

Acerca de Citrix Receiver 13.4 para Linux

Jan 05, 2017

Citrix Receiver para Linux es un cliente de software que le permite acceder a escritorios, aplicaciones y datos de forma sencilla y segura desde muchos tipos de dispositivos Linux. Al trabajar con una infraestructura de IT preparada para usar productos Citrix, Receiver le ofrece la movilidad, comodidad y libertad que necesita para poder realizar su trabajo.

Citrix Receiver para Linux 13.4

Esta versión ofrece las siguientes mejoras y nuevas funcionalidades. Asimismo, resuelve varios problemas que se han informado anteriormente acerca de la experiencia de usuario.

- Desktop Viewer

Desktop Viewer le permite interactuar con varios escritorios virtuales y sus escritorios nativos simultáneamente. La funcionalidad de la barra de herramientas de Desktop Viewer le permite alternar entre una sesión en modo de ventana y una sesión a pantalla completa; además, incluye respaldo para varios monitores para los monitores intersecados. Puede alternar entre sesiones de escritorio y trabajar con más de un escritorio mediante varias conexiones de XenDesktop en el mismo dispositivo de usuario. Con tal de gestionar mejor las sesiones de los usuarios, se ofrecen botones para minimizar todas las sesiones de escritorio, el envío de la secuencia Ctrl+Alt+Supr, la desconexión y el cierre de sesión.

- Respaldo para los modos de puntero absoluto y relativo
- SDK de inserción de credenciales (CISDK) para la integración de tarjetas de proximidad y OEM de cliente ligero
- Respaldo para CID de SecMaker
- Respaldo para H264 selectivo

Es posible que los clientes que usen SDK de SoC deban actualizar la optimización de H264.

- Mejoras en los diálogos de autenticación

Ahora, Citrix Receiver para Linux permite que se cambien los títulos de los diálogos de autenticación por un encabezado de respuesta HTTP con el nombre X-Citrix-AM-Título. El usuario puede saber más fácilmente en qué está iniciando sesión.

- Experiencia de primer uso mejorada, sobre todo cuando se usa la autenticación SMS

Para obtener más información, consulte [CTX205892](#).

- Mejorado el respaldo predeterminado para tarjetas inteligentes

Al conectarse a un servidor StoreFront que permite la autenticación por tarjeta inteligente, si no se ha establecido ningún valor en "PKCS11module" en el archivo de configuración \$ICAROOT/config/AuthManConfig.xml, Receiver usa el controlador opensc-pkcs11.so si lo encuentra en una de las ubicaciones estándar. Lo que significa que se le puede pedir que inserte un lector o tarjeta sin realizar cambios en AuthManConfig.xml. Si no quiere usar tarjeta inteligente, seleccione el enlace "Log on with another method" (Inicie sesión con otro método).

- En el marco de la mejora constante de seguridad, ahora Receiver para Linux usa la versión 1.0.1t de OpenSSL para conexiones TLS.

Problemas resueltos en esta versión

Problemas conocidos en esta versión

- El respaldo de proxy para los comandos selfservice y storebrowse no está disponible de manera predeterminada. Para usar un servidor proxy con un servidor StoreFront, establezca las variables de entorno http_proxy y/o HTTPS_PROXY antes de iniciar esos comandos. Utilice el siguiente formato para la variable de entorno: .[:]

[#403729]

- Citrix Receiver para Linux no reconoce la tarjeta inteligente PIV al iniciar un escritorio por primera vez.

[#491235]

- Aparecen mensajes de error poco claros cuando Citrix Receiver para Linux no encuentra el servidor inmediatamente después de reiniciarse.

[#553886]

- Aparece un diálogo de mensaje incorrecto cuando el temporizador de fiabilidad de la sesión caduca.

[#556899]

- Aparece un mensaje de error (por ejemplo: "Unknown Error 1000047") al conectar con el VDA con el protocolo SSLv3 habilitado.

[#558641]

- Aparece un error de red genérico al conectarse a un servidor StoreFront con el protocolo SSLv3 habilitado.

[#558653]

- Cambiar el parámetro SharedUserMode mediante storebrowse, -c SharedUserMode[=valor], requiere coincidencia exacta (mayúsculas y minúsculas) entre las letras del parámetro de valor. Al usar el parámetro de valor para storebrowse, -c SharedUserMode[=valor], debe especificar las letras mayúsculas y minúsculas exactas mediante "True" o "False". No aparece ningún mensaje de error si se utiliza un parámetro de valor no válido. Por ejemplo: -c SharedUserMode=True.

[#559402]

- Al conectar con un servidor de terminales (por ejemplo, RDS) con solo el protocolo SSLv3 habilitado, la conexión falla, como es de esperar, pero puede que no falle con un error de contacto inicial (handshake) con el homólogo SSL.

[#567407]

- La entrada de cámara Web de USB genérico falla en sistemas de 64 bits.

[#568556]

- El comando storebrowse -d no elimina la información de almacén en caché previamente borrada, creada por selfservice. Lo que significa que, si a continuación se agrega el almacén, la interfaz de usuario de selfservice se cargará desde el estado anterior en caché.

[#569806]

- La Central de conexiones no admite IPv6.

[#571743]

- Al especificar un valor negativo para una entrada de configuración de número entero, como TCPRecvBufferSize en \$HOME/.ICAClient/All_Regions.ini, el valor se pasa erróneamente a WFICA como valor positivo. Para resolver este problema, use \$ICAROOT/config/module.ini para definir un valor negativo para TCPRecvBufferSize.

[#575474]

- Los servicios auxiliares de GStreamer muestran una advertencia relacionada con un problema de subprocesos de GLIB.

[#580753]

- El plug-in de explorador ARMEL no funciona en esta versión.

[#588044]

- El reproductor de Windows Media en un escritorio con Windows 7 iniciado desde Receiver para Linux de 64 bits no reproduce vídeo ni audio si el plug-in H264 de gstreamer no está disponible. Si esto ocurre, se invoca el vídeo generado por el servidor.

[#588298]

- Una sesión de pantalla completa no se puede reducir al modo de ventana mediante la barra de herramientas de Desktop Viewer si se utiliza el argumento "-span 0" para sobrescribir la redirección de ventanas de sesión.

Para solucionar este problema, no utilice la opción "-span 0". Use un administrador de ventanas con respaldo _NET_WM_FULLSCREEN_MONITORS o inhabilite Desktop Viewer.

[#634855]

- Es posible que la sesión secundaria no aparezca cuando se haga clic en su nombre bajo el botón Cambiar en Desktop Viewer.

[#648716]

- Receiver para Linux deja de responder indefinidamente cuando se cambia de la interfaz de usuario X1 a la clásica.

Si la interfaz de usuario de SelfService muestra el error "NoWebUI 0", reinicie el proceso selfservice para revertir la interfaz

de usuario de SelfService a la normal.

[#652810]

- La redirección de Flash usa la ubicación equivocada con clientes con varios monitores.

Cuando se usa la redirección de Flash en un cliente con varios monitores, el contenido Flash puede aparecer en el monitor equivocado o fuera de la pantalla. Para evitar este problema, compruebe que la sesión se ejecuta en todos los monitores disponibles antes de usar la funcionalidad de redirección de Flash.

[#653550]

- Actualizarse a esta versión puede producir errores debido a las opciones que se obtienen de All_Regions.ini.

[#654826]

- Al iniciarse el programa, la redirección de cámaras Web HDX se inhabilita durante 45 segundos.

Para evitarlo, agregue la entrada HDXRTMEWebCamLaunchDelayTime=0 a la sección [wfclient] de ~/.ICAClient/wfclient.ini (o %ICAROOT%/config/module.ini).

Si quiere usar el plug-in de RTME en vez de la redirección de cámaras Web HDX, no cambie este valor.

[#655775]

Requisitos del sistema

Jan 05, 2017

En este tema, se describen los requisitos del sistema y del usuario para instalar Citrix Receiver para Linux.

Dispositivos

- Kernel de Linux versión 2.6.29 o posterior, con respaldo para glibcxx 3.4.15 o posterior, glibc 2.11.3 o posterior, gtk 2.20.1 o posterior, libcap1 o libcap2 y udev.
- Para la interfaz de usuario de autoservicio:
 - libwebkit o libwebkitgtk 1.0
 - libxml2 2.7.8
 - libxerces-c 3.1
- Bibliotecas de códecs ALSA (libasound2), Speex y Vorbis.
- Al menos 20 MB de espacio libre en disco para la versión instalada de Receiver y al menos 40 MB si expande el paquete de instalación en el disco. Para comprobar el espacio en disco disponible, escriba el siguiente comando en una ventana de terminal:
df -k
- Al menos 1 GB de RAM para dispositivos SoC (system-on-a-chip) que usen la redirección de Flash de HDX MediaStream.
- Pantalla de vídeo de 256 colores o superior.
- Conexión de red TCP/IP.

H.264

Para los dispositivos x86, las velocidades de procesador de al menos 1.6 GHz muestran correctamente las sesiones de monitor único con las resoluciones típicas (por ejemplo, 1280 x 1024). Si utiliza la función HDX 3D Pro, se requiere un controlador de gráficos nativo acelerado por hardware y una velocidad de procesador mínima de 2 GHz.

Para dispositivos ARM, se requiere un decodificador de hardware H.264 para el respaldo general de H.264 y HDX 3D Pro. El rendimiento también es mejor con velocidades de reloj de procesador más altas.

Redirección de Flash HDX MediaStream

Para ver todos los requisitos de la redirección de Flash de HDX MediaStream, consulte [CTX134786](#).

Citrix recomienda hacer pruebas con el plug-in más reciente antes de implementar una nueva versión para, así, aprovechar las correcciones más recientes relacionadas con la seguridad y la funcionalidad.

Compresión de vídeo de cámara Web HDX RealTime

La compresión de vídeo de cámara Web HDX RealTime requiere:

- Una cámara Web compatible con Video4Linux.
- GStreamer 0.10.25 (o una versión posterior 0.10.x), incluido el paquete "plugins-good" de la distribución.

Redirección de Windows Media de HDX MediaStream

La redirección de Windows Media de HDX MediaStream requiere

- GStreamer 0.10.25 (o una versión posterior 0.10.x), incluido el paquete "plugins-good" de la distribución; en general, la versión 0.10.15 o posterior es suficiente para la redirección de Windows Media de HDX MediaStream.

Nota: Puede descargar GStreamer desde <http://gstreamer.freedesktop.org>. El uso de ciertos códecs puede requerir una licencia del fabricante de esa tecnología. Consulte con su departamento de asuntos legales para determinar si los códecs que piensa utilizar requieren licencias adicionales.

Phillips SpeechMike

Si piensa utilizar dispositivos Phillips SpeechMike con Receiver, es posible que deba instalar los controladores correspondientes en el dispositivo del usuario. Para obtener información y descargar el software, visite el sitio Web de Phillips.

Respaldo para tarjetas inteligentes

Para configurar el respaldo para tarjetas inteligentes en Citrix Receiver para Linux, primero debe configurar el sitio de servicios de StoreFront para habilitar la autenticación de tarjetas inteligentes.

Nota

Nota: Las tarjetas inteligentes no están respaldadas por el sitio de servicios XenApp para las configuraciones de Interfaz Web (antes, PNAgent) ni por el sitio "PNAgent antiguo" que puede proporcionar un servidor StoreFront.

Citrix Receiver para Linux respalda lectores de tarjeta inteligente que sean compatibles con PCSC-Lite y tarjetas inteligentes con controladores PKCS#11 para la plataforma correspondiente de Linux. Ahora, de forma predeterminada, Receiver para Linux ubica `opensc-pkcs11.so` en una de las ubicaciones estándar. Para asegurarse de que Receiver para Linux encuentra otro controlador PKCS#11 u `opensc-pkcs11.so` en una ubicación que no sea estándar, almacene la ubicación en un archivo de configuración mediante los siguientes pasos:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Busque la línea `PKCS11module` y agregue la ubicación del controlador al elemento que hay justo después de la línea.
Nota: Si se introduce un nombre de archivo para la ubicación del controlador, Receiver navega hasta ese archivo en el directorio `$ICAROOT/PKCS#11`. Si no, también puede utilizar una ruta de acceso absoluta si esta empieza por `"/`.

Para configurar el comportamiento de Citrix Receiver para Linux cuando se quita una tarjeta inteligente, actualice `SmartCardRemovalAction` en el archivo de configuración siguiendo estos pasos:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Busque la línea `SmartCardRemovalAction` y agregue `'noaction'` o `'forcelogoff'` al elemento que hay justo después de la línea.

El comportamiento predeterminado es `'noaction'`. No se realiza ninguna acción para borrar las credenciales almacenadas y los tokens generados al quitar tarjetas inteligentes. La acción `'forcelogoff'` borra todas las credenciales y tokens de StoreFront al quitar tarjetas inteligentes.

Servidores Citrix

- XenApp (cualquiera de los productos siguientes):
 - XenApp 7.9
 - XenApp 7.8
 - XenApp 7.7
 - XenApp 7.6

- XenApp 7.5
- XenApp 6.5, Feature Pack 2, para Windows Server 2008 R2
- XenApp 6.5, Feature Pack 1, para Windows Server 2008 R2
- XenApp 6.5 para Windows Server 2008 R2
- XenApp 6 para Windows Server 2008 R2
- XenApp 5 para Windows Server 2008
- XenDesktop (cualquiera de los productos siguientes):
 - XenDesktop 7.9
 - XenDesktop 7.8
 - XenDesktop 7.7
 - XenDesktop 7.6
 - XenDesktop 7.5
 - XenDesktop 7.1
 - XenDesktop 7.0
 - XenDesktop 5.6, Feature Pack 1
 - XenDesktop 5.6
 - XenDesktop 5.5
 - XenDesktop 5
- VDI-in-a-Box
 - VDI-in-a-Box 5.3
 - VDI-in-a-Box 5.2
- Se puede usar el acceso de explorador Web de Citrix Receiver para Linux 13.4 junto con Receiver para Web de StoreFront y la Interfaz Web, con o sin NetScaler Gateway Plug-in.

StoreFront:

- StoreFront 3.x, 2.6, 2.5 y 2.1
Para acceder directamente a almacenes de StoreFront.
- StoreFront configurado con un sitio de Citrix Receiver para Web
Para acceder a los almacenes de StoreFront a través de un explorador Web. Para ver las limitaciones de esta implementación, consulte "Consideraciones importantes" en [Sitios de Receiver para Web](#).

Interfaz Web junto con cliente NetScaler VPN:

- Sitios Web de Interfaz Web 5.4 para Windows.
Da acceso a aplicaciones y escritorios virtuales desde un explorador Web.
- Interfaz Web 5.4 para Linux con sitios de servicios XenApp o sitios de servicios XenDesktop.
- Formas de implementar Citrix Receiver para los usuarios:
 - Habilitar a los usuarios para descargarlo desde receiver.citrix.com y, a continuación, configurarlo mediante el uso de una dirección de correo electrónico o de servicios junto con StoreFront.
 - Ofrecer la instalación desde el sitio de Citrix Receiver para Web (configurado con StoreFront).
 - Ofrecer la instalación de Receiver desde la Interfaz Web de Citrix 5.4.

Explorador Web

- Mozilla Firefox 18.x (versión mínima respaldada)

- Google Chrome versión 21 ó 20 (requiere StoreFront).

Nota: Para obtener más información sobre cambios en el respaldo para Google Chrome NPAPI, consulte el artículo del blog de Citrix, [Preparing for NPAPI being disabled by Google Chrome](#).

Conectividad

Citrix Receiver para Linux respalda conexiones HTTPS y conexiones ICA sobre TLS a través de las siguientes configuraciones.

- Para conexiones LAN:
 - StoreFront con sitios de Receiver para Web o de servicios StoreFront
 - Interfaz Web 5.4 para Windows, mediante la Interfaz Web o sitios de servicios XenApp

Para obtener más información sobre dispositivos unidos a un dominio y dispositivos no unidos a un dominio, consulte la documentación de XenDesktop 7.

- Para conexiones locales o remotas seguras:
 - Citrix NetScaler Gateway 11.1
 - Citrix NetScaler Gateway 11.0
 - Citrix NetScaler Gateway 10.5
 - Citrix NetScaler Gateway 10.1
 - Citrix Access Gateway Enterprise Edition 10
 - Citrix Access Gateway Enterprise Edition 9.x
 - Citrix Access Gateway VPX

Para obtener información sobre las versiones de NetScaler Gateway y Access Gateway respaldadas en StoreFront, consulte los [requisitos del sistema para StoreFront](#).

Nota: Las referencias a NetScaler Gateway en este tema también se aplican a Access Gateway, a menos que se indique lo contrario.

Acerca de las conexiones seguras y los certificados

Nota: Para obtener más información sobre certificados de seguridad, consulte los temas en las secciones [Conexiones seguras](#) y [Comunicaciones seguras](#).

Certificados privados (autofirmados)

Si se ha instalado un certificado privado en la puerta de enlace remota, el certificado raíz de la entidad de certificación de la organización debe estar instalado en el dispositivo de usuario para poder acceder correctamente a los recursos de Citrix mediante Receiver.

Nota: Si el certificado de la puerta de enlace remota no se puede verificar en la conexión (debido a que no se incluyó el certificado raíz en el almacén de claves local), se muestra un mensaje de error sobre la presencia de un certificado que no es de confianza. El certificado raíz debe instalarse en el almacén de certificados del cliente.

Instalación de certificados raíz en los dispositivos de los usuarios

Para obtener más información sobre cómo instalar certificados raíz en los dispositivos de los usuarios además de configurar la Interfaz Web para el uso de certificados, consulte [Protección de las comunicaciones de Receiver](#).

Certificados comodín

Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo

dominio. Citrix Receiver para Linux respalda el uso de certificados comodín, aunque deben usarse solo de acuerdo con la directiva de seguridad de la organización. En la práctica, se puede considerar la posibilidad de usar alternativas a certificados comodines, como por ejemplo, un certificado que contenga la lista de nombres de servidor dentro de la extensión de nombre de sujeto alternativo (Subject Alternative Name o SAN). Estos certificados pueden ser emitidos por entidades de certificación tanto privadas como públicas.

Certificados intermedios y NetScaler Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá añadir este certificado intermedio al certificado de servidor de NetScaler Gateway. Para obtener información, consulte [Configuración de certificados intermedios](#).

Requisitos de usuario

Aunque no necesita iniciar sesión como usuario con privilegios (root) para instalar Citrix Receiver para Linux, el respaldo para USB se habilita únicamente si se ha iniciado sesión como usuario con privilegios al instalar y configurar Receiver. Sin embargo, las instalaciones realizadas por usuarios sin privilegios permitirán que los usuarios accedan a los recursos publicados con StoreFront a través de uno de los exploradores Web admitidos, o bien a través de la interfaz de usuario nativa de Receiver.

Compruebe si el dispositivo cumple los requisitos del sistema

Citrix ofrece un script, `hdxcheck.sh`, como parte del paquete de instalación de Receiver. El script comprueba si su dispositivo cumple con todos los requisitos del sistema para poder aprovechar todas las funcionalidades de Receiver para Linux. Este script está ubicado en el directorio Utilities del paquete de instalación.

Para ejecutar el script `hdxcheck.sh`

1. Abra una ventana de terminal.
2. Escriba `cd $ICAROOT/util` y presione `INTRO` para navegar hasta el directorio Utilities del paquete de instalación.
3. Escriba `./hdxcheck.sh` para ejecutar el script.

Instalación y configuración

Jan 05, 2017

A continuación se detallan los paquetes disponibles para Citrix Receiver para Linux. Puede acceder a los paquetes en la sección de descargas del [sitio Web](#) de Citrix.

Nombre del paquete	Contenido
Paquetes Debian (Ubuntu, Debian, Linux Mint, etc.)	
icaclient_13.4.0.10109380_amd64.deb	Respaldo para autosevicio, 64 bits x86_64
icaclient_13.4.0.10109380_i386.deb	Respaldo para autosevicio, 32 bits x86
icaclient_13.4.0.10109380_armhf.deb	Respaldo para autosevicio, ARM HF
icaclient_13.4.0.10109380_armel.deb	Respaldo para autosevicio, ARM EL
icaclientWeb_13.4.0.10109380_amd64.deb	Solo Receiver para Web, 64 bits x86_64
icaclientWeb_13.4.0.10109380_i386.deb	Solo Receiver para Web, 32 bits x86
icaclientWeb_13.4.0.10109380_armhf.deb	Solo Receiver para Web, ARM HF
icaclientWeb_13.4.0.10109380_armel.deb	Solo Receiver para Web, ARM EL
ctxusb_2.7.10109380_amd64.deb	Paquete USB, 64 bits x86_64
ctxusb_2.7.10109380_i386.deb	Paquete USB, 32 bits x86
ctxusb_2.7.10109380_armhf.deb	Paquete USB, ARM HF
ctxusb_2.7.10109380_armel.deb	Paquete USB, ARM EL
Paquetes RedHat (RedHat, SUSE, Fedora, etc.)	
ICAClient-rhel-13.4.0.10109380-0.x86_64.rpm	Respaldo para autosevicio, basado en RedHat (incluido VDA Linux), 64 bits x86_64

ICAClient-rhel-13.4.0.10109380-0.i386.rpm	Respaldo para autoserivicio, basado en RedHat, 32 bits x86
ICAClientWeb-rhel-13.4.0.10109380-0.x86_64.rpm	Solo Receiver para Web, basado en RedHat, 64 bits x86_64
ICAClientWeb-rhel-13.4.0.10109380-0.i386.rpm	Solo Receiver para Web, basado en RedHat, 32 bits x86
ICAClient-suse-13.4.0.10109380-0.x86_64.rpm	Respaldo para autoserivicio, basado en SUSE, 64 bits x86_64
ICAClient-suse-13.4.0.10109380-0.i386.rpm	Respaldo para autoserivicio, basado en SUSE, 32 bits x86
ICAClient-suse11sp3-13.4.0.10109380-0.x86_64.rpm	Respaldo para autoserivicio, basado en SUSE 11 sp3 (incluido VDA Linux), 64 bits x86_64
ICAClient-suse11sp3-13.4.0.10109380-0.i386.rpm	Respaldo para autoserivicio, basado en SUSE 11 sp3, 32 bits x86
ICAClientWeb-suse-13.4.0.10109380-0.x86_64.rpm	Solo Receiver para Web, basado en SUSE, 64 bits x86_64
ICAClientWeb-suse-13.4.0.10109380-0.i386.rpm	Solo Receiver para Web, basado en SUSE, 32 bits x86
ctxusb-2.7.10109380-1.x86_64.rpm	Paquete USB, 64 bits x86_64
ctxusb-2.7.10109380-1.i386.rpm	Paquete USB, 32 bits x86
Tarballs (Instalación por script para cualquier distribución)	
linuxx64-13.4.0.10109380.tar.gz	Intel de 64 bits
linuxx86-13.4.0.10109380.tar.gz	Intel de 32 bits
linuxarmhf-13.4.0.10109380.tar.gz	ARM EL
linuxarm-13.4.0.10109380.tar.gz	ARM HF

La diferencia entre paquetes que ofrecen respaldo para Receiver para Web y los que ofrecen respaldo para autoserivicio es que estos últimos requieren de otros elementos dependientes para el autoserivicio además de los necesarios para Receiver

para Web. Los elementos dependientes para el autoservicio son un conjunto más grande que los requeridos para Receiver para Web, pero los archivos instalados son idénticos.

Si solo requiere respaldo para Receiver para Web o si su distribución no cuenta con los paquetes necesarios para dar respaldo al autoservicio, instale el paquete que solo incluye Receiver para Web.

Nota

Si su distribución lo permite, instale Citrix Receiver desde el paquete Debian o desde el paquete RPM. Estos archivos suelen ser más fáciles de usar, ya que instalan automáticamente los paquetes que sean necesarios. Si quiere controlar la ubicación de instalación, instale Citrix Receiver desde el paquete tarball.

Para instalar Citrix Receiver para Linux desde un paquete Debian

Si quiere instalar Receiver desde el paquete Debian en Ubuntu, es conveniente que abra los paquetes en el Centro de software de Ubuntu.

En las siguientes instrucciones, reemplace **nombre_del_paquete** por el nombre del paquete que desea instalar.

Este procedimiento usa una línea de comandos y el administrador de paquetes nativo de Ubuntu/Debian/Mint. En su lugar, puede instalar el paquete haciendo doble clic en el paquete .deb descargado, dentro del explorador de archivos. Normalmente, se inicia un administrador de paquetes que descarga el software necesario que falte. Si no hay ningún administrador de paquetes disponible, Citrix recomienda usar **gdebi**, una herramienta de línea de comandos que realiza esta función.

Para instalar el paquete usando la línea de comandos

1. Inicie sesión como usuario con privilegios (root).
2. Abra una ventana de terminal.
3. Ejecute la instalación de los 3 paquetes siguientes, escribiendo **gdebi nombreDelpaquete.deb**. Por ejemplo:
 - gdebi icaclient_13.4.0.10109380_amd64.deb
 - gdebi icaclientWeb_13.4.0.10109380_amd64.deb
 - gdebi ctxusb_2.7.10109380_amd64.deb

Nota: Para usar dpkg en los ejemplos anteriores, reemplace “gdebi” por “dpkg -i”.

El usuario debe instalar el paquete icaclient o el paquete icaclientWeb. El paquete ctxusb es opcional y ofrece respaldo a la redirección USB genérica.

4. Si usa dkpg, escriba **sudo apt-get -f install** para instalar las dependencias que falten.
5. Acepte el contrato de licencia (EULA).

Para instalar Citrix Receiver para Linux desde un paquete RPM

Si está instalando Citrix Receiver con el paquete RPM en SUSE, use las utilidades YaST o Zypper, en lugar de rpm. La utilidad rpm no descarga ni instala los paquetes dependientes necesarios, solo instala el paquete .rpm. Si faltan paquetes dependientes necesarios, verá un error.

Nota: Para seguir un ejemplo de una instalación con un paquete RPM, consulte este artículo del Blog de Citrix: "[Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop.](#)"

En las siguientes instrucciones, reemplace **nombre_del_paquete** por el nombre del paquete que desea instalar.

Nota: Si recibe un error donde se indica que la instalación requiere "libwebkitgtk-1.0.so.0" en distribuciones basadas en Red Hat (RHEL, CentOS, Fedora, etc.), debe agregar el repositorio EPEL (consulte <https://fedoraproject.org/wiki/EPEL>), que puede suministrar el paquete que falta, o cambie la variante Web del paquete.

Para configurar el repositorio EPEL en Red Hat

1. Descargue el paquete fuente RPM apropiado desde aquí:

https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3

2. Por ejemplo, para Red Hat Enterprise 7.x:

```
yum localinstall epel-release-latest-7 .noarch.rpm
```

Sugerencia: El Administrador de paquetes RPM no instala el software necesario que falte. Para descargarlo e instalarlo, Citrix recomienda usar **zypper install <nombre de archivo>** en una línea de comandos en OpenSUSE, o bien **yum localinstall <nombre de archivo>** en Fedora/RedHat.

Después de configurar el repositorio EPEL, instale Receiver desde el paquete RPM

1. Inicie sesión como usuario con privilegios (root).

2. Escriba zypper en nombreDelpaquete.rpm para ejecutar la instalación de los 3 paquetes siguientes.

Nota: El usuario debe instalar el paquete icaclient o el paquete icaclientWeb. El paquete ctxusb es opcional y ofrece respaldo a la redirección USB genérica.

3. Abra una ventana de terminal.

Para instalaciones en SUSE:

```
zypper in ICAClient-suse-13.4.0.10109380-0.x86_64.rpm
```

```
zypper in ICAClient-suse-13.4.0.10109380-0.i386.rpm
```

```
zypper in ctxusb-2.7.10109380-1.x86_64.rpm
```

Para instalaciones en Red Hat:

```
yum localinstall ICAClient-rhel-13.4.0.10109380-0.i386.rpm
```

```
yum localinstall ICAClientWeb-rhel-13.4.0.10109380-0.i386.rpm
```

```
yum localhost ctxusb-2.7.10109380-1.i386.rpm
```

4. Acepte el contrato de licencia (EULA).

Para instalar Citrix Receiver para Linux desde un paquete tarball

Nota: El paquete tarball no comprueba ni instala los elementos dependientes que falten. Es necesario resolver por separado

todas las dependencias del sistema.

1. Abra una ventana de terminal.
2. Descomprima el archivo .tar.gz y extraiga el contenido en un directorio temporal vacío. Por ejemplo, escriba: `tar xvfz nombre_del_paquete.tar.gz`.
3. Escriba `./setupwfc` y presione Intro para ejecutar el programa de instalación.
4. Acepte el valor predeterminado de 1 (para instalar Receiver) y presione Intro.
5. Escriba la ruta y el nombre del directorio de instalación requerido y, a continuación, presione Intro; también puede presionar directamente Intro para instalar Receiver en la ubicación predeterminada.

El directorio predeterminado para las instalaciones de usuarios con privilegios (root) es `/opt/Citrix/ICAClient`.

El directorio predeterminado para las instalaciones de usuarios sin privilegios es `$HOME/ICAClient/plataforma`.

Donde `platform` es un identificador generado por el sistema para el sistema operativo que tenga instalado. Por ejemplo, `$HOME/ICAClient/linuxx86` para la plataforma Linux/x86).

Nota: Si especifica una ubicación no predeterminada, establézcala en `$ICAROOT` en `$HOME/.profile` o `$HOME/.bash_profile`.

6. Cuando se le solicite continuar, escriba `y`, y luego presione Intro.

7. Es posible elegir si se quiere integrar Receiver en el entorno del escritorio. La instalación crea una opción de menú desde la cual los usuarios pueden iniciar Receiver. Escriba `y` en el símbolo del sistema para habilitar la integración.

Nota: Para garantizar que la integración funcione correctamente cuando Receiver se instala en una ubicación distinta a la predeterminada, establezca la ubicación en `$ICAROOT` en `$HOME/.profile` o `$HOME/.bash_profile`.

8. Si ya ha instalado GStreamer, puede elegir si quiere integrar GStreamer en Receiver y, así, ofrecer respaldo a la aceleración multimedia HDX MediaStream. Para integrar Receiver en GStreamer, escriba `y` en el símbolo del sistema.

Nota: En algunas plataformas, si se instala el cliente desde una distribución de tarball, el sistema se cuelga después de pedir al usuario la integración con KDE y GNOME. Este problema ocurre con la primera inicialización de `gst-0.10`. Si encuentra este problema, cancele el proceso de instalación (usando `ctrl+c`) y ejecute este comando: **`gst-inspect-0.10 --gst-disable-registry-fork --version`**. Después de ejecutar este comando, puede volver a ejecutar la instalación tarball sin que se cuelgue el sistema.

9. Si inicia sesión como usuario con privilegios (root), elija instalar el respaldo USB para aplicaciones VDI publicadas con XenDesktop y XenApp. Escriba `y` en el símbolo del sistema para instalar el respaldo USB.

Nota: Si no ha iniciado sesión como usuario con privilegios (root), aparecerá un mensaje para advertirle que solo los usuarios root pueden instalar el respaldo USB. Ejecute el instalador como root para acceder a esta opción de instalación.

10. Cuando la instalación se haya completado, volverá a aparecer el menú principal de la instalación. Para salir del programa de instalación, escriba `3` y pulse Intro.

Personalización de la instalación de Citrix Receiver para Linux

Jan 05, 2017

Para personalizar la configuración antes de la instalación, modifique el contenido del paquete de Citrix Receiver y, a continuación, vuelva a empaquetar los archivos. Los cambios se incluirán en todas las versiones instaladas con el paquete modificado.

Nota

Para seguir un ejemplo de una instalación, consulte este artículo del Blog de Citrix: "[Installing Citrix Receiver for Linux 13.2.1 on SUSE Linux Enterprise Desktop.](#)"

Para personalizar una instalación de Citrix Receiver para Linux

1. Expanda el archivo del paquete de Citrix Receiver en un directorio vacío. El archivo del paquete se llama `plataforma.mayor.menor.versión.compilación.tar.gz` (por ejemplo, `linuxx86.13.2.0.nnnnnn.tar.gz` para la plataforma Linux/x86).
2. Realice los cambios requeridos en el paquete de Receiver. Por ejemplo, puede agregar un nuevo certificado raíz TLS al paquete si desea utilizar un certificado de una entidad de certificación que no forma parte de la instalación estándar de Receiver. Para agregar un nuevo certificado raíz TLS al paquete, consulte *— Instalación de certificados raíz en los dispositivos de usuario* en el sitio de documentación de productos de Citrix. Para obtener más información acerca de los certificados integrados, consulte *— Configuración y habilitación de SSL y TLS* en sitio de documentación de productos de Citrix.
3. Abra el archivo `PkgID`.
4. Agregue la siguiente línea para indicar que se ha modificado el paquete: `MODIFIED=traceinfo` donde `traceinfo` es la información que indica quién realizó el cambio y cuándo lo hizo. El formato exacto de esta información no es importante.
5. Guarde y cierre el archivo.
6. Abra la lista de archivos del paquete, `plataforma/plataforma.psf` (por ejemplo, `linuxx86/linuxx86.psf` para la plataforma Linux/x86).
7. Actualice la lista de archivos del paquete para reflejar los cambios que ha realizado al paquete. Si no actualiza este archivo, pueden producirse errores al instalar el paquete nuevo. Los cambios pueden consistir en una actualización en el tamaño de todos los archivos modificados, o la inclusión de nuevas líneas para cualquiera de los archivos agregados al paquete. Las columnas en la lista de archivos del paquete son:
 - Tipo de archivo
 - Ruta relativa
 - Subpaquete (que siempre debe estar configurado como `cor`)
 - Permisos
 - Propietario
 - Grupo
 - Tamaño
8. Guarde y cierre el archivo.

9. Use el comandotar para volver a generar el archivo del paquete de Receiver; por ejemplo:tar czf ../nuevoPaquete.tar.gz *
donde nuevoPaquete es el nombre del nuevo archivo del paquete de Receiver.

Inicio de Citrix Receiver para Linux

Jan 05, 2017

Puede iniciar Citrix Receiver desde una interfaz de terminal o desde alguno de los entornos de escritorio respaldados.

Si Citrix Receiver no se instaló en el directorio de instalación predeterminado, asegúrese de que la variable de entorno ICAROOT esté configurada para apuntar al directorio de instalación real.

Sugerencia

Las instrucciones siguientes no se aplican a instalaciones realizadas a partir de paquetes Web ni a aquellas en que se usa tarball, pero los requisitos de selfservice no se han cumplido.

Para iniciar Citrix Receiver en el símbolo del sistema de un terminal

En el símbolo del sistema, escriba `/opt/Citrix/ICAClient/selfservice` y presione INTRO (donde `/opt/Citrix/ICAClient` es el directorio en el que se instaló Citrix Receiver).

Para iniciar Citrix Receiver desde el escritorio Linux

Para iniciar Citrix Receiver desde un entorno de escritorio para Linux, búsquelo con un administrador de archivos.

En algunos escritorios, también puede iniciar Citrix Receiver desde un menú. Receiver puede estar ubicado en distintos menús, según la distribución de Linux que se esté utilizando.

Uso de Citrix Receiver para Linux como proxy de ICA a X

Jan 05, 2017

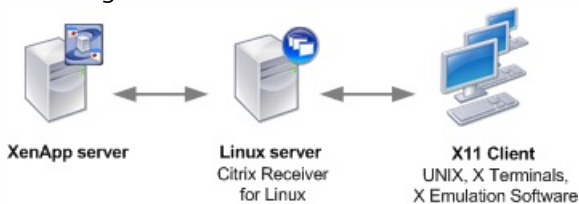
Puede utilizar una estación de trabajo que ejecuta Citrix Receiver como servidor y redirigir la salida a otro dispositivo compatible con X11. Se recomienda realizar esto para entregar aplicaciones de Microsoft Windows a terminales X o estaciones de trabajo UNIX en las que Citrix Receiver no está disponible.

Nota

El software de Citrix Receiver está disponible para muchos dispositivos X y en esos casos la mejor solución es instalar el software en los dispositivos. Esta forma de ejecutar Citrix Receiver, como proxy de ICA a X, se conoce también como ICA en el lado del servidor.

Cuando se ejecuta Citrix Receiver, se lo puede considerar como un conversor de ICA a X11 que dirige la salida de X11 al escritorio de Linux local. Sin embargo, también es posible redirigir la salida a otra pantalla de X11. De este modo, puede ejecutar simultáneamente varias copias de Citrix Receiver en un sistema para que cada una de ellas envíe su salida a un dispositivo diferente.

En este gráfico se muestra un sistema con Citrix Receiver para Linux configurado como proxy de ICA a X:



Para configurar este tipo de sistema, necesita un servidor Linux que actúe como el proxy de ICA a X11:

- Si ya tiene terminales X, puede ejecutar Citrix Receiver en el servidor Linux que normalmente proporciona las aplicaciones X para los terminales X.
- Si desea implementar estaciones de trabajo UNIX en las que Citrix Receiver no está disponible, necesita tener un servidor adicional que actúe como proxy. Esta función puede cumplirla un PC que ejecute Linux.

Funcionalidades admitidas

El dispositivo final recibe las aplicaciones a través de X11, usando las capacidades del protocolo ICA. De forma predeterminada, puede utilizar la asignación de unidades solamente para acceder a las unidades en el proxy. Esto no supone ningún problema si utiliza terminales X que, por lo general, no tienen unidades locales. Si distribuye aplicaciones a otras estaciones de trabajo UNIX, puede:

- Montar la estación de trabajo UNIX local mediante NFS en la estación de trabajo que actúa como proxy y, a continuación, crear una asignación de unidad del cliente al punto de montaje NFS en el proxy.
- Utilizar un proxy de NFS a SMB, como SAMBA, o bien, un cliente NFS en el servidor, como Microsoft Services para UNIX.

Algunas funciones no se transfieren al dispositivo final:

- No se transferirá sonido al dispositivo X11, aunque el servidor que actúa como proxy admita sonido.

- Las impresoras de los clientes no se transfieren al dispositivo X11. Debe acceder a la impresora de UNIX desde el servidor de forma manual a través de la impresión LPD, o bien, utilizar una impresora de red.

Para iniciar Citrix Receiver con ICA en el lado del servidor desde un terminal X o una estación de trabajo UNIX

1. Utilice ssh o telnet para conectarse al dispositivo que actúa como proxy.
2. En un intérprete de comandos del dispositivo proxy, configure la variable de entorno **DISPLAY** para el dispositivo local. Por ejemplo, en un intérprete de comandos de C, escriba:
setenv DISPLAY <local:0>

Nota: Si utiliza el comando ssh -X para conectarse al dispositivo que actúa como proxy, no necesita configurar la variable de entorno **DISPLAY**.

3. En un símbolo del sistema del dispositivo local, escriba xhost <nombre del servidor proxy>
4. Si Receiver no está instalado en el directorio de instalación predeterminado, asegúrese de que la variable de entorno ICAROOT esté configurada para apuntar hacia el directorio de instalación real.
5. Ubique el directorio donde está instalado Citrix Receiver. Escriba lo siguiente en una interfaz de comandos: selfservice &

Para desinstalar Citrix Receiver para Linux

Jan 05, 2017

Este procedimiento se ha probado con el paquete tarball. Quite los paquetes RPM y Debian usando las herramientas estándar del sistema operativo.

La variable de entorno ICAROOT se debe establecer en el directorio de instalación del cliente. El directorio predeterminado para las instalaciones de usuarios sin privilegios es \$HOME/ICAclient/plataforma. La variable plataforma es un identificador generado por el sistema para el sistema operativo que tenga instalado. Por ejemplo, \$HOME/ICAclient/linuxx86 para la plataforma Linux/x86. La ubicación predeterminada en la instalación con un usuario con permisos es /opt/Citrix/ICAclient.

1. Ejecute el programa de instalación; para ello, escriba \$ICAROOT/setupwfc y presione INTRO.
2. Para quitar el cliente, escriba 2 y presione INTRO.

Nota

Para desinstalar Citrix Receiver para Linux tiene que haber iniciado una sesión con la misma cuenta de usuario que utilizó para instalarlo.

Conectar

Jan 05, 2017

Citrix Receiver ofrece a los usuarios acceso de autoseguro de aplicaciones y escritorios virtuales, y acceso bajo demanda a aplicaciones de Windows, Web y de Software como servicio (SaaS). Las páginas Web de Citrix StoreFront, o las páginas Web antiguas creadas con la Interfaz Web, administran el acceso de los usuarios.

Para conectarse a los recursos mediante la interfaz de usuario de Citrix Receiver

La página de inicio de Citrix Receiver muestra las aplicaciones y los escritorios virtuales que están disponibles para los usuarios, basándose en los parámetros de cuenta del usuario (es decir, el servidor al que se conecta) y en los parámetros configurados por los administradores de Citrix XenApp o Citrix XenDesktop. Mediante la página Preferencias > Cuentas, los usuarios pueden realizar esa configuración por sí mismos escribiendo la dirección URL de un servidor StoreFront o, si la detección de cuentas basada en correo electrónico está configurada, escribiendo su dirección de correo electrónico.

Sugerencia

Si se utiliza el mismo nombre para varios almacenes en el servidor StoreFront, la página Cuentas mostrará esos almacenes como iguales. Para evitar confundir a los usuarios de este modo, los administradores deben utilizar nombres de almacén únicos al configurarlos. Para PNAgent, se muestra la URL del almacén y esta identifica de manera exclusiva dicho almacén.

Después de conectarse a un almacén, los usuarios pueden buscar escritorios y aplicaciones, o examinarlos, haciendo clic en el signo más (+) en la página de inicio de Citrix Receiver. Al hacer clic en el icono de un escritorio o de una aplicación, el recurso se copia a la página de inicio, desde la que los usuarios pueden iniciarlo con otro clic. Cuando lo hacen, se crea una conexión.

Configuración de los parámetros de conexión

Puede configurar distintos parámetros predeterminados para las conexiones entre Citrix Receiver y los servidores de XenApp y XenDesktop. También puede cambiar esos parámetros para conexiones individuales, si es necesario.

El resto de esta sección contiene procedimientos que ofrecen respaldo para la realización de tareas típicas de los usuarios de Citrix Receiver. Aunque las tareas y responsabilidades de los administradores y los usuarios pueden superponerse, en esta sección el término “usuario” se emplea para distinguir las tareas generales de los usuarios de las realizadas típicamente por los administradores.

- [Conexión con recursos desde una línea de comandos o explorador](#)
- [Solución de problemas en las conexiones con recursos](#)
- [Personalización de Receiver mediante archivos de configuración](#)

Conexión con recursos desde una línea de comandos o explorador

Jan 05, 2017

Cuando se hace clic en el icono de una aplicación o de un escritorio en la página de inicio de Receiver se crea una conexión con un servidor. Además, se pueden abrir conexiones desde una línea de comandos o desde un explorador Web.

Para crear una conexión a un servidor StoreFront o Program Neighborhood usando una línea de comandos

Como requisito previo, asegúrese de que el almacén está disponible en el servidor. Si es necesario, agréguelo mediante el comando siguiente:

```
./util/storebrowse --addstore
```

1. Obtenga el ID único del escritorio o de la aplicación con que desea conectarse. Esta es la primera cadena entre comillas en una línea adquirida en uno de los siguientes comandos:

- Lista de todos los escritorios y las aplicaciones en el servidor:

```
./util/storebrowse -E
```

- Lista de los escritorios y las aplicaciones a los que se ha suscrito:

```
./util/storebrowse -S
```

2. Ejecute el siguiente comando para iniciar el escritorio o la aplicación:

```
./util/storebrowse -L
```

Si no puede conectarse con un servidor, es posible que el administrador tenga que cambiar la ubicación del servidor o los detalles del proxy SOCKS. Para obtener información más detallada, consulte [Conexión a través de un servidor proxy](#).

Para crear una conexión desde un explorador Web

Si configura Mozilla, Netscape o Chrome, normalmente la configuración de la conexión se lleva a cabo automáticamente durante la instalación.

Si necesita configurar de forma manual los archivos .mailcap y MIME para Firefox, Mozilla o Chrome, utilice las siguientes modificaciones para que los archivos .ica inicien el archivo ejecutable de Receiver, wfica. Para utilizar otros exploradores, debe modificar la configuración del explorador, según corresponda.

1. Para modificar el archivo .mailcap, en \$HOME, cree o modifique el archivo .mailcap y agregue la línea:
application/x-ica; /opt/Citrix/ICAClient/wfica.sh %s; x-mozilla-flags=plugin:Citrix ICA
2. Para modificar el archivo MIME, en \$HOME, cree o modifique el archivo de tipos .mime y agregue la línea:
application/x-ica ica

La cadena x- delante del formato ica indica que ica es un tipo MIME no oficial que no es compatible con la Agencia de asignación de números de Internet (IANA).

Solución de problemas en las conexiones con recursos

Jan 05, 2017

Los usuarios pueden administrar sus conexiones activas con la Central de conexiones. La Central de conexiones es una herramienta de productividad que permite a usuarios y administradores solucionar inconvenientes en conexiones lentas o problemáticas. Con la Central de conexiones, los usuarios pueden administrar las conexiones de este modo:

- Cerrar aplicaciones.
- Cerrar la sesión. Esto finaliza la sesión y cierra todas las aplicaciones que hubiera abiertas.
- Desconectarse de una sesión. Esto interrumpe la conexión seleccionada con el servidor sin cerrar ninguna aplicación que haya abierta (a menos que el servidor esté configurado para cerrar aplicaciones en caso de desconexión)
- Ver estadísticas de transporte de la conexión.

Para administrar una conexión

1. En el menú de Receiver, haga clic en Central de conexiones.
Se muestran los servidores que se están utilizando y, para cada servidor, hay una lista de sesiones activas.
2. Lleve a cabo una de las siguientes acciones:
 - Seleccione un servidor y desconéctese de él, cierre la sesión en él, o vea sus propiedades.
 - Seleccione una aplicación y cierre la ventana en la que se muestra.

Personalización mediante archivos de configuración

Jan 05, 2017

Acerca de los archivos de configuración

Para cambiar parámetros más avanzados o menos comunes, puede modificar los archivos de configuración de Receiver. Estos archivos de configuración se leen cada vez que wfica se inicia. Puede actualizar distintos tipos de archivos en función del efecto que desee lograr con los cambios.

Tenga en cuenta que, si el uso compartido de sesiones está habilitado, puede que se use una sesión existente en lugar de una recién configurada. Esto puede hacer que la sesión ignore los cambios hechos en el archivo de configuración.

Aplicación de cambios para todos los usuarios de Citrix Receiver

Si desea que los cambios se apliquen a todos los usuarios de Citrix Receiver, modifique el archivo de configuración module.ini en el directorio \$ICAROOT/config.

Nota

No necesita agregar una entrada a All_Regions.ini para que se lea un valor de configuración desde module.ini, a menos que desee que otros archivos de configuración anulen el valor en module.ini. Si una entrada en All_Regions.ini configura un valor predeterminado, no se utilizará el valor en module.ini.

Aplicación de cambios para los usuarios nuevos de Citrix Receiver

Si el archivo \$HOME/.ICAClient/wfclient.ini no existe, wfica lo crea copiando \$ICAROOT/config/wfclient.template. Los cambios que realice en este archivo de plantilla se aplicarán a todos los usuarios nuevos de Citrix Receiver a partir del cambio.

Aplicación de cambios para todas las conexiones de usuarios específicos

Si desea que los cambios se apliquen a todas las conexiones de un usuario específico, modifique el archivo wfclient.ini en el directorio \$HOME/.ICAClient de ese usuario. La configuración de este archivo se aplica a las conexiones futuras de ese usuario.

Validación de las entradas del archivo de configuración

Si desea limitar los valores permitidos para las entradas en wfclient.ini, puede especificar las opciones o los rangos de opciones permitidos en All_Regions.ini. Para obtener más información, consulte el archivo All_Regions.ini en el directorio \$ICAROOT/config.

Nota

Si una entrada aparece en más de un archivo de configuración, su valor en wfclient.ini tiene prioridad sobre su valor en module.ini.

Acerca de los parámetros de los archivos

Los parámetros enumerados en cada archivo se agrupan en secciones. Cada sección comienza con un nombre entre corchetes que indica que sus parámetros están relacionados; por ejemplo, [ClientDrive] para los parámetros relacionados con la asignación de unidades del cliente.

Se proporcionan valores predeterminados automáticamente para los parámetros que falten excepto donde se indique. Si el parámetro está presente, pero no tiene ningún valor asignado, el valor predeterminado se aplica automáticamente; por ejemplo, si InitialProgram está seguido de un signo igual (=), pero no hay ningún valor, se aplica el valor predeterminado para este parámetro (que es no ejecutar ningún programa después de iniciar sesión).

Precedencia

All_Regions.ini especifica qué parámetros se pueden establecer por otros archivos. Puede restringir los valores de los parámetros o establecerlos de forma precisa. Si desea que los cambios se apliquen a todos los usuarios de Receiver, modifique module.ini.

Para una conexión cualquiera, los archivos normalmente se comprueban por este orden:

1. All_Regions.ini. Los valores de este archivo anulan los de:
 - El archivo .ica de la conexión
 - wfclient.ini
2. module.ini. Los valores de este archivo se utilizan si no se han establecido en All_Regions.ini, el archivo .ica de la conexión o wfclient.ini, pero no están limitados por entradas de All_Regions.ini.

Si no se encuentra ningún valor en ninguno de estos archivos, se usa el valor predeterminado en el código de Receiver.

Nota

Hay excepciones en este orden de prioridad. Por ejemplo, el código lee algunos valores específicamente de wfclient.ini por razones de seguridad, para asegurarse de que no se han establecido por un servidor.

Configuración de conexiones con Citrix XenApp (anteriormente PNAgent) usando la Interfaz Web

Jan 05, 2017

Este tema solo es aplicable a implementaciones que usan servicios XenApp en la Interfaz Web o el "PNAgent antiguo" en StoreFront.

Las opciones selfservice, storebrowse y pnbrowse permiten que los usuarios se conecten con recursos publicados (es decir, aplicaciones publicadas y escritorios de servidor) a través de un servidor que ejecuta un sitio de servicios XenApp. Estos programas pueden iniciar conexiones directamente o se pueden usar para crear elementos de menú a través de los cuales los usuarios pueden acceder a recursos publicados. pnbrowse también puede crear elementos de escritorio con este fin.

Las opciones personalizables para todos los usuarios que ejecutan Citrix XenApp en la red se definen en un archivo de configuración, config.xml, que se almacena en el servidor de la Interfaz Web. Cuando un usuario inicia uno de estos programas, el programa lee los datos de configuración desde el servidor. Después de eso, actualiza periódicamente su configuración e interfaz de usuario, en los intervalos especificados en el archivo config.xml.

Important

El archivo config.xml afecta a todas las conexiones definidas por el sitio de servicios XenApp.

Publicar contenido

Un sitio de servicios XenApp también puede publicar un archivo, en lugar de una aplicación o un escritorio. Este proceso se denomina publicación de contenido y permite que pnbrowse abra el archivo publicado.

Existe una limitación en los tipos de archivos que reconoce Receiver. Para que el sistema reconozca el tipo de archivo del contenido publicado y que los usuarios lo vean a través de Receiver, debe asociarse una aplicación publicada con el tipo de archivo publicado. Por ejemplo, para ver un archivo Adobe PDF publicado a través de Receiver, debe publicarse una aplicación como Adobe PDF Viewer. A menos que se publique una aplicación adecuada, los usuarios no podrán ver el contenido publicado.

Optimización

Jan 05, 2017

Al optimizar el entorno, obtendrá el mejor rendimiento de Citrix Receiver y ofrecerá la mejor experiencia para el usuario. Puede mejorar y optimizar el rendimiento mediante lo siguiente:

- [Asignación de dispositivos de usuario](#)
- [Configuración del respaldo USB](#)
- [Mejora del rendimiento en conexiones con poco ancho de banda](#)
- [Optimización del rendimiento multimedia](#)
- [Optimización del rendimiento de los cuadros de pantalla](#)

Asignación de dispositivos de usuario

Citrix Receiver admite la asignación de dispositivos del cliente para conexiones a servidores XenApp y XenDesktop. La asignación de dispositivos del cliente permite que una aplicación remota que se ejecuta en el servidor acceda a dispositivos conectados al dispositivo del usuario local. El usuario puede usar las aplicaciones y los recursos del sistema como si se ejecutaran localmente. Antes de utilizar estas funciones, asegúrese de que el servidor admita la asignación de dispositivos del cliente.

Nota: El modelo de seguridad SELinux, Security-Enhanced Linux, puede afectar al funcionamiento de la asignación de unidades del cliente y la redirección USB (tanto en XenApp como en XenDesktop). Si se requieren estas características, inhabilite SELinux antes de configurarlas en el servidor.

Asignación de unidades del cliente

La asignación de unidades del cliente permite redirigir letras de unidades del servidor de XenApp o XenDesktop a directorios existentes en el dispositivo del usuario local. Por ejemplo, la unidad H de una sesión de un usuario de Citrix se puede asignar a un directorio en el dispositivo del usuario local que ejecuta Receiver.

La asignación de unidades del cliente puede hacer que cualquier directorio montado en el dispositivo del usuario local, incluidos CD-ROM, DVD o dispositivos USB portátiles, esté disponible para el usuario durante una sesión, siempre que el usuario local tenga permiso para acceder a él. Cuando un servidor está configurado para permitir la asignación de unidades del cliente, los usuarios pueden acceder a los archivos guardados localmente, trabajar con ellos durante su sesión y, luego, guardarlos nuevamente en una unidad local o en una unidad del servidor.

Existen dos tipos de asignación de unidades disponibles:

- **Asignación de unidades del cliente estática:** Permite que los administradores asignen cualquier parte del sistema de archivos del dispositivo del usuario a una letra de unidad especificada en el servidor cuando se inicia la sesión. Por ejemplo, puede utilizarse para asignar total o parcialmente el directorio de inicio (home) o /tmp de un usuario, y también los puntos de montaje de dispositivos de hardware como CD-ROM, DVD o dispositivos de memoria USB.
- **Asignación de unidades del cliente dinámica:** Supervisa los directorios en los que, por lo general, los dispositivos de hardware como CD-ROM, DVD y dispositivos USB portátiles se montan en el dispositivo del usuario, y todos los dispositivos nuevos que aparezcan durante una sesión se asignan automáticamente a la siguiente letra de unidad disponible en el servidor.

Cuando Citrix Receiver se conecta a XenApp o XenDesktop, se restablecen las asignaciones de unidades del cliente a menos que la asignación de dispositivos del cliente esté inhabilitada. También pueden utilizarse directivas para tener mayor control sobre la forma en que se aplica la asignación de dispositivos del cliente. Para obtener más información, consulte la

documentación de [XenApp](#) y [XenDesktop](#).

Los usuarios pueden asignar unidades mediante el cuadro de diálogo Preferencias. Para obtener más información, consulte [Definición de preferencias](#).

Nota: De manera predeterminada, al habilitar la asignación de unidades del cliente estática también se habilita la asignación de unidades del cliente dinámica. Para inhabilitar esta última dejando habilitada la primera, configure DynamicCDM con el valor False en wfclient.ini.

Asignación de impresoras del cliente

Citrix Receiver respalda la impresión en impresoras de red e impresoras conectadas localmente a los dispositivos de usuario. De forma predeterminada, a menos que se creen directivas para modificarlo, XenApp permite a los usuarios:

- Imprimir en todos los dispositivos de impresión accesibles desde el dispositivo de usuario.
- Agregar impresoras

Sin embargo, es posible que estos parámetros no sean los adecuados para todos los entornos. Por ejemplo, la configuración predeterminada que permite a los usuarios imprimir en todas las impresoras accesibles desde el dispositivo de usuario es la más fácil de administrar inicialmente, pero puede crear inicios de sesión lentos en algunos entornos. En esta situación, quizás desee limitar la lista de impresoras configuradas en el dispositivo del usuario.

También es posible que las directivas de seguridad de la empresa no permitan que los usuarios asignen puertos locales de impresión. Para ello, en el servidor, configure la directiva de ICA Conectar automáticamente puertos COM del cliente como Inhabilitada.

Para limitar la lista de impresoras configuradas en el dispositivo del usuario

1. Abra el archivo de configuración, wfclient.ini, en uno de los siguientes directorios:
 - %HOME%/.ICAClient, para limitar las impresoras de un solo usuario
 - %SICAROOT%/config, para limitar las impresoras de todos los usuarios de Receiver (en este caso, todos los usuarios se refiere a aquellos que utilicen primero el programa selfservice después del cambio)
2. En la sección [WFClient] del archivo, escriba:
ClientPrinterList=impresora1:impresora2:impresora3

donde impresora1, impresora2 y sucesivos son los nombres de las impresoras elegidas. Separe los nombres de las impresoras con dos puntos (:).

3. Guarde y cierre el archivo.

Asignación de impresoras del cliente en XenApp para Windows

Citrix Receiver para Linux admite el controlador de impresora universal PS de Citrix. De modo que, en la mayoría de los casos, no se requiere ninguna configuración local para que los usuarios utilicen impresoras de red o impresoras conectadas localmente a los dispositivos de usuario. Sin embargo, es posible que deba asignar manualmente impresoras del cliente en XenApp para Windows si, por ejemplo, el software de impresión del dispositivo del usuario no admite el controlador de impresora universal.

Para asignar una impresora local en un servidor

1. En Citrix Receiver, establezca una conexión de servidor e inicie sesión en un equipo que ejecute XenApp.
2. En el menú Inicio, haga clic en Configuración > Impresoras.

3. En el menú Archivo, haga clic en Agregar impresora.

Aparecerá el asistente Agregar impresora.

4. Utilice el asistente para agregar una impresora de red desde la red del cliente, dominio del cliente. En la mayoría de los casos, se tratará de un nombre de impresora estándar, similar a los creados por los Servicios de escritorio remoto nativos, como "HP LaserJet 4 de nombre del cliente en la sesión 3".

Para obtener más información sobre cómo agregar impresoras, consulte la documentación de su sistema operativo Windows.

Asignación de impresoras del cliente en XenApp para UNIX

En un entorno UNIX, se ignoran los controladores de impresora definidos por Citrix Receiver. El sistema de impresión en el dispositivo del usuario debe tener la capacidad de manejar el formato de impresión generado por la aplicación.

Antes de que los usuarios puedan utilizar una impresora del cliente desde Citrix XenApp para UNIX, el administrador debe habilitar la impresión. Para obtener más información, consulte la sección [XenApp for UNIX](#) en la documentación de XenApp y XenDesktop.

Asignación de sonido del cliente

La asignación de sonido del cliente permite que las aplicaciones que se ejecutan en el servidor XenApp o XenDesktop reproduzcan sonidos a través de dispositivos de sonido instalados en el dispositivo de usuario. Puede definir la calidad del sonido para cada conexión en el servidor, pero los usuarios también pueden definirla en el dispositivo del usuario. Si los parámetros de calidad de sonido del dispositivo de usuario y del servidor son diferentes, se utilizará el parámetro de calidad más bajo.

La asignación de sonido del cliente puede suponer una carga excesiva para los servidores y para la red. Cuanto mayor es la calidad de sonido, mayor ancho de banda se requiere para transferir los datos de sonido. El sonido de calidad más alta también consume más recursos de la CPU para su procesamiento.

Configure la asignación de sonido del cliente a través de directivas. Para obtener más información, consulte la documentación de [XenApp](#) y de [XenDesktop](#).

Nota: La asignación de sonido del cliente no recibe respaldo en conexiones a Citrix XenApp para UNIX.

Para configurar un dispositivo de sonido no predeterminado

Por lo general, el dispositivo de sonido predeterminado es el dispositivo ALSA predeterminado configurado para el sistema. Utilice el siguiente procedimiento para especificar un dispositivo diferente:

1. Elija y abra un archivo de configuración teniendo en cuenta los usuarios que desee afectar con sus cambios. Para obtener más información sobre la forma en que las actualizaciones a archivos de configuración específicos afectan a los diferentes usuarios, consulte [Personalización de Receiver mediante archivos de configuración](#).
2. Agregue la siguiente opción y cree la sección si es necesario:

```
[ClientAudio]
```

```
AudioDevice = <dispositivo>
```

donde la información de dispositivo está ubicada en el archivo de configuración de ALSA del sistema operativo.

Nota: La ubicación de esta información no es estándar en todos los sistemas operativos Linux. Citrix le recomienda consultar la documentación del sistema operativo para obtener más detalles sobre cómo ubicar esta información.

Configuración del respaldo USB

El respaldo USB permite a los usuarios interactuar con una amplia variedad de dispositivos USB cuando se conectan con un escritorio virtual. Los usuarios pueden conectar dispositivos USB a sus equipos, para utilizarlos de forma remota en sus escritorios virtuales. Los dispositivos USB disponibles para la comunicación remota son, entre otros, las unidades flash, los teléfonos inteligentes, las impresoras, los escáneres, los reproductores MP3, los dispositivos de seguridad y las PC tabletas.

La redirección de USB requiere XenApp 7.6 (o versiones posteriores) o XenDesktop. Tenga en cuenta que XenApp no respalda la redirección de dispositivos USB de almacenamiento masivo y requiere una configuración especial para dar respaldo a dispositivos de sonido. Para obtener más información, consulte la documentación de XenApp 7.6.

Los entornos LAN típicos de alta velocidad y baja latencia admiten las funciones isócronas de los dispositivos USB como cámaras Web, micrófonos, altavoces y auriculares, aunque, en la mayoría de los casos, es más adecuada la redirección estándar del sonido o la cámara Web.

Los siguientes tipos de dispositivos se admiten directamente en una sesión XenDesktop y por lo tanto no utilizan respaldo USB:

- Teclados
- Punteros (ratones)
- Tarjetas inteligentes
- Auriculares con micro
- Cámaras Web

Nota: Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y punteros 3D) pueden configurarse para utilizar respaldo USB. Para obtener información sobre cómo configurar reglas de directivas para otros dispositivos USB especializados, consulte [CTX 119722](#).

De manera predeterminada, existen ciertos tipos de dispositivos USB que no tienen respaldo para la comunicación remota a través de XenDesktop. Por ejemplo, un usuario puede tener una tarjeta de interfaz de red conectada a la placa del sistema mediante un dispositivo USB interno. Colocar este dispositivo en comunicación remota no sería apropiado. Los siguientes tipos de dispositivos USB no tienen respaldo predeterminado para ser utilizados en una sesión de XenDesktop:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Concentradores USB

Para actualizar la lista predeterminada de los dispositivos USB disponibles para la comunicación remota, edite el archivo `usb.conf`, ubicado en `$ICAROOT/`. Para obtener más información, consulte [Actualización de la lista de dispositivos USB que se encuentran disponibles para la comunicación remota](#).

Para permitir la comunicación remota de los dispositivos USB con escritorios virtuales, habilite la regla de directivas USB. Para obtener más información, consulte la documentación de [XenDesktop](#).

Funcionamiento del respaldo USB

Cuando un usuario conecta un dispositivo USB, éste se coteja con la directiva USB y, si está permitido, se lo redirige al escritorio virtual. Si la directiva predeterminada rechaza el dispositivo, sólo estará disponible para el escritorio local.

En el caso de los escritorios a los que se accede mediante el modo Desktop Appliance, cuando un usuario conecta un dispositivo USB, ese dispositivo se redirige automáticamente al escritorio virtual. El escritorio virtual es el que controla el dispositivo USB y lo muestra en la interfaz de usuario.

Para que la redirección tenga lugar, la ventana de la sesión debe tener el foco cuando el usuario conecta el dispositivo USB, a menos que se esté usando el modo Desktop Appliance.

Dispositivos de almacenamiento masivo

Si un usuario se desconecta de un escritorio virtual cuando un dispositivo USB de almacenamiento masivo se encuentra aún conectado con el escritorio local, ese dispositivo no se redirigirá al escritorio virtual de nuevo cuando el usuario se reconecte. Para garantizar que el dispositivo de almacenamiento masivo se redirija al escritorio virtual, el usuario debe retirar y volver a introducir el dispositivo después de reconectar.

Nota: Si introduce un dispositivo de almacenamiento masivo en una estación de trabajo Linux que se ha configurado para rechazar el respaldo remoto de dispositivos de almacenamiento masivo USB, el software de Receiver no aceptará el dispositivo y es posible que se abra un explorador de archivos de Linux aparte. Por lo tanto, Citrix recomienda que configure previamente los dispositivos de usuarios sin seleccionar el parámetro Browse removable media when inserted de forma predeterminada. En los dispositivos basados en Debian, para realizar esta acción mediante la barra del menú Debian, seleccione Desktop > Preferencias > Removable Drives and Media, y en la ficha Storage, en Removable Storage, anule la selección de la casilla de verificación Browse removable media when inserted.

Nota: Si la directiva de servidor Redirección de dispositivos USB del cliente está activada, los dispositivos de almacenamiento masivo se redirigen siempre como dispositivos USB, incluso aunque la asignación de unidades del cliente esté activada.

Cámaras Web

De forma predeterminada, el rendimiento óptimo de la cámara Web se logra a través de la compresión de vídeo de cámara Web HDX RealTime. Sin embargo, en algunas circunstancias, es posible que se requiera que los usuarios conecten cámaras Web mediante el respaldo USB. Para realizar esta acción, debe inhabilitar la compresión de vídeo de cámara Web HDX RealTime. Para obtener más información, consulte [Configuración de la compresión de vídeo de cámara Web HDX RealTime](#).

Clases de USB permitidas de forma predeterminada

Las reglas de directivas USB predeterminadas admiten las siguientes clases de dispositivos USB:

Sonido (clase 01)

Incluye micrófonos, altavoces, auriculares y controladores MIDI.

Interfaz física (clase 05)

Estos dispositivos son similares a los dispositivos HID, pero, en general, proporcionan respuesta o información en tiempo real. Incluyen joystick de Force Feedback, plataformas de movimiento y exoesqueletos de Force Feedback.

Digitalización de imágenes fijas (clase 06)

Abarca los escáneres y las cámaras digitales. Las cámaras digitales suelen admitir la clase de digitalización de imagen fija que utiliza el protocolo de transferencia de imágenes (PTP) o el protocolo de transferencia multimedia (MTP) para transferir imágenes a un equipo u otro dispositivo periférico. Las cámaras también pueden aparecer como dispositivos de almacenamiento masivo y puede ser posible configurar una cámara para que utilice cualquiera de las clases mediante el menú de configuración que proporciona la cámara propiamente dicha.

Tenga en cuenta que si una cámara se muestra como un dispositivo de almacenamiento masivo, se utiliza la asignación de unidades del cliente y no se requiere respaldo USB.

Impresoras (clase 07)

En general, la mayoría de las impresoras se incluyen en esta clase, aunque algunas utilizan protocolos específicos del fabricante (clase ff). Las impresoras multifunción pueden tener un concentrador interno o ser dispositivos compuestos. En ambos casos, el elemento de impresión generalmente utiliza la clase de la impresora y el elemento de fax o de escaneado utiliza otra clase, por ejemplo, la digitalización de imágenes fijas.

Las impresoras normalmente funcionan de forma adecuada sin el respaldo USB.

Almacenamiento masivo (clase 08)

Los dispositivos de almacenamiento masivo más comunes son las unidades flash USB. Otros incluyen las unidades de disco duro con conexión USB, las unidades de CD/DVD y los lectores de tarjetas SD/MMC. Existe una amplia variedad de dispositivos con almacenamiento interno que también presentan una interfaz de almacenamiento masivo, por ejemplo, reproductores multimedia, cámaras digitales y teléfonos móviles. Las subclases conocidas, entre otras, son:

- 01 Dispositivos flash limitados
- 02 Dispositivos CD/DVD típicos (ATAPI/MMC-2)
- 03 Dispositivos de cinta típicos (QIC-157)
- 04 Unidades de disquete típicas (UFI)
- 05 Unidades de disquete típicas (SFF-8070i)
- 06 La mayoría de los dispositivos de almacenamiento masivo utiliza esta variante de SCSI

A menudo se puede acceder a los dispositivos de almacenamiento masivo a través de la asignación de unidades del cliente y por lo tanto no se requiere el respaldo USB.

Importante: Se sabe que algunos virus se propagan en forma activa utilizando todos los tipos de almacenamiento masivo. Considere cuidadosamente si existe o no una necesidad comercial de permitir el uso de los dispositivos de almacenamiento masivo, ya sea a través de la asignación de unidades del cliente o mediante el respaldo USB. Para minimizar el riesgo, el servidor puede configurarse para evitar que los archivos se ejecuten mediante la asignación de unidades del cliente.

Seguridad del contenido (clase 0d)

Los dispositivos para seguridad del contenido aplican la protección del contenido, generalmente para la administración de derechos digitales o para la gestión de licencias. Esta clase incluye las llaves.

Atención médica personal (clase 0f)

Estos dispositivos incluyen los dispositivos de atención médica personal como los sensores de presión arterial, los monitores de frecuencia cardíaca, podómetros, monitores de píldoras y espirómetros.

Específico del proveedor y de la aplicación (clases fe y ff)

Muchos dispositivos utilizan protocolos específicos del proveedor o protocolos no estandarizados por el consorcio USB, que generalmente se muestran como específicos del proveedor (clase ff).

Clases de dispositivos USB que se rechazan de manera predeterminada

Las reglas de directivas USB predeterminadas rechazan las siguientes clases de dispositivos USB:

Comunicaciones y control CDC (clases 02 y 0a)

Incluye módems, adaptadores ISDN, adaptadores de red y algunos teléfonos y equipos de fax.

La directiva USB predeterminada no permite estos dispositivos porque es posible que uno de ellos proporcione la conexión al escritorio virtual propiamente dicho.

Dispositivos de interfaz humana (HID) (clase 03)

Incluye una amplia variedad de dispositivos de entrada y de salida. Los dispositivos de interfaz humana (HID, por su sigla en inglés) típicos son los teclados, punteros (como el ratón o Mouse), los dispositivos señaladores, las tabletas gráficas, los controladores de juegos, los botones y las funciones de control.

La subclase 01 se conoce como la clase de interfaz de arranque, y se utiliza para los teclados y punteros.

La directiva USB predeterminada no permite teclados USB (clase 03, subclase 01, protocolo 1) ni punteros USB (clase 03, subclase 01, protocolo 2). Esto se debe a que la mayoría de los teclados y punteros se gestionan de manera apropiada sin respaldo USB y a que normalmente es necesario utilizar estos dispositivos de forma local y de forma remota cuando se conecta con un escritorio virtual.

Concentradores USB (clase 09)

Los concentradores USB permiten conectar dispositivos adicionales al equipo local. No es necesario acceder a estos dispositivos de forma remota.

Tarjeta inteligente (clase 0b)

Los lectores de tarjetas inteligentes incluyen lectores de tarjetas inteligentes con y sin contacto, y tokens USB con un chip de tarjeta inteligente equivalente incorporado.

Se accede a los lectores de tarjeta inteligente utilizando la comunicación remota de la tarjeta inteligente y no se requiere respaldo USB.

Vídeo (clase 0e)

La clase vídeo abarca los dispositivos que se utilizan para controlar vídeos o material relacionado con vídeos, como las cámaras web, videograbadoras digitales, conversores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión por secuencias de vídeo.

De forma predeterminada, el rendimiento óptimo de la cámara Web se logra a través de la compresión de vídeo de cámara Web HDX RealTime.

Controladores inalámbricos (clase e0)

Abarca una amplia variedad de controladores inalámbricos como los controladores de banda ultra-ancha y Bluetooth.

Es posible que algunos de estos dispositivos proporcionen acceso de red crítico o conecten periféricos críticos como punteros o teclados Bluetooth.

La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que en el caso de dispositivos particulares sea apropiado proporcionar acceso mediante respaldo USB.

Actualización de la lista de dispositivos USB disponibles para la comunicación

remota

Puede actualizar el rango de dispositivos USB disponibles para comunicación remota con escritorios editando la lista de reglas predeterminadas que contiene el archivo `usb.conf`, ubicado en el dispositivo del usuario en `$ICAROOT/`.

Para actualizar la lista, agregue reglas de directivas nuevas para permitir o denegar dispositivos USB no incluidos en el rango predeterminado. Las reglas creadas de este modo por el administrador controlan qué dispositivos se ofrecerán al servidor. Las reglas en el servidor controlan cuáles de ellos se aceptarán.

La configuración de directivas predeterminada para los dispositivos inhabilitados es la siguiente:

```
DENY: class=09 # Hub devices
```

```
DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)
```

```
DENY: class=0b # Smartcard
```

```
DENY: class=e0 # Wireless Controllers
```

```
DENY: class=02 # Communications and CDC Control
```

```
DENY: class=03 # UVC (webcam)
```

```
DENY: class=0a # CDC Data
```

```
ALLOW: # Ultimate fallback: allow everything else
```

Creación de reglas de directivas de USB

Sugerencia: Cuando cree nuevas reglas de directivas, consulte los códigos de clase USB que se encuentran disponibles en el sitio Web de USB <http://www.usb.org/>.

Las reglas de directivas de `usb.conf` en el dispositivo del usuario adoptan el formato `{ALLOW:|DENY:}` seguido de un conjunto de expresiones basadas en valores para las siguientes etiquetas:

Etiqueta	Descripción
VID	Identificador del proveedor tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
Class	Clase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
Subclass	Subclase del descriptor del dispositivo o de un descriptor de la interfaz
Prot	Protocolo tomado del descriptor del dispositivo o de un descriptor de la interfaz

Al crear nuevas reglas de directivas, tenga en cuenta lo siguiente:

- Las reglas no distinguen entre mayúsculas y minúsculas.
- Las reglas pueden tener un comentario optativo al final, que se introduce con el signo "#". No es obligatorio utilizar un delimitador y el comentario se ignora para la comparación.
- Se ignoran las líneas en blanco y las que son exclusivamente de comentario.
- El espacio en blanco que se utiliza como separador se ignora, pero no puede aparecer en el medio de un número o de un identificador. Por ejemplo, Deny: Class=08 SubClass=05 es una regla válida; pero Deny: Class=0 8 Sub Class=05 no lo es.
- Las etiquetas deben utilizar el operador de coincidencia "=". Por ejemplo: VID=1230.

Ejemplo

El siguiente ejemplo muestra una sección del archivo usb.conf en el dispositivo del usuario. Para que se implementen estas reglas, el mismo conjunto de reglas debe existir en el servidor.

```
ALLOW: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
```

```
DENY: Class=08 SubClass=05 # Mass Storage Devices
```

```
DENY: Class=0D # All Security Devices
```

Configuración de los modos de inicio

Con el modo Desktop Appliance es posible cambiar cómo un escritorio virtual gestiona los dispositivos USB conectados con anterioridad. En la sección WfClient del archivo \$ICAROOT/config/module.ini de cada dispositivo del usuario, configure DesktopApplianceMode = booleano como se describe a continuación.

TRUE	Todos los dispositivos USB que ya están conectados al inicio, siempre que los dispositivos no estén inhabilitados con una regla de denegación (DENY) en las directivas de USB en el servidor (entrada del Registro) o en el dispositivo del usuario (archivo de configuración de reglas de directivas).
FALSE	No se inicia ningún dispositivo USB.

Mejora del rendimiento en conexiones con poco ancho de banda

Citrix recomienda utilizar la versión más reciente de XenApp o XenDesktop en el servidor y Receiver en el dispositivo del usuario.

Si utiliza una conexión con poco ancho de banda, puede realizar varios cambios en la configuración de Receiver y en la forma en que lo utiliza para mejorar el rendimiento.

- **Configure la conexión de Receiver:** la configuración de las conexiones de Receiver puede reducir el ancho de banda que ICA requiere y mejorar el rendimiento.
- **Cambie la forma en que se utiliza Receiver:** cambiar la forma en que se utiliza Receiver también puede reducir el ancho de banda requerido para una conexión de alto rendimiento.
- **Habilite el sonido UDP:** esta función puede mantener un nivel de latencia regular en redes sobrecargadas durante conexiones Voice-over-IP (VoIP).
- **Utilice las versiones más recientes de XenApp y Receiver para Linux:** Citrix aumenta y mejora constantemente el rendimiento en cada versión, y muchas funcionalidades de rendimiento requieren la versión más reciente de Receiver y el

software de servidor.

Configuración de conexiones

En dispositivos con una capacidad de procesamiento limitada o un ancho de banda limitado, se intercambia rendimiento por funcionalidad y viceversa. Los usuarios y los administradores pueden elegir una combinación aceptable de funcionalidad y rendimiento interactivo. Llevando a cabo al menos uno de estos cambios, a menudo en el servidor y no en el dispositivo del usuario, se puede reducir el ancho de banda requerido para la conexión y se puede mejorar el rendimiento:

- **Habilite la reducción de retardo SpeedScreen:** la reducción de retardo SpeedScreen mejora el rendimiento en conexiones con altos niveles de latencia al proporcionar comentarios instantáneos al usuario en respuesta a los datos introducidos o a las acciones con el puntero. Use el Administrador de reducción de retardo SpeedScreen para habilitar esta función en el servidor. En Receiver, de forma predeterminada, esta opción está inhabilitada para el teclado y solo está habilitada para el puntero en conexiones con una latencia elevada. Consulte la *— guía de referencia de OEM de Citrix Receiver para Linux (en inglés)*.
- **Habilite la compresión de datos:** la compresión de datos reduce la cantidad de datos transferidos a través de la conexión. Esto requiere recursos adicionales del procesador para comprimir y descomprimir datos, pero puede aumentar el rendimiento en conexiones de poco ancho de banda. Use las configuraciones de directiva de Citrix Calidad de sonido y Compresión de imágenes para habilitar esta característica.
- **Reduzca el tamaño de la ventana:** cambie la dimensión de la ventana al tamaño utilizable más pequeño posible. En el sitio de servicios XenApp configurado, defina las Opciones de sesión.
- **Reduzca la cantidad de colores:** reduzca la cantidad de colores a 256. En el sitio de servicios XenApp configurado, defina las Opciones de sesión.
- **Reduzca la calidad de sonido:** si la asignación de sonido está habilitada, reduzca la calidad de sonido al parámetro más bajo mediante la configuración de directiva de Citrix Calidad de sonido.

Habilitación del sonido UDP

El sonido UDP puede mejorar la calidad de las llamadas telefónicas que se realizan a través de Internet. Se utiliza el protocolo UDP (User Datagram Protocol) en lugar del protocolo TCP (Transmission Control Protocol).

Tenga en cuenta lo siguiente:

- El sonido UDP no está disponible en las sesiones cifradas (es decir, las sesiones donde se utiliza el cifrado TLS o ICA). En esas sesiones, la transmisión de sonido se realiza mediante TCP.
 - La prioridad del canal ICA puede afectar el sonido UDP.
1. Configure las siguientes opciones en la sección ClientAudio de module.ini:
 - Establezca EnableUDPAudio en el valor True. De forma predeterminada, este valor está establecido en False, lo que inhabilita el sonido UDP.
 - Especifique los números de puerto mínimo y máximo para el tráfico de sonido UDP mediante UDPAudioPortLow y UDPAudioPortHigh respectivamente. De forma predeterminada, se utilizan los puertos 16500 a 16509.
 2. Establezca los parámetros de sonido de cliente y de servidor de la manera que se detalla a continuación a fin de que el sonido resultante sea de calidad mediana (es decir, ni alta ni baja).

					Calidad de sonido en el cliente				
					Alta	Media	Baja		

Calidad de sonido en el servidor	Alta	Alta	Media	Baja
	Media	Media	Media	Baja
	Baja	Baja	Baja	Baja

Si el sonido UDP está habilitado, pero la calidad resultante no es mediana, se utilizará TCP, no UDP, en la transmisión de sonido.

Cambio en la forma en que se utiliza Receiver

La tecnología ICA está altamente optimizada y, en general, no necesita requisitos elevados de ancho de banda ni de CPU. Sin embargo, si utiliza una conexión con muy poco ancho de banda, tenga en cuenta lo siguiente para preservar el rendimiento:

- **Evite el acceso a archivos grandes mediante la asignación de unidades del cliente.** Cuando se accede a un archivo grande con la asignación de unidades del cliente, el archivo se transfiere a través de la conexión del servidor. En conexiones lentas, puede tardar mucho tiempo.
- **Evite imprimir documentos grandes en impresoras locales.** Al imprimir un documento en una impresora local, el archivo que debe imprimirse se transfiere a través de la conexión del servidor. En conexiones lentas, puede tardar mucho tiempo.
- **Evite reproducir contenido multimedia.** La reproducción de contenido multimedia utiliza una gran cantidad de ancho de banda y puede reducir el rendimiento.

Optimización del rendimiento multimedia

Receiver abarca un amplio conjunto de tecnologías que ofrece una experiencia de alta definición para los usuarios en entornos con abundantes recursos multimedia, típicos de la actualidad. Estas tecnologías mejoran la experiencia de los usuarios cuando estos se conectan a aplicaciones y escritorios alojados, como se muestra a continuación:

- Redirección de Windows Media de HDX MediaStream
- Redirección de Flash HDX MediaStream
- Compresión de vídeo de cámara Web HDX RealTime
- Respaldo para H.264

Configuración de la redirección de Windows Media de HDX MediaStream

La redirección de Windows Media de HDX MediaStream supera la necesidad de contar con anchos de banda elevados para la captura y reproducción multimedia en escritorios virtuales Windows a los que se accede desde dispositivos de usuario Linux. La redirección de Windows Media ofrece un mecanismo para reproducir los archivos en tiempo de ejecución multimedia en el dispositivo del usuario y no en el servidor, reduciendo así los requisitos de ancho de banda para reproducir archivos multimedia.

La redirección de Windows Media mejora el rendimiento del Reproductor de Windows Media y de los reproductores compatibles que se ejecutan en escritorios virtuales Windows. Existe un amplio rango de formatos de archivo compatibles, entre ellos:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)

- MPEG Audio Layer-3 (MP3)
- Archivos de sonido WAV

Receiver incluye una tabla basada en texto, `MediaStreamingConfig.tbl`, para traducir los GUID de formatos multimedia específicos de Windows a tipos MIME que GStreamer puede usar. Esta tabla de traducciones puede actualizarse para realizar las siguientes acciones:

- Agregar a la tabla filtros o formatos de archivos multimedia previamente desconocidos o no respaldados
- Bloquear los GUID problemáticos para recurrir a la generación en el lado del servidor
- Agregar parámetros adicionales a las cadenas MIME existentes para permitir la solución de problemas en formatos que no funcionen correctamente mediante la modificación de los parámetros de GStreamer en las secuencias
- Administrar y distribuir configuraciones personalizadas según los tipos de archivo multimedia respaldados por GStreamer en un dispositivo del usuario

Con la obtención de contenido en el lado del cliente, también es posible permitir que el dispositivo del usuario transmita por secuencias multimedia directamente desde las direcciones URL con el formato `http://`, `mms://` o `rtsp://` en lugar de transmitir por secuencias multimedia a través de un servidor Citrix. El servidor se encarga de dirigir el dispositivo del usuario al contenido multimedia y de enviar los comandos de control (incluidos Reproducir, Pausar, Detener, Volumen y Buscar), pero no manipula los datos multimedia. Esta característica requiere bibliotecas avanzadas multimedia de GStreamer en el dispositivo.

Para implementar la redirección de Windows Media

1. Instale GStreamer 0.10, un marco de trabajo multimedia de código abierto, en cada dispositivo del usuario que lo requiera. Por lo general, GStreamer se debe instalar antes de instalar Receiver. La mayoría de las distribuciones de Linux incluyen GStreamer. De forma alternativa, puede descargar GStreamer desde <http://gstreamer.freedesktop.org>.
2. Para habilitar la obtención de contenido en el lado del cliente, instale los plugins de *origen de protocolo* de GStreamer para los tipos de archivo que los usuarios planean reproducir en el dispositivo. La utilidad `gst-launch` permite verificar que el plugin se encuentre instalado y funcione correctamente. Si `gst-launch` puede reproducir la dirección URL, el plugin requerido funciona correctamente. Por ejemplo, ejecute `gst-launch-0.10 playbin2 uri=http://example-source/file.wmv` y compruebe que el vídeo se reproduce correctamente.
3. Al instalar Receiver en el dispositivo, seleccione la opción GStreamer.

Tenga en cuenta lo siguiente con respecto a la funcionalidad de obtención de contenido en el lado del cliente:

- De manera predeterminada, esta funcionalidad está habilitada. Es posible inhabilitarla mediante la opción `SpeedScreenMMACSFEnabled` en la sección Multimedia de `All-Regions.ini`. Si esta opción se establece en `False`, se utiliza la redirección de Windows Media para el procesamiento de medios.
- De forma predeterminada, todas las funcionalidades de `MediaStream` utilizan el protocolo `playbin2` de GStreamer. Es posible revertir al protocolo `playbin` anterior en todas las funcionalidades de `MediaStream`, excepto la obtención de contenido en el lado del cliente que continuará utilizando `playbin2`, mediante la opción `SpeedScreenMMAEnablePlaybin2` en la sección Multimedia de `All-Regions.ini`.
- Receiver no reconoce archivos de lista de reproducción ni archivos de información de configuración de secuencia como `.asx` o `.nsc`. Cuando sea posible, los usuarios deben especificar una dirección URL estándar que no haga referencia a estos tipos de archivo. Utilice `gst-launch` para verificar que una dirección URL determinada sea válida.

Configuración de la redirección de Flash de HDX MediaStream

La Redirección de Flash de HDX MediaStream habilita el contenido de Adobe Flash para que se reproduzca de forma local

en los dispositivos de los usuarios, y les brinda una reproducción de sonido y vídeo de alta definición sin aumentar los requisitos de ancho de banda.

1. Asegúrese de que el dispositivo del usuario cumpla los requisitos de esta función. Para obtener más información, consulte [Requisitos del sistema](#).
2. Agregue los siguientes parámetros a la sección [WFClient] de wfclient.ini (para todas las conexiones hechas por un usuario específico) o a la sección [Client Engine\Application Launching] de All_Regions.ini (para todos los usuarios del entorno):
 - **HDXFlashUseFlashRemoting=Ask | Never | Always**
Habilita HDX MediaStream para Flash en el dispositivo del usuario. De forma predeterminada, este parámetro está establecido en **Never** y se presenta un cuadro de diálogo a los usuarios para preguntarles si quieren optimizar el contenido de Flash al conectarse a páginas Web que contienen Flash.
 - **HDXFlashEnableServerSideContentFetching=Disabled | Enabled**
Habilita o inhabilita la obtención de contenido en el servidor para Receiver. De forma predeterminada, este parámetro está configurado como inhabilitado: **Disabled**.
 - **HDXFlashUseServerHttpCookie=Disabled | Enabled**
Habilita o inhabilita la redirección de cookies HTTP. De forma predeterminada, este parámetro está configurado como inhabilitado: **Disabled**.
 - **HDXFlashEnableClientSideCaching=Disabled | Enabled**
Habilita o inhabilita el almacenamiento en caché del cliente del contenido Web obtenido por Receiver. De forma predeterminada, este parámetro está configurado como habilitado: **Enabled**.
 - **HDXFlashClientCacheSize= [25-250]**
Define el tamaño en megabytes (MB) del caché en el cliente. Puede introducirse cualquier tamaño entre 25 y 250 MB. Cuando se alcance el tamaño máximo, se eliminará el contenido existente en el caché para permitir el almacenamiento de contenido nuevo. De forma predeterminada, este parámetro está configurado como **100**.
 - **HDXFlashServerSideContentCacheType=Persistent | Temporary | NoCaching**
Define el tipo de almacenamiento en caché que utiliza Receiver para el contenido que se obtiene en el servidor. De forma predeterminada, este parámetro está configurado como persistente: **Persistent**.
Nota: Este parámetro se requiere solamente si **HDXFlashEnableServerSideContentFetching** está configurado como habilitado: **Enabled**.
3. La redirección de Flash está inhabilitada de forma predeterminada. En /config/module.ini, cambie FlashV2=Off por FlashV2=On para habilitar la función.

Configuración de la compresión de vídeo de cámara Web HDX RealTime

HDX RealTime ofrece una opción de compresión de vídeo de cámara Web para mejorar la eficiencia del ancho de banda durante la conferencia de vídeo, y de ese modo garantizar que los usuarios experimenten un rendimiento óptimo al utilizar aplicaciones como GoToMeeting con HD Faces o Skype Empresarial.

1. Asegúrese de que el dispositivo del usuario cumpla los requisitos de esta función.
2. Asegúrese de que el canal virtual Multimedia esté habilitado. Para hacerlo, abra el archivo de configuración module.ini, ubicado en el directorio \$ICAROOT/config y verifique que MultiMedia en la sección [ICA3.0] esté configurado como "On".
3. Habilite la entrada de sonido haciendo clic en Usar mi micrófono y mi cámara Web en la página Micrófono y cámara Web del cuadro de diálogo Preferencias.

Inhabilitación de la compresión de vídeo de cámara Web HDX RealTime

De forma predeterminada, el rendimiento óptimo de la cámara Web se logra a través de la compresión de vídeo de cámara Web HDX RealTime. Sin embargo, en algunas circunstancias, es posible que se requiera que los usuarios conecten cámaras Web mediante el respaldo USB. Para ello, debe hacer lo siguiente:

- Inhabilite la compresión de vídeo de cámara Web HDX RealTime
- Habilite el respaldo USB para cámaras Web

1. Agregue el parámetro siguiente en la sección [WFClient] del archivo .ini apropiado:

```
HDXWebCamEnabled=Off
```

Para obtener más información, consulte [Personalización de Receiver mediante archivos de configuración](#).

2. Abra el archivo usb.conf que, por lo general, se encuentra en \$ICAROOT/usb.conf.

3. Elimine o convierta en comentario la siguiente línea:

```
DENY: class=0e # UVC (default via HDX RealTime Webcam Video Compression)
```

4. Guarde y cierre el archivo.

Configuración de respaldo para H.264

Receiver respalda la presentación de gráficos H.264, incluidos gráficos HDX 3D Pro, servidos por XenDesktop 7. Este respaldo utiliza la característica de códec de compresión profunda, que se encuentra habilitada de forma predeterminada. Esta característica ofrece un mejor rendimiento de las aplicaciones de gráficos de nivel profesional en redes WAN, comparado con el códec de JPEG existente.

Siga las instrucciones en este tema para inhabilitar esta característica (y procesar gráficos mediante el códec de JPEG en su lugar). También puede inhabilitar el seguimiento de texto pero mantener habilitado el respaldo para el códec de compresión profunda. Esto ayuda a reducir los costos de CPU durante el procesamiento de gráficos que incluyen imágenes complejas, con cantidades de texto relativamente pequeñas o de poca importancia.

Importante: Para configurar esta característica, no use ninguna opción con pérdida en la directiva Calidad visual de XenDesktop. Si lo hace, la codificación H.264 se inhabilita en el servidor y no funciona en Receiver.

Para inhabilitar el respaldo para el códec de compresión profunda:

En wfclient.ini, establezca H264Enabled con el valor False. Esto también inhabilita el seguimiento de texto.

Para inhabilitar solo el seguimiento de texto

Con el respaldo para el códec de compresión profunda habilitado, en el archivo wfclient.ini configure TextTrackingEnabled con el valor False.

Optimización del rendimiento de los cuadros de pantalla

Es posible mejorar la manera en que se procesan los cuadros de pantalla codificados con JPEG mediante las funcionalidades Decodificación de mapas de bits directamente en la pantalla, Decodificación de cuadros por lotes y XSync diferida.

1. Asegúrese de que su biblioteca JPEG respalda estas funciones.
2. En la sección Thinwire3.0 de wfclient.ini, establezca DirectDecode y BatchDecode en True.

Nota: La habilitación de la decodificación de cuadros por lotes también habilita la XSync diferida.

Mejora de la experiencia del usuario

Jan 05, 2017

Es posible mejorar la experiencia de los usuarios a través de las siguientes funciones compatibles:

- [Configuración de preferencias](#)
- [Configuración del suavizado de fuentes de ClearType](#)
- [Configuración de la redirección de carpetas especiales](#)
- [Configuración de la redirección de contenido servidor-cliente](#)
- [Control del comportamiento del teclado](#)
- [Uso de xcapture](#)
- [Reconectar usuarios automáticamente](#)
- [Cómo garantizar la fiabilidad de las sesiones](#)
- [Puntero relativo](#)

Configuración de preferencias

Para definir sus preferencias, haga clic en Preferencias en el menú de Citrix Receiver. Puede controlar cómo se muestran los escritorios, conectar con diferentes aplicaciones y escritorios, y administrar el acceso de dispositivos y archivos.

Para administrar una cuenta

Para acceder a los escritorios y las aplicaciones, necesita una cuenta con XenDesktop o XenApp. El equipo de asistencia técnica de TI puede pedirle que agregue una nueva cuenta a Citrix Receiver con este fin, o puede pedirle que use un servidor NetScaler Gateway o Access Gateway distinto para una cuenta existente. También puede quitar cuentas de Citrix Receiver.

1. En la página de Cuentas del cuadro de diálogo Preferencias, realice una de las siguientes acciones:
 - Para agregar una cuenta, haga clic en Agregar. El departamento de asistencia técnica también puede proporcionarle un archivo de aprovisionamiento con la información de cuenta que usted puede usar para crear una cuenta nueva.
 - Para cambiar los detalles de un almacén utilizado por la cuenta (por ejemplo, la puerta de enlace predeterminada), haga clic en Editar.
 - Para quitar una cuenta, haga clic en Quitar.
2. Siga las instrucciones en pantalla. Es posible que tenga que autenticarse en el servidor.

Para cambiar cómo se ven los escritorios

Esta característica no está disponible en sesiones de Citrix XenApp para UNIX.

Puede mostrar los escritorios en toda la pantalla del dispositivo de usuario (el modo de Pantalla completa), que es el valor predeterminado, o puede mostrarlos en una ventana aparte (modo de Ventana).

- En la página General del cuadro de diálogo Preferencias, seleccione uno de esos mediante la opción **Mostrar escritorio en**.

Ahora, Receiver para Linux tiene la funcionalidad de la barra de herramientas de **Desktop Viewer**, de modo que puede modificar de forma dinámica la configuración de la ventana de las sesiones remotas y cambiar los parámetros originales especificados por la configuración aquí mencionada.

Desktop Viewer

Cada empresa tiene sus propias necesidades de negocio. Los requisitos para el acceso por parte de los usuarios a los escritorios virtuales pueden variar de usuario a usuario y a medida que evolucionan las necesidades de la empresa. La experiencia del usuario a la hora de conectarse con los escritorios virtuales, así como su interacción en la configuración de las conexiones, depende de cómo se configure Receiver para Linux.

Use Desktop Viewer cuando los usuarios necesiten interactuar con el escritorio virtual. El escritorio virtual del usuario pueden ser un escritorio virtual publicado, o un escritorio compartido o escritorio dedicado. En este caso de acceso, la funcionalidad de la barra de herramientas de Desktop Viewer permite al usuario alternar entre una sesión en modo de ventana y una sesión a pantalla completa; además, incluye respaldo para varios monitores para los monitores intersecados. Los usuarios pueden alternar entre sesiones de escritorio y trabajar mediante varias conexiones de XenDesktop en el mismo dispositivo de usuario. Con tal de gestionar mejor las sesiones de los usuarios, se ofrecen botones para minimizar todas las sesiones de escritorio, el envío de la secuencia Ctrl+Alt+Supr, la desconexión y el cierre de sesión.

Como una funcionalidad de accesibilidad de Desktop Viewer, al presionar Ctrl+Alt+Interrumpir se muestran los botones de la barra de herramientas de Desktop Viewer en una ventana emergente.

Consulte la guía de OEM de Linux para ver entradas de configuración avanzada a fin de habilitar o inhabilitar Desktop Viewer o de cambiar la secuencia de teclas de accesibilidad.

Para reconectar automáticamente las sesiones

Citrix Receiver puede volver a conectarse a escritorios y aplicaciones de los que se ha desconectado (por ejemplo, si se produce un problema de infraestructura de la red):

- En la página General del cuadro de diálogo Preferencias, seleccione una opción en Reconectar aplicaciones y escritorios.

Para controlar cómo se accede a los archivos locales

Es posible que un escritorio virtual o una aplicación necesiten acceder a archivos ubicados en el dispositivo. El usuario puede controlar este acceso.

1. En la página Acceso a archivos del cuadro de diálogo Preferencias, seleccione una unidad asignada y, a continuación, una de las siguientes opciones:
 - Lectura y escritura: Para permitir que el escritorio o la aplicación lean y escriban en los archivos locales.
 - Solo lectura: Para permitir que el escritorio o la aplicación lean, pero no escriban, en los archivos locales.
 - Sin acceso: Para impedir que el escritorio o la aplicación accedan a los archivos locales.
 - Preguntar siempre: Para pedir permiso al usuario cada vez que el escritorio o la aplicación necesiten acceder a los archivos locales.
2. Si selecciona alguna de las opciones que concede acceso a los archivos locales, también puede ahorrar tiempo al ir a sus ubicaciones en el dispositivo de usuario. Haga clic en Agregar, especifique la ubicación y seleccione una unidad para asignársela.

Para configurar un micrófono o una cámara Web

Puede cambiar el modo en que un escritorio virtual o una aplicación acceden a su micrófono o cámara Web locales:

En la página Micrófono y cámara Web del cuadro de diálogo Preferencias, seleccione alguna de las siguientes opciones:

- Usar mi micrófono y mi cámara Web: Permitir que el escritorio o la aplicación usen el micrófono y la cámara Web.
- No usar mi micrófono ni mi cámara Web: Prohibir que el escritorio o la aplicación usen el micrófono y la cámara Web.

Para configurar el reproductor de Flash

Puede elegir cómo se muestra el contenido de Flash. Este contenido se muestra normalmente con el reproductor de Flash e incluye animaciones, vídeo y aplicaciones:

En la página Flash del cuadro de diálogo Preferencias, seleccione una de las siguientes opciones:

- Optimizar el contenido: Mejorar la calidad de la reproducción, con el riesgo de disminuir la seguridad.
- No optimizar el contenido: Proporcionar calidad de reproducción básica, sin disminuir la seguridad.
- Preguntar siempre: Preguntar cada vez que se muestra contenido de Flash.

Configuración del suavizado de fuentes de ClearType

El suavizado de fuentes ClearType (también conocido como presentación de fuentes de subpixel) mejora la calidad de las fuentes en pantalla más allá de las posibilidades que permite el suavizado de fuentes estándar o "anti-aliasing". Puede activar o desactivar esta función, o especificar el tipo de suavizado, editando este parámetro en la sección [WFClient] del archivo de configuración apropiado:

FontSmoothingType = número

donde número puede tomar uno de los siguientes valores:

Valor	Comportamiento
0	Se usa la preferencia local existente en el dispositivo. Esto está definido por el parámetro FontSmoothingTypePref.
1	Sin suavizado
2	Suavizado estándar
3	Suavizado ClearType (subpixel horizontal)

Tanto el suavizado estándar como el ClearType pueden aumentar los requisitos de ancho de banda de Receiver.

Importante: El servidor puede configurar FontSmoothingType mediante el archivo ICA. Esto tiene prioridad sobre el valor que esté definido en [WFClient]. Si el servidor establece el valor en 0, la preferencia local está determinada por otro parámetro en [WFClient]:

FontSmoothingTypePref = número

donde número puede tomar uno de los siguientes valores:

Valor	Comportamiento
0	Sin suavizado
1	
2	Suavizado estándar

Valor	Comportamiento
	FontWeight: ClearType (subpixel horizontal) (valor predeterminado)

Configuración de la redirección de carpetas especiales

En este contexto, existen solo dos carpetas especiales por usuario:

- La carpeta Escritorio del usuario
- La carpeta Documentos del usuario (Mis Documentos en Windows XP)

La redirección de carpetas especiales le permite especificar las ubicaciones de las carpetas especiales de un usuario para que permanezcan fijas en diferentes tipos de servidores y configuraciones de comunidades de servidores. Esto es particularmente importante si, por ejemplo, un usuario móvil necesita iniciar sesión en servidores de distintas comunidades de servidores. En el caso de estaciones de trabajo estáticas y basadas en escritorios, donde el usuario puede iniciar sesión en servidores que residen en una sola comunidad de servidores, la redirección de carpetas especiales rara vez es necesaria.

Para configurar la redirección de carpetas especiales

El procedimiento tiene dos partes. En primer lugar, debe habilitar la redirección de carpetas especiales a través de una entrada en `module.ini`; a continuación, debe especificar las ubicaciones de las carpetas en la sección `[WFClient]`, según se describe aquí:

1. Agregue el siguiente texto en `module.ini` (por ejemplo, `$ICAROOT/config/module.ini`):

```
[ClientDrive]
```

```
SFRAllowed = True
```

2. Agregue el texto siguiente en la sección `[WFClient]` (por ejemplo, `$HOME/.ICAClient/wfclient.ini`):

```
DocumentsFolder = documentos
```

```
DesktopFolder = escritorio
```

`documentos` y `escritorio` son los nombres de archivo de UNIX, incluida la ruta completa, de los directorios que se quiere utilizar como las carpetas Escritorio y Documentos respectivamente de los usuarios. Por ejemplo:

```
DesktopFolder = $HOME/.ICAClient/desktop
```

- Puede especificar cualquier componente en la ruta con una variable de entorno, por ejemplo, `$HOME`.
- Debe especificar valores para ambos parámetros.
- Los directorios que especifique deben estar disponibles a través de la asignación de dispositivos del cliente, es decir que el directorio debe estar en el subdirectorio de un dispositivo asignado del cliente.
- Como letras de unidad, debe utilizar `C` o superiores.

Configuración de la redirección de contenido servidor-cliente

La redirección de contenido servidor-cliente permite que los administradores especifiquen que las URL en aplicaciones publicadas se abran con aplicaciones locales. Por ejemplo, cuando se abre un enlace correspondiente a una página Web mientras se utiliza Microsoft Outlook en una sesión, el archivo se abre en el explorador Web del dispositivo del usuario. La redirección de contenido servidor-cliente permite que los administradores asignen recursos de Citrix de forma más eficiente, para brindar un mejor rendimiento a los usuarios.

Los siguientes tipos de URL pueden redirigirse:

- HTTP (protocolo de transferencia de hipertexto)
- HTTPS (protocolo de transferencia de hipertexto seguro)
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (versiones anteriores de Real Player)

Si Citrix Receiver no tiene una aplicación apropiada o no puede acceder directamente al contenido, la URL se abre con la aplicación del servidor.

La redirección de contenido servidor-cliente se configura en el servidor y se habilita de forma predeterminada en Citrix Receiver siempre que la ruta incluya RealPlayer y al menos una de las siguientes opciones: Firefox, Mozilla o Netscape.

Nota

Para obtener más información sobre RealPlayer para Linux, consulte <http://www.real.com/resources/unix/>.

Para habilitar la redirección de contenido servidor-cliente si en la ruta no se encuentran RealPlayer ni un explorador

1. Abra el archivo de configuración wfclient.ini.
2. En la sección [Browser], modifique los siguientes parámetros:

Path=ruta

Command=comando

donde ruta es el directorio donde está ubicado el archivo ejecutable del explorador y comando es el nombre del archivo ejecutable utilizado para controlar las URL de exploradores redirigidas, junto a la URL enviada por el servidor. Por ejemplo:

```
SICAROOT/nslaunch netscape,firefox,mozilla
```

Este parámetro especifica lo siguiente:

- Se ejecutará la utilidad nslaunch para insertar la URL en una ventana del explorador existente.
 - Se prueba cada uno de los exploradores en la lista sucesivamente hasta que pueda mostrarse el contenido de forma correcta.
3. En la sección [Player], modifique los siguientes parámetros:

Path=ruta

Command=comando

donde ruta es el directorio donde está ubicado el archivo ejecutable de RealPlayer y comando es el nombre del archivo ejecutable utilizado para controlar las URL multimedia redirigidas, junto a la URL enviada por el servidor.

4. Guarde y cierre el archivo.

Nota

En el caso de los dos parámetros Path, solo es necesario especificar el directorio donde están ubicados los archivos ejecutables del explorador y de RealPlayer. No es necesario especificar la ruta completa a los archivos ejecutables. Por ejemplo, en la sección [Browser], la ruta puede configurarse como /usr/X11R6/bin en lugar de /usr/X11R6/bin/netscape. Además, puede especificar varios nombres de directorios en una lista de elementos separados con dos puntos. Si no se especifican estos parámetros, se utilizará la ruta \$PATH actual del usuario.

Para inhabilitar la redirección de contenido servidor-cliente desde Receiver

1. Abra el archivo de configuración module.ini.
2. Cambie el parámetro CREnabled a Off.
3. Guarde y cierre el archivo.

Control del comportamiento del teclado

Para generar una combinación de teclas Ctrl+Alt+Supr remota:

1. Decida la combinación de teclas que creará la combinación Ctrl+Alt+Supr en el escritorio virtual remoto.
2. En la sección WFClient del archivo de configuración apropiado, configure UseCtrlAltEnd según sea necesario:
 - True significa que Ctrl+Alt+Fin pasa la combinación Ctrl+Alt+Supr al escritorio remoto.
 - False (valor predeterminado) significa que Ctrl+Alt+INTRO pasa la combinación Ctrl+Alt+Supr al escritorio remoto.

Uso de xcapture

El paquete de Citrix Receiver incluye una aplicación auxiliar, xcapture, para el intercambio de datos gráficos entre el portapapeles del servidor y las aplicaciones de X Windows no compatibles con ICCCM en el escritorio X. Los usuarios pueden utilizar xcapture para:

- Capturar cuadros de diálogo o áreas de la pantalla y copiarlos entre el escritorio del dispositivo del usuario (incluidas aplicaciones no compatibles con ICCCM) y una aplicación que se ejecuta en una ventana de conexión
- Copiar gráficos entre una ventana de conexión y las utilidades xmag o xv que sirven para la manipulación de gráficos X

Para iniciar xcapture desde la línea de comandos

En el símbolo del sistema, escriba:/opt/Citrix/ICAClient/util/xcapture y presione INTRO (donde /opt/Citrix/ICAClient es el directorio donde instaló Receiver).

Para copiar desde el escritorio del dispositivo del usuario

1. En el cuadro de diálogo xcapture, haga clic en From Screen. El cursor adoptará la forma de una cruz.
2. Elija entre las siguientes tareas:
 - Select a window. Mueva el cursor por la ventana que desea copiar y haga clic con el botón central del puntero.
 - Select a region. Mantenga presionado el botón principal del puntero y arrastre el cursor para seleccionar el área que desea copiar.
 - Cancel the selection. Haga clic con el botón secundario del puntero. Puede cancelar la selección mientras arrastra el cursor. Para eso, debe hacer clic con el botón secundario del puntero sin soltar el botón principal o central.
3. En el cuadro de diálogo xcapture, haga clic en To ICA. El botón xcapture cambia de color para indicar que está procesando la información.
4. Cuando se complete la transferencia, utilice el comando de pegar adecuado en la aplicación ejecutada desde la ventana

de conexión.

Para copiar desde xv a una aplicación en una ventana de conexión

1. Desde xv, copie la información.
2. En el cuadro de diálogo xcapture, haga clic en From XV y luego en To ICA. El botón xcapture cambia de color para indicar que está procesando la información.
3. Cuando se complete la transferencia, utilice el comando de pegar adecuado en la aplicación ejecutada desde la ventana de conexión.

Para copiar desde una aplicación en una ventana de conexión a xv

1. Desde la aplicación en una ventana de conexión, copie la información.
2. En el cuadro de diálogo xcapture, haga clic en From ICA y luego en To XV. El botón xcapture cambia de color para indicar que está procesando la información.
3. Cuando se complete la transferencia, pegue la información en xv.

Reconectar usuarios automáticamente

Este apartado describe la función de reconexión automática de clientes de HDX Broadcast. Citrix recomienda utilizar esto en combinación con la función de fiabilidad de sesiones de HDX Broadcast.

Las sesiones se pueden desconectar debido a redes poco fiables, una latencia en la red muy variable o limitaciones en el alcance de los dispositivos inalámbricos. Con la función de reconexión automática de clientes de HDX Broadcast, Citrix Receiver puede detectar desconexiones accidentales de las sesiones y volver a conectar automáticamente las sesiones afectadas.

Cuando esta función está habilitada en el servidor, los usuarios no tienen que volver a conectarse de forma manual para continuar trabajando. Citrix Receiver lleva a cabo un número determinado de intentos de reconectar la sesión hasta que lo logra, o hasta que el usuario cancela los intentos de reconexión. Si es necesaria la autenticación del usuario, aparece un cuadro de diálogo para ingresar las credenciales durante la reconexión automática. La reconexión automática no se produce si los usuarios salen de las aplicaciones sin realizar el cierre de la sesión. Los usuarios sólo pueden volver a conectarse a sesiones desconectadas.

De forma predeterminada, Citrix Receiver espera 30 segundos antes de intentar volver a conectarse a una sesión desconectada y realiza tres intentos de volver a conectarse a esa sesión.

Al conectarse mediante Access Gateway, ACR no se encuentra disponible. Para protegerse ante interrupciones de red, compruebe que la función de fiabilidad de la sesión está habilitada tanto en el servidor como en el cliente, y que, además, está configurada en Access Gateway.

Para obtener instrucciones acerca de la configuración de la reconexión automática de clientes de HDX Broadcast, consulte la documentación de XenApp y XenDesktop.

Cómo garantizar la fiabilidad de las sesiones

Este apartado describe la función de fiabilidad de sesiones de HDX Broadcast, que se encuentra habilitada de forma predeterminada.

Con la función de fiabilidad de sesiones de HDX Broadcast, los usuarios seguirán viendo una ventana con la aplicación publicada si la conexión a la aplicación se interrumpe. Por ejemplo, los usuarios inalámbricos que pasen por un túnel pueden

perder la conexión al entrar pero volverán a conectarse al salir del túnel. Durante el período de inactividad, todos los datos, entradas de teclado y otras interacciones del usuario se almacenan, mientras que la aplicación parece bloqueada y no responde. Cuando la conexión se restablece, dichas interacciones se reproducen en la aplicación.

Cuando se configuran la reconexión automática de clientes y la fiabilidad de sesiones, esta última tiene prioridad si se produce algún problema de conexión. La función de fiabilidad de sesiones intenta volver a establecer una conexión con la sesión existente. Se puede tardar hasta 25 segundos en detectar un problema de conexión y, luego, tarda un período de tiempo configurable (la duración predeterminada es de 180 segundos) para intentar la reconexión. Si la función de fiabilidad de sesiones no consigue completar la reconexión, es la reconexión automática de clientes la que intenta completarla.

Si la función de fiabilidad de sesiones de HDX Broadcast está habilitada, el puerto predeterminado que se utiliza para la comunicación de la sesión cambia de 1494 a 2598.

Los usuarios de Citrix Receiver no pueden anular la configuración del servidor. Para obtener más información sobre estas funciones, consulte la documentación de XenApp y XenDesktop.

Important

La función de fiabilidad de sesiones de HDX Broadcast necesita que otra función, el protocolo CGP, esté habilitada (mediante la configuración de directivas) en el servidor. Si se inhabilita el protocolo CGP, también se inhabilita la función de fiabilidad de sesiones de HDX Broadcast.

Puntero relativo

El respaldo al puntero relativo ofrece una opción para interpretar la posición del puntero de un modo relativo en lugar de hacerlo de un modo absoluto. Esta funcionalidad se necesita para aplicaciones que exigen la entrada de datos de un puntero relativo y no de un puntero absoluto.

Nota

Esta función está disponible únicamente en sesiones con XenApp o XenDesktop 7.8 (o una versión más reciente). De forma predeterminada, está inhabilitada.

Para habilitar la función:

En el archivo `$HOME/.ICAClient/wfclient.ini`, en la sección `[WFClient]`, agregue la entrada `RelativeMouse=1`.

Esto habilita la función, pero la mantiene inactiva hasta que usted la active.

Sugerencia

Consulte la sección [Valores alternativos de puntero relativo](#) para obtener información adicional acerca de la habilitación de funciones de puntero relativo.

Para activar la función:

Introduzca Ctrl/F12.

Una vez que la función se haya habilitado, introduzca Ctrl/F12 de nuevo para sincronizar la posición del puntero del servidor con el cliente (las posiciones de los punteros del servidor y del cliente no están sincronizadas cuando se usa el puntero relativo).

Para desactivar la función:

Introduzca Ctrl-Mayús/F12.

La función también se desactiva cuando la ventana de una sesión deja de estar activa y en primer plano.

Valores alternativos de puntero relativo

También puede considerar los siguientes valores de `RelativeMouse`:

- `RelativeMouse=2`. Habilita la función y la activa siempre que se enfoque la ventana de una sesión.
- `RelativeMouse=3`. Habilita y activa la función, y la mantiene activa en todo momento.

Para cambiar los comandos del teclado, agregue parámetros como:

- `RelativemouseOnChar=F11`
- `RelativeMouseOnShift=Shift`
- `RelativemouseOffChar=F11`
- `RelativeMouseOffShift=Shift`

Los valores admitidos de **`RelativemouseOnChar`** y **`RelativemouseOffChar`** se recogen en [Hotkey Keys], en el archivo `config/module.ini` del árbol de instalación de Citrix Receiver. Los valores de **`RelativeMouseOnShift`** y **`RelativeMouseOffShift`** establecen las teclas modificadoras para usarse, y se recogen en el título [Hotkey Shift States].

Seguridad

Jan 05, 2017

En este artículo:

- [Conexión a través de un servidor proxy](#)
- [Conexión con Secure Gateway o Traspaso SSL Citrix](#)
- [Conexiones a través de NetScaler Gateway](#)

Para proteger la comunicación entre la comunidad de servidores y Citrix Receiver, se pueden integrar las conexiones de Receiver con la comunidad de servidores a través de diversas tecnologías de seguridad, que incluyen:

- Un servidor proxy SOCKS o un servidor proxy de seguridad (también conocido como servidor proxy seguro, un servidor proxy HTTPS o un servidor proxy de canalización TLS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.
- Soluciones de Secure Gateway o Traspaso SSL con protocolos TLS (Transport Layer Security) Se respaldan las versiones de TLS de 1.0 a 1.2.
- Un firewall. Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si desea utilizar Receiver a través de un firewall que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, traducción de direcciones de red, NAT), configure las direcciones externas.

Conexión a través de un servidor proxy

Los servidores proxy se utilizan para limitar el acceso hacia la red y desde ella, y para gestionar conexiones entre Citrix Receiver y los entornos de Citrix XenApp o Citrix XenDesktop. Citrix Receiver admite el protocolo SOCKS, junto con Secure Gateway y Traspaso SSL Citrix, el protocolo de proxy seguro y la autenticación de desafío y respuesta de Windows NT (NTLM).

La lista de tipos de proxy respaldados está restringida por el contenido de Trusted_Regions.ini y Untrusted_Regions.ini a los tipos Auto (automático), None (ninguno) y Wpad. Si necesita usar otros tipos (SOCKS, Secure o Script), modifique esos archivos para agregarlos a la lista de permitidos.

Nota

Para garantizar una conexión segura, habilite TLS.

Conexión a través de un servidor proxy seguro

La configuración de conexiones para utilizar el protocolo de proxy seguro también permite respaldo para la autenticación de desafío y respuesta de Windows NT (NTLM). Si este protocolo está disponible, se detectará y se utilizará en el momento de la ejecución sin ninguna configuración adicional.

Important

El respaldo para NTLM requiere que la biblioteca de OpenSSL, libcrypto.so, esté instalada en el dispositivo del usuario. Con frecuencia, esta biblioteca se incluye en las distribuciones de Linux, pero puede descargarse desde <http://www.openssl.org/>, si es necesario, en una ventana nueva.

Conexión con Secure Gateway o Traspaso SSL Citrix

Puede integrar Receiver con los servicios Secure Gateway o Secure Sockets Layer (SSL) Relay. Receiver respalda el protocolo TLS (Transport Layer Security). TLS es la versión estándar más reciente del protocolo SSL. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de SSL como un estándar abierto. TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para las comunicaciones de datos seguras. Estas organizaciones también pueden exigir el uso de cifrado validado, como FIPS 140 (Estándar federal de procesamiento de información). FIPS 140 es un estándar para cifrado.

Conexión con Secure Gateway

Es posible usar Secure Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre Citrix Receiver y el servidor. No se necesita ninguna configuración de Citrix Receiver si se utiliza Secure Gateway en el modo Normal y los usuarios se conectan a través de la Interfaz Web.

Citrix Receiver usa parámetros que se configuran de forma remota en el servidor que ejecuta la Interfaz Web para conectarse a los servidores que ejecutan Secure Gateway. Para obtener más información sobre la configuración de los parámetros de servidores proxy para Citrix Receiver, consulte la documentación de la [Interfaz Web](#).

Si se instala Secure Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Gateway Proxy en modo de traspaso (Relay). Para obtener más información, consulte la documentación de [XenApp](#) (Secure Gateway).

Si se utiliza el modo Relay, el servidor Secure Gateway funciona como un proxy y es necesario configurar Citrix Receiver para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor Secure Gateway.
- El número de puerto del servidor Secure Gateway. Tenga en cuenta que el modo Relay no recibe respaldo en la versión 2.0 de Secure Gateway.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Nombre de host
- Dominio intermedio
- Dominio superior

Por ejemplo: `mi_equipo.mi_empresa.com` es un nombre de dominio completo porque contiene el nombre de host (`mi_equipo`), un dominio intermedio (`mi_empresa`) y un dominio superior (`com`). Por lo general, la combinación de nombre de dominio intermedio y dominio superior (`mi_empresa.com`) se conoce como nombre de dominio.

Conexión con el Traspaso SSL Citrix

De forma predeterminada, el Traspaso SSL Citrix utiliza el puerto TCP 443 en el servidor XenApp para las comunicaciones protegidas con TLS. Cuando el Traspaso SSL recibe una conexión TLS, descifra los datos antes de redirigirlos al servidor.

Si configuró el Traspaso SSL para un puerto de escucha distinto a 443, debe especificar en Citrix Receiver ese número de puerto de escucha no estándar.

Puede utilizar el Traspaso SSL Citrix para proteger las comunicaciones:

- Entre un dispositivo de usuario habilitado con TLS y un servidor
- Con la Interfaz Web, entre el servidor XenApp y el servidor Web

Para obtener más información sobre la configuración y el uso del Traspaso SSL para proteger la instalación, consulte la documentación de [XenApp](#). Para obtener más información sobre la configuración de la Interfaz Web para utilizar el cifrado TLS, consulte la documentación de la [Interfaz Web](#).

Configuración y habilitación de TLS

Se puede controlar las versiones del protocolo TLS que se pueden negociar añadiendo las siguientes opciones de configuración en la sección [WFClient]:

- MinimumTLS=1.0
- MaximumTLS=1.2

Estos son los valores predeterminados implementados en el código. No obstante, puede ajustarlos según sea necesario.

Nota: Estos valores se leen en el momento de iniciar los programas. Si los cambia después de haber iniciado selfservice o storebrowse debe introducir lo siguiente: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse.**

Nota: Esta versión de Citrix Receiver para Linux inhabilita el uso del protocolo SSLv3.

Para conexiones TCP, Citrix Receiver para Linux da respaldo a TLS 1.0, 1.1 y 1.2 con las siguientes conexiones de conjuntos de cifrado TLS entre Receiver y XenApp/XenDesktop:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Para conexiones UDP, Citrix Receiver para Linux da respaldo a DTLS 1.0 con las siguientes conexiones de conjuntos de cifrado TLS entre Receiver y XenApp/XenDesktop:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Instalación de certificados raíz en los dispositivos de los usuarios

Para utilizar TLS necesita un certificado raíz en el dispositivo del usuario que pueda verificar la firma de la entidad de certificación en el certificado del servidor. De manera predeterminada, Citrix Receiver admite los siguientes certificados.

Certificado	Autoridad emisora
Class4PCA_G2_v2.pem	VeriSign Trust Network
Class3PCA_G2_v2.pem	VeriSign Trust Network

BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

No es obligatorio que obtenga e instale certificados raíz en el dispositivo del usuario para utilizar los certificados de estas entidades de certificación. Sin embargo, si desea utilizar una entidad de certificación diferente, deberá obtener e instalar un certificado raíz de la entidad de certificación en cada dispositivo del usuario.

Importante: Citrix Receiver no admite claves de más de 4096 bits. Debe asegurarse de que los certificados raíz e intermedios de la entidad de certificación, además de sus certificados del servidor, tengan una longitud menor o igual que 4096 bits.

Nota: Receiver para Linux 13.0 usa `c_rehash` desde el dispositivo local. La versión 13.1 y versiones posteriores usan la herramienta `ctx_rehash` según se describe en los siguientes pasos.

Uso de un certificado raíz

Si necesita autenticar un certificado de servidor que fue emitido por una entidad de certificación pero el dispositivo de usuario todavía no confía en él, siga estas instrucciones antes de agregar un almacén de StoreFront.

1. Obtenga el certificado raíz en formato PEM.
Sugerencia: Si no puede encontrar un certificado en este formato, use la utilidad `openssl` para convertir un certificado en formato CRT a un archivo `.pem`.
2. Mediante la cuenta de usuario con la que instaló el paquete (normalmente `root`):
 1. Copie el archivo en `$ICAROOT/keystore/cacerts`.
 2. Ejecute el comando siguiente:
`$ICAROOT/util/ctx_rehash`

Uso de un certificado intermedio

Si el servidor StoreFront no puede proporcionar los certificados intermedios que coincidan con el certificado que está utilizando, o si usted necesita instalar certificados intermedios para respaldar a usuarios de tarjetas inteligentes, siga estas instrucciones antes de agregar un almacén de StoreFront.

1. Obtenga los certificados intermedios por separado en formato PEM.
Sugerencia: Si no puede encontrar un certificado en este formato, use la utilidad `openssl` para convertir un certificado en formato CRT a un archivo `.pem`.
2. Mediante la cuenta de usuario con la que instaló el paquete (normalmente `root`):
 1. Copie los archivos en `$ICAROOT/keystore/intcerts`.
 2. Ejecute el siguiente comando como usuario que instaló el paquete:
`$ICAROOT/util/ctx_rehash`

Habilitación del respaldo para tarjetas inteligentes

Citrix Receiver para Linux ofrece respaldo para distintos lectores de tarjetas inteligentes. Si el respaldo para tarjetas inteligentes está habilitado para el servidor y Receiver, puede utilizar tarjetas inteligentes para los siguientes fines:

- Autenticación de inicio de sesión con tarjetas inteligentes. Utilice tarjetas inteligentes para autenticar usuarios en servidores de Citrix XenApp.
- Respaldo para aplicaciones de tarjetas inteligentes. Habilite las aplicaciones publicadas compatibles con tarjetas inteligentes para que puedan acceder a dispositivos de tarjetas inteligentes locales.

Los datos de la tarjeta inteligente contienen información de seguridad, y deben transmitirse a través de un canal autenticado y seguro, como TLS.

El respaldo para tarjetas inteligentes tiene los siguientes requisitos previos:

- Sus lectores de tarjetas inteligentes y aplicaciones publicadas deben ser compatibles con el estándar de la industria PC/SC.
- Debe instalar el controlador apropiado para su tarjeta inteligente.
- Debe instalar el paquete PC/SC Lite.
- Debe instalar y ejecutar el demonio pcscd, lo que proporciona al middleware acceso mediante PC/SC a las tarjetas inteligentes.
- En un sistema de 64 bits, las versiones de 32 y 64 bits del paquete "libpcsc-lite1" deben estar presentes.

Importante: Si utiliza el terminal SunRay con, al menos, la versión 2.0 del software del servidor SunRay, debe instalar el paquete de desvío de PC/SC SRCOM, que puede descargarse en <http://www.sun.com/>.

Para obtener más información sobre cómo configurar el respaldo para tarjetas inteligentes en los servidores, consulte la documentación de [XenDesktop](#) y [XenApp](#).

Conexiones a través de NetScaler Gateway

Citrix NetScaler Gateway (antes llamado Access Gateway) protege las conexiones a los almacenes de StoreFront, y permite a los administradores un control detallado del acceso de los usuarios a los escritorios y las aplicaciones.

Para conectarse a escritorios y aplicaciones a través de NetScaler Gateway

1. Especifique la dirección URL de NetScaler Gateway que le suministre el administrador. Puede hacerlo mediante alguno de estos procedimientos:
 - La primera vez que use la interfaz de usuario de autoservicio, se le solicitará que introduzca la dirección URL en el cuadro de diálogo Agregar cuenta
 - Cuando utilice más tarde la interfaz de usuario de autoservicio, puede introducir la URL en Preferencias > Cuentas > Agregar
 - Si desea establecer una conexión mediante el comando storebrowse, escriba la dirección URL en la línea de comandos. La dirección URL especifica la puerta de enlace y, opcionalmente, un almacén concreto:
 - Para conectar con el primer almacén que encuentre Receiver, use una URL con el formato `https://gateway.company.com`.
 - Para conectar con un almacén específico, use una URL con el formato `https://gateway.company.com/?`. Tenga en cuenta que esta dirección URL dinámica no tiene el formato estándar; no incluya = (el signo igual) en la URL. Si desea establecer una conexión a un almacén concreto con storebrowse, es probable que se necesiten comillas alrededor de la dirección URL en el comando storebrowse.

2. Cuando se le solicite, conéctese al almacén (a través de la puerta de enlace) con su nombre de usuario, contraseña y token de seguridad. Para obtener más información sobre este paso, consulte la documentación de NetScaler Gateway. Una vez completado el proceso de autenticación, se muestran los escritorios y las aplicaciones.

Solución de problemas

Jan 05, 2017

Este artículo contiene información que ayudará a los administradores a solucionar problemas con Citrix Receiver para Linux.

- [Problemas de conexión](#)
- [Problemas de presentación](#)
- [Problemas con el explorador Web](#)
- [Otros problemas](#)
- [Errores de configuración de conexión](#)
- [Errores de configuración de wfclient.ini](#)
- [Errores de archivos PAC](#)
- [Otros errores](#)
- [Envío de información de diagnóstico a la asistencia técnica de Citrix](#)

Problemas de conexión

Es posible que se encuentre con los siguientes problemas de conexión.

El Reproductor de Windows Media no puede reproducir archivos de ciertos formatos

Es posible que Citrix Receiver no tenga los plug-ins de GStreamer para gestionar un formato solicitado. Normalmente, esto hace que el servidor solicite un formato distinto. Algunas veces la comprobación inicial de plug-ins adecuados indica, incorrectamente, que sí que existen. Esto debería detectarse y debe aparecer un diálogo de error en el servidor para indicar que el Reproductor de Windows Media encontró un problema al reproducir el archivo. Al volver a intentar reproducir el archivo dentro de la sesión, la operación funciona porque Citrix Receiver ha rechazado el formato, y como resultado de ello, el servidor ha solicitado un formato distinto o lo ha reproducido él mismo.

En algunas circunstancias, la inexistencia de un plug-in adecuado no se detecta y el archivo no se reproduce correctamente, a pesar de que el indicador de progreso se mueve en el Reproductor de Windows Media.

Para evitar ver este error o evitar el fallo de reproducción en futuras sesiones:

1. Como solución temporal, agregue la opción de configuración "SpeedScreenMMAVerbose=On" en la sección [WFClient] del archivo `$Home/.ICAClient/wfclient.ini`, por ejemplo.
2. Reinicie WFICA desde un selfservice que se haya iniciado desde un terminal.
3. Reproduzca un vídeo que pueda generar este error.
4. Tome nota (en la salida de seguimiento) del tipo MIME asociado con el plug-in que falta, o el tipo MIME que debería ser compatible pero no se reproduce (por ejemplo, "video/x-h264...").
5. Modifique `$ICAROOT/config/MediaStreamingConfig.tbl`; en la línea con el tipo MIME anotado, introduzca un signo '?' entre los dos puntos ':' y el tipo MIME. Esto inhabilita el formato.
6. Repita los pasos anteriores del 2 al 5 para otros formatos de medios que provoquen este error.
7. Distribuya el archivo `MediaStreamingConfig.tbl` modificado a otras máquinas con el mismo conjunto de plug-ins GStreamer.

Nota: Como alternativa, después de identificar el tipo MIME puede ser posible instalar un plug-in GStreamer para decodificarlo.

No puedo conectarme adecuadamente a una sesión de escritorio o a un recurso publicado

Si al establecer una conexión con un servidor Windows aparece un cuadro de diálogo con el mensaje “Connecting to server...”, pero no aparece la subsiguiente ventana de conexión, es posible que deba configurar el servidor con una licencia de acceso de cliente (CAL). Para obtener más información sobre las licencias, consulte [Licencias de productos](#).

En ocasiones no puedo conectarme cuando intento reconectar con sesiones

A veces, el intento de reconectar con una sesión que tiene una profundidad de color mayor que la solicitada por Receiver hace que la conexión falle. Esto se debe a una falta de memoria disponible en el servidor. Si la reconexión falla, Receiver intentará utilizar la profundidad de color original. En caso contrario, el servidor intentará iniciar una sesión nueva con la profundidad de color solicitada y dejará la sesión original en estado desconectado. Sin embargo, también puede ocurrir un error en la segunda conexión si sigue faltando memoria disponible en el servidor.

No puedo conectarme a un servidor con su nombre de Internet completo

Citrix recomienda configurar el servidor de nombres de dominio (DNS) en su red para poder resolver los nombres de servidores a los que desea conectarse. Si el servidor DNS no está configurado, quizás no sea posible resolver el nombre de un servidor en una dirección IP. También puede especificar el servidor mediante su dirección IP, en lugar de su nombre, pero tenga en cuenta que las conexiones TLS requieren un nombre de dominio completo, no una dirección IP.

Recibo el mensaje de error “Proxy detection failure” al conectarme

Si su conexión está configurada para utilizar la detección automática del proxy y recibe el mensaje de error “Proxy detection failure: Javascript error” al intentar conectarse, copie el archivo wpad.dat en \$ICAROOT/util. Ejecute el siguiente comando, donde hostname es el nombre de host del servidor al que intenta conectarse:

```
cat wpad.dat | ./pacexec pac.js FindProxyForURL http://hostname hostname 2>&1 | grep “undeclared variable”
```

Si no obtiene resultados, existe un problema grave con el archivo wpad.dat en el servidor y debe investigarlo. Sin embargo, si observa un resultado como “assignment to undeclared variable...”, puede solucionar el problema. Abra pac.js y, para cada variable mencionada en los resultados, agregue una línea en la parte superior del archivo con el siguiente formato, donde “...” es el nombre de la variable.

```
var ...;
```

Las sesiones demoran mucho en iniciarse

Si una sesión no se inicia hasta tanto mueva el puntero, es posible que haya un problema con la generación del número aleatorio en el kernel de Linux. Para solucionarlo, ejecute un demonio que genere entropía como rngd (que está basado en hardware) o haveged (de Magic Software).

Me gustaría configurar el parámetro de un puerto serie

Para configurar un único puerto serie, agregue las siguientes entradas en el archivo de configuración \$ICAROOT/config/module.ini:

```
LastComPortNum=1 ComPort1=
```

Para configurar dos puertos serie o más, agregue las siguientes entradas en el archivo de configuración SICAROOT/config/module.ini:

```
LastComPortNum=2 ComPort1= ComPort2=
```

Errores de conexión

Aparece un diálogo de error donde se avisa de un "Error en la conexión: Se ha producido un error de protocolo al comunicarse con el servicio de autenticación". Hay varios problemas que pueden ser la causa de esta condición de error, entre ellos los siguientes:

- Cuando el equipo local y el equipo remoto no pueden negociar un protocolo TLS común.
- Cuando el equipo remoto no pide el certificado de cliente de la manera apropiada. IIS solo debe "aceptar" o "solicitar" certificados para "Citrix/Authentication/Certificate".
- Otros problemas.

Problemas de presentación

¿Por qué se ve la pantalla partida?

El problema de pantalla partida se produce cuando dos o más fotogramas distintos aparecen en pantalla al mismo tiempo, en bloques horizontales. Esto es visible principalmente en áreas grandes de contenido que cambia rápidamente en la pantalla. Aunque los datos se capturan en el VDA de modo que no se partan los fotogramas, y los datos se pasan al cliente de manera que tampoco se introduzca ese problema, X11 (el subsistema de gráficos de Linux/Unix) no ofrece un modo coherente de dibujar en pantalla de forma que se evite este problema.

Para evitar la partición de la imagen, Citrix recomienda el enfoque estándar, que sincroniza el dibujo de la aplicación con el dibujo de la pantalla; es decir, esperar a vsvnc, para iniciar el dibujo del fotograma siguiente. Hay una serie de opciones al utilizar Linux, dependiendo del hardware de gráficos que se tenga en el cliente y del administrador de ventanas que se utilice. Estas opciones se dividen en dos grupos de soluciones:

- Parámetros de GPU de X11
- Usar un administrador de composición

Parámetros de GPU de X11

Para gráficos Intel HD, cree un archivo llamado **20-intel.conf** en la carpeta xorg.conf.d, con este contenido:

```
Section "Device"
    Identifier "Intel Graphics"
    Driver "intel"
    Option "AccelMethod" "sna"
    Option "TearFree" "true"
EndSection
```

Para gráficos Nvidia, busque en la carpeta xorg.conf.d el archivo que contenga la opción "MetaModes" para su configuración. Para cada uno de los MetaModes utilizados, separados por comas, agregue lo siguiente:

```
{ForceFullCompositionPipeline = On}
```

Por ejemplo:

```
Option "MetaModes" "DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}"
```

Nota: Las distintas distribuciones de Linux usan rutas diferentes para la carpeta xorg.conf.d. Por ejemplo: /etc/X11/xorg.conf.d, o /user/share/X11/xorg.conf.d.

Administradores de composición

Use lo siguiente:

- Compriz (integrado en Ubuntu Unity). Tendrá que instalar el administrador de parámetros "ComprizConfig Settings Manager."

Ejecute "ComprizConfig Settings Manager"

En "General->Composition", deje sin marcar la casilla "Undirect Fullscreen Windows"

Nota: "ComprizConfig Settings Manager" debe usarse con cuidado, ya que si se cambian incorrectamente sus valores, el sistema puede dejar de responder y no iniciarse.

- Compton (una herramienta instalada como complemento). Consulte la documentación o la página man de Compton para ver información detallada. Por ejemplo, ejecute el comando:

```
compton --vsync opengl --vsync -aggressive
```

Cuando uso el teclado, aparecen entradas de teclado incorrectas

Si utiliza un teclado en un idioma que no sea el inglés, es posible que la presentación en la pantalla no coincida con las entradas del teclado. En este caso, debe especificar el tipo y la distribución del teclado que utiliza. Para obtener más información acerca de la especificación de teclados, consulte [Control del comportamiento del teclado](#).

Hay un redibujado excesivo al mover las ventanas integradas

Algunos administradores de ventanas informan continuamente de la posición nueva de las ventanas al moverlas, lo que puede producir un redibujado excesivo. Para solucionar este problema, cambie el administrador de ventanas a un modo que solo dibuje los contornos de las ventanas cuando se muevan.

Compatibilidad de iconos

Receiver crea iconos de ventanas que funcionan con la mayoría de los administradores de ventanas, pero no son completamente compatibles con la convención de comunicación del protocolo X Inter-Client.

Para ofrecer una compatibilidad total de iconos

1. Abra el archivo de configuración wfclient.ini.
2. Edite la línea siguiente en la sección [WFClient]: UseIconWindow=True
3. Guarde y cierre el archivo.

Tengo problemas para ver el cursor

Puede ser difícil ver el cursor si tiene el mismo color, o uno similar, al color del fondo. Para solucionar este problema, establezca que las áreas del cursor sean de color negro o blanco.

Para cambiar el color del cursor

1. Abra el archivo de configuración wfclient.ini.
2. Agregue una de las líneas siguientes a la sección [WFClient]:
CursorStipple=ffff,ffff (para que el cursor sea negro)

CursorStipple=0,0 (para que el cursor sea blanco)

3. Guarde y cierre el archivo.

Los colores en la pantalla parpadean

Cuando mueva el puntero en una ventana de conexión, o fuera de ella, es posible que los colores en la ventana fuera de foco comiencen a parpadear. Esta es una limitación conocida al utilizar X Windows System con presentaciones en PseudoColor. De ser posible, utilice una profundidad de color mayor para la conexión afectada.

Experimento cambios rápidos de colores con las presentaciones en color verdadero

Los usuarios tienen la opción de utilizar 256 colores cuando se conectan a un servidor. Esta opción asume que el hardware del vídeo tiene el respaldo de la paleta para permitir que las aplicaciones cambien rápidamente los colores de la paleta con el fin de producir presentaciones animadas.

Las presentaciones en color verdadero no tienen ninguna capacidad para emular la habilidad de producir animaciones cambiando rápidamente la paleta. La emulación de software de esta capacidad es costosa en términos de tiempo y tráfico de red. Para reducir este costo, Receiver almacena en búfer los cambios rápidos de la paleta y actualiza la paleta real solamente cada pocos segundos.

Los caracteres japoneses se muestran de forma incorrecta en mi pantalla

Receiver utiliza la codificación de caracteres EUC-JP o UTF-8 para los caracteres japoneses, mientras que el servidor utiliza la codificación de caracteres SJIS. Receiver no traduce entre estos grupos de caracteres. Esto puede ocasionar problemas al mostrar los archivos que están guardados en el servidor y que se ven localmente, o bien, que están guardados localmente y se ven en el servidor. Este problema afecta además a los caracteres japoneses en los parámetros utilizados en el traspaso de parámetros extendidos.

Deseo realizar una sesión con varios monitores

Las sesiones de pantalla completa abarcan todos los monitores, pero también está disponible una opción de línea de comandos para el control de la presentación en entornos de varios monitores, `-span`. Con esta opción se pueden ejecutar sesiones de pantalla completa y abarcar varios monitores.

La funcionalidad de la barra de herramientas de Desktop Viewer le permite alternar entre una sesión en modo de ventana y una sesión a pantalla completa; además, incluye respaldo para varios monitores para los monitores intersecados. Para obtener más información, consulte [Mejora de la experiencia de usuario](#).

Importante: `-span` no tiene ningún efecto en sesiones de ventanas integradas o normales (incluidas aquellas en ventanas maximizadas).

La opción `-span` tiene el siguiente formato:

```
-span [h][o][a | mon1[,mon2[,mon3,mon4]]]
```

Si `h` se especifica, se imprime una lista de monitores en `stdout`. Además, si ese es el valor completo de la opción, `wfica` se cierra.

Si `o` se especifica, la ventana de la sesión tendrá el atributo de redirección `override-redirect`.

Precaución: No se recomienda el uso de este valor de opción. Debe considerarse como último recurso, para utilizar con los administradores de ventanas que presenten dificultades de uso. El administrador de ventanas no podrá ver la ventana de la

sesión, además la ventana no tendrá un icono y no se podrá volver a apilar. Solo se podrá quitar finalizando la sesión. Si -a se especifica, Receiver intenta crear una sesión que cubra todos los monitores.

Receiver supone que el resto del valor de la opción -span es una lista de números de monitores. Un único valor selecciona un monitor específico, dos valores seleccionan los monitores en las esquinas superior izquierda e inferior derecha del área requerida, cuatro especifican los monitores en los bordes superior, inferior, izquierdo y derecho del área.

Si o no se ha especificado, wfica utilizará el mensaje `_NET_WM_FULLSCREEN_MONITORS` para solicitar una disposición de ventanas adecuada desde el administrador de ventanas, en el caso de sea compatible. De lo contrario, utilizará las directrices de tamaño y posición para solicitar la disposición deseada.

El siguiente comando se puede utilizar para probar el respaldo del administrador de ventanas:

```
xprop -root | grep _NET_WM_FULLSCREEN_MONITORS
```

Si no obtiene resultados, no hay respaldo. Si no hay respaldo, es posible que necesite una ventana con el atributo `override-redirect`. Puede configurar una ventana con el atributo `override-redirect` mediante -span o.

Para realizar una sesión que abarque varios monitores desde la línea de comandos:

1. Escriba lo siguiente en una interfaz de comandos:

```
/opt/Citrix/ICAClient/wfica -span h
```

Se imprime una lista de los números de los monitores actualmente conectados al dispositivo del usuario en stdout y wfica se cierra.

2. Tome nota de estos números de monitores.
3. Escriba lo siguiente en una interfaz de comandos:

```
/opt/Citrix/ICAClient/wfica -span [w[x,y,z]]
```

donde [w],[x], [y] y [z] son números de monitores obtenidos en el paso 1 mencionado anteriormente, y un único valor w especifica un monitor en particular, dos valores w y x especifican monitores en las esquinas superior izquierda e inferior derecha del área requerida y los cuatro valores (w, x, y, z) especifican monitores en los bordes superior, inferior, izquierdo y derecho del área.

Importante: Debe definir la variable `WFICA_OPTS` antes de iniciar selfservice o conectarse con la Interfaz Web a través de un explorador Web. Para hacer esto, edite su archivo de perfil que, por lo general, se encuentra en `$HOME/.bash_profile` o `$HOME/.profile`, y agregue una línea para definir la variable `WFICA_OPTS`. Por ejemplo:

```
export WFICA_OPTS="-span a"
```

Tenga en cuenta que este cambio afecta a las sesiones de XenApp y XenDesktop.

Si ya ha iniciado selfservice o storebrowse debe quitar los procesos que iniciaron para que la nueva variable de entorno tenga efecto. Quítelos con:

```
killall AuthManagerDaemon ServiceRecord storebrowse
```

No puedo salir de una sesión a pantalla completa para utilizar aplicaciones locales u otras sesiones

Esto ocurre porque la IU del sistema del cliente está oculta y la función de transparencia de teclado inhabilita el comando habitual del teclado (por ejemplo, Alt+Tab) y, en su lugar, envía el comando al servidor.

Para evitar que esto ocurra, presione Ctrl+F2 para desactivar temporalmente la función de teclado transparente hasta que

la ventana de la sesión vuelva a estar activa y en primer plano. Una solución alternativa consiste en definir `TransparentKeyPassthrough` a `No` en `$ICAROOT/config/module.ini`. Así, se inhabilita la función de transparencia de teclado, pero es posible que tenga que anular el archivo `ICA` y agregar este parámetro al archivo `All_regions.ini`.

Problemas con el explorador Web

Cuando hago clic en un vínculo en una sesión de Windows, el contenido aparece en un explorador local

La redirección de contenido servidor-cliente está habilitada en `wfclient.ini`. Esto provoca que se ejecute una aplicación local. Para inhabilitar la redirección de contenido entre servidor y cliente, consulte [Configuración de la redirección de contenido servidor-cliente](#).

Al acceder a recursos publicados, mi explorador me solicita guardar un archivo

Los exploradores Web distintos de Firefox y Chrome pueden requerir cierta configuración para poder conectar con un recurso publicado. Si se conecta a través de la Interfaz Web, quizás pueda acceder a la página de inicio de la Interfaz Web con la lista de recursos. Sin embargo, al intentar acceder a un recurso haciendo clic en su icono en la página, el explorador Web le solicitará guardar el archivo `ICA`.

Para configurar un explorador diferente con el fin de utilizarlo con la Interfaz Web

Los detalles varían según el explorador Web, pero se pueden configurar los tipos de datos MIME en el explorador de forma que `$ICAROOT/wfica` se ejecute como una aplicación auxiliar cuando el explorador encuentre datos con el tipo MIME `application/x-ica` o un archivo `.ica`.

El programa de instalación no admite un explorador específico

Si tiene problemas para utilizar un explorador Web específico, configure la variable de entorno `BROWSER` para especificar la ruta local y el nombre del explorador Web requerido antes de ejecutar `setupwfc`.

Cuando inicio escritorios o aplicaciones en Firefox, no ocurre nada

Pruebe a habilitar el plugin `ICA`.

El plugin `ICA` está habilitado en Firefox, pero no se inician ni las sesiones de escritorio ni las sesiones de aplicación

Pruebe a inhabilitar el plug-in `ICA`.

Otros problemas

Es posible que se encuentre con los siguientes problemas adicionales.

Quiero saber si el servidor ha ordenado a Receiver que cierre una sesión

Puede usar el programa `wfica` para que capture un registro cuando reciba un comando desde el servidor para terminar una sesión.

Para grabar esta información en el sistema de `syslog`, añada `SyslogThreshold` con el valor 6 a la sección `[WFClient]` del

archivo de configuración. Esto habilita la captura de registros de mensajes que tienen una prioridad de LOG_INFO o mayor. El valor predeterminado para *SyslogThreshold* es 4 (=LOG_WARNING).

Igualmente, para que *wfica* envíe la información a la salida de "standard error", añada *PrintLogThreshold* con el valor a la sección [WFClient]. El valor predeterminado de *PrintLogThreshold* es 0 (=LOG_EMERG).

Consulte la documentación del sistema operativo para obtener instrucciones sobre cómo configurar el sistema de syslog.

Los parámetros de mi archivo de configuración ya no funcionan

Para cada entrada de *wfclient.ini*, debe haber una entrada correspondiente en *All_Regions.ini* para que el parámetro tenga efecto. Además, para cada entrada en las secciones [Thinwire3.0], [ClientDrive] y [TCP/IP] de *wfclient.ini*, debe haber una entrada correspondiente en *canonicalization.ini* para que el parámetro tenga efecto. Consulte los archivos *All_Regions.ini* y *canonicalization.ini* en el directorio *\$ICAROOT/config* para obtener más información.

Tengo problemas para ejecutar aplicaciones publicadas que acceden a un puerto serie

Si una aplicación publicada debe acceder a un puerto serie, es posible que la aplicación falle (con o sin mensajes de error, según la aplicación propiamente dicha) si otra aplicación bloqueó el puerto. En tales circunstancias, verifique si hay alguna aplicación que haya bloqueado temporalmente el puerto serie, o bien, que haya bloqueado el puerto serie y que se haya cerrado sin desbloquearlo.

Para solucionar este problema, detenga la aplicación que bloquea el puerto serie. En el caso de los bloqueos de tipo UUCP, es posible que quede algún archivo de bloqueo después de que se cierra la aplicación. La ubicación de estos archivos de bloqueo depende del sistema operativo que utilice.

No puedo iniciar Receiver

Si Receiver no se inicia y aparece el mensaje de error "Application default file could not be found or is out of date", esto puede ocurrir porque la variable de entorno ICAROOT no se definió correctamente. Esto es un requisito si instaló Receiver en una ubicación no predeterminada. Para solucionar este problema, Citrix recomienda que realice alguna de las siguientes acciones:

- Defina ICAROOT como el directorio de instalación.

Para verificar que la variable de entorno ICAROOT esté definida correctamente, intente iniciar Receiver desde una sesión de terminal. Si el mensaje de error continúa, es probable que la variable de entorno ICAROOT no esté definida correctamente.

- Vuelva a instalar Receiver en la ubicación predeterminada. Para obtener más información acerca de la instalación de Receiver, consulte [Descarga e instalación de Receiver para Linux](#).

Si Receiver se instaló anteriormente en la ubicación predeterminada, elimine el directorio */opt/Citrix/ICAclient* o *\$HOME/ICAclient/platform* antes de volver a instalarlo.

Las teclas de acceso rápido no funcionan correctamente

Si el administrador de ventanas utiliza las mismas combinaciones de teclas para proporcionar funcionalidad nativa, las combinaciones de teclas podrían no funcionar correctamente. Por ejemplo, el administrador de ventanas KDE utiliza las

combinaciones de teclas desde CTRL+MAYÚS+F1 a CTRL+MAYÚS+F4 para cambiar entre los escritorios 13 a 16. Si observa este problema, intente alguna de estas soluciones:

- El modo traducido en el teclado, asigna un conjunto de combinaciones de teclas locales a combinaciones de teclas en el lado del servidor. Por ejemplo, de forma predeterminada en el modo traducido, la combinación CTRL+MAYÚS+F1 está asignada a la combinación ALT+F1 en el lado del servidor. Para reconfigurar esta asignación a una combinación de teclas local alternativa, actualice esta entrada de la sección [WFClient] del archivo \$HOME/.ICAClient/wfclient.ini. Esto asigna la combinación de teclas local ALT+CTRL+F1 a ALT+F1:
 - Cambie Hotkey1Shift=Ctrl+Shift a Hotkey1Shift=Alt+Ctrl.
- El modo directo en el teclado envía todas las combinaciones de teclas directamente al servidor. Es decir, no se procesan localmente. Para configurar el modo directo, en la sección [WFClient] de \$HOME/.ICAClient/wfclient.ini, defina TransparentKeyPassthrough a Remota.
- Reconfigure el administrador de ventanas de modo que suprima las combinaciones de teclado predeterminadas.

Quiero habilitar un teclado croata remoto

Este procedimiento garantiza que los caracteres ASCII se envíen correctamente a los escritorios virtuales remotos con distribuciones de teclado croatas.

1. En la sección WFClient del archivo de configuración apropiado, establezca UseEUKSforASCII en True.
2. Establezca UseEUKS en 2.

Me gustaría encontrar el número de versión de Citrix SSLSDK o de OpenSSL

Para confirmar el número de versión de Citrix SSLSDK o de OpenSSL que está utilizando, puede utilizar el siguiente comando:

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

También puede ejecutar este comando en AuthManagerDaemon o en PrimaryAuthManager.

Me gustaría utilizar el teclado japonés en el cliente

Para configurar el uso del teclado japonés, actualice la siguiente entrada en el archivo de configuración wfclient.ini: KeyboardLayout=Japanese (JIS)

Me gustaría utilizar el teclado ABNT2 en el cliente

Para configurar el uso del teclado ABNT2, actualice la siguiente entrada en el archivo de configuración wfclient.ini: KeyboardLayout=Brazilian (ABNT2)

Algunas teclas de mi teclado local no se comportan según lo esperado

Elija la mejor distribución de servidores de la lista que hay en \$ICAROOT/config/module.ini.

Errores de configuración de conexión

Estos errores pueden producirse si configuró incorrectamente una entrada de conexión.

E_MISSING_INI_SECTION - Verifique el archivo de configuración: "...". Falta la sección "..." en el archivo de configuración.

El archivo de configuración se editó incorrectamente o está dañado.

E_MISSING_INI_ENTRY - Verifique el archivo de configuración: "...". La sección "... " debe contener una entrada "...".

El archivo de configuración se editó incorrectamente o está dañado.

E_INI_VENDOR_RANGE - Verifique el archivo de configuración: "...". El rango de proveedores de servidor X "... " en el archivo de configuración no es válido.

La información sobre el proveedor del servidor X en el archivo de configuración está dañada. Comuníquese con Citrix.

Errores de configuración de wfclient.ini

Estos errores pueden producirse si ha editado incorrectamente wfclient.ini.

E_CANNOT_WRITE_FILE - No se puede escribir el archivo: "..."

Se produjo un problema al guardar la base de datos de la conexión; por ejemplo, no hay espacio en el disco.

E_CANNOT_CREATE_FILE - No se puede crear el archivo: "..."

Se produjo un problema al crear una nueva base de datos de la conexión.

E_PNAGENT_FILE_UNREADABLE - Cannot read XenApp file "...": No such file or directory.

O bien:

Cannot read XenApp file "...": Permission denied.

Está intentando acceder a un recurso a través de un menú o un elemento de escritorio, pero el archivo XenApp del recurso no está disponible. Actualice la lista de los recursos publicados. Para hacerlo, seleccione Application Refresh en el menú View e intente acceder nuevamente al recurso. Si el error persiste, compruebe las propiedades del elemento de menú o del icono del escritorio y también del archivo XenApp al que se refiere el icono o el elemento.

Errores de archivos PAC

Estos errores pueden producirse si el entorno utiliza archivos PAC (configuración automática del proxy) para especificar configuraciones del proxy.

Fallo de detección de proxy: La URL de configuración automática no es válida.

Se especificó una dirección en el explorador con un tipo de URL no válido. Los tipos válidos son http:// y https://. No se admite ningún otro tipo. Cambie la dirección a un tipo de URL válido e inténtelo nuevamente.

Fallo de detección de proxy: La descarga HTTP del script .PAC falló: la conexión falló.

Compruebe que no se haya introducido una dirección o un nombre incorrecto. En caso afirmativo, corrija la entrada e inténtelo nuevamente. En caso contrario, es posible que el servidor esté inactivo. Inténtelo nuevamente más tarde.

Fallo de detección de proxy: La descarga HTTP del script .PAC falló: ruta no encontrada.

El archivo PAC solicitado no se encuentra en el servidor. Cambie esta opción en el servidor o vuelva a configurar el explorador.

Fallo de detección de proxy: La descarga HTTP del script .PAC falló.

Ocurrió un fallo de conexión al descargar el archivo PAC. Vuelva a conectarse e inténtelo nuevamente.

Fallo de detección de proxy: El script de configuración automática está vacío.

El archivo PAC está vacío. Cambie esta opción en el servidor o vuelva a configurar el explorador.

Fallo de detección de proxy: No hay respaldo para JavaScript.

Falta el archivo ejecutable PAC o el archivo de texto pac.js. Vuelva a instalar Receiver.

Fallo de detección de proxy: Error de JavaScript.

El archivo PAC contiene código JavaScript no válido. Corrija el archivo PAC en el servidor. Consulte también [Problemas de conexión](#).

Fallo de detección de proxy: El resultado del script de configuración automática no es válido.

Se recibió una respuesta con formato incorrecto por parte del servidor. Corrija esto en el servidor o vuelva a configurar el explorador.

Otros errores

Este tema contiene una lista de otros mensajes de error comunes que pueden aparecer al utilizar Receiver.

An error occurred. The error code is 11 (E_MISSING_INI_SECTION). Please refer to the documentation. Exiting.

Al ejecutar Receiver desde la línea de comandos, esto normalmente significa que la descripción otorgada en la línea de comandos no se ha encontrado en el archivo appsv.ini.

E_BAD_OPTION - The option "... " is invalid.

Falta el argumento para la opción "...".

E_BAD_ARG - The option "... " has an invalid argument: "...".

Se especificó un argumento no válido para la opción "...".

E_INI_KEY_SYNTAX - La clave "... " en el archivo de configuración "... " no es válida.

La información sobre el proveedor del servidor X en el archivo de configuración está dañada. Cree un archivo de configuración nuevo.

E_INI_VALUE_SYNTAX - El valor "... " en el archivo de configuración "... " no es válido.

La información sobre el proveedor del servidor X en el archivo de configuración está dañada. Cree un archivo de configuración nuevo.

E_SERVER_NAMELOOKUP_FAILURE - No se puede conectar con el servidor "...".

No puede resolverse el nombre del servidor.

No se puede escribir en uno o varios archivos: "...". Corrija los problemas de disco lleno o de permisos, y vuelva a intentarlo.

Verifique si existen problemas de disco lleno o problemas de permisos. Si se detecta y corrige un problema, vuelva a intentar la operación que originó el mensaje de error.

Se perdió la conexión con el servidor. Vuelva a conectarse e inténtelo nuevamente. These files might be missing data: "...".

Vuelva a conectarse y vuelva a intentar la operación que originó el error.

Envío de información de diagnóstico a la asistencia técnica de Citrix

Si tiene problemas con Receiver, es posible que la asistencia técnica de Citrix le pida información de diagnóstico. Esta información permite al equipo diagnosticar el problema y ofrecer la ayuda necesaria para solucionarlo.

Para obtener información de diagnóstico sobre Receiver

1. En el directorio de instalación, escriba `util/lurdump`. Se recomienda que haga esto en una sesión abierta y, si es posible, mientras el problema siga activo.
Se genera un archivo que contiene información de diagnóstico detallada, incluidos los detalles de la versión, el contenido de los archivos de configuración de Receiver y los valores de diversas variables del sistema.
2. Revise el archivo para ver si contiene información confidencial antes de enviarlo al departamento de asistencia técnica de Citrix.

Parámetros de línea de comandos

Jan 05, 2017

En las siguientes tablas se enumeran los parámetros de la línea de comandos de Citrix Receiver para Linux.

Nota

Se puede obtener una lista de los parámetros escribiendo `wfica` o `storebrowse` con las opciones `-?`, `-help` o `-h`.

wfica

Puede usar un archivo de conexión simplemente escribiendo su nombre después de `wfica` sin ninguna de las opciones siguientes.

Para	Escriba
Especificar la conexión personalizada para usar desde el archivo de conexión. Nota: Con la nueva interfaz de usuario de autoservicio, no puede establecer una conexión personalizada de este modo.	-desc descripción -description descripción
Especificar un archivo de escritorio para el inicio.	-desktop nombre de archivo
Especificar un archivo de conexión.	-file connection nombre de archivo
Establecer un archivo de protocolo alternativo. Esto permite el uso de un archivo <code>module.ini</code> alternativo.	-protocolfile nombre de archivo
Establecer un archivo de configuración del cliente alternativo. Esto permite el uso de un archivo <code>wfclient.ini</code> alternativo.	-clientfile nombre de archivo
Mostrar un nombre diferente para Citrix Receiver, especificado por nombre, toda vez que aparezca ese nombre. El nombre predeterminado es el nombre del dispositivo. Sin embargo, si utiliza un dispositivo Sunray, el nombre predeterminado deriva de la dirección MAC del dispositivo. Esto se anula por la entrada <code>ClientName</code> en <code>.ICAClient/wfclient.ini</code> , que a su vez se anula al emitir el comando <code>-clientname nombre</code> .	-clientname nombre
Mostrar esta lista de parámetros.	-help
Mostrar información de la versión.	-version

Mostrar números y cadenas de error. Para	Entorno Escriba
Establecer la ubicación de los archivos de instalación de Receiver. Esto equivale a establecer la variable de entorno ICAROOT.	-icaroot directorio
Suprimir los cuadros de diálogo de conexión.	-quiet
Habilitar el registro de clave.	-keylog
Establecer la geometría de sesión.	-geometry WxH+X+Y
Establecer la profundidad del color.	-depth <4 8 16 24 auto>
Establecer la expansión del monitor.	-span [h][o] [a mon1[,mon2[,mon3,mon4]]]
Utilizar el mapa de colores privado.	-private
Utilizar el mapa de colores compartido.	-share
Especificar una cadena que se agregará a una aplicación publicada.	-param cadena
Especificar la ruta de UNIX a la que se accederá a través de la asignación de unidades del cliente mediante una aplicación publicada.	-fileparam ruta unix
Especificar un nombre de usuario.	-username nombre de usuario
Especificar una contraseña oculta.	-password contraseña
Especificar una contraseña no cifrada.	-clearpassword "contraseña no cifrada"
Especificar un dominio.	-domain dominio
Especificar un programa inicial.	-program programa
Especificar un directorio que utilizará el programa inicial.	-directory directorio
Activar el sonido.	-sound

Desactivar el sonido. Para	no sound Escriba
Establecer los valores para reemplazar la asignación de unidades. Tienen la forma A\$=ruta, donde ruta puede contener una variable de entorno (por ejemplo, A\$=\$HOME/tmp). Esta opción se debe repetir para reemplazar cada unidad. Para que funcione el valor, debe haber una asignación existente, aunque no es necesario habilitarla.	-drivemap cadena

Sugerencia: Todas las opciones de línea de comandos de wfica también se pueden especificar en la variable de entorno WFICA_OPTS, lo que permite utilizarlas con la interfaz de usuario nativa de Receiver o con Citrix StoreFront. storebrowse

La siguiente tabla documenta las opciones que se pueden utilizar con la utilidad storebrowse.

Opción	Descripción	Notas
-L, --launch	Especifica el nombre del recurso publicado con el cual se desea establecer una conexión. Esta opción inicia una conexión con un recurso publicado. A continuación, se finaliza la utilidad y se obtiene una sesión conectada correctamente.	
-E, --enumerate	Enumera los recursos disponibles.	De forma predeterminada, se muestra el nombre del recurso, el nombre simplificado y la carpeta del recurso. Es posible mostrar información adicional mediante --details como opción.
-S, --subscribed	Enumera los recursos suscritos.	De forma predeterminada, se muestra el nombre del recurso, el nombre simplificado y la carpeta del recurso. Es posible mostrar información adicional mediante --details como opción.
-M, --details Usar junto con -E o -S como opción.	Selecciona los atributos de las aplicaciones publicadas que se deben devolver. Esta opción toma un argumento que es la suma de los números correspondientes a los detalles requeridos: Publisher(0x1), VideoType(0x2), SoundType(0x4), AppInStartMenu(0x8), AppOnDesktop(0x10), AppIsDesktop(0x20), AppIsDisabled(0x40), WindowType(0x80), WindowScale(0x100), DisplayName(0x200), and AppIsMandatory(0x10000). CreateShortcuts (0x100000) puede usarse junto con -S, -s y -u para crear entradas de menú para las aplicaciones suscritas.	Algunos de estos detalles no se encuentran disponibles a través de storebrowse. En ese caso, la salida es 0. Los valores pueden expresarse en decimal además de hexadecimal (por ejemplo, 512 para 0x200).

Opción	Descripción	Notas
	RemoveShortcuts (0x200000) se pueden usar con -S para eliminar todas las entradas de menú.	
-v, --version	Escribe el número de versión de storebrowse en la salida estándar.	
-?, -h, --help	Detalla los usos para storebrowse.	Aparecerá una versión abreviada de esta tabla.
-U, --username	Pasa el nombre de usuario al servidor.	Cuando se utiliza con StoreFront, el sitio debe configurarse para admitir HTTP BasicAuth; de lo contrario, se ignorarán.
-P, --password	Pasa la contraseña al servidor.	
-D, --domain	Pasa el dominio al servidor.	
-r, --icaroot	Especifica el directorio raíz de la instalación de Receiver para Linux.	Si no se especifica, el valor se determina durante la ejecución.
-i, --icons Usar junto con -E o -S como opción.	<p>Obtiene iconos de escritorio o de aplicación, en formato PNG, del tamaño y la profundidad indicados por best o size como argumento.</p> <p>Si el comando best , se obtiene el icono que tenga el mejor tamaño y esté disponible en el servidor. Puede convertirlo a cualquier tamaño necesario. El parámetro best es la más eficiente para el almacenamiento y el ancho de banda, y puede simplificar la creación de scripts.</p> <p>Si el comando size , se obtiene un icono con el tamaño y la profundidad indicados.</p> <p>En ambos casos, los iconos se guardan en un archivo para cada uno de los recursos que devuelve la opción -E o -S.</p>	<p>El parámetro best crea un icono con el formato: .png.</p> <p>El parámetro size tiene el formato WxB, donde W es la anchura del icono (todos los iconos son cuadrados, por lo que solo se necesita un valor para especificar el tamaño) y B es la profundidad de color (es decir, el número de bits por píxel). W es obligatorio pero B es optativo. Si no se especifica, se obtienen iconos de todas las profundidades de imagen disponibles para ese tamaño. Los archivos creados reciben un nombre con el formato _WxWxB.png.</p>
-u, --unsubscribe	Cancela la suscripción al recurso especificado del almacén suministrado.	
-s, --subscribe	Suscribe al recurso especificado del almacén suministrado.	Si usa un Receiver diferente, las suscripciones en servidores de Program Neighborhood se pierden.
-W [r R], --reconnect [r R]	Vuelve a conectar las sesiones activas y desconectadas.	-r vuelve a conectar todas las sesiones desconectadas para el usuario. R vuelve a conectar todas las sesiones activas y

Opción	Descripción	Notas
-WD, --disconnect	Desconecta todas las sesiones.	desconectadas. Solamente se aplica a las sesiones en el almacén especificado en la línea de comandos.
-WT, --logoff	Cierra todas las sesiones.	Solamente se aplica a las sesiones en el almacén especificado en la línea de comandos.
-l, --liststores	Muestra los almacenes de StoreFront conocidos, es decir, aquellos con los que puede contactar storebrowse. Estos son los almacenes registrados con el proxy de ServiceRecord. También enumera los sitios de Program Neighborhood.	
-a, --addstore	Registra un nuevo almacén, incluidos sus detalles de puerta de enlace y balizas, con el demonio de Service Record.	Devuelve la dirección URL completa del almacén. Si esto falla, se notifica un error.
-g, --storegateway	Establece la puerta de enlace predeterminada para un almacén que ya está registrado en el demonio de Service Record.	Este comando tiene el siguiente formato: ./util/storebrowse --storegateway "" "" Importante: El nombre exclusivo de la puerta de enlace debe estar en la lista de puertas de enlace para el almacén especificado.
-d, --deletestore	Cancela el registro de un almacén con el demonio de Service Record.	
-c, --configselfservice	Obtiene y establece los parámetros de interfaz de usuario de autoservicio que se guardan en StoreCache.ctx. Toma un argumento con el formato . Si solo está presente la entrada, se imprime el valor actual del parámetro. Si hay un valor, se usa para configurar el parámetro.	Ejemplo: storebrowse --configselfservice SharedUserMode=True Importante: Ambos, entrada y valor, distinguen entre mayúsculas y minúsculas. Los comandos que usen esta opción no funcionarán si el uso de minúsculas y mayúsculas es distinto del documentado en el parámetro mismo (en StoreCache.ctx).
-C, --addCR	Lee el archivo de Citrix Receiver (CR) suministrado, y solicita al usuario que agregue cada almacén.	La salida es la misma que -a, pero puede contener varios almacenes, separados por líneas nuevas.
-K, --killdaemon	Cierra el proceso de demonio de storebrowse.	Se eliminan todas las credenciales y todos los tokens.

pnabrowse

Importante: La utilidad pnabrowse es obsoleta, pero puede seguir consultando sitios de Agente de Program Neighborhood que ejecuten la Interfaz Web para obtener las listas de servidores y recursos publicados. También puede utilizarla para conectarse a un recurso publicado. Citrix recomienda no usar pnabrowse con almacenes de StoreFront; utilice storebrowse

en su lugar. La utilidad storebrowse puede pedir credenciales para sitios y almacenes. Las opciones -U, -P y -D solo funcionan con sitios de Agente de Program Neighborhood.

Un argumento optativo de pnbrowse especifica el servidor al que conectarse. Esto puede ser:

- El nombre del servidor XenApp, para las opciones -S y -A.
- La dirección URL del servidor que ejecuta la Interfaz Web, para las opciones -E y -L.

La utilidad pnbrowse devuelve un valor de salida que indica el éxito o el fracaso de la operación, y puede emplear las siguientes opciones con XenApp:

Opción	Descripción
-S	Lista de servidores, uno por línea.
-A	Lista de aplicaciones publicadas, una por línea.
-m	Usada conjuntamente con -A, esta opción amplía la información devuelta acerca de las aplicaciones publicadas, para incluir otros detalles: Publisher, Video Type, Sound Type, AppInStartMenu, AppOnDesktop, AppIsDesktop, AppIsDisabled, Window Type, WindowScale y Display Name.
-M	Usada conjuntamente con -A, esta opción selecciona columnas individuales de información devuelta sobre las aplicaciones publicadas. Toma un argumento (1-1023) que es la suma de los números correspondientes a los detalles requeridos: Publisher(1), VideoType(2), Sound Type(4), AppInStartMenu(8), AppOnDesktop(16), AppIsDesktop(32), AppIsDisabled(64), Window Type(128), Window Scale(256), y DisplayName(512).
-c	Cuando se agrega a la opción -A, crea archivos que especifican la cantidad mínima de información que el motor del cliente necesita para conectarse a aplicaciones publicadas; por ejemplo, el nombre de la aplicación, el servidor de exploración, la resolución de la ventana, la profundidad del color, parámetro de sonido y cifrado. Los nombres de archivo tienen el formato: /tmp/xxx_1.ica, /tmp/xxx_2.ica donde xxx se sustituye por el identificador de proceso decimal para el proceso de pnbrowse.
-d	Se usa en conjunción con -L para especificar el archivo de escritorio XDG.
-e	Muestra números de error.
-i	Incluye las rutas de los archivos que contienen las imágenes de iconos para las aplicaciones publicadas en la salida de la opción -A. Se devuelven archivos .xpm o .png, dependiendo del uso de la opción "size" (WxB): <ul style="list-style-type: none"> • -i devuelve iconos de 16x16 en formato XPM con 4 bits por píxel • -iWxB devuelve iconos WxW en formato PNG con B bits por píxel
-f	Incluye los nombres de carpetas de Citrix XenApp para las aplicaciones publicadas en la salida de la opción -A.
-u	Especifica un nombre de usuario para autenticar el usuario con un servidor proxy.

Opción	Descripción
-D	Especifica una contraseña para autenticar el usuario con un servidor proxy.

Las siguientes opciones proporcionan la funcionalidad de los servicios de Citrix XenApp (Agente de Program Neighborhood) y pueden utilizarse tanto con la funcionalidad de XenApp como con la de XenDesktop:

Opción	Descripción
-D	Especifica un dominio para autenticar el usuario en el servidor que ejecuta la Interfaz Web o el servidor que ejecuta el servicio de Citrix XenApp (Agente de Program Neighborhood).
-E	<p>Invoca Citrix XenApp y enumera todos los recursos publicados.</p> <p>Si se especifica tanto -E como -L, se aplica la última opción en la línea de comandos. La utilidad luego se cierra, dejando posiblemente una conexión abierta.</p> <p>Para cada recurso, se escriben los detalles siguientes en la salida estándar, entre comillas simples y separados por tabuladores:</p> <p>Nombre: El nombre simplificado tomado del cuadro de diálogo Propiedades de la aplicación de Access Management Console.</p> <p>Carpeta: La carpeta de Program Neighborhood, tomada del cuadro de diálogo Propiedades de la aplicación de Access Management Console.</p> <p>Tipo: Puede ser Aplicación o Contenido.</p> <p>Icono: La ruta completa de acceso a un archivo de icono con el formato .xpm.</p>
-L	Especifica el nombre del recurso publicado con el cual se desea establecer una conexión. Esto invoca a Citrix XenApp e inicia una conexión a un recurso publicado. Si se especifican tanto -E como -L, tiene efecto la última de las opciones de la línea de comandos. La utilidad luego se cierra, dejando posiblemente una conexión abierta.
-N	Especifica una contraseña nueva. Esta opción se debe usar con las credenciales existentes y solo es válida cuando la contraseña ha caducado, según lo indica el código de salida 238: E_PASSWORD_EXPIRED.
-P	Especifica una contraseña para autenticar el usuario en el servidor que ejecuta la Interfaz Web o el servidor que ejecuta el servicio de Citrix XenApp (Agente de Program Neighborhood).
-U	Especifica un nombre de usuario para autenticar el usuario en el servidor que ejecuta la Interfaz Web o el servidor que ejecuta el servicio de Citrix XenApp (Agente de Program Neighborhood).
-WD	Desconecta todas las sesiones activas del usuario.
-WT	Cierra todas las sesiones del usuario.

Opción	Descripción
-w	Reconecta todas las sesiones desconectadas del usuario.
-WR	Reconecta todas las sesiones (activas o desconectadas) del usuario.
-k	Usa un tíquet de Kerberos para autenticar, en lugar de nombre de usuario, contraseña y dominio. Esto requiere una configuración del cliente y el servidor. Para obtener más información, consulte la guía <i>— Uso de Kerberos con Citrix Receiver para Linux (Using Kerberos with Citrix Receiver for Linux Guide)</i> . Esta guía puede obtenerse de Citrix bajo un acuerdo de no divulgación.

Se usan las siguientes opciones comunes:

Opción	Descripción
-q	Modo silencioso; no mostrar mensajes de error.
-r	Incluye datos de icono sin formato para las aplicaciones publicadas en la salida de las opciones -E o -A.
-V	Muestra información detallada de la versión.
-h	Imprime un mensaje de uso con las opciones.
-?	Imprime un mensaje de uso con las opciones.