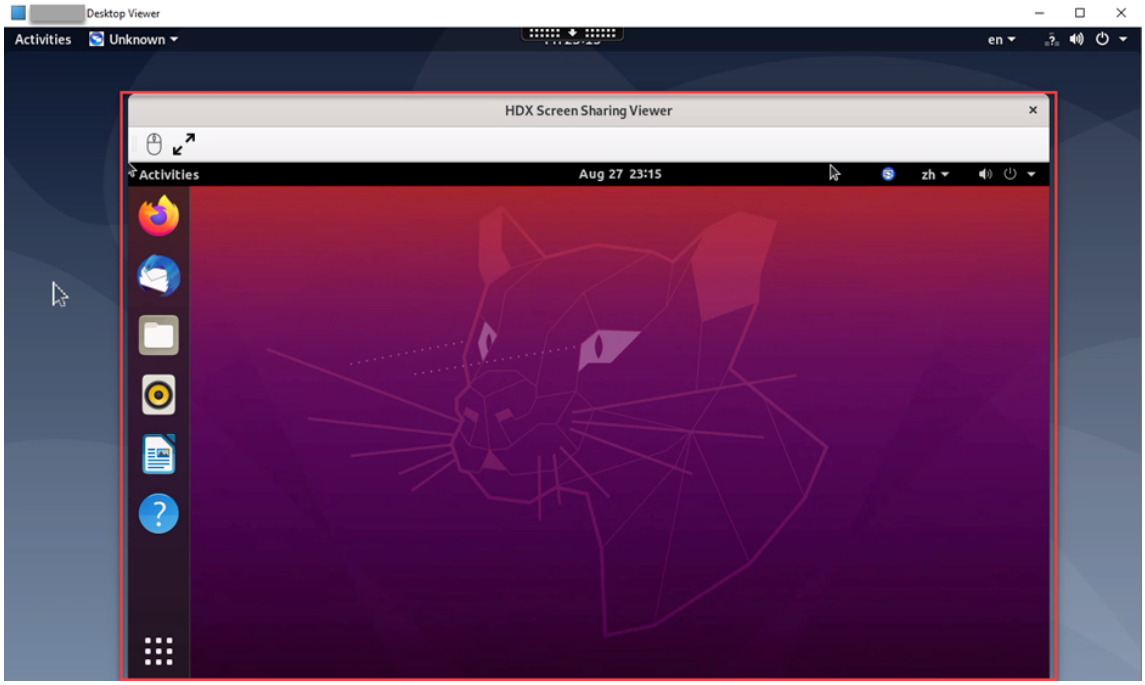
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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.

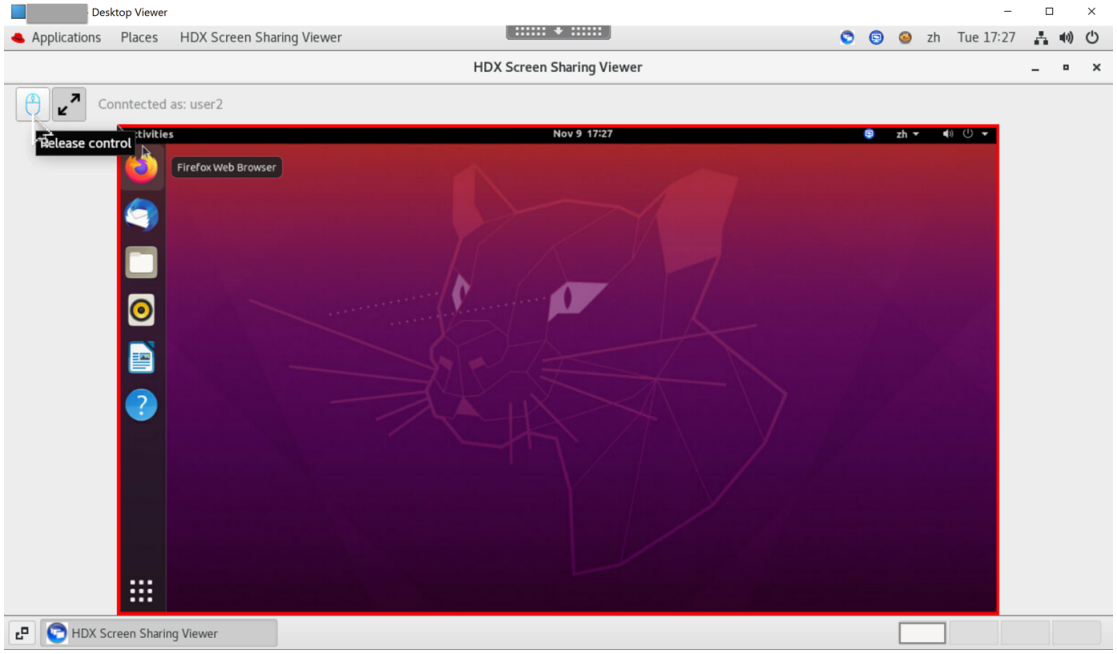


5. Para solicitar el control sobre la pantalla compartida, haga clic en el icono del mouse situado en la esquina superior izquierda.

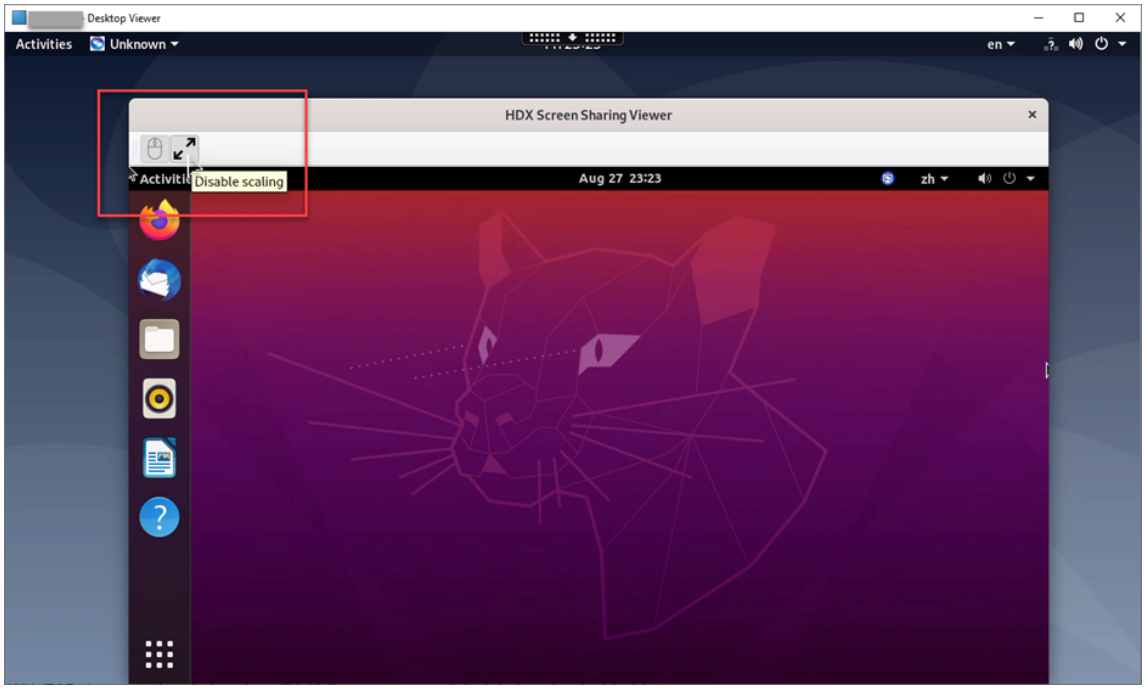
> **Sugerencia:**
>
> - Si el usuario que comparte la pantalla no acepta su solicitud en 30 segundos, la solicitud caduca.
> - Solo un espectador tiene permiso para controlar una pantalla compartida.

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.

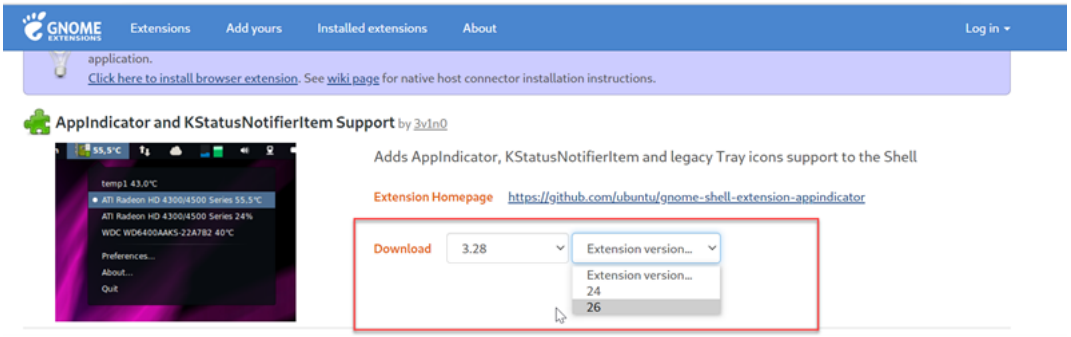
1. Habilite la directiva de indicador de estado de gráficos en Citrix Studio.
2. Para Citrix Virtual Apps and Desktops 2112 y versiones posteriores, habilite la directiva **Uso compartido de la pantalla** en Citrix Studio.
3. (Opcional) Para Citrix Virtual Apps and Desktops 2109 y versiones anteriores, 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"
```

4. Permita los puertos 52525-52625 en su firewall.
5. (Opcional) Si utiliza RHEL 8.x, Debian 11 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

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

> uso compartido de pantalla, haga el archivo **metadata.json** legible también para 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.

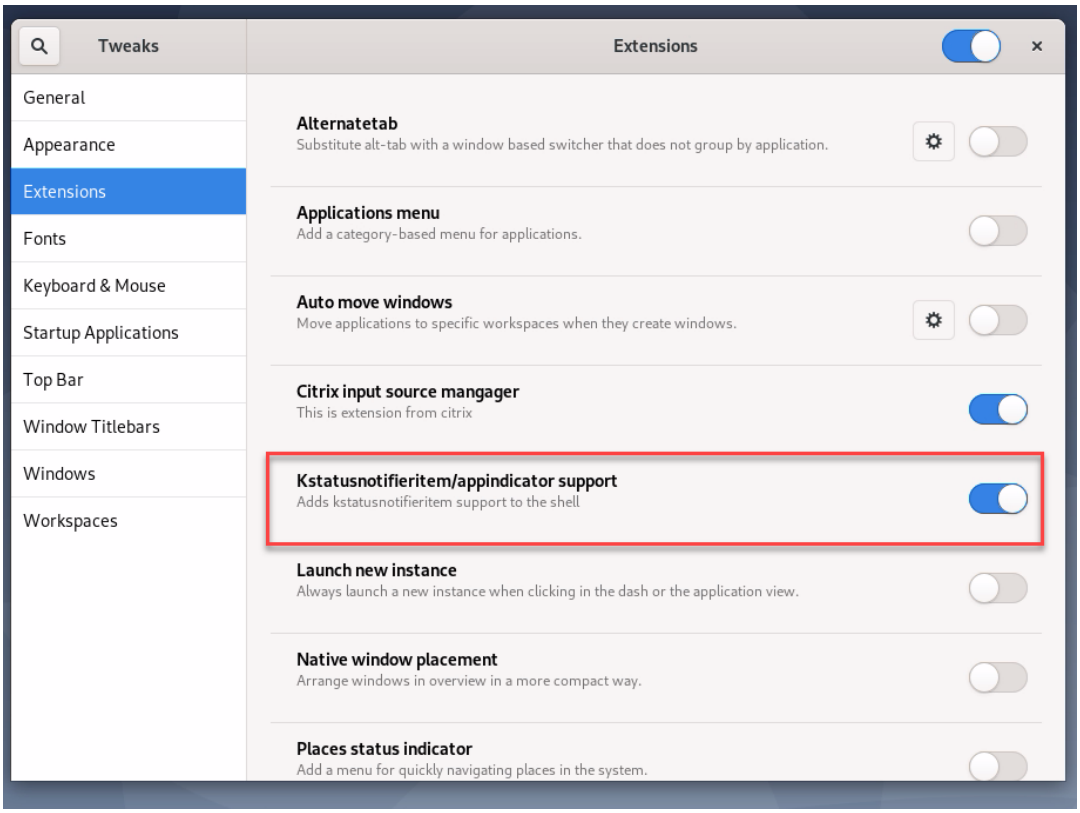
6. (Opcional) Si utiliza Debian 11.3 instalado con GNOME, complete los siguientes pasos para instalar y habilitar los iconos de la bandeja del sistema de GNOME:

   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.

GPU no virtualizadas

March 11, 2024

En la documentación de Linux VDA, las GPU no virtualizadas hacen referencia a:

- GPU utilizadas en casos de acceso con Remote PC
- GPU transferidas desde un hipervisor

Este artículo proporciona información sobre cómo habilitar HDX 3D Pro para GPU no virtualizadas.

Requisitos previos

- Habilite HDX 3D Pro. Para ello, establezca `CTX_XDL_HDX_3D_PRO` en `Y` al instalar Linux VDA. Para obtener información sobre las variables de entorno, consulte Paso 8: Configure el entorno en tiempo de ejecución para completar la instalación.
- En el caso de GPU compatibles con NVIDIA Linux Capture SDK, la aceleración de hardware se habilita de forma predeterminada después de habilitar HDX 3D Pro. No se requiere ninguna configuración adicional.
- Para las GPU no compatibles con NVIDIA Linux Capture SDK, instale `XDamage`. Por ejemplo, puede ejecutar `sudo apt-get install -y libxdamage1` para instalar XDamage en Ubuntu 20.04. Por lo general, XDamage existe como una extensión de XServer.

Configuración

Modificar los archivos de configuración de Xorg

Para GPU no virtualizadas de NVIDIA Los archivos de configuración se instalan y se configuran automáticamente.

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

Para otras GPU 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
- 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 GPU para obtener información sobre la configuración. Se puede generar un archivo de configuración nativo. Compruebe que la GPU pueda funcionar en un entorno local con el archivo de configuración nativo.

   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.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
    DriverName" -d "intel" --force
```

Habilitar XDamage

Si utiliza una GPU que no aparece en la sección de hardware compatible de las notas de publicación de NVIDIA Linux Capture SDK habilite `XDamage` mediante:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
    XDamageEnabled" -d "0x00000001" --force
```

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

Puesta en blanco del monitor para VDA de acceso con Remote PC

Linux VDA admite la puesta en blanco del monitor físico para los VDA de acceso con Remote PC que utilizan GPU no virtualizadas.

Entre las distribuciones de Linux totalmente probadas que admiten esta función se incluyen Ubuntu 20.04 y Debian 11.3.

Esta función está inhabilitada de forma predeterminada. Para habilitarla, complete estos dos pasos:

1. Instale el paquete `evdi-dkms` correspondiente a su distribución Linux:

```
sudo apt install evdi-dkms
```

2. Habilite la transferencia de la presentación de gráficos a EVDI:

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

3. Si utiliza una GPU de Intel, inhabilite el administrador de pantallas. De lo contrario, la GPU de Intel está ocupada con el administrador de pantallas y no está disponible para las sesiones remotas de Citrix.

```
sudo systemctl disable --now gdm
```

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

Si usa `Xdamage`, solo se admite la codificación por software.

Marca de agua de la sesión

March 27, 2023

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

La marca de agua de la sesión ayuda a disuadir del robo de datos y a rastrear los datos robados. La información rastreable aparece en los escritorios de sesiones como un elemento de disuasión para usuarios que se valen de fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua como capa de texto o imagen PNG con canal alfa. La marca de agua se muestra en la pantalla de toda la sesión sin cambiar el contenido del documento original.

> **Importante:**
>
> La marca de agua de la sesión no es una función de seguridad. 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. Le recomendamos que combine esta funcionalidad con otras soluciones de seguridad, según corresponda.

La marca de agua de la sesión contiene información para rastrear datos robados. La información más importante es la identidad del usuario, rastreada por sus credenciales de inicio de sesión, 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 siguientes configuraciones de directiva de marca de agua para definir la ubicación y la apariencia de la marca de agua en la pantalla.

Configuraciones de directiva de Marca de agua de la sesión

Habilitar marca de agua de la sesión

Cuando habilita esta configuración, aparece una marca de agua opaca que muestra información específica de la sesión en la pantalla de la sesión. Las demás configuraciones de marca de agua dependen de que esta configuración esté habilitada.

De forma predeterminada, la marca de agua de la sesión está inhabilitada.

Incluir dirección IP del cliente

Cuando habilita esta configuración, la sesión muestra la dirección IP del cliente actual como una marca de agua.

De forma predeterminada, **Incluir dirección IP del cliente** está inhabilitado.

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

Incluir la hora de la conexión

Cuando habilita esta configuración, la marca de agua de la sesión muestra la hora de la conexión. El formato es: aaaa/mm/dd hh:mm. La hora que aparece se basa en el reloj del sistema y la zona horaria.

De forma predeterminada, **Incluir la hora de la conexión** está inhabilitado.

Incluir nombre de usuario de inicio de sesión

Cuando habilita esta configuración, la sesión muestra el nombre del usuario que ha iniciado la sesión como una marca de agua. El formato es: NOMBREDEUSUARIO@NOMBREDEDOMINIO. Recomendamos que el nombre de usuario tenga un máximo de 20 caracteres. Cuando un nombre de usuario tiene más de 20 caracteres, pueden aparecer fuentes de tamaño más pequeño o puede haber truncamiento de caracteres, con lo que disminuye la eficacia de la marca de agua.

De forma predeterminada, **Incluir nombre de usuario de inicio de sesión** está habilitado.

Incluir nombre de host del VDA

Cuando habilita esta configuración, la sesión muestra el nombre de host del VDA perteneciente a la sesión ICA actual como una marca de agua.

De forma predeterminada, **Incluir nombre de host del VDA** está habilitado.

Incluir dirección IP del VDA

Cuando habilita esta configuración, la sesión muestra la dirección IP del VDA perteneciente a la sesión ICA actual como una marca de agua.

De forma predeterminada, **Incluir dirección IP del VDA** está inhabilitado.

Estilo de la marca de agua de la sesión

Esta configuración controla si se muestra una sola etiqueta de texto de la marca de agua o varias etiquetas. Elija **Múltiple** o **Única** en el menú desplegable **Valor**.
Para obtener más opciones de estilo, consulte la sección **Texto personalizado de la marca de agua** de este artículo.

La opción **Múltiple** muestra cinco etiquetas de marca de agua en la sesión. Una en el centro y cuatro en las esquinas.

La opción **Única** muestra una sola etiqueta de marca de agua en el centro de la pantalla de la sesión.

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

De forma predeterminada, el **estilo de la marca de agua de la sesión** es **Múltiple**.

Transparencia de la marca de agua

Puede especificar una opacidad de la marca de agua que oscile entre 0 y 100. Cuanto mayor sea el valor especificado, más opaca será la marca de agua.

De forma predeterminada, el valor es 17.

Texto personalizado de la marca de agua

El valor está en blanco de forma predeterminada. Puede escribir una cadena que no esté vacía, establecer una sintaxis para formar una cadena o usar la combinación para mostrarla en la marca de agua de la sesión. Las cadenas no vacías admiten hasta 25 caracteres Unicode por línea. Las cadenas más largas se truncan al llegar a 25 caracteres.

Por ejemplo, puede establecer la directiva en el siguiente valor:

```
<date> <time><newline><username><style=single><fontsize=40><font=
Ubuntu><position=center><rotation=0><newline><serverip><newline><
clientip><newline>Citrix Linux VDA<newline>Version 2207
```

Para obtener una descripción de todas las opciones de sintaxis, consulte la tabla siguiente:

Opción de sintaxis	Descripción	Configuración válida (distingue mayúsculas de minúsculas)	Valor predeterminado	Observaciones
`<style>`	Estilo de diseño de la marca de agua	`xstyle`, `single`, `tile`, `horizontal`	`xstyle`	-
`<position>`	Posición de la marca de agua	`center`, `topleft`, `topright`, `bottomleft`, `bottomright`	`center`	Solo es válido cuando el estilo de diseño está establecido en **único**.
`<rotation>`	Rotación de la marca de agua a un ángulo determinado	-180–180	0	-

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

Opción de sintaxis	Descripción	Configuración válida (distingue mayúsculas de minúsculas)	Valor predeterminado	Observaciones
<transparency>	Opacidad de la marca de agua	0–100	17	-
<font>	-	Una fuente compatible con el sistema	Sans	-
<fontsize>	-	20–50	0 (calculado automáticamente)	-
<fontzoom>	Porcentaje de los tamaños de fuente e imagen que establecen <fontsize> y <image>	0 –	100	-
<image>	Marca de agua PNG	Ruta a una imagen PNG en el VDA	N/D	Esta sintaxis configura una marca de agua PNG. Solo se admite PNG con un canal alfa. Con una marca de agua PNG en uso, solo son aplicables las opciones de sintaxis <style>, <position>, <rotation>, <transparency> y <fontzoom>.

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

Opción de sintaxis	Descripción	Configuración válida (distingue mayúsculas de minúsculas)	Valor predeterminado	Observaciones
<date>	Marcador de posición para la fecha de conexión de la sesión (AAAA/MM/DD)	N/D	N/D	-
<time>	Marcador de posición para la hora de conexión de la sesión (HH:MM)	N/D	N/D	-
<domain>	Marcador de posición para el dominio de la cuenta de usuario	N/D	N/D	-
<username>	Marcador de posición para el nombre de usuario que ha iniciado la sesión actual (excluido el dominio de la cuenta de usuario)	N/D	N/D	-
<hostname>	Marcador de posición para el nombre de host del VDA	N/D	N/D	-
<clientip>	Marcador de posición para la dirección IP del cliente	N/D	N/D	-

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

Opción de sintaxis	Descripción	Configuración válida (distingue mayúsculas de minúsculas)	Valor predeterminado	Observaciones
`<serverip>`	Marcador de posición para la dirección IP del VDA	N/D	N/D	-

> **Nota:**
>
> Si se especifica el **texto personalizado de la marca de agua** con una configuración de sintaxis válida, se ignoran todas las demás directivas de marca de agua de sesión, excepto **Habilitar marca de agua de la sesión**.
>
> Si deja una opción de sintaxis sin especificar o la establece en un valor no admitido, se utilizará su valor predeterminado.

Limitaciones

- La marca de agua de sesión se admite en cualquiera de los siguientes casos:
  - Cuando **Usar códec de vídeo para compresión** está establecida en **Para la pantalla entera**.
  - Cuando **Usar códec de vídeo para la compresión** está establecida en **Usar si se prefiere** y la opción Optimizar para cargas de trabajo de gráficos 3D está habilitada.
- La marca de agua de sesión no se admite 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 define como 2 en el Registro).
- La marca de agua no es visible en el remedo de sesiones.
- Si se presiona la tecla Imprimir pantalla, la pantalla capturada en el lado del VDA no incluirá la marca de agua. Le recomendamos que tome las medidas oportunas para evitar que se copien las imágenes capturadas.

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

Presentación progresiva de Thinwire

March 27, 2023

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 baja a menos de 2 Mbps
- La latencia de red supera los 200 ms.

En este modo:

Por ejemplo, en el siguiente gráfico, donde el modo de actualización progresiva está activo, las letras **F** y **e** tienen artefactos azules, y la imagen está muy comprimida. Este 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.

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.

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

Features

Para ofrecer imágenes más nítidas, se utiliza un método aleatorio por bloques. Para el texto, se definen letras individuales o partes de palabras. El proceso de nitidez se produce en varias tramas. De esta manera, se evita el retraso que conlleva usar una sola trama grande para la nitidez.

Las imágenes transitorias (vídeo) se siguen gestionando con la pantalla adaptable o H.264 selectivo.

Cómo se usa el modo progresivo

De forma predeterminada, el modo progresivo está en espera en las configuraciones de la directiva **Calidad visual**: **Alta**, **Media** (predeterminado) y **Baja**.

El modo progresivo se desactiva (no se usa) cuando:

- **Calidad visual** = **Siempre sin pérdida** o **Gradual sin pérdida**
- **Preferencia de profundidad de color para gráficos sencillos** = 8 bits
- **Usar códec de vídeo para compresión** = **Para la pantalla entera** (cuando se prefiere H.264 a pantalla completa)

Si el modo progresivo está en espera, se habilita de forma predeterminada cuando se da una de las siguientes condiciones:

- El ancho de banda disponible baja a menos de 2 Mbps
- La latencia de red aumenta por encima de 200 ms

Después de un cambio de modo, transcurre un mínimo de 10 segundos en ese modo, aunque las condiciones adversas de la red fueran temporales.

Cambiar el comportamiento del modo progresivo

Para cambiar el comportamiento del modo progresivo, ejecute el siguiente comando:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplay" -d "<value>" --force
```

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

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
```

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
```

Donde <value> es <umbral en ms> (predeterminado = 200)

Ejemplo: 100 = activa el modo progresivo si la latencia de la red baja de 100 ms.

Redirección de contenido general

March 27, 2023

Asignación de unidades del cliente y redirección de carpetas de cliente

Si	Entonces
habilita solo la asignación de unidades del cliente en el host (VDA),	los volúmenes completos del lado del cliente se asignan automáticamente a las sesiones del subdirectorio **ctxmnt** del directorio principal.
habilita la redirección de carpetas del cliente en el host (VDA) y el usuario la configura en el dispositivo del usuario (cliente),	se redirige la parte del volumen local especificada por el usuario.

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

Redirección de dispositivos USB

Los dispositivos USB se comparten entre la aplicación Citrix Workspace y el escritorio de Linux VDA. Cuando un dispositivo USB se redirige al escritorio, puede usar ese dispositivo como si estuviera conectado localmente.

Asignación de unidades del cliente

March 27, 2023

Puede utilizar la asignación de unidades del cliente y la redirección de carpetas del cliente para hacer que los archivos del lado del cliente sean accesibles en la sesión del lado del host. La comparación entre la asignación de unidades del cliente y la redirección de carpetas del cliente es la siguiente:

Si	Entonces
habilita solo la asignación de unidades del cliente en el host (VDA),	los volúmenes completos del lado del cliente se asignan automáticamente a las sesiones del subdirectorio **ctxmnt** del directorio principal.
habilita la redirección de carpetas del cliente en el host (VDA) y el usuario la configura en el dispositivo del usuario (cliente),	se redirige la parte del volumen local especificada por el usuario.

Habilitar asignación de unidades del cliente

Para habilitar la asignación de unidades del cliente, establezca la directiva **Redirección de unidades del cliente** en **Permitido** en Citrix Studio. Para obtener más información sobre la directiva, consulte Configuraciones de directiva de Redirección de archivos.

Habilitar la redirección de carpetas del cliente y especificar qué carpetas redirigir

Para habilitar la redirección de carpetas del cliente, ejecute el siguiente comando en el VDA:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\Client
    Folder Redirection" -t "REG_DWORD" -v "CFROnlyModeAvailable" -d "0
    x00000001" --force
```

Para especificar qué carpetas se redirigirán desde el cliente a la sesión del servidor, siga estos pasos en el dispositivo del usuario:

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

1. Compruebe que está instalada la versión más reciente de la aplicación Citrix Workspace.
2. En el directorio de instalación de la aplicación Citrix Workspace, inicie **CtxCFRUI.exe**.
3. Seleccione el botón de opción **Personalizada** y agregue, modifique o quite carpetas.
4. Desconecte y vuelva a conectar sus sesiones para que la configuración tenga efecto.

Redirección de dispositivos USB

September 23, 2024

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 la redirección de dispositivos USB cuando la latencia de red es inferior a 100 milisegundos. No utilice la redirección de dispositivos USB cuando la latencia de red sea superior a 200 milisegundos.

La redirección de dispositivos USB incluye tres áreas principales de funcionalidad:

- Proyecto USB/IP de código abierto
- Módulo de sesión USB de Citrix
- Módulo de servicio USB de Citrix

Proyecto USB/IP de código abierto:

El proyecto USB/IP 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.

Linux VDA implementa la redirección de dispositivos USB basada en el proyecto USB/IP de código abierto y reutiliza el controlador de kernel y las bibliotecas de modos de usuario de USB/IP. Sin embargo, todas las transferencias de datos USB que se realizan entre Linux VDA y la aplicación Citrix Workspace se encapsulan en el protocolo USB de Citrix ICA.

Módulo de sesión USB de Citrix:

El módulo de sesión USB de Citrix actúa como puente de comunicación entre el módulo del kernel de USB/IP y la aplicación Citrix Workspace.

Módulo de servicio USB de Citrix:

El módulo de servicio USB de Citrix administra todas las operaciones en dispositivos USB, como, por ejemplo, conectar o desconectar dispositivos USB.

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

Cómo funciona la redirección de dispositivos 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 desde el cliente.

Dispositivos USB admitidos

> **Sugerencia:**
>
> Ahora se pueden usar puertos USB 3.0. Puede insertar dispositivos USB 3.0 en puertos USB 3.0 de un dispositivo cliente.

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:

Dispositivos de almacenamiento USB	VID:PID	Sistema de archivos
`Netac Technology Co., Ltd`	0dd8:173c	FAT32, NTFS
`Kingston Datatraveler 101 II`	0951:1625	FAT32, NTFS
`Kingston Datatraveler GT101 G2`	1567:8902	FAT32, NTFS
`SanDisk SDCZ80 flash drive`	0781:5580	FAT32, NTFS
`WD HDD`	1058:10B8	FAT32, NTFS
`Toshiba Kingston DataTraveler 3.0 USB device`	0930:6545	FAT32, NTFS
`Taiwan OEM – OBSOLETE VendorCo ProductCode Disk 2.0`	FFFF:5678	FAT32, NTFS

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

Dispositivos de almacenamiento USB	VID:PID	Sistema de archivos
TD-RDF5A Transcend USB device	8564:4000	FAT32, NTFS

> **Nota:**
>
> Para usar NTFS en Amazon Linux 2, CentOS, RHEL, Rocky Linux y SUSE, habilite primero la compatibilidad con NTFS en estas distribuciones.

Mouse 3D por USB	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

Escáner USB	VID:PID
Epson Perfection V330 photo	04B8: 0142

Yubico USB	VID:PID
Yubico YubiKey OTP+FIDO+CCID - Keyboard, HID	1050:0407

Cámara web USB	VID:PID
Logitech composite USB device – WebCam, Audio	0460:0825

Configurar la redirección de dispositivos USB

Instalar o compilar el módulo del kernel de USB/IP (solo para CentOS, RHEL y Rocky Linux)

Linux VDA usa USB/IP como controlador de hosts virtuales para la redirección de dispositivos USB. Dado que, en la mayoría de los casos, el módulo del kernel de USB/IP se publica con la versión 3.17 del kernel de Linux y versiones posteriores, no es necesario compilar el módulo del kernel de forma

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

predeterminada. Sin embargo, el módulo del kernel de USB/IP no está disponible para CentOS, RHEL ni Rocky Linux. Para utilizar la redirección de dispositivos USB con estas distribuciones de Linux, debe instalar o compilar el módulo del kernel de USB/IP. Descargue e instale USB/IP en https://pkgs.org/download/kmod-usbip según su distribución de Linux.

Establecer directivas de redirección de dispositivos 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 de dispositivos USB para Linux VDA, configure la directiva y las reglas siguientes:

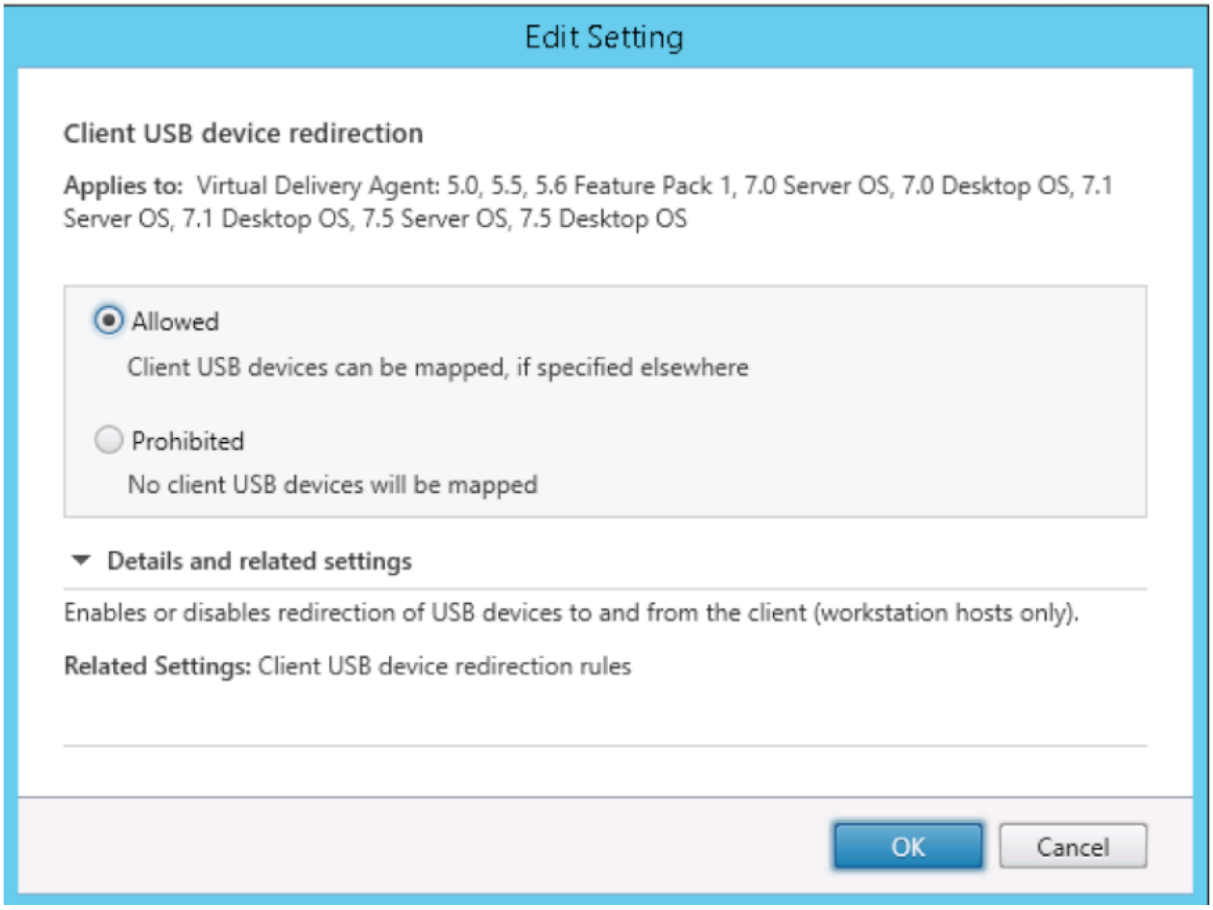
- Directiva de Redirección de dispositivos USB del cliente
- Reglas de redirección de dispositivos USB del cliente

Habilitar la redirección de dispositivos USB En Citrix Studio, habilite (o inhabilite) la redirección de dispositivos USB desde el cliente (solo para hosts de estación de trabajo).

En el diálogo **Modificar configuración**:

1. Seleccione la opción **Permitido**.
2. Haga clic en **Aceptar**.

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

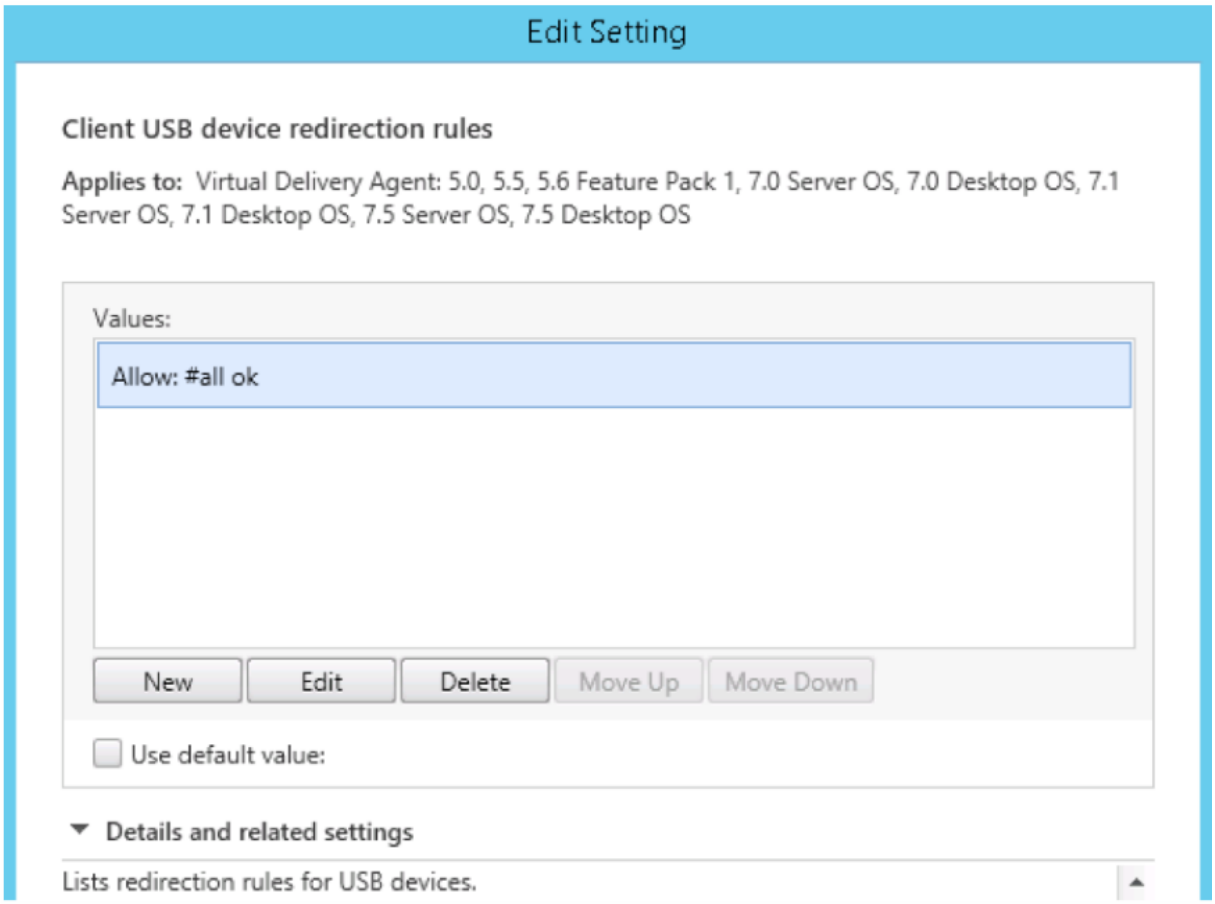


Configurar reglas de redirección de dispositivos USB Después de habilitar la directiva de redirección USB, configure las reglas de redirección mediante Citrix Studio. Para ello, deberá especificar los dispositivos permitidos (o denegados) en el Linux VDA.

En el cuadro de diálogo **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 dispositivos USB genéricos, consulte Citrix Generic USB Redirection Configuration Guide.

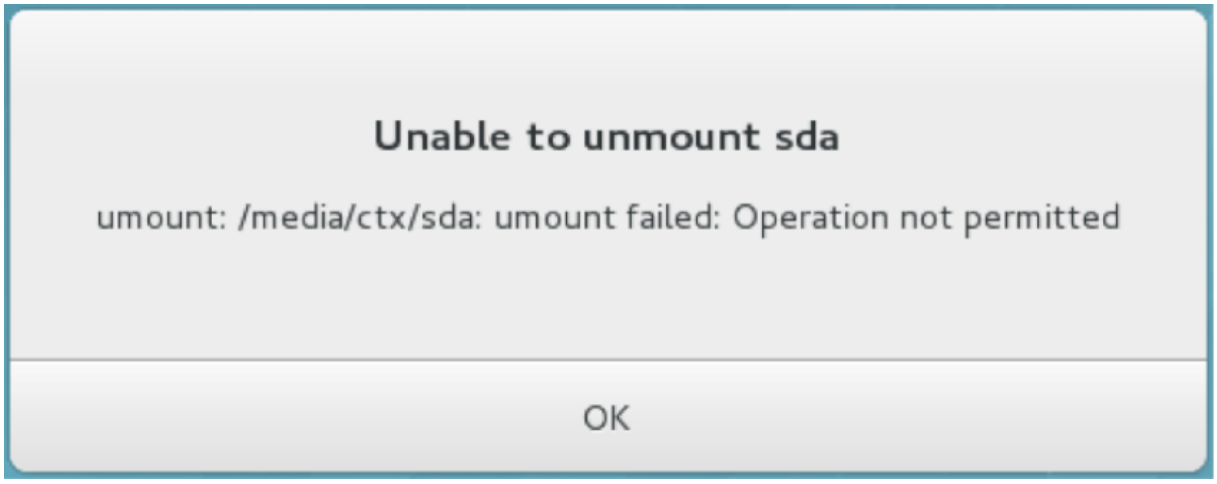
Solucionar problemas de redirección de dispositivos USB

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.

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



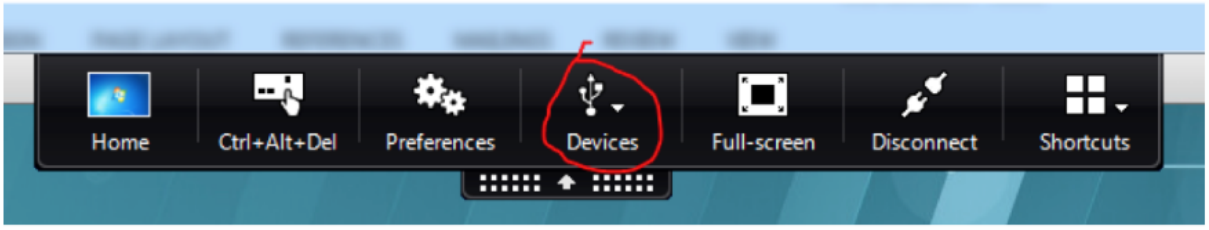
Se pierde el archivo cuando se detiene la redirección de un disco USB

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 **sync** en un terminal para vaciar datos en el disco antes de detener la redirección USB.

No hay ningún dispositivo en la barra de herramientas de la aplicación Citrix Workspace

En algunos casos, puede que no aparezcan dispositivos en la barra de herramientas de la aplicación Citrix Workspace, lo que indica que no se está realizando la redirección USB.



Si tiene este problema, compruebe lo siguiente:

- La directiva está configurada para permitir la redirección de dispositivos USB.
- Se está ejecutando el módulo del servicio USB de Citrix.

Si la directiva no está configurada correctamente, consulte la sección Establecer directivas de redirección de dispositivos USB de este artículo y corríjala como corresponda.

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

Si el módulo del servicio USB de Citrix no se está ejecutando, complete estos pasos:

1. Compruebe si hay un módulo de kernel de USB/IP disponible en su distribución de Linux mediante este comando:

```
modinfo usbip-core
```

2. Si el resultado se muestra de la siguiente manera, instale o compile el módulo del kernel de USB/IP según su distribución de Linux:

```
modinfo: ERROR: Module usbip-core not found.
```

   - Para Amazon Linux 2, CentOS, RHEL y Rocky Linux, consulte la sección Instalar o compilar el módulo del kernel de USB/IP de este artículo.
   - Para SUSE, descargue e instale el paquete USB/IP desde https://software.opensuse.org/package/usbip.
   - Para Ubuntu/Debian, complete estos pasos para compilar e instalar el módulo del kernel de USB/IP:

     a) Descargue el código fuente del módulo del kernel de USB/IP.

     Vaya al repositorio del núcleo de Linux en https://github.com/torvalds/linux/tree/master/drivers/usb/usbip, seleccione la etiqueta de la versión del núcleo de Linux de destino (v4.15 o una posterior) y obtenga un enlace como https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip.

     Vaya a DownGit e introduzca el enlace anterior para crear un enlace de descarga desde el que descargar el código fuente de USB/IP.

     b) Descomprima el archivo de origen con estos comandos:

```
unzip ${
 USBIP_SRC }
 .zip

cd usbip
```

     c) Modifique el archivo **Makefile** de la siguiente manera:

```
# SPDX-License-Identifier: GPL-2.0

ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG

obj-$(CONFIG_USBIP_CORE) += usbip-core.o

usbip-core-y := usbip_common.o usbip_event.o

obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o

```

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

```
vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o

#obj-$(CONFIG_USBIP_HOST) += usbip-host.o

#usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o

#obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o

#usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.
   o vudc_transfer.o vudc_main.o
```

d) Compile el código fuente:

```
apt-get install linux-headers-`uname -r`

make -C /lib/modules/`uname -r`/build M=$PWD
```

e) Instale el módulo del kernel de USB/IP:

```
cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
```

f) Reinicie el servicio **ctxusbsd** para cargar el módulo del kernel de USB/IP:

```
service ctxusbsd restart
```

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

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.

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

> **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.

Teclado

March 27, 2023

Esta sección contiene estos temas:

- 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

March 27, 2023

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.

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

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

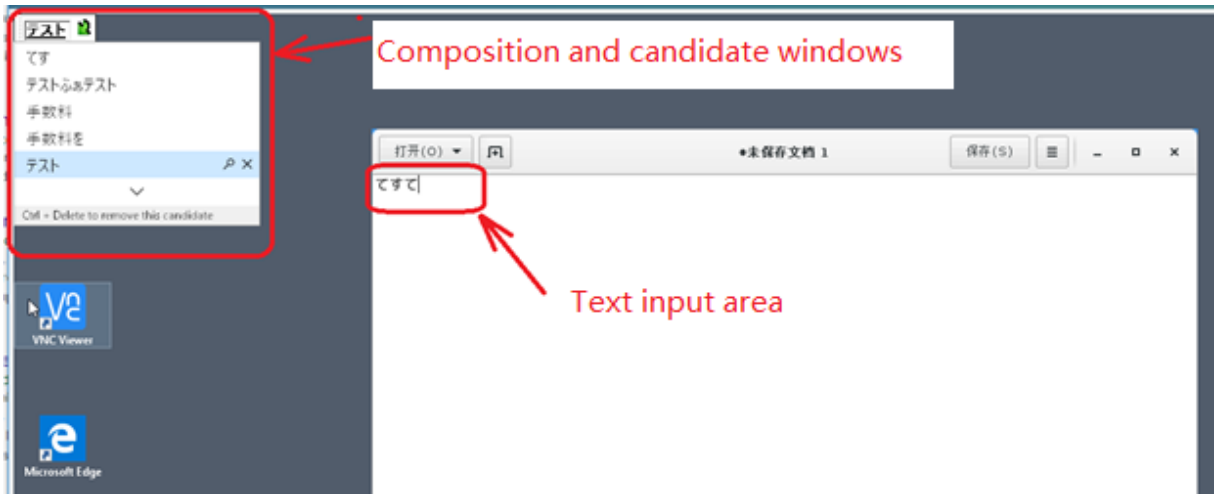
- Es necesario hacer doble clic en una celda en una hoja de cálculo de Google para poder usar el IME del cliente para introducir caracteres en la celda.
- El IME del cliente no se inhabilita automáticamente en los campos de contraseña.
- La interfaz de usuario de IME no sigue al cursor en el área de entrada.

Sincronización de la interfaz de usuario IME del cliente

March 27, 2023

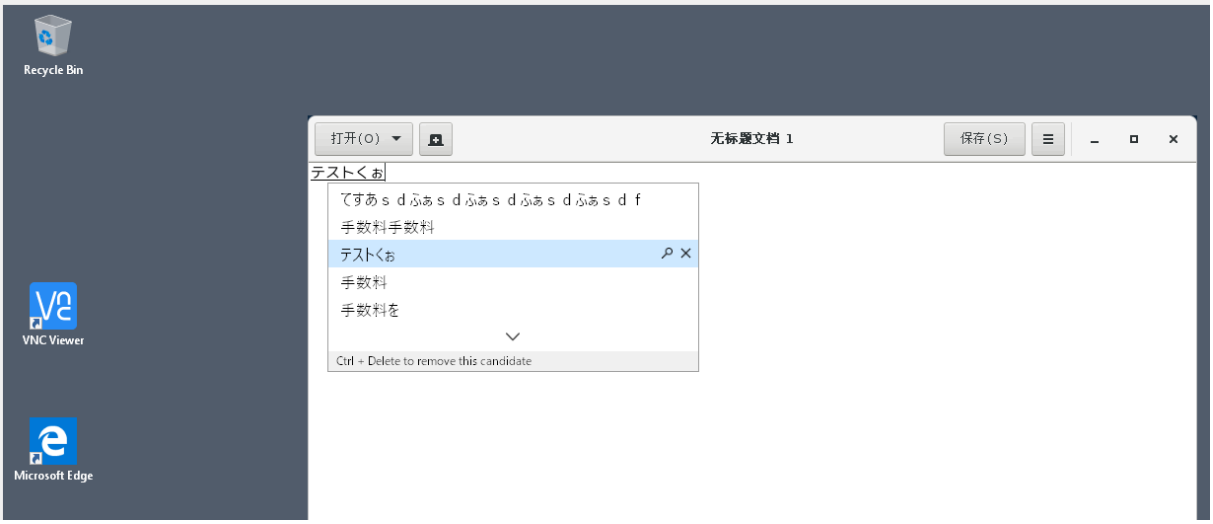
Información general

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`.

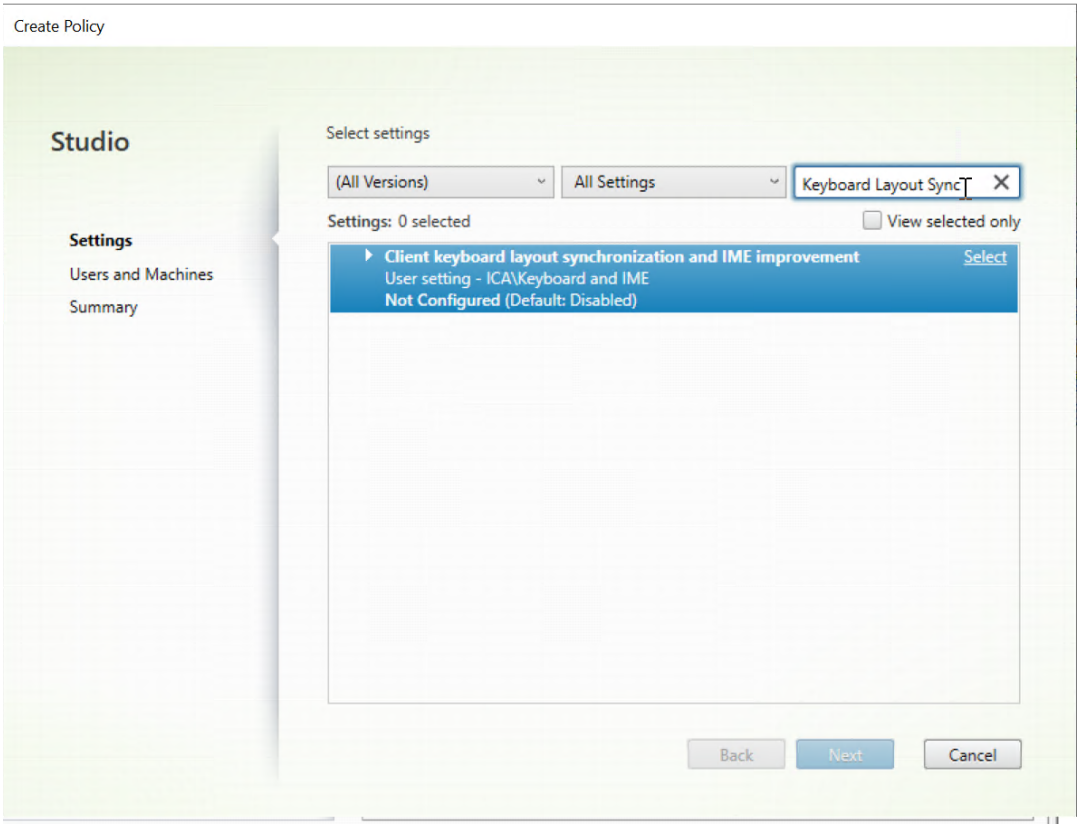
> **Nota:**
>
> La directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** tiene prioridad sobre la configuración del Registro y se puede aplicar a los objetos de usuario y máquina especificados o a todos los objetos del sitio. La configuración del Registro en un Linux VDA es-

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

> pecífico se aplica a todas las sesiones de ese VDA.

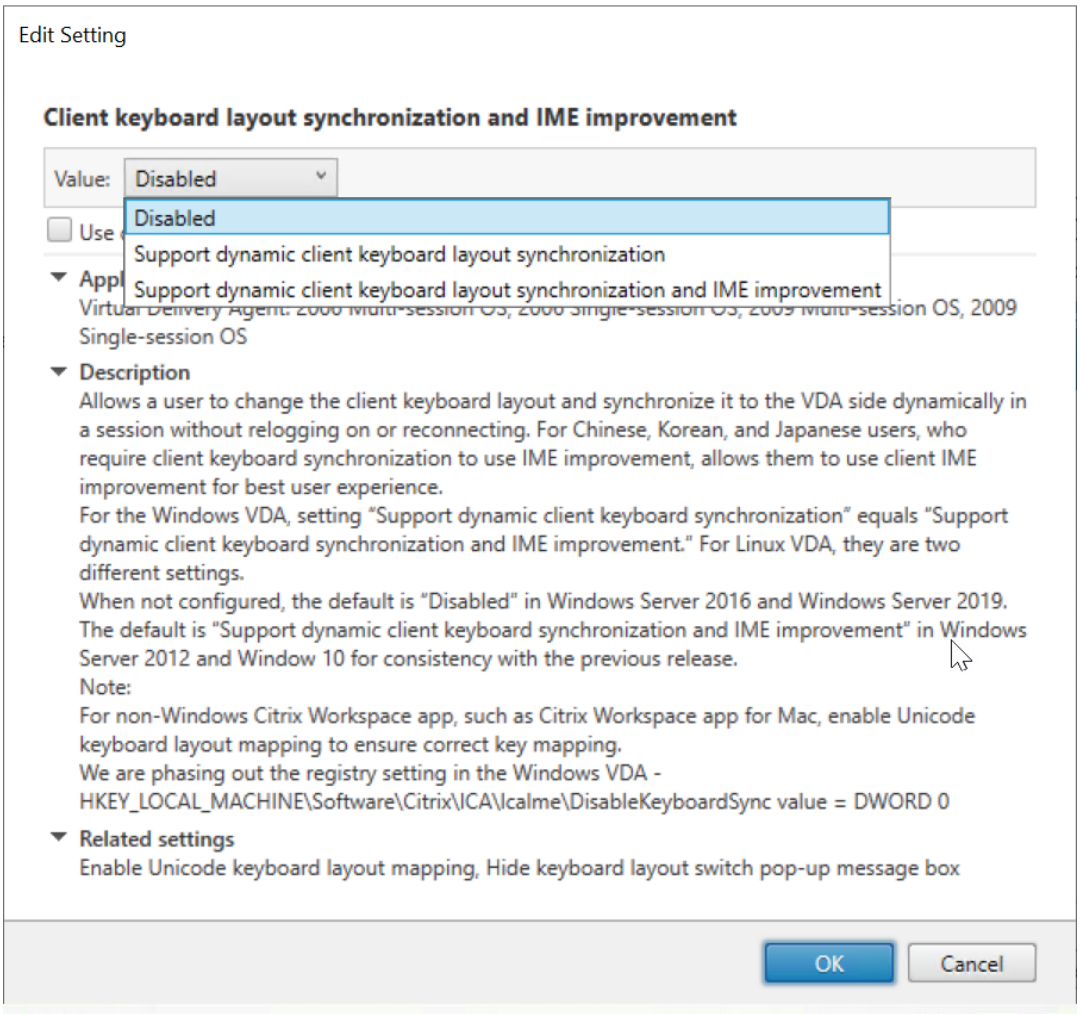
- Establezca la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** para habilitar o inhabilitar la función de sincronización de la interfaz de usuario del IME del cliente:

  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**.



  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"
```

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"
```

Sincronización de la distribución de teclado dinámico

March 27, 2023

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`.

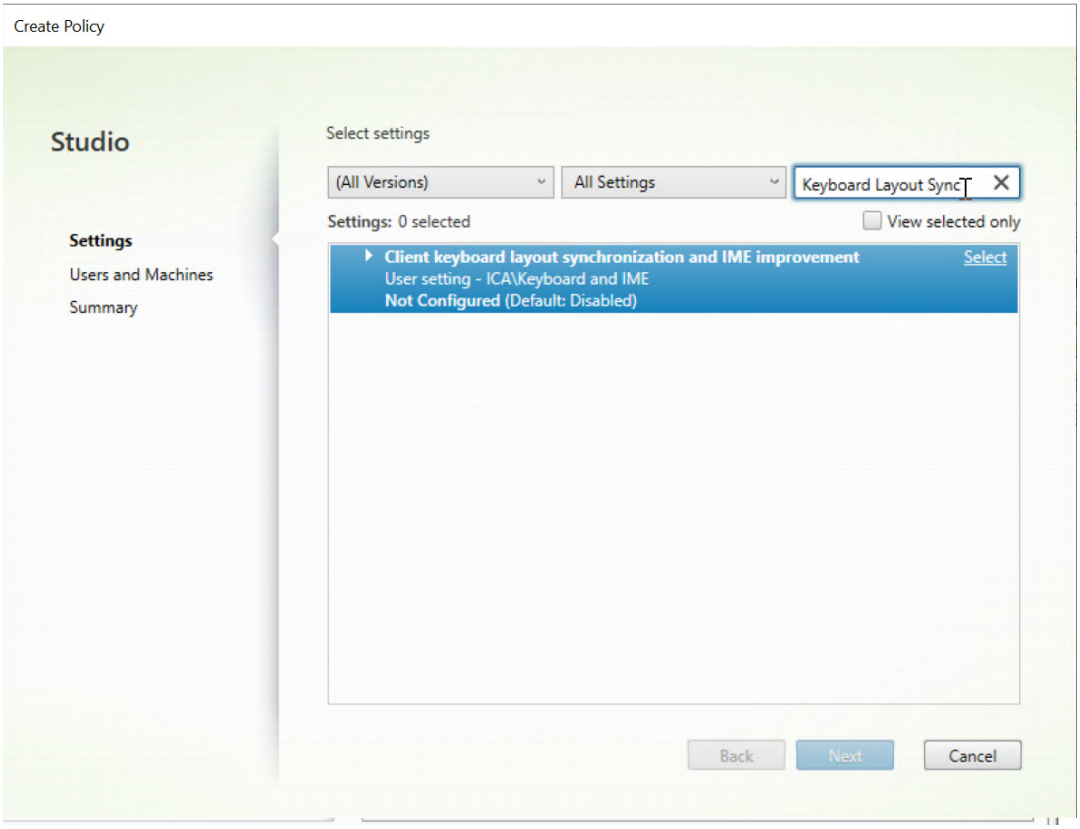
> **Nota:**
>
> La directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** tiene prioridad sobre la configuración del Registro y se puede aplicar a los objetos de usuario y máquina

© 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.

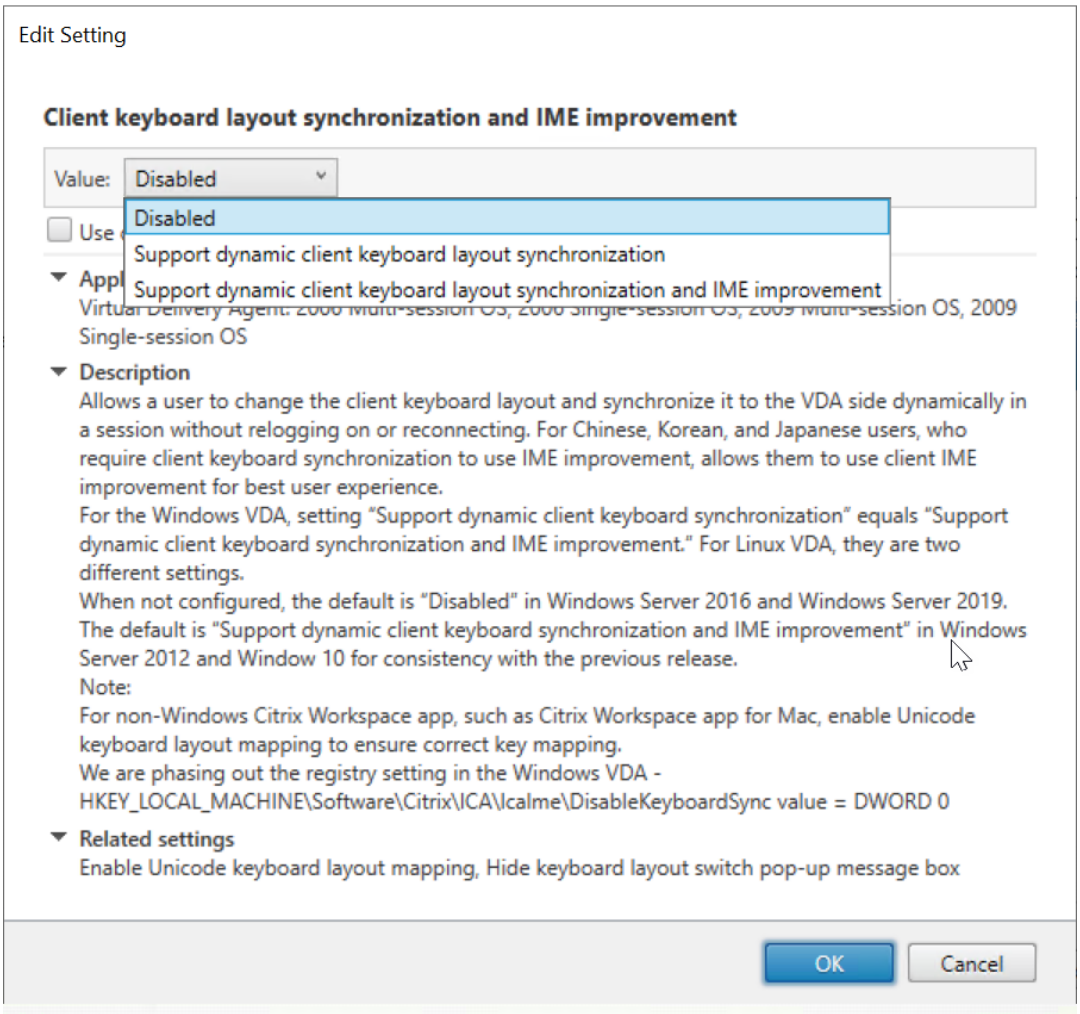
- Establezca la directiva **Sincronización de la distribución del teclado del cliente y mejora de IME** para habilitar o inhabilitar la función de sincronización dinámica de la distribución del teclado:

  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"
```

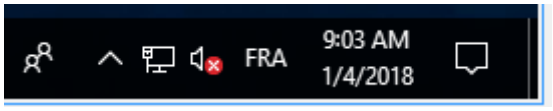
Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\LanguageBar" -v "
    SyncKeyboardLayout" -d "0x00000000"
```

Uso

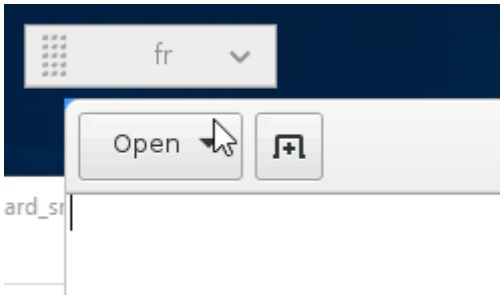
Con esta función habilitada, cuando la distribución del teclado cambia en el dispositivo cliente durante una sesión, también cambia la distribución del teclado de la sesión.

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:

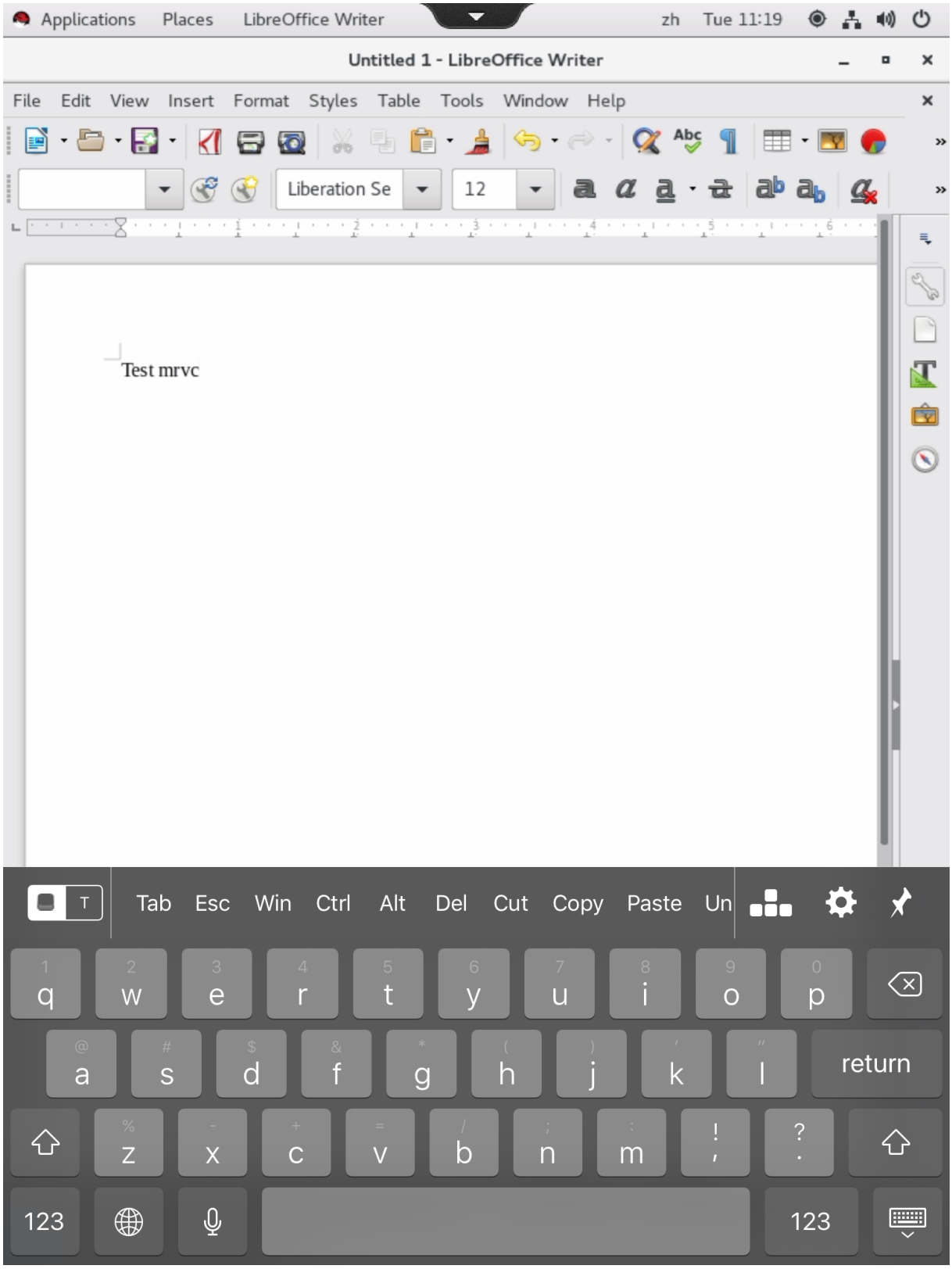
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Teclado en pantalla

March 27, 2023

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 se puede usar 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"
```

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
```

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"
```

> **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.
- 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.

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

- 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

March 27, 2023

A partir de Linux VDA 1.4, Citrix ha comenzado a admitir aplicaciones publicadas. Los usuarios pueden acceder a una aplicación Linux sin el entorno de escritorio Linux.

No obstante, la barra de idioma nativo de Linux VDA no estaba disponible para la aplicación publicada porque esa barra está integrada en el entorno de escritorio Linux. En consecuencia, los usuarios no podían introducir texto en un idioma que necesitara IME, como coreano, japonés o chino. Además, los usuarios tampoco podían cambiar de distribuciones de teclado durante una sesión de aplicación.

Para solucionar esos problemas, esta función ofrece una barra de idiomas para las aplicaciones publicadas que acepten la entrada de texto. La barra de idiomas permite a los usuarios seleccionar un IME en el lado del servidor y alternar entre diferentes distribuciones de teclado durante una sesión de aplicación.

Configuración

Puede usar la utilidad **ctxreg** para habilitar o inhabilitar esta función (inhabilitada de manera predeterminada). Configurar la función en un servidor Linux VDA determinado significa que esa función se aplicará a todas las aplicaciones publicadas en ese VDA.

La clave de configuración es “HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar” y el tipo es DWORD.

Para habilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
    x00000001"
```

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

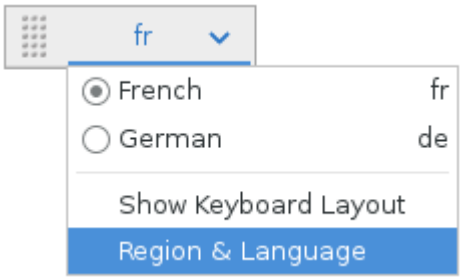
Para inhabilitar esta función, ejecute el comando:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
    x00000000"
```

Uso

El uso es bastante sencillo.

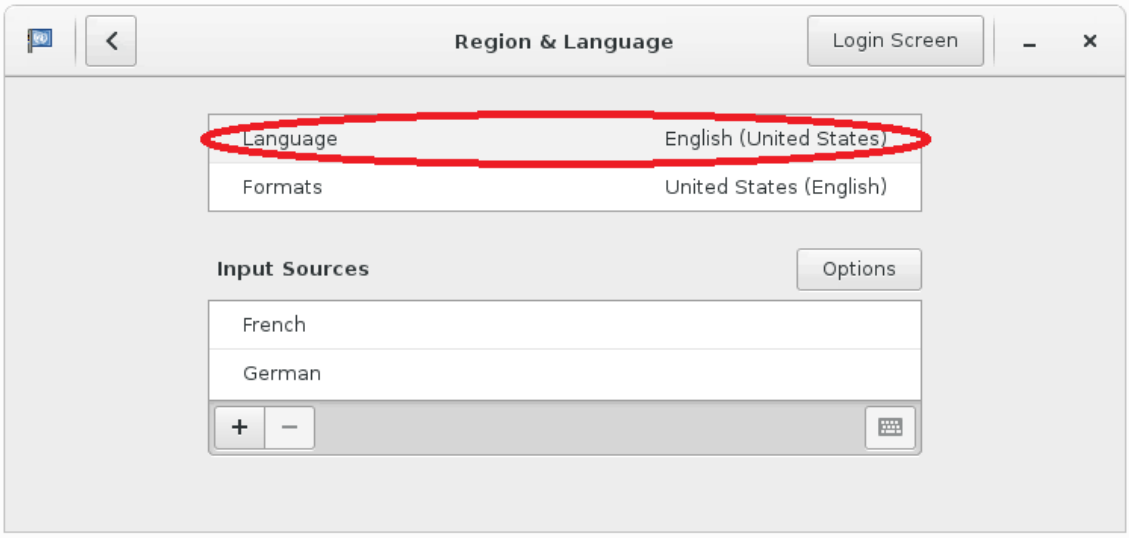
1. Habilite la función.
2. Acceda a una aplicación publicada que acepte la entrada de texto. Aparece una barra de idioma en la sesión, junto a la aplicación.
3. En el menú desplegable, seleccione **Region & Language** (Región e idioma) para agregar el idioma pertinente (origen de entrada).



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

March 27, 2023

Esta sección contiene estos temas:

- Funciones de audio
- Redirección de contenido del explorador web
- Compresión de vídeo de cámara web HDX

Funciones de audio

August 8, 2023

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.

Redirección de contenido del explorador web

March 27, 2023

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.

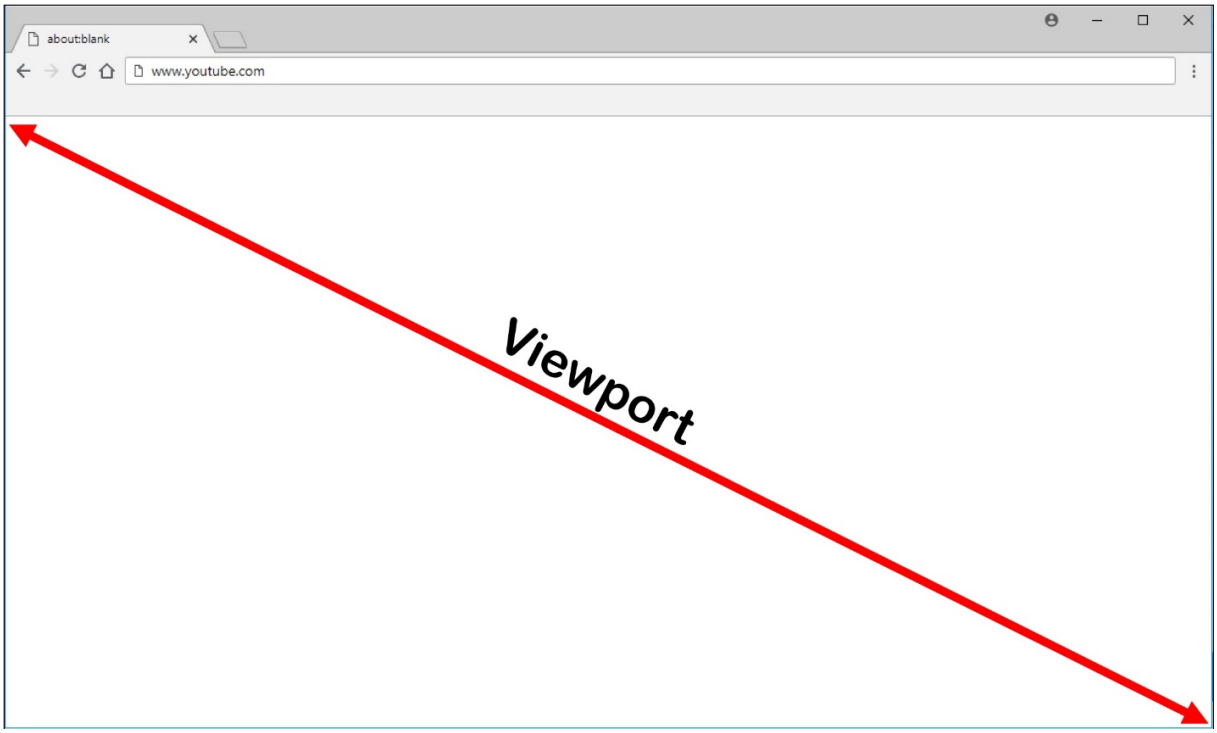
> **Nota:**
>
> Mediante una lista de permitidos, puede especificar qué páginas web se redirigen al lado del cliente. A la inversa, mediante una lista de bloqueados, puede especificar qué páginas web no se redirigen al lado del cliente.

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.

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,

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

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

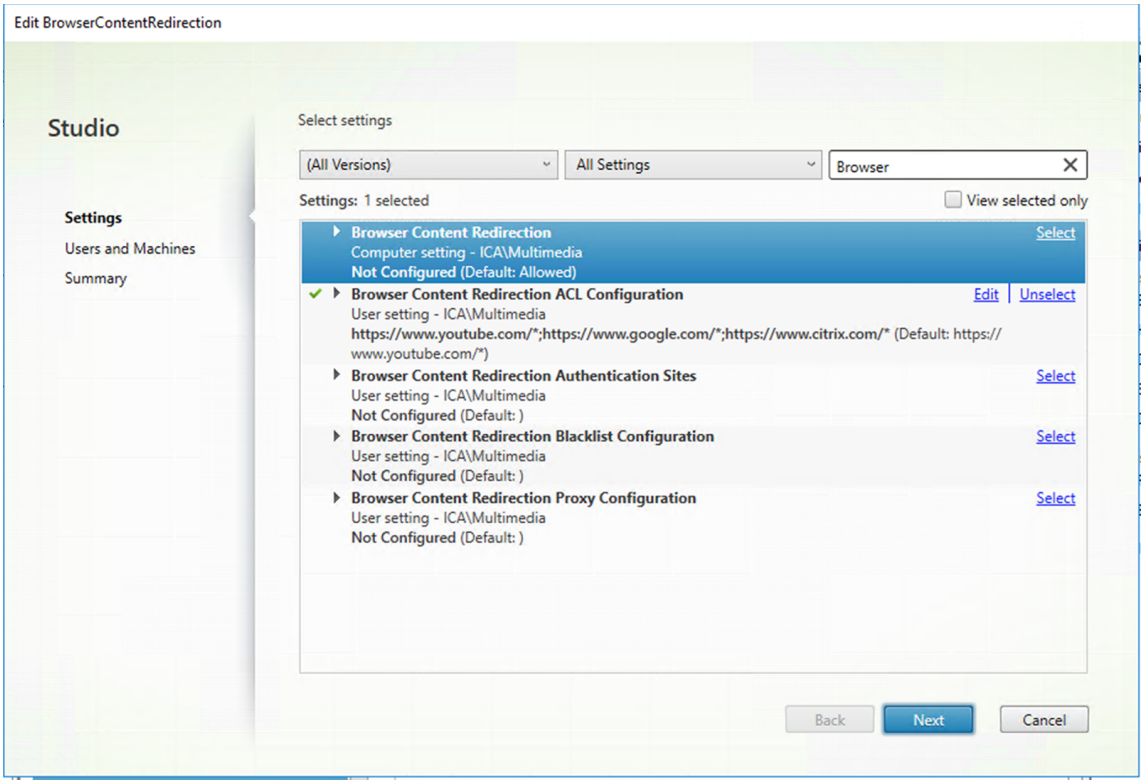
Linux VDA:

- Explorador en el VDA: Google Chrome v66 o una versión posterior con la extensión de redirección de contenido de explorador Citrix agregada

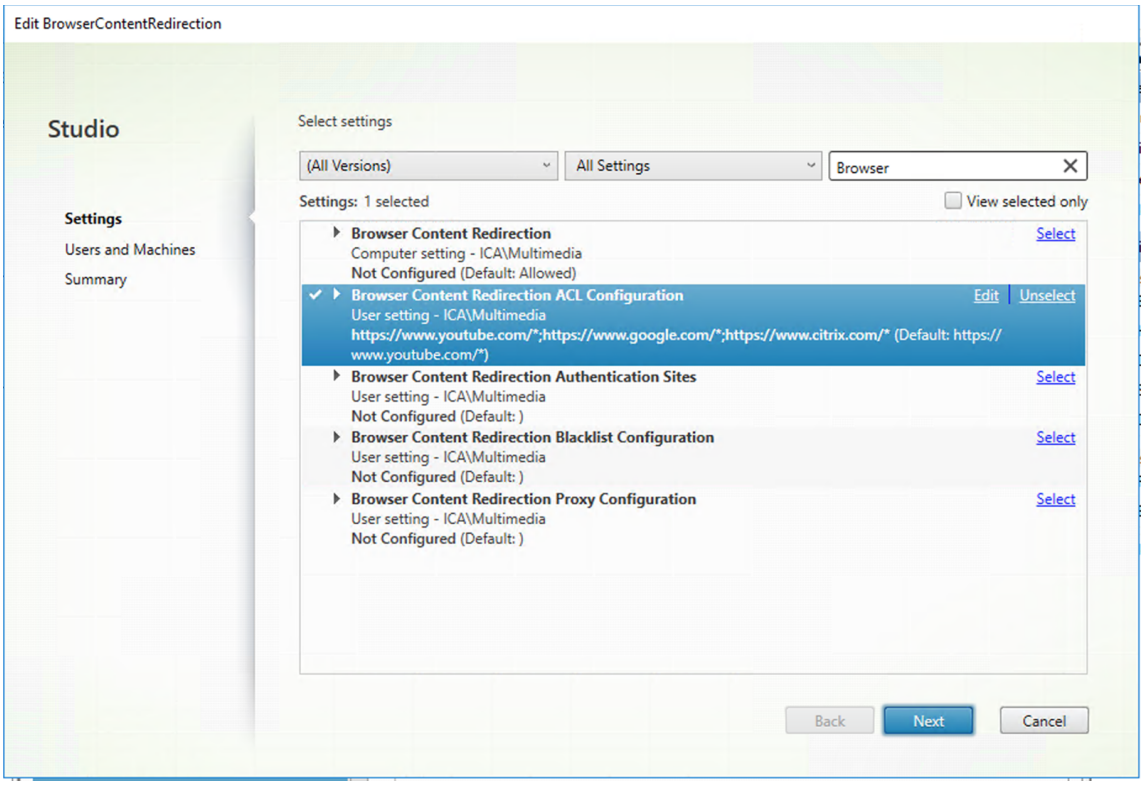
Configurar la redirección de contenido de explorador

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.

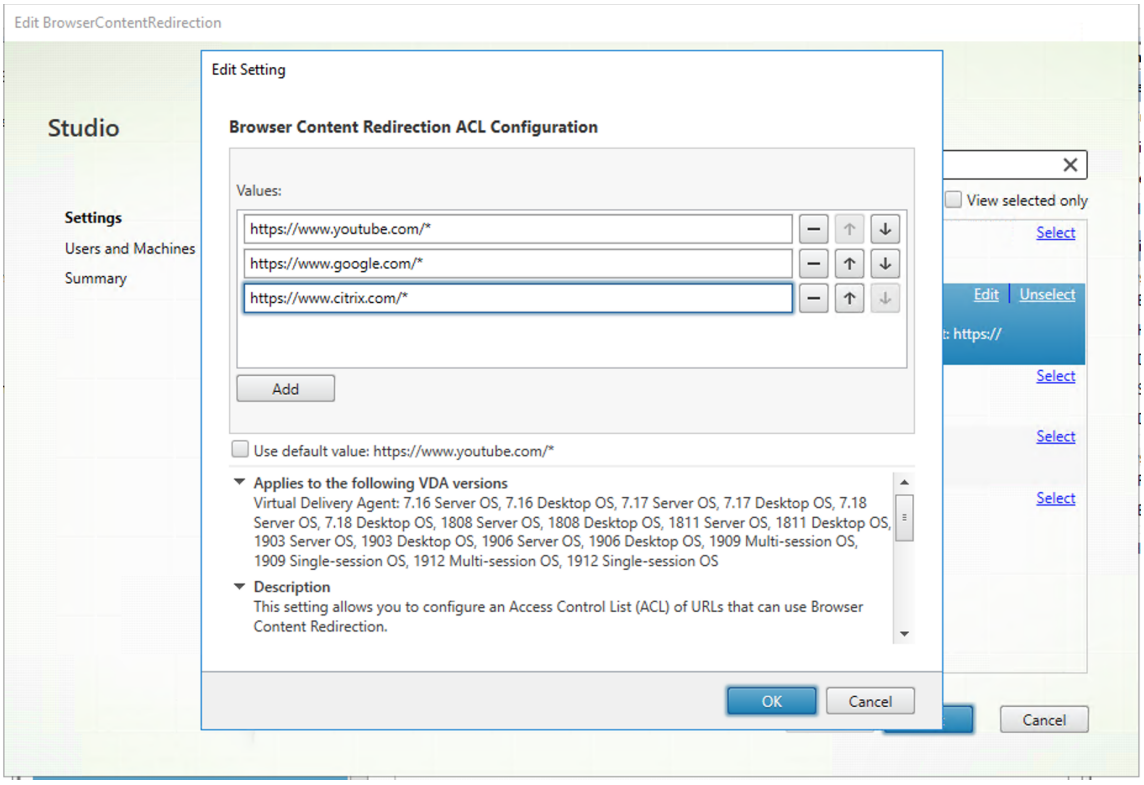
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



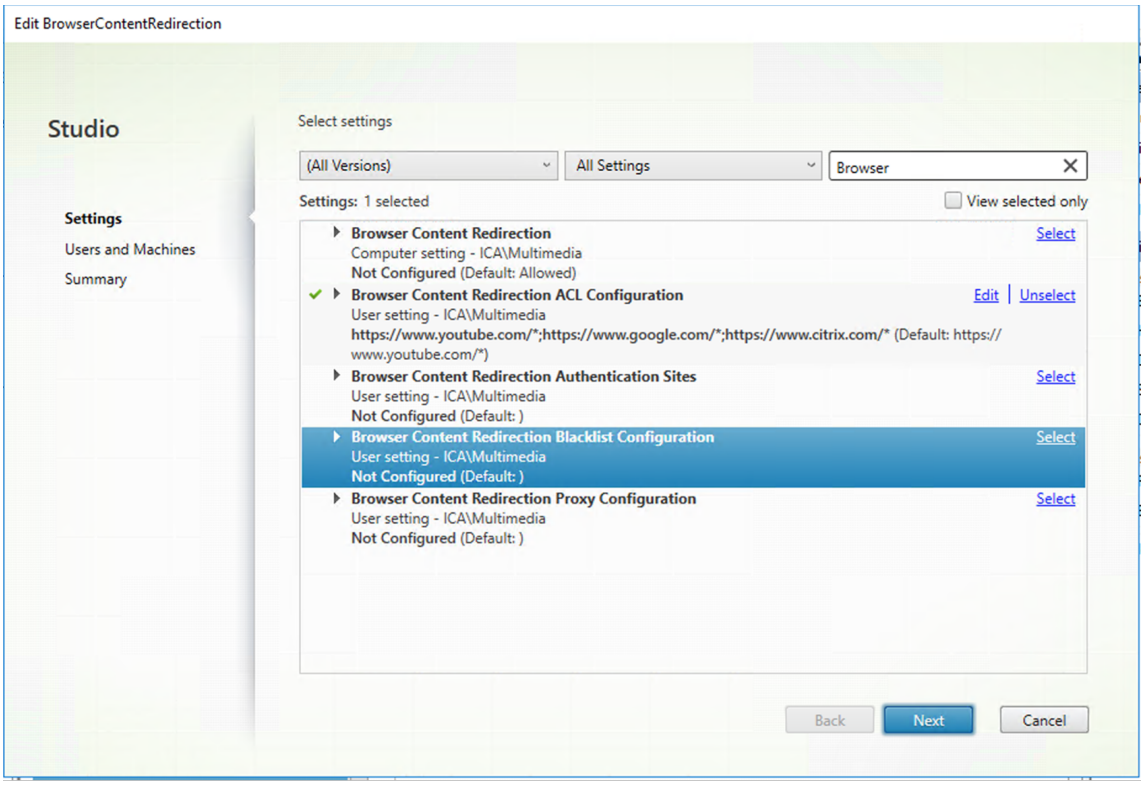
El parámetro **Configuración de lista ACL para redirección de contenido del explorador web** especifica una lista de direcciones URL que pueden utilizar la redirección de contenido de explorador.



© 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.

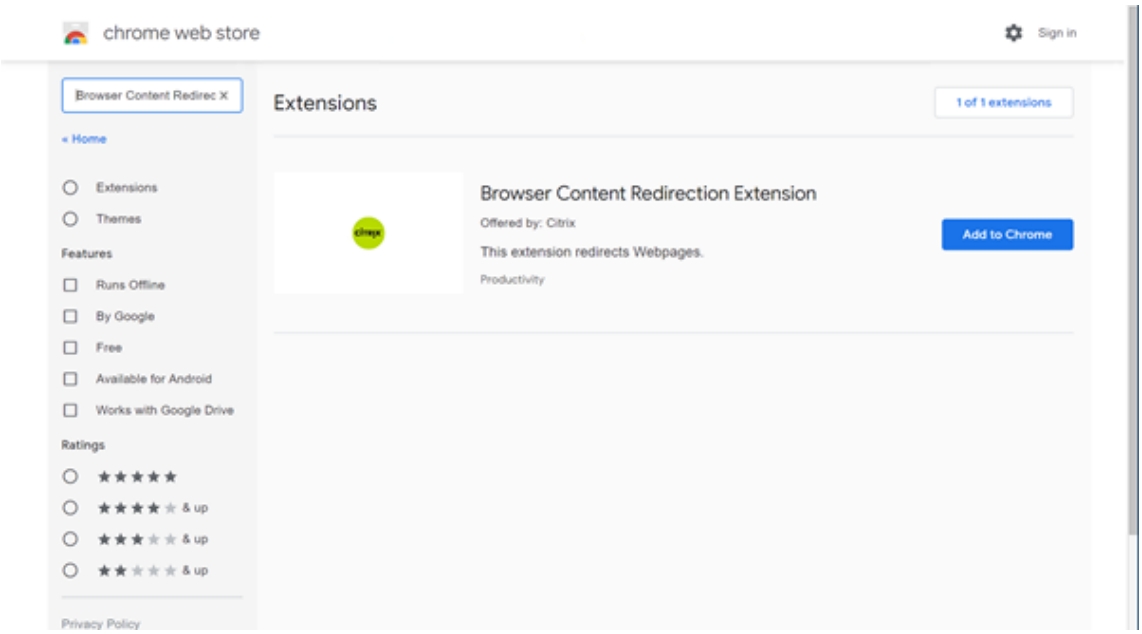


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

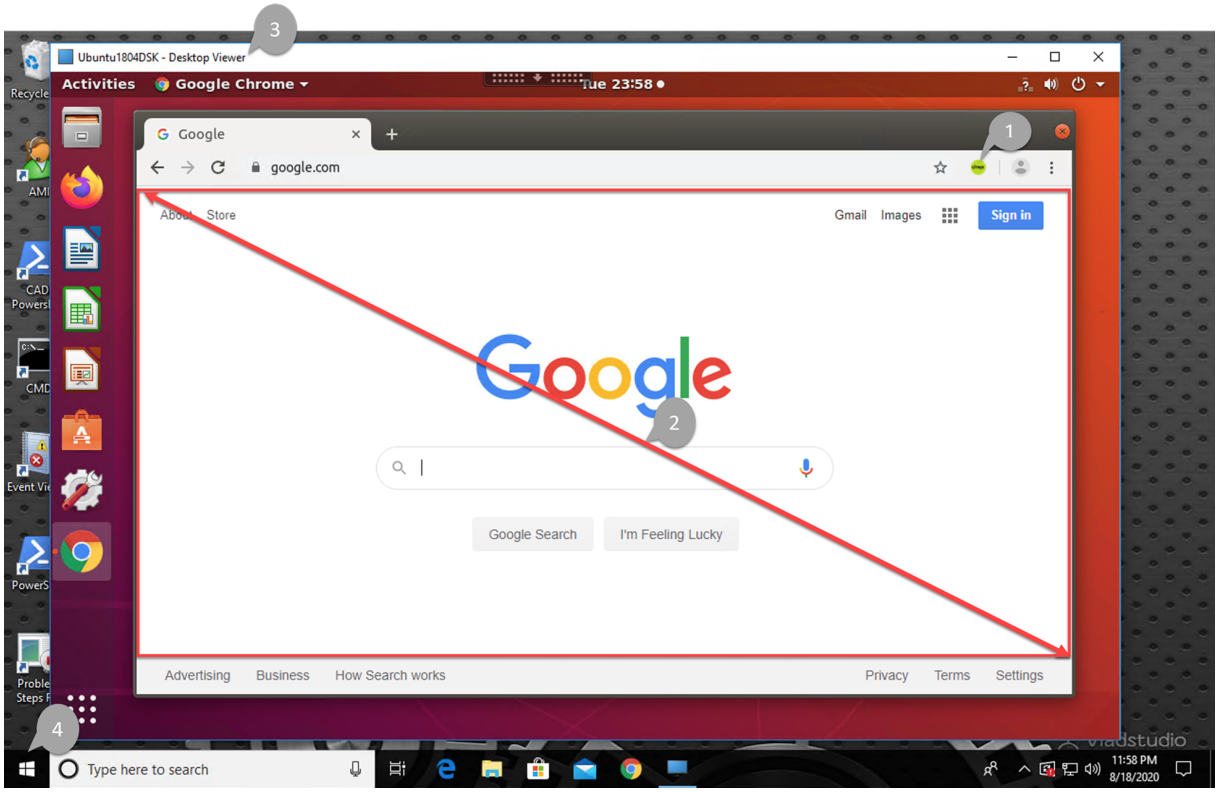
> **Importante:**
>
> La extensión no es necesaria en el cliente. Agréguela solo al VDA.
>
> Las extensiones de Chrome se instalan basándose en el usuario. No es necesario actualizar una imagen maestra para agregar o eliminar una extensión.



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:

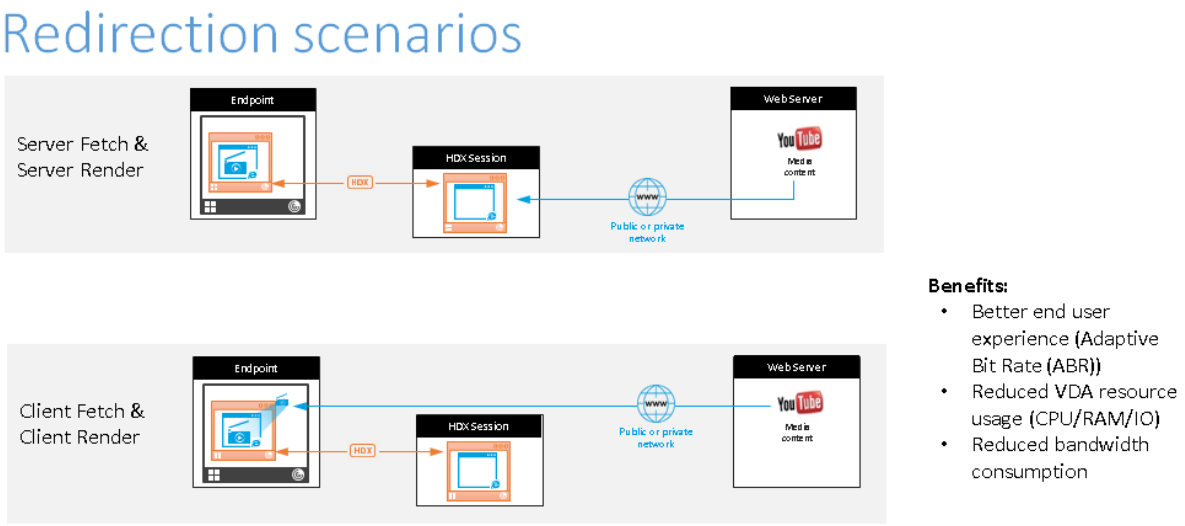
   - Verde: Activo y conectado
   - Gris: No activo/inactivo en la ficha actual
   - Rojo: No funciona

2. Ventanilla generada en el cliente o integrada en el escritorio virtual
3. Linux VDA
4. Cliente Windows

Casos 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

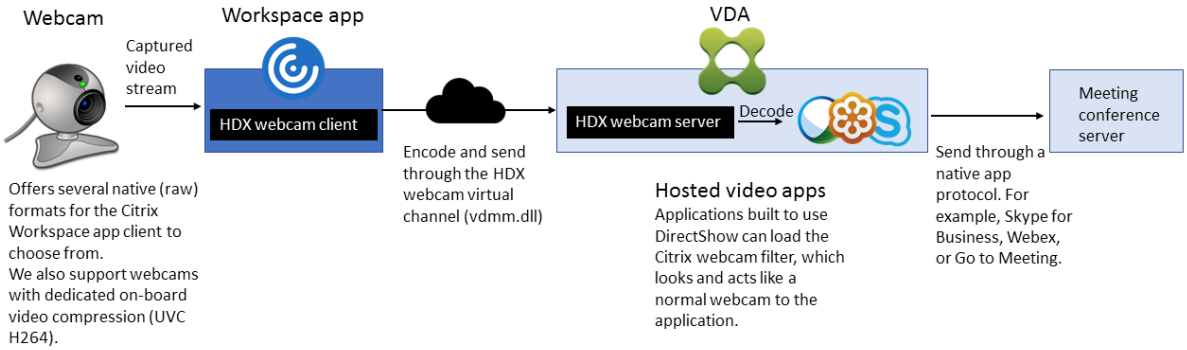
Los usuarios de aplicaciones de videoconferencia que se ejecutan en sesiones de Linux VDA ahora pueden usar sus cámaras web con compresión de vídeo HDX. Esta función está activada de forma

© 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.

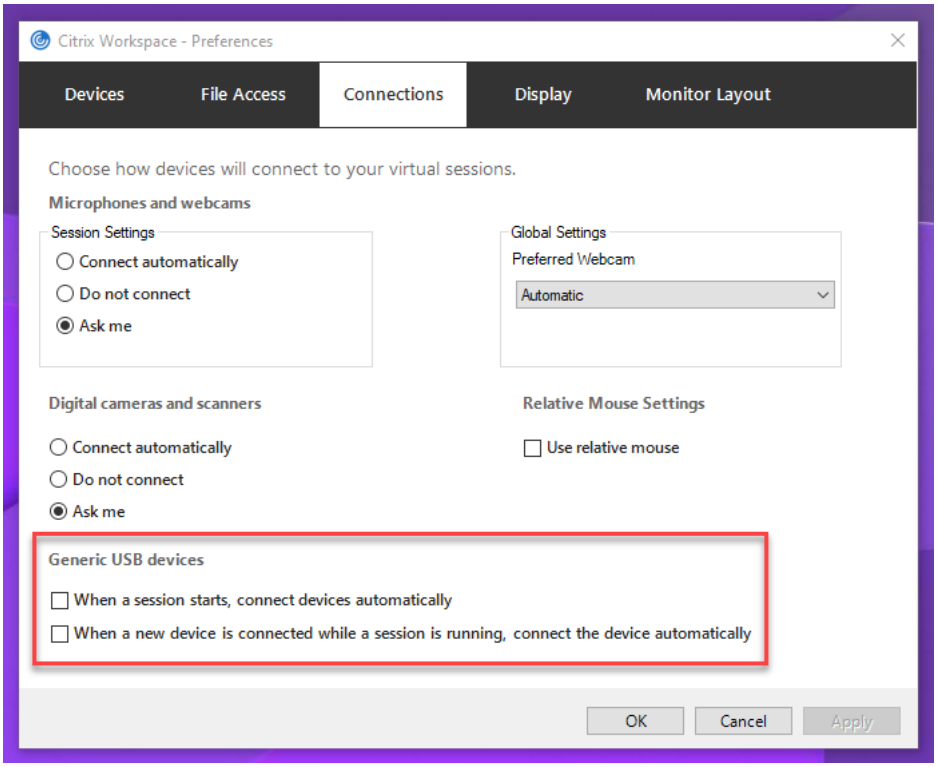
El cliente gestiona la comunicación con la cámara web. El cliente envía el vídeo solo al servidor que puede mostrarlo correctamente. El servidor no trata directamente con la cámara web, pero su integración le ofrece la misma experiencia en el escritorio que un tratamiento directo. La aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mejor capacidad de recuperación en conexiones WAN.



Nota:

- La función no está disponible para las máquinas de Azure porque el módulo del kernel **videodev** del que depende la función no está en las máquinas de Azure.
- La 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.



Aplicación Citrix Workspace compatible

La compresión de vídeo de cámaras web de HDX admite las siguientes versiones de la aplicación Citrix Workspace:

Plataforma	Procesador
Aplicación Citrix Workspace para Windows	La aplicación Citrix Workspace para Windows admite la compresión de vídeo de 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.

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

Cámaras web probadas por completo

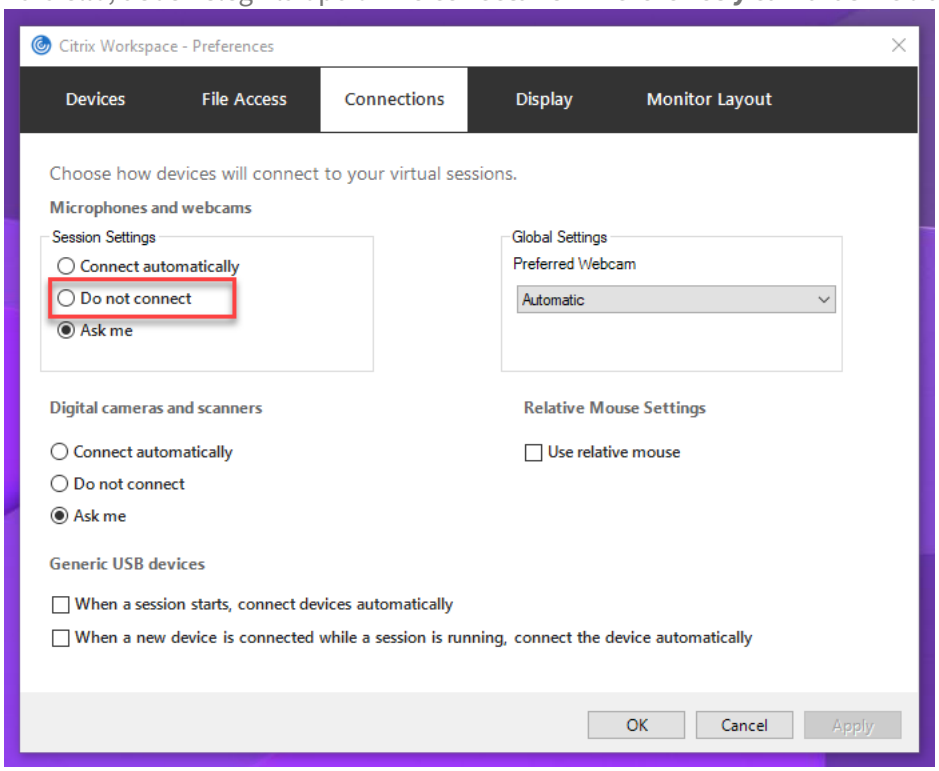
Las distintas cámaras web ofrecen diferentes velocidades de fotogramas y tienen diferentes niveles de brillo y contraste. Citrix utiliza las siguientes cámaras web para la validación inicial de funciones:

- 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.



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

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

tiene acceso a Internet, vaya al paso 3.

> **Nota:**
>
> Puede haber discrepancias de kernel entre `uname -r` y los encabezados del kernel. Esta discrepancia hace que el script ctxwcamcfg.sh falle. Para usar correctamente la compresión de vídeo de cámara web HDX, ejecute **sudo apt-get dist-upgrade**, reinicie el VDA y, a continuación, vuelva a ejecutar el script "ctxwcamcfg.sh".

Si el VDA se implementa en Debian, 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
```

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
```

El script ctxwcamcfg.sh ayuda a:

a) Instalar los programas `kernel-devel` y DKMS (Dynamic Kernel Module Support) en el 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.

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

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.

Linux VDA no unidos a ningún dominio

March 27, 2023

Información general

Los VDA no unidos a ningún dominio eliminan la necesidad de unir los VDA a dominios de Active Directory para la autenticación de VDA y usuario. Al crear un VDA no unido a ningún dominio, se genera un par de claves público-privadas para registrar el VDA en el plano de control de la nube. Por lo tanto, ya no es necesario unirse a un dominio de Active Directory. Cuando un usuario inicia una sesión desde un VDA que no está unido a ningún dominio, el VDA crea una cuenta de asignación local con el nombre de usuario que el usuario utiliza para iniciar sesión en la aplicación Citrix Workspace. El VDA asigna una contraseña aleatoria que la cuenta de asignación local utiliza para el inicio de sesión único (SSO) y la reconexión de sesiones. Si se cambia la contraseña aleatoria, SSO y la reconexión de sesiones fallarán. Para inhabilitar SSO, consulte Autenticación sin SSO.

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

> **Importante:**
>
> - Los VDA que no están unidos a ningún dominio son compatibles con Citrix DaaS.
> - Su plano de control debe implementarse a través de Citrix DaaS.
> - Puede implementar VDA que no estén unidos a un dominio en una nube pública o en un centro de datos local. El plano de control de Citrix DaaS administra los VDA que no están unidos a un dominio.
> - Puede configurar Rendezvous V2 para omitir los Citrix Cloud Connectors. De lo contrario, debe instalar Cloud Connectors para conectar VDA a su plano de control.
> - Para crear VDA no unidos a ningún dominio, debe usar Machine Creation Services (MCS).
> - MCS no es compatible con servidores bare metal.

Funciones disponibles para Linux 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:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
    CreateWithUidGid" -d "0x00000001" --force
```

2. Especifique estos atributos en el script `/var/xdl/getuidgid.sh` de la ruta de instalación del VDA:

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.

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

Atributo	Obligatorio u opcional	Descripción
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

##############################################################################
#
# Citrix Virtual Apps & Desktops For Linux Script: Get uid and gid for the user
#
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#

export LC_ALL="en_US.UTF-8"

function get_uid_gid_for_user()
{

echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
echo "shell:/bin/sh"
 }


get_uid_gid_for_user $1
```

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

Autenticación sin SSO

De forma predeterminada, Linux VDA tiene habilitado el inicio de sesión único (SSO). Los usuarios inician sesión en la aplicación Citrix Workspace y en las sesiones de VDA con un conjunto de credenciales.
Para que los usuarios inicien sesión en sesiones de VDA con un conjunto diferente de credenciales, inhabilite el inicio de sesión SSO en Linux VDA. Para obtener más información, consulte Autenticación sin SSO.

Autenticación con Azure Active Directory

Los VDA no unidos a ningún dominio que se implementan en Azure se integran con el servicio de identidad de AAD para proporcionar autenticación de usuario. Para obtener más información, consulte Autenticación con Azure Active Directory.

Rendezvous V2

Los VDA que no están unidos a ningún dominio son compatibles con el uso de Rendezvous V2 para omitir los Citrix Cloud Connectors. Para obtener más información, consulte Rendezvous V2.

Crear Linux VDA no unidos a ningún dominio

Utilice MCS para crear Linux VDA no unidos a ningún dominio en Citrix DaaS. Para obtener más información, consulte Crear Linux VDA no unidos a ningún dominio.

Lista de directivas disponibles

March 27, 2023

Lista de directivas admitidas en Linux VDA

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Limitar el cliente del porta-papeles al tamaño de la trans-ferencia de la sesión	LimitClipboardTransferC2H	boolean	ICA	Inhabilitado (0)
Limitar la sesión del porta-papeles al tamaño de la trans-ferencia del cliente	LimitClipboardTransferH2C	boolean	ICA	Inhabilitado (0)

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Usar la hora local del cliente	UseLocalTimeOfClient	Unsigned	ICA/Control de zona horaria	Usar zona horaria del servidor
Cálculo del tiempo de retorno ICA	IcaRoundTripCheckEnable	Enumeration	ICA/Supervisión de usuario final	Habilitado (1)
Intervalo de cálculo del tiempo de retorno ICA	IcaRoundTripCheckInterval	Unsigned	ICA/Supervisión de usuario final	15
Cálculo del tiempo de retorno ICA para conexiones inactivas	IcaRoundTripCheckOnIdleSession	Enumeration	ICA/Supervisión de usuario final	Habilitado (0)

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Límite de ancho de banda global de la sesión	LimitOverallBw	UserBw	ICA\Ancho de banda	0
Límite de ancho de banda de redirección de sonido	LimitAudioBw	UserBw	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de sonido	LimitAudioBwPercent	UserBw	ICA\Ancho de banda	0

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Límite de ancho de banda de redirección de dispositivos USB del cliente	LimitUSBBw	Usuario	ICA\Ancho de banda	0
Porcentaje de ancho de banda de redirección de dispositivos USB del cliente	LimitUSBBwPercent	Usuario	ICA\Ancho de banda	0

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
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 predetermi-nado
Límite de ancho de banda de redi-rec-ción de archivos	LimitCdmBsu	Bsu	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redi-rec-ción de archivos	LimitCdmBsuPerc	BsuPerc	ICA\Ancho de banda	0

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Límite de ancho de banda de redirección de impresoras	LimitPrinterBandwidth	Entero	ICA\Ancho de banda	0
Porcentaje límite de ancho de banda de redirección de impresoras	LimitPrinterBandwidthPercent	Entero	ICA\Ancho de banda	0
Conexiones con WebSockets	AcceptWebSocketsConnections	Booleano	ICA\WebSockets	Inhabilitada

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Número de puerto de Web-Sockets	WebSocketsPort	Equipo	ICA\WebSockets	8008
Lista de servidores de origen de Web-Sockets de confianza	WSTrustedOriginServers	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 predetermi-nado
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	ReconnectUiTransparency	Equipo	ICA\Reconexión automática de clientes	Recomendado

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
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 predetermi-nado
Crear automáticamente la impresora universal de PDF	AutoCreateUniversalPrinter	Impresión		Inhabilitado (0)
Asignación y compatibilidad de controladores de impresora	DriverMappingList	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 predetermi-nado					
Redirección del porta-papeles del cliente	AllowClipboardRedir	Usuario	Portapapeles	Permitido (1)					
Redirección de dis-positivos USB del cliente	AllowUSBRedir	Usuario	USB	Prohibido (0)					
Reglas de redi-rec-ción de dis-posi-tivos USB del cliente	USBDeviceRules	Usuario	USB	”	**Reglas de redi-rec-ción de dis-posi-tivos USB del cliente**	USBDeviceRules	Usuario	USB	“\0” ”
Compresión de imá-genes en movimiento	MovingImageCompression	Usuario	Gráficos	Habilitado (1)					

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
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 predetermi-nado
Usar codificación por hardware para códec de vídeo	UseHardwareEncoding	Varios	Thinwire Video	Habilitado (1)
Permitir compresión sin pérdida visual	AllowVisualLossless	Varios	Thinwire Compression	Inhabilitado (0)
Optimizar para cargas de trabajo de gráficos 3D	OptimizeForGraphics	Varios	Thinwire	Inhabilitado (0)

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Profundidad de color preferida para gráficos simples	PreferredColorDepth	Usuario	Thinwire	24 bits por píxel (1)
Calidad de audio	SoundQuality	Usuario	Audio	Alto – Sonido de alta definición (2)
Redirección de micrófonos del cliente	AllowMicrophoneRedir	Usuario	Audio	Permitido (1)
Número máximo de sesiones	MaximumNumberOfSessions	Equipo	Administración de carga	250

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Tolerancia de inicios de sesión simultáneos	ConcurrentLogonTolerance	Entero	Administración de carga	2
Habilitar actualización automática de Controllers	EnableAutoUpdateOfControllers	Equipo	Configuración de Virtual Delivery Agent	Permitido (1)
Modo de actualización de la selección en el portapapeles	ClipboardSelectionUpdateMode	Portapapeles		

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Modo de actualización de la selección primaria	PrimarySelectionUpdateMode	UserInterface	Portapapeles	1
Calidad máxima de Speex	MaxSpeexQuality	Quality	Audio	5
Conectar automáticamente las unidades del cliente	AutoConnectDrives	UserDrives	Redirección de archivos/Asignación de unidades del cliente	Habilitado (1)
Unidades ópticas del cliente	AllowCdromDrive	UserDrives	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 predetermi-nado
Unidades fijas del cliente	AllowFixedDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades de disco flexible del cliente	AllowFloppyDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Unidades de red del cliente	AllowNetworkDrives	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)
Redirección de unidades del cliente	AllowDriveRedir	Usuario	Redirección de archivos/Asignación de unidades del cliente	Permitido (1)

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Acceso de lectura solamente a unidades del cliente	ReadOnlyMapped Drive	Usuario	Redirección de archivos/Asignación de unidades del cliente	Inhabilitado (0)
Presentación au-tomática del teclado	AllowAutoKeyboardPopUp	Usuario	VDA	Inhabilitado (0)
Permitir trans-ferencia de archivos entre es-crito-rio y cliente.	AllowFileTransfer	Usuario	Transferencia de archivos	Se per-mite
Descargar archivos desde el es-crito-rio	AllowFileDownload	Usuario	Transferencia de archivos	Se per-mite

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
Cargar archivos al escritorio	AllowFileUpload	Upload	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	Inhabilitado (0)

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

Directiva de Studio	Nombre de la clave	Tipo	Módulo	Valor predetermi-nado
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.

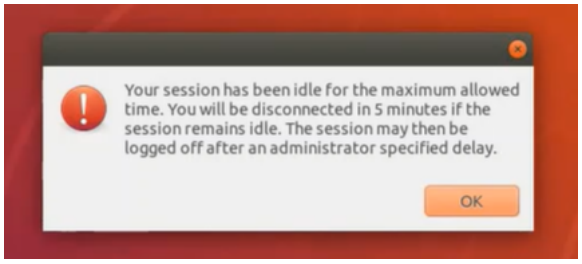
Puede usar los siguientes parámetros de directiva Citrix para configurar temporizadores de conexión de sesión en Citrix Studio:

- **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]

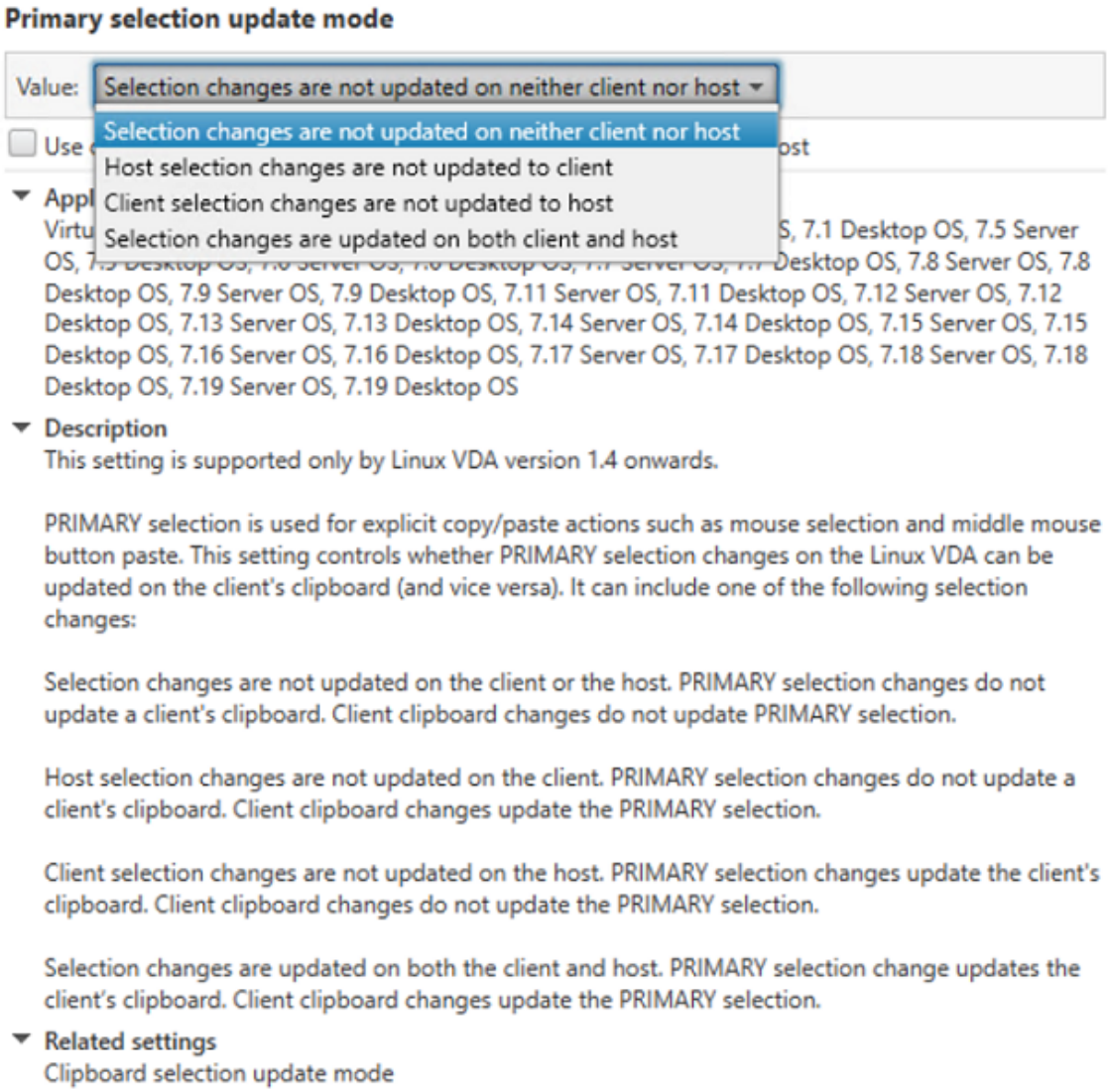
  Valor predeterminado: 3

© 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]

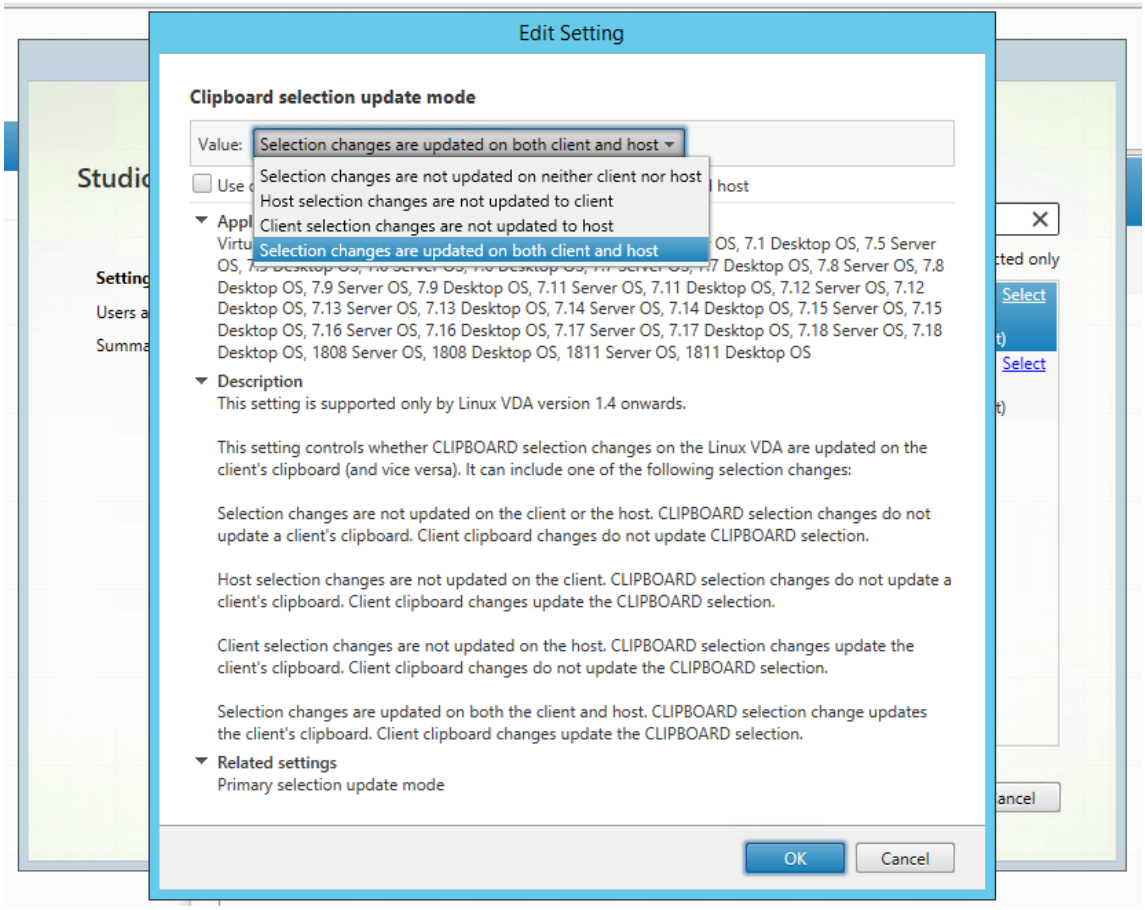
  Valor predeterminado: 3

  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 de 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 la selección primaria con el mismo valor.

Impresión

March 27, 2023

Esta sección contiene estos temas:

- Prácticas recomendadas de impresión
- Impresión de PDF

Prácticas recomendadas de impresión

March 27, 2023

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
```

Configuraciones de directiva de Impresión

Redirección de impresoras del cliente

Este parámetro controla si las impresoras del cliente se asignan a una sesión de VDA.
La asignación de impresoras cliente está permitida de forma predeterminada.

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

Crear automáticamente las impresoras del cliente

Este parámetro especifica las impresoras del cliente que se pueden asignar a sesiones de VDA. De forma predeterminada, está establecido en **Crear automáticamente todas las impresoras cliente**, lo que significa que todas las impresoras del cliente se asignan a sesiones de VDA. Para obtener más información sobre este parámetro, consulte Crear automáticamente las impresoras del cliente en la documentación de Citrix Virtual Apps and Desktops.

Crear automáticamente la impresora universal de PDF

Para utilizar la funcionalidad de impresión en PDF, establezca esta directiva en **Habilitada**.

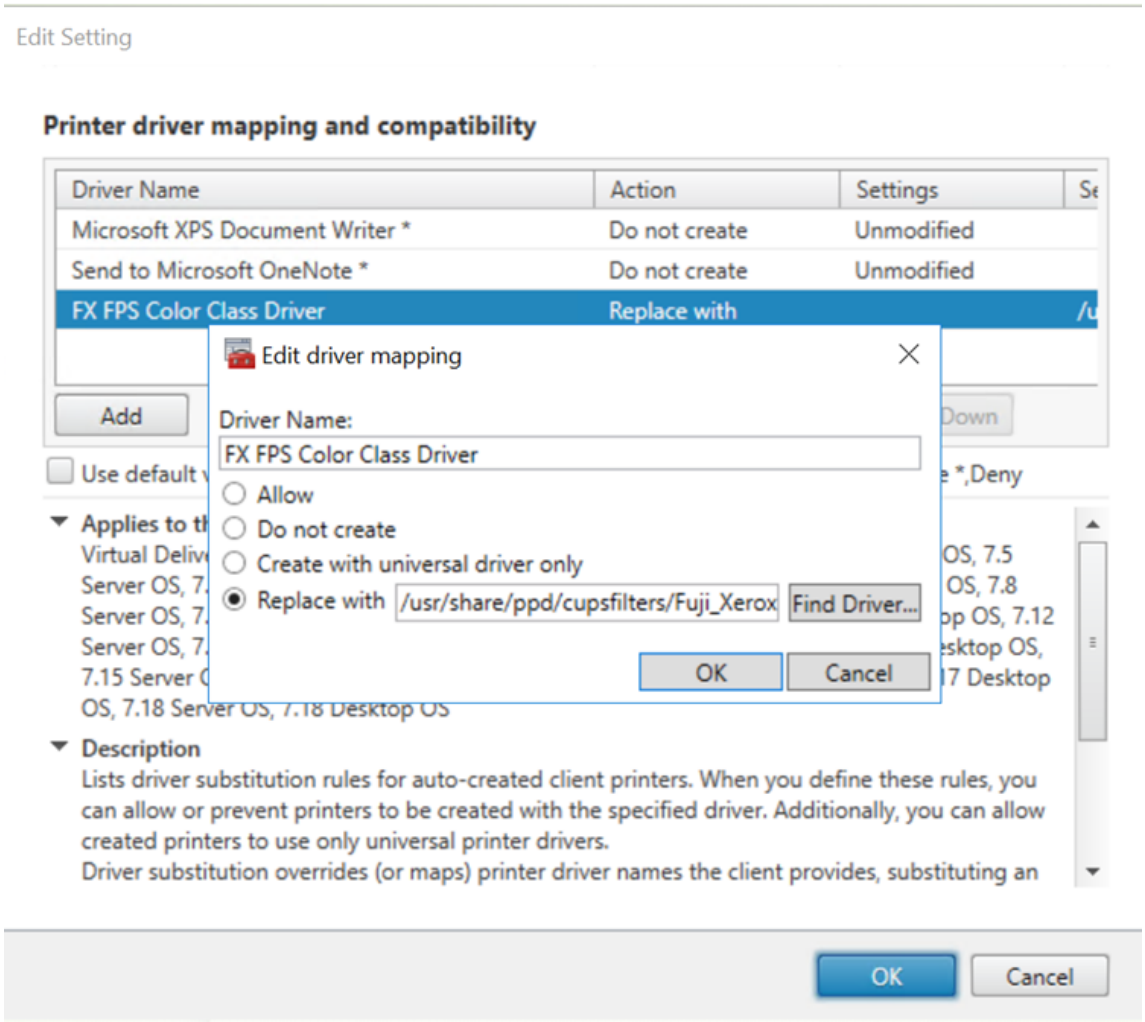
Asignación y compatibilidad de controladores de impresora

Citrix proporciona tres tipos de controladores de impresora universales (postscript, pcl5 y pcl6). Sin embargo, es posible que el controlador de impresora universal no sea compatible con la impresora del cliente. En este caso, la única opción posible en versiones anteriores era modificar el archivo de configuración ~/.CtxlpProfile$CLIENT_NAME. A partir de la versión 1906, en su lugar, puede configurar la directiva **Asignación y compatibilidad de controladores de impresora** en Citrix Studio.

Para configurar la directiva **Asignación y compatibilidad de controladores de impresora** en Citrix Studio.

1. Seleccione la directiva **Asignación y compatibilidad de controladores de impresora**.
2. Haga clic en **Agregar**.
3. Introduzca el **nombre del controlador** de la impresora del cliente. Si utiliza la aplicación Citrix Workspace para Linux, introduzca el nombre de la impresora.
4. Elija **Reemplazar por** y escriba la ruta absoluta del archivo de controlador en el VDA.

© 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. Todas las impresoras del cliente se pueden asignar a una sesión de VDA. El nombre de la impresora debe ser diferente entre los escritorios y las aplicaciones.

- Para los escritorios publicados:
  `<client printer name>:$CLIENT_NAME:dsk$SESSION_ID`
- Para las aplicaciones publicadas:
  `<client printer name>:$CLIENT_NAME:app$SESSION_ID`

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

> **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.

```
ps -ef | grep ctxlpmngt
```

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:

```
service ctxcups status
```

Pasos adicionales para recopilar registros de CUPS

Para recopilar registros de CUPS, ejecute los siguientes comandos para configurar el archivo de servicio de CUPS. De lo contrario, los registros de CUPS no se 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
```

> **Nota:**
>
> Esta configuración solo sirve para recopilar el registro completo de impresión cuando surja al-

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

> gún 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=
```

> **Importante:**
>
> El campo **printername** contiene el nombre de la impresora actual predeterminada del cliente. Es un valor de solo lectura. No debe modificarlo.
>
> Los campos **ppdpath**, **model** y **drivertype** no se pueden establecer a la vez, ya que solo uno tiene efecto en la impresora asignada.

- Si el controlador de impresora universal no es compatible con la impresora del cliente, configure el modelo del controlador de la impresora nativa con la opción **model**=. Puede buscar el nombre del modelo actual de la impresora con el comando **lpinfo**:

  ```
  lpinfo  – m

  …

  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
  ```

  A continuación, puede configurar el modelo para que coincida con la impresora:

  ```
  model=xerox/ph3115.ppd.gz
  ```

- Si el controlador de impresora universal no es compatible con la impresora cliente, configure la ruta 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:

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

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

- 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
  ```

El tamaño de la salida es cero

Pruebe diferentes tipos de impresoras. Asimismo, pruebe una impresora virtual (como CutePDF y PDFCreator) para averiguar si el problema está relacionado con el controlador de la impresora.

El trabajo de impresión depende del controlador de impresora establecido en la impresora predeterminada del cliente. Es importante identificar el tipo de controlador activo actual. Si la impresora cliente usa un controlador PCL5, pero Linux VDA elige un controlador PostScript, se puede producir un problema.

Si el tipo de controlador de la impresora es correcto, puede identificar el problema siguiendo estos pasos:

1. Inicie sesión en una sesión de escritorio publicada.
2. Ejecute el comando **vi ~/.CtxlpProfile$CLIENT_NAME**.
3. Agregue el siguiente campo al archivo de cola de impresión guardado en Linux VDA:

   ```
   deletespoolfile=no
   ```

4. Cierre la sesión y vuelva a iniciarla para cargar los cambios de configuración.
5. Imprima el documento para reproducir el problema. Después de imprimir, 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.

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

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
   ```

   c) Elija la impresora asignada **CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID** y **Modify Printer**. Esta operación requiere privilegios de administrador.

   d) Conserve la conexión **cups-ctx** y, a continuación, haga clic en **Continue** para modificar el controlador de la impresora.

   e) En los campos **Make** y **Model**, elija otro controlador de impresora del controlador UPD de Citrix. Por ejemplo, si está instalada la impresora virtual CUPS-PDF, puede seleccionar el controlador de impresora genérica CUPS-PDF. Guarde el cambio.

   f) Si este proceso se realiza correctamente, configure la ruta al archivo PPD del controlador en **.CtxlpProfile$CLIENT_NAME** para permitir que la impresora asignada use el controlador recién seleccionado.

Problemas conocidos

Se han identificado los siguientes problemas al imprimir con Linux VDA:

El controlador CTXPS no es compatible con algunas impresoras PLC

Si se dañan las impresiones, establezca el controlador de impresora al controlador nativo que haya proporcionado el fabricante.

Impresión lenta de documentos grandes

Al imprimir un documento grande en una impresora local del cliente, el archivo que debe imprimirse se transfiere a través de una conexión de servidor. En conexiones lentas, esta transferencia puede tardar mucho tiempo.

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

La impresora y las notificaciones de trabajos de impresión aparecen en otras sesiones

Linux no tiene el mismo concepto de sesión que Windows. Por lo tanto, todos los usuarios reciben notificaciones de todo el sistema. Para inhabilitar esas notificaciones, debe modificar el archivo de configuración CUPS: **/etc/cups/cupsd.conf**.

En el archivo, busque el nombre de la directiva actual configurada:

```
DefaultPolicy default
```

Si el nombre de la directiva es *default*, agregue las siguientes líneas al bloque XML de la directiva predeterminada:

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default

     … …

     <Limit Create-Printer-Subscription>

          Require user @OWNER

          Order deny,allow

     </Limit>

     <Limit All>

          Order deny,allow

     </Limit>

</Policy>
```

Impresión de PDF

March 27, 2023

Con una versión de la aplicación Citrix Workspace que admita la impresión de PDF, puede imprimir

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

archivos PDF convertidos en las sesiones de Linux VDA. Los trabajos de impresión de la sesión se envían a la máquina local donde está instalada la aplicación Citrix Workspace. En la máquina local, puede abrir los archivos PDF desde su visor de PDF e imprimirlos en la impresora que elija.

Linux VDA admite la impresión de archivos PDF en las siguientes versiones de la aplicación Citrix Workspace:

- Citrix Receiver para HTML5 de la versión 2.4 a la 2.6.9, la aplicación Citrix Workspace 1808 para HTML5 y versiones posteriores
- Citrix Receiver para Chrome de la versión 2.4 a la 2.6.9, la aplicación Citrix Workspace 1808 para Chrome y versiones posteriores
- Aplicación Citrix Workspace 1905 para Windows y versiones posteriores

Configuración

Aparte de usar una versión de la aplicación Citrix Workspace que admita la impresión de PDF, establezca las siguientes directivas en Citrix Studio:

- Establezca **Redirección de impresoras del cliente** en **Permitido** (**Permitido** es la opción predeterminada)
- Establezca **Crear automáticamente la impresora universal de PDF**en **Habilitado** (**Inhabilitado** es la opción predeterminada)
- Establezca **Crear automáticamente las impresoras del cliente** en **Crear automáticamente todas las impresoras del cliente**.

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 15, 2024

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

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

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:

- 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:

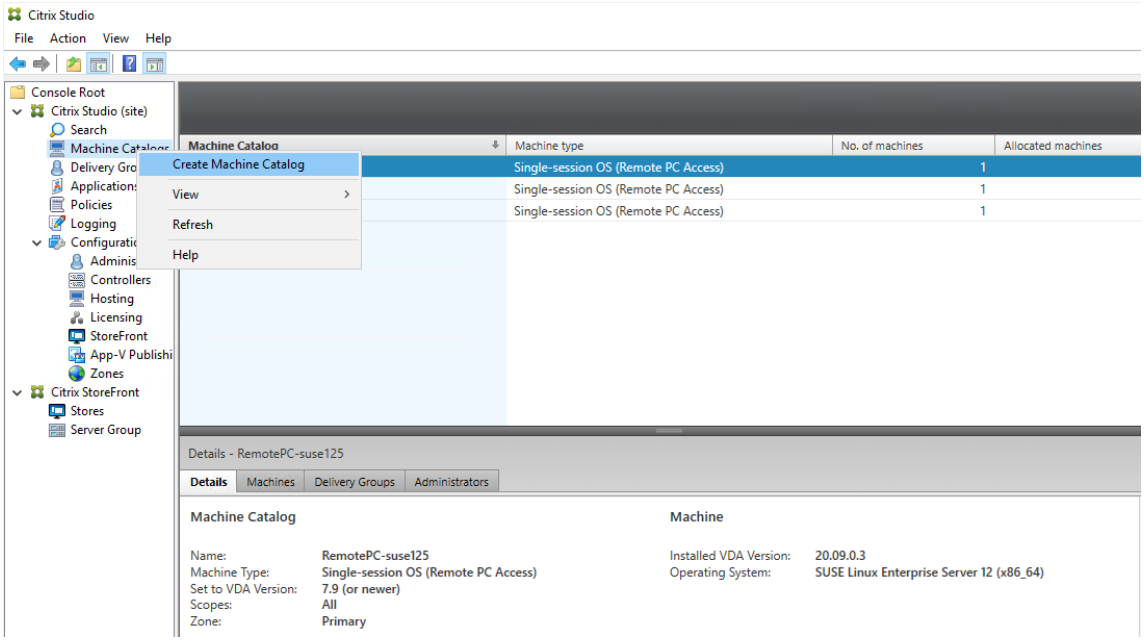
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Paso 1 - Instalar Linux VDA en los equipos de destino

Se recomienda utilizar Easy Install para instalar Linux VDA. Durante la instalación, establezca el valor de la variable `CTX_XDL_VDI_MODE` en `Y`.

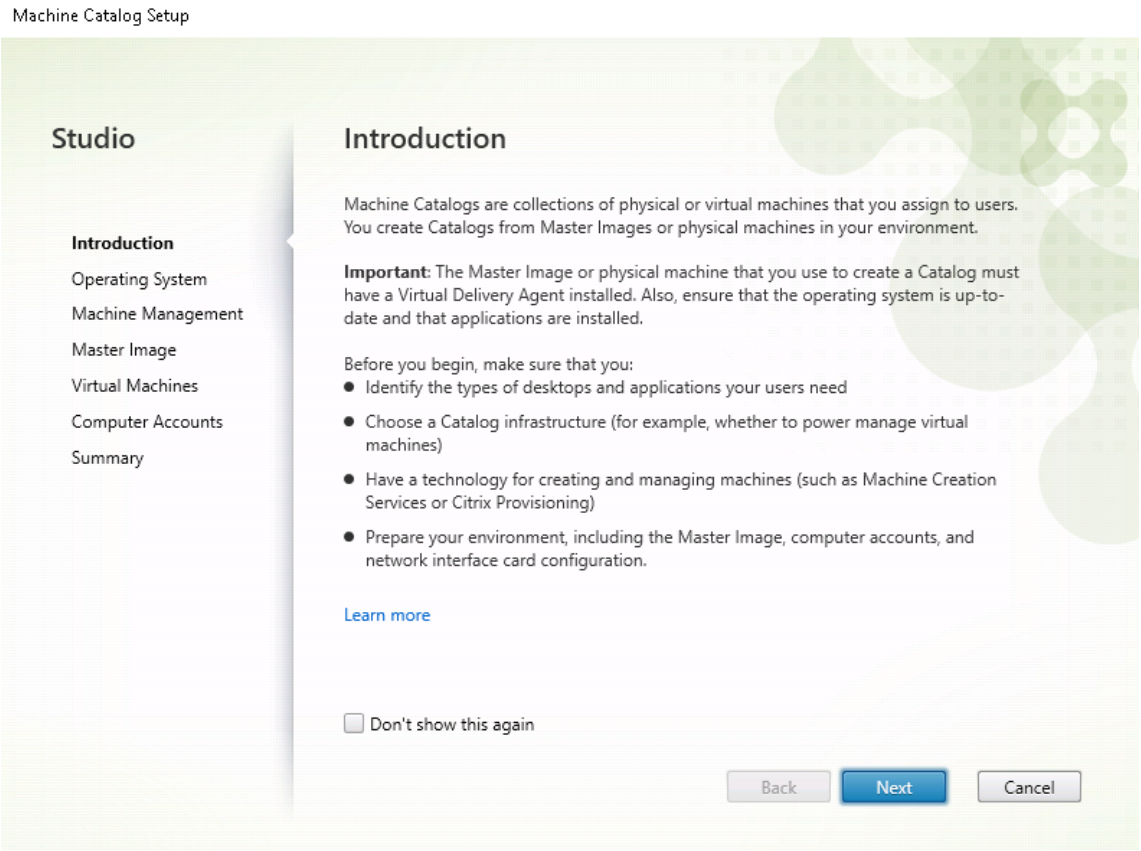
Paso 2 - Crear un catálogo de máquinas de tipo Acceso con Remote PC

1. En Citrix Studio, haga clic con el botón secundario en **Catálogos de máquinas** y seleccione **Crear catálogo de máquinas** en el menú contextual.



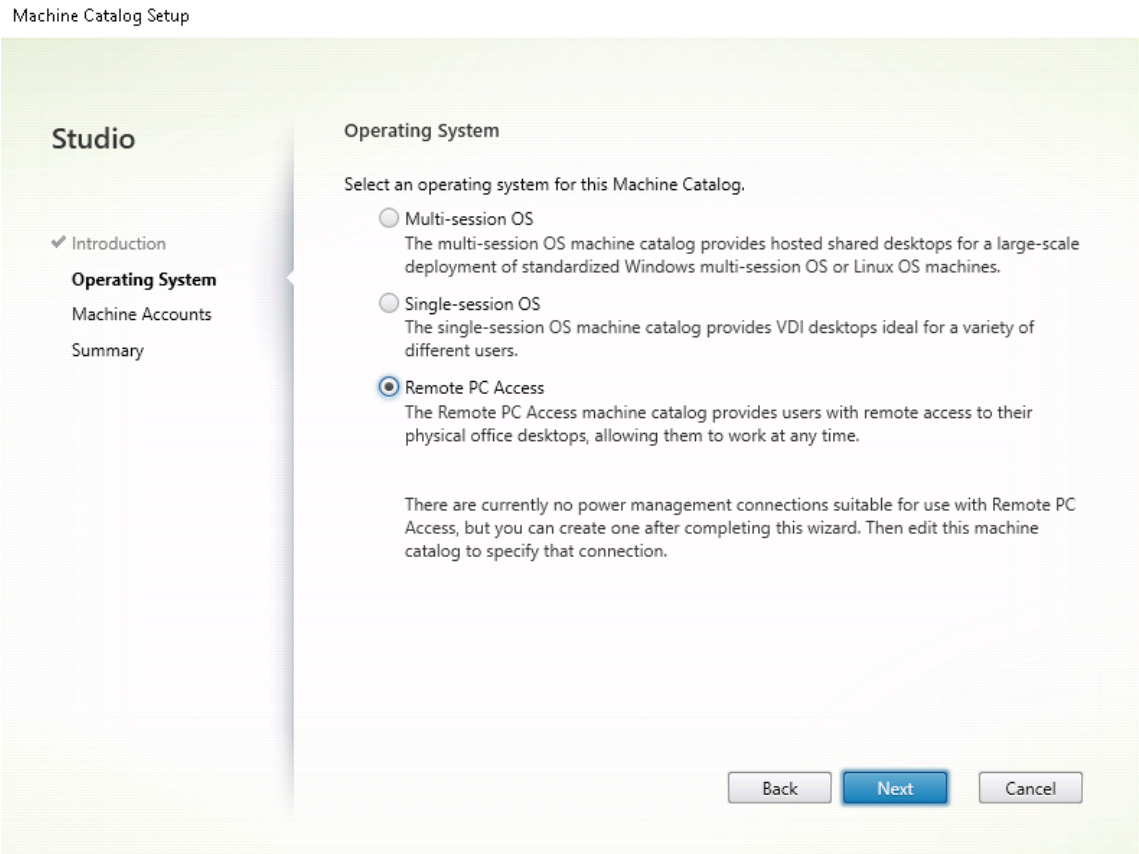
2. En la página **Introducción**, haga clic en **Siguiente**.

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



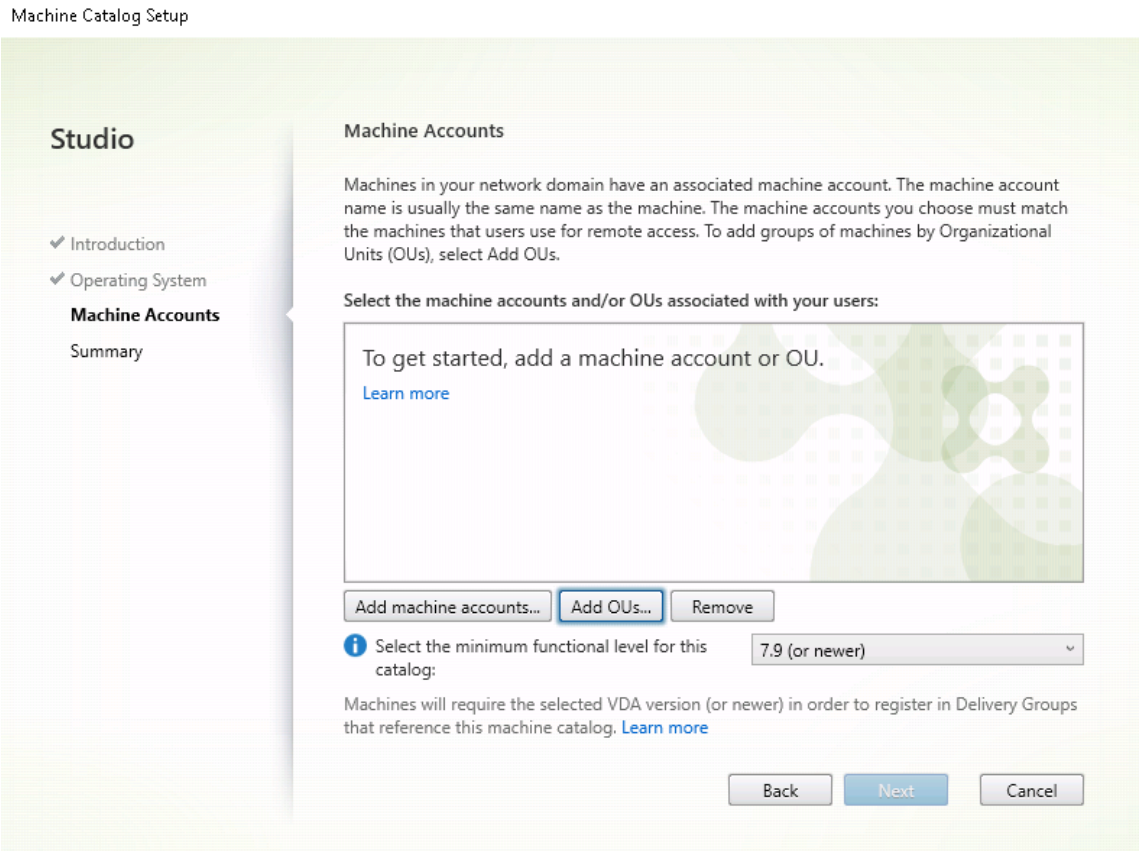
3. En la página **Sistema operativo**, seleccione **Acceso con Remote PC**.

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



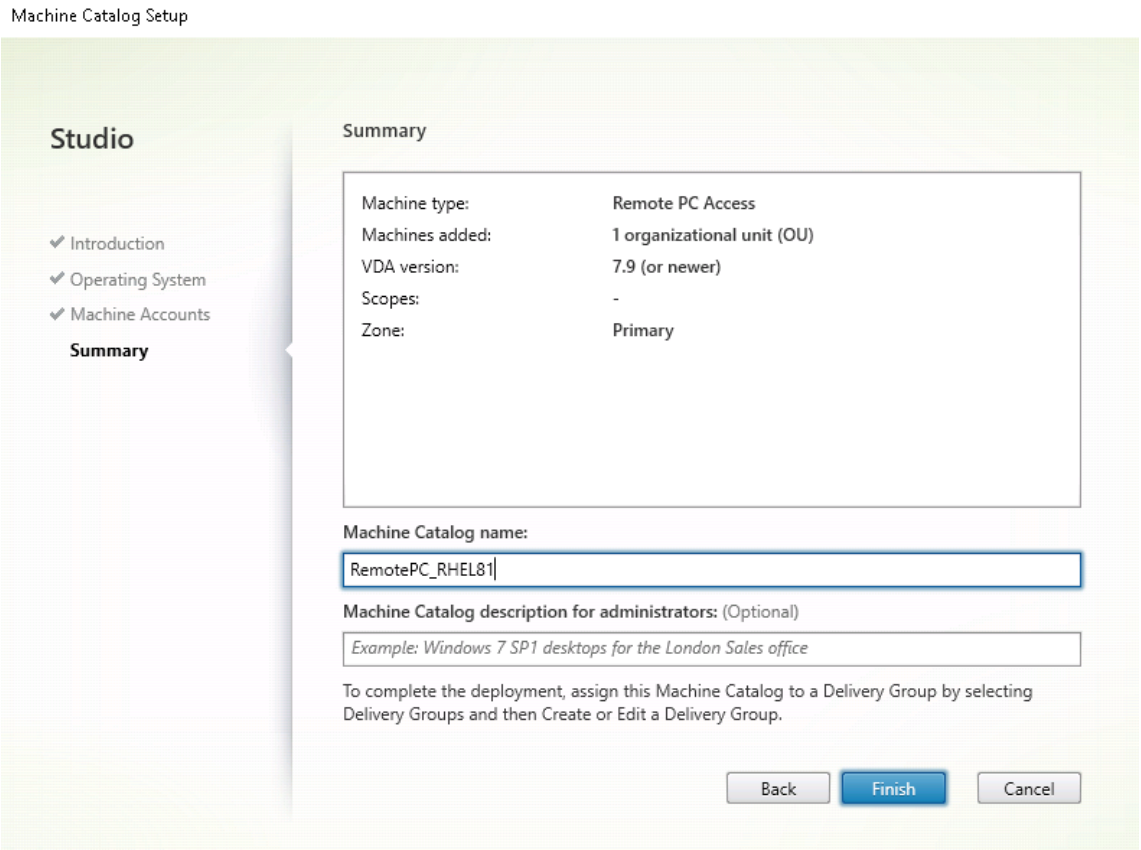
4. Haga clic en **Agregar unidades organizativas** para seleccionar las unidades organizativas que contendrán los equipos de destino o haga clic en **Agregar cuentas de máquina** para agregar máquinas individuales al catálogo de máquinas.

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

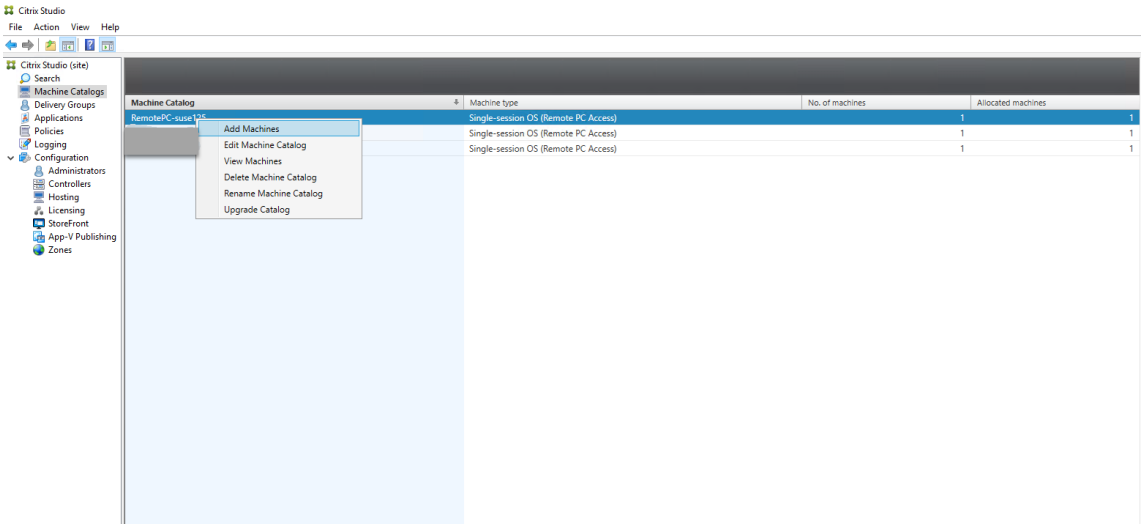


5. Asigne un nombre al catálogo de máquinas.

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



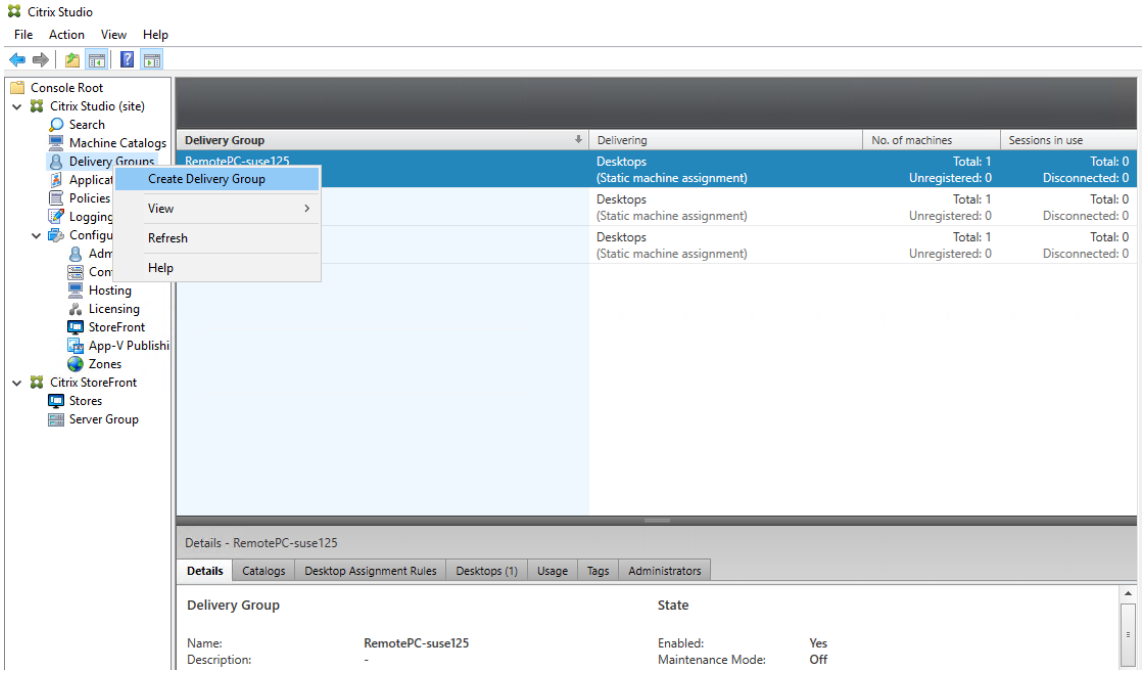
6. (Opcional) Haga clic con el botón secundario en el catálogo de máquinas para realizar las operaciones relevantes.



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

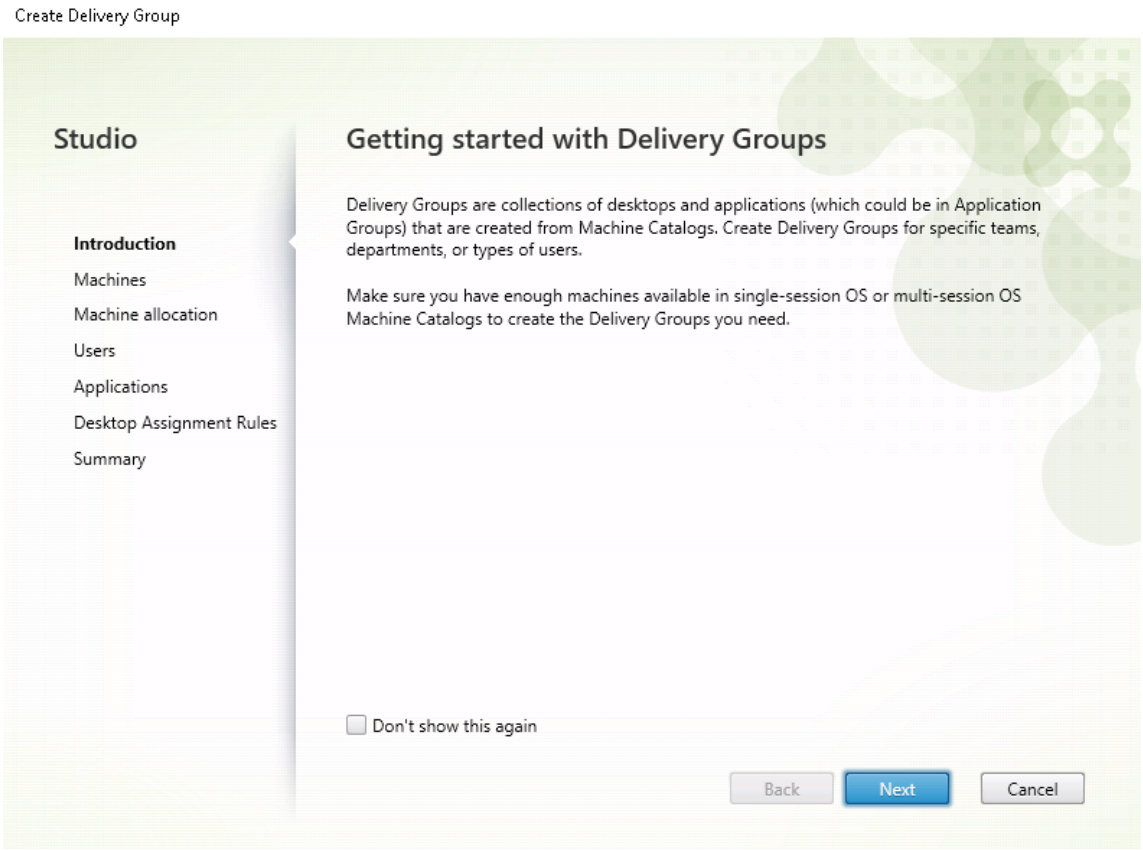
Paso 3 - Crear un grupo de entrega para que los PC del catálogo de máquinas estén disponibles para los usuarios que soliciten acceso

1. En Citrix Studio, haga clic con el botón secundario en **Grupos de entrega** y seleccione **Crear grupo de entrega** en el menú contextual.



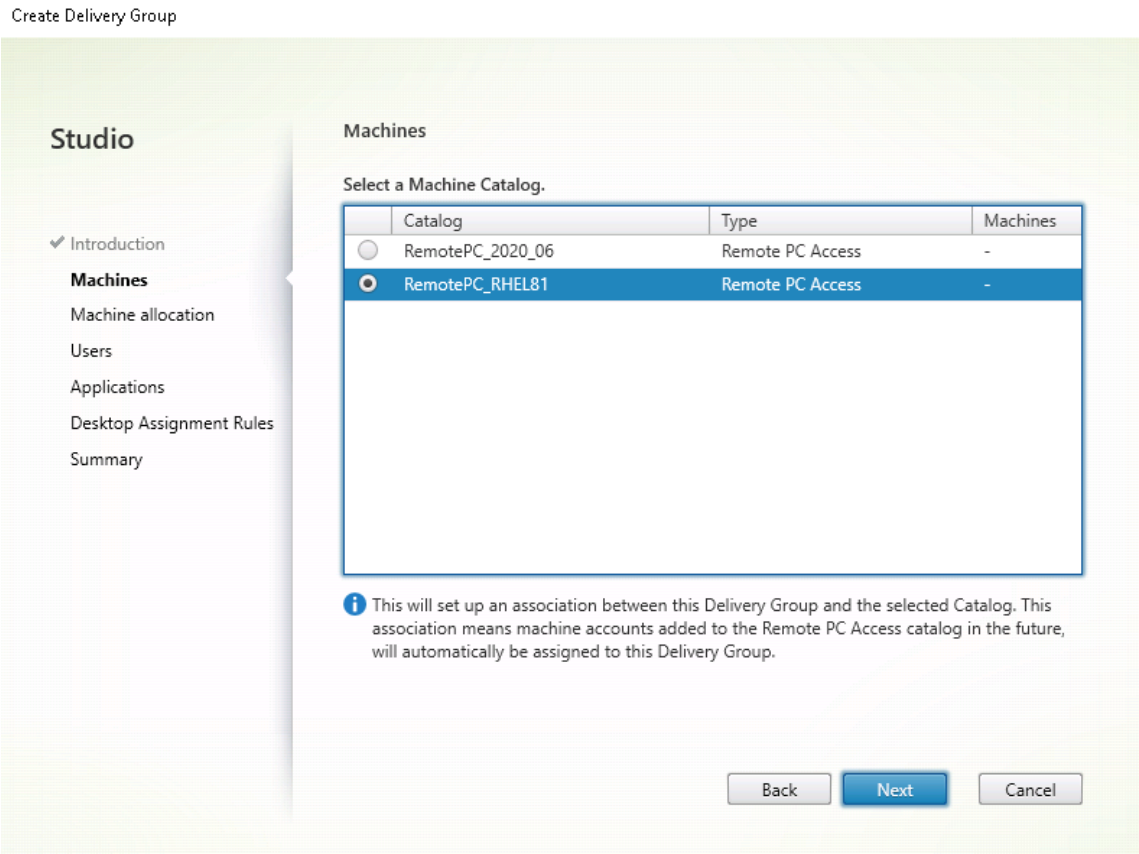
2. Haga clic en **Siguiente** en la página **Introducción a los grupos de entrega**.

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



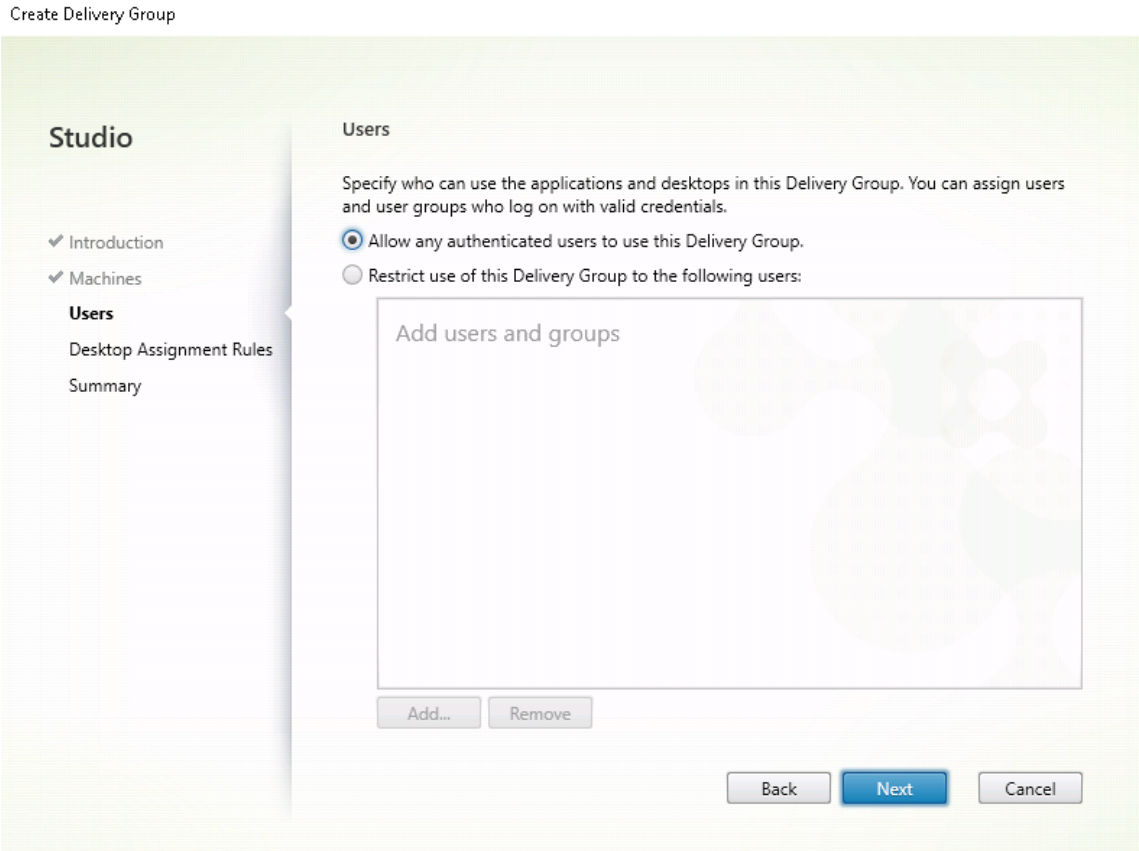
3. Seleccione el catálogo de máquinas creado en el paso 2 para asociarlo al grupo de entrega.

© 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
 }
```

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
```

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
```

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:
        - 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.

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

- 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
```

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"
```

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.
- 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.

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

- 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

March 27, 2023

Esta sección contiene estos temas:

- Transporte adaptable
- Iniciar sesión con un directorio de inicio temporal

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

- Publicar aplicaciones
- Fiabilidad de la sesión
- Rendezvous V1
- Rendezvous V2
- Sesiones de usuario seguras mediante TLS
- Sesiones de usuario seguras mediante DTLS

Transporte adaptable

March 27, 2023

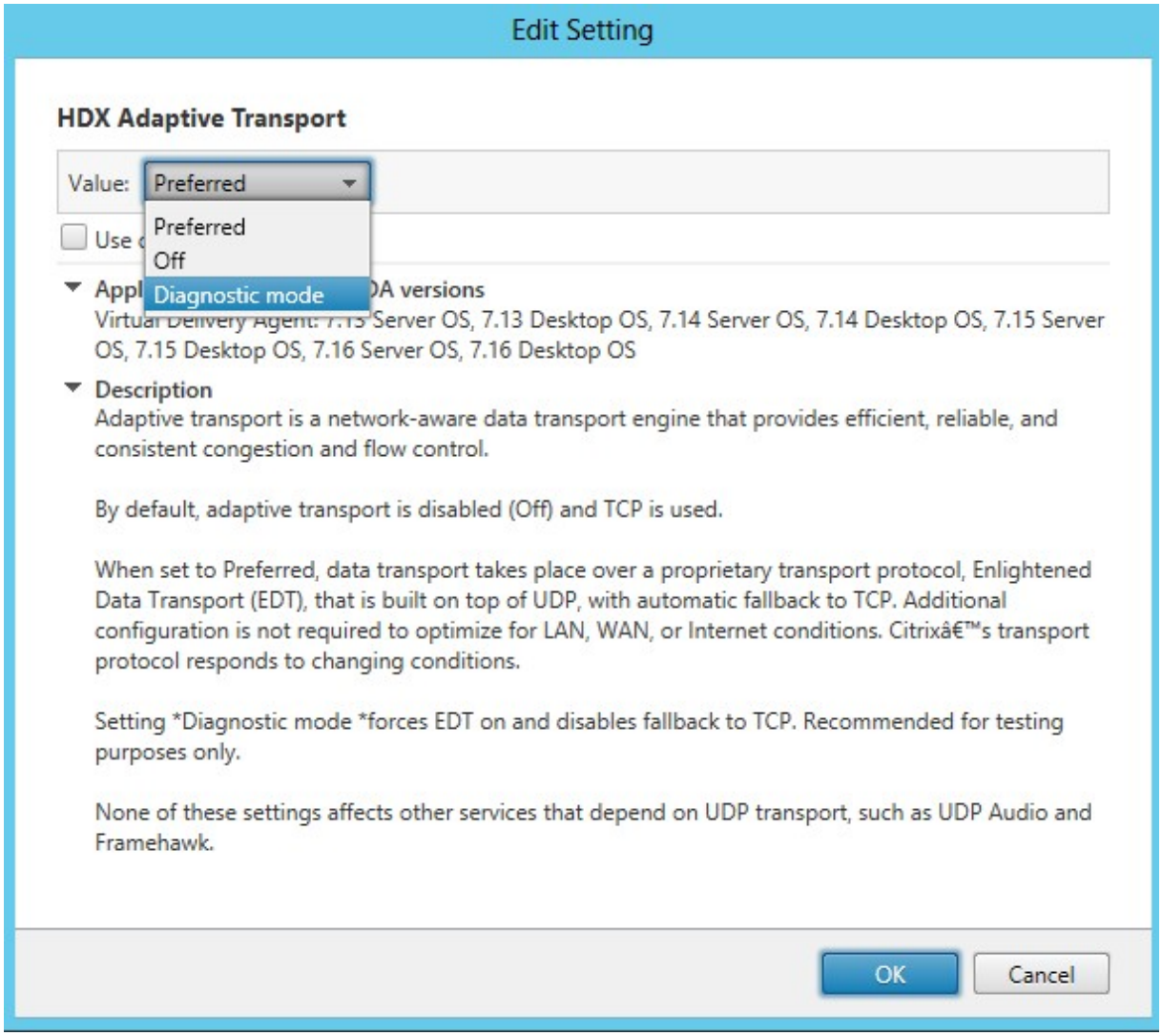
El transporte adaptable es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops. Es más rápido, más escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones de Internet y WAN difíciles de largo recorrido. Para obtener más información sobre el transporte 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"
```

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                 :::*
```

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 una plataforma de cliente o versión que no admite 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.

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

May 4, 2023

Puede usar los siguientes comandos para agregar un fondo o un mensaje de pancarta personalizado a las pantallas de **inicio de sesión**. Para agregar tanto un fondo como un mensaje de pancarta a las pantallas de **inicio de sesión**, puede insertar el mensaje de pancarta en la imagen de fondo.

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
    "LogonDisplayString" -d "<text of custom logon banner message>" --
   force
```

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
    "BackgroundImagePath" -d "<path to your custom logon screen
   background image>" --force
```

Para usar la función en SUSE 15.4, instale `imlib2` desde http://download.opensuse.org/distribution/leap/15.3/repo/oss/.

> **Sugerencia:**
>
> Si agrega un mensaje de pancarta personalizado mediante LogonDisplayString, el fondo de la pantalla de inicio de sesión es azul de forma predeterminada.

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

Entornos de escritorio personalizados por los usuarios de las sesiones

March 27, 2023

Puede especificar un entorno de escritorio para los usuarios de las sesiones mediante la variable **CTX_XDL_DESKTOP_ENVIRONMENT**. A partir de la versión 2209, los usuarios de las sesiones pueden personalizar sus propios entornos de escritorio. Para habilitar esta función, debe instalar los entornos de escritorio en el VDA con antelación.

Esta tabla muestra las distribuciones de Linux y los entornos de escritorio que admiten entornos de escritorio personalizados por usuarios de sesión.

Distribución de Linux	Escritorio compatible
Debian 11.3	MATE, GNOME, GNOME-Classic, KDE
RHEL 8.6, RHEL 8.4	MATE, GNOME, GNOME-Classic
RHEL 7.9	MATE, GNOME, GNOME-Classic, KDE
Rocky Linux 8.6	MATE, GNOME, GNOME-Classic, KDE
SUSE 15.3	MATE, GNOME, GNOME-Classic
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	MATE, GNOME, GNOME-Classic, KDE

Comandos para cambiar de escritorio

Para cambiar a un entorno de escritorio de destino, ejecute el comando correspondiente en la sesión:

Si el entorno de escritorio de destino es	Ejecute el comando
GNOME	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME`
GNOME Classic	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC`
MATE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE`
KDE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE`

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

Consejos para KDE

- Es posible que Magnus no se cargue al iniciar KDE. Como solución temporal, puede quitar el paquete Magnus tras ejecutar `sudo apt remove magnus`.
- Para inhabilitar las advertencias de QT que se producen durante el inicio de KDE, modifique `/usr/share/qt5/qtlogging.ini` como usuario raíz. Para ello, agregue estas entradas:

```
qt.qpa.xcb.xcberror.error=false
qt.qpa.xcb.warning=false
qt.qpa.xcb.error=false
```

- Es posible que el desbloqueo de pantalla falle en KDE. Como solución temporal, le recomendamos inhabilitar la función de bloqueo automático del escritorio.

Iniciar sesión con un directorio de inicio temporal

March 27, 2023

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 del 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/CTXSmf_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

March 27, 2023

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

March 27, 2023

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:

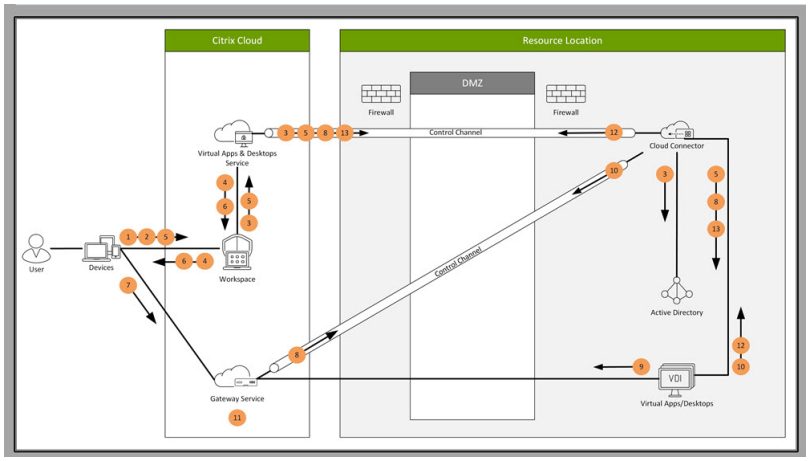
1. Inicie un terminal en el VDA.
2. Ejecute `/opt/Citrix/VDA/bin/ctxquery -f iP`
3. Los PROTOCOLOS DE TRANSPORTE en uso indican el tipo de conexión:
    - TCP Rendezvous: TCP - TLS - CGP - ICA
    - EDT Rendezvous: UDP - DTLS - CGP - ICA
    - Proxy a través de Cloud Connector: TCP - PROXY - SSL - CGP - 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

March 27, 2023

© 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
```

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.
- 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.

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

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:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -t "REG_DWORD" -v "GctRegistration" -d "0
    x00000001" --force
```

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.

> **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.

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

Sesiones de usuario seguras mediante DTLS

March 27, 2023

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:**
>
> Linux VDA admite DTLS 1.0 y DTLS 1.2, y usa DTLS 1.2 de forma predeterminada. Compruebe qué versión de DTLS se está usando en su aplicación Citrix Workspace. Asegúrese de que se usa la misma versión de DTLS tanto en Linux VDA como en la aplicación Citrix Workspace. Si la aplicación Citrix Workspace solo admite DTLS 1.0 (por ejemplo, Citrix Receiver para Windows 4.11), configure **SSLMinVersion** en **TLS_1.0** y **SSLCipherSuite** en **COM** o **ALL** mediante la herramienta **enable_vdassl.sh**.

Sesiones de usuario seguras mediante TLS

March 27, 2023

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.

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

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
gYOAMIGJAoGBALCTTOdxcivbIOLOF66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9
t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEwl3YxM6COyBf7L6psrsCDNnBP1q8TJH
4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8yOw
gZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMAOGCSqGSIb3DQEBBQUAA4GB
AD5axBYHwIxJCJzNt2zdXnbp2O0yUToWElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68
Vel8u1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbuOIjOtr3pkxAe
b6CFJtNLudHUrwF6lOrB72zbyz3PiIx+HEwt1jOj8Z4K
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCwkOzncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
R+MaDyF1HmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea
FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSxOYb/lAdck/
FXzUOtqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1KRZjIN5uz
Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri9O+OoEPxclvvp5ne8QOzUpshbjFEPbOC
ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
fIenmTrfZ+Wo4DaKg+8ar2OvOnKFOHFAmDECQQDEWRlH6cE3WyCfN1u942M9XkhR
GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
h5eEmxSZS5OTvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
EjAQBgNVBAgTCUNhbWJyaWRnZTE5MBAGA1UEBxMJQ2FtYm9lcmSlMRQwEgYDVQQK
EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
KoZIhvcNAQEBBQADgYOAMIGJAoGBAKVZmF7Uj7uOnvO3Qwdfi0nr3QkNH2DXpWrZ
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.

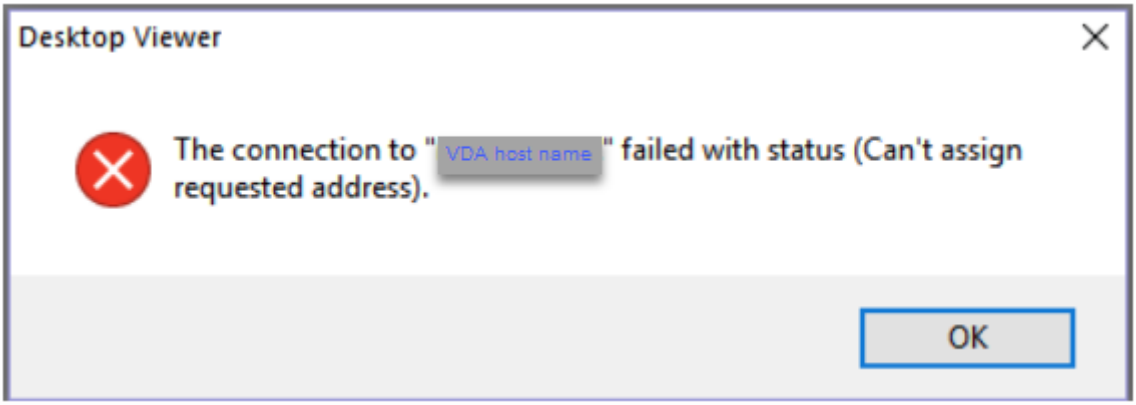
> **Nota:**
>
> Para asegurarse de que solo los nombres de dominio completos de los VDA están contenidos en el archivo de una sesión ICA, también puede ejecutar el comando `Set-BrokerSite –DnsResolutionEnabled $true`. Este comando habilita la resolución DNS. Si inhabilita la resolución DNS, el archivo 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

March 27, 2023

© 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.

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
    fEnableWinStation" -d "0x00000000"
```

Nota: Reinicie el servicio HDX para que la configuración surta efecto. Inhabilitar la escucha TCP no inhabilita la fiabilidad de la sesión. La fiabilidad de la sesión seguirá estando disponible a través de otros agentes de escucha (por ejemplo, SSL) si la función sigue habilitada en la directiva **Conexiones de fiabilidad de la sesión**.

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

- **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"
```

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
```

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:

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

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
   ```

   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"
   ```

Grabación de sesiones (experimental)

March 27, 2023

Como función experimental, puede grabar y reproducir sesiones alojadas en un Linux VDA.

Habilitar o inhabilitar la grabación de sesiones

Para habilitar o inhabilitar la grabación de sesiones en Linux VDA, establezca **SmAudAllowed** en **1** o **0**, respectivamente. Puede utilizar estos comandos:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
   SmAudAllowed" -d "0x00000001" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
   SmAudAllowed" -d "0x00000000" --force
```

> **Nota:**
>
> Tras habilitar la grabación de sesiones en Linux VDA, los usuarios reciben una notificación sobre la grabación de sus sesiones cuando inician sesión en ellas.

Especificar el tamaño del archivo para las grabaciones

A medida que las grabaciones aumentan de tamaño, los archivos de grabación tardan más en descargarse y en reaccionar al usar el control deslizante para navegar por la reproducción. Para controlar

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

el tamaño de los archivos, especifique un límite para un archivo. Cuando la grabación alcanza este límite, el archivo actual se cierra y se crea un archivo adicional para continuar grabando. Esta acción se llama renovar.

Con estos comandos, puede especificar dos umbrales para una renovación:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    RolloverFileSizeInMB" -d "0x00000032" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    RolloverTimeInHours" -d "0x0000000c" --force
```

- **RolloverFileSizeInMB**. El archivo actual se cierra cuando alcanza el tamaño y se abre un archivo nuevo. De forma predeterminada, la renovación se produce cuando el tamaño supera los 50 MB. Valores admitidos: 10-300.
- **RolloverTimeInHours**. Cuando se alcanza la duración, el archivo actual se cierra y se abre un archivo nuevo. De forma predeterminada, la renovación se produce cuando la sesión se graba durante 12 horas. Valores admitidos: 1-24.

Las renovaciones se producen cuando se cumple la primera de las dos condiciones anteriores. Por ejemplo: Especifique 17 MB de tamaño de archivo y 6 horas de duración. Cuando la grabación alcance los 17 MB en 3 horas, la grabación de sesiones cierra el archivo y abre uno nuevo.

Para evitar que se creen muchos archivos pequeños, la renovación no tiene lugar hasta que pasa al menos una hora, independientemente del valor especificado en el tamaño de archivo. La excepción a esta regla se da cuando el tamaño del archivo sobrepasa 300 MB.

Especificar dónde se almacenan las grabaciones

Los archivos de grabación se almacenan en `/var/xdl/session_recordings` de forma predeterminada. Para especificar una ruta diferente, ejecute este comando:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_SZ" -v "Path"
     -d "<your custom storage path>" --force
```

Puede almacenar grabaciones en una unidad local o en un punto de montaje que apunte a una ruta de red. Configure los permisos de acceso adecuados a la ruta de almacenamiento que haya establecido y conceda al usuario `ctxsrvr` el permiso de escritura en la ruta.

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

Ver las grabaciones

Para ver las grabaciones, siga estos pasos para instalar el reproductor de Grabación de sesiones o el reproductor web de Grabación de sesiones:

1. Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de Citrix Virtual Apps and Desktops y descargue el archivo del producto. Descomprima el archivo.
2. Haga doble clic en SessionRecordingPlayer.msi y SessionRecordingWebPlayer.msi, y siga las instrucciones para completar la instalación.

> **Sugerencia:**
>
> Para utilizar el reproductor web de Grabación de sesiones, instálelo únicamente en el servidor de Grabación de sesiones y asegúrese de que las grabaciones estén disponibles en el servidor de Grabación de sesiones. Para obtener más información, consulte la documentación de Grabación de sesiones de Citrix.

Limitaciones

- En el caso de las sesiones de aplicaciones virtuales, es posible que las notificaciones de grabaciones no estén centradas.

Virtual Channel SDK (experimental)

March 27, 2023

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 del SDK de Citrix Virtual Channel para Linux VDA.

El SDK de Citrix Virtual Channel 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.

Wayland (experimental)

March 27, 2023

Como funcionalidad experimental, Linux VDA admite Wayland en GNOME, en RHEL 9.0, Rocky Linux 9.0 y Ubuntu 22.04. Las siguientes capacidades están plenamente probadas en Wayland:

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

- Audio
- Portapapeles
- Asignación de unidades del cliente (CDM)
- Impresión
- Redirección de dispositivos USB

> **Nota:**
>
> - HDX 3D Pro no es compatible.
> - No se admiten sesiones de aplicación virtual de Linux.

Habilitar Wayland

Para usar Wayland, establezca la clave de registro **EnableWayland** en **1**. Para ello, ejecute el siguiente comando:

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

De forma predeterminada, la clave de registro **EnableWayland** está establecida en **0**, lo que significa que se utiliza X11.

Compruebe si Wayland está en uso

1. Abre una ventana de Terminal en Linux.
2. Ejecute el comando **echo $XDG_SESSION_TYPE**.

Si Wayland está en uso, aparecerá "**wayland**" en el resultado.

Limitaciones

Con Wayland en uso, se identifican las siguientes limitaciones:

- La distribución del teclado del dispositivo cliente no está sincronizada con la distribución del teclado del VDA.
- Se tarda unos 20 segundos en cerrar sesión en RHEL 9.0, Rocky Linux 9.0.

© 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).