

Acerca de Citrix Receiver para Linux 13.5

Jul 07, 2017

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

Citrix Receiver para Linux 13.5

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

- Respaldo para ICA de secuencias múltiples
- Respaldo para la redirección de vídeos HTML5
- Respaldo para GStreamer 1.x
- Respaldo a la extensión Indicación de nombre de servidor (SNI) para TLS. Esto permite que un servidor que aloja varios sitios seguros presente el certificado correcto a Citrix Receiver.

Problemas resueltos de Citrix Receiver para Linux 13.5

Jul 07, 2017

Se han solucionado los problemas siguientes en Receiver para Linux 13.x:

[Receiver para Linux 13.5](#)

[Receiver para Linux 13.4](#)

[Receiver para Linux 13.3](#)

[Receiver para Linux 13.2](#)

[Receiver para Linux 13.1](#)

[Receiver para Linux 13.0](#)

Receiver para Linux 13.5

Se han solucionado los problemas siguientes desde la versión 13.4:

[Redirección de Flash de HDX MediaStream](#)

[Experiencia de usuario](#)

[Sesión/Conexión](#)

[Interfaz de usuario](#)

[Excepciones del sistema](#)

Redirección de Flash de HDX MediaStream

- Si cambia el tamaño de una ventana de Microsoft Internet Explorer que tenga habilitada la redirección de Flash de HDX MediaStream, los sitios Web con contenido Flash podrían no cambiar correctamente de tamaño para ajustarse a la ventana de Internet Explorer modificada.

[#LC6126]

Sesión/Conexión

- Al reproducir un clip multimedia en la sesión de escritorio ejecutada en un cliente ligero HP, el Reproductor de Windows Media podría generar el siguiente mensaje de error:

"El Reproductor de Windows Media encontró un problema al reproducir el archivo".

En algunos casos, puede aparecer una ventana vacía o en negro.

[#LC5508]

- Los menús desplegables correspondientes a las aplicaciones publicadas pueden desaparecer inmediatamente después de aparecer cuando las aplicaciones se inician desde Citrix Receiver para Linux.

[#LC5574]

- Al iniciar una sesión y, a continuación, cancelar la barra de progreso de la conexión, el proceso wfica puede enviar SIGTERM a todos los procesos que se encuentren dentro de su grupo de proceso. Los procesos pueden cerrarse inesperadamente mientras comparten el grupo de procesos.

[#LC5858]

- En un entorno de varios monitores, cuando se ejecuta una aplicación integrada en el segundo monitor, cambiar entre las áreas de trabajo en Gnome 3 puede provocar que la aplicación integrada se vea incorrectamente. El problema se produce si "workspaces-only-on-primary" está habilitado en Gnome 3.

[#LC5897]

- El método abreviado de teclado "Ctrl + Alt + Supr" en la barra de herramientas de Desktop Viewer puede no funcionar en sesiones de Linux VDA.

[#LC6164]

- Cuando intenta iniciar una aplicación haciendo clic en el icono correspondiente del escritorio, la aplicación podría no iniciarse.

[#LC6285]

- Si intenta iniciar una sesión habilitada con respaldo a la codificación H.264 en Linux VDA, puede producirse un error de segmentación en wfica.

[#LC6603]

Excepciones del sistema

- Si intenta conectarse a determinados sitios XenApp o XenDesktop, AuthManagerDaemon puede cerrarse inesperadamente.

[#LC6166]

Experiencia de usuario

- Cuando se inicia una aplicación integrada que contiene varias ventanas secundarias, no podrá mover determinadas ventanas secundarias. Además, es posible que no pueda cambiar el foco a estas ventanas.

[#LC4342]

- Cuando cierre la sesión en un escritorio local con el cuadro de diálogo de credenciales de autoserivicio abierto, los intentos posteriores de iniciar sesión en el autoserivicio pueden fallar y el autoserivicio podría no pasar nunca al cuadro de diálogo de autenticación.

[#LC4939]

- Cuando se inicia Microsoft Excel en el modo integrado, el foco del teclado a veces no se mueve a la ventana "Buscar" en la aplicación.

[#LC5964]

Interfaz de usuario

- Los iconos "Sametime" pueden no aparecer en el área de notificaciones cuando se usa Citrix Receiver para Linux.
[#LC3956]
- Si se mueve la ventana de chat de Microsoft Lync a una nueva posición, esta podría no volver a dibujarse completamente.
[#LC5583]
- Cuando se inicia Microsoft Excel en el modo integrado, puede que la ventana "Buscar" de la aplicación no se mueva.
[#LC5963]
- Si minimiza una ventana secundaria (por ejemplo, la ventana principal de Spy++ es la ventana principal y la ventana de detección de ventanas concretas es la ventana secundaria), el tamaño de la barra minimizada de título puede parecer más pequeña.
[#LC6210]

Receiver para Linux 13.4

Se han solucionado los problemas siguientes desde la versión 13.3:

[Problemas en el dispositivo cliente](#)

[Tarjetas inteligentes](#)

[Mejoras](#)

[Excepciones del sistema](#)

[Inicio de sesión/Autenticación](#)

[Experiencia de usuario](#)

[Sesión/Conexión](#)

[Interfaz de usuario](#)

Problemas en el dispositivo cliente

- Con la asignación de unidades del cliente habilitada, a veces las unidades asignadas tardan más tiempo del esperado en acceder.
[#LC3930]

Mejoras

- En esta versión, se introduce el respaldo al mouse relativo, una característica que ofrece una opción para interpretar la posición del puntero de un modo relativo en lugar de hacerlo de un modo absoluto. Esta funcionalidad se necesita para aplicaciones que exigen la entrada de datos de un puntero relativo y no de un puntero absoluto.

Nota: Esta funcionalidad está disponible únicamente en sesiones con XenApp o XenDesktop 7.8. De forma predeterminada, está inhabilitada.

- Para habilitar la funcionalidad:*

En el archivo \$HOME/.ICAClient/wfclient.ini, en la sección [WFClient], agregue la entrada RelativeMouse=1. Esto habilita la función, pero la mantiene inactiva hasta que usted la active.

- Para activar la función:

Introduzca Ctrl/F12.

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

- Para desactivar la función:

Introduzca Ctrl-Mayús/F12.

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

* También puede considerar los siguientes valores de RelativeMouse:

RelativeMouse=2. Habilita la función y la activa siempre que se enfoque la ventana de una sesión.

RelativeMouse=3. Habilita y activa la función, y la mantiene activa en todo momento.

Para cambiar los comandos del teclado, agregue parámetros como:

RelativemouseOnChar=F11

RelativeMouseOnShift=Shift

RelativemouseOffChar=F11

RelativeMouseOffShift=Shift

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

[#LC5000]

Inicio de sesión/Autenticación

- La versión 13.3 de Citrix Receiver para Linux no pasa algunos parámetros de línea de comandos (como la opción -clearpassword) a versiones más antiguas de XenApp. Por eso, es posible que los usuarios no consigan iniciar sesión.

[#LC4594]

Sesión/Conexión

- Pueden fallar los inicios de sesión en el modo de pantalla completa con la opción de línea de comandos "-span".

[#LC3394]

- En una configuración de varios monitores, después de cambiar el tamaño del monitor secundario, es posible que la barra de tareas de Windows no vuelva a la ubicación original.

[#LC3856]

- En wfica, un error de segmentación puede provocar que las sesiones se desconecten o dejen de responder durante las actualizaciones de pantalla que resultan de actividades como resaltados o desplazamientos.

[#LC3947]

- Al reconectarse a una sesión desconectada de varios monitores en Ubuntu 14.04, la ventana de sesión solo aparece en un monitor (en lugar de aparecer en todos).

[#LC4181]

- Es posible que no se pueda establecer conexión con una tienda anónima y aparezcan los siguientes mensajes de error: "NoWebUIAuth 0" y "Cannot complete your request".

[#LC4270]

- Los intentos de iniciar un escritorio publicado pueden fallar si se utiliza un proxy host de SSL como Traspaso SSL.

[#LC4739]

- Es posible que una instancia publicada de Internet Explorer pierda el foco y se duplique cuando aparezca una ventana emergente en la ventana original del explorador.

[#LC5066]

Tarjetas inteligentes

- Si se utiliza una tarjeta inteligente con pnbrowse, el PIN no se puede pasar al VDA y la autenticación puede fallar. La sesión se inicia, pero aparece la pantalla de inicio de sesión.

[#LC4241]

Excepciones del sistema

- Después de reproducir medios con el Reproductor de Windows Media en un cliente Linux basado en ARM hard float (armhf), las sesiones se desconectan.

[#LC4625]

Experiencia de usuario

- En sesiones que se ejecuten en XenApp o XenDesktop 7.6, la calidad de sonido puede ser baja.

[#LC3124]

- En implementaciones ARM hard float (armhf), a veces la barra de tareas no se ilumina para indicar mensajes nuevos de Lync 2010.

[#LC3688]

- Después de desbloquear una sesión de usuario en una configuración de dos monitores, es posible que las ventanas minimizadas no vuelvan a la posición correcta y puede parecer que han dejado de responder.

[#LC3984]

- En un escritorio Gnome 3, cuando se inicia una aplicación y se maximiza, la posición del cursor puede cambiar por la distancia de la barra superior de Gnome 3.

[#LC4738]

- A veces, la redirección de cámaras Web no funciona en sesiones que se ejecutan en agentes VDA 7.6.

[#LC4751]

Interfaz de usuario

- A veces, la función "Copiar y pegar" falla entre servidor y servidor, y entre el servidor y el dispositivo del usuario.

[#LC4157]

- El cursor desaparece cuando se reproduce un vídeo en pantalla completa no vuelve a aparecer hasta que el vídeo deja de estar en pantalla completa.

[#LC4428]

- Puede producirse un error de segmentación cuando algunas aplicaciones externas publicadas generan un cuadro de diálogo. El cursor deja de verse si intenta reconectarse a la aplicación que se ha cerrado inesperadamente.

[#LC4955]

Receiver para Linux 13.3

Se han solucionado los problemas siguientes desde la versión 13.2:

[Sesión/Conexión](#)

[Experiencia de usuario](#)

[Excepciones del sistema](#)

[Interfaz de usuario](#)

Sesión/Conexión

- Después de restaurar una ventana integrada maximizada, algunas partes del escritorio no se actualizan automáticamente. Este problema solo se da en algunos entornos de escritorio, como Ubuntu 12.04 Unity 2D.

[#LC0602]

- Cuando se usa el parámetro "ProxyType=Secure", puede producirse un error de segmentación.

[#LC3396]

- Si intenta copiar contenido de una aplicación publicada y pegarlo en una aplicación local, es posible que el proceso del componente del motor ICA (wfica) se cierre inesperadamente por un error de segmentación.

[#LC3480]

- En algunas instancias, la lista de aplicaciones en caché puede quedar desincronizada.

[#556245]

Excepciones del sistema

- En algunos casos, la autenticación con tarjeta inteligente provoca un cierre inesperado de sesión.

[#582550]

Experiencia de usuario

- Con esta corrección, la información de la zona horaria de Rusia se puede actualizar para Receiver para Linux.

Para habilitar esta corrección:

- En XenApp 6.5, es necesario instalar como mínimo el Hotfix Rollup Pack 5 o alguno de los posteriores, para redirigir correctamente todas las zonas horarias.
- Para el VDA de sistema operativo de XenApp y XenDesktop 7.6 es necesario instalar la revisión hotfix ICATS760WX64014.
- Si el sistema operativo del servidor es Windows Server 2008 R2 Service Pack 1, debe instalarse la revisión hotfix de Microsoft KB2870165 en el servidor.
- Actualice los sistemas operativos del servidor y del dispositivo de usuario para aplicar la información de zona horaria más reciente.
- Debe instalar la revisión hotfix KB2998527 de Microsoft para Windows y después actualizar la información de zona horaria en Linux.

[#LC1971]

Interfaz de usuario

- Es posible que los iconos de las aplicaciones publicadas no se muestren correctamente en la barra de tareas.

[#LC3405]

- Es posible que los iconos de una sesión integrada no aparezcan en la barra de tareas cuando se usan plataformas ARM hard float (armhf).

[#LC4051]

- Se muestra un mensaje incorrecto de dependencia al iniciar selfservice después de instalar Citrix Receiver con el paquete de distribución tar.gz en Fedora 21.

[#582071]

Receiver para Linux 13.2

Se han solucionado los problemas siguientes desde la versión 13.1:

[HDX Plug and Play](#)

[Sesión/Conexión](#)

[Inicio de sesión/Autenticación](#)

[Experiencia de usuario](#)

[Administración de servidores/comunidades](#)

[Interfaz de usuario](#)

HDX Plug and Play

- Es posible que la cámara Web no funcione con Citrix GoToMeeting y Cisco WebEx cuando se utiliza HDX RealTime Optimization Pack (Linux) para Microsoft Lync 2010. Para habilitar esta corrección en su totalidad, debe instalar dos

revisiones hotfix: una de Receiver para Linux y otra de HDX RealTime Optimization Pack (Linux) para Microsoft Lync 2010 que incluya la corrección #LA0339.

Nota: Después de instalar esta corrección, si inicia Microsoft Lync en una sesión de agente VDA mientras se ejecute una conferencia de vídeo de Citrix GoToMeeting o Cisco WebEx, la cámara Web podría dejar de funcionar. Si esto sucede, detenga y reinicie la cámara desde la conferencia de vídeo.

[#LC0339]

Inicio de sesión/Autenticación

- Cuando los usuarios inician sesión con tarjeta inteligente mediante la interfaz de usuario Unicon, no pueden enumerar ni iniciar aplicaciones si la tarjeta inteligente contiene más de dos certificados y solo uno de ellos es un certificado de autenticación. Si la tarjeta inteligente contiene un certificado de cliente para la autenticación, los usuarios pueden enumerar e iniciar aplicaciones. Sin embargo, aparecerá siempre el siguiente mensaje de error: "Cert Client Authentication OID info set, but unexpected value:...".

[#LC2098]

Administración de servidores/comunidades

- Si las conexiones con Receiver para Linux se producen a través de una interfaz de red privada virtual (VPN), Receiver falla al iniciar una aplicación publicada.

[#LC1284]

- Si ejecuta el comando "ctx_rehash" para instalar un certificado raíz o intermedio en el dispositivo del usuario, es posible que no pueda crear el enlace o el algoritmo hash correctos y que aparezca el siguiente mensaje de error: "Error adding store:AM_ERROR_HTTP_SERVER_CERTIFICATE_NOT_TRUSTED[65150]". Cuando esto ocurre, Receiver no puede utilizar el certificado y fallan los intentos de agregar una tienda.

[#LC1513]

- Con esta corrección, si el usuario agrega una tienda (ya sea mediante el comando "\$ICAROOT/util/storebrowse --addstore , o bien mediante Self-service Plug-in) y el parámetro de "detección" no está incluido en la URL, ese parámetro se anexa a la URL de forma automática.

[#LC1517]

Sesión/Conexión

- Cuando se maximiza la ventana de una aplicación publicada de Microsoft Office en el modo integrado, la ventana se maximiza, pero su contenido se puede desplazar y es posible que los marcos izquierdos y superiores no se generen.

[#LC0118]

- En un entorno de varios monitores, si se gira el segundo monitor o este tiene otra resolución, al iniciar una aplicación publicada en el modo integrado y al maximizar luego la ventana, el servidor no muestra la ventana maximizada y la ventana no se puede usar.

Para habilitar esta corrección, abra el archivo \$HOME/.ICAClient/wfclient.ini y, en la sección [WFClient], agregue la entrada "TWIAvoidFullScreenWhenMaximized=True".

[#LC0354]

- En un entorno de varios monitores, si se maximiza y se restaura varias veces el tamaño de la ventana de una aplicación publicada en el modo integrado, es posible que, en ocasiones, aparezca un fondo de color gris en el segundo monitor en lugar de la ventana de la aplicación.

[#LC0355]

- En un entorno de varios monitores, es posible que, en el segundo monitor, no se pueda cambiar el tamaño de la ventana de una aplicación publicada en el modo integrado mientras se utilice el cambio de tamaño en el lado del cliente.

[#LC0356]

- Al cambiar entre dos sesiones de escritorio remoto (RDP) publicado en el modo de pantalla completa (por ejemplo, mstsc1 y mstsc2), la barra de conexión no se actualiza correctamente y muestra mstsc2 como la ventana principal incluso después de cambiar a mstsc1.

[#LC0437]

- Es posible que, al intentar iniciar una sesión mediante Receiver para Linux, la sesión se desconecte cuando se transfieran datos de forma continua mediante la redirección USB genérica de Citrix o la redirección de unidades del cliente.

[#LC0522]

- Al intentar iniciar sesión en la Interfaz Web mediante la dirección IP, puede darse un fallo de segmentación (segfault) y que pnbrowse se cierre inesperadamente.

[#LC0648]

- Cuando se cambia entre una aplicación publicada y Microsoft SQL Server 2012 Management Studio, si los usuarios maximizan ambas ventanas y luego solo minimizan la ventana de la aplicación publicada, la ventana de Microsoft SQL Server 2012 Management Studio no se genera correctamente y algunas partes de esa ventana no se actualizan.

[#LC0739]

- El foco de ventana permanece en la ventana principal en lugar de cambiar al cuadro de diálogo. Por ejemplo, al intentar cerrar un Bloc de notas publicado con contenido modificado, aparece un mensaje que solicita si quiere guardar el contenido. El cuadro de diálogo del mensaje no es la ventana activa.

[#LC0952]

- Receiver para Linux puede cerrarse inesperadamente al copiar una imagen desde una aplicación publicada a una aplicación local.

[#LC1017]

- Es posible que no pueda iniciar sesión mediante Receiver para Linux a través de Citrix NetScaler Gateway.

[#LC1103]

- Puede aparecer una ventana de error si un usuario abre una aplicación en una sesión de agente VDA que necesita la cámara Web si otra aplicación local ya la está utilizando.

[#LC1135]

- Al conectarse a un agente VDA de XenDesktop 5.6, si el dispositivo de usuario está conectado a dos monitores, es posible que exista un problema de presentación en el segundo monitor. Además, al maximizar la ventana en el segundo monitor, es posible que la ventana no se expanda por completo en la pantalla.

[#LC1148]

- Si una sesión se inicia o cambia de tamaño, es posible que el plug-in del búfer de fotogramas no borre la pantalla.

[#LC1515]

- Receiver falla si la URL de un servidor proxy automático se ha configurado en el dispositivo del usuario. Aparece el siguiente error de syslog en el Registro:

```
Ubuntu1204LTSi386 kernel: [xxxx.xxxxxx] wfica [xxxx] segfault at 2 ip bxxxxxxx sp bxxxxxxx error 4 in libproxy.so[bxxxxxxx+xxxx]
```

[#LC1584]

- Cuando la función de fiabilidad de la sesión está habilitada y se transfieren datos de forma continua a través del USB genérico de Citrix, es posible que la sesión existente se desconecte.

[#LC1588]

- Es posible que la versión de 64 bits de Receiver para Linux no registre el plug-in del explorador.

[#LC1712]

- En sistemas donde la corrección #LC1127 esté instalada, Receiver para Linux 13.1.3 puede dejar de responder al desconectarse de una sesión de escritorio que haya publicado XenDesktop.

[#LC2365]

- Cuando los usuarios inician sesión con Receiver para Linux e intentan pegar contenido dentro de un escritorio alojado publicado en XenApp 5.0, si hacen clic con el botón secundario y sitúan el puntero sobre la opción de pegado, la sesión se desconecta y se puede producir un error de segmentación de datos.

[#LC2467]

- Al conectarse con Receiver para Web, después de descargar un archivo de aprovisionamiento (.cr) de servicios StoreFront y, a continuación, ejecutar el comando de storebrowse `./util/storebrowse -C /tmp/receiverconfig.cr`, el diálogo "Add Service Record Add Store" no aparece y la tienda no se crea.

[#LC2669]

- Cuando se usa Receiver para Linux 13.1, si los usuarios hacen clic con el botón secundario en el icono que se encuentra en el área de notificaciones de Windows, la sesión de Receiver puede dejar de responder y las entradas de teclado o puntero pueden dejar de funcionar hasta que la sesión se haya cerrado y se haya vuelto a abrir.

[#LC2824]

Experiencia de usuario

- Es posible que aparezca un mensaje de error al desplazarse por un documento de gran tamaño en Receiver para Linux. Los usuarios deben responder al mensaje de error para continuar trabajando en la sesión.

[#LC1127]

- Si la resolución de pantalla original de un dispositivo de usuario cambia durante una sesión de Receiver, la sesión no conserva la configuración de pantalla completa. Como resultado, es posible que cambie el tamaño de la sesión, por lo que puede no coincidir con las resoluciones de pantalla actuales y originales.

[#LC1222]

- Si un nombre de icono contiene una barra invertida ("\"), es posible que los iconos de la aplicación no se muestren correctamente en Receiver para Linux.

[#LC1364]

- Es posible que no pueda copiar y pegar el contenido de aplicaciones Java en aplicaciones publicadas, o bien es posible que se pegue el contenido anterior del Portapapeles. El problema ocurre cuando Receiver para Linux no puede sincronizar el dispositivo del usuario con la información del Portapapeles que hay en el servidor.

[#LC1856]

- En un dispositivo ligero de Hewlett-Packard que usa el decodificador de hardware para gráficos H.264, en una sesión de agente VDA y después de iniciar una aplicación en la sesión, no se puede copiar y pegar texto en documentos abiertos. Además, no se puede copiar texto desde la ventana de una aplicación a la ventana de otra aplicación que se está ejecutando en un agente VDA.

[#LC2985]

Interfaz de usuario

- Si StoreFront está configurado con un grupo de agregación y si el nombre de la aplicación contiene una barra invertida ("\"), es posible que no se inicien las aplicaciones en Receiver para Linux. Aparece el siguiente mensaje de error:

"Archivo ICA dañado"

[#LC1268]

Receiver para Linux 13.1

Se han solucionado los problemas siguientes desde la versión 13.0:

[Redirección de Windows Media de HDX MediaStream](#)

[Remedo](#)

[Redirección de Flash de HDX MediaStream](#)

[Excepciones del sistema](#)

[Teclado](#)

[Otros problemas](#)

[Sesión/Conexión](#)

Redirección de Windows Media de HDX MediaStream

- Receiver para Linux 13.0 elige la salida Motion JPEG (MJPEG) para la cámara Web aunque esté disponible la salida YUYV.
[#LA5740]

Redirección de Flash de HDX MediaStream

- Cuando HDX MediaStream para Flash está habilitado, al recargar ciertos vídeos de Flash en Internet Explorer, la recarga puede fallar.
[#LA4345]
- Al reproducir un vídeo en YouTube, es posible que el sonido y el vídeo no se reproduzcan correctamente en Internet Explorer. Esto ocurre cuando los usuarios se conectan con Receiver para Linux y la redirección de Flash de HDX MediaStream está habilitada.
[#LA5833]
- Si la redirección de Flash está habilitada, la selección del control de tamaño del vídeo en YouTube puede hacer que la redirección de Flash recurra a la generación en el lado del servidor.
[#LA5834]

Teclado

- Al presionar combinaciones de teclas que incluyen las teclas Alt, Mayús o Ctrl, es posible que dichas teclas permanezcan en estado presionado en una sesión remota.
[#LA5730]
- Esta corrección se ocupa de este problema, que tiene lugar al interpretar el estado de la tecla Bloq Núm:
Al mover el puntero fuera de la ventana de una aplicación publicada y volverlo a mover dentro de ella, y a continuación presionar varias teclas del teclado numérico cuando la tecla Bloq Núm está presionada, la primera tecla presionada en el teclado numérico no aparece en la sesión.
[#LC0146]

Sesión/Conexión

- Cuando está habilitada la *redirección del portapapeles del cliente*, puede fallar el copiado y pegado de archivos en una sesión de cliente (usando, por ejemplo, el Explorador de Windows publicado en ventana integrada).
[#LA5254]
- Las ventanas de aplicaciones publicadas sin entrada en la barra de tareas no toman el foco de entrada a menos que exista otra ventana publicada para la misma aplicación.
[#LA5617]
- Al mover una ventana integrada, la ventana puede no dibujarse correctamente en algunos casos.
Para habilitar esta corrección, agregue la entrada "TWIRedrawAfterMove=TRUE" en la sección [WFClient] de cualquiera de los archivos ~/.ICAClient/wfclient.ini file o config/All_Regions.ini.

[#LA5669]

- Esta solución mejora la velocidad de la transferencia de archivos en entornos de baja latencia.

[#LA5725]

- Receiver para Linux 13.0 elige la salida Motion JPEG (MJPEG) para la cámara Web aunque esté disponible la salida YUYV.

[#LA5742]

- Las consultas DNS que devuelven varias respuestas para una única búsqueda, como sucede frecuentemente en una configuración round robin, pueden hacer que fallen los intentos de conexión segura y que Receiver se cierre inesperadamente.

[#LA5752]

- Al restaurar una ventana después de maximizarla en el servidor, la ventana local se restaura pero el contenido de la ventana no es correcto y hay un desplazamiento del puntero.

[#LA5926]

- Si mueve una ventana de aplicación publicada iniciada en modo integrado, el contenido de la ventana puede verse dañado. Para resolver este problema, lleve a cabo lo siguiente:
 - En el servidor, configure la directiva "Ver contenido de las ventanas al arrastrar" como "Prohibida".
 - En el dispositivo del usuario, en el archivo "\$HOME/wfclient.ini", busque la sección [WFClient] y agregue las entradas "TWICoordinateWinPosition=True" y "TWIRedrawAfterMove=True".

[#LA5935]

- La presentación en pantalla de sesiones en VDA 7.5 configuradas con una directiva de **Presentación visual** donde la **Calidad visual** tiene un valor distinto del predeterminado (calidad Media) puede dejar de responder desde el momento en que se inicia.

[#LC0043]

- El intento de conectar con aplicaciones o escritorios publicados a través de NetScaler Gateway puede fallar y puede aparecer un error similar al siguiente:

No se puede contactar con el servidor de la aplicación <>.

El comando del examinador de servidores contiene un parámetro que no es válido.

No puede resolverse el nombre del servidor.

Este problema ocurre en situaciones en que se ha configurado un Secure Ticket Authority adicional tanto en NetScaler Gateway como en StoreFront.

[#LC0059]

- Al intentar autenticarse en la Interfaz Web mediante un tíquet de Kerberos, es posible que se produzca un fallo de segmentación (segfault) y que pnbrowse se cierre inesperadamente.

[#LC0065]

- Al presionar Alt+Tab para navegar entre varias ventanas abiertas y traer al frente la ventana de inicio de sesión de

Escritorio remoto, la ventana no puede tomar el foco.

[#LC0069]

- Cuando el cursor se encuentra dentro de una ventana de aplicación, la acción Alt+Tab puede fallar al intentar traer la ventana al frente.

[#LC0070]

- Al arrastrar una ventana en un escritorio iniciado por Receiver para Linux puede quedar una sombra.

[#LA0128]

- Esa solución evita que aparezcan ocasionalmente unos mensajes de error inesperados e innecesarios, donde se indica que hay problemas de conectividad y se presenta a los usuarios las opciones Salir o Reintentar.

[#LC0129]

- El sonido por UDP puede fallar inesperadamente al cabo de unos momentos de iniciarse la sesión.

[#LC0137]

- Las sesiones de XenDesktop pueden dejar de responder al transferir datos sobre un puerto serie con Receiver para Linux.

[#LC0296]

- Cuando los usuarios conectan con Receiver para Linux y el cliente ligero HP t610 se ejecuta en un sistema operativo HP ThinPro 4.4, y la zona horaria es GMT +8 en las siguientes ubicaciones, aparece un mensaje de error similar a "No se reconoce la zona horaria actual":

- Singapur
- Brunéi
- Macasar
- Kuala Lumpur
- Kuching
- Manila

[#LC0299]

- Al cambiar entre Microsoft Word y la ventana del Cliente de Microsoft Terminal Services (MSTSC), el contenido que aparece en las ventanas puede estar dañado.

[#LC0308]

- El comando pnabrowse -WT no puede terminar una sesión de escritorio.

Para habilitar la solución, abra el archivo \$HOME/wfclient.ini y, en la sección [WFClient], agregue la entrada "LogoffDesktopThroTWI=True".

[#LC0345]

- No se puede interactuar con algunos campos desplegables al usar Receiver para Linux.

[#LC0365]

Remedo

- Si la resolución del cliente Linux se cambia y se inicia una aplicación publicada desde el servidor XenApp usando Receiver para Linux, es posible que el usuario que remeda no pueda actualizar su pantalla correctamente mientras la sesión está siendo remedada desde la consola de administración.

[#LA5165]

Excepciones del sistema

- Receiver para Linux puede fallar si habilita PersistentCacheSize.

[#LC0528]

Otros problemas

- Los paquetes tarball y RPM actuales no se pueden integrar con GStreamer en distribuciones recientes de Fedora, Red Hat y CentOS AMD (x86_64).

[#LA4212]

- Si se instala un certificado de infraestructura de clave pública (PKI) x.509 con ciertas restricciones de directiva en NetScaler Gateway, es posible que no puedan iniciarse aplicaciones con Receiver para Linux y aparezca un error 85 de SSL.

Para iniciar aplicaciones, hay que definir la clave siguiente en el archivo All_Regions.ini:

```
[Network\SSL]
```

```
EnableCertificatePolicyVerification=1
```

[#LA5609]

- Esta mejora de funcionalidad añade respaldo para certificados SHA-2 en Receiver para Linux.

[#LC0136]

Receiver para Linux 13.0

[Redirección de Windows Media de HDX MediaStream](#)

[Experiencia de usuario](#)

[Teclado](#)

[Interfaz de usuario](#)

[Sesión/Conexión](#)

[Otros problemas](#)

[Excepciones del sistema](#)

Redirección de Windows Media de HDX MediaStream

- Cuando HDX RealTime está habilitado, el proceso gst_read puede experimentar una pérdida lenta de memoria a lo largo de cierto tiempo, a medida que redirige datos de cámara Web.

[#LA1933]

Teclado

- Al conectar desde Receiver para Linux con un escritorio virtual de Windows 7, el mensaje "Bloq Mayús activado" en la página de inicio de sesión de Windows 7 puede no reflejar el estado preciso de la tecla Bloq Mayús en el cliente hasta que se presiona una tecla de carácter.

[#LA1784]

- Cuando se cambia de una aplicación local a una publicada y viceversa, la primera tecla que se presiona después de presionar Ctrl se ignora o puede aparecer otra tecla distinta de la presionada.

[#LA3397]

- **Importante:** La instalación de esta solución en sistemas donde está instalada la solución #LA1965 hace que #LA1965 deje de funcionar. No instale esta solución en sistemas donde instaló la solución #1965 y ésta es necesaria.

Las teclas de acceso rápido, como la combinación Alt+Tab, pueden no transferirse a la sesión y, en su lugar, se interpretan en el cliente.

De la descripción de la solución #LA1965:

Al conectar en modo no integrado, el usuario de Receiver para LINUX puede encontrar una pantalla gris destelleando (durante aproximadamente un segundo) antes de que aparezca la aplicación o escritorio publicados.

[#LA3660]

- Cuando una aplicación publicada está configurada para ejecutar una macro en una de las teclas LED (Bloq Mayús, Bloq Núm o Bloq Despl), al presionar la tecla puede suceder que la macro se ejecute varias veces.

Para habilitar esta solución, agregue la entrada "BypassSetLED=True" en la sección [WFClient] en el archivo wfclient.ini ubicado en la carpeta ~/.ICAClient. Si la carpeta ~/.ICAClient no está presente, modifique el archivo /opt/Citrix/ICAClient/nls/en/wfclient.ini en su lugar.

[#LA3825]

- Cuando se usa la versión en japonés de Receiver para Linux en una sesión de escritorio virtual, el estado de la tecla Bloq Mayús en la barra del editor IME puede ser incorrecto al presionar las teclas Mayús+Eisu.

[#LA4072]

- Cuando se usa Receiver para Linux en una sesión de escritorio virtual con el editor IME para japonés instalado y seleccionado en el VDA, el estado de la tecla Bloq Mayús en la barra del IME puede no coincidir con su estado en el punto final mientras se presiona las teclas Mayús+Eisu.

[#LA4422]

Sesión/Conexión

- En un entorno de varios monitores, Receiver para Linux puede configurar incorrectamente el tamaño de una ventana maximizada en un segundo monitor. Como resultado, el tamaño de la ventana puede ser mayor que el tamaño del monitor.

[#LA0663]

- Cuando se inicia IBM Lotus Notes con cualquier otra aplicación publicada (por ejemplo, Microsoft Excel) dentro de una sesión y se intenta abrir un archivo adjunto, puede suceder que la ventana del adjunto se actualice incorrectamente y aparezca por encima de las otras ventanas. Esto puede provocar que otras ventanas aparezcan como rectángulos negros o de otro color de fondo.

[#LA1490]

- Cuando la redirección de la zona horaria está habilitada, la hora mostrada y aplicada en la sesión puede corresponder a la hora correcta, según lo previsto. Sin embargo, al abrir Fecha y hora en el Panel de control, aparece el siguiente mensaje de error:

"No se reconoce la zona horaria actual. Seleccione una zona horaria válida mediante el vínculo siguiente".

[#LA1828]

- En sistemas donde está instalado el administrador de ventanas IceWM, el comando **-span o** no puede abarcar la sesión entre dos monitores. En su lugar, la sesión se muestra solo en uno de ellos.

[#LA2178]

- Al intentar abrir un archivo cuyo nombre contiene el símbolo Yen 5C (codificado con Shift-JIS) desde un dispositivo USB asignado en el lado del cliente, la operación puede fallar.

[#LA2183]

- Esta solución amplía el parámetro SucConnTimeout (<http://support.citrix.com/proddocs/topic/ica-settings/ica-settings-succonntimeout.html>) de modo que lo apliquen no solo las aplicaciones publicadas, sino también los escritorios publicados. Como resultado, cuando se abren varios escritorios, estos esperan durante los segundos especificados en SucConnTimeout antes de iniciarse.

Para modificar el valor de SucConnTimeout:

Edite la sección [WFClient] del archivo ~/.ICAClient/wfclient.ini de este modo:

```
[WFClient]
```

```
Version=2
```

```
SucConnTimeout=60
```

```
KeyboardLayout=(User Profile)
```

```
KeyboardMappingFile=automatic.kbd
```

```
KeyboardDescription=Automatic (User Profile)
```

Si la carpeta ~/.ICAClient/ no está presente en el directorio home del usuario, modifique el archivo /opt/Citrix/ICAClient/nls/en/wfclient.ini como se muestra más arriba. El archivo se copiará en la carpeta ~/.ICAClient cuando el usuario se conecte por primera vez. También puede agregar ApplySucConnTimeoutToDesktops=True a la misma sección que SucConnTimeout, si es necesario.

[#LA2679]

- Los intentos de iniciar una aplicación publicada desde Receiver para Linux usando credenciales de dominio con Centrif

pueden fallar.

[#LA3270]

- Esta mejora permite que Receiver para Linux lea y escriba en archivos ubicados en unidades asignadas del cliente que usan un sistema de archivos XFS.

[#LA3610]

- Cuando se cambia de un espacio de trabajo A a un espacio de trabajo B y de vuelta al espacio de trabajo A, el foco no se restaura en la última ventana que tenía el foco en ese espacio de trabajo.

Nota: Esta solución resuelve el problema entornos de escritorio KDE, Xfce y Gnome. No funciona para escritorios Unity.

[#LA3432]

- El uso de pnbrowse en un entorno donde hay varios dominios puede fallar si se usa un dominio alternativo para la autenticación de usuario. Este problema ocurre porque la implementación del código original separa el nombre de usuario del dominio. Como resultado, el uso de pnbrowse con un dominio alternativo no funciona.

Por ejemplo, se puede hacer referencia a un usuario como usuario1@esta.empresa o como usuario1@esta.local (donde el dominio principal es *esta.empresa* y el dominio alternativo es *esta.local*). Con esta solución, las dos opciones siguientes funcionarán:

```
> ./pnbrowse -L desk -U user1 -D this.company -P company123
```

```
> ./pnbrowse -L desk -U user1@this.local -P company123
```

[#LA3551]

- Los canales virtuales personalizados pueden no inicializarse después de una reconexión automática de Receiver para LINUX.

[#LA3572]

- Incluso aunque esté habilitada la opción "Mover automáticamente el puntero al botón predeterminado en un cuadro de diálogo" en el servidor (la función que lleva el puntero del Mouse al botón predeterminado en un cuadro de diálogo que está abierto), esta característica puede no funcionar dentro de una aplicación publicada usando Receiver para Linux.

[#LA4285]

- El borde derecho y la parte inferior de ciertas ventanas de aplicaciones de Java (por ejemplo, jEdit) en modo integrado pueden no redibujarse correctamente cuando se mueven o se restauran.

Para habilitar la solución, agregue la entrada "TWISetFocusBeforeRestore=True" en la sección [WFClient] del archivo \$HOME/.ICAClient/wfclient.ini.

[#LA4450]

- La redirección de dispositivos USB puede ser lenta en Receiver para Linux en implementaciones con NetScaler.

[#LA4549]

- Cuando se arrastra una ventana de una aplicación publicada (por ejemplo, Token 2) desde cualquier lugar menos su barra de título, la ventana de la aplicación integrada puede minimizarse.

Para habilitar esta solución, agregue la entrada "TWIMoveResizeHideWindowType=2" en la sección [WFClient] del archivo wfclient.ini.

[#LA4737]

Excepciones del sistema

- Cuando se define CommPollSize=On en module.ini esto puede provocar que el proceso wfica.exe se cierre inesperadamente.

[#LA2155]

- Los intentos de imprimir desde una aplicación basada en Java en un escritorio publicado pueden hacer que Receiver para Linux se cierre inesperadamente.

[#LA3321]

- Receiver puede cerrarse inesperadamente al pegar una gran cantidad de datos desde el portapapeles.

[#LA3608]

- Receiver puede cerrarse inesperadamente. Este problema puede ocurrir cuando una aplicación publicada contiene más de 50 caracteres en chino en la barra de título.

[#LA4119]

Experiencia de usuario

- Si presiona la tecla ALT mientras arrastra la ventana de una aplicación publicada desde cualquier lugar menos su barra de título, el contenido de la ventana no se mueve al unísono que el contorno de la misma. Además, cuando se suelta el botón del Mouse, el movimiento de arrastre que se acaba de hacer se repite.

[#LA0837]

- El puntero del Mouse puede colocarse en una ubicación incorrecta al maximizar la ventana del monitor secundario. Los menús y los botones pueden activarse incorrectamente al mantener el Mouse sobre ellos. El problema ocurre cuando el monitor secundario tiene una resolución de píxeles vertical menor que la del monitor principal.

Por ejemplo: el monitor 1 tiene una resolución de 1920x1080 y el monitor 2 tiene 1280x1024 píxeles. Cuando se inicia una aplicación publicada en el monitor 1 y luego se arrastra la aplicación al monitor 2 y se maximiza, el puntero del Mouse puede quedar colocado a una distancia de aproximadamente un centímetro del botón de destino. Como resultado de ello, puede aparecer un cuadro de información emergente para el botón Maximizar cuando el puntero se encuentra a una distancia de un centímetro del botón.

[#LA2071]

- Cuando se cierra un menú emergente relativo a un icono del área de notificación de una aplicación publicada integrada, el área del menú emergente no se redibuja correctamente y una parte del contenido del menú permanece visible.

[#LA4139]

Interfaz de usuario

- Esta mejora en la utilidad pnbrowse permite mostrar iconos de mayor resolución para los recursos publicados.

[#LA1994]

- Cuando se expande un menú desplegable en una aplicación publicada, puede aparecer una entrada en la barra de tareas con el nombre "Ventana sin título".

[#LA3422]

Otros problemas

- Esto es una mejora que permite limitar la redirección USB desde un cliente especificado basándose en el usuario. Para limitar la redirección de USB para un usuario concreto, ejecute los comandos siguientes en el cliente como usuario root o administrador:

1. Quite el bit setuid del binario ctxusb:

```
# chmod u-s /opt/Citrix/ICAClient/ctxusb
```

2. Inserte un dispositivo USB y busque el dispositivo en el sistema de archivos usando:

```
# ls -lR /dev/bus/usb
```

3. Asigne permisos de usuario (por ejemplo, al usuario1), donde /dev/bus/usb/001/041 está determinado como el dispositivo USB del paso 2:

```
# chown user1 /dev/bus/usb/001/041
```

[#LA1952]

- La integración de GStreamer (una aplicación de terceros) con Citrix Receiver puede fallar para la versión 12.04 de Ubuntu.

[#LA2016]

- En sistemas de 64 bits (como, por ejemplo, la distribución de Ubuntu de 64 bits), el script hdxcheck.sh no puede ubicar la versión de 32 bits de las bibliotecas siguientes: libpcsc-lite.so, libcrypto.so, libjpeg.so, libdapsdk.so, y libcap.so, lo que provoca la aparición de estos mensajes de advertencia:

"Warning! - libpcsc-lite.so missing, check that the file exists. (Advertencia: No se puede encontrar la librería libpcsc-lite.so. Compruebe que existe el archivo.)

Warning! - libcrypto.so is not installed. This is required if you use NTLM proxies. (Advertencia: La librería libcrypto.so no está instalada. Es necesaria si utiliza servidores proxy NTLM.)

Warning! - libjpeg.so is not installed! This is needed for SpeedScreen Image and Browser Acceleration. (Advertencia: La librería libjpeg.so no está instalada. Es necesaria para la aceleración de explorador e imagen SpeedScreen.)

Warning! - libdapsdk.so is not installed! This is only needed if you use Novell Netware Services.

A compatible version of libcap could not be located!" (Advertencia: La librería libdapsdk.so no está instalada. Es necesaria solamente si utiliza los servicios Novell Netware. No se ha podido encontrar ninguna versión compatible de libcap.)

El problema ocurre porque el script intenta buscar esas bibliotecas solo en /user/lib. En las distribuciones de Linux de 64 bits, las versiones de 32 bits de esas bibliotecas pueden estar instaladas en /usr/lib/i386-linux-gnu o en /lib/i386-linux-gnu/. Con esta solución, el script también intenta buscar las bibliotecas en /lib. Si la búsqueda tiene éxito, aparecen los mensajes siguientes, en lugar de los mensajes de advertencia:

"Success! - Libpcsc-lite.so installed. Smartcard support enabled. (La librería Libpcsc-lite.so se ha instalado correctamente. Se ha habilitado el respaldo a las tarjetas inteligentes.)

Success! All OS dependencies found! (Se han encontrado todas las dependencias de SO.)
A compatible version of libcap is installed!" (Se ha instalado una versión compatible de libcap.)

[#LA2204]

- Esta mejora introduce respaldo para el marco multimedia Open Source playbin2 en HP T510. Para habilitar el respaldo para playbin2, debe configurar estas opciones en el archivo All_Regions.ini:

```
SpeedScreenMMAClosePlayerOnEOS=True  
SpeedScreenMMAEnablePlaybin2=True
```

[#LA2566]

- Esta solución se ocupa de una serie de problemas encontrados con la solución #LA2566, una mejora que introduce respaldo para el marco multimedia Open Source playbin2 en HP T510.

[#LA2757]

Problemas conocidos de Citrix Receiver para Linux 13.5

Jul 07, 2017

Problemas conocidos en Citrix Receiver para Linux 13.5

Se han observado los siguientes problemas conocidos en esta versión:

- La URL de StoreFront no se agrega si Citrix Receiver para Linux se instala en una ruta personalizada localizada que contiene uno o varios caracteres de 4 bytes.

[RFLNX-613]

- Con la redirección de Windows Media de HDX MediaStream con GStreamer 1.0 habilitado, OpenGL puede provocar la aparición inesperada de ventanas emergentes en algunas plataformas.

[RFLNX 949]

- Con la redirección de Windows Media de HDX MediaStream con GStreamer 1.4 o posterior habilitado, en el modo de obtención de contenido en el servidor, algunos archivos multimedia (del tipo MPG1, MPEG2 y H264) no se reproducen.

[RFLNX-952]

- En un dispositivo con escalado de frecuencia de CPU (como Raspberry Pi), si tiene cortes de sonido intermitentes o problemas de rendimiento general, Citrix recomienda establecer el regulador de escalado al modo de rendimiento. Para ver el regulador de rendimiento actual que tiene cada núcleo, ejecute el siguiente comando, donde es el núcleo:

```
cat /sys/devices/system/cpu/cpu/cpufreq/scaling_governor
```

De forma predeterminada, esta configuración es a petición, y no es siempre lo suficientemente dinámica como para proporcionar el rendimiento necesario en tiempo real.

Para establecer el regulador de escalado al modo de rendimiento, ejecute el siguiente comando como superusuario:

```
echo performance > /sys/devices/system/cpu/cpu/cpufreq/scaling_governor
```

Repita este comando para cada núcleo .

[RFLNX-1003]

- El plugin del decodificador H264 de hardware acelerado para HDX Ready Pi no funciona correctamente si se cambia la resolución del búfer de fotogramas con los parámetros `framebuffer_width` y `framebuffer_height` en el archivo `/boot/config.txt`. Como solución temporal, cambie la resolución de Pi con los parámetros `hdmi_group` y `hdmi_mode`.

[RFLNX-1049]

Problemas conocidos en Citrix Receiver para Linux 13.4

Se han observado los siguientes problemas conocidos en esta versión:

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

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

[#634855]

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

[#648716]

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

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

[#652810]

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

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

[#653550]

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

[#654826]

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

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

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

Problemas conocidos en Citrix Receiver para Linux 13.3

Se han observado los siguientes problemas conocidos en esta versión:

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

[#491235]

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

[#553886]

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

[#556899]

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

[#558641]

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

[#558653]

- Para cambiar SharedUserMode mediante storebrowse, -c SharedUserMode[=value], se necesita que el valor coincida en mayúsculas y minúsculas. Cuando se usa el parámetro de valor de storebrowse, -c SharedUserMode[=value], hay que especificar un valor que coincida en mayúsculas y minúsculas con "True" o "False". No se ve ningún mensaje de error cuando se introduce un valor que no es válido. Por ejemplo: -c SharedUserMode=True.

[#559402]

- Al conectarse a un servidor de terminales (por ejemplo, RDS) solo con el protocolo SSL 3 habilitado, la conexión falla, como es de esperar, pero puede que no falle con un error de contacto inicial (handshake) con el homólogo SSL.

[#567407]

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

[#568556]

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

[#569806]

- Los nuevos valores para TLS no se aplican para conexiones con el servidor StoreFront que usen selfservice/storebrowse, cuando los valores de TLS se cambian después de haber aceptado el contrato de licencia de usuario final (EULA). Tenga en cuenta que un AuthManager en ejecución no lee un parámetro de TLS modificado.

[#570725]

- La Central de conexiones no admite IPv6.

[#571743]

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

[#575474]

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

[#580753]

- El plugin de explorador ARMEL no funciona en esta versión.

[#588044]

- Si observa que hay problemas con las zonas horarias que no se asignan correctamente a sesiones de XenApp o XenDesktop 7.6, compruebe que tiene instalada la revisión hotfix a la que se hace referencia en el artículo [CTX142640](#), y siga los pasos de la entrada 7 [De ICATS760WX64014]. Si eso no resuelve el problema, intente cambiar /etc/timezone (o /etc/localtime si /etc/timezone no existe) para que sea un vínculo simbólico a un nombre de ciudad de /usr/share/zoneinfo/...

Si su zona horaria sigue sin ser admitida, puede que necesite abrir un tiquet de asistencia para que se le agregue una asignación al servidor.

[#LC1061, #606648]

- En el SDK de optimización de plataforma, los plug-ins para entornos distintos de X11 presentan dos problemas:
 - Las sesiones en servidores Windows para XenDesktop 7.x fallan si se usa fiabilidad de la sesión.
 - Las sesiones con una profundidad de color de 16 bits muestran vídeo defectuoso.

Estos problemas existen tanto en la implementación SDL_plugin basada en bibliotecas SDL como en la implementación FB_plugin de Raw Kernel basada en Framebuffer. Los mismos problemas pueden ocurrir en cualquier otro plug-in desarrollado por el usuario.

Problemas conocidos en Citrix Receiver para Linux 13.2.1

Se han observado los siguientes problemas conocidos en esta versión:

- El plugin para explorador ARMEL (utilizado para iniciar sesiones desde un explorador Web) no se inicia, lo que impide que el usuario pueda abrir una sesión. Para resolverlo, inhabilite el plugin desde los parámetros del explorador Web, lo que permitirá que se recurra al mecanismo alternativo.

[#580782]

- Cuando se ejecuta en SLED 11sp3, al iniciar storebrowse o selfservice desde un terminal pueden producirse errores en varios programas, con mensajes similares a: “libidn.so.11: no version information available”. Este problema afecta muy poco al comportamiento de Citrix Receiver, si es que afecta.

[#582512]

- La redirección de Flash no está disponible en clientes de 64 bits. Si esta funcionalidad es importante para su entorno, póngase en contacto con el equipo de Product Management de Citrix o use los foros de asistencia de Citrix para obtener ayuda.

[#582627]

- Receiver no agrega las aplicaciones favoritas cuando se selecciona Agregar a favoritos en la vista Detalles. Este problema se produce cuando se ejecuta SUSE SLED 11sp3 sin instalar las actualizaciones. Para evitar este problema, el paquete libwebkit-1_0-2 debe ser de la versión 1.2.7-0.17.1 (o posterior).

[#585295]

- Se produce un problema de terceros en EPEL 2.2.4 de libwebkitgtk+. Citrix recomienda usar el repositorio EPEL (Extra Packages for Enterprise Linux) como método para obtener la versión GTK+2 de libwebkitgtk en RedHat 7 y CentOS 7. No obstante, se produce un problema con la versión de EPEL suministrada cuando se usan caracteres de idioma japonés o chino en los nombres de aplicaciones publicadas en el servidor. Como resultado de ello, Receiver no puede asegurar un método seguro para obtener una compilación de libwebkitgtk estable en RedHat 7 y CentOS 7 adecuada para caracteres de idiomas asiáticos.

[#586967]

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

[#587640]

- En algunos entornos de escritorio Gnome, un cliente puede experimentar un bloqueo del sistema al iniciar la aplicación de Escritorio remoto de Microsoft (Mstsc). Este problema se produce después de conectarse a un escritorio remoto. Después de introducir las credenciales de inicio de sesión, la sesión no se puede cerrar correctamente haciendo clic en el símbolo 'X' (aparece un error que indica que ha ocurrido un problema y el sistema no puede recuperarse del mismo.)

[#587922]

- El Reproductor de Windows Media muestra un mensaje de error donde indica que encontró un problema al reproducir el archivo. Esta condición de error se puede descartar cerrando el cuadro de mensaje y haciendo clic en el icono Reproducir.

[#588009]

- El Reproductor de Windows Media en un escritorio Windows 7 puede no reproducir sonido ni vídeo cuando se inicia desde un Receiver de 64 bits. Este problema ocurre debido a un problema conocido con Ubuntu 14.04; los componentes de GStreamer necesarios no se instalan como sería de esperar. Consulte la sección "El Reproductor de Windows Media no puede reproducir archivos de ciertos formatos" en el artículo [Solución de problemas](#).

[#588298]

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

Problemas conocidos en Citrix Receiver para Linux 13.2

Se han observado los siguientes problemas conocidos en esta versión:

- Se ha agregado un nuevo script que crea asociaciones de tipo de archivo entre cliente y servidor. Este script, `ctx_app_bind`, permite usar una aplicación publicada para abrir un tipo de archivo concreto. Este script acepta el nombre de la aplicación publicada, o un archivo de ejemplo o un tipo MIME, y da la opción de incluir un nombre o URL de servidor. Por ejemplo:

```
ctx_app_bind example_file published_app_name server
ctx_app_bind application/some-mime-name published_app_name
```

Use la opción `-p` para usar `pnbrowse` en lugar de `storebrowse` para el inicio de sesión.

Nota: Citrix recomienda ejecutar este script con cuidado. No se ha probado en todos los entornos posibles de sistema operativo.

[#558649]

- Si un usuario no puede conectar con la tienda, puede habilitar la captura de registros de conexión en Receiver para averiguar el origen del problema. Para habilitar la captura de registros de conexión en Receiver:

1. Edite el archivo `/opt/citrix/ICAclient/config/AuthManConfig.xml` con los parámetros siguientes utilizando una cuenta de usuario con privilegios de administrador:

```
TracingEnabled
true
```

```
LoggingMode
verbose
```

2. Detenga los procesos siguientes: `AuthManagerDaemon`, `selfservice`, `ServiceRecord`, `storebrowse`.
3. Inicie Receiver y conéctese a la tienda.
4. Revise los registros creados en `$HOME/.ICAclient/logs`.

La compresión de vídeo de cámara Web HDX RealTime requiere:

- Una cámara Web compatible de Video4Linux

- GStreamer 0.10.25 (o una versión 0.10.x posterior), incluido el paquete "plugins-good" de la distribución

[#559817]

- Cuando se utiliza Linux Receiver X1 para quitar una aplicación, la aplicación sigue presente al cerrar la sesión y volver a la tienda.

[#561719]

Problemas conocidos en Citrix Receiver para Linux 13.1

Se han observado los siguientes problemas conocidos en esta versión:

- 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]

- Aparece un error si un usuario abre la IU de autosevicio para conectarse a la tienda de StoreFront y, a continuación, cierra la ventana de Receiver para Linux cuando el cuadro de diálogo de Authentication Manager está abierto.

[#430193]

- Receiver para Linux no permite conexiones a una tienda de StoreFront que no sea segura (http://). Según la configuración de la tienda, 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]

- 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. Una prueba de ejemplo podría ser:

```
pkcs11-tool --module /usr/lib/libgtop11dotnet.so -
```

Si esto también resulta en un error de segmentación, debe ponerse en contacto con el proveedor del controlador. También puede probar un controlador de otra fuente 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]

- Si inserta una tarjeta inteligente errónea al intentar conectarse a la tienda de StoreFront, es posible que vea un mensaje de error del tipo "Error de protocolo" o "Tienda especificada no encontrada", con lo que el problema no se explica.

[#496904]

- 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]

- 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]

- Una revisión hotfix para 12.1 agregó el código de salida pnbrowse 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. Sin embargo, los valores indicados por pnbrowse -erno siguen mostrando significados sin corregir para los valores que van del 220 al 240.

[#502550]

Problemas conocidos en Citrix Receiver para Linux 13

Se han observado los siguientes problemas conocidos en esta versión:

Problemas en la instalación

- libxerces-c 3.1 es un componente necesario para esta versión. Sin embargo, no está disponible en algunas de las distribuciones de Linux que usan paquetes RPM. Si este componente no está en su distribución, búsquelo en un sitio Web apropiado y agréguelo a su instalación de Linux.

[#384324]

- Para las plataformas que no cumplen alguno o ninguno de los requisitos de sistema relacionados con libxerces o libwebkitgtk, puede instalar Receiver con el paquete tarball. También puede forzar la instalación de los paquetes Debian o RPM, y usar Receiver para Web, basado en explorador Web, para iniciar las conexiones. Por ejemplo, no se puede instalar el paquete RPM en sistemas CentOS porque se necesita libwebkitgtk-1.0.so.0, que no está disponible en dichos entornos. Para solucionar este problema, instale el paquete con --nodeps o --force, o use el paquete Tarball en su lugar. A continuación, inicie un explorador Web e introduzca la URL correspondiente a la tienda de Receiver para Web.

[#426176]

- Puede usar el paquete RPM para instalar Receiver en la versión de 32 bits de OpenSUSE 13.1, pero el programa falla al intentar ejecutarlo. Como solución temporal, descargue e instale primero el paquete RPM siguiente y repita la instalación: <ftp://rpmfind.net/linux/opensuse/factory/repo/oss/suse/i586/libpng12-0-1.2.50-7.3.i586.rpm>.

[#429879]

- Después de instalar Receiver desde el paquete RPM de 64 bits en un entorno Fedora 19.1 de 64 bits, hay que llevar a cabo una serie de pasos adicionales antes de usar pnbrowse o el motor del cliente, wfica, para iniciar conexiones. (Estos pasos corrigen storebrowse y selfservice, que no pueden funcionar debido a limitaciones en la versión de curl en este entorno.) Para solucionar este problema:

1. Instale el paquete libpng12 de 32 bits con este comando:

```
yum install libpng12.i686
```

2. Para minimizar la cantidad de errores de sonido, instale el plug-in de ALSA de 32 bits con este comando:

```
yum install alsa-plugins-pulseaudio.i686
```

3. Para minimizar la cantidad de errores de GtK, instale los siguientes paquetes con los comandos siguientes:

```
yum install adwaita-gtk2-theme.i686
yum install PackageKit-gtk3-module.i686
yum install libcanberra-gtk2.i686
```

4. Para permitir el inicio de conexiones desde Firefox, instale el plug-in nspluginwrapper.i686 y regístrelo en el explorador Web con estos comandos:

```
yum install nspluginwrapper.i686
mozilla-plugin-config
```

[#429886]

Problemas generales

- Cuando se reanuda la reproducción de sonido puede haber ruido. El ruido se produce solo cuando el sonido se pone en pausa y luego se reinicia, no cuando se reproduce por primera vez. Esto se ha observado en conexiones de XenDesktop que usan la característica de acceso con Remote PC. No existe ninguna solución para este problema.

[#308772]

- Algunos tipos de medios solo pueden reproducirse en el dispositivo de usuario si el códec adecuado está disponible en el servidor, incluso aunque GStreamer debería poder conectarse directamente al origen de los medios y reproducirlos con los decodificadores del dispositivo. No existe ninguna solución para este problema.

[#339394]

- En Ubuntu 12.04 con el escritorio Gnome 3, los iconos de las aplicaciones publicadas situados en el área de notificaciones no se integran con el escritorio nativo. En su lugar, aparecen en una ventana aparte del área de notificación. No existe ninguna solución para este problema.

[#395140]

- Los usuarios de Linux no pueden usar sus direcciones de correo electrónico para configurar las tiendas de StoreFront. En su lugar, los usuarios deben agregar la URL de las tiendas requeridas desde la página Cuentas del cuadro de diálogo Preferencias. También puede proporcionar un archivo de aprovisionamiento con la información de la cuenta que se usa para crear una cuenta nueva.

[#395394]

- 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]

- La redirección de contenido de cliente a servidor (colocar contenido publicado sobre un icono del escritorio) no funciona con la interfaz de usuario de autoservicio. No existe ninguna solución para este problema.

[#403739]

- El módulo de seguridad de Linux con Seguridad Mejorada (SELinux - Security-Enhanced Linux) en Fedora de RedHat 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.

[#413554]

- La característica de Redirección de Flash de HDX MediaStream no ha sido probada en la plataforma ARM Hard Float (armhf) porque, en esta versión, Receiver no funciona con los plugins de Flash en esa plataforma.

[#414253]

- Si configura una velocidad de fotogramas que no es compatible con la cámara Web, la cámara usará un valor diferente predeterminado, que puede ser mayor de lo esperado.

[#414576]

- Si en Receiver se configura una resolución no predeterminada para una cámara Web, no se podrá realizar secuencia de vídeo la primera vez que se use con Citrix GoToMeeting. La cámara Web parece estar activa y `gst_read` se está ejecutando, pero no hay imagen. Para solucionar este problema, detenga y reinicie la cámara Web en GoToMeeting.

[#414878]

- Si no hay decoraciones de ventana en el entorno de escritorio (por ejemplo, en un entorno LXDE con las decoraciones inhabilitadas), puede que no sea posible cerrar los cuadros de diálogo de autoservicio.

[#416689]

- Con algunas versiones de XenApp o XenDesktop, después de iniciar un escritorio o una aplicación, no se puede comprobar el nombre de servidor usado en la conexión porque no aparece ningún servidor listado en la Central de conexiones. Para solucionar este problema, haga clic en Propiedades. El nombre del servidor se muestra en el cuadro de diálogo Propiedades.

[#417114]

- Si al iniciar una sesión en Receiver, se introducen las credenciales después de una demora de unos cinco minutos, la interfaz de usuario de autoservicio no muestra las aplicaciones. Para solucionar este problema, seleccione "Actualizar aplicaciones" desde el menú desplegable en la interfaz de usuario y vuelva a escribir sus credenciales.

[#417564]

- Un administrador que remeda una sesión de un usuario puede notar errores de presentación si su pantalla es más pequeña que la del dispositivo del usuario. Por ejemplo, es posible que las barras de desplazamiento no quepan en la pantalla del administrador y que algunas áreas de la pantalla del usuario no sean accesibles. No existe ninguna solución para este problema. Además, si se cambia el tamaño de la sesión remedada desde la máquina del administrador se puede bloquear la sesión en el dispositivo de usuario. Para solucionar este problema, haga clic en el botón Restaurar en la ventana de sesión en la máquina del administrador (no en el dispositivo de usuario).

[#418672, #418690]

- La interfaz de usuario de autosevicio y los componentes de StoreFront asociados (Authentication Manager y el demonio Service Record) no están respaldados para Fedora debido a incompatibilidades entre las bibliotecas. Receiver se instala sin errores, pero no funciona después de la instalación. Para solucionar este problema, inicie Receiver a través de la Interfaz Web (un componente antiguo) o a través de Receiver para Web.

[#419662]

- Si se ha suscrito a muchas aplicaciones o escritorios, la interfaz de usuario de autosevicio incluye una barra de desplazamiento. Esta desaparece (como se espera) cuando la interfaz de usuario cambia de tamaño para mostrar todos los iconos de aplicaciones y escritorios. No obstante, la barra de desplazamiento no vuelve a mostrarse si a continuación se reduce el tamaño de la interfaz de usuario. Este problema se ha observado solo en Ubuntu 13.04. Para solucionar el problema, haga clic en la opción de menú Actualizar, repita la operación de cambio de tamaño unas cuantas veces, o bien, detenga y reinicie Receiver.

[#422520]

- La primera vez que se establece una conexión, se pueden notar demoras que varían considerablemente en función de la red. Es probable que una conexión mediante 3G sea más lenta que la conexión con ADSL.

[#423663]

- Al introducir una dirección HTTPS de tienda en la interfaz de usuario de autosevicio, se muestra el siguiente mensaje de error si no hay ningún certificado: "Su cuenta no puede agregarse usando esta dirección de servidor. Compruebe que la ha introducido correctamente". Este error se muestra aunque la dirección sea correcta cuando no hay ningún certificado presente. Para solucionar este problema, instale un certificado.

[#423757, #424674]

- Puede aplicar una directiva de XenDesktop para incrementar la velocidad de fotogramas máxima en sesiones de Receiver por encima de 30 fotogramas por segundo (FPS). No obstante, este valor no se cumple y la velocidad de fotogramas de las sesiones nunca excede este valor porque está limitado por la función de control de flujo. Este problema se ha observado en XenDesktop 7 y 7.1. Para solucionar este problema, inhabilite el control de flujo.

[#423950]

- Para cambiar de cuenta (y acceder a escritorios y aplicaciones desde otra tienda), utilice el menú Cuentas en la interfaz de usuario de autosevicio. Esto puede no ser obvio para los usuarios.

[#424027]

- Si usa storebrowse en varias configuraciones regionales que no están codificadas como UTF-8, parte del texto en el cuadro de diálogo de inicio de sesión puede estar dañado. Por ejemplo, en la configuración regional de español no hay texto en el botón Iniciar sesión. Para solucionar este problema, cambie a una configuración regional UTF-8 (por ejemplo, mediante la creación de un script contenedor de storebrowse y los ejecutables de demonio de Service Record y Authentication Manager).

[#424052]

- 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.

[#424847]

- Cuando se usa storebrowse para iniciar una sesión en un escritorio virtual de un grupo en el que todos los escritorios están apagados, se muestra un valor de estado de salida de 255 EXEC_FAILED (a veces se muestra después de cierta demora). Esto indica que el inicio ha fallado. No obstante, en lugar de un error, el escritorio está en realidad iniciándose o registrándose y estará disponible en breve. Para solucionar este problema, indique a los usuarios que intenten iniciar de nuevo el escritorio, o asegúrese de que el script de inicio lo haga.

[#425076, #425103]

- En las versiones de Receiver en japonés y en chino simplificado, los accesos directos de teclado no funcionan en algunos cuadros de diálogo.

[#425275, #425278, #425281, #425332]

- En las versiones de Receiver en alemán, francés y español ejecutadas en la plataforma Ubuntu, los accesos directos de teclado no se ven en algunos cuadros de diálogo, pero funcionan.

[#425282, #425285, #425289, #425294, #425339]

- En la versión de Receiver en alemán, hay accesos directos de teclado duplicados en algunos cuadros de diálogo.

[#425284, #425338]

- La herramienta de openssl c_rehash se usa para importar y aplicar hash en los certificados raíz que se usan para proteger las comunicaciones con StoreFront. Algunas versiones de c_rehash no manipulan correctamente los certificados que contienen finales de línea MS-DOS. Si la salida de c_rehash no genera los vínculos simbólicos para el certificado, es posible que tenga que convertir los finales de línea al formato UNIX. Puede hacerlo mediante la siguiente línea de comando:

```
tr -d '\r' < root_certificate_name.pem > new_root_certificate_name.pem
```

A continuación, ejecute el script de `c_rehash` en el nuevo certificado raíz creado a partir de este comando.

[#425775]

- En las plataformas Debian, el demonio `ctxusbd` no se reinicia cuando el sistema se reinicia, lo que provoca un fallo en la redirección USB. Esto se debe a que el script `init`, `/etc/init.d/ctxusbd`, contiene una variable, `###INIT_UDEV###`, que debe expandirse como `udev`. Como solución temporal, edite `/etc/init.d/ctxusbd` de este modo. Debe tener permisos de root para ello:

```
sed -ie's,###INIT_UDEV###,udev,g' /etc/init.d/ctxusbd
```

A continuación, vuelva a ejecutar manualmente `insserv` (de nuevo, con permisos de root):

```
/sbin/insserv /etc/init.d/ctxusbd
```

Este problema se ha observado solo en plataformas Debian.

[#425810]

- Al conectarse a sitios de Agente de Program Neighborhood, cuando faltan certificados o éstos están caducados, la interfaz de usuario de Receiver puede destellar, pedir repetidamente las credenciales de usuario, o consumir altos niveles de CPU. Como solución temporal, Citrix recomienda instalar los certificados correctamente y llevar a cabo un mantenimiento regular de los mismos. Este problema no se ha observado cuando se conecta con sitios de StoreFront.

[#425848]

- Los iconos de la interfaz de usuario de autoservicio pueden no mostrarse cuando usuarios nuevos buscan aplicaciones o escritorios. Como solución temporal, haga clic en Actualizar aplicaciones.

[#426364]

- Cuando se utiliza `pnabrowse` para conectar con un sitio de Agente de Program Neighborhood protegido por HTTPS en algunos servidores Microsoft Server 2012 en entornos `armhf` (hard float), se muestra un mensaje de error genérico y la conexión falla. Este problema no está definido del todo, pero puede ser debido a que los servidores tienen un nombre de dominio completo (FQDN) que termina en `.local`, o bien, porque el tamaño de clave especificado en el campo Clave pública del certificado en los servidores es de 2048 bits, en lugar de 1024 bits. Este problema no ocurre con `storebrowse` y solo se ha observado en entornos `armhf`.

[#426420]

- Si se cierra la sesión de Receiver (haciendo clic en Cerrar sesión en la interfaz de usuario de autoservicio) pero, a continuación, intenta conectar con un escritorio o aplicación y cancela el diálogo que pide credenciales, aparece el mensaje "No se puede procesar la solicitud". Puede ignorar este mensaje. El cierre de sesión tuvo lugar correctamente.

[#426424]

- Ocurre un error de segmentación, y Receiver falla, cuando se usa la interfaz de usuario de autoservicio por primera vez

para conectarse a un sitio de Agente de Program Neighborhood, al hacer clic en Cancelar en el cuadro de diálogo de inicio de sesión, hacer clic en Actualizar aplicaciones, y cerrar la ventana de Receiver. No existe ninguna solución para este problema.

[#426625]

- Cuando varios procesos llaman a procedimientos de almacén de datos o de carga al mismo tiempo, esto puede dar lugar a una pérdida de datos en los archivos que están en memoria (por ejemplo, StoreCache.xml). El último cambio hecho en un archivo se conserva, pero los cambios anteriores se pierden. No hay peligro de dañar el archivo.

[#426692]

- Si quita y, a continuación, agrega una tienda, la página Cuentas del cuadro de diálogo Preferencias no muestra la nueva tienda hasta que se cierra y se vuelve a abrir el cuadro de diálogo.

[#426735]

- Cuando la preferencia para Reconectar aplicaciones y escritorios está configurada con la opción Al iniciar o actualizar aplicaciones, y se está estableciendo una conexión con un escritorio o con una aplicación, si se selecciona Actualizar aplicaciones desde el menú de Receiver, la interfaz de usuario deja de responder hasta que se establece la conexión.

[#426761]

- No aparece ningún mensaje de error cuando se intenta agregar una tienda o una puerta de enlace que ya están incluidas en Receiver. No existe ninguna solución temporal para este problema, pero no se crean entradas duplicadas y la tienda o la puerta de enlace existentes continúan funcionando correctamente.

[#427379]

- Los menús de las aplicaciones publicadas desaparecen cuando se hace clic en ellos. Esto se ha observado con ventanas de aplicación maximizadas en entornos de escritorio GNOME 3 en Ubuntu 12.04 pero no en entornos Unity en Ubuntu 12.04.3.

[#429686]

- Precaución: Una limitación de Windows provoca que el nivel de volumen de sonido se maximiza cuando una sesión se vuelve a conectar automáticamente después de una interrupción de la red. No existe ninguna solución para este problema.

[#430160]

- Las preferencias de Receiver solo afectan a sesiones nuevas o reconectadas, no a sesiones desconectadas. Por ejemplo, puede iniciar Citrix GoToMeeting desde un escritorio virtual y luego desconectarse de la sesión de escritorio (pero no de GoToMeeting). A continuación, puede seleccionar Usar mi micrófono y mi cámara Web en la página Micrófono y cámara Web del cuadro de diálogo Preferencias, pero esto no iniciará la cámara Web en la sesión de GoToMeeting. Como solución temporal, cierre y reinicie la sesión afectada (en este ejemplo, la sesión de GoToMeeting).

[#430692]

- Si se ejecuta selfservice desde un terminal y el terminal se cierra antes de haber cerrado selfservice, se envía la señal de cierre estándar a todos los procesos en primer plano alojados por el terminal. Otros procesos de Receiver para Linux, como los demonios de Service Record y Authentication Manager no ignoran la señal, pero selfservice sí lo hace. Esto hace que selfservice deje de responder porque sus procesos dependientes se han finalizado. Como solución temporal, inicie los demonios usando storebrowse en una ventana, y luego, en una segunda ventana, ejecute selfservice. Esto permite cerrar la ventana de terminal donde se ejecuta selfservice pero los demonios siguen funcionando en segundo plano y la interfaz de usuario no se cuelga.

[#430697]

Requisitos del sistema

Jul 07, 2017

Dispositivos

- Kernel de Linux versión 2.6.29 o posterior, con respaldo para glibcxx 3.4.15 o posterior, glibc 2.11.3 o posterior, gtk 2.20.1 o posterior, libcap1 o libcap2 y udev.
- Para la interfaz de usuario de autoservicio:
 - libwebkit o libwebkitgtk 1.0
 - libxml2 2.7.8
 - libxerces-c 3.1
- Bibliotecas de códecs ALSA (libasound2), Speex y Vorbis.
- Al menos 55 MB de espacio libre en disco para la versión instalada de Receiver y al menos 110 MB si expande el paquete de instalación en el disco. Para comprobar el espacio en disco disponible, escriba el siguiente comando en una ventana de terminal:
df -k
- Al menos 1 GB de RAM para dispositivos SoC (system-on-a-chip) que usen la redirección de Flash de HDX MediaStream.
- Pantalla de vídeo de 256 colores o superior.
- Conexión de red TCP/IP.

H.264

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

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

Redirección de Flash de HDX MediaStream

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

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

Compresión de vídeo de cámara Web HDX RealTime

La compresión de vídeo de cámara Web HDX RealTime requiere:

- Una cámara Web compatible con Video4Linux.
- GStreamer 0.10.25 (o una versión posterior 0.10.x), incluido el paquete "plugins-good" de la distribución.
GStreamer 1.0 (o una versión 1.x posterior), incluidos los paquetes "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly" y "gstreamer-libav" de la distribución.

Redirección de Windows Media de HDX MediaStream

La redirección de Windows Media de HDX MediaStream requiere

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

GStreamer 1.0 (o una versión 1.x posterior), incluidos los paquetes "plugins-base", "plugins-good", "plugins-bad", "plugins-ugly" y "gstreamer-libav" de la distribución.

Nota: Si GStreamer no está incluido en su distribución de Linux, puede descargarlo desde <http://gstreamer.freedesktop.org>. Usar ciertos códigos (por ejemplo, los de "plugins-ugly") puede requerir una licencia del fabricante de esa tecnología. Consulte su departamento de asuntos legales para determinar si los códigos que piensa utilizar requieren licencias adicionales.

Philips 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, vaya al sitio Web de Philips.

Respaldo para tarjetas inteligentes

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

Nota

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

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

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

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

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

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

Servidores Citrix

- XenApp: Todas las versiones que Citrix admite en estos momentos. Para obtener más información, consulte la [matriz de productos de Citrix](#).
- XenDesktop: Todas las versiones que Citrix admite en estos momentos. Para obtener más información, consulte la [matriz](#)

[de productos de Citrix.](#)

- VDI-in-a-Box: Todas las versiones que Citrix admite en estos momentos. Para obtener más información, consulte la [matriz de productos de Citrix](#).
- Se puede usar el acceso de explorador Web de Citrix Receiver para Linux 13.5 junto con Receiver para Web de StoreFront y la Interfaz Web, con o sin NetScaler Gateway Plug-in.

StoreFront:

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

Interfaz Web junto con cliente NetScaler VPN:

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

Browser (Explorador Web)

Citrix recomienda que utilice la última versión de Mozilla Firefox o Google Chrome.

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

Conectividad

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

- Para conexiones LAN:
 - StoreFront con sitios de Receiver para Web o de servicios StoreFront
 - Interfaz Web 5.4 para Windows, mediante la Interfaz Web o sitios de servicios XenApp
- Para conexiones locales o remotas seguras:
 - Citrix NetScaler Gateway 11.1
 - Citrix NetScaler Gateway 11.0
 - Citrix NetScaler Gateway 10.5
 - Citrix NetScaler Gateway 10.1
 - Citrix Access Gateway Enterprise Edition 10
 - Citrix Access Gateway Enterprise Edition 9.x
 - Citrix Access Gateway VPX

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

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

contrario.

Acerca de las conexiones seguras y los certificados

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

Certificados privados (autofirmados)

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

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

Instalación de certificados raíz en los dispositivos de los usuarios

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

Certificados comodín

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

Certificados intermedios y NetScaler Gateway

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

Requisitos de usuario

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

Compruebe si el dispositivo cumple los requisitos del sistema

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

Para ejecutar el script `hdxcheck.sh`

1. Abra una ventana de terminal.
2. Escriba `cd $ICAROOT/util` y presione Entrar para navegar hasta el directorio Utilities del paquete de instalación.

3. Escriba `./hdxcheck.sh` para ejecutar el script.

Instalación y configuración

Jul 07, 2017

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

Nombre del paquete	Contenido
Paquetes Debian (Ubuntu, Debian, Linux Mint, etc.)	
icaclient_13.5.0.10185126_amd64.deb	Respaldo para autosevicio, 64 bits x86_64
icaclient_13.5.0.10185126_i386.deb	Respaldo para autosevicio, 32 bits x86
icaclient_13.5.0.10185126_armhf.deb	Respaldo para autosevicio, ARM HF
icaclient_13.5.0.10185126_armel.deb	Respaldo para autosevicio, ARM EL
icaclientWeb_13.5.0.10185126_amd64.deb	Solo Receiver para Web, 64 bits x86_64
icaclientWeb_13.5.0.10185126_i386.deb	Solo Receiver para Web, 32 bits x86
icaclientWeb_13.5.0.10185126_armhf.deb	Solo Receiver para Web, ARM HF
icaclientWeb_13.5.0.10185126_armel.deb	Solo Receiver para Web, ARM EL
ctxusb_2.7.10185126_amd64.deb	Paquete USB, 64 bits x86_64
ctxusb_2.7.10185126_i386.deb	Paquete USB, 32 bits x86
ctxusb_2.7.10185126_armhf.deb	Paquete USB, ARM HF
ctxusb_2.7.10185126_armel.deb	Paquete USB, ARM EL
Paquetes RedHat (RedHat, SUSE, Fedora, etc.)	
ICAClient-rhel-13.5.0.10185126-0.x86_64.rpm	Respaldo para autosevicio, basado en RedHat (incluido VDA Linux), 64 bits x86_64

ICAClient-rhel-13.5.0.10185126-0.i386.rpm	Respaldo para autoserivicio, basado en RedHat, 32 bits x86
ICAClientWeb-rhel-13.5.0.10185126-0.x86_64.rpm	Solo Receiver para Web, basado en RedHat, 64 bits x86_64
ICAClientWeb-rhel-13.5.0.10185126-0.i386.rpm	Solo Receiver para Web, basado en RedHat, 32 bits x86
ICAClient-suse-13.5.0.10185126-0.x86_64.rpm	Respaldo para autoserivicio, basado en SUSE, 64 bits x86_64
ICAClient-suse-13.5.0.10185126-0.i386.rpm	Respaldo para autoserivicio, basado en SUSE, 32 bits x86
ICAClient-suse11sp3-13.5.0.10185126-0.x86_64.rpm	Respaldo para autoserivicio, basado en SUSE 11 sp3 (incluido VDA Linux), 64 bits x86_64
ICAClient-suse11sp3-13.5.0.10185126-0.i386.rpm	Respaldo para autoserivicio, basado en SUSE 11 sp3, 32 bits x86
ICAClientWeb-suse-13.5.0.10185126-0.x86_64.rpm	Solo Receiver para Web, basado en SUSE, 64 bits x86_64
ICAClientWeb-suse-13.5.0.10185126-0.i386.rpm	Solo Receiver para Web, basado en SUSE, 32 bits x86
ctxusb-2.7.10185126-1.x86_64.rpm	Paquete USB, 64 bits x86_64
ctxusb-2.7.10185126-1.i386.rpm	Paquete USB, 32 bits x86
Tarballs (Instalación por script para cualquier distribución)	
linuxx64-13.5.0.10185126.tar.gz	Intel de 64 bits
linuxx86-13.5.0.10185126.tar.gz	Intel de 32 bits
linuxarmhf-13.5.0.10185126.tar.gz	ARM EL
linuxarm-13.5.0.10185126.tar.gz	ARM HF

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

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

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

Nota

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

Para instalar Citrix Receiver para Linux desde un paquete Debian

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

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

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

Para instalar el paquete usando la línea de comandos

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

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

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

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

Para instalar Citrix Receiver para Linux desde un paquete RPM

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

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

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

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

Para configurar el repositorio EPEL en Red Hat

1. Descargue el paquete fuente RPM apropiado desde aquí:

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

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

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

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

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

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

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

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

3. Abra una ventana de terminal.

Para instalaciones en SUSE:

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

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

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

Para instalaciones en Red Hat:

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

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

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

4. Acepte el contrato de licencia (EULA).

Para instalar Citrix Receiver para Linux desde un paquete tarball

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

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

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

El directorio predeterminado para las instalaciones de usuarios sin privilegios es `$HOME/ICAClient/plataforma`. Donde "plataforma" es un identificador generado por el sistema para el sistema operativo que tenga instalado. Por ejemplo, `$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, luego, presione Entrar.
7. Puede elegir si quiere integrar Receiver en 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.
8. Si ha instalado GStreamer previamente, puede elegir si quiere 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.

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

- 9 Si ha iniciado sesión como usuario con privilegios (root), podrá elegir si quiere 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 un mensaje para advertirle que 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 Entrar.

Personalización de la instalación de Citrix Receiver para Linux

Jul 07, 2017

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

Para personalizar una instalación de Citrix Receiver para Linux

1. Expanda el archivo del paquete de Citrix Receiver en un directorio vacío. El archivo del paquete se llama `platform.major.minor.release.build.tar.gz` (por ejemplo, `linuxx86.13.2.0.nnnnnn.tar.gz` para la plataforma Linux/x86).
2. Realice los cambios requeridos en el paquete de Citrix Receiver. Por ejemplo, puede agregar un nuevo certificado raíz TLS al paquete si desea utilizar un certificado de una entidad de certificación que no forma parte de la instalación estándar de Receiver. Para agregar un nuevo certificado raíz TLS al paquete, consulte [— Instalación de certificados raíz en los dispositivos de usuario](#) en el sitio de documentación de productos de Citrix. Para obtener más información acerca de los certificados integrados, consulte [— Configuración y habilitación de SSL y TLS](#) en [sitio de documentación de productos de Citrix](#).
3. Abra el archivo `PkgID`.
4. Agregue la línea siguiente para indicar que el paquete se ha modificado: `MODIFIED=traceinfo`, donde `traceinfo` es la información que indica quién realizó el cambio y cuándo se realizó. 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 comando `tar` para volver a generar el archivo del paquete de Receiver; por ejemplo: `tar czf ../newpackage.tar.gz *`, donde `newpackage` es el nombre del nuevo archivo del paquete de Receiver.

Inicio de Citrix Receiver para Linux

Jul 07, 2017

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

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

Sugerencia

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

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

En la interfaz de terminal, escriba `/opt/Citrix/ICAClient/selfservice` y presione Entrar (donde `/opt/Citrix/ICAClient` es el directorio donde instaló Citrix Receiver).

Para iniciar Citrix Receiver desde el escritorio Linux

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

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

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

Jul 07, 2017

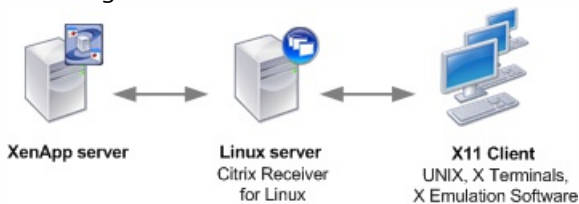
Puede utilizar una estación de trabajo que ejecuta Citrix Receiver como servidor y redirigir la salida a otro dispositivo compatible con X11. Se recomienda realizar esto para entregar aplicaciones de Microsoft Windows a terminales X o estaciones de trabajo UNIX en las que Citrix Receiver no está disponible.

Nota

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

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

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



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

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

Funcionalidades admitidas

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

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

Algunas funciones no se transfieren al dispositivo final:

- Redirección USB

- Redirección de tarjetas inteligentes
- Redirección de puertos COM
- 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.
- No se espera que la redirección de entrada multimedia funcione porque requiere una cámara Web en la máquina que ejecuta Citrix Receiver, que es el servidor que actúa como un proxy. Sin embargo, la redirección de salida multimedia funciona con GStreamer instalado en el servidor que actúa como proxy (no comprobado).

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

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

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

3. En un símbolo del sistema del dispositivo local, escriba xhost <proxy server name>
4. Si Receiver no está instalado en el directorio de instalación predeterminado, compruebe que la variable de entorno ICAROOT esté configurada para apuntar hacia el directorio de instalación real.
5. Ubique el directorio donde está instalado Citrix Receiver. En un símbolo del sistema, escriba selfservice &

Para desinstalar Citrix Receiver para Linux

Jul 07, 2017

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

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

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

Nota

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

Conectar

Jul 07, 2017

Citrix Receiver ofrece a los usuarios acceso de autoserivicio 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 antiguas creadas con la Interfaz Web, administran el acceso de los usuarios.

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

La página de inicio de Citrix Receiver muestra las aplicaciones y los escritorios virtuales que están disponibles para los usuarios, basándose en los parámetros de cuenta del usuario (es decir, el servidor al que se conecta) y en los parámetros configurados por los administradores de Citrix XenApp o Citrix XenDesktop. Desde 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 utiliza el mismo nombre para varias tiendas en el servidor StoreFront, puede evitar duplicados agregando números a esos nombres. Los nombres de dichas tiendas dependen del orden en que se agregaron. Para PNAgent, se muestra la URL de la tienda y esta identifica de manera exclusiva dicha tienda.

Después de conectarse a una tienda, el autoserivicio muestra las fichas Favoritos, Escritorios y Aplicaciones. Para iniciar una sesión, haga clic en el icono correspondiente. Para agregar un icono a Favoritos, haga clic en el enlace "Detalles" situado junto al icono y seleccione "Agregar a Favoritos".

Configuración de los parámetros de conexión

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

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

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

Conexión con recursos desde una línea de comandos o explorador

Jul 07, 2017

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

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

Como requisito previo, compruebe que Citrix Receiver conoce la tienda. 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 a un servidor, es posible que el administrador tenga que cambiar la ubicación del servidor o los detalles del proxy SOCKS. Para obtener más información, consulte [Conexión a través de un servidor proxy](#).

Para crear una conexión desde un explorador Web

Por regla general, la configuración para iniciar sesiones desde un explorador web se realiza automáticamente durante la instalación. Tenga en cuenta que, debido a la gran variedad de exploradores y sistemas operativos, puede ser necesaria alguna configuración manual.

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. Ejecute los siguientes comandos para una instalación de Citrix Receiver sin privilegios de administrador. La configuración de ICAROOT se puede cambiar si se instala en una ubicación no predeterminada. Puede comprobar el resultado con el comando "xdg-mime query default application/x-ica", que debe devolver "wfica.desktop".

```
setenv ICAROOT=/opt/Citrix/ICAClient
```

```
xdg-icon-resource install --size 64 "$ICAROOT/icons/000_Receiver_64.png Citrix-Receiver"
```

```
xdg-mime default wfica.desktop application/x-ica
```

```
xdg-mime default new_store.desktop application/vnd.citrix.receiver.configure
```

2. Crea o extienda el archivo /etc/xdg/mimeapps.list (para la instalación de administrador) o \$HOME/.local/share/applications/mimeapps.list (mimeapps.list). El archivo debe comenzar por [Default Applications] y seguir con:

```
application/x-ica=wfica.desktop;
```

```
application/vnd.citrix.receiver.configure=new_store.desktop;
```

Tenga en cuenta que quizá deba configurar la página Preferencias o Aplicaciones de Firefox. Para Citrix ICA settings file content", seleccione "Citrix Receiver Engine (default)" en el menú desplegable. O seleccione "Utilizar otros..." y, a continuación, seleccione el archivo /usr/share/applications/wfica.desktop (para una instalación de administrador de Receiver) o \$HOME/.local/share/applications/wfica.desktop (para una instalación sin privilegios de administrador).

Solución de problemas en las conexiones con recursos

Jul 07, 2017

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

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

Para administrar una conexión

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

Personalización mediante archivos de configuración

Jul 07, 2017

Acerca de los archivos de configuración

Para cambiar parámetros más avanzados o menos comunes, puede modificar los archivos de configuración de Receiver. Estos archivos de configuración se leen cada vez que wfica se inicia. Puede actualizar varios archivos, según el efecto que quiera 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 opciones predeterminadas a todos los usuarios de Citrix Receiver

Si quiere cambiar las opciones predeterminadas de todos los usuarios de Citrix Receiver, modifique el archivo de configuración module.ini en el directorio \$ICAROOT/config.

Nota

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

Aplicación de cambios para los usuarios nuevos de Citrix Receiver

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

Aplicación de cambios para todas las conexiones de usuarios específicos

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

Validación de las entradas del archivo de configuración

Si quiere limitar los valores permitidos para las entradas en wfclient.ini, puede especificar las opciones o los rangos de opciones permitidos en All_Regions.ini. Si especifica un solo valor posible, se utiliza ese valor. Tenga en cuenta que \$HOME/.ICAClient/All_Regions.ini solo puede coincidir con los valores posibles establecidos en \$ICAROOT/config/All_Regions.ini o limitarlos, pero no puede quitarles las restricciones. 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.

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

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

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

Nota

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

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

Jul 07, 2017

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

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

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

Important

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

Publicar contenido

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

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

Optimización

Jul 07, 2017

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

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

Asignación de dispositivos de usuario

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

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

Asignación de unidades del cliente

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

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

Existen dos tipos de asignación de unidades disponibles:

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

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

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

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

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

Asignación de impresoras del cliente

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

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

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

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

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

1. Abra el archivo de configuración, wfclient.ini, en uno de los siguientes directorios:
 - \$HOME/.ICAClient, para limitar las impresoras de un solo usuario
 - \$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=printer1:printer2:printer3

donde printer1, printer2 y sucesivos son los nombres de las impresoras elegidas. Separe los nombres de las impresoras con dos puntos (:).

3. Guarde y cierre el archivo.

Asignación de impresoras del cliente en XenApp para Windows

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

Para asignar una impresora local en un servidor

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

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

Aparecerá el asistente Agregar impresora.

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

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

Asignación de impresoras del cliente en XenApp para UNIX

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

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

Asignación de sonido del cliente

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

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

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

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

Para configurar un dispositivo de sonido no predeterminado

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

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

```
[ClientAudio]
```

```
AudioDevice = <device>
```

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

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

Configuración del respaldo USB

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

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

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

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

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

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

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

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

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

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

Funcionamiento del respaldo USB

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

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

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

Dispositivos de almacenamiento masivo

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

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

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

Cámaras Web

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

Clases de USB permitidas de forma predeterminada

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

Sonido (clase 01)

Incluye micrófonos, altavoces, auriculares y controladores MIDI.

Interfaz física (clase 05)

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

Digitalización de imágenes fijas (clase 06)

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

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

Impresoras (clase 07)

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

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

Almacenamiento masivo (clase 08)

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

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

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

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

Seguridad del contenido (clase 0d)

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

Atención médica personal (clase 0f)

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

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

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

Clases de dispositivos USB que se rechazan de manera predeterminada

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

Comunicaciones y control CDC (clases 02 y 0a)

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

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

Dispositivos de interfaz humana (HID) (clase 03)

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

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

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

Concentradores USB (clase 09)

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

Tarjeta inteligente (clase 0b)

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

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

Vídeo (clase 0e)

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

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

Controladores inalámbricos (clase e0)

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

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

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

Actualización de la lista de dispositivos USB disponibles para la comunicación

remota

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

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

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

Denegar: clase 09 # Dispositivos Hub

Denegar: clase 03 subclase 01 # Dispositivos de arranque HID (teclados y mouse)

Denegar: clase 0b # Tarjeta inteligente

Denegar: clase e0 # Controladores inalámbricos

Denegar: clase 02 # Control CDC y comunicaciones

Denegar: clase 03 # UVC (cámara Web)

Denegar: clase 0a # Datos de CDC

Permitir: # Recurso de reserva definitivo: permitir todo lo demás

Creación de reglas de directivas de USB

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

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

Etiqueta	Descripción
VID	Identificador del proveedor tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
Clase	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.

Permitir: VID=1230 PID=0007 # Otra Industria, Otra unidad de Flash

Denegar: Clase 08 subclase 05 # Dispositivos de almacenamiento masivo

Denegar: Clase 0D # Todos los dispositivos de seguridad

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 = Boolean 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.

Mejora del rendimiento en conexiones con poco ancho de banda

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

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

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

software de servidor.

Configuración de conexiones

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

- **Habilite la reducción de retardo SpeedScreen:** la reducción de retardo SpeedScreen mejora el rendimiento en conexiones con altos niveles de latencia al proporcionar comentarios instantáneos al usuario en respuesta a los datos introducidos o a las acciones con el puntero. Use el Administrador de reducción de retardo SpeedScreen para habilitar esta función en el servidor. En Receiver, de forma predeterminada, esta opción está inhabilitada para el teclado y solo está habilitada para el puntero en conexiones con una latencia elevada. Consulte la *— guía de referencia de OEM de Citrix Receiver para Linux (en inglés)*.
- **Habilite la compresión de datos:** La compresión de datos reduce la cantidad de datos transferidos a través de la conexión. Esto requiere recursos adicionales del procesador para comprimir y descomprimir datos, pero puede aumentar el rendimiento en conexiones de poco ancho de banda. Use las configuraciones de directiva de Citrix Calidad de sonido y Compresión de imágenes para habilitar esta característica.
- **Reduzca el tamaño de la ventana:** Cambie 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	Medio	Baja		

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

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

Cambio en la forma en que se utiliza Receiver

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

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

Optimización del rendimiento multimedia

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

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

Configuración de la redirección de Windows Media de HDX MediaStream

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

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

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

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

Citrix 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 de HDX MediaStream

1. Instale GStreamer 0.10, un marco de trabajo multimedia de código abierto, en cada dispositivo del usuario que lo requiera. Por regla general, GStreamer se instala antes de instalar a Citrix Receiver para que, durante el proceso de instalación Citrix Receiver, este se configure para utilizar GStreamer. La mayoría de las distribuciones de Linux incluyen GStreamer. De forma alternativa, puede descargar GStreamer desde <http://gstreamer.freedesktop.org>.
2. Para habilitar la obtención de contenido en el lado del cliente, instale los plugins de *origen de protocolo* de GStreamer para los tipos de archivo que los usuarios reproducirán en el dispositivo. La utilidad `gst-launch` permite verificar que el plugin se encuentre instalado y funcione correctamente. Si `gst-launch` puede reproducir la dirección URL, el plugin requerido funciona correctamente. Por ejemplo, ejecute `gst-launch-0.10 playbin2 uri=http://example-source/file.wmv` y compruebe que el vídeo se reproduce correctamente.
3. Cuando instale Citrix Receiver en el dispositivo, seleccione la opción de GStreamer si está utilizando el script `tarball` (esto se hace automáticamente para los paquetes `.deb` y `.rpm`).

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 URL estándar que no haga referencia a estos tipos de archivo. Utilice `gst-launch` para verificar que una dirección URL determinada sea válida.

Nota sobre GStreamer 1.0:

- De forma predeterminada, se utiliza GStreamer 0.10 para la redirección de Windows Media de HDX MediaStream. GStreamer 1.0 solo se utiliza cuando GStreamer 0.10 no está disponible.
- Si quiere utilizar GStreamer 1.0, siga estas instrucciones:
 1. Busque el directorio de instalación de los plugins de GStreamer. La ubicación de instalación de los plugins varía en función de la distribución, la arquitectura del sistema operativo y la instalación en sí de GStreamer. La ruta de instalación típica es `/usr/lib/x86_64-linux-gnu/gstreamer-1.0` o `$HOME/.local/share/gstreamer-1.0`.
 2. Busque el directorio de instalación de Citrix Receiver para Linux. El directorio predeterminado para las instalaciones de usuarios con privilegios (root) es `/opt/Citrix/ICAClient`. El directorio predeterminado para las instalaciones de usuarios sin privilegios es `$HOME/ICAClient/platform` (donde "platform" puede ser `linuxx64`, por ejemplo). Para obtener más información, consulte [Instalación y configuración](#).
 3. Instale `libgstflatstm1.0.so` mediante un vínculo simbólico en el directorio de plugins de GStreamer: `ln -sf $ICAClient_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so`. Este paso puede requerir permisos elevados (como `sudo`, por ejemplo).
 4. Use `gst_play1.0` como reproductor en: `ln -sf $ICAClient_DIR/util/gst_play1.0 $ICAClient_DIR/util/gst_play`. Este paso puede requerir permisos elevados (como `sudo`, por ejemplo).
- Si quiere usar GStreamer 1.0 para la compresión de vídeo de cámara Web HDX RealTime, use `gst_read1.0` como el lector: `ln -sf $ICAClient_DIR/util/gst_read1.0 $ICAClient_DIR/util/gst_read`.

Configuración de la redirección de Flash de HDX MediaStream

La Redirección de Flash de HDX MediaStream habilita el contenido de Adobe Flash para que se reproduzca de forma local en los dispositivos de los usuarios, y les brinda una reproducción de sonido y vídeo de alta definición sin aumentar los requisitos de ancho de banda.

1. Asegúrese de que el dispositivo del usuario cumpla los requisitos de esta función. Para obtener más información, consulte [Requisitos del sistema](#).
2. Agregue los siguientes parámetros a la sección [WFClient] de `wfclient.ini` (para todas las conexiones hechas por un usuario específico) o a la sección [Client Engine\Application Launching] de `All_Regions.ini` (para todos los usuarios del entorno):
 - **HDXFlashUseFlashRemoting=Ask | Never | Always**
Habilita HDX MediaStream para Flash en el dispositivo del usuario. De forma predeterminada, este parámetro está establecido en **Never** y se presenta un cuadro de diálogo a los usuarios para preguntarles si quieren optimizar el contenido de Flash al conectarse a páginas Web que contienen Flash.
 - **HDXFlashEnableServerSideContentFetching=Disabled | Enabled**
Habilita o inhabilita la obtención de contenido en el servidor para Receiver. De forma predeterminada, este parámetro está configurado como inhabilitado: **Disabled**.
 - **HDXFlashUseServerHttpCookie=Disabled | Enabled**
Habilita o inhabilita la redirección de cookies HTTP. De forma predeterminada, este parámetro está configurado como inhabilitado: **Disabled**.
 - **HDXFlashEnableClientSideCaching=Disabled | Enabled**
Habilita o inhabilita el almacenamiento en caché del cliente del contenido Web obtenido por Receiver. De forma predeterminada, este parámetro está configurado como habilitado: **Enabled**.

- **HDXFlashClientCacheSize= [25-250]**

Define el tamaño en megabytes (MB) del caché en el cliente. Puede introducirse cualquier tamaño entre 25 y 250 MB. Cuando se alcance el tamaño máximo, se eliminará el contenido existente en el caché para permitir el almacenamiento de contenido nuevo. De forma predeterminada, este parámetro está configurado como **100**.

- **HDXFlashServerSideContentCacheType=Persistent | Temporary | NoCaching**

Define el tipo de almacenamiento en caché que utiliza Receiver para el contenido que se obtiene en el servidor. De forma predeterminada, este parámetro está configurado como persistente: **Persistent**.

Nota: Este parámetro se requiere solamente si **HDXFlashEnableServerSideContentFetching** está configurado como habilitado: **Enabled**.

3. La redirección de Flash está inhabilitada de forma predeterminada. En /config/module.ini, cambie FlashV2=Off por FlashV2=On para habilitar la función.

Configuración de la compresión de vídeo de cámara Web HDX RealTime

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

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

Inhabilitación de la compresión de vídeo de cámara Web HDX RealTime

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

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

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

```
HDXWebCamEnabled=Off
```

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

2. Abra el archivo usb.conf que, por lo general, se encuentra en \$ICAROOT/usb.conf.
3. Elimine o convierta en comentario la siguiente línea:

```
Denegar: clase 0e # UVC (opción predeterminada a través de la compresión de vídeo de cámara Web 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

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

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

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

Mejora de la experiencia del usuario

Jul 07, 2017

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

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

Configuración de preferencias

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

Para administrar una cuenta

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

1. En la página Cuentas del cuadro de diálogo Preferencias, lleve a cabo 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 una tienda utilizada por la cuenta (por ejemplo, la puerta de enlace predeterminada), haga clic en Editar.
 - Para quitar una cuenta, haga clic en Quitar.
2. Siga las instrucciones en pantalla. Es posible que tenga que autenticarse en el servidor.

Para cambiar cómo se ven los escritorios

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

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

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

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

Desktop Viewer

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

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

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

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

Para reconectar automáticamente las sesiones

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

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

Para controlar cómo se accede a los archivos locales

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

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

Para configurar un micrófono o una cámara Web

Puede cambiar el modo en que un escritorio virtual o una aplicación acceden a su micrófono o cámara Web locales: En la página Micrófono y cámara Web del cuadro de diálogo Preferencias, seleccione alguna de las siguientes opciones:

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

Para configurar el reproductor de Flash

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

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

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

Configuración del suavizado de fuentes de ClearType

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

FontSmoothingType = number

donde number 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 subpixel horizontal pueden aumentar los requisitos de ancho de banda de Receiver.

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

FontSmoothingTypePref = number

donde number puede tomar uno de los siguientes valores:

Valor	Comportamiento
0	Sin suavizado
1	
2	Suavizado estándar

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

Configuración de la redirección de carpetas especiales

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

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

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

Para configurar la redirección de carpetas especiales

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

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

```
[ClientDrive]
```

```
SFRAllowed = True
```

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

```
DocumentsFolder = documentos
```

```
DesktopFolder = escritorio
```

donde `documentos` y `escritorio` 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

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

Los siguientes tipos de URL pueden redirigirse:

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

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

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

Nota

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

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

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

Path=path

Command=command

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

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

Este parámetro especifica lo siguiente:

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

Path=path

Command=command

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

Para inhabilitar la redirección de contenido servidor-cliente desde Receiver

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

Control del comportamiento del teclado

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

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

Uso de xcapture

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

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

Para iniciar xcapture desde la línea de comandos

En el símbolo del sistema, escriba /opt/Citrix/ICAClient/util/xcapture y presione INTRO (donde /opt/Citrix/ICAClient es el directorio en el que se 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 (Seleccionar una ventana). Mueva el cursor por la ventana que desea copiar y haga clic con el botón central del puntero.
 - Select a region (Seleccionar una región). Mantenga presionado el botón principal del puntero y arrastre el cursor para seleccionar el área que desea copiar.
 - Cancel the selection (Cancelar la selección). 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.

Reconexión automática de usuarios

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

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

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

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

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

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

Cómo garantizar la fiabilidad de las sesiones

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

Con la función de fiabilidad de sesiones de HDX Broadcast, los usuarios seguirán viendo una ventana con la aplicación publicada si la conexión a la aplicación se interrumpe. Por ejemplo, los usuarios inalámbricos que pasen por un túnel pueden perder la conexión al entrar pero volverán a conectarse al salir del túnel. Durante el período de inactividad, todos los datos, entradas de teclado y otras interacciones del usuario se almacenan, mientras que la aplicación parece bloqueada y no responde. Cuando la conexión se restablece, dichas interacciones se reproducen en la aplicación.

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

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

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

Important

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

Mouse relativo

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

Nota

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

Para habilitar la función:

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

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

Sugerencia

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

Para activar la función:

Introduzca Ctrl/F12.

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

Para desactivar la función:

Introduzca Ctrl-Mayús/F12.

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

Valores alternativos de puntero relativo

También puede considerar los siguientes valores de `RelativeMouse`:

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

Para cambiar los comandos del teclado, agregue parámetros como:

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

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

Seguridad

Jul 07, 2017

En este artículo:

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

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

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

Conexión a través de un servidor proxy

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

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

Nota

Para garantizar una conexión segura, habilite TLS.

Conexión a través de un servidor proxy seguro

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

Important

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

Conexión con Secure Gateway o Traspaso SSL Citrix

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

Conexión con Secure Gateway

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

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

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

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

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

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

- Nombre de host
- Dominio intermedio
- Dominio superior

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

Conexión con el Traspaso SSL Citrix

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

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

Puede utilizar el Traspaso SSL Citrix para proteger las comunicaciones:

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

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

Configuración y habilitación de TLS

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

- MinimumTLS=1.0
- MaximumTLS=1.2

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

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

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

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

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

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

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Instalación de certificados raíz en los dispositivos de los usuarios

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

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

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

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

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

Nota: Receiver para Linux 13.0 emplea `c_rehash` del dispositivo local. La versión 13.1 y las versiones siguientes utilizan la herramienta `ctx_rehash` tal y como se describe a continuación.

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 una tienda 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 siguiente comando:

```
$ICAROOT/util/ctx_rehash
```

Uso de un certificado intermedio

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

1. Obtenga los certificados intermedios por separado en formato PEM.

Sugerencia: Si no puede encontrar un certificado en este formato, use la utilidad `openssl` para convertir un certificado en formato CRT a un archivo `.pem`.

2. Mediante la cuenta de usuario con la que instaló el paquete (normalmente `root`):

1. Copie los archivos en `$ICAROOT/keystore/intcerts`.

2. Ejecute el siguiente comando como usuario que instaló el paquete:

```
$ICAROOT/util/ctx_rehash
```


Habilitación del respaldo para tarjetas inteligentes

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

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

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

El respaldo para tarjetas inteligentes tiene los siguientes requisitos previos:

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

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

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

Conexiones a través de NetScaler Gateway

Citrix NetScaler Gateway (antes llamado Access Gateway) protege las conexiones a las tiendas 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, una tienda concreta:
 - Para conectar con la primera tienda que encuentre Receiver, use una URL con el formato `https://puertaDeEnlace.empresa.com`.
 - Para conectar con una tienda específica, 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 una tienda concreta con storebrowse, es probable que se necesiten comillas alrededor de la dirección URL en el comando storebrowse.

2. Cuando se le solicite, conéctese a la tienda (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

Jul 07, 2017

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

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

Problemas de conexión

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

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

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

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

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

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

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

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

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

En ocasiones no puedo conectarme cuando intento reconectar con sesiones

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

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

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

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

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

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

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

```
var ...;
```

Las sesiones demoran mucho en iniciarse

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

Me gustaría configurar el parámetro de un puerto serie

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

```
LastComPortNum=1 ComPort1=
```

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

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

Errores de conexión

Aparece un diálogo de error donde se avisa de un error de conexión: "Error in connection: A protocol error occurred while communicating with the Authentication Service". Hay varios problemas que pueden ser la causa de esta condición de error, entre ellos los siguientes:

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

Problemas de presentación

¿Por qué se ve la pantalla partida?

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

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

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

Parámetros de GPU de X11

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

```
Sección "Dispositivo"  
    Identificador: "Graphics"  
    Controlador: "intel"  
    Opción: "AccelMethod" "sna"  
    Opción: "TearFree" "true"  
Fin de la sección
```

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

```
{ForceFullCompositionPipeline = On}
```

Por ejemplo:

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

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

Administradores de composición

Use lo siguiente:

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

Ejecute "ComprizConfig Settings Manager"

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

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

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

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

Cuando uso el teclado, aparecen entradas de teclado incorrectas

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

Hay un redibujado excesivo al mover las ventanas integradas

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

Compatibilidad de iconos

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

Para ofrecer una compatibilidad total de iconos

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

Tengo problemas para ver el cursor

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

Para cambiar el color del cursor

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

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

3. Guarde y cierre el archivo.

Los colores en la pantalla parpadean

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

Experimento cambios rápidos de colores con las presentaciones en color verdadero

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

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

Los caracteres japoneses se muestran de forma incorrecta en mi pantalla

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

Deseo realizar una sesión con varios monitores

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

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

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

La opción `-span` tiene el siguiente formato:

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

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

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

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

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

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

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

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

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

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

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

1. Escriba lo siguiente en una interfaz de comandos:

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

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

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

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

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

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

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

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

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

```
killall AuthManagerDaemon ServiceRecord storebrowse
```

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

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

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

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

Problemas con el explorador Web

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

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

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

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

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

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

El programa de instalación no admite un explorador específico

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

Cuando inicio escritorios o aplicaciones en Firefox, no ocurre nada

Pruebe a habilitar el plugin ICA.

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

Pruebe a inhabilitar el plug-in ICA.

Otros problemas

Es posible que se encuentre con los siguientes problemas adicionales.

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

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

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

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

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

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

Los parámetros de mi archivo de configuración ya no funcionan

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

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

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

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

No puedo iniciar Receiver

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

- Defina ICAROOT como el directorio de instalación.

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

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

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

Las teclas de acceso rápido no funcionan correctamente

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

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

- El modo traducido en el teclado, asigna un conjunto de combinaciones de teclas locales a combinaciones de teclas en el lado del servidor. Por ejemplo, de forma predeterminada en el modo traducido, la combinación CTRL+MAYÚS+F1 está asignada a la combinación ALT+F1 en el lado del servidor. Para reconfigurar esta asignación a una combinación de teclas local alternativa, actualice esta entrada de la sección [WFClient] del archivo \$HOME/.ICAClient/wfclient.ini. Esto asigna la combinación de teclas local ALT+CTRL+F1 a ALT+F1:
 - Cambie Hotkey1Shift=Ctrl+Shift 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.

Quiero habilitar un teclado croata remoto

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

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

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

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

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

También puede ejecutar este comando en AuthManagerDaemon o en PrimaryAuthManager.

Me gustaría utilizar el teclado japonés en el cliente

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

Me gustaría utilizar el teclado ABNT2 en el cliente

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

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

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

Errores de configuración de conexión

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

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

El archivo de configuración se editó incorrectamente o está dañado.

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

El archivo de configuración se editó incorrectamente o está dañado.

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

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

Errores de configuración de wfclient.ini

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

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

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

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

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

E_PNAGENT_FILE_UNREADABLE. No se puede leer el archivo XenApp "...": No existe tal archivo o directorio.

O bien:

No se puede leer archivo XenApp "...": Permiso denegado.

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

Errores de archivos PAC

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

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

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

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

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

Error de detección de proxy: Falló la descarga HTTP del script .PAC. Ruta no encontrada.

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

Error de detección de proxy: Falló la descarga HTTP del script .PAC.

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

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

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

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

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

Error de detección de proxy: Error de JavaScript.

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

Error de detección de proxy: Resultados no válidos del script de configuración automática del proxy.

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

Otros errores

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

Ha ocurrido un error. El código del error es 11 (E_MISSING_INI_SECTION). Consulte la documentación. Cerrándose.

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

E_BAD_OPTION. La opción "..." no es válida.

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

E_BAD_ARG. La opción "..." tiene un argumento no válido: "...".

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

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

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

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

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

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

No puede resolverse el nombre del servidor.

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

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

Se perdió la conexión con el servidor. Vuelva a conectarse e inténtelo nuevamente. Puede que faltan datos en estos archivos: "...".

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

Envío de información de diagnóstico a la asistencia técnica de Citrix

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

Para obtener información de diagnóstico sobre Receiver

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

SDK y API

Jul 07, 2017

Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) ofrece respaldo para la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para canales virtuales adicionales con el protocolo ICA. Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores XenApp o XenDesktop. Esta versión del SDK ofrece respaldo para la escritura de canales virtuales nuevos en Receiver para Linux. Si desea escribir controladores virtuales para otras plataformas cliente, póngase en contacto con Citrix.

El Virtual Channel SDK ofrece:

- La API para Citrix Virtual Driver (VD-API), que se usa con las funciones de canal virtual en el SDK de WF-API (Citrix Server API SDK) para crear nuevos canales virtuales. El respaldo para canales virtuales proporcionado por VD-API está diseñado para hacer más sencilla la creación de sus propios canales virtuales.
- Código fuente operacional de varios ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.
- El Virtual Channel SDK requiere el SDK de WF-API para escribir la parte del lado del servidor del canal virtual.

Para obtener más información sobre el SDK, consulte [Citrix Virtual Channel SDK para Citrix Receiver para Linux 13.5](#).

Referencias y parámetros de línea de comandos

Para obtener información sobre las referencias y los parámetros de la línea de comandos, consulte [Referencia de comandos de Citrix Receiver para Linux 13.5](#).