Acerca de esta versión

Nov 19, 2015

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.

Este apartado presenta las nuevas funciones de la versión 13.1 de Receiver para Linux, los problemas conocidos de dicha versión y un enlace a los problemas resueltos en esta versión y en versiones anteriores.

Novedades en la versión 13.1

Las siguientes funciones de Receiver para Linux 13.1 son nuevas:

- Uso de SSL v3 inhabilitado. Para evitar nuevos ataques, como el de POODLE, contra el protocolo SSLv3, esta versión de Receiver para Linux inhabilita su uso. Consulte http://support.citrix.com/article/ctx200238.
  Importante: Debe asegurarse de que TLS 1.0, 1.1 ó 1.2 esté habilitado.

Problemas resueltos en la versión 13.1

Problemas conocidos en la versión 13.1

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 la variable de entorno
— http_proxy
antes de iniciar esos comandos. Utilice el siguiente formato para la variable de entorno:

.[:]
[#403729]

Si Receiver para Linux genera un error de segmentación al acceder a tarjetas inteligentes, podría deberse a un problema con la biblioteca PKCS#11. Puede comprobar la biblioteca con la herramienta pkcs11-tool. La herramienta pkcs11-tool forma parte del paquete opensc. He aquí una prueba de ejemplo:
pkcs11-tool --module /usr/lib/libgtop11dotnet.so -l
Si esto también genera un error de segmentación, debería ponerse en contacto con el proveedor del controlador. También puede probar un controlador de una fuente distinta para el mismo tipo de tarjeta. Este problema se ha visto con el controlador Gemalto .NET que se incluye en Fedora 19 y en Fedora 20. [#493172]
Receiver para Linux respalda varios lectores de tarjetas; no obstante, solo se puede usar una tarjeta inteligente a la vez. [#494524]

El nombre de host de la máquina Linux no debería contener más de 20 caracteres para que las conexiones funcionen. Puede examinar y modificar este parámetro mediante el comando hostname . Cualquier usuario puede examinar el nombre de host, pero, para establecer uno, se necesita ser el usuario root o tener privilegios de administrador. [#494740]

Al trabajar con XenDesktop en modo de pantalla completa en Receiver para Linux 13.x, es posible que el protector de pantalla local no se active. Se trata de un problema externo, y el comportamiento puede variar según el sistema operativo del cliente. [#496398]

Receiver para Linux no permite conexiones a un almacén de StoreFront que no sea seguro (http://). Según la configuración del almacén, el usuario recibirá un mensaje de error del tipo "Error: No se puede recuperar el documento de descubrimiento"

o la primera conexión se realizará por HTTP, aunque las siguientes se cambiarán a HTTPS. También, si utiliza la dirección IP del nombre de host, es posible que vea errores acerca de los servicios de Citrix XenApp (antes conocido como PNAgent). Para evitarlo, utilice de forma explícita https:// o no anteponga http:// al nombre del servidor cuando escriba la URL. [#473027, #478667 y #492402]

Receiver para Linux no respalda el inicio de sesión con tarjetas inteligentes que contengan varios certificados de autenticación. [#488614]

En algunos dispositivos de bajo rendimiento que se encuentren en una sesión a pantalla completa, el proceso de inicio de sesión con autenticación mediante tarjeta inteligente puede tardar más de lo esperado, por lo que se agota el tiempo de espera. Puede evitar este problema si inhabilita el uso de H.264. Para inhabilitar el uso de H.264, siga las siguientes instrucciones:

1. Abra el archivo wfclient.ini.
2. Busque la sección "Thinwire3.0".
3. Agregue la entrada "H264Enabled=False".

Este problema se ha visto en máquinas basadas en armhf (ARM Hard Float) sin H.264 acelerado por hardware. [#497720]
Si un servidor PNAgent permite que el usuario contacte directamente con el controlador del dominio para cambiar contraseñas caducadas, esto solo se puede hacer con la versión compatible MIT de la biblioteca: libkcpm.so. Esto se debe a problemas con la versión compatible de Heimdal. Esta restricción se aplica a x86, armel y x64 (que utiliza el pnabrowse de x86). No se aplica a armhf. [#498037]

Aparece un error si un usuario abre la IU de autoservicio para conectarse al almacén de StoreFront y, a continuación, cierra la ventana de Receiver para Linux cuando el cuadro de diálogo de Authentication Manager está abierto. [#430193]

Si inserta una tarjeta inteligente errónea al intentar conectar con el almacén de StoreFront, es posible que vea un mensaje de error del tipo "Error de protocolo" o "Almacén especificado no encontrado", con lo que el problema no se explica [#496904].

Receiver para Linux requiere libpng12.so, pero no suele estar disponible en los repositorios estándar de los sistemas basados en Fedora. En este caso, busque por Internet un RPM adecuado a su sistema. Para openSUSE, libpng12.so está disponible, pero debe instalarse por separado. [#501937]

No se puede desconectar o cerrar la sesión de los escritorios virtuales desde la Central de conexiones. El botón Desconectar no está disponible y el botón Cerrar sesión no funciona. Para solucionar este problema, desconecte o cierre la sesión desde la sesión de escritorio, en lugar de hacerlo desde la Central de conexiones. Este problema no se ha observado con las aplicaciones virtuales. [#423651, #424847]

Una revisión hotfix para la versión 12.1 añadió a pnabrowse un código de salida E_SSLSDK_PASSWORD_LOCKED con el valor 220. Esto cambió el código de salida E_PASSWORD_EXPIRED a 239, que tenía un valor anterior de 238. En 13.0, el valor de E_SSLSDK_PASSWORD_LOCKED se cambió a 240, lo que restableció el valor correcto de E_PASSWORD_EXPIRED. No obstante, los valores listados por pnabrowse -errno todavía muestran significados incorrectos para los valores desde el 220 al 240. [#502550]

Requisitos del sistema

Nov 19, 2015

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

Devices

- 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 descodificador 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.

La versión del plug-in de Adobe Flash que se ejecuta en el dispositivo del usuario debe ser la misma que la ejecutada en el servidor XenApp o XenDesktop (o una versión posterior) para poder dar respaldo a la generación en el lado del cliente. Si este no es el caso, solo es posible la generación en el lado del servidor.

Citrix recomienda siempre actualizarse a la última versión del plug-in para obtener las funciones y correcciones de seguridad más recientes.

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 posterior.

Redirección de Windows Media de HDX MediaStream

La redirección de Windows Media de HDX MediaStream requiere

- GStreamer 0.10.15 o posterior.

Nota: De forma alternativa, 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 Philips 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 Philips.

Respaldo para tarjetas inteligentes

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

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.

Receiver para Linux respalda lectores de tarjeta inteligente que son compatibles con PCSC-Lite y tarjetas inteligentes con controladores PKCS#11 para la plataforma Linux adecuada. Para comprobar que Receiver para Linux encuentra el controlador PKCS#11, siga estos pasos y guarde la ubicación en un archivo de configuración:

1. Busque el archivo de configuración: $ICAROOT/config/AuthManConfig.xml.
2. Busque la línea PKCS11module y agregue la ubicación del controlador al elemento que sigue inmediatamente a 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 que comience por "/".

Para quitar la autenticación con tarjeta inteligente en Receiver para Linux, actualiceSmartCardRemovalAction 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 sigue inmediatamente a 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.

Disponibilidad de las funcionalidades de Receiver para Linux 13.x

Algunas de las funciones y características de Receiver están disponibles solo al conectarse con las versiones más recientes de XenApp y XenDesktop, y además puede requerir las últimas revisiones hotfix para esos productos.

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. Escribacd $ICAROOT/util y presione INTRO para navegar hasta el directorio Utilities del paquete de instalación.
3. Escribash hdxcheck.sh para ejecutar el script.

Instalación y configuración

Nov 19, 2015

A continuación se detallan los paquetes disponibles para Receiver para Linux:

- **Debian (archivo .deb)**:
  - x86: Paquetes de 32 bits y 64 bits (que contienen los binarios de 32 bits).
  - ARM: Paquetes de 32 bits para plataformas armel y armhf.
- **RPM Package Manager (archivo .rpm)**:
  - x86: Paquete de 32 bits.
- **Tarball (archivo .tar.gz)**:
  - x86 y ARM: Binarios de 32 bits en un paquete tarball para plataformas x86, armel y armhf.
  - x86 de 64 bits: Binarios de 64 bits en un paquete tarball para sistemas de 64 bits.

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

Puede acceder a los paquetes en la sección Descargas del sitio Web de Citrix (http://www.citrix.com/downloads/).

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

Instalación de Receiver para Linux desde un paquete Debian

Al instalar el paquete Debian de Receiver de 64 bits en un sistema Debian 7 (o una versión más antigua) de 64 bits, primero debe habilitar los paquetes i386. Para comprobar si los paquetes i386 ya están habilitados, escriba el comando siguiente en la línea de comandos: `dpkg --print-foreign-architectures`. A continuación, fíjese en los siguientes aspectos según el resultado:

- Si `i386` aparece en la salida, puede proceder e instalar el paquete.
- Si `i386` no aparece en la salida, escriba la siguiente serie de comandos para habilitar los paquetes:

1. `sudo dpkg --add-architecture i386`
2. `sudo apt-get update`

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

Sugerencia: Este procedimiento utiliza una línea de comandos. 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.

1. Inicie sesión como usuario con privilegios (root).
2. Abra una ventana de terminal.
3. Ejecute la instalación escribiendo `dpkg -i nombre_del_paquete.deb`.
4. Instale los paquetes dependientes que falten, escribiendo `sudo apt-get -f install`.
5. Instale el paquete de respaldo USB mediante el mismo comando de ejecución.

Para instalar Receiver para Linux desde un paquete RPM

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

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

1. Inicie sesión como usuario con privilegios (root).
2. Abra una ventana de terminal.
3. Para ejecutar la instalación, escriba zypper install nombre del paquete.rpm. Por ejemplo, zypper install ./ICAClient-suse11sp3-13.2.1.328635-0.x86_64.rpm.
4. Instale el paquete de respaldo USB mediante el mismo comando de ejecución.

Para instalar Receiver para Linux desde un paquete tarball

1. Abra una ventana de terminal.
2. Descomprima el archivo .tar.gz y extraiga el contenido en un directorio temporal vacío. Por ejemplo, para plataformas Linux, 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 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. (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).

   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 presione Intro.
7. Es posible elegir integrar Receiver con el entorno de escritorios. 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 asegurarse de 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 ha instalado GStreamer previamente, puede elegir si desea integrarlo con Receiver y ofrecer así respaldo para la aceleración multimedia HDX MediaStream. Para integrar Receiver con GStreamer, escriba y en el símbolo del sistema.
9. Si ha iniciado sesión como usuario con privilegios (root), podrá elegir si desea instalar el respaldo USB para las aplicaciones VDI publicadas de 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 la siguiente advertencia: Solo los usuarios root pueden instalar el respaldo de USB. Ejecute el instalador como root para acceder a esta opción de instalación.
10. Una vez completada la instalación, aparecerá nuevamente el menú principal de instalación. Para salir del programa de instalación, escriba 3 y presione Intro.

Para desinstalar Citrix Receiver para Linux

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

1. Ejecute el programa de instalación escribiendo $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.

Personalización de la instalación de Receiver para Linux

Nov 19, 2015

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

Para personalizar una instalación de Receiver para Linux

1. Expanda el archivo del paquete de Receiver en un directorio vacío. El archivo del paquete se llama plataforma.mayor.menor.versión.compilación.tar.gz (por ejemplo, linuxx86.13.1.0.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*. Para obtener más información acerca de los certificados integrados, consulte *— Configuración y habilitación de SSL y TLS*.
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 Receiver para Linux

Nov 19, 2015

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

Si 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.

Para iniciar Receiver en el símbolo del sistema de un terminal

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

Para iniciar Receiver desde el escritorio de Linux

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

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

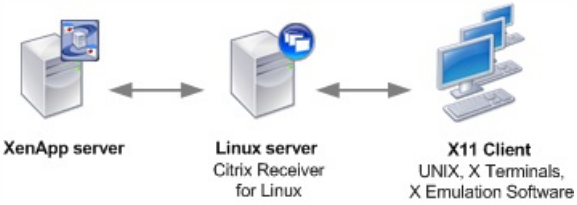
Uso de Receiver para Linux como proxy de ICA a X

Nov 19, 2015

Puede utilizar una estación de trabajo que ejecuta Receiver como servidor y redirigir la salida a otro dispositivo compatible con X11. Se recomienda realizar esto para distribuir aplicaciones de Microsoft Windows a terminales X o estaciones de trabajo UNIX en las que Receiver no está disponible. Tenga en cuenta que el software de Receiver está disponible para varios dispositivos X y en esos casos la solución preferida es instalar el software en los dispositivos. Esta forma de ejecutar Receiver, como proxy de ICA a X, se conoce también como ICA en el lado del servidor.

Cuando se ejecuta 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 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 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 Receiver en el servidor Linux que normalmente proporciona las aplicaciones X para los terminales X.
- Si desea distribuir estaciones de trabajo UNIX en las que 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 Receiver con ICA en el lado del servidor desde una 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 usa el comandossh -X para conectarse al dispositivo que actúa como proxy, no necesita configurar la variable de entorno **DISPLAY**.

3. En el símbolo del sistema del dispositivo local, escribaxhost <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 Receiver. Escriba lo siguiente en el símbolo del sistema:selfservice &

Configuración de Receiver para Linux

Nov 19, 2015

Receiver ofrece a los usuarios acceso de autoservicio seguro 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 heredadas, creadas con la Interfaz Web, administran el acceso de los usuarios.

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

La página de inicio de 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 usa el mismo nombre para varios almacenes en el servidor StoreFront, éstos aparecerán de forma idéntica en la página Cuentas. Para evitar confundir al usuario, los administradores deben usar nombres exclusivos para los almacenes cuando los configuren. 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 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 Receiver y los servidores de XenApp y XenDesktop. También puede cambiar esos parámetros para conexiones individuales, si es necesario.

Conexión con recursos desde una línea de comandos o explorador

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 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

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 o un escritorio y cierre la ventana en la que se muestra.

Personalización de Receiver mediante 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 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 Receiver

Si desea que los cambios se apliquen a todos los usuarios de 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 permitir 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 Receiver

Si desea que los cambios se apliquen a todos los futuros usuarios nuevos de Receiver, modifique los archivos de configuración en el directorio $ICAROOT/config. Para que los cambios se apliquen a todas las conexiones, actualice wfclient.ini en este directorio.

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.

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Citrix XenApp permite a los usuarios conectarse a recursos publicados (es decir, aplicaciones publicadas, escritorios de servidor y contenido publicado) a través de un servidor que ejecuta un sitio de servicios XenApp. Además, Citrix XenApp crea los elementos de menú y de escritorio para que los usuarios puedan acceder a los recursos publicados.

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 Citrix XenApp, el programa lee los datos de configuración del servidor. Después de eso, Citrix XenApp actualiza periódicamente su configuración e interfaz de usuario, según los intervalos especificados en el archivo config.xml.

Importante: config.xml afecta a todas las conexiones definidas por el servidor de la Interfaz Web.

Publicar contenido

Por lo general, Receiver se conecta con aplicaciones y escritorios. Receiver también puede abrir archivos específicos asociados a una aplicación. En este caso, el administrador publica un archivo en lugar de una aplicación. Este proceso se denomina publicación de contenido y es una manera útil de compartir cualquier tipo de información electrónica con los usuarios de la red.

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 del entorno de Receiver

Nov 19, 2015

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

- Asignación de dispositivos del usuario
- Configuración del respaldo para 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 del usuario

Nov 19, 2015

Receiver admite la asignación de dispositivos del cliente para conexiones a servidores de 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 de Linux con Seguridad Mejorada (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 USB portátiles.
- 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 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 al respecto, 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

Receiver admite la impresión en impresoras de red e impresoras conectadas localmente a los dispositivos de usuarios. 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
   - Directorio $ICAROOT/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

Receiver para Linux admite el controlador PS de impresora universal 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 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.
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 nombredelcliente en la sesión 3".

Asignación de impresoras del cliente en XenApp para UNIX

En un entorno UNIX, se ignoran los controladores de impresora definidos por 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 para UNIX en eDocs.

Asignación de sonido del cliente

La asignación de sonido del cliente permite que las aplicaciones que se ejecutan en el servidor XenApp 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 de XenApp, 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 con 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 para USB

Nov 19, 2015

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.

Los entornos LAN típicos de alta velocidad y baja latencia admiten funciones isócronas en los dispositivos USB como cámaras web, micrófonos, altavoces y auriculares. Esto permite a estos dispositivos interactuar con paquetes como Microsoft Office Communicator y Skype.

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 dispositivos 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 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.

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 > Preferences > Removable Drives and Media, y en la ficha Storage, en Removable Storage, deje sin marcar la casilla Browse removable media when inserted.
Nota: Si la directiva del 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

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 del siguiente modo.

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.

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 los menús 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.

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.

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.

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 que se encuentran 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 un administrador se aplican antes de las reglas predeterminadas, cuando se inicia un escritorio virtual. Esto permite sobrescribir las reglas predeterminadas de XenDesktop.

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

Crear 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

Mejora del rendimiento en conexiones con poco ancho de banda

Nov 19, 2015

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 las 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 las dimensiones de la ventana al tamaño utilizable más pequeño posible. En el sitio de servicios XenApp, defina las Opciones de sesión.
- **Reduzca la cantidad de colores**: Reduzca la cantidad de colores a 256. En el sitio de servicios XenApp, 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 con 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

Nov 19, 2015

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.

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, 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 plugin 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 si el vídeo se muestra 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.

Para configurar 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 configurado para preguntar (**Ask**) y se presenta un cuadro de diálogo a los usuarios para preguntarles si desean 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. Para permitir que las sesiones de Receiver administren la introducción de datos con el teclado o el mouse tanto dentro como fuera de cualquier ventana que reproduzca contenido Flash, en /config/module.ini cambie FlashV2=Off para FlashV2=On.

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, Skype o Microsoft Office Communicator.

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 (predeterminado vía compresión de vídeo de cámara Web de HDX RealTime)
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

Nov 19, 2015

Es posible mejorar la manera en que se procesan los cuadros de pantalla codificados con JPEG mediante las funciones de 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

Nov 19, 2015

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

- Preferences
- Suavizado de fuentes ClearType
- Redirección de carpetas especiales
- Redirección de contenido de servidor a cliente
- Comportamiento del teclado
- xcapture

Definición de preferencias

Nov 19, 2015

Para definir sus preferencias, haga clic en Preferencias en el menú de 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 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 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).

1. En la página General del cuadro de diálogo Preferencias, seleccione uno de esos modos para Mostrar escritorios en.

Para reconectar automáticamente las sesiones

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).

1. 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.

1. 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 Flash Player e incluye animaciones, vídeo y aplicaciones.

1. 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 ClearType

Nov 19, 2015

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 wfclient.ini.

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 aumentan significativamente 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.ini. Si el servidor establece el valor en 0, la preferencia local está determinada por otro parámetro en wfclient.ini:
FontSmoothingTypePref = número

donde número puede tomar uno de los siguientes valores:

Valor	Comportamiento
0	Sin suavizado
1	
2	Suavizado estándar
3	Suavizado ClearType (subpixel horizontal) (valor predeterminado)

Configuración de la redirección de carpetas especiales

Nov 19, 2015

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 wfclient.ini, según se describe aquí:

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

   SFRAllowed = True

2. Agregue el siguiente texto en wfclient.ini (por ejemplo, $HOME/.ICAClient/wfclient.ini):
   DocumentsFolder = documentos

   DesktopFolder = escritorio

   dondedocumentos yescritorio son los nombres de archivo de UNIX, incluida la ruta completa, de los directorios que desea 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

Nov 19, 2015

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 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 Receiver siempre que la ruta incluya a RealPlayer y al menos una de las siguientes opciones: Firefox, Mozilla o Netscape.

Nota: RealPlayer para Linux puede obtenerse en http://proforma.real.com/real/player/unix/unix.html.

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:

   $ICAROOT/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 path es el directorio donde está ubicado el archivo ejecutable de RealPlayer y command 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 ambos parámetrosPath 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

Nov 19, 2015

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+Entrar pasa la combinación Ctrl+Alt+Supr al escritorio remoto.

Uso de xcapture

Nov 19, 2015

El paquete de 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

Nov 19, 2015

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, 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. Receiver intenta repetidamente 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, Receiver espera 36 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 AccessGateway, ACR no se encuentra disponible. Para resguardarse de exclusiones de red, compruebe que la función de fiabilidad de sesiones está habilitada tanto en el servidor como en el cliente, y que, además, está configurada en AccessGateway.

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

Nov 19, 2015

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.

Importante: La función de fiabilidad de sesiones de HDX Broadcast necesita que otra característica, Common Gateway Protocol, 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.
Los usuarios de Receiver no pueden anular la configuración del servidor. Para obtener más información sobre estas funciones, consulte la documentación de XenApp y XenDesktop.

Protección de las comunicaciones de Receiver

Nov 19, 2015

Para proteger la comunicación entre la comunidad de servidores y 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

Nov 19, 2015

Los servidores proxy se utilizan para limitar el acceso hacia la red y desde ella, y para gestionar conexiones entre Receiver y los entornos de Citrix XenApp o Citrix XenDesktop. Receiver admite el protocolo SOCKS, junto con Secure Gateway y Traspaso SSL Citrix, el protocolo de proxy seguro y la autenticación Challenge/Response 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.

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

Importante: 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.

Conexión con Secure Gateway o Traspaso SSL Citrix

Nov 19, 2015

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.

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

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 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 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 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:

- Host name
- 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.

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 SSL/TLS, descifra los datos antes de redirigirlos al servidor o a Citrix XML Service (si el usuario ha seleccionado la exploración TLS+HTTPS).

Si configuró el Traspaso SSL para un puerto de escucha distinto a 443, debe especificar en 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.

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.

Para forzar la conexión de Receiver únicamente con TLS, debe especificar TLS en el servidor Secure Gateway o en el Traspaso SSL. Para obtener más información, consulte la documentación de Secure Gateway o del servicio del Traspaso SSL.
Nota: Esta versión de Receiver para Linux inhabilita el uso del protocolo SSLv3.
Para obtener más información sobre Secure Gateway para Windows o Traspaso SSL Citrix, consulte la documentación de XenApp.

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, 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

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: 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

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

Nov 19, 2015

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 "libpscslite1" 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.

Conexión a través de NetScaler Gateway

Nov 19, 2015

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://puertaDeEnlace.empresa.com.
   - Para conectar con un almacén específico, use una URL con el formato https://puertaDeEnlace.empresa.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 de Receiver para Linux

Nov 19, 2015

Esta sección de eDocs contiene información que ayudará a los administradores a solucionar todo tipo de problemas técnicos con Receiver para Linux.

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 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 los archivos para ver si contienen información confidencial antes de enviarlos al departamento de asistencia técnica de Citrix.

Problemas de conexión

Nov 19, 2015

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

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.

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.

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.

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 ...;

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).

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 $ICAROOT/config/module.ini:

LastComPortNum=2 ComPort1= ComPort2=

Problemas de presentación

Nov 19, 2015

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

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 sobre la especificación de teclados, consulte Control del comportamiento del teclado.

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.

El modo integrado elimina los accesorios locales del administrador de ventanas, como la barra de título y los bordes, y en su lugar utiliza accesorios enviados desde el servidor. Los diferentes administradores de ventanas utilizan distintas formas de eliminar los accesorios de las ventanas.

Receiver define la directriz _MOTIF_DECORATIONS para eliminar los accesorios. También define la clase de todas las ventanas integradas en “Wfica_Seamless”, de modo que se pueda ordenar a un administrador de ventanas que no reconoce la directriz Motif que elimine los accesorios a través de entradas en archivos de recursos.

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.

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.

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.

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.

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.

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.

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]]]

Sih está especificado, se imprime una lista de monitores en stdout. Además, si ese es el valor completo de la opción, wfica se cierra.

Sio está especificado, la ventana de la sesión tendrá el atributo de redirección override-redirect.

Precaución: No se recomienda usar 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.
Sia está especificado, 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.

Asumiendo queo no se especificó, wfica utilizará el mensaje _NET_WM_FULLSCREEN_MONITORS para solicitar al

administrador de ventanas una disposición de ventanas adecuada, 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 usando -span o.

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

1. Escriba lo siguiente en el símbolo del sistema: /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 el símbolo del sistema: /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.

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 con el valorNo 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

Nov 19, 2015

Es posible que se encuentre con los siguientes problemas con el explorador.

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 desde el servidor al cliente, consulte Configuración de la redirección de contenido servidor-cliente.

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.

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.

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.

Pruebe a habilitar el plugin ICA.

Pruebe a inhabilitar el plugin ICA.

Otros problemas

Nov 19, 2015

Es posible que se encuentre con los siguientes problemas adicionales.

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.

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.

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 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.

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:

  - Change Hotkey1Shift=Ctrl+Shift por 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 con el valor Remote.
- Reconfigure el administrador de ventanas de modo que suprima las combinaciones de teclado predeterminadas.

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 con el valor True.
2. Establezca UseEUKS con el valor 2.

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.

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

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

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

Mensajes de error comunes

Nov 19, 2015

En esta sección se proporcionan descripciones para los mensajes de error comunes.

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

E_MISSING_INI_SECTION - Verify the configuration file: "...". The section "..." is missing in the configuration file.

El archivo de configuración se editó incorrectamente o está dañado.

E_MISSING_INI_ENTRY - Verify the configuration file: "...". The section "..." must contain an entry "...".

El archivo de configuración se editó incorrectamente o está dañado.

E_INI_VENDOR_RANGE - Verify the configuration file: "...". The X server vendor range "..." in the configuration file is invalid.

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

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

E_CSM_MUST_SPECIFY_SERVER - You must enter a server.

Debe introducirse un nombre de servidor en la página Network del cuadro de diálogo Properties.

E_CANNOT_WRITE_FILE - Cannot write file: "..."

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 - Cannot create file: "..."

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

E_CSM_CONNECTLIST_INVALID - Cannot find selected connection.

El archivo de configuración está dañado. Cree un archivo de configuración nuevo.

E_CSM_CONNECTION_NOTFOUND - Cannot find selected connection.

El archivo de configuración está dañado. Cree un archivo de configuración nuevo.

E_CSM_APPSERVERLIST_MISSING - Verify the configuration file "...". Section "..." is missing. Cree un archivo de configuración nuevo.

El archivo de configuración está dañado. Cree un archivo de configuración nuevo.

E_CSM_APPSRV_SECTION_MISSING - Verify the configuration file "...". Section "..." is missing. Cree un archivo de configuración nuevo.

El archivo de configuración está dañado. Cree un archivo de configuración nuevo.

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.

E_CSM_DESCRIPTION_NONUNIQUE - The Description must be unique. This description is already in use.

El texto Description en la página Network del cuadro de diálogo Properties debe ser único.

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

Proxy detection failure: Improper auto-configuration URL.

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.

Proxy detection failure: .PAC script HTTP download failed: Connect failed.

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.

Proxy detection failure: .PAC script HTTP download failed: Path not found.

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

Proxy detection failure: .PAC script HTTP download failed.

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

Proxy detection failure: Empty auto-configuration script.

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

Proxy detection failure: No JavaScript support.

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

Proxy detection failure: JavaScript error.

El archivo PAC contiene código JavaScript no válido. Corrija el archivo PAC en el servidor. Consulte también Problemas de conexión.

Proxy detection failure: Improper result from proxy auto-configuration script.

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

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 appsrv.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 - The key "..." in the configuration file "..." is invalid.

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 - The value "..." in the configuration file "..." is invalid.

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 - Cannot connect to server "...".

No puede resolverse el nombre del servidor.

Please contact your help desk with the following information: Cannot browse NDS tree: "...".

Comuníquese con el personal de asistencia técnica para darles los detalles sobre este mensaje de error.

Cannot write to one or more files: "...". Correct any disk full issues or permissions problems and try again.

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.

Server connection lost. Vuelva a conectarse e inténtelo nuevamente. These files might be missing data: "...".

Parámetros de línea de comandos

Nov 19, 2015

En la siguiente tabla se enumeran los parámetros de la línea de comandos de Receiver para Linux.

Nota: Se puede obtener una lista de parámetros escribiendo wfica o storebrowse con -?, -help, o -h .

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 module.ini alternativo.	-protocolfile nombre de archivo
Establecer un archivo de configuración del cliente alternativo. Esto permite el uso de un archivo wfclient.ini alternativo.	-clientfile nombre de archivo
Mostrar un nombre diferente para 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 ClientName en .ICAClient/wfclient.ini, que a su vez se anula al emitir el comando -clientname nombre.	-clientname nombre
Mostrar esta lista de parámetros.	-help
Mostrar información de la versión.	-version
Mostrar números y cadenas de error.	-errno
Establecer la ubicación de los archivos de instalación de Receiver. Esto equivale a establecer la variable de entorno ICAROOT.	-icaroot directorio

Para	Escriba
Suprimir los cuadros de diálogo de conexión.	-quiet
Registrar el proceso de conexión.	-log
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 password
Especificar una contraseña no cifrada.	-clearpassword "contraseña no cifrada"
Especificar un dominio.	-domain domain
Especificar un programa inicial.	-program programa
Especificar un directorio que utilizará el programa inicial.	-directory directorio
Activar el sonido.	-sound
Desactivar el sonido.	-nosound

Para	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.

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 la opción --details .
-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 la opción --details .
-M, --details Úsela junto con la opción -E o -S .	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. RemoveShortcuts (0x200000) se pueden usar con -S para eliminar todas las entradas de menú.	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
-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.	Estas opciones están obsoletas y es posible que se eliminen en futuras versiones. Funcionan con sitios de Agente de Program Neighborhood, pero se omiten en los sitios de StoreFront. Citrix recomienda no usar estas opciones y, en su lugar, dejar que el sistema solicite a los usuarios sus credenciales.
-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 Úsela junto con la opción -E, o -S .	Obtiene iconos de escritorio o de aplicación, en formato PNG, del tamaño y la profundidad indicados por los argumentos best o size . Si se usa el argumento best se obtiene el icono que tenga el mejor tamaño y esté disponible en el servidor. Puede convertirlo a cualquier tamaño necesario. El argumento best es el más eficiente para el almacenamiento y el ancho de banda, y puede simplificar la creación de scripts. Si se usa el argumento size se obtiene un icono con el tamaño y la profundidad indicados. En ambos casos, los iconos se guardan en un archivo para cada uno de los recursos que devuelve la opción –E o -S.	El argumento best crea un icono con el formato: .png. El argumento 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.
-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 reconecta todas las sesiones desconectadas para el usuario. R reconecta todas las sesiones activas y desconectadas.
-WD, --disconnect	Desconecta todas las sesiones.	Solamente se aplica a las sesiones en el almacén especificado en la línea de comandos.

Opción	Descripción	Notas
-O, --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.

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, y permite conectarse a un recurso publicado. Citrix desaconseja el uso de pnabrowse con almacenes StoreFront; use storebrowse en su lugar. storebrowse puede pedir credenciales desde sitios y almacenes. Las opciones -U, -P y -D solo funcionan con sitios de Agente de Program Neighborhood.

Un argumento optativo de pnabrowse 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 pnabrowse 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 pnabrowse.
-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): • -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.
-p	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	Invoca Citrix XenApp y enumera todos los recursos publicados. 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. Para cada recurso, se escriben los detalles siguientes en la salida estándar, entre comillas simples y separados por tabuladores: Nombre: El nombre simplificado tomado del cuadro de diálogo Propiedades de la aplicación de Access Management Console. Carpeta: La carpeta de Program Neighborhood, tomada del cuadro de diálogo Propiedades de la aplicación de Access Management Console. Tipo: Puede ser Aplicación o Contenido. Icono: La ruta completa de acceso a un archivo de icono con el formato .xpm.
-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.
-Wr	Reconecta todas las sesiones desconectadas del usuario.

Opción	Descripción
-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 *— Uso de Kerberos con Citrix Receiver para Linux (Using Kerberos with Citrix Receiver for Linux Guide)* . 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.