Aplicación Citrix Workspace para Linux

Contents

Acerca de esta versión

May 9, 2023

Novedades de la versión 2303

Inicio de sesión persistente

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

La función de inicio de sesión persistente le permite mantener la sesión iniciada el período (de 2 a 365 días) configurado por su administrador. Cuando esta función está habilitada, no necesita proporcionar las credenciales de inicio de sesión para la aplicación Citrix Workspace durante el período configurado.

Con esta funcionalidad, las sesiones de SSO en Citrix DaaS se prolongan hasta 365 días. Esta ampliación se basa en el tiempo de vida de los tokens de larga duración. Sus credenciales se almacenan en la caché de forma predeterminada durante 4 días o la duración definida, lo que sea inferior. Y, luego, se prolonga cuando hay actividad de nuevo dentro de estos 4 días al conectarse a la aplicación Citrix Workspace.

Para obtener más información, consulte Inicio de sesión persistente.

Compatibilidad con la autenticación mediante FIDO2 en sesiones HDX

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

Con esta versión, puede autenticarse dentro de una sesión de HDX mediante claves de seguridad FIDO2 sin contraseña. Las claves de seguridad FIDO2 ofrecen un modo intuitivo de autenticación para empleados corporativos en aplicaciones o escritorios compatibles con FIDO2 sin necesidad de introducir un nombre de usuario o una contraseña. Para obtener más información sobre FIDO2, consulte Autenticación FIDO2.

> **Nota:**
>
> Si utiliza el dispositivo FIDO2 mediante la redirección de USB, quite la regla de redirección de USB de su dispositivo FIDO2 del archivo `usb.conf` de la carpeta `$ICAROOT/`. Esta actualización le ayuda a cambiar al canal virtual FIDO2.

De forma predeterminada, la autenticación FIDO2 está inhabilitada.

Para obtener más información, consulte Función de autenticación mediante FIDO2.

Función de eliminación de eco de audio mejorada

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

A partir de esta versión, la aplicación Citrix Workspace admite la eliminación de eco. Esta función está diseñada para casos de usuario con audio en tiempo real y mejora la experiencia del usuario. La función de eliminación de eco opera con audio de calidad baja, calidad media y adaptable. Para obtener un rendimiento óptimo, Citrix recomienda usar audio adaptable.

Para obtener más información, consulte Función de eliminación de eco de audio mejorada.

Tiempo de espera por inactividad para la aplicación Citrix Workspace

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

La función de tiempo de espera por inactividad cierra su sesión de la aplicación Citrix Workspace en función de un valor que establece el administrador. Los administradores pueden especificar el tiempo de inactividad que se permite antes de que se cierre la sesión de usuario automáticamente en la aplicación Citrix Workspace. Se cierra la sesión automáticamente cuando no hay actividad del mouse, del teclado ni táctil durante el intervalo de tiempo especificado dentro de la ventana de la aplicación Citrix Workspace. El tiempo de espera por inactividad no afecta a las sesiones de Citrix Virtual Apps and Desktops y Citrix DaaS ni a almacenes de Citrix StoreFront.

El valor del tiempo de espera por inactividad se puede establecer desde 10 minutos a 1440 minutos. El intervalo para cambiar este valor de tiempo de espera debe estar en múltiplos de 5. Por ejemplo: 10, 15, 20 o 25 minutos. De forma predeterminada, el tiempo de espera por inactividad no está configurado.

> **Nota:**
>
> Esta función solo es aplicable en implementaciones en la nube.

Para obtener más información sobre cómo configurar InactivityTimeoutInMinutes, consulte la sección Tiempo de espera por inactividad para la aplicación Citrix Workspace.

Desenfoque de fondo para la redirección de cámaras web

Ahora, la aplicación Citrix Workspace para Linux admite el desenfoque de fondo para la redirección de cámaras web.

Para obtener más información, consulte Desenfoque de fondo para la redirección de cámaras web.

Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web

A partir de la versión 2303 de la aplicación Citrix Workspace, se le solicita que configure la ruta de almacenamiento de datos temporales para el explorador web basado en CEF.

Para obtener más información, consulte Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web.

Compatibilidad con nuevas tarjetas PIV

En esta versión, la aplicación Citrix Workspace admite estas tarjetas nuevas de verificación de identificación personal (PIV):

- Tarjeta inteligente IDEMIA de nueva generación
- Tarjeta inteligente TicTok de DELL

Optimización del rendimiento del controlador de tarjetas inteligentes

La versión 2303 de la aplicación Citrix Workspace incluye correcciones y optimizaciones relacionadas con el rendimiento para el controlador de tarjetas inteligentes `VDSCARDV2.DLL`. Estas mejoras ayudan a superar a la versión 1 `VDSCARD.DLL`.

Mejoras de Microsoft Teams

Limitar resoluciones de vídeo [Technical Preview]

Los administradores que tienen usuarios en dispositivos de punto final clientes de bajo rendimiento pueden optar por limitar las resoluciones de vídeos entrantes o salientes para reducir el impacto de la codificación y la decodificación de vídeo en dichos dispositivos. A partir de la aplicación Citrix Workspace 2303 para Linux, puede limitar estas resoluciones mediante las opciones de configuración del cliente.

Para obtener más información, consulte Limitar resoluciones de vídeo.

Puede enviar sus comentarios sobre esta Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios

> en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Configurar una interfaz de red preferida

Ahora, a partir de la versión 2303 de la aplicación Citrix Workspace, puede configurar una interfaz de red preferida para el tráfico de contenido multimedia. Con esta mejora, si tiene varias conexiones de red y el rendimiento de la predeterminada no es bueno, puede cambiar a otra red.

Para obtener más información, consulte Configurar una interfaz de red preferida.

Problemas resueltos en la versión 2303

- Al acceder a Hyperspace a través de Citrix Virtual Apps, es posible que la página de inicio de sesión específica de Hyperspace aparezca encima de las aplicaciones que ya están iniciadas. [CVADHELP-20368]
- Al acceder a una segunda aplicación, es posible que la sesión actual se cierre y que la sesión se reinicie. Es posible que los datos de la sesión anterior no estén presentes y que se actualicen como si la sesión se hubiera iniciado en el momento en que se inició la segunda aplicación. Este problema no se produce al iniciar la aplicación inicial en una sesión. [CVADHELP-21914]
- Es posible que no pueda actualizar el formato horario de 24 horas en la sección **Autoservicio** > **Perfil** > **Parámetros de cuenta** > **Configuración regional** > **Formato de hora**. Este problema solo se produce en almacenes de la nube. [CVADHELP-20866]
- Es posible que la sesión se cierre de forma abrupta después de desenchufar el dispositivo USB mientras arrastra varios archivos de la sesión de VDA al dispositivo USB. Este problema solo se produce en Ubuntu. [HDX-30219]
- Es posible que tenga problemas de rendimiento al iniciar sesión en la aplicación Citrix Workspace con una tarjeta inteligente que tenga la versión del controlador VDSCARDV2.DLL. Este problema solo se produce en las distribuciones de eLux. [HDX-44314]

Problemas conocidos en la versión 2303

- Al instalar la aplicación Citrix Workspace mediante la interfaz de usuario, es posible que no pueda instalar la función de protección de aplicaciones en Ubuntu 20.04 ni 22.04. Como solución temporal, instale la aplicación mediante la interfaz de línea de comandos. [APPP-1067]
- Es posible que no pueda iniciar sesiones en la versión 2303 de la aplicación Citrix Workspace si el valor de `AllowMultistream` está establecido en **True** en Ubuntu 22.04. [HDX-49916]
- Es posible que no pueda autenticarse en la versión 2303 de la aplicación Citrix Workspace para Linux con tarjetas inteligentes. Este problema se produce en las distribuciones Red Hat, Ubuntu 22.04 y Debian 11 de Linux. [RFLNX-9620]

- Si sale de la aplicación Citrix Workspace desde el indicador de aplicaciones, es posible que la aplicación deje de responder y que aparezca este mensaje de error:

  "GLib (gthread-posix.c): Unexpected error from C library during 'pthread_setspecific': Invalid argument".

  Como solución temporal, compruebe que usa la versión 2.76 de glib o una posterior. [RFLNX-9445]

> **Nota:**
>
> Para obtener una lista completa de los problemas de las versiones anteriores, consulte Problemas conocidos.

Versiones anteriores

En esta sección se proporciona información sobre las nuevas funciones y los problemas resueltos en las versiones anteriores disponibles según lo indicado en Lifecycle Milestones for Citrix Workspace app.

2302

Novedades

Tiempo de espera por inactividad para la aplicación Citrix Workspace [Technical Preview]

La función de tiempo de espera por inactividad cierra su sesión de la aplicación Citrix Workspace en función de un valor que establece el administrador. Los administradores pueden especificar el tiempo de inactividad que se permite antes de que se cierre la sesión de usuario automáticamente en la aplicación Citrix Workspace. Se cierra la sesión automáticamente cuando no hay actividad del mouse, del teclado ni táctil durante el intervalo de tiempo especificado dentro de la ventana de la aplicación Citrix Workspace. El tiempo de espera por inactividad no afecta a las sesiones de Citrix Virtual Apps and Desktops y Citrix DaaS ni a almacenes de Citrix StoreFront.

El valor del tiempo de espera por inactividad se puede establecer desde 10 minutos a 1440 minutos. El intervalo para cambiar este valor de tiempo de espera debe estar en múltiplos de 5. Por ejemplo: 10, 15, 20 o 25 minutos. De forma predeterminada, el tiempo de espera por inactividad no está configurado. Los administradores pueden configurar la propiedad inactivityTimeoutInMinutes mediante un módulo de PowerShell.

Para obtener más información sobre cómo configurar InactivityTimeoutInMinutes, consulte la sección Tiempo de espera por inactividad para la aplicación Citrix Workspace.

Puede enviar sus comentarios sobre esta Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Disponible en coreano

Ahora la aplicación Citrix Workspace para Linux está disponible en coreano.

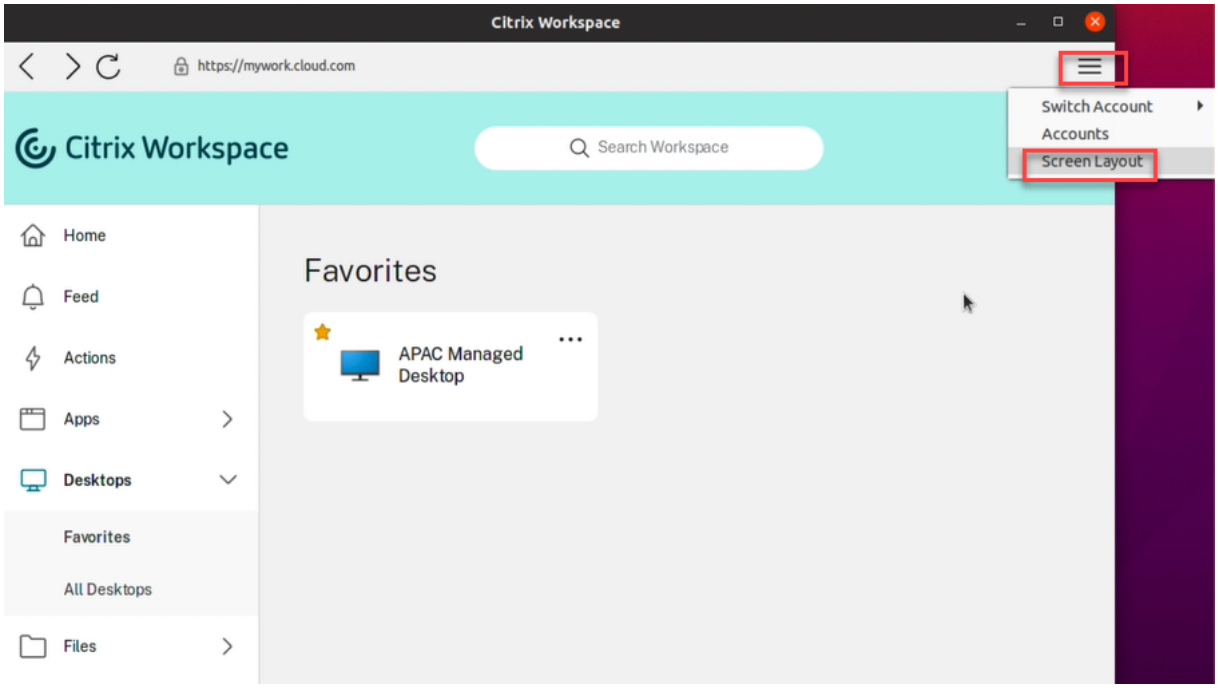
Anclaje de pantallas en almacenes web personalizados [Technical Preview]

A partir de la versión 2302, puede guardar la selección para el diseño de pantalla con varios monitores en almacenes web personalizados.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
<key>ScreenPinEnabled</key>
<value> true </value>
<!--NeedCopy-->
```

Una vez agregada la clave anterior, podrá ver la opción **Diseño de pantalla** en el menú de la aplicación Citrix Workspace.



Para obtener más información, consulte la sección Anclaje de pantallas en almacenes web personalizados [Technical Preview].

Puede enviar sus comentarios sobre esta Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Optimización del rendimiento de la aplicación Citrix Workspace

A partir de esta versión, el rendimiento de la aplicación Citrix Workspace para Linux mejora al autenticarse mediante AuthmanLite.

Problemas resueltos

- Es posible que sufra un conflicto entre ctxlogd.service de la aplicación Citrix Workspace para Linux y ctxlogd.service de Linux VDA. [HDX-44569]
- Es posible que no pueda aplicar correctamente imágenes de fondo en reuniones de Microsoft Teams optimizado. Este problema se produce en sistemas operativos específicos, incluido el sistema operativo HP ThinPro. [HDX-47166]

2212

Novedades

Compatibilidad con cursor de 32 bits [Technical Preview]

Anteriormente, cuando se utilizaba el cursor personalizado de 32 bits, podía aparecer un cuadro negro alrededor del mismo. Con esta versión, la aplicación Citrix Workspace para Linux admite el cursor de 32 bits. De este modo se ha resuelto el problema del cuadro negro que aparecía alrededor del cursor.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Adición de un mecanismo de búfer de vibración del lado del cliente [Technical Preview]

Esta función garantiza un audio fluido incluso cuando la latencia de la red fluctúa. De forma predeterminada, esta función está inhabilitada.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya al archivo de configuración `/opt/Citrix/ICAClient/config/module.ini` y modifíquelo.
2. Inhabilite el control de latencia de audio de la siguiente manera:

```
`AudioLatencyControlEnabled = FALSE`
```

3. Habilite el búfer de vibración de la siguiente manera:

```
`JitterBufferEnabled = TRUE`
```

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Compatibilidad con varios dispositivos de audio

A partir de esta versión, la aplicación Citrix Workspace muestra todos los dispositivos de audio locales disponibles en una sesión con sus nombres. Además, también se admite la funcionalidad plug-and-play.

La funcionalidad de redireccionamiento de varios dispositivos de audio está habilitada de forma predeterminada. Para inhabilitar esta función, establezca el valor de `AudioRedirectionV4` en False en el archivo module.ini.

Compatibilidad con la grabación de audio

A partir de esta versión, la funcionalidad de grabación de audio está habilitada de forma predeterminada. Los dispositivos para grabar audio aparecen cuando se inicia una sesión.

Para inhabilitar esta función, establezca el valor de `AllowAudioInput` en False en el archivo wfclient.ini.

Desenfoque y reemplazo de fondo para Teams optimizado por Citrix [Technical Preview]

Requisito previo:

Asegúrese de haber instalado wget.

Teams optimizado por Citrix en la aplicación Citrix Workspace para Linux ahora admite el desenfoque y el reemplazo de fondo. Para usar esta función, seleccione **More** > **Apply Background Effects** cuando esté en una reunión o en una llamada punto a punto (P2P).

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Problemas resueltos

- Es posible que no encuentre un certificado de tarjeta inteligente válido después de retirar la tarjeta inteligente y volver a insertarla. [CVADHELP-20787]
- Es posible que no pueda iniciar sesión en la aplicación Citrix Workspace con la tarjeta inteligente TicTok. [CVADHELP-20578]

- Es posible que no pueda iniciar sesión en la aplicación Citrix Workspace con una tarjeta inteligente de IDEMIA. [CVADHELP-20652]
- Es posible que la aplicación Citrix Workspace deje de responder cuando la redirección de audio utilice el códec Speex con varios dispositivos de audio habilitados. [CVADHELP-21212]
- Al cerrar sesión en la aplicación Citrix Workspace e iniciar sesión de nuevo, la aplicación Citrix Workspace se inicia sin introducir las credenciales de inicio de sesión. Este problema solo se produce en implementaciones de la nube y si el valor del parámetro `longLivedTokenSupport` está establecido en *True*. [RFLNX-9160]
- Es posible que aparezcan mensajes de error de ID de transacción al iniciar una sesión. Por ejemplo: "The option '-transactionid' is invalid". [HDX-45618]
- Al instalar la aplicación Citrix Workspace e iniciar la sesión con privilegios de "root", es posible que la sesión se cierre. [HDX-46967]
- Al instalar e iniciar la aplicación Citrix Workspace, es posible que aparezca este mensaje de error:

  "The X request 130.1 caused error:"10: BadAccess(Attempt to access private resource denied". [HDX-44416]

2211

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

- Es posible que el VDA se cierre de forma inesperada después de redirigir la interfaz de audio del dispositivo. Este problema se produce al habilitar la directiva "Redirección de dispositivos USB del cliente" en el DDC y al conectar dispositivos USB compuestos al dispositivo de punto final, como los auriculares USB con micrófono. [HDX-44117]
- Es posible que el teclado QWERTY de Bloomberg 4 se quede bloqueado en la sesión después de utilizar la redirección de USB. [HDX-44555]
- Es posible que no pueda registrar ni utilizar sus dispositivos YubiKey con el código PIN en la aplicación Citrix Workspace. [HDX-44951]
- Cuando el proceso snap-store se ejecuta en segundo plano, es posible que no pueda iniciar aplicaciones y escritorios protegidos. [APPP-110]

2209

Novedades

Función de autenticación mediante FIDO2 [Tech Preview]

Con esta versión, puede autenticarse dentro de una sesión de HDX mediante claves de seguridad FIDO2 sin contraseña. Las claves de seguridad FIDO2 ofrecen un modo intuitivo de autenticación para empleados corporativos en aplicaciones o escritorios compatibles con FIDO2 sin necesidad de introducir un nombre de usuario o una contraseña. Para obtener más información sobre FIDO2, consulte Autenticación FIDO2.

> **Nota:**
>
> Si utiliza el dispositivo FIDO2 mediante la redirección de USB, quite la regla de redirección de USB de su dispositivo FIDO2 del archivo `usb.conf` de la carpeta `$ICAROOT/`. Esta actualización le ayuda a cambiar al canal virtual FIDO2.

De forma predeterminada, la autenticación FIDO2 está inhabilitada. Para habilitar la autenticación FIDO2, haga lo siguiente:

1. Vaya al archivo `<ICAROOT>/config/module.ini`.
2. Vaya a la sección ICA 3.0.
3. Defina `FIDO2= On`.

Esta función admite actualmente autenticadores móviles (solo USB) con código PIN y funciones táctiles. Puede configurar la autenticación basada en claves de seguridad FIDO2. Para obtener información sobre los requisitos previos y el uso de esta función, consulte Autorización local y autenticación virtual mediante FIDO2.

Al acceder a una aplicación o un sitio web que admite FIDO2, aparece un mensaje que solicita acceso a la clave de seguridad. Si ya registró su clave de seguridad con un PIN (como mínimo, 4 caracteres, y como máximo, 64), debe introducir el PIN al iniciar sesión.

Si ya registró su clave de seguridad sin un PIN, solo tiene que tocar la clave de seguridad para iniciar sesión.

Limitación:

Es posible que no pueda registrar el segundo dispositivo en una misma cuenta mediante la autenticación FIDO2.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios

> en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Mejoras en el modo de entrada del teclado [Technical Preview]

Antes solo podía habilitar diferentes modos de entrada del teclado al actualizar el valor de `KeyboardEventMode` en el archivo de configuración. No había ninguna opción de interfaz de usuario para seleccionar el modo de entrada del teclado.

A partir de la aplicación Citrix Workspace 2209, puede configurar diferentes modos de entrada del teclado desde la sección **Parámetros del modo de entrada de teclado** recientemente incorporada. Puede seleccionar **Scancode** o **Unicode** como modo de entrada del teclado.

Para obtener más información, consulte **Mejoras en el modo de entrada del teclado** de la documentación sobre Sincronización de la distribución del teclado.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Compatibilidad con distribuciones de teclado extendido [Technical Preview]

A partir de la versión 2209 de la aplicación Citrix Workspace, el modo de entrada de teclado Scancode admite estas distribuciones de teclado extendido:

- Teclado 106 japonés
- Teclados ABNT/ABNT2 portugueses
- Teclados multimedia

El modo de entrada de teclado Scancode admite las distribuciones de teclado extendidas junto con todos los modos de sincronización de distribución del teclado.

Esta funcionalidad está habilitada de forma predeterminada.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios

> en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Mejoras de Microsoft Teams

- **Uso compartido de aplicaciones habilitado:** A partir de la aplicación Citrix Workspace 2209 para Linux y Citrix Virtual Apps and Desktops 2109, puede compartir una aplicación mediante la función de compartir pantalla de Microsoft Teams.
- **Mejoras en la compatibilidad con un nivel elevado de PPP:** Cuando la función de PPP elevado está habilitada y usa monitores 4K, las superposiciones de vídeo de Microsoft Teams están en la posición adecuada y tienen el tamaño correcto. Independientemente de los parámetros de la pantalla, como la disposición de uno o varios monitores, las superposiciones siempre aparecen correctamente y no se amplían ni aparecen en posiciones no deseadas. Para habilitar esta mejora, asegúrese de que el parámetro `DPIMatchingEnabled` del archivo de configuración `wfclient.ini` esté establecido en **True**. Para obtener más información, consulte Compatibilidad con la correspondencia de PPP.
- **Actualización de la versión del SDK de WebRTC:** La versión del SDK de WebRTC que se utiliza para Microsoft Teams optimizado se actualizó a la versión M98.

Versión mejorada de las bibliotecas de compatibilidad

A partir de esta versión, la aplicación Citrix Workspace para Linux es compatible con estas bibliotecas:

- `glibc` 2.27 o una versión posterior
- `glibcxx` 3.4.25 o una versión posterior

Actualización de protección de aplicaciones

> **Nota:**
>
> La protección de aplicaciones no es compatible con Ubuntu 22.04. Como resultado, si instala el módulo de protección de aplicaciones en Ubuntu 22.04, es posible que no pueda iniciar aplicaciones ni escritorios virtuales en la aplicación Citrix Workspace. Para obtener más información sobre la protección de aplicaciones, consulte Protección de aplicaciones.

Problemas resueltos

- Cuando la función de protección de aplicaciones está habilitada, es posible que la protección contra el registro de tecleo no funcione para la interfaz de Authentication Manager, que carga la página web en una ventana independiente. [RFLNX-9004]

- Tras actualizar la versión de la aplicación Citrix Workspace a la versión 2007 para Linux, es posible que agregar un almacén mediante Storebrowse lleve mucho tiempo, ya que el almacén intenta contactar con el servicio de configuración de aplicaciones, al que no se puede acceder. [CVADHELP-20618]
- Al conectarse a un almacén de la nube desde la interfaz de usuario de autoservicio, es posible que aparezca una rueda giratoria en la página de inicio de sesión. [CVADHELP-20039]
- Al iniciar dos aplicaciones de dos grupos de entrega diferentes, es posible que se produzca una demora al iniciar la segunda aplicación. [CVADHELP-18198]

2207

Novedades

Mejora en la calidad del audio

Antes, el valor máximo del búfer de salida para reproducir audio sin problemas era de 200 ms en la aplicación Citrix Workspace. Debido a este conjunto de valores, se agregó una latencia de 200 ms en los casos de reproducción. Este valor máximo de búfer de salida también tenía un impacto en las aplicaciones de audio interactivo.

Con esta mejora, el valor máximo de búfer de salida se reduce a 50 ms en la aplicación Citrix Workspace. Como resultado, mejora la experiencia del usuario en la aplicación de audio interactivo. Además, el tiempo de ida y vuelta (RTT) se reduce en 150 ms.

A partir de esta versión, puede seleccionar el umbral de reproducción y el prebúfer de audio por pulsos adecuados para mejorar la calidad del audio. Para esta mejora, se agregan estos parámetros en la sección [ClientAudio] del archivo `module.ini`:

- `PlaybackDelayThreshV4`: Especificar el nivel inicial de búfer de salida en milisegundos. La aplicación Citrix Workspace intenta mantener este nivel de almacenamiento en búfer durante toda la sesión. El valor predeterminado de `PlaybackDelayThreshV4` es de 50 ms. Este parámetro solo es válido cuando `AudioRedirectionV4` se establece en **True**.
- `AudioTempLatencyBoostV4`: Cuando el procesamiento de audio sufre un pico repentino o no tiene un nivel suficiente para una red inestable, este valor aumenta el valor del búfer de salida. Este aumento en el valor del búfer de salida proporciona una calidad de audio fluida. Sin embargo, es posible que el audio se retrase un poco. El valor predeterminado de `AudioTempLatencyBoostV4` se establece en 100 ms. Este parámetro solo es válido cuando `AudioRedirectionV4` se establece en **True** y `AudioLatencyControlEnabled` en **True**. De forma predeterminada, el valor de `AudioLatencyControlEnabled` se establece en True.

Para obtener más información sobre cómo habilitar esta mejora, consulte la sección **Mejora en pro de la calidad del audio** de la documentación de Audio.

Compatibilidad con la correspondencia de PPP [Technical Preview]

Con esta versión, los valores de resolución de pantalla y escala de PPP establecidos en la aplicación Citrix Workspace se corresponden con los valores respectivos en la sesión de aplicaciones y escritorios virtuales. Puede establecer el valor de escala requerido en el cliente Linux y el escalado de la sesión del VDA se actualizará automáticamente.

El escalado de PPP se utiliza principalmente con monitores de gran tamaño y alta resolución. Esta función ayuda a mostrar los elementos siguientes a un tamaño que permite verlos cómodamente:

- Aplicaciones
- Texto
- Imágenes
- Otros elementos gráficos

Limitación:

Actualmente, la funcionalidad de correspondencia de PPP no admite el escalado fraccional en el lado del cliente. Si el valor de la escala de PPP es elevado, es posible que la optimización de Microsoft Teams no funcione como es debido.

Para obtener más información sobre cómo habilitar esta funcionalidad, consulte Compatibilidad con la correspondencia de PPP.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Redirección de dispositivos USB compuestos

A partir de esta versión, la aplicación Citrix Workspace permite dividir dispositivos USB compuestos. Un dispositivo USB compuesto puede realizar más de una función. Esto se logra mediante la exposición de cada una de esas funciones desde interfaces diferentes. Ejemplos de dispositivos USB compuestos incluyen dispositivos HID que cuentan con entrada y salida de audio y vídeo.

Actualmente, la redirección de dispositivos USB compuestos solo está disponible en la sesión de escritorio. Los dispositivos divididos aparecen en Desktop Viewer.

Antes, cuando un dispositivo se desconectaba y conectaba durante una sesión, se redirigía automáticamente. Como resultado, se conectaba automáticamente al VDA. Con esta versión, debe habilitar

manualmente la redirección automática a través de los parámetros del archivo de configuración. La redirección automática de dispositivos USB compuestos está inhabilitada de forma predeterminada.

Para obtener más información sobre cómo configurar la redirección de dispositivos USB compuestos, consulte la sección **Redirección de dispositivos USB compuestos** en la documentación de USB.

Función de eliminación de eco de audio mejorada [Tech Preview]

A partir de esta versión, la aplicación Citrix Workspace admite la eliminación de eco. Esta función está diseñada para casos de usuario con audio en tiempo real y mejora la experiencia del usuario. La función de eliminación de eco opera con audio de calidad baja, calidad media y adaptable. Para obtener un rendimiento óptimo, Citrix recomienda usar audio adaptable.

De forma predeterminada, la función de eliminación de eco está inhabilitada. Durante los casos de usuario con audio en tiempo real, se recomienda activar la eliminación de eco si se utiliza el altavoz en lugar de los auriculares.

Limitación:

Por diseño, la función de eliminación de eco está inhabilitada para proporcionar audio de alta calidad.

Para obtener más información, consulte la sección **Función de eliminación de eco de audio mejorada** en la documentación de Audio .

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Compatibilidad con timbre secundario

Puede utilizar la función de timbre secundario para seleccionar un dispositivo secundario en el que recibir la notificación de llamada entrante cuando Microsoft Teams está optimizado (Citrix HDX optimizado en Acerca de/Versión). Por ejemplo, considere que ha establecido un altavoz como timbre secundario y que su dispositivo de punto final está conectado a los auriculares. En este caso, Microsoft Teams envía la señal de llamada entrante al altavoz aunque los auriculares sean el periférico principal para la llamada de audio. No se puede establecer un timbre secundario en los siguientes casos:

- Cuando no se ha conectado a más de un dispositivo de audio
- Si el periférico no está disponible (por ejemplo, auriculares Bluetooth)

> **Nota:**
>
> Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Para saber cuándo implementa Microsoft la actualización, consulte el Plan de desarrollo de Microsoft 365. También puede consultar CTX253754 para obtener la actualización de la documentación y el anuncio.

Problemas resueltos

- Al iniciar un escritorio en modo de pantalla completa con Lightweight X11 Desktop Environment (LXDE) y desconectar de la red, aparece un mensaje de **error de pérdida de conexión con < XXX>** que incluye una opción **Salir** en el cuadro de diálogo. El mensaje aparece si la directiva Reconexión automática de clientes (ACR) o Fiabilidad de la sesión (SR) han caducado. Al hacer clic en **Salir**, el escritorio del usuario desaparece. Sin embargo, si se hace clic en cualquier otro lugar de la pantalla, es posible que el botón **Salir** no aparezca en el cuadro de diálogo. Debe salir manualmente del escritorio del usuario pulsando la tecla **Esc** o **Intro**. [CVADHELP-17478]
- La aplicación Citrix Workspace para Linux puede interpretar las URL que contienen la cadena **cloud** (por ejemplo, <*xxx-yyy-cloud.com*>) como URL de dominio de nube, incluso si representan URL locales. [CVADHELP-19480]
- Es posible que la sesión se desconecte mientras intenta usar la cámara web HDX. El problema solo se produce en la versión 2203 del VDA. [CVADHELP-20223]
- Podría producirse un error al copiar y pegar contenido entre aplicaciones publicadas, sesiones de VDI o una sesión de VDI y una aplicación publicada. Es posible que la sesión o la aplicación dejen de responder durante algún tiempo. [CVADHELP-19899]
- Es posible que tenga problemas en la desconexión de sesiones al conectarse a través de dispositivos de punto final con la versión 2205 de la aplicación Citrix Workspace para Linux. Este problema se produce si configura la pantalla de bloqueo con la configuración de directiva **Forzar una imagen de pantalla de bloqueo predeterminada específica** con ciertos tipos de archivos JPEG y la aplica a Citrix VDA 2203. [CVADHELP-21572]
- Al previsualizar un vídeo con una cámara web en Skype, es posible que la vista previa muestre una pantalla en negro. [HDX-37860]
- La compresión de vídeo de cámara web HDX RealTime no admite cámaras con formato de vídeo MJPEG en la aplicación Citrix Workspace. [HDX-40352]
- Mientras comparte la pantalla o una aplicación durante llamadas de Microsoft Teams, es posible que sus compañeros vean artefactos visuales. Este problema se produce por velocidades de fotogramas inestables, como una reproducción de vídeo incorrecta (fotogramas negros congelados o transitorios). Esta versión incluye velocidades de fotogramas o de muestreo mejoradas que ayudan a reducir los artefactos visuales. [HDX-38032]
- Es posible que el vídeo o la imagen de la aplicación Citrix Workspace no se representen correctamente. Este problema se produce cuando se utiliza la aplicación Citrix Workspace junto con

la versión 2109 del VDA o una posterior. [HDX-40287]

- Al iniciar wfica con el comando `-span o`, es posible que la sesión no se inicie y abarque todos los monitores disponibles. Del mismo modo, al iniciar wfica con el comando `-span h`, es posible que no se imprima la lista de los monitores conectados actualmente al dispositivo del usuario. [HDX-32519]
- Al iniciar wfica con el comando `-span o`, es posible que la sesión no se inicie y abarque todos los monitores disponibles. Del mismo modo, al iniciar wfica con el comando `-span h`, es posible que no se imprima la lista de los monitores conectados actualmente al dispositivo del usuario. Para obtener más información, consulte la referencia de comandos. [HDX-32519]
- Cuando se produce un error de SSL en un protocolo durante un intento de conexión TCP y EDT/UDP, es posible que las dos conexiones fallen debido a la condición de carrera. Este error de SSL puede producirse si la configuración de TLS difiere entre los protocolos y el cliente no puede conectarse a través de un protocolo. [RFLNX-8747]
- Cuando intenta conectarse de forma remota a una máquina que tiene instalada la aplicación Citrix Workspace con protección de aplicaciones, el servidor x11vnc se cierra de forma inesperada y la conexión falla. Como resultado, es posible que no pueda conectarse remotamente a la máquina a través del servidor x11vnc. [RFLNX-8933]
- Al agregar un almacén con los parámetros predeterminados, es posible que la enumeración de Storebrowse falle. Este problema solo ocurre en el sistema operativo Debian de 32 bits. [RFLNX-8743]
- Es posible que reciba un mensaje de error al instalar la aplicación Citrix Workspace con la función de protección de aplicaciones habilitada en máquinas Linux de 32 bits. [RFLNX-8809]
- Al agregar un almacén con el comando `storebrowse -a` y hacer una enumeración con el comando `storebrowse -E`, es posible que la enumeración de Storebrowse falle. Este problema solo ocurre en el sistema operativo Raspberry Pi. [RFLNX-8803]

2205

Novedades

Mejora de la autenticación para Storebrowse

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

A partir de esta versión, el cuadro de diálogo de autenticación está presente en la aplicación Citrix Workspace y los detalles del almacén se muestran en la pantalla de inicio de sesión. Esta función ofrece una mejor experiencia de usuario. Los tokens de autenticación se cifran y se almacenan para que no tenga que introducir credenciales de nuevo cuando se reinicie el sistema o la sesión.

También puede activar o desactivar la mejora de la autenticación para la función Storebrowse con la

clave `StorebrowseIPC` del archivo `AuthmanConfig.xml`. De forma predeterminada, la funcionalidad del botón para activar/desactivar está inhabilitada.

La mejora de la autenticación permite usar storebrowse para estas operaciones:

- Storebrowse -E: Enumera los recursos disponibles.
- Storebrowse -L: Inicia una conexión con un recurso publicado.
- Storebrowse -S: Muestra los recursos suscritos.
- Storebrowse -T: Cierra todas las sesiones del almacén especificado.
- Storebrowse -Wr: Conecta de nuevo las sesiones desconectadas, pero todavía activas, del almacén especificado. La opción [r] conecta de nuevo todas las sesiones desconectadas.
- storebrowse -WR: Conecta de nuevo las sesiones desconectadas, pero todavía activas, del almacén especificado. La opción [R] conecta de nuevo todas las sesiones activas y desconectadas.
- Storebrowse -s: Suscribe el recurso especificado de un almacén.
- Storebrowse -u: Cancela la suscripción del recurso especificado de un almacén.
- Storebrowse -q: Inicia una aplicación mediante la URL directa. Este comando solo funciona para almacenes de StoreFront.

> **Nota:**
>
> - Puede seguir utilizando los comandos de storebrowse restantes como se usaban antes (con AuthManagerDaemon).
> - La mejora de la autenticación solo se aplica a las implementaciones de la nube.
> - Con esta mejora, se admite la función de inicio de sesión persistente.

Para obtener más información, consulte Mejora de la autenticación.

Inicio de sesión persistente [Technical Preview]

La función de inicio de sesión persistente le permite mantener la sesión iniciada el período (de 2 a 365 días) configurado por su administrador. Cuando esta función está habilitada, no necesita proporcionar las credenciales de inicio de sesión para la aplicación Citrix Workspace durante el período configurado.

Con esta funcionalidad, las sesiones de SSO en Citrix DaaS se prolongan hasta 365 días. Esta ampliación se basa en el tiempo de vida de los tokens de larga duración. Sus credenciales se almacenan en la caché de forma predeterminada durante 4 días o la duración definida, lo que sea inferior. Y, luego, se prolonga cuando hay actividad de nuevo dentro de estos 4 días al conectarse a la aplicación Citrix Workspace.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de

> producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Para obtener más información, consulte Inicio de sesión persistente.

Detección automática de almacenes por dirección de correo electrónico

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

Ya puede proporcionar su dirección de correo electrónico en la aplicación Citrix Workspace para detectar automáticamente el almacén asociado a esa dirección de correo electrónico. Si hay varios almacenes asociados a un dominio, de forma predeterminada se agrega el primer almacén devuelto por Global App Configuration Service como el almacén elegido. Los usuarios siempre pueden cambiar a otro almacén si fuera necesario.

Para obtener más información, consulte la sección **Detección automática de almacenes por dirección de correo electrónico** en la documentación de Agregar URL de almacén a la aplicación Citrix Workspace.

Disposición para inhabilitar el servicio de LaunchDarkly

A partir de esta versión, puede inhabilitar el servicio de LaunchDarkly en la aplicación Citrix Workspace.

Para obtener más información, consulte la documentación de Administrar marcas de función.

Problemas resueltos

- Es posible que el servidor DNS de un entorno de cliente con acceso limitado a Internet no resuelva la URL `clientstream.launchdarkly.com`. Como resultado, la aplicación Citrix Workspace envía una gran cantidad de consultas DNS (más de 1000 en 3 segundos al día) a la URL. [CVADHELP-19559]
- Cuando la función de protección de aplicaciones está habilitada, es posible que la protección contra el registro de tecleo no funcione para la interfaz de Authentication Manager que usa la biblioteca `UIDialogLibWebKit3.so`. Este problema se ha resuelto en entornos de escritorio gnome y kde. [RFLNX-8027]
- Es posible que, al intentar imprimir desde una sesión de VDA activa en un cliente armhf de la versión 3 o 4 de Raspberry Pi, la sesión deje de responder. [CVADHELP-18506]

- Al iniciar la interfaz de usuario de autoservicio con los parámetros predeterminados, es posible que aparezca este mensaje de error:

  "Response for Secondary Token request is not 200/400/404 42".

  Este problema se produce en Fedora 35. [RFLNX-8603]

2203

Novedades

Compatibilidad con IPv6 de EDT

A partir de esta versión, la aplicación Citrix Workspace admite IPv6 de EDT.

Compatibilidad con la versión 1.3 del protocolo TLS

A partir de esta versión, la aplicación Citrix Workspace admite la versión 1.3 del protocolo Transport Layer Security (TLS).
Para obtener más información, consulte TLS.

Almacenes web personalizados

A partir de la versión 2203, esta función está disponible de forma general para la aplicación Citrix Workspace. Puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace.

> **Nota:**
>
> La función para anclar el diseño de pantalla con varios monitores no está disponible en el almacén web personalizado.

Para obtener más información, consulte Almacenes web personalizados.

Función experimental de mejora de la autenticación

A partir de esta versión, la mejora de la autenticación permite usar storebrowse para estas operaciones:

- Storebrowse -E para enumerar los recursos disponibles.
- Storebrowse -L para iniciar una conexión con un recurso publicado.
- Storebrowse -S para mostrar los recursos suscritos.

> **Nota:**
>
> Puede seguir utilizando los comandos de storebrowse restantes en `AuthMangerDaemon`, y en la

> próxima versión se aceptará la mejora de la autenticación.

Para obtener más información, consulte Mejora de la autenticación para Storebrowse.

Mejora de la sincronización de la distribución de teclado

La sincronización de la distribución del teclado le permite cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada. Al habilitarse, la distribución del teclado del cliente se sincroniza automáticamente con la sesión de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

A partir de la versión 2203, la aplicación Citrix Workspace ofrece estos tres modos de sincronización de la distribución del teclado:

- **Sincronizar solo una vez, cuando se inicia la sesión**: Según el valor de `KeyboardLayout` en el archivo `wfclient.ini`, la distribución del teclado del cliente se sincroniza con la del servidor cuando se inicia la sesión. Si el valor de `KeyboardLayout` es `0`, el teclado del sistema se sincroniza con el VDA. Si el valor de `KeyboardLayout` se establece en un idioma específico, el teclado del idioma se sincroniza con el VDA. Los cambios que haga en la distribución del teclado del cliente durante la sesión no surtirán efecto inmediatamente. Para aplicar los cambios, cierre la sesión de la aplicación e inicie sesión de nuevo. El modo **Sincronizar solo una vez: al iniciarse la sesión** es la distribución de teclado predeterminada seleccionada para la aplicación Citrix Workspace.
- **Permitir sincronización dinámica**: Esta opción sincroniza la distribución del teclado del cliente con el servidor al cambiar la distribución del teclado del cliente.
- **No sincronizar**: Indica que el cliente utiliza la distribución del teclado presente en el servidor.

Para obtener más información, consulte Sincronizar la distribución del teclado.

Chat y reuniones multiventana para Microsoft Teams

Puede usar varias ventanas para reuniones y chats en Microsoft Teams con la optimización de HDX en Citrix Virtual Apps and Desktops 2112 o una versión posterior. Puede separar las conversaciones o las reuniones de varias maneras. Para obtener detalles sobre la función de ventana emergente, consulte Teams Pop-Out Windows for Chats and Meetings.

Si utiliza una versión anterior de la aplicación Citrix Workspace o Virtual Delivery Agent (VDA), recuerde que Microsoft retirará el código de las ventanas únicas en el futuro. Sin embargo, puede actualizar el VDA o la aplicación Citrix Workspace a una versión que admita varias ventanas (2203 o una versión posterior). Para actualizarlos a una versión posterior, dispondrá de un mínimo de 9 meses después de que esta función esté disponible de forma general.

> **Nota:**
>
> Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

Mejora de la redirección automática de dispositivos USB

Antes, cuando un dispositivo se desconectaba y conectaba durante una sesión, se redirigía automáticamente. Como resultado, se conectaba automáticamente al VDA. Con esta versión, debe habilitar manualmente la redirección automática a través de los parámetros del archivo de configuración. La redirección automática de dispositivos USB está inhabilitada de forma predeterminada. Para obtener más información, consulte la sección USB.

Problemas resueltos

- Al agregar un almacén y autenticarlo en la aplicación Citrix Workspace, la ventana de autenticación se carga por segunda vez aunque la autenticación sea correcta. Este problema se produce cuando inicia sesión por primera vez en la aplicación Citrix Workspace después de establecer `AuthManLiteEnabled` en **True**. [RFLNX-8694]
- Después de instalar la aplicación Citrix Workspace con la función de protección de aplicaciones habilitada en un SO que utiliza `glibc 2.34` o una versión posterior, es posible que, al reiniciar el sistema, el SO no arranque. [RFLNX-8358]
- Al usar Microsoft Teams para asistir a una reunión o realizar una llamada entre dos usuarios y tener que esperar un tiempo, es posible que la carga de un núcleo de CPU aumente al 100 % por un error de socket. [HDX-38974]
- La aplicación Citrix Workspace no es compatible con la nueva versión de Raspberry Pi OS basada en Debian Bullseye. [HDX-37000]
- Al iniciar una sesión con el archivo ICA y cerrar la sesión, el valor de retorno esperado que recibe de la línea de comandos `wfica` es 0. Sin embargo, en lugar del valor esperado, el valor que recibe es 2. Este problema se produce a partir de la versión 2106 de la aplicación Citrix Workspace. [HDX-38916]
- En la aplicación Citrix Workspace, es posible que se produzcan errores intermitentes al responder o realizar llamadas de Microsoft Teams. Aparece el siguiente mensaje de error:

  “No se pudo establecer la llamada”.

  [HDX-38819]

2202

Novedades en la versión 2202

Audio UDP a través de Citrix Gateway

> **Nota:**
>
> Esta mejora está generalmente disponible en la aplicación Citrix Workspace.

A partir de esta versión, la aplicación Citrix Workspace admite el protocolo de seguridad Datagram Transport Layer Security (DTLS) para audio UDP. Como resultado, puede acceder al audio UDP a través de Citrix Gateway.

Para habilitar el audio UDP mediante Citrix Gateway:

1. Vaya a la carpeta <ICAROOT>/config y abra el archivo module.ini.
2. Vaya a la sección [WFClient] y configure esta entrada:

   EnableUDPThroughGateway=True
3. Vaya a la sección [ClientAudio] y configure esta entrada:

   EnableUDPAudio=True

Para obtener más información, consulte la sección **Habilitar el audio UDP** de la documentación de Audio.

> **Nota:**
>
> Si usa la configuración de default.ica de StoreFront, el valor de EnableUDPThroughGateway establecido en la sección [Application] tiene prioridad sobre el valor establecido en el archivo module.ini. Sin embargo, puede establecer el valor EnableUDPAudio de la sección [ClientAudio] solo con el archivo module.ini. Además, no tiene prioridad sobre el valor establecido en la configuración de default.ica de StoreFront.

Problemas resueltos

- Al instalar la aplicación Citrix Workspace, agregar un almacén e iniciar un escritorio, es posible que no aparezca la ventana de la sesión. Este problema se produce si la biblioteca libpcscd no está instalada en Ubuntu 16.04. [HDX-36574]
- En la aplicación Citrix Workspace 2112, es posible que vea un uso elevado de la CPU en el dispositivo de punto final cuando una cámara web está encendida en videollamadas de Microsoft Teams optimizado. [HDX-37168]
- Tiene problemas de rendimiento debido a la utilización del 100% de la CPU. [RFLNX-8200]

- En una sesión de escritorio iniciada mediante la interfaz gráfica de usuario de autoservicio, es posible que, al guardar el diseño de la sesión actual con el botón **Guardar diseño** de la barra de herramientas de **Desktop Viewer**, se produzca un error con este mensaje:

  "No se puede guardar la distribución de la sesión".

  Sin embargo, el diseño de la sesión se puede restaurar durante la siguiente reconexión de sesión.
  [CVADHELP-18971]

- Es posible que no se creen carpetas o archivos en unidades asignadas mediante la asignación de unidades del cliente en VDA con Windows que se ejecutan en versiones más recientes de sistemas operativos cliente con este mensaje de error:

  "You need permission to perform this action".
  Los sistemas operativos pueden ser Ubuntu 21.04 y Fedora 34 o versiones posteriores.
  [CVADHELP-18448]

- Es posible que el servidor DNS de un entorno de cliente con acceso limitado a Internet no resuelva la URL `clientstream.launchdarkly.com`. Como resultado, la aplicación Citrix Workspace para Linux envía consultas DNS a la URL de forma constante. Es posible que esta acción provoque millones de consultas DNS para cientos de clientes Linux en línea, lo que desconectaría el servidor DNS. [CVADHELP-19140]

  > **Nota:**
  >
  > Es posible que las consultas de DNS a los sitios relacionados con LaunchDarkly se envíen durante tres segundos al día.

2112

Novedades en la versión 2112

Función para invertir el color del cursor

Antes, la aplicación Citrix Workspace mostraba un cursor punteado con el mismo color que el fondo blanco y negro de un texto. Como consecuencia, era difícil ubicar la posición del cursor.

A partir de esta versión, el color del cursor se invierte en función del color de fondo del texto. Así, puede ubicar fácilmente la posición del cursor en el texto. De forma predeterminada, esta función está inhabilitada.

Requisitos previos:

- Si `.ICAClient` ya está presente en la carpeta de inicio del usuario actual:

  Elimine el archivo `All_Regions.ini`.

  O bien:

Para conservar el archivo `All_Regions.ini`, agregue estas líneas al final de la sección [Virtual Channels\Thinwire Graphics]:

InvertCursorEnabled=

InvertCursorRefreshRate=

InvertCursorMode=

Si la carpeta `.ICAClient` no está presente, entonces es que indica una nueva instalación de la aplicación Citrix Workspace. En ese caso, se conserva la configuración predeterminada para la función.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya al archivo de configuración `$HOME/.ICAClient/wfclient.ini`.
2. Vaya a la sección [Thinwire3.0] y configure esta entrada:

   InvertCursorEnabled=True

> **Nota:**
>
> El cursor no se invierte cuando el valor de la directiva **Usar códec de vídeo para compresión** en Citrix Studio está establecido en **No usar códec de vídeo**.

Actualización de audio adaptable

Ahora el audio adaptable funciona cuando se usa la entrega de audio del protocolo User Datagram Protocol (UDP). Para obtener más información, consulte Audio adaptable.

> **Nota:**
>
> Esta mejora requiere la versión 2112 de VDA o una posterior.

Para obtener información sobre la configuración del audio UDP mediante audio adaptable en la aplicación Citrix Workspace, consulte la sección **Habilitar el audio UDP** de la documentación de Audio.

Compatibilidad con varios dispositivos de audio [Technical Preview]

A partir de esta versión, la aplicación Citrix Workspace muestra todos los dispositivos de audio locales disponibles en una sesión con sus nombres. Además, también se permite conectar y usar directamente dispositivos de audio Bluetooth y HDMI.

> **Nota:**
>
> A partir de esta versión, se cambia el nombre del atributo `VdcamVersion4Support` del archivo `module.ini` a `AudioRedirectionV4`.

Esta función está inhabilitada de forma predeterminada. Para habilitar esta función, establezca el valor de `AudioRedirectionV4` en **True** en el archivo module.ini.

Para obtener más información, consulte Audio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Audio UDP a través de Citrix Gateway [Technical Preview]

A partir de esta versión, la aplicación Citrix Workspace admite el protocolo de seguridad Datagram Transport Layer Security (DTLS) para audio UDP. Como resultado, puede acceder al audio UDP a través de Citrix Gateway.

Para habilitar el audio UDP mediante Citrix Gateway:

1. Vaya a la carpeta <ICAROOT>/config y abra el archivo module.ini.
2. Vaya a la sección [WFClient] y configure esta entrada:

   EnableUDPThroughGateway=True
3. Vaya a la sección [ClientAudio] y configure esta entrada:

   EnableUDPAudio=True

> **Nota:**
>
> Si usa la configuración de default.ica de StoreFront, el valor de EnableUDPThroughGateway establecido en la sección [Application] tiene prioridad sobre el valor establecido en el archivo module.ini. Sin embargo, puede establecer el valor EnableUDPAudio en la sección [ClientAudio] solo con el archivo module.ini y no tiene prioridad sobre el valor establecido en la configuración de default.ica de StoreFront.

Para obtener más información, consulte la sección **Habilitar el audio UDP** de la documentación de Audio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Mejora en la compatibilidad con tarjetas inteligentes

> **Nota:**
>
> Esta mejora está generalmente disponible en la aplicación Citrix Workspace.

Con esta versión, la aplicación Citrix Workspace admite la funcionalidad Plug and Play para lectores de tarjetas inteligentes.

Al insertar una tarjeta inteligente, el lector de tarjetas inteligentes detecta la tarjeta inteligente en el servidor y en el cliente. Puede conectar y usar directamente varias tarjetas al mismo tiempo, y todas estas tarjetas se detectan.

Requisitos previos:

Instale la biblioteca `libpcscd` en el cliente Linux.

> **Nota:**
>
> Es posible que esta biblioteca se instale de forma predeterminada en las versiones recientes de la mayoría de las distribuciones de Linux. Sin embargo, es posible que deba instalar la biblioteca `libpcscd` en versiones anteriores de algunas distribuciones de Linux, como Ubuntu 1604.

Para inhabilitar esta mejora:

1. Vaya a la carpeta `<ICAROOT>/config/module.ini`.
2. Vaya a la sección `SmartCard`.
3. Configure esta opción: `DriverName=VDSCARD.DLL`.

Mejoras en la optimización de Microsoft Teams

> **Nota:**
>
> Estas funciones están disponibles solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

- **Solicitar control en Microsoft Teams**

En esta versión, durante una llamada de Microsoft Teams, puede solicitar el control cuando un participante comparte la pantalla. Una vez que tenga el control, puede realizar selecciones, modificaciones u otras acciones en la pantalla compartida.

Para tomar el control cuando se comparte una pantalla, haga clic en **Solicitar control** en la parte superior de la pantalla de Microsoft Teams. El participante de la reunión que comparte la pantalla puede aceptar o rechazar su solicitud.

Mientras tenga el control, puede realizar selecciones, modificaciones y otras acciones en la pantalla compartida. Cuando haya terminado, haga clic en **Liberar control**.

Limitaciones:

- Los usuarios de un cliente Linux no pueden *dar* el control a otros usuarios. En otras palabras, después de que el usuario del cliente Linux comience a compartir contenido, la opción **Dar control** no aparece en la barra de herramientas de uso compartido. Se trata de una limitación de Microsoft.
- La opción **Solicitar el control** no está disponible durante las llamadas de par a par entre los siguientes usuarios:
  - Un usuario optimizado
  - Un usuario del cliente de escritorio nativo de Microsoft Teams que se ejecute en el dispositivo de punto final.

  Como solución temporal, los usuarios pueden unirse a una reunión para obtener la opción **Solicitar el control**.
- **Compatibilidad con e911 dinámico**

Con esta versión, la aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, proporciona la capacidad de:

- configurar y redirigir llamadas de emergencia
- notificar al personal de seguridad

La notificación se proporciona en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams que se ejecuta en el VDA.

La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. A partir de la aplicación Citrix Workspace 2112 para Linux, la optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum. Para que esta función esté disponible, la biblioteca LLDP debe incluirse en la distribución del sistema operativo del cliente ligero.

Problemas resueltos

- Al reproducir vídeos largos, el audio se detiene, pero el vídeo continúa reproduciéndose normalmente. El problema se producía al establecer `VdcamVersion4Support` (ahora denominado `AudioRedirectionV4`) en **True**. [RFLNX-6472]
- Durante las llamadas de audio entre dos usuarios de Microsoft Teams, es posible que el audio no funcione durante los primeros 15 segundos de la llamada. [HDX-29526]
- Durante la sesión de pantalla compartida, el borde rojo que indica la pantalla compartida ocupa varias pantallas cuando Microsoft Teams se ejecuta en el modo integrado y en la configuración con varios monitores. [HDX-34978]

- Durante las videollamadas de Microsoft Teams, es posible que la cámara parpadee. [HDX-36345]
- Las sesiones de doble salto no admiten la funcionalidad Plug and Play para lectores de tarjetas inteligentes. [HDX-34582]
- Es posible que no se puedan iniciar sesiones mediante la autenticación con tarjeta inteligente. El problema se produce con la versión 2104 de la aplicación Citrix Workspace para Linux y versiones posteriores. [CVADHELP-18402]
- Es posible que la repetición de audio durante una sesión deteriore factores de rendimiento de la red, como el tiempo de ida y vuelta y la fiabilidad de la sesión. [CVADHELP-18723]
- Es posible que la aplicación Citrix Workspace 2106 y versiones posteriores instaladas en un cliente ligero fallen al conectarse al escritorio virtual con el códec Opus (ahora denominado audio adaptable) habilitado. Este problema se producía porque el archivo opus.dll integrado en el directorio `ICAClient` incluía el archivo opus lib creado en un repositorio diferente. Este archivo opus lib incluía el conjunto de instrucciones AVX-512 que no admite parte de la CPU del cliente ligero. [HDX-36440]
- Al conectarse a un almacén de la nube desde la interfaz de usuario de autoservicio, es posible que aparezca una rueda giratoria en la página de inicio de sesión. [RFLNX-8486]
- Después de iniciar sesión en la interfaz de usuario de autoservicio, es posible que se produzca un error al intentar finalizar el proceso de autoservicio mediante el comando `Killall selfservice` desde la línea de comandos. [RFLNX-8248]

2111

Novedades

Workspace con funciones inteligentes [Technical Preview]

Esta versión de la aplicación Citrix Workspace está optimizada para sacar partido de las funciones inteligentes de Workspace cuando se publiquen. Para obtener más información, consulte Funciones inteligentes de Workspace: Microaplicaciones.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Indicador de estado de la batería

Antes, el estado de la batería de los dispositivos no aparecía en el área de notificaciones de los VDA de servidor.

Con esta versión, sí se muestra el indicador de estado de la batería para los VDA de servidor.

Función de almacenes web personalizados [Technical Preview]

Con esta versión, puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace.

Para usar esta función, el administrador debe agregar el dominio o el almacén web personalizado a la lista de URL permitidas en Global App Configuration Service. Una vez agregada la URL, puede proporcionar la URL del almacén web personalizado en la pantalla **Agregar cuenta** de la aplicación Citrix Workspace. El almacén web personalizado se abre en la ventana de la aplicación Workspace nativa.

Para obtener más información sobre cómo configurar las direcciones URL de almacén web para los usuarios finales, consulte Global App Configuration Service.

Para quitar el almacén web personalizado, vaya a **Cuentas** > **Agregar o quitar cuentas**, seleccione la URL del almacén web personalizado y haga clic en **Quitar**.

Como requisito previo, debe habilitar el almacén web personalizado en el archivo `AuthManConfig.xml`. Para obtener más información, consulte Almacenes web personalizados.

> **Nota:**
>
> - Solo puede usar las URL que figuran en el archivo `AuthManConfig.xml` para el almacén web personalizado. Puede agregar diferentes direcciones URL al archivo `AuthManConfig.xml` que quiera tener en cuenta para el almacén web personalizado.
> - Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Redirección de cámaras web para 64 bits [Technical Preview]

En esta versión, se mejoró el rendimiento y la estabilidad generales de la cámara web cuando se trata de aplicaciones de 32 bits. También empezó a ofrecerse la redirección de cámaras web en aplicaciones de 64 bits. Para obtener más información, consulte Cámaras web.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Mejora en la compatibilidad con tarjetas inteligentes [Technical Preview]

Con esta versión, la aplicación Citrix Workspace admite la funcionalidad Plug and Play para lectores de tarjetas inteligentes.

Al insertar una tarjeta inteligente, el lector de tarjetas inteligentes detecta la tarjeta inteligente en el servidor y en el cliente. Puede conectar y usar directamente varias tarjetas al mismo tiempo, y todas estas tarjetas se detectan.

Para configurar esta función:

1. Vaya a la carpeta <ICAROOT>/config/module.ini.
2. Vaya a la sección SmartCard.
3. Configure esta opción: DriverName=VDSCARDV2.DLL.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Mejoras de Microsoft Teams

- Incorporación de una nueva dependencia para llvm-12: En esta versión, se agrega una nueva dependencia llamada libunwind-12 library para llvm-12. Sin embargo, de forma predeterminada, no existe en el repositorio original. Instale el repositorio libunwind-12 library manualmente. Para obtener más información sobre la instalación de libunwind-12 library, consulte Optimización para Microsoft Teams.
- Mejora en las configuraciones de la eliminación de eco, el control automático de ganancias y la supresión de ruido: Si Microsoft Teams configura las opciones de control automático de ganancias y supresión de ruido, la instancia de Microsoft Teams redirigida por Citrix respeta los valores

tal y como están configurados. De lo contrario, estas opciones están habilitadas de forma predeterminada. Sin embargo, de forma predeterminada, la opción de eliminación de eco está desactivada. Para obtener más información, consulte Optimización para Microsoft Teams.

Problemas resueltos

- Es posible que se intente reconectar a la sesión solo una vez durante la reconexión automática de clientes. Como resultado, es posible que la directiva **Reconexión automática de clientes** no funcione según lo previsto. [HDX-34114]
- Se producen fallos en las llamadas al realizar una llamada P2P desde la aplicación Citrix Workspace para Linux 2109 a la aplicación Citrix Workspace para Windows 2109 o Citrix Workspace para Mac 2109. [HDX-35223]

2109

Novedades

Mejora de la fiabilidad de la sesión

Antes, con la función de fiabilidad de sesiones de HDX Broadcast, se seguía viendo una ventana con la aplicación publicada si la conexión a la aplicación se interrumpía.

Con esta versión, puede ver los cambios en la pantalla cuando se inicia la fiabilidad de la sesión. La ventana de sesión se oscurece y aparece un temporizador de cuenta atrás que muestra el tiempo que falta hasta que se intente la siguiente reconexión.

> **Nota:**
>
> Esta función solo está disponible en Citrix Virtual Desktops.

Mejora del registro

Antes no había ninguna herramienta disponible para recopilar archivos de registros en la aplicación Citrix Workspace. Los archivos de registros estaban presentes en diferentes carpetas. Había que recopilar manualmente archivos de registros de diferentes carpetas.

A partir de esta versión, la aplicación Citrix Workspace presenta la herramienta collectlog.py, que le permite recopilar archivos de registros de diferentes carpetas. Puede ejecutar esta herramienta mediante la línea de comandos. Los archivos de registros se generan como un archivo de registros comprimido. Puede descargar este archivo de registros comprimido desde el servidor local. Para obtener más información, consulte Registros.

Continuidad del servicio

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar Citrix Virtual Apps and Desktops y Citrix DaaS independientemente del estado de los servicios de la nube.

Para obtener información sobre los requisitos que permiten la continuidad del servicio en la aplicación Citrix Workspace, consulte Requisitos del sistema.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

Continuidad del servicio con la extensión web de Citrix Workspace para Google Chrome [Technical Preview pública]

La continuidad del servicio con la extensión web de Citrix Workspace para Google Chrome está disponible en la versión Technical Preview pública. Puede usar la extensión web de Workspace para Google Chrome con la aplicación Citrix Workspace para Linux 2109. Esta extensión está disponible en Google Chrome Web Store. La aplicación Workspace se comunica con la extensión web de Citrix Workspace mediante el protocolo del host de mensajería nativa para la extensión de explorador. Juntos, la aplicación Workspace y la extensión web de Workspace utilizan las concesiones de conexión de Workspace para proporcionar a los usuarios del explorador acceso a sus aplicaciones y escritorios durante desconexiones. Para obtener más información, consulte Continuidad del servicio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Audio adaptable

Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en los VDA. El audio adaptable optimiza los parámetros del entorno y sustituye los formatos de compresión de audio obsoletos para proporcionar una excelente experiencia de usuario. El audio adaptable está habilitado de forma predeterminada. Para obtener más información, consulte Audio adaptable.

> **Nota:**
>
> Si se requiere la entrega de audio por UDP para aplicaciones de audio en tiempo real, el audio adaptable debe estar inhabilitado en el VDA para que se pueda recurrir a la entrega de audio por UDP.

Mejora de Storebrowse para la continuidad del servicio

Antes, los archivos de concesión de conexiones de Workspace se sincronizaban con archivos disponibles en el servidor remoto solamente si se conectaba mediante Self-Service Plug-in. Como resultado, la función de continuidad del servicio no estaba disponibles al iniciar aplicaciones o sesiones de escritorio mediante storebrowse. La mayoría de los proveedores externos de clientes ligeros utilizan storebrowse para conectarse a la plataforma Workspace, y la función de continuidad del servicio no estaba habilitada para ellos.

A partir de esta versión, los archivos de concesión de conexiones de Workspace también se sincronizan con archivos disponibles en el servidor remoto al conectarse mediante storebrowse. Esta función ayuda a los proveedores externos de clientes ligeros a acceder a Workspace incluso cuando no hay conexión.

> **Nota:**
>
> - Esta mejora solo está disponible cuando la continuidad del servicio está habilitada en implementaciones en la nube. Para obtener más información, consulte la sección Configurar la continuidad del servicio de la documentación de Citrix Workspace.

Global App Config Service [Technical Preview pública]

El nuevo Citrix Global App Configuration Service para Citrix Workspace ofrece a los administradores de Citrix entregar direcciones URL de servicio de Workspace a través de un servicio administrado de forma centralizada.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
1       <key>AppConfigEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Para obtener más información sobre los parámetros de las direcciones URL de servicio de Workspace, consulte la documentación de Global App Configuration Service.

> **Nota:**
>
> - La aplicación Citrix Workspace para Linux usa Global App Configuration Service solamente para entregar direcciones URL de servicio de Workspace.
> - Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Detección de MTU en Enlightened Data Transport (EDT)

Ahora la aplicación Citrix Workspace permite la detección de unidades de transmisión máxima (MTU) en Enlightened Data Transport (EDT). Aumenta la fiabilidad y la compatibilidad del protocolo EDT y mejora la experiencia de usuario.
Para obtener más información, consulte la sección Detección de MTU en EDT de la documentación de Citrix Virtual Apps and Desktops.

Crear cadenas personalizadas user-agent en una solicitud de red

Con esta versión, la aplicación Citrix Workspace presenta una opción para agregar las cadenas User-Agent a la solicitud de red e identificar el origen de una solicitud de red. En función de esta solicitud de cadenas User-Agent, puede decidir cómo administrar su solicitud de red. Esta función le permite aceptar solicitudes de red solo desde dispositivos de confianza.

> **Nota:**
>
> Esta función está disponible en implementaciones en la nube de la aplicación Citrix Workspace. También se admiten los paquetes x86, x64 y armhf.

Para obtener más información, consulte Crear cadenas personalizadas user-agent en una solicitud de red.

Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, podemos inhabilitar de manera dinámica una función afectada en la aplicación Citrix Workspace aunque dicha función ya se haya publicado. Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly. No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva.

Para obtener más información, consulte Administrar marcas de función.

Problemas resueltos

- Al abrir Microsoft Excel a través de la aplicación Citrix Workspace para Linux e ir a **Datos** > **Nueva consulta**, es posible que el menú emergente **Configuración de origen de datos** no se abra como se esperaba. [CVADHELP-16509]
- Al usar la versión 2106 de VDA, es posible que no se pueda usar la función de uso compartido de la pantalla de Microsoft Teams en el modo **optimizado**. [HDX-34002]
- En Ubuntu 20.04, es posible que la interfaz de usuario de autoservicio no funcione como es debido cuando se usa un almacén en la nube. [RFLNX-8155]

2108

Novedades en la versión 2108

Protección de aplicaciones

Ahora la función de protección de aplicaciones es completamente funcional.

La protección de aplicaciones requiere instalar una licencia adicional en el servidor de licencias. También debe haber presente una licencia de Citrix Virtual Desktops. Para obtener información sobre las licencias, consulte la sección **Configuración** de la documentación de Citrix Virtual Apps and Desktops.

La función de protección de aplicaciones está disponible en sesiones de escritorios y aplicaciones, y está habilitada de forma predeterminada. Sin embargo, debe configurar la función en el archivo `AuthManConfig.xml` para habilitarla en las interfaces del administrador de autenticación y de Self-Service Plug-in.

A partir de esta versión, puede iniciar recursos protegidos desde la aplicación Citrix Workspace mientras se ejecuta Mozilla Firefox.

Para obtener más información, consulte Protección de aplicaciones.

Mejora de la configuración de audio

Antes, el valor predeterminado del atributo `VdcamVersion4Support` en el archivo `module.ini` estaba configurado como **True**. Con esta versión, el valor predeterminado es **False**. Como resultado, solo aparece en la sesión el dispositivo de audio predeterminado con el nombre **Citrix HDX Audio**. Esta mejora tiene como objetivo minimizar los problemas de audio que ocurren cuando el atributo está configurado en **True**.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya a la carpeta `\<ICAROOT\>/config/` y abra el archivo `module.ini`.

2. Vaya a la sección `clientaudio` y agregue la siguiente entrada:

   `VdcamVersion4Support=True`

3. Vuelva a iniciar la sesión para que los cambios surtan efecto.

Problemas resueltos

- Es posible que no se pueda copiar texto del dispositivo del usuario y pegarlo en la sesión. [CVADHELP-16828]
- Es posible que la redirección de contenido del explorador web falle al usar una superposición basada en `WebkitGTK+` para generar el contenido. [CVADHELP-17748]
- Al instalar la protección de aplicaciones, es posible que la interfaz de usuario del escritorio deje de responder y se recupere al cabo de unos segundos. [RFLNX-7729]
- Es posible que la protección de aplicaciones no funcione como es debido en una nueva instalación de la aplicación Citrix Workspace. [RFLNX-7858]
- En una sesión de escritorio, después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, es posible que el enfoque del teclado permanezca en la superposición de la redirección. El enfoque del teclado no cambia a otras aplicaciones abiertas. [RFLNX-7704]
- Durante una reunión Microsoft Teams, es posible que la relación de aspecto del vídeo no se muestre como es debido al seleccionar la opción `Fill frame`. [HDX-31929]
- Durante una videollamada de Microsoft Teams, es posible que Desktop Viewer deje de responder. [HDX-32435]
- Es posible que no se puedan iniciar escritorios ni aplicaciones con la aplicación Citrix Workspace y que el archivo `ICAClient.log` muestre este mensaje:

  "Waiting for handler grpc to be ready".

  [HDX-32575]

2106

Novedades en la versión 2106

Chromium Embedded Framework (CEF) para la redirección de contenido del explorador web (Browser Content Redirection o BCR)

La redirección de contenido del explorador web basada en CEF ya es totalmente funcional. Esta función está activada de forma predeterminada.

> **Nota:**
>
> Esta función no está disponible en la plataforma armhf.

Para obtener más información, consulte Habilitar la redirección de contenido de explorador web basada en CEF.

Indicador de estado de la batería

Ahora el estado de la batería del dispositivo se muestra en el área de notificaciones de las sesiones de Citrix Desktop.

> **Nota:**
>
> El indicador de estado de la batería no aparece en los agentes VDA de servidor.

Para obtener más información, consulte Indicador de estado de la batería.

Continuidad del servicio (versión Technical Preview pública)

> **Nota:**
>
> Esta función se halla actualmente en versión Technical Preview pública para la aplicación Citrix Workspace.

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar Citrix Virtual Apps and Desktops y Citrix DaaS independientemente del estado de los servicios de la nube.

Para obtener información sobre los requisitos que permiten la continuidad del servicio en la aplicación Citrix Workspace, consulte Requisitos del sistema.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Mejora de la protección de aplicaciones [función experimental]

Antes, el administrador de autenticación y los cuadros de diálogo de **Self-Service Plug-in** no estaban protegidos incluso tras instalar y habilitar la protección de aplicaciones.

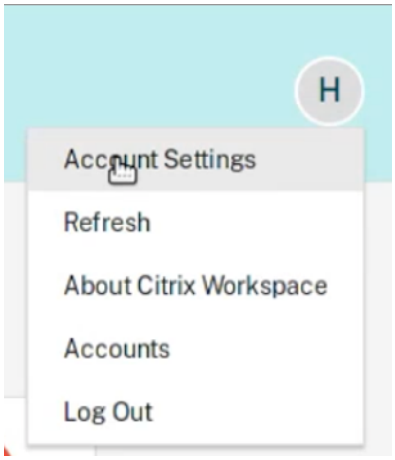
A partir de esta versión, la aplicación Citrix Workspace presenta una opción que le permite configurar las funciones de protección contra el registro de tecleo y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-Service Plug-in.

Para obtener más información, consulte Protección de aplicaciones.

Mejora de la interfaz de usuario

Antes, el menú de parámetros estaba disponible en la opción **Preferencias** de Desktop Viewer.

A partir de esta versión, el menú de parámetros aparece al lado de Self-Service Plug-in. Las opciones de menú se han mejorado para alinearse con la apariencia de la versión nativa de Citrix Workspace. Esta mejora ofrece una experiencia de usuario mejor y más fluida.



> **Nota:**
>
> Esta mejora está disponible de forma predeterminada en la versión 2106 de la aplicación Citrix Workspace en implementaciones en la nube.

Para volver a la apariencia nativa y antigua, haga lo siguiente:

Vaya a `$ICAROOT/config/AuthManConfig.xml` y establezca el valor de `WebUISettings` en **False**.

Mejora para Microsoft Teams

- Antes, al hacer clic en **Compartir pantalla**, la vista previa de un monitor principal o predeterminado solo estaba disponible para el uso compartido de la pantalla.

  Con esta versión, se muestra una vista previa de todas las pantallas en el menú del selector de pantallas. Puede seleccionar una pantalla para compartirla en el entorno de VDA. Aparece un cuadrado rojo en el monitor seleccionado y una pequeña imagen del contenido de la pantalla seleccionada en el menú del selector de pantallas.

En el modo integrado, puede seleccionar una de todas las pantallas para compartirla. Cuando Desktop Viewer cambia el modo de ventana (maximizada, restaurada o minimizada), la pantalla compartida se detiene.

Problemas resueltos

- Al utilizar la aplicación Citrix Workspace 1912 para Linux, es posible que la redirección del portapapeles falle, con lo que la sesión deja de responder. El problema se produce al copiar y pegar una gran cantidad de datos. [CVADHELP-16210]
- Es posible que las videollamadas de Microsoft Teams no optimizadas no tengan audio. El audio no se puede recuperar hasta que haya desconectado y haya vuelto a conectar la sesión. [CVADHELP-16846]
- Es posible que no se puedan descargar archivos alojados en un recurso de red local. [CVADHELP-17337]
- Es posible que las sesiones iniciadas en dispositivos de punto final Linux fallen. El problema se produce cuando la directiva Multisecuencia está habilitada. [RFLNX-6960]
- Al utilizar la versión 1.15.1 de GStreamer, es posible que la redirección de cámaras web falle y que la sesión se desconecte. [HDX-30550]

2104

Novedades en la versión 2104

Protección de aplicaciones en Red Hat Package Manager (RPM) [función experimental]

Ahora, la función de protección de aplicaciones está disponible en la versión RPM de la aplicación Citrix Workspace.

Para obtener más información, consulte Protección de aplicaciones.

Mejora del protocolo HDX Enlightened Data Transport (EDT)

En versiones anteriores, al establecer `HDXoverUDP` en `Preferred`, el transporte de datos por EDT se utiliza como transporte principal, y TCP queda como opción de emergencia.

Con la fiabilidad de la sesión habilitada, se intentan EDT y TCP en paralelo en los siguientes casos:

- Conexión inicial
- Reconexión de fiabilidad de la sesión
- Reconexión automática de clientes

Esta mejora reduce el tiempo de conexión cuando se prefiere EDT. No obstante, el transporte UDP subyacente necesario no está disponible y se debe utilizar TCP.

De forma predeterminada, después de recurrir a TCP, el transporte adaptable vuelve a intentar utilizar EDT cada cinco minutos.

Optimización de Microsoft Teams

Con esta versión, la función de eliminación de eco está inhabilitada de forma predeterminada. Le recomendamos no usar los altavoces y el micrófono integrados para las llamadas. Utilice unos auriculares en su lugar.

Esta corrección tiene como objetivo resolver problemas de audio entrecortado detectados en clientes ligeros.

Continuidad del servicio [Technical Preview]

> **Nota:**
>
> Esta función se halla actualmente en Technical Preview. Citrix recomienda utilizar esta función solo en entornos que no sean de producción. Para registrarse, use este formulario de registro de Podio: Sign up: Service Continuity Tech Preview for Citrix Workspace.

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar Citrix Virtual Apps and Desktops y Citrix DaaS independientemente del estado de los servicios de la nube.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Problemas resueltos

- Al utilizar la redirección de contenido del explorador web, el enfoque del teclado no regresa a la ventana principal incluso después de buscar contenido en la barra de búsqueda de YouTube. [RFLNX-5349]
- Al compartir una pantalla en Microsoft Teams durante una llamada entre dos usuarios, es posible que el audio se oiga distorsionado. El problema se produce con los clientes ligeros Dell Wyse 5070 y 5470. [RFLNX-6537]

- Al utilizar Microsoft Teams en la aplicación Citrix Workspace para Linux, es posible que algunas llamadas se desconecten de manera inesperada. [RFLNX-6719]
- En esta versión se resolvieron varios problemas para mejorar la estabilidad y el rendimiento generales. [RFLNX-7006]
- Al utilizar Chromium Embedded Framework, es posible que la redirección de contenido del explorador web provoque una alta utilización de la CPU. [RFLNX-7217]
- Al utilizar el indicador `cefenablemediadevices` con Microsoft Teams, el micrófono no funciona como es debido. El problema se produce cuando se utiliza la redirección de contenido del explorador web basada en CEF con Microsoft Teams. [RFLNX-6689]
- Al cambiar entre aplicaciones publicadas y locales, es posible que la ventana de la aplicación publicada no escale correctamente en el modo de pantalla completa. [CVADHELP-14812]
- Al abrir Microsoft Excel a través de la aplicación Citrix Workspace para Linux e ir a **Datos** > **Nueva consulta**, es posible que el menú emergente **Configuración de origen de datos** no se abra como se esperaba. [CVADHELP-16509]
- Es posible que las versiones 2101 y 2102 de la aplicación Citrix Workspace para Linux muestren una dirección IP de cliente no válida en Citrix Director. [CVADHELP-16923]
- Es posible que el nombre del dispositivo de audio no se pueda leer. El problema se produce en los sistemas operativos en chino. [CVADHELP-17290]

2103

Novedades en la versión 2103

Anclar el diseño de pantalla con varios monitores

Con esta versión, puede guardar la selección del diseño de pantalla con varios monitores. El diseño es la manera en que se muestra una sesión de escritorio. Anclarlo ayuda a reiniciar una sesión con el diseño seleccionado, lo que ofrece una mejor experiencia de usuario.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas para habilitar la función de anclaje de diseño de pantalla:

```
1       <key>ScreenPinEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Solo después de agregar la clave anterior, podrá ver la opción **Diseño de pantalla** en el **indicador de aplicaciones**.

Para obtener más información, consulte Anclar el diseño de pantalla con varios monitores.

Aumento de la cantidad de canales virtuales admitidos

En versiones anteriores del cliente, las sesiones admitían hasta 32 canales virtuales.

Con esta versión, puede utilizar hasta 64 canales virtuales en una sesión.

Mejoras de Microsoft Teams

Ahora el códec de vídeo VP9 está inhabilitado de forma predeterminada.

Problemas resueltos

- Es posible que, al intentar realizar una videollamada no optimizada, se pierda audio. El audio no se puede recuperar hasta que haya desconectado y haya vuelto a conectar la sesión. [CVADHELP-16846]
- Durante las videollamadas de Microsoft Teams, es posible que el LED de la cámara parpadee y que el vídeo de vista previa se detenga. [CVADHELP-16383]
- Esta corrección establece el valor predeterminado de AudioLatencyControlEnabled en True, lo que reduce la latencia de audio. [RFLNX-6620]
- Es posible que la función de uso compartido de la pantalla en Microsoft Teams falle en el modo integrado. [RFLNX-6659]
- Cuando una sesión se cierra o se desconecta de manera abrupta, es posible que el proceso `HdxRtcEngine.exe` se cierre de manera inesperada. [RFLNX-5885]

2101

Novedades en la versión 2101

Mejora de la asignación de unidades de cliente (CDM)

Con esta versión, el acceso a las unidades asignadas viene con una función adicional de seguridad.

Ahora, puede seleccionar el nivel de acceso a la unidad asignada desde cada almacén de la sesión.

Para evitar que aparezca el cuadro de diálogo de nivel de acceso cada vez, seleccione la opción **No volver a preguntarme**. La configuración se aplica a ese almacén concreto.

Si decide no seleccionar la opción, puede establecer los niveles de acceso que aparecen cada vez que se inicie una sesión.

Protección de aplicaciones en paquetes Debian [función experimental]

Ahora, la función de protección de aplicaciones está disponible en la versión Debian de la aplicación Citrix Workspace.

Para una instalación silenciosa del componente de protección de aplicaciones, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:


```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"
sudo debconf-show icaclient
* app_protection/install_app_protection: yes
sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

Mejoras de Microsoft Teams

- Ahora el instalador de la aplicación Citrix Workspace incluye tonos de llamada de Microsoft Teams.
- La salida de audio cambia automáticamente a los dispositivos de audio recién conectados y se establece un volumen de audio adecuado.
- El proxy HTTP está disponible para la autenticación anónima.

Problemas resueltos

- Cuando se utiliza un proxy personalizado, puede aparecer un mensaje de autenticación adicional. El problema se debe a Chromium Embedded Framework (CEF) que utiliza el explorador web para redirigir el contenido. Como solución temporal, configure el agente para omitir el mensaje adicional. [CVADHELP-14804]
- Al intentar volver a conectarse a una sesión, es posible que la sesión deje de responder. El problema se produce con las sesiones habilitadas para tarjetas inteligentes. Como solución temporal, vuelva a insertar la tarjeta inteligente. [CVADHELP-15028]
- Con Microsoft Teams en modo **Optimizado**, es posible que la reproducción de vídeo deje de responder durante las llamadas de conferencias. El problema se produce cuando un participante cambia de una cámara integrada a una cámara USB. [CVADHELP-16400]
- Con Microsoft Teams en modo **Optimizado**, es posible que el proceso `HdxRtcEngine.exe` se cierra de forma inesperada. [CVADHELP-16504]

Problemas conocidos

Problemas conocidos en la versión 2211

- Es posible que aparezcan mensajes de error de ID de transacción al iniciar una sesión. Por ejemplo: “The option ‘-transactionid’ is invalid”. Como solución temporal, haga clic en **Aceptar** para cerrar el cuadro del mensaje y continuar. [HDX-45618]
- Al instalar e iniciar la aplicación Citrix Workspace, es posible que aparezca este mensaje de error:

"The X request 130.1 caused error:" 10: BadAccess (Attempt to access private resource denied)

Haga clic en **Cancelar** para continuar con la sesión.

Como solución temporal, vaya al archivo de configuración `$HOME/.ICAClient/wfclient.ini` y sustituya `IgnoreErrors=9,15` por `IgnoreErrors=9,15,32`. [HDX-44416]

- Al cerrar sesión en la aplicación Citrix Workspace e iniciar sesión de nuevo, la aplicación Citrix Workspace se inicia sin introducir las credenciales de inicio de sesión. Este problema solo se produce en implementaciones de la nube y si el valor del parámetro `longLivedTokenSupport` está establecido en *True*. Como solución temporal, haga lo siguiente:

  1. Vaya al archivo `/config/AuthManConfig.xml`.
  2. Vaya a la sección [AuthManLite] y actualice esta entrada:

  ```
  <longLivedTokenSupport>false</longLivedTokenSupport>
  ```

  [RFLNX-9160]

Problemas conocidos en la versión 2209

- Al iniciar una sesión de la aplicación Microsoft Edge, el icono de Microsoft Edge se muestra aleatoriamente para diferentes escalas. Este error se produce si aplicó estos parámetros:
  - El valor `DPIMatchingEnabled` está establecido en **True**
  - La escala de clientes en la pantalla no está configurada al 100 %

  [HDX-39764]

- Es posible que no se puedan iniciar sesiones de VDA de servidor mediante la autenticación con tarjeta inteligente en el caso de una tarjeta inteligente con varios usuarios. Como solución temporal, inserte la tarjeta de nuevo. [HDX-44255]

- Es posible que el VDA se cierre de forma inesperada después de redirigir la interfaz del dispositivo. Este problema se produce al habilitar la directiva "Redirección de dispositivos USB del cliente" en el DDC y al conectar dispositivos USB compuestos al dispositivo de punto final, como auriculares USB con micrófono. Además, agregue el valor de entrada en el archivo usb.conf como `vid=** pid=** split=01 and intf=00,01`. Después de eso, inicie la sesión desde la aplicación Citrix Workspace y configure la redirección de la interfaz del dispositivo. [HDX-44117]

- Es posible que no se pueda iniciar la sesión en el sistema operativo Raspberry Pi ARMHF basado en Debian 11 Citrix recomienda utilizar el sistema operativo Raspberry Pi ARM64 basado en Debian 11 o el sistema operativo Raspberry Pi ARMHF anterior basado en Debian 10. [HDX-41729]

- Al quitar una cuenta principal, es posible que las credenciales de inicio de sesión no se eliminen de la caché de autoservicio. Como resultado, es posible que pueda iniciar sesión en el almacén

sin proporcionar las credenciales. Como solución temporal, cierre el autoservicio para eliminar las credenciales. [RFLNX-9051]

- Después de proporcionar las credenciales de inicio de sesión e iniciar el autoservicio, es posible que aparezca una pantalla blanca. Como solución temporal, cierre el autoservicio y reinícielo. [RFLNX–8951]
- En OpenSUSE SLES 15, es posible que se muestre una rueda giratoria al conectarse a un almacén de la nube. [RFLNX–9109]
- Es posible que no pueda iniciar el autoservicio en RHEL9 y Fedora 36. Como solución temporal, asegúrese de que el valor de `AuthManLiteEnabled` esté establecido en *False* en el archivo `$ICAROOT/config/AuthManConfig.xml`. [RFLNX-9128]

Problemas conocidos en 2207

- Podría ocurrir un sondeo de DNS para la recopilación de datos CAS con un inicio directo de ICA y con almacenes de CAS inhabilitados. [CVADHELP-20018]
- Al usar los comandos de storebrowse, si se agrega y enumera un segundo almacén, es posible que no puedan iniciarse las aplicaciones o los escritorios desde el primer almacén. Como solución temporal, debe volver a enumerar el almacén específico antes de iniciar cualquier aplicación o escritorio. [RFLNX-8953]
- En una sesión de escritorio, al reproducir un vídeo con Reproductor de Windows Media, es posible que el cursor del mouse desaparezca en el vídeo RAVE. Este problema solo se produce si ha establecido las siguientes directivas en Desktop Delivery Controller de la siguiente manera:
  - "Usar códec de vídeo para la compresión" como "Para áreas en cambio constante"
  - "Redirección de Windows Media" como "Permitida" (configuración predeterminada)
  - "Redirección de contenido del explorador web" como "Permitida" (configuración predeterminada)
  - "InvertCursorEnabled" como "BOTH" y se agregan los siguientes valores en el archivo ~/.ICAClient/wfclient.ini:
    - InvertCursorEnabled=True
    - InvertCursorRefreshRate=60
    - InvertCursorMode=1

[HDX-37259]

Problemas conocidos en la versión 2205

- Es posible que tenga problemas en la desconexión de sesiones al conectarse a través de dispositivos de punto final con la versión 2205 de la aplicación Citrix Workspace para Linux.

Este problema se produce si configura la pantalla de bloqueo con la configuración de directiva **Forzar una imagen de pantalla de bloqueo predeterminada específica** con ciertos tipos de archivos JPEG y la aplica a Citrix VDA 2203. Como solución temporal, actualice la aplicación Citrix Workspace a la versión 2207 o a una posterior. [CVADHELP-21572]

- Cuando se produce un error de SSL en un protocolo durante un intento de conexión TCP y EDT/UDP, es posible que las dos conexiones fallen debido a la condición de carrera. Este error de SSL puede producirse si la configuración de TLS difiere entre los protocolos y el cliente no puede conectarse a través de un protocolo. Como solución temporal, active o desactive el atributo HDXoverUDP en el archivo ICA. [RFLNX-8747]
- La compresión de vídeo de cámara web HDX RealTime no admite cámaras con formato de vídeo MJPEG en la aplicación Citrix Workspace. [HDX-40352]
- Es posible que el vídeo o la imagen de la aplicación Citrix Workspace no se representen correctamente. Este problema se produce cuando se utiliza la aplicación Citrix Workspace junto con la versión 2109 del VDA o una posterior. Como solución temporal, haga lo siguiente.

  1. Inicie sesión en Citrix Studio.
  2. Modifique los parámetros de la directiva Usar códec de vídeo para compresión.
  3. Seleccione la opción **Para la pantalla entera** en la lista desplegable **Valor**. [HDX-40287]

- Al agregar un almacén con el comando `storebrowse -a` y hacer una enumeración con el comando `storebrowse -E`, es posible que la enumeración de Storebrowse falle. Este problema solo ocurre en el sistema operativo Raspberry Pi. Como solución temporal, haga lo siguiente:

  1. Vaya a /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Agregue la siguiente entrada:

```
<StorebrowseIPCDisabled> true</StorebrowseIPCDisabled>
<!--NeedCopy-->
```

  [RFLNX-8803]

- Al agregar un almacén con los parámetros predeterminados, es posible que la enumeración de Storebrowse falle. Este problema solo ocurre en el sistema operativo Debian de 32 bits. Como solución temporal, haga lo siguiente:

  1. Vaya a /opt/Citrix/ICAClient/config/AuthmanConfig.xml.
  2. Agregue la siguiente entrada:

```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

  [RFLNX-8743]

- Es posible que no pueda instalar el paquete Debian de la aplicación Citrix Workspace en Ubuntu 22.04 LTS. El motivo de este error es que el paquete `libidn11` requerido para `ICAClient` no está presente en Ubuntu 22.04 LTS. Como solución temporal, instale `libidn11` de manera independiente en Ubuntu 22.04 LTS antes de instalar el paquete Debian de la aplicación Citrix Workspace. [RFLNX-8839]

Problemas conocidos en la versión 2203

- Al iniciar una aplicación publicada del Protocolo de escritorio remoto (RDP) con varios monitores en un dispositivo de punto final de Ubuntu, solo un monitor muestra el contenido aunque la máquina cliente tenga varios monitores. La casilla "Usar todos mis monitores para la sesión remota" en la opción de visualización de la aplicación RDP está seleccionada antes de conectarse a un escritorio remoto a través de RDP. El problema se produce en el modo integrado y en la configuración con varios monitores. [CVADHELP-16768]
- La aplicación Citrix Workspace no transmite los parámetros `Clientname` ni `clientaddress` al DDC durante la enumeración de recursos. Como resultado, es posible que `Set-BrokerAccessPolicyRule` filtrado con el nombre del cliente o la IP del cliente no funcione correctamente. [CVADHELP-17667]
- Al previsualizar un vídeo con una cámara web en Skype, es posible que la vista previa muestre una pantalla en negro. [HDX-37860]

Problema conocido en la versión 2202

- Al iniciar la interfaz de usuario de autoservicio con los parámetros predeterminados, es posible que aparezca este mensaje de error:

  "Response for Secondary Token request is not 200/400/404 42".

  Este problema se produce en Fedora 35. Como solución temporal, instale `gnome-keyring` o inhabilítelo en `authmanconfig.xml`.

  Para inhabilitar `gnome-keyring`, haga lo siguiente:

1. Vaya a `/opt/Citrix/ICAClient/config/AuthmanConfig.xml`.
2. Agregue la siguiente entrada:

```
1 ```
2 <GnomeKeyringDisabled>true</GnomeKeyringDisabled>
3 <!--NeedCopy--> ```
```

[RFLNX-8603]

Problemas conocidos en la versión 2112

- En la aplicación Citrix Workspace 2112, es posible que vea un uso elevado de la CPU en el dispositivo de punto final cuando una cámara web está encendida en videollamadas de Microsoft Teams optimizado.

Como solución temporal, ejecute este comando en el terminal:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{
      "UseDefaultCameraConfig":0  }
 `

<!--NeedCopy-->
```

[HDX-37168]

- Después de instalar la aplicación Citrix Workspace con la función de protección de aplicaciones habilitada en un SO que utiliza `glibc 2.34` o una versión posterior, es posible que, al reiniciar el sistema, el SO no arranque. Para recuperarse de un error de arranque del SO, realice una de estas acciones:
  - Instale de nuevo el sistema operativo. Sin embargo, no admitimos la función de protección de aplicaciones en el sistema operativo que usa `glibc 2.34` o una versión posterior.
  - Vaya al modo de **recuperación** del sistema operativo y desinstale la aplicación Citrix Workspace desde el terminal.
  - Arranque el sistema desde el SO en directo y quite el archivo `rm -rf /etc/ld.so.preload` del SO existente.
    [RFLNX-8358]
- Al intentar introducir texto, el cursor se vuelve de color blanco. El problema se produce en un caso de doble salto al conectarse desde una máquina Linux de punto final. [CVADHELP-16170]
- Al instalar la aplicación Citrix Workspace, agregar almacenes e iniciar escritorios, es posible que la ventana de la sesión no aparezca si la biblioteca `libpcscd` no está instalada en Ubuntu 16.04. Como solución temporal, haga lo siguiente:
  1. Instale la biblioteca `libpcscd` en el cliente Linux. Por ejemplo, use el comando `apt install libpcscd` para instalar la biblioteca `libpcscd` en Ubuntu 16.04.
  2. Si no puede instalar la biblioteca `libpcscd`, reemplace el atributo `VDSCARDV2.DLL` por el atributo `VDSCARD.DLL` de DriverName en el archivo de configuración `/opt/Citrix/ICAClient/config/module.ini`:

[SmartCard]

DriverName=VDSCARD.DLL

[HDX-36574]

- En la aplicación Citrix Workspace, es posible que se produzcan errores intermitentes al responder o realizar llamadas de Microsoft Teams. Aparece el siguiente mensaje de error:

  "No se pudo establecer la llamada".

  Como solución temporal, intente establecer de nuevo la llamada de Microsoft Teams. [HDX-38819]

Problemas conocidos en la versión 2111

- Las sesiones de doble salto no admiten la funcionalidad Plug and Play para lectores de tarjetas inteligentes. [HDX-34582]
- Al iniciar sesión en un almacén en la nube, es posible que la pantalla aparezca en blanco. [RFLNX-8337]
- Al intentar iniciar la aplicación Citrix Workspace, es posible que no se pueda abrir la interfaz de usuario de autoservicio y aparezca este mensaje de error:

  "User-defined signal 2"

  El problema ocurre en la compilación de depuración y en Debian 10 de las VM de Azure. [RFLNX-8336]

- Después de instalar la aplicación Citrix Workspace con la función de protección de aplicaciones habilitada en un SO que utiliza glibc 2.34 o una versión posterior, es posible que, al reiniciar el sistema, el SO no arranque. Para recuperarse de un error de arranque del SO, realice una de estas acciones:
  - Instale de nuevo el sistema operativo. Sin embargo, no admitimos la función de protección de aplicaciones en el sistema operativo que usa glibc 2.34 o una versión posterior.
  - Vaya al modo de **recuperación** del sistema operativo y desinstale la aplicación Citrix Workspace desde el terminal.
  - Arranque el sistema desde el SO en directo y quite el archivo `rm -rf /etc/ld.so.preload` del SO existente. [RFLNX-8358]

Problemas conocidos en la versión 2109

- Al desinstalar la aplicación Citrix Workspace, es posible que no se quiten automáticamente los archivos de caché desactualizados que hay en `$HOME/.local/share/webkitgtk`. Como solución temporal, quite manualmente los archivos de caché. [HDX-28187]

- Es posible que no se puedan iniciar escritorios o aplicaciones mediante la aplicación Citrix Workspace cuando la directiva Puertos múltiples está habilitada en DDC. [HDX-31016]
- Es posible que no se puedan iniciar sesiones mediante la autenticación con tarjeta inteligente. El problema se produce con la versión 2104 de la aplicación Citrix Workspace para Linux y versiones posteriores. Como solución temporal, introduzca manualmente las credenciales de la tarjeta inteligente. [CVADHELP-18402]
- Es posible que se intente reconectar a la sesión solo una vez durante la reconexión automática de-clientes. Como resultado, es posible que la directiva **Reconexión automática de clientes** no funcione según lo previsto. [HDX-34114]
- Al cerrar la barra de progreso que muestra el progreso del inicio de una aplicación, es posible que el proceso wfica falle. Por eso, es posible que la aplicación se inicie y desaparezca de la pantalla. [HDX-34701]

Problemas conocidos en la versión 2108

- Cuando la función de protección de aplicaciones está habilitada, es posible que la protección contra el registro de tecleo no funcione para la interfaz del administrador de autenticaciones que usa la biblioteca `UIDialogLibWebKit3.so`. [RFLNX-8027]
- Si utiliza Global Server Load Balancing (GSLB), es posible que las respuestas del sistema de nombres de dominio (DNS) no se almacenen en la caché durante el período de vida (TTL). Como resultado, es posible que la autenticación con WebView falle. [RFLNX-3673]
- Cuando intenta conectarse de forma remota a una máquina que tiene instalada la aplicación Citrix Workspace con protección de aplicaciones, el servidor x11vnc se cierra de forma inesperada y la conexión falla. Como resultado, es posible que no pueda conectarse remotamente a la máquina a través del servidor x11vnc. [RFLNX-8933]

Problemas conocidos en la versión 2106

- En una sesión de escritorio, después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, es posible que el enfoque del teclado permanezca en la superposición de la redirección (por ejemplo, en la búsqueda de YouTube). El enfoque del teclado no cambia a otras aplicaciones abiertas. El problema se produce solo tras iniciar sesiones con Self-Service Plug-in o StoreBrowse. Como solución temporal, para cambiar el enfoque a otras aplicaciones, haga clic en la barra de herramientas de la sesión y seleccione el botón **Inicio**. [RFLNX-7704]
- En una sesión de escritorio, después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, el enfoque del teclado cambia a la ubicación actual del mouse. El problema se debe a una limitación de terceros con CEF de código abierto. [RFLNX-7724]

- Al intentar hacer clic en la superposición de la redirección de contenido del explorador web (por ejemplo, en la búsqueda de YouTube) con otra aplicación en primer plano, la página del explorador no aparece en primer plano. [RFLNX-7730]
- Después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, al cerrar la página web redirigida, se captura un fallo de segmentación en los registros de errores. [RFLNX-7667]
- Durante las llamadas de audio entre dos usuarios de Microsoft Teams, es posible que el audio no funcione durante los primeros 15 segundos de la llamada. Como solución temporal, en el archivo `module.ini`, establezca el atributo `VdcamVersion4Support` en **False**. [HDX-29526]

Problema conocido en la versión 2104

- En la versión 1912 LTSR CU2 de VDA, es posible que se desconecten sesiones. El problema se produce al habilitar la directiva **Multisecuencia** en el Delivery Controller. Como solución temporal, actualice la versión del VDA a la versión 2012 o a una posterior. [RFLNX-6960]

Problema conocido en la versión 2103

- Durante una videollamada o al compartir la pantalla, es posible que Microsoft Teams deje de responder y que la llamada se corte. [CVADHELP-16918]

Problemas conocidos en la versión 2101

- Al reproducir vídeos largos, el audio se detiene, pero el vídeo continúa reproduciéndose normalmente. El problema se produce cuando se establece `VdcamVersion4Support` en **True**. Como solución temporal, establezca `VdcamVersion4Support` en **False** para inhabilitar la opción de audio múltiple. [RFLNX-6472]
- Durante las reuniones de Microsoft Teams, es posible que el audio suene entrecortado cuando tiene el micrófono silenciado. El problema se produce en clientes ligeros. [RFLNX-6537]
- A veces, es posible que la aplicación Citrix Workspace no pueda generar vídeos entrantes en Microsoft Teams. [RFLNX-6662]
- Al utilizar el indicador `cefenablemediadevices` con Microsoft Teams, el micrófono no funciona como es debido. El problema se produce cuando se utiliza la redirección de contenido del explorador web basada en CEF con Microsoft Teams. [RFLNX-6689]

Documentación antigua

Para ver las versiones de productos que han alcanzado el fin de su vida (EOL), consulte Documentación antigua.

Avisos de terceros

La aplicación Citrix Workspace puede incluir software de terceros con licencias definidas en las condiciones del siguiente documento:

Avisos legales de terceros de la aplicación Citrix Workspace para Linux (descarga de PDF)

Funciones experimentales

En ocasiones, Citrix publica funciones experimentales como mecanismo para buscar comentarios de los clientes sobre la conveniencia potencial de nuevas tecnologías o funciones. Citrix no acepta casos de asistencia para funciones experimentales, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. Citrix no se compromete a producir funciones experimentales y puede retirarlas por cualquier motivo en cualquier momento.

Requisitos del sistema y compatibilidad

April 18, 2023

Requisitos

Requisitos de hardware

Kernel de Linux:

- Versión 2.6.29 o una posterior

Espacio en disco:

- 55 MB como mínimo
- 110 MB adicionales si expande o extrae el paquete de instalación en el disco
- 1 GB de RAM como mínimo para dispositivos SoC (system-on-a-chip) que usen la redirección de Flash de HDX MediaStream

Pantalla de vídeo en color:

- Pantalla de vídeo de 256 colores o más

Bibliotecas y códec

Bibliotecas:

- `glibcxx` 3.4.25 o una versión posterior

- glibc 2.27 o una versión posterior
- gtk 2 (2.20.1 o versiones posteriores)
- libcap1 o libcap2
- libjson-c (para la instrumentación)
- X11 o X.Org (Wayland no es compatible)
- Función udev
- Advanced Linux Sound Architecture (ALSA) libasound2
- PulseAudio

Interfaz de usuario de autoservicio:

- webkit2gtk 2.16.6 o una versión posterior
- libxml2 2.7.8
- libxerces-c 3.1

Bibliotecas de códecs:

- Speex
- Bibliotecas de códecs Vorbis

Requisitos de distribución basados en Red Hat Package Manager (RPM):

- chkconfig

Requisitos de la red

Protocolo de red:

- TCP/IP

Requisitos de H.264

Para dispositivos x86:

- Una velocidad de procesador de 1,6 GHz como mínimo

Para la función HDX 3D Pro:

- Una velocidad de procesador de 2 GHz como mínimo
- Un hardware nativo con controlador de gráficos acelerados

Para dispositivos ARM:

- Se necesita un descodificador de hardware H.264 para ofrecer la funcionalidad general de H.264 y HDX 3D Pro

Redirección de HDX MediaStream para Flash

Para ver todos los requisitos de la redirección de Flash de HDX MediaStream, consulte el artículo CTX134786 de Knowledge Center.

Le recomendamos probar el artículo con el plug-in más reciente antes de implementar una nueva versión para, así, aprovechar la funcionalidad y las correcciones más recientes relacionadas con la seguridad.

Requisitos de la integración en CEIP (Programa para la mejora de la experiencia del usuario)

- `zlib` 1.2.3.3
- `libtar` 1.2 o una versión posterior
- `libjson` 7.6.1 o una versión posterior

Requisitos de la compresión de vídeo de cámara web HDX RealTime

- Una cámara web compatible con Video4Linux
- `GStreamer` 0.10.25 (o una versión 0.10.x posterior), incluido el paquete “plug-ins-good” de la distribución

  O bien:

- `GStreamer` 1.0 (o una versión 1.x posterior), incluidos los paquetes “plug-ins-base”, “plug-ins-good”, “plug-ins-bad”, “plug-ins-ugly” y “gstreamer-libav” de la distribución.

Requisitos de la redirección de Windows Media de HDX MediaStream

- `GStreamer` 0.10.25 (o una versión 0.10.x posterior), incluido el paquete “plug-ins-good” de la distribución. En general, la versión 0.10.15 o posterior es suficiente para la Redirección de Windows Media para HDX MediaStream

  O bien:

- `GStreamer` 1.0 (o una versión 1.x posterior), incluidos los paquetes “plug-ins-base”, “plug-ins-good”, “plug-ins-bad”, “plug-ins-ugly” y “gstreamer-libav” de la distribución.

> **Notas:**
>
> - Si `GStreamer` no está incluido en su distribución de Linux, puede descargarlo desde la página de GStreamer.
> - Es posible que usar ciertos códigos (por ejemplo, “plug-ins-ugly”) requiera una licencia del fabricante de esa tecnología. Contacte con el administrador del sistema para obtener ayuda.

Requisitos de la redirección de contenido del explorador web

- Versión 2.16.6 de webkit2gtk
- `glibcxx` 3.4.25 o una versión posterior

Requisitos de Philips SpeechMike

- Visite el sitio web de Philips para instalar los controladores pertinentes.

Requisitos de protección de aplicaciones

La protección de aplicaciones funciona mejor con estos sistemas operativos y GNOME Display Manager:

- Ubuntu 18.04 y Ubuntu 20.04 de 64 bits
- Debian 9 y Debian 10 de 64 bits
- CentOS 7 de 64 bits
- RHEL 7 de 64 bits
- Sistema operativo Raspberry Pi (Buster) con armhf de 32 bits (basado en Debian 10)

> **Nota:**
>
> - Si utiliza una versión de la aplicación Citrix Workspace anterior a 2204, la función de protección de aplicaciones no es compatible con los sistemas operativos que utilizan `glibc` 2.34 o una versión posterior.
> - En Ubuntu 20.04.5 o una versión posterior, al hacer doble clic en el archivo del paquete `.deb`, se abre el instalador de Snap Store. Este instalador no admite instrucciones del usuario. Por lo tanto, debe instalar la aplicación Citrix Workspace mediante la línea de comandos en un terminal o mediante otros instaladores de software como `gnome-software` , `gdebi` o `synaptics`.

Requisitos de la optimización de Microsoft Teams

Versión mínima:

- Aplicación Citrix Workspace 2006

Software:

- `GStreamer` 1.0 o una versión posterior y Cairo 2
- libc++-9.0 o una versión posterior
- `libgdk` 3.22 o una versión posterior
- OpenSSL 1.1.1d
- Distribución de Linux x64

Hardware:

- Como mínimo, una CPU de doble núcleo de 1,8 GHz que admita una resolución de 720p HD durante llamadas de conferencia en vídeo de punto a punto
- CPU de doble o cuádruple núcleo con una velocidad base de 1,8 GHz y una velocidad Intel Turbo Boost alta de al menos 2,9 GHz

Mejora en la autenticación:

- Biblioteca `Libsecret`
- Biblioteca libunwind-12

Requisitos de la continuidad del servicio

A partir de la versión 2106, puede instalar Continuidad del servicio en la versión Debian de la aplicación Citrix Workspace.

Ejecute estos comandos desde el terminal antes de instalar la aplicación Citrix Workspace:

```
sudo apt-get update -y
```

Bibliotecas obligatorias preinstaladas:

- Versión 2.30.1 de libwebkit2gtk-4.0-37 o una posterior
  - Si utiliza Debian, ejecute este comando:

    ```
    1 sudo apt-get install libwebkit2gtk-4.0-37
    2 <!--NeedCopy-->
    ```

  - Si utiliza RPM, ejecute este comando:

    ```
    1 sudo yum install libwebkit2gtk-4*
    2 <!--NeedCopy-->
    ```

  - Para Ubuntu, RHEL, SUSE, Fedora o Debian, Citrix recomienda instalar la versión 2.30.1 o una posterior de libwebkit2gtk-4.0-37.
  - Para Raspberry Pi con Buster OS, Citrix recomienda instalar la versión 2.30.1 de libwebkit2gtk-4.0-37.
- gnome-keyring 3.18.3 o una versión posterior
  - Si utiliza Debian, ejecute este comando:

    ```
    1 sudo apt-get install gnome-keyring
    2 <!--NeedCopy-->
    ```

  - Si utiliza RPM, ejecute este comando:


```
sudo yum install gnome-keyring
<!--NeedCopy-->
```

- Libsecret
  - Si utiliza Debian, ejecute este comando:

```
sudo apt-get install libsecret-1-0
<!--NeedCopy-->
```

  - Si utiliza RPM, ejecute este comando:

```
sudo yum install libsecret-1*
<!--NeedCopy-->
```

> **Notas:**
>
> A partir de la versión 1910, la aplicación Citrix Workspace funciona como es debido solo si el sistema operativo cumple estos criterios de versión de GCC:
>
> - Versión de GCC para la arquitectura x64: 4.8 o posterior
> - Versión de GCC para la arquitectura armhf: 4.9 o posterior
>
> A partir de la versión 2101, la aplicación Citrix Workspace funciona como es debido solo si el sistema operativo cumple estos requisitos:
>
> - Versión 4.9 de GCC o una posterior
> - glibcxx 3.4.20 o una versión posterior
>
> A partir de la versión 2209, la aplicación Citrix Workspace funciona como es debido solo si el sistema operativo cumple este requisito:
>
> glibcxx 3.4.25 o una versión posterior

Tabla de compatibilidad

La aplicación Citrix Workspace es compatible con todas las versiones actualmente compatibles de los productos Citrix.

Para obtener más información acerca de la vida útil de los productos Citrix y para determinar cuándo deja Citrix de ofrecer versiones específicas de los productos, consulte Citrix Product Lifecycle Matrix.

Requisitos del servidor

StoreFront

- Puede utilizar todas las versiones admitidas de la aplicación Citrix Workspace para acceder a los almacenes de StoreFront mediante conexiones desde la red interna y a través de Citrix Gateway:
  - StoreFront 1811 y versiones posteriores.
  - StoreFront 3.12.
- Puede usar el almacén de StoreFront que está configurado con Workspace para Web. Workspace para Web ofrece acceso a los almacenes de StoreFront desde un explorador web. Para conocer las limitaciones de esta implementación, consulte Consideraciones importantes en la documentación de StoreFront.

Conexiones y certificados

Conexiones

La aplicación Citrix Workspace para Linux admite conexiones HTTPS y conexiones ICA sobre TLS a través de las siguientes configuraciones.

- Para conexiones LAN:
  - StoreFront con servicios de StoreFront o Workspace para Web
- Para conexiones locales o remotas seguras:
  - Citrix Gateway 12.0 y versiones posteriores
  - NetScaler Gateway 10.1 y versiones posteriores
  - NetScaler Access Gateway Enterprise Edition 10
  - NetScaler Access Gateway Enterprise Edition 9.x
  - NetScaler Access Gateway VPX

  Para obtener información sobre las versiones de Citrix Gateway admitidas en StoreFront, consulte los requisitos del sistema para StoreFront.

Certificados

Para garantizar transacciones seguras entre el servidor y el cliente, use los siguientes certificados:

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. Esta instalación ayuda a acceder a recursos de Citrix mediante la aplicación Citrix Workspace.

> **Nota:**
>
> Aparece una advertencia de certificado que no es de confianza si el certificado de la puerta de enlace remota no se puede verificar durante la conexión. Es posible que esta verificación falle

> porque el certificado raíz no está incluido en el almacén de claves local. Si elige ignorar la advertencia y continuar con la conexión, se mostrarán aplicaciones, pero no se podrán iniciar. El certificado raíz debe instalarse en el almacén de certificados del cliente.

Certificados raíz

Para máquinas unidas a un dominio, use la plantilla administrativa de objeto de directiva de grupo para distribuir y confiar en certificados de CA.

Para máquinas que no están unidas a ningún dominio, cree un paquete de instalación personalizado para distribuir e instalar el certificado de CA. Póngase en contacto con el administrador del sistema para recibir ayuda.

Instalación de certificados raíz en los dispositivos de usuario

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, la aplicación Citrix Workspace admite los siguientes certificados.

Certificado	Entidad 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

Certificados comodín

Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo dominio. La aplicación Citrix Workspace admite el uso de certificados comodín, aunque deben usarse solamente de acuerdo con las directivas de seguridad de su organización.

Se puede considerar la posibilidad de usar alternativas a certificados comodines, como, por ejemplo, un certificado que incluya la lista de nombres de servidor dentro de la extensión de nombre de sujeto alternativo (Subject Alternative Name o SAN). Entidades de certificación tanto privadas como públicas emiten estos certificados.

Agregar un certificado intermedio a Citrix Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá agregar este certificado al certificado del servidor de Citrix Gateway. Para obtener información, consulte Configurar certificados intermedios en la documentación de Citrix Gateway.

Si el servidor de StoreFront no consigue proporcionar los certificados intermedios que coincidan con el certificado que está utilizando, o si instala certificados intermedios para admitir usuarios de tarjetas inteligentes, siga estas instrucciones antes de agregar un almacén de StoreFront:

1. Obtenga uno o varios certificados intermedios por separado en formato PEM.

   > **Sugerencia:**
   >
   > Si no puede encontrar un certificado con la extensión de archivo .pem, use la utilidad `openssl` para convertir un certificado a la extensión de archivo .pem.

2. Al instalar el paquete (normalmente raíz):

   a) Copie uno o varios archivos a $ICAROOT/keystore/intcerts.

   b) Ejecute este comando después de instalar el paquete:

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

Directiva de validación conjunta de certificados de servidor

La aplicación Citrix Workspace tiene una directiva más estricta para validar los certificados de servidor.

> **Importante:**
>
> Antes de instalar la aplicación Citrix Workspace, confirme que los certificados presentes en el servidor o la puerta de enlace se hayan configurado correctamente como se describe aquí. Las conexiones pueden fallar si:
>
> - La configuración del servidor o la puerta de enlace incluye un certificado raíz incorrecto
> - La configuración del servidor o la puerta de enlace no incluye todos los certificados intermedios
> - La configuración del servidor o la puerta de enlace incluye un certificado intermedio caducado o no válido
> - La configuración del servidor o la puerta de enlace incluye un certificado intermedio con firmas cruzadas

Al validar un certificado de servidor, la aplicación Citrix Workspace usa todos los certificados suministrados por el servidor (o la puerta de enlace) para validarlo. Al igual que en versiones anteriores de la aplicación Citrix Workspace, esto verifica que los certificados son de confianza. Si algún certificado no es de confianza, la conexión falla.

Esta directiva es más estricta que la directiva de certificados presente en los exploradores web. Muchos exploradores web incluyen un gran conjunto de certificados raíz en los que confían.

El servidor (o la puerta de enlace) debe estar configurado con el conjunto correcto de certificados. Es posible que un conjunto incorrecto de certificados provoque que falle la conexión de la aplicación Citrix Workspace.

Si se configura una puerta de enlace con estos certificados válidos, utilice la siguiente configuración para una validación más estricta. Esta configuración determina exactamente qué certificado raíz usa la aplicación Citrix Workspace:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio
- Ejemplo de certificado raíz

La aplicación Citrix Workspace verifica que todos los certificados sean válidos. La aplicación Citrix Workspace también verifica que ya confía en el certificado raíz de ejemplo. Si la aplicación Citrix Workspace no confía en el certificado raíz de ejemplo, la conexión falla.

> **Importante:**
>
> - Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar esta validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente. Por ejemplo, actualmente hay dos certificados (DigiCert/GTE CyberTrust Global Root y DigiCert Baltimore Root/Baltimore CyberTrust Root) que pueden validar los mismos certificados de servidor. En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En otros dispositivos, solo uno está disponible (DigiCert Baltimore Root/Baltimore CyberTrust Root).
> - Si configura el certificado GTE CyberTrust Global Root en la puerta de enlace, fallarán las conexiones de la aplicación Citrix Workspace en esos dispositivos de usuario. Consulte la documentación de la entidad de certificación para determinar qué certificado raíz debe usarse. Tenga en cuenta que los certificados raíz también caducan, como todos los demás certificados.
> - Algunos servidores y puertas de enlace nunca envían el certificado raíz, aunque se haya configurado. En esos casos, esta validación más estricta no es posible.

Si hay una puerta de enlace configurada con estos certificados válidos, se puede utilizar esta configuración sin el certificado raíz:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio

La aplicación Citrix Workspace usa estos dos certificados. Busca un certificado raíz en el dispositivo del usuario. Si la aplicación Citrix Workspace encuentra un certificado raíz que se valida correctamente y también es de confianza (por ejemplo, el ejemplo de certificado raíz), la conexión se realiza

correctamente. De lo contrario, la conexión falla. Esta configuración proporciona el certificado intermedio que necesita la aplicación Citrix Workspace, pero también permite que la aplicación Citrix Workspace elija cualquier certificado raíz válido y de confianza.

Si se configura una puerta de enlace con estos certificados:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio
- Certificado raíz incorrecto

Un explorador web podría ignorar el certificado raíz incorrecto. No obstante, la aplicación Citrix Workspace no ignora el certificado raíz incorrecto y la conexión falla.

Algunas entidades de certificación usan más de un certificado intermedio. En este caso, la puerta de enlace se configura con todos los certificados intermedios (pero sin el certificado raíz):

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio 1
- Ejemplo de certificado intermedio 2

> **Importante:**
>
> - Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas. Este certificado se usa donde hay más de un certificado raíz y donde un certificado raíz anterior sigue usándose como un certificado raíz posterior. En este caso, hay al menos dos certificados intermedios. Por ejemplo, el certificado raíz anterior *Class 3 Public Primary Certification Authority* tiene el certificado intermedio correspondiente de firmas cruzadas *Verisign Class 3 Public Primary Certification Authority - G5*. No obstante, un certificado raíz posterior correspondiente *Verisign Class 3 Public Primary Certification Authority - G5* también está disponible y reemplaza a *Class 3 Public Primary Certification Authority*. El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.
> - El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo nombre de sujeto (Emitido para). Pero el certificado intermedio con firmas cruzadas tiene otro nombre de emisor (Emitido por). Esto distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como el ejemplo de certificado intermedio 2).

Se recomienda esta configuración, sin certificado raíz y sin certificado intermedio con firmas cruzadas:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio

No configure la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque seleccionará el certificado raíz anterior:

- Ejemplo de certificado de servidor

- Ejemplo de certificado intermedio
- Ejemplo de certificado intermedio con firmas cruzadas [no recomendado]

No se recomienda configurar la puerta de enlace solamente con el certificado del servidor:

- Ejemplo de certificado de servidor

En este caso, si la aplicación Citrix Workspace no puede localizar todos los certificados intermedios, la conexión falla.

Workspacecheck

Ofrecemos un script, workspacecheck.sh, como parte del paquete de instalación de la aplicación Citrix Workspace. El script comprueba si su dispositivo cumple todos los requisitos del sistema para poder utilizar todas las funcionalidades de la aplicación Citrix Workspace. El script se halla en el directorio `Utilities` del paquete de instalación.

Para ejecutar el script workspacecheck.sh

1. Abra el terminal de su máquina Linux.
2. Escriba `cd $ICAROOT/util` y presione **Entrar** para ir al directorio `Utilities` del paquete de instalación.
3. Escriba `./workspacecheck.sh` para ejecutar el script.

Aplicaciones y sistemas operativos que ya no se mantienen

Citrix no ofrece asistencia ni desarrollo en el contexto de aplicaciones y sistemas operativos que ya no desarrollan sus proveedores.

Al intentar solucionar y resolver un problema notificado, Citrix evalúa si el problema está relacionado directamente con una aplicación o sistema operativo obsoletos. Para ayudarle a determinarlo, es posible que Citrix le solicite reproducir un problema con la versión compatible de la aplicación o del sistema operativo. Si el problema puede estar relacionado con la aplicación o sistema operativo obsoletos, Citrix no investigará más el problema.

Instalación, actualización y desinstalación

April 18, 2023

Para instalar la aplicación Citrix Workspace, descargue el archivo desde el sitio web Descargas de Citrix.

Verificar la versión de la aplicación Citrix Workspace

Siga estos pasos para verificar la versión actual de la aplicación Citrix Workspace instalada en el sistema:

1. Abra una ventana de terminal.
2. Ejecute este comando:

   Para paquetes Debian:

   ```
   dpkg --list | grep -i icaclient
   <!--NeedCopy-->
   ```

   O BIEN:

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   <!--NeedCopy-->
   ```

   Para paquetes RedHat:

   ```
   rpm -qa | grep -i icaclient

   <!--NeedCopy-->
   ```

   O BIEN:

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   <!--NeedCopy-->
   ```

   Para paquetes Tarball:

   ```
   cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
   <!--NeedCopy-->
   ```

Instalación manual

Descargue los siguientes paquetes desde la página Descargas de Citrix.

Paquetes Debian

Instale el paquete `Icaclient` según la arquitectura de su sistema operativo.

Para utilizar la redirección USB genérica, instale uno de los paquetes `ctxusb`, según la arquitectura de su sistema operativo.

> **Nota:**
>
> Para evitar el problema de compatibilidad, asegúrese de instalar la misma versión de los paquetes `Icaclient` y `ctxusb`.

Nombre del paquete	Contenido
Paquetes Debian (Ubuntu, Debian, Linux Mint, etc.)	
`icaclient_<version>_amd64.deb`	Compatibilidad con el autoservicio, x86_64 de 64 bits
`icaclient_<version>_i386.deb`	Compatibilidad con el autoservicio, x86 de 32 bits
`icaclient_<version>_armhf.deb`	Compatibilidad con el autoservicio, armhf
`ctxusb_<version>_amd64.deb`	Paquete USB, x86_64 de 64 bits
`ctxusb_<version>_i386.deb`	Paquete USB, x86 de 32 bits
`ctxusb_<version>_armhf.deb`	Paquete USB, armhf

Instalación con un paquete Debian

> **Requisitos previos:**
>
> Compruebe que ha instalado todos los requisitos del sistema necesarios, tal y como se indica en la sección Requisitos del sistema.

Al instalar la aplicación Citrix Workspace desde el paquete Debian en Ubuntu, abra los paquetes en el Centro de software de Ubuntu.

En estas instrucciones, reemplace
nombre_del_paquete por el nombre del paquete que intenta instalar.

Este procedimiento usa una línea de comandos y el administrador de paquetes nativo de Ubuntu, Debian o Mint. En su lugar, para instalar el paquete, haga doble clic en el paquete DEB descargado, dentro del explorador de archivos. Normalmente, esta acción inicia un administrador de paquetes que descarga el software necesario que falte. Si no hay ningún administrador de paquetes disponible, Citrix recomienda utilizar **gdebi**, una herramienta de línea de comandos.

> **Nota:**
>
> En Ubuntu 20.04.5 o una versión posterior, al hacer doble clic en el archivo del paquete `.deb`, se abre el instalador de Snap Store. Este instalador no admite instrucciones del usuario. Por lo

> tanto, debe instalar la aplicación Citrix Workspace mediante la línea de comandos en un terminal o mediante otros instaladores de software como `gnome-software`, `gdebi` o `synaptics`.

Para instalar el paquete mediante la línea de comandos:

1. Inicie sesión como usuario con privilegios (root).
2. Abra una ventana de terminal.
3. Ejecute la instalación mediante uno de estos comandos:
   - `apt`: Utilice este comando para instalar la aplicación Citrix Workspace con dependencia:

     ```
     sudo apt install -f ./icaclient_<version>._amd64.deb
     <!--NeedCopy-->
     ```

     Para instalar el paquete USB, ejecute este comando:

     ```
     sudo apt install -f ctxusb_<version>._amd64.deb
     <!--NeedCopy-->
     ```

   - `dpkg -i`: Utilice este comando para instalar la aplicación Citrix Workspace:

     ```
     sudo dpkg -i icaclient_<version>_amd64.deb
     sudo apt-get -f install
     <!--NeedCopy-->
     ```

     Para instalar el paquete USB, ejecute este comando:

     ```
     sudo dpkg -i ctxusb_<version>_amd64.deb
     sudo apt-get -f install
     <!--NeedCopy-->
     ```

   - `gdebi`: Utilice este comando para instalar la aplicación Citrix Workspace:

     ```
     gdebi icaclient_<version>_amd64.deb
     <!--NeedCopy-->
     ```

   Para instalar el paquete USB, ejecute este comando:

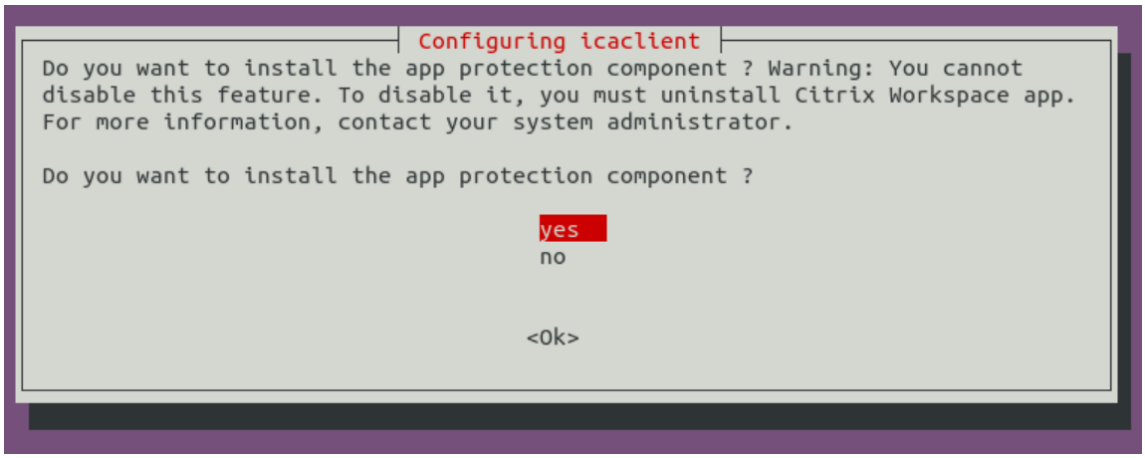
   ```
   ```
   gdebi ctxusb_<version>_amd64.deb
   <!--NeedCopy--> ```
   ```

   > **Nota:**

 
   ```

> El paquete `ctxusb` es opcional para ofrecer la funcionalidad de redirección de USB genérico

4. A partir de la versión 2101, aparece este mensaje interactivo, donde se le pide que instale la protección de aplicaciones:



5. Seleccione **Sí** para continuar con la instalación con el componente de protección de aplicaciones.

Instalación silenciosa del componente de protección de aplicaciones en paquetes Debian

A partir de la versión 2102, la protección de aplicaciones se ofrece en la versión Debian de la aplicación Citrix Workspace.

Para una instalación silenciosa del componente de protección de aplicaciones, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:

```
export DEBIAN_FRONTEND="noninteractive"
<!--NeedCopy-->
```

```
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"
<!--NeedCopy-->
```

```
sudo debconf-show icaclient
<!--NeedCopy-->
```

```
sudo apt install -f ./icaclient_<version>._amd64.deb`

<!--NeedCopy-->
```


Paquetes Red Hat

Instale el paquete `ICAClient` según la arquitectura de su sistema operativo.

Para utilizar la redirección USB genérica, instale uno de los paquetes `ctxusb`, según la arquitectura de su sistema operativo.

> **Nota:**
>
> Para evitar el problema de compatibilidad, asegúrese de instalar la misma versión de los paquetes `Icaclient` y `ctxusb`.

Nombre del paquete	Contenido
Paquetes Red Hat (Red Hat, SUSE, Fedora, etc.)	
`ICAClient-rhel-<version>.x86_64.rpm`	Compatibilidad con el autoservicio, basado en Red Hat (incluido Linux VDA), x86_64 de 64 bits
`ICAClient-rhel-<version>.i386.rpm`	Compatibilidad con el autoservicio, basado en Red Hat, x86 de 32 bits
`ICAClient-suse-<version>.x86_64.rpm`	Compatibilidad con el autoservicio, basado en SUSE, x86_64 de 64 bits
`ICAClient-suse-<version>.i386.rpm`	Compatibilidad con el autoservicio, basado en SUSE, x86 de 32 bits
`ctxusb-<version>.x86_64.rpm`	Paquete USB, x86_64 de 64 bits
`ctxusb-<version>.i386.rpm`	Paquete USB, x86 de 32 bits

> **Nota:**
>
> El paquete RPM `SuSE 11 SP3 Full Package (Self-Service Support)` se ha retirado.

Instalación con un paquete RPM

Si está instalando la aplicación Citrix Workspace desde el paquete RPM en SUSE, use las utilidades YaST o Zypper. La utilidad RPM instala el paquete `.rpm`. Se produce un error si faltan las dependencias necesarias.

> **Sugerencia:**
>
> El Administrador de paquetes RPM no instala el software necesario que falte.
>
> - Para los clientes que utilizan SUSE, descargue e instale el software mediante `zypper`

> `install <file name>` desde una línea de comandos en OpenSUSE.
> - Para los clientes que utilizan Red Hat, descargue e instale el software mediante `yum localinstall <filename>` en Fedora/Red Hat.

Para la instalación a partir del paquete RPM

> **Requisitos previos:**
>
> Compruebe que ha instalado todos los requisitos del sistema necesarios, tal y como se indica en la sección Requisitos del sistema.

1. Configure el repositorio EPEL.

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

2. Inicie sesión como usuario con privilegios (root).
3. Abra una ventana de terminal.
4. Escriba Zypper en para ejecutar la instalación de estos tres paquetes.

   > **Nota:**
   >
   > - `ctxusb` es un paquete opcional. Instale el paquete para ofrecer la redirección de USB genérico.
   > - `ctxappprotection` es un paquete opcional. Instale el paquete solo si quiere instalar el componente de protección de aplicaciones.

   Para las instalaciones de SUSE:

   - `zypper in ICAClient-suse-<version>.x86_64.rpm`
   - `zypper in ctxusb-<version>.x86_64.rpm`
   - `zypper in ctxappprotection-<version>.x86_64.rpm`

   Para las instalaciones de Red Hat:

   - `yum localinstall ICAClient-rhel-<version>.x86_64.rpm`
   - `yum localinstall ctxusb-<version>.x86_64.rpm`
   - `yum localinstall ctxappprotection-<version>.x86_64.rpm`

Para instalar un paquete que falta

En una distribución basada en Red Hat (RHEL, CentOS, Fedora, etc.), si aparece el siguiente mensaje de error:

```
1  "… requires libwebkitgtk-1.0.so.0"
```

Agregue un repositorio EPEL (los detalles se pueden consultar en https://docs.fedoraproject.org/en-US/epel/).

Paquetes tarball

Instale uno de los paquetes siguientes, según la arquitectura de su sistema operativo.

Nombre del paquete	Contenido
Tarballs (instalación por script para cualquier distribución)	
`linuxx64-<version>.tar.gz`	Intel de 64 bits
`linuxx86-<version>.tar.gz`	Intel de 32 bits
`linuxarmhf-<version>.tar.gz`	armhf

> **Nota:**
>
> - Si quiere personalizar la ubicación de instalación, instale la aplicación Citrix Workspace desde el paquete tarball. Si quiere instalar los paquetes necesarios automáticamente, instale la aplicación Citrix Workspace desde el paquete Debian o desde el paquete RPM.
> - No utilice dos métodos de instalación diferentes en la misma máquina. Si lo hace, es probable que vea mensajes de error y un comportamiento no deseado.

Instalación con un paquete tarball

> **Nota:**
>
> El paquete tarball no realiza comprobaciones de dependencias ni instala dependencias. Es necesario resolver por separado todas las dependencias del sistema.

1. Abra una ventana de terminal.
2. Extraiga el contenido del archivo `.tar.gz` en un directorio vacío. Por ejemplo, escriba: `tar xvfz packagename.tar.gz`.
3. Escriba `./setupwfc` y presione Entrar para ejecutar el programa de instalación.

4. Acepte el valor predeterminado de `1` (para instalar la aplicación Citrix Workspace) y presione **Entrar**.
5. Escriba la ruta y el nombre del directorio de instalación requerido y, a continuación, presione Entrar. O bien presione Entrar para instalar la aplicación Citrix Workspace 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 `$HOME/ICAClient/platform`. "Platform" es un identificador generado por el sistema para el sistema operativo instalado; por ejemplo, `$HOME/ICAClient/linuxx86` para la plataforma Linux/x86.

   > **Nota:**
   >
   > Si especifica una ubicación no predeterminada, establezca la ubicación de $ICAROOT en `$HOME/.profile` o en `$HOME/.bash\\_profile`.

6. Cuando se le pida que continúe, escriba `y` y, a continuación, presione Entrar.
7. Puede elegir si quiere integrar la aplicación Citrix Workspace en el entorno de escritorio. La instalación crea una opción de menú desde la cual los usuarios pueden iniciar la aplicación Citrix Workspace. Escriba `y` en el símbolo del sistema para habilitar la integración.
8. Si ha instalado `GStreamer` previamente, puede elegir si quiere integrar `GStreamer` en la aplicación Citrix Workspace y ofrecer la aceleración multimedia HDX MediaStream. Para integrar la aplicación Citrix Workspace en `GStreamer`, escriba `y` en el símbolo del sistema.

   > **Nota:**
   >
   > En algunas plataformas, instalar el cliente a partir de un paquete tarball puede provocar que el sistema deje de responder tras solicitarle una integración en KDE y GNOME. Este problema ocurre con la primera inicialización de gstreamer-0.10. Si se produce este problema, finalice el proceso de instalación (con la combinación de teclas Ctrl+C) y ejecute el comando `gst-inspect-0.10 -- gst-disable-registry-fork --version`. Después de ejecutar el comando, puede volver a ejecutar el paquete tarball sin sufrir el problema.

9. Si inicia sesión como usuario privilegiado (raíz), elija instalar la compatibilidad con USB para aplicaciones VDI publicadas de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Escriba `y` en el símbolo del sistema para instalar la compatibilidad con USB.

> **Nota:**
>
> Si no ha iniciado sesión como usuario con privilegios (root), aparecerá esta advertencia:
>
> "USB support cannot be installed by non-root users. Run the installer as root to access this install option".

10. Una vez completada la instalación, aparecerá nuevamente el menú principal de instalación. Para salir de la instalación, escriba 3 y presione Entrar.

Desinstalación

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 `$HOME/ICAClient/platform`. La variable "platform" es un identificador generado por el sistema para el sistema operativo instalado; por ejemplo, `$HOME/ICAClient/linuxx86` para la plataforma Linux/x86. El valor predeterminado de las instalaciones con usuarios con privilegios es `/opt/Citrix/ICAClient`.

> **Notas:**
>
> - Para desinstalar la aplicación Citrix Workspace, tiene que haber iniciado sesión como el mismo usuario que la instaló.
> - Al desinstalar la aplicación Citrix Workspace, es posible que no se quiten automáticamente los archivos de caché desactualizados que hay en `$HOME/.local/share/webkitgtk`. Como solución temporal, quite manualmente los archivos de caché.

Para desinstalar la aplicación Citrix Workspace en el paquete tarball

1. Para ejecutar la instalación, escriba `$ICAROOT/setupwfc` y presione Entrar.
2. Para quitar el cliente, escriba 2 y presione **Entrar**.

Para desinstalar la aplicación Citrix Workspace en sistemas operativos Debian/Ubuntu

1. Abra una ventana de terminal.
2. Ejecute la instalación mediante uno de estos comandos:

```
sudo apt remove icaclient -y
<!--NeedCopy-->
```

```
sudo apt autoremove -y
<!--NeedCopy-->
```

O bien:


```
sudo apt remove icaclient -y
<!--NeedCopy-->
```

```
sudo apt purge icaclient -y
<!--NeedCopy-->
```

> **Nota:**
>
> También puede quitar el paquete Debian con las herramientas estándar de su sistema operativo.

Para desinstalar la aplicación Citrix Workspace en los sistemas operativos Fedora/RHEL/CentOS

1. Abra una ventana de terminal.
2. Ejecute la instalación con este comando:

```
yum remove icaclient -y
<!--NeedCopy-->
```

> **Nota:**
>
> También puede quitar el paquete RPM con las herramientas estándar de su sistema operativo.

Verifique si la desinstalación de la aplicación Citrix Workspace se ha realizado correctamente. Para obtener más información, consulte la sección Verificar la versión de la aplicación Citrix Workspace.

Actualización

Antes de actualizar la aplicación Citrix Workspace, verifique la versión actual de la aplicación Citrix Workspace instalada en el sistema. Para obtener más información, consulte la sección Verificar la versión de la aplicación Citrix Workspace.

Para actualizar la aplicación Citrix Workspace a una versión más reciente, descargue e instale la aplicación Citrix Workspace más reciente desde Descargas de Citrix. Para el procedimiento de instalación, puede seguir los pasos que se mencionan en esta sección de la instalación:

- Paquetes Debian
- Paquetes Red Hat
- Paquetes tarball

Si tiene la aplicación Citrix Workspace instalada en su sistema, el sistema detecta la aplicación existente y la actualiza a una versión más reciente. Sin embargo, para los paquetes Tarball, considere el caso en el que haya instalado la versión anterior de la aplicación en una carpeta y haya instalado la

versión más reciente de la aplicación en una carpeta diferente. En este caso, es posible que existan ambas versiones de la aplicación en el sistema.

La superposición de pantalla de **Citrix Workspace** aparece en el primer inicio de la aplicación, al actualizar la aplicación, y al desinstalarla y reinstalarla. Haga clic en **Aceptar** para seguir usando la aplicación Citrix Workspace o haga clic en **Más información** para obtener más detalles.

Introducción

January 18, 2023

Este artículo es un documento de referencia que le servirá de ayuda a la hora de empezar a usar la aplicación Citrix Workspace para Linux.

Verifique la versión actual de la aplicación Citrix Workspace instalada en su sistema. Para obtener más información, consulte la sección Verificar la versión de la aplicación Citrix Workspace.

Almacén

Un **almacén** reúne las aplicaciones y los escritorios disponibles para un usuario en un mismo lugar. Un usuario puede tener varios almacenes y cambiar de uno a otro según sea necesario. Un administrador entrega la URL del almacén que tiene recursos y parámetros preconfigurados. Puede acceder a estos almacenes a través de la aplicación Citrix Workspace.

Para obtener más información sobre los almacenes, consulte la documentación de StoreFront.

Tipos de almacenes

Puede agregar estos tipos de almacenes en la aplicación Citrix Workspace:

- Workspace
- StoreFront
- Almacén de Citrix Gateway
- Almacén web personalizado

Workspace

Citrix Workspace es un almacén de aplicaciones de empresa basado en la nube que proporciona acceso seguro y unificado a aplicaciones, escritorios y contenido (recursos) desde cualquier lugar y en cualquier dispositivo. Estos recursos pueden ser Citrix DaaS, aplicaciones de contenido, aplicaciones locales y móviles, aplicaciones web y SaaS y aplicaciones para explorador web. Para obtener más información, consulte Descripción general de Citrix Workspace.

StoreFront

StoreFront es un intuitivo almacén de aplicaciones de empresa local que combina aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops en un solo almacén.

Para obtener más información, consulte la documentación de StoreFront.

Almacén de Citrix Gateway

Configure Citrix Gateway para permitir que los usuarios se conecten desde fuera de la red interna. Por ejemplo, usuarios que se conectan desde Internet o ubicaciones remotas.

Almacenes web personalizados

A partir de la versión 2203, esta función está disponible de forma general para la aplicación Citrix Workspace. Puede acceder al almacén web personalizado de su organización desde la aplicación Citrix Workspace.

Para usar esta función, si Global App Configuration Service está disponible:

El administrador debe agregar el dominio o el almacén web personalizado a la lista de URL permitidas en Global App Configuration Service. Tras agregar el dominio o el almacén web personalizado, proporcione la URL del almacén web personalizado o la dirección de correo electrónico en la pantalla **Agregar cuenta** de la aplicación Citrix Workspace. El almacén web personalizado se abre en la ventana de la aplicación Workspace nativa.

Para obtener más información sobre cómo configurar las direcciones URL de almacén web para los usuarios finales, consulte Global App Configuration Service.

> **Nota:**
>
> La función para anclar el diseño de pantalla con varios monitores no está disponible en el almacén web personalizado.

Para quitar el almacén web personalizado, vaya a **Cuentas** > **Agregar o quitar cuentas**, seleccione la URL del almacén web personalizado y haga clic en **Quitar**.

Como requisito previo, debe habilitar el almacén web personalizado en el archivo `AuthManConfig.xml`. Para habilitarlo:

1. Vaya al archivo de configuración `$ICAROOT/config/AuthManConfig.xml`.
2. Agregue estas entradas:

```
<key>AppConfigEnabled</key>
<value>true</value>
<!--NeedCopy-->
```


Para usar esta función, si Global App Configuration Service no está disponible:

Haga estos cambios en la configuración:

1. Vaya al archivo de configuración `$ICAROOT/config/AuthManConfig.xml`.
2. Agregue estas entradas:

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

3. Agregue la lista de direcciones URL que deben tenerse en cuenta para el almacén web personalizado de la siguiente manera.

```
<AllowedWebStoreCache>
<value><URL1></value>
<value><URL2></value>
..
<value>....</value>
</AllowedWebStoreCache>
<!--NeedCopy-->
```

> **Nota:**
>
> Solo puede usar las URL que figuran en el archivo `AuthManConfig.xml` para el almacén web personalizado. Puede agregar direcciones URL adicionales al archivo `AuthManConfig.xml` que quiera tener en cuenta para el almacén web personalizado.

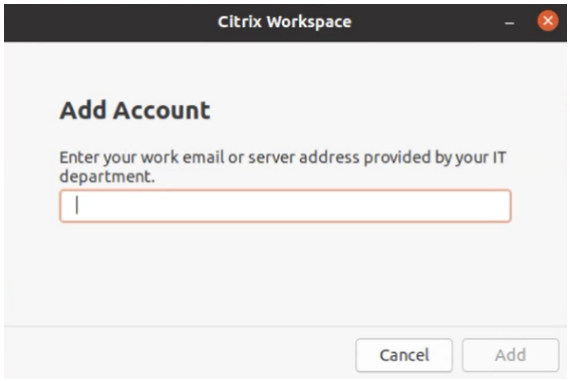
Agregar URL de almacén a la aplicación Citrix Workspace

Puede hacer lo siguiente para proporcionar a los usuarios la información de cuenta que necesitan para acceder a sus escritorios y aplicaciones virtuales:

- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente
- Configurar la detección automática basada en correo electrónico
- Agregar almacén a través de la CLI

Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Tras instalar correctamente la aplicación Citrix Workspace y al iniciar la aplicación por primera vez, aparece esta pantalla. Los usuarios deben introducir una dirección de correo electrónico o de servidor para acceder a las aplicaciones y escritorios. Cuando un usuario introduce la información de una cuenta nueva, la aplicación Citrix Workspace intenta verificar la conexión. Si la conexión puede establecerse, la aplicación Citrix Workspace solicita al usuario que inicie sesión en la cuenta.



Para permitir que los usuarios configuren sus cuentas manualmente, distribuya la información que necesitan para conectarse con sus escritorios y aplicaciones virtuales.

- Para conectarse a un almacén de Workspace, proporcione la URL de Workspace.
- Para conectarse a un almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: `https://servername.company.com`.
- Para conectarse a través de Citrix Gateway, proporcione a los usuarios el nombre de dominio completo de Citrix Gateway.

Detección automática de almacenes por dirección de correo electrónico

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

Ya puede proporcionar su dirección de correo electrónico en la aplicación Citrix Workspace para detectar automáticamente el almacén asociado a esa dirección de correo electrónico. Si hay varios almacenes asociados a un dominio, de forma predeterminada se agrega el primer almacén devuelto por Global App Configuration Service como el almacén elegido. Los usuarios siempre pueden cambiar a otro almacén si fuera necesario.

Para inhabilitar esta función, haga lo siguiente:

1. Vaya al archivo `$ICAROOT/config/AuthManConfig.xml`.
2. Establezca esta entrada en false.

```
<key>AppConfigEnabled</key>
<value>false</value>
<!--NeedCopy-->
```

Agregar almacén a través de la CLI

Instale la aplicación Citrix Workspace para Linux como administrador desde la interfaz de línea de comandos.

Para obtener más información, consulte la sección Storebrowse.

Configuración

Puede descargar el paquete de instalación, personalizar la configuración y, a continuación, instalar la aplicación Citrix Workspace.

Puede modificar el contenido del paquete de la aplicación Citrix Workspace y, a continuación, reempaquetar los archivos.

Personalizar la instalación

1. Expanda el archivo del paquete de la aplicación Citrix Workspace en un directorio vacío. El archivo del paquete se llama platform.major.minor.release.build.tar.gz (por ejemplo, `linuxx86-<version>.tar.gz` para la plataforma Linux/x86).
2. Realice los cambios requeridos en el paquete de la aplicación Citrix Workspace. Por ejemplo, puede agregar un certificado raíz TLS para utilizar un certificado de una entidad de certificación que no forma parte de la instalación estándar de la aplicación Citrix Workspace.
3. Abra el`PkgID` archivo.
4. Agregue la siguiente línea para indicar que se ha modificado el paquete:

   MODIFIED=traceinfo

   donde `traceinfo` es la información que indica quién realizó el cambio y cuándo lo hizo.
5. Guarde el archivo y ciérrelo.
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 se actualiza, puede producirse un error al instalar el nuevo paquete. Los cambios pueden consistir en una actualización en el tamaño de todos los archivos modificados, o la inclusión de nuevas líneas en cualquiera de los archivos agregados al paquete. Las columnas en la lista de archivos del paquete son:

   - Tipo de archivo
   - Ruta relativa
   - Subpaquete (siempre establecido en `cor`)
   - Permisos
   - Propietario
   - Grupo
   - Tamaño

8. Guarde el archivo y ciérrelo.
9. Use el comando tar para reconstruir el archivo de paquete de la aplicación Citrix Workspace. Por ejemplo, `tar czf ../newpackage.tar.gz *`, donde `newpackagez` es el nombre del nuevo archivo de paquete de la aplicación Citrix Workspace.

El webkit más reciente está disponible

La aplicación Citrix Workspace para Linux necesita libwebkit2gtk (2.16.6 o una versión posterior).

libwebkit2gtk tiene las siguientes ventajas:

- Experiencia de interfaz de usuario mejorada. webkit2gtk es compatible con la función de redirección de contenido del explorador web. Utilice la versión 2.24 de webkit2gtk o una posterior para obtener una mejor experiencia de visionado en YouTube.
- La versión 2.16.6 de webkit2gtk y posteriores mejoran la experiencia de inicio de sesión y el tiempo que se tarda en iniciar sesión.
- La aplicación funciona mejor con distribuciones de Linux más recientes y ofrece las últimas correcciones de seguridad del WebKit.

> **Nota:**
>
> webkit2gtk no está disponible en algunas distribuciones de Linux. Como solución temporal, tenga en cuenta las siguientes opciones:
>
> - Compile webkit2gtk a partir de la fuente antes de instalar la versión 1906 de la aplicación Citrix Workspace.
> - Mueva a una distribución de Linux posterior que admita webkit2gtk 2.16.6 o una versión más reciente.

Inicio

Puede iniciar la aplicación Citrix Workspace en el símbolo del sistema de un terminal o desde alguno de los entornos de escritorio admitidos.

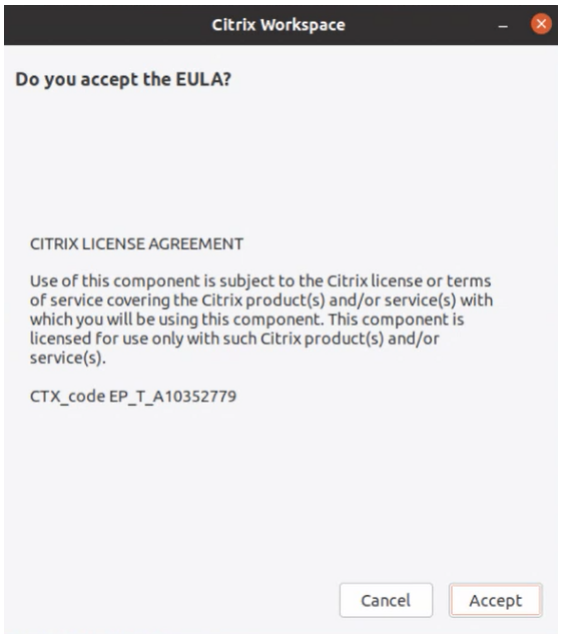
Compruebe que la variable de entorno `ICAROOT` está establecida de modo que apunte al directorio de instalación real.

> **Sugerencia:**
>
> Estas instrucciones no se aplican a instalaciones realizadas a partir de paquetes web ni a aquellas en que se usa tarball. Se aplican cuando no se cumplen los requisitos de autoservicio.

Símbolo del sistema de un terminal

Para iniciar la aplicación Citrix Workspace en el símbolo del sistema de un terminal:

1. Escriba `/opt/Citrix/ICAClient/selfservice`
2. Presione Entrar (donde /opt/Citrix/ICAClient es el directorio en el que se instaló la aplicación Citrix Workspace).
   Aparece el cuadro de diálogo **¿Acepta los términos del contrato de licencia?**



3. Haga clic en **Aceptar** para pasar a agregar el almacén.

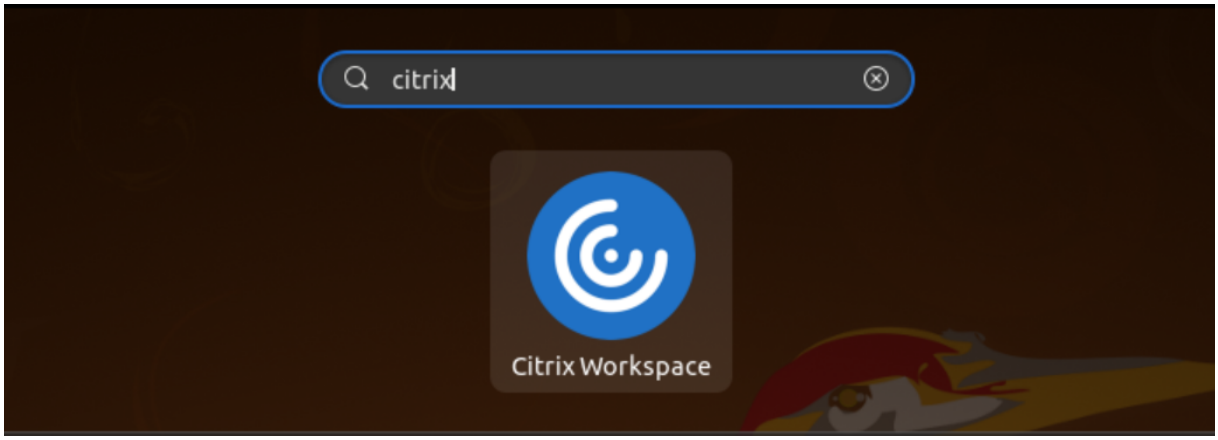
> **Nota:**
>
> El cuadro de diálogo **¿Acepta los términos del contrato de licencia?** solo aparece si accede a la aplicación Citrix Workspace para Linux por primera vez después de la instalación.

Escritorio Linux

Para iniciar la aplicación Citrix Workspace desde un entorno de escritorio, búsquela con un administrador de archivos.

En algunos escritorios, también puede iniciar la aplicación Citrix Workspace desde un menú. La aplicación Citrix Workspace está disponible en distintos menús, según su distribución de Linux.

En Ubuntu, el icono de la aplicación Citrix Workspace aparece de esta manera:



Preferencias

Para definir sus preferencias, haga clic en **Preferencias** en el menú de la aplicación Citrix Workspace. Puede controlar lo siguiente:

- Cómo se muestran los escritorios
- Conectarse a diferentes aplicaciones y escritorios
- Administrar el acceso a archivos y dispositivos

Administración de una cuenta

Para acceder a escritorios y aplicaciones, necesita una cuenta de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Es posible que su servicio de asistencia de TI le pida que agregue una cuenta a Citrix Workspace para este fin. También pueden pedirle que use un servidor Citrix Gateway o Access Gateway diferente para una cuenta existente. También puede quitar cuentas de Citrix Workspace.

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**. Para obtener más información, contacte con el administrador del sistema.
   - Para cambiar los datos de un almacén utilizado por la cuenta (por ejemplo, la puerta de enlace predeterminada), haga clic en **Modificar**.
   - Para quitar una cuenta, haga clic en **Quitar**.
2. Siga las instrucciones en pantalla. Cuando se le solicite, autentíquese en el servidor.

Pantalla de escritorio

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**.

Utilice la funcionalidad de la barra de herramientas **You can enable Desktop Viewer** para modificar dinámicamente la configuración de la ventana de la sesión remota.

Desktop Viewer

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.

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, admite varios monitores para los monitores intersecados. Los usuarios pueden alternar entre sesiones de escritorio y usar más de un escritorio mediante varias conexiones de Citrix Virtual Apps and Desktops o Citrix DaaS 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.

Al presionar **Ctrl+Alt+Inter**, se muestran los botones de la barra de herramientas de **Desktop Viewer** en una ventana emergente.

Reconexiones de sesión automáticas

La aplicación Citrix Workspace puede volver a conectarse a escritorios y aplicaciones que se hayan desconectado. Por ejemplo, tras un problema de infraestructura de red.

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

Acceso a los archivos locales

Es posible que un escritorio virtual o una aplicación necesiten acceder a archivos ubicados en el dispositivo. Usted puede controlar el alcance de 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 acceden a archivos locales.

2. Haga clic en **Agregar**, especifique la ubicación y seleccione una unidad para asignársela.

Micrófono y cámara web

Para configurar un micrófono o una cámara web, puede cambiar la forma 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 una de las siguientes opciones:

- **Usar mi micrófono y mi cámara web**: Para permitir que el escritorio o la aplicación usen el micrófono y la cámara web.
- **No usar mi micrófono ni mi cámara web**: Para prohibir que el escritorio o la aplicación usen el micrófono y la cámara web.

Flash Player

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

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

- **Optimizar el contenido**: Para mejorar la calidad de la reproducción, con el riesgo de disminuir la seguridad.
- **No optimizar el contenido**: Proporciona calidad de reproducción básica, sin disminuir la seguridad.
- **Preguntar siempre**: Para pedir permiso cada vez que se muestra contenido de Flash.

Conexión

La aplicación Citrix Workspace ofrece a los usuarios acceso de autoservicio seguro a aplicaciones y escritorios virtuales, y acceso a 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 Workspace

La página de inicio de la aplicación Citrix Workspace 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 Virtual Apps and Desktops o Citrix DaaS. Desde la página **Preferencias** > **Cuentas**, puede configurar la dirección URL de un servidor de StoreFront o, si está configurada la detección de cuentas basada en correo electrónico, escribir la dirección de correo electrónico.

> **Sugerencia:**
>
> Si utiliza el mismo nombre para varios almacenes en el servidor de StoreFront, agregue números a esos nombres para evitar duplicados. Los nombres de dichos almacenes dependen del orden en que se agregaron. Para la aplicación Citrix Workspace, se muestra la URL del almacén y esta identifica de forma única el almacén.

Después de conectarse a un almacén, el autoservicio 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 la aplicación Citrix Workspace y los servidores de Citrix Virtual Apps and Desktops o Citrix DaaS. También puede cambiar esos parámetros para conexiones individuales, si es necesario.

Aunque las tareas y responsabilidades de los administradores y los usuarios pueden superponerse, el término “usuario” se emplea para distinguir las tareas de los usuarios de las de los administradores.

Conexión con recursos desde una línea de comandos o explorador

Cuando se hace clic en el icono de una aplicación o de un escritorio en la página de inicio de la aplicación Citrix Workspace, 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 de StoreFront o Program Neighborhood mediante una línea de comandos

Requisito previo:

Asegúrese de que la aplicación Citrix Workspace conoce el almacén. Si es necesario, agréguelo mediante el comando siguiente:

```
./util/storebrowse --addstore \<store URL\>
```

1. Obtenga el ID único del escritorio o de la aplicación con que quiere conectarse. Este ID es la primera cadena entre comillas en una línea adquirida en uno de estos comandos:
    - Lista de todos los escritorios y las aplicaciones en el servidor:

      ```
      ./util/storebrowse -E <store URL>
      ```


- Genera una lista de los escritorios y las aplicaciones a los que se ha suscrito:

  ```
  ./util/storebrowse -S <store URL>
  ```

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

   ```
   ./util/storebrowse -L <desktop or application ID> <store URL>
   ```

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 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. Debido a la gran variedad de exploradores y sistemas operativos, puede ser necesaria alguna configuración manual.

Si configura manualmente los archivos `.mailcap` y `MIME` para Firefox, Mozilla o Chrome, use estas modificaciones de archivo. Con estas modificaciones, los archivos `.ICA` inician el ejecutable de la aplicación Citrix Workspace, `wfica`. Para utilizar otros exploradores, modifique la configuración del explorador, según corresponda.

1. Ejecute los siguientes comandos para una instalación de la aplicación Citrix Workspace sin privilegios de administrador. La configuración de ICAROOT se puede cambiar si se instala en una ubicación no predeterminada. Puede probar el resultado con el comando

   `xdg-mime query default application/x-ica`, el cual debe devolver “wfica.desktop”.

   ```
   export ICAROOT=/opt/Citrix/ICAClient
   ```

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

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

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

2. Cree 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;
   ```

   Quizá deba configurar la página Preferencias o Aplicaciones de Firefox.

   Para “Citrix ICA settings file content”, seleccione:

- “Citrix Workspace app Engine (predeterminado)” en el menú desplegable

  O bien:

- “Utilizar otros…” y, a continuación, seleccione el archivo /usr/share/applications/wfica.desktop (para una instalación de administrador de la aplicación Citrix Workspace)

  O bien:

- $HOME/.local/share/applications/wfica.desktop (para una instalación que sea de no administrador).

Central de conexiones

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. Este paso finaliza la sesión y cierra todas las aplicaciones que hubiera abiertas.
- Desconectarse de una sesión. Este paso 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.

Administración de una conexión

Para administrar una conexión desde la **Central de conexiones**:

1. En el menú de la aplicación Citrix Workspace, haga clic en **Central de conexiones**.

   Aparecerán los servidores que se utilizan y todas las sesiones activas.

2. Lleve a cabo una de las siguientes acciones:

   - Seleccione un servidor, desconecte o cierre la sesión, o consulte sus propiedades.
   - Seleccione una aplicación, cierre la ventana.

Configurar

May 9, 2023

Cuando se utiliza la aplicación Citrix Workspace para Linux, los siguientes pasos de configuración permiten a los usuarios acceder a sus aplicaciones y escritorios alojados.

Parámetros

Archivos de configuración

Para cambiar parámetros más avanzados o menos comunes, puede modificar los archivos de configuración de la aplicación Citrix Workspace. 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.

Si se pueden compartir sesiones, puede que se use una sesión existente en lugar de una recién configurada. Este parámetro puede hacer que la sesión ignore los cambios hechos en el archivo de configuración.

Parámetros predeterminados

Si quiere que los cambios se apliquen a todos los usuarios de la aplicación Citrix Workspace, modifique el archivo de configuración `module.ini` del directorio `$ICAROOT/config`.

> **Nota:**
>
> Si una entrada en `All\\_Regions.ini` se establece en un valor específico, el valor de esa entrada en `module.ini` no se utiliza. Los valores indicados en `All\\_Regions.ini` tienen prioridad sobre el valor en `module.ini`.

Archivo de plantilla

Si el archivo `$HOME/.ICAClient/wfclient.ini` no existe, `wfica` copia `$ICAROOT/config/wfclient.template` para crearlo. Cuando se realizan cambios en este archivo de plantilla, estos se aplican a todos los usuarios de la aplicación Citrix Workspace.

Configuración de usuario

Para aplicar cambios de configuración a un usuario, modifique el archivo `wfclient.ini` en el directorio `$HOME/.ICAClient` del usuario. La configuración de este archivo se aplica a las conexiones futuras de ese usuario.

Validación de las entradas del archivo de configuración

Para limitar los valores permitidos de las entradas en `wfclient.ini`, especifique las opciones o los intervalos de opciones que se permiten en `All\\_Regions.ini`.

Si especifica solo un valor, se utilizará ese valor. El archivo `$HOME/.ICAClient/All\\_Regions.ini` puede coincidir o reducir los valores posibles establecidos en el archivo `$ICAROOT/config/All\\_Regions.ini`; no puede eliminar las restricciones.

> **Nota:**
>
> El valor establecido en `wfclient.ini` tiene prioridad sobre el valor de `module.ini`.

Parámetros

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

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, considere que el parámetro `InitialProgram` va seguido de un signo igual (=) y que no se proporciona ningún valor. En este ejemplo, se aplica el valor predeterminado (no ejecutar un programa después de iniciar sesión).

Precedencia

El archivo `All\\_Regions.ini` especifica parámetros que pueden definir otros archivos. Puede restringir los valores de los parámetros o establecerlos de forma precisa.

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

1. `All\\_Regions.ini`: Los valores de este archivo supeditan los valores de:
   - El archivo `.ICA` de conexiones
   - `wfclient.ini`
2. `module.ini`: Los valores de este archivo se utilizan si no se han establecido en `All\\_Regions.ini`, en el archivo `.ICA` de conexiones ni en `wfclient.ini`. Sin embargo, estos valores no se restringen con las 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 la aplicación Citrix Workspace.

> **Nota:**
>
> Hay excepciones en este orden de prioridad. Por ejemplo, el código lee algunos valores específicamente de `wfclient.ini` por razones de seguridad.

Tiempo de espera por inactividad para la aplicación Citrix Workspace

> **Nota:**
>
> A partir de la versión 2303, esta función está disponible de forma general para la aplicación Citrix Workspace.

La función de tiempo de espera por inactividad cierra su sesión de la aplicación Citrix Workspace en función de un valor que establece el administrador. Los administradores pueden especificar el tiempo de inactividad que se permite antes de que se cierre la sesión de usuario automáticamente en la aplicación Citrix Workspace. Se cierra la sesión automáticamente cuando no hay actividad del mouse, del teclado ni táctil durante el intervalo de tiempo especificado dentro de la ventana de la aplicación Citrix Workspace. El tiempo de espera por inactividad no afecta a las sesiones de Citrix Virtual Apps and Desktops y Citrix DaaS ni a almacenes de Citrix StoreFront.

El valor del tiempo de espera por inactividad se puede establecer desde 10 minutos a 1440 minutos. El intervalo para cambiar este valor de tiempo de espera debe estar en múltiplos de 5. Por ejemplo: 10, 15, 20 o 25 minutos. De forma predeterminada, el tiempo de espera por inactividad no está configurado.

> **Nota:**
>
> Esta función solo es aplicable en implementaciones en la nube.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
<key>ITOEnabled</key>
<value>true</value>
<!--NeedCopy-->
```

Los administradores pueden configurar la propiedad inactivityTimeoutInMinutes mediante un módulo de PowerShell.

Pasos para configurar InactivityTimeoutInMinutes en la máquina cliente:

1. Descargue el módulo Configuring Citrix Workspace using PowerShell.
2. Para usar el módulo, debe generar un secreto y un ID de cliente de la API. Para obtener más información sobre cómo obtener credenciales y empezar a utilizar las API de Citrix Cloud, consulte Introducción a las API de Citrix Cloud.
3. Para importar este módulo, pase la ruta del directorio Citrix.Workspace.StoreConfigs al cmdlet Import-Module; es decir, desde el directorio que contiene este archivo, ejecute `Import-Module ./Citrix.Workspace.StoreConfigs`.
4. Una vez importado el módulo, ejecute `Get-Help -Full` para obtener ayuda sobre un cmdlet específico. Por ejemplo: `Get-Help Set-WorkspaceCustomConfigurations -Full`
5. Ejecute este comando para configurar `inactivityTimeoutInMinutes` en 1 hora. Por ejemplo:

```
Set-WorkspaceCustomConfigurations -WorkspaceUrl -ClientId -
    ClientSecret -InactivityTimeoutInMinutes "60"
```



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

No necesita ejecutar el comando anterior en todos los clientes; solo necesita ejecutarlo una vez y probarlo.

La experiencia del usuario final es la siguiente:

- Aparecerá una notificación tres minutos antes de que se le cierre la sesión, con la opción de mantener la sesión abierta o cerrar la sesión.
- Los usuarios pueden hacer clic en **Mantener sesión abierta** para descartar la notificación y seguir utilizando la aplicación. En ese caso, el temporizador de inactividad se restablece a su valor configurado. También puede hacer clic en **Cerrar sesión** para finalizar la sesión del almacén actual.

> **Nota:**
>
> La función de tiempo de espera por inactividad no admite distribuciones que tengan Wayland como el protocolo gráfico predeterminado. Para las distribuciones que tengan Wayland, quite la marca de comentario de cualquiera de estas opciones: `WaylandEnable=false` en `/etc/gdm/custom.conf` o en `/etc/gdm3/custom.conf`.

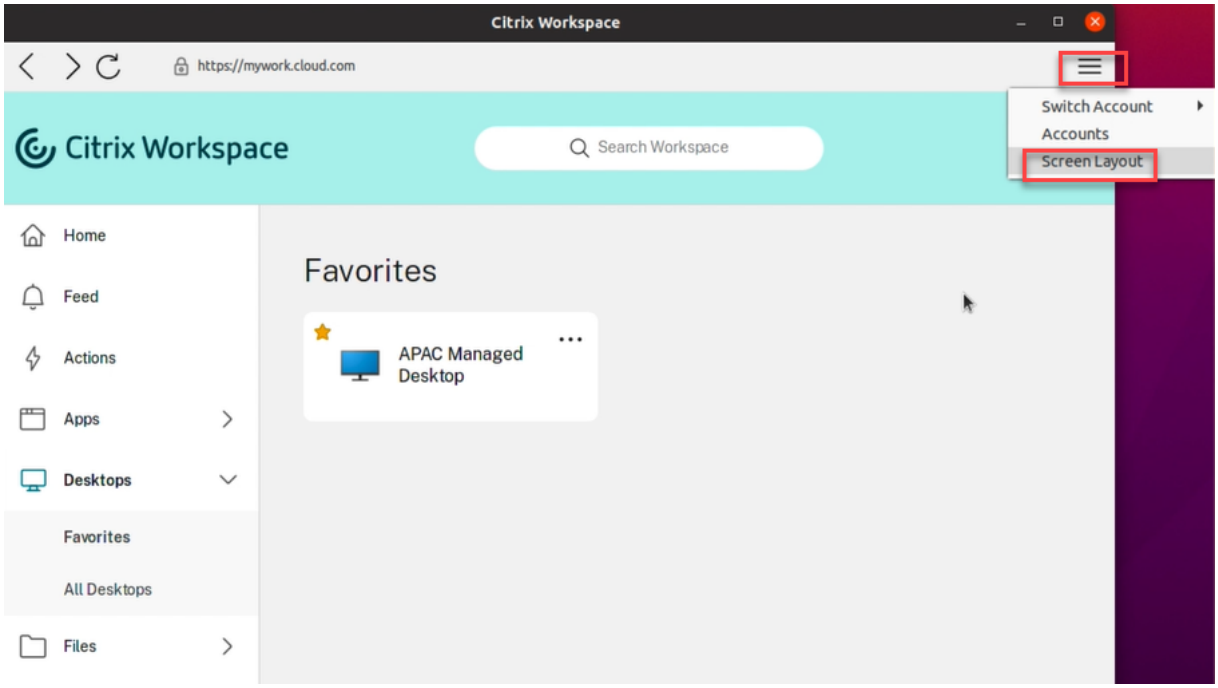
Anclaje de pantallas en almacenes web personalizados [Technical Preview]

A partir de la versión 2302, puede guardar la selección para el diseño de pantalla con varios monitores en almacenes web personalizados.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
<key>ScreenPinEnabled</key>
<value> true </value>
<!--NeedCopy-->
```

Una vez agregada la clave anterior, podrá ver la opción **Diseño de pantalla** en el menú de la aplicación Citrix Workspace.



Para seleccionar el diseño de pantalla, seleccione **Diseño de pantalla** en el menú de la aplicación Citrix Workspace. Aparece el cuadro de diálogo **Diseño de pantalla**.

Seleccione un escritorio virtual en el menú desplegable. La selección del diseño se aplica solamente al escritorio que seleccione.

Seleccione uno o varios mosaicos para formar una selección rectangular del diseño. A continuación, la sesión se muestra según la selección del diseño.

Limitaciones:

- Al habilitar el anclaje de pantalla, se inhabilita la función para guardar el diseño durante las sesiones.
- Esta función solo se aplica a escritorios marcados como favoritos.

Puede enviar sus comentarios sobre esta Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Optimización del rendimiento de la aplicación Citrix Workspace

A partir de la versión 2302, el rendimiento de la aplicación Citrix Workspace para Linux mejora al autenticarse mediante AuthManLite.

Global App Config Service [Technical Preview pública]

El nuevo Citrix Global App Configuration Service para Citrix Workspace ofrece a los administradores de Citrix entregar direcciones URL de servicio de Workspace a través de un servicio administrado de forma centralizada.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
1       <key>AppConfigEnabled</key>
2       <value> true </value>
3  <!--NeedCopy-->
```

Para obtener más información sobre los parámetros de las direcciones URL de servicio de Workspace, consulte la documentación de Global App Configuration Service.

> **Nota:**
>
> - La aplicación Citrix Workspace para Linux usa Global App Configuration Service solamente para entregar direcciones URL de servicio de Workspace.
> - Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en

> Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Workspace con funciones inteligentes [Technical Preview]

La aplicación Citrix Workspace 2111 está optimizada para sacar partido de las funciones inteligentes de Workspace cuando se publiquen. Para obtener más información, consulte Funciones inteligentes de Workspace: Microaplicaciones.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Compatibilidad con la correspondencia de PPP [Technical Preview]

A partir de la versión 2207, los valores de resolución de pantalla y escala de PPP establecidos en la aplicación Citrix Workspace se corresponden con los valores respectivos en la sesión de aplicaciones y escritorios virtuales. Puede establecer el valor de escala requerido en el cliente Linux y el escalado de la sesión del VDA se actualizará automáticamente.

El escalado de PPP se utiliza principalmente con monitores de gran tamaño y alta resolución. Esta función ayuda a mostrar los elementos siguientes a un tamaño que permite verlos cómodamente:

- Aplicaciones
- Texto
- Imágenes
- Otros elementos gráficos

Esta función está inhabilitada de forma predeterminada. Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya al archivo de configuración $HOME/.ICAClient/wfclient.ini.
2. Vaya a la sección [WFClient] y configure esta entrada:

   DPIMatchingEnabled=TRUE

Limitación:

Actualmente, la funcionalidad de correspondencia de PPP no admite el escalado fraccional en el lado del cliente.
Si el valor de la escala de PPP es elevado, es posible que la optimización de Microsoft Teams no funcione como es debido.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Inicio de sesión persistente

> **Nota:**
>
> A partir de la versión 2303, esta función está disponible de forma general para la aplicación Citrix Workspace.

La función de inicio de sesión persistente le permite mantener la sesión iniciada el período (de 2 a 365 días) configurado por su administrador. Cuando esta función está habilitada, no necesita proporcionar las credenciales de inicio de sesión para la aplicación Citrix Workspace durante el período configurado.

Con esta funcionalidad, las sesiones de SSO en Citrix DaaS se prolongan hasta 365 días. Esta ampliación se basa en el tiempo de vida de los tokens de larga duración. Sus credenciales se almacenan en la caché de forma predeterminada durante 4 días o la duración definida, lo que sea inferior. Y, luego, se prolonga cuando hay actividad de nuevo dentro de estos 4 días al conectarse a la aplicación Citrix Workspace.

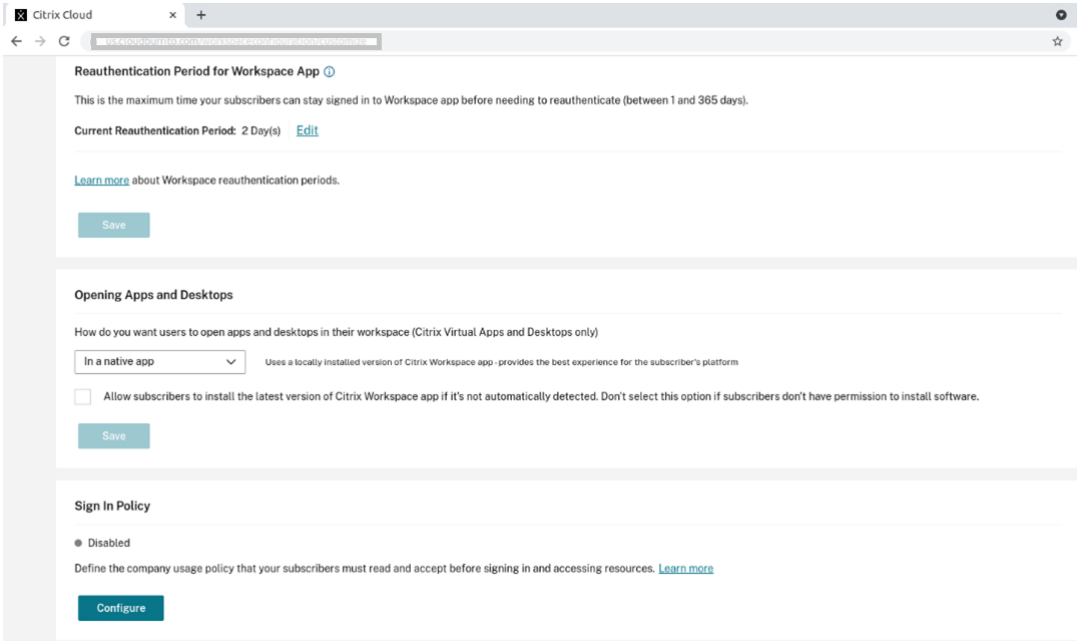
Configurar la función de inicio de sesión persistente

Un administrador debe configurar el inicio de sesión persistente en el entorno de Workspace con este procedimiento:

1. Inicie sesión en Citrix Cloud.
2. En la consola de Citrix Cloud, haga clic en el menú de la esquina superior izquierda de la pantalla.
3. Seleccione la opción **Configuración del Workspace** > **Personalizar** > **Preferencias**.
4. Desplácese hacia abajo hasta **Período de reautenticación de la aplicación Workspace**.
5. Haga clic en **Modificar** junto al campo **Período de reautenticación actual**.
6. Introduzca los días necesarios en el campo **Período de reautenticación actual**.

7. Debe introducir dos días o más en el campo **Período de reautenticación actual**.

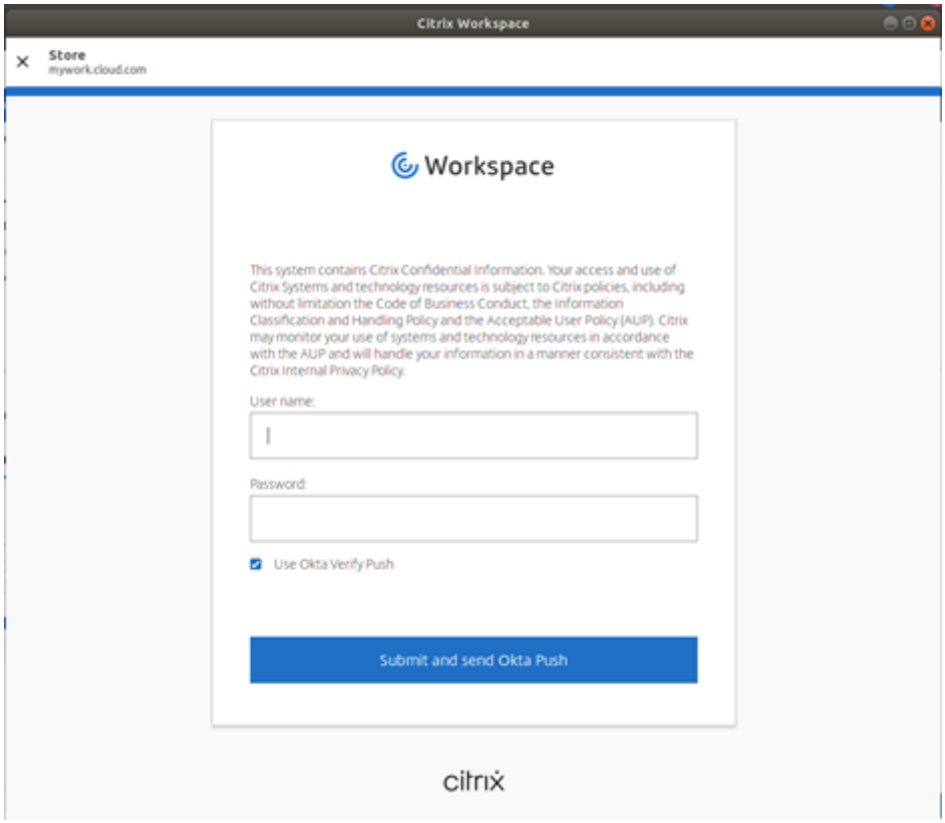
Para obtener más información, consulte las instrucciones de la **sección Período de reautenticación para la aplicación Workspace** en esta imagen:



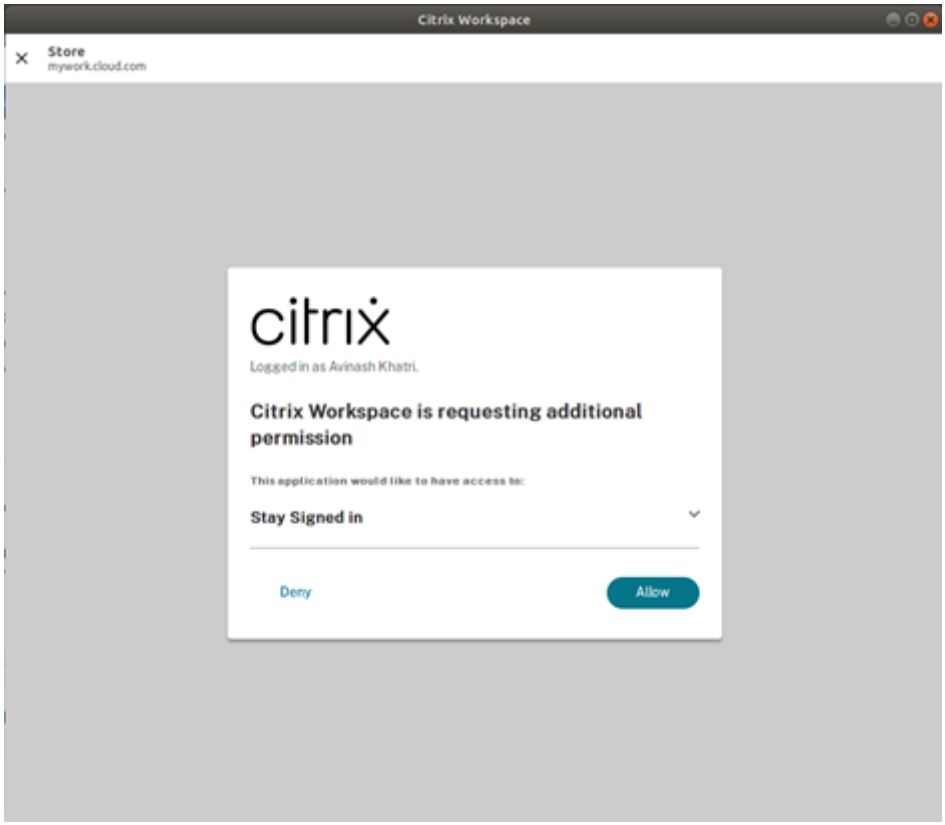
Experiencia con la autenticación mejorada

La ventana de inicio de sesión persistente está integrada en la ventana de autoservicio.

1. Acceda a la aplicación Citrix Workspace.
   Aparece la ventana de autenticación.



2. Inicie sesión con sus credenciales.
   Se le redirigirá a la solicitud de permiso para aceptar.



3. Haga clic en **Permitir**.

> **Nota:**
>
> Si selecciona **Denegar** y rechaza el consentimiento, verá una segunda solicitud de inicio de sesión, y tendrá que iniciar sesión en la aplicación Citrix Workspace cada 24 horas.

Inhabilitar la función de inicio de sesión

Un administrador puede inhabilitar la función de inicio de sesión persistente en la interfaz de usuario de Citrix Cloud o en el archivo `AuthManConfig.xml`. Sin embargo, el valor establecido en el archivo `AuthManConfig.xml` supedita el valor establecido en la interfaz de usuario de Citrix Cloud.

Usar la interfaz de usuario Citrix Cloud

1. Inicie sesión en Citrix Cloud.
2. En la consola de Citrix Cloud, haga clic en el menú de la esquina superior izquierda de la pantalla.
3. Seleccione la opción **Configuración del Workspace** > **Personalizar** > **Preferencias**.
4. Desplácese hacia abajo hasta **Período de reautenticación de la aplicación Workspace**.
5. Haga clic en **Modificar** junto al campo **Período de reautenticación actual**.
6. Introduzca un día en el campo **Período de reautenticación actual**.

Usar el archivo AuthManConfig.xml

Para inhabilitar la función de inicio de sesión persistente, haga lo siguiente:

1. Vaya al archivo <ICAROOT>/config/AuthManConfig.xml.
2. Defina los valores de esta manera:

```
<AuthManLite>

<primaryTokenLifeTime>1.00:00:00</primaryTokenLifeTime>

<secondaryTokenLifeTime>0.01:00:00</secondaryTokenLifeTime>

<longLivedTokenSupport>false</longLivedTokenSupport>

<nativeLoggingEnabled>true</nativeLoggingEnabled>

<platform>linux</platform>

<saveTokens>true</saveTokens>

</AuthManLite>
<!--NeedCopy-->
```

Crear cadenas personalizadas user-agent en una solicitud de red

A partir de la versión 2109, la aplicación Citrix Workspace presenta una opción para agregar las cadenas User-Agent a la solicitud de red e identificar el origen de una solicitud de red. En función de esta solicitud de cadenas User-Agent, puede decidir cómo administrar su solicitud de red. Esta función le permite aceptar solicitudes de red solo desde dispositivos de confianza.

> **Nota:**
>
> - Esta función está disponible en implementaciones en la nube de la aplicación Citrix Workspace. También se admiten los paquetes x86, x64 y armhf.

Para personalizar las cadenas User-Agent, haga lo siguiente:

1. Busque el archivo de configuración $ICAROOT/config/AuthManConfig.xml.
2. Agregue un valor a esta entrada:

```
<UserAgentSuffix> </UserAgentSuffix>
```

Ejemplo que incluye la aplicación y la versión en el texto personalizado:

```
<UserAgentSuffix>App/AppVersion </UserAgentSuffix>
```

Si quiere agregar App y AppVersion, sepárelos con una barra diagonal (“/”).

- Si la solicitud de red procede de la aplicación Citrix Workspace basada en interfaz de usuario, aparece este User-Agent en las solicitudes de red:

  `CWAWEBVIEW/CWAVersion App/AppVersion`

- Si la solicitud de red procede de la aplicación Citrix Workspace basada en interfaz de usuario, aparece este User-Agent en las solicitudes de red:

  `CWA/CWAVersion App/AppVersion`

> **Notas:**
>
> - Si no agrega AppVersion al final de la cadena UserAgentSuffix, la versión de la aplicación Citrix Workspace se adjunta a las solicitudes de red.
> - Reinicie `AuthManagerDaemon` y `ServiceRecord` para que los cambios surtan efecto.

Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, podemos inhabilitar de manera dinámica una función afectada en la aplicación Citrix Workspace aunque dicha función ya se haya publicado. Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly.

No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva.
Puede habilitar el tráfico y la comunicación en LaunchDarkly de las siguientes formas:

Permitir el tráfico a las siguientes URL

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- firehose.launchdarkly.com
- mobile.launchdarkly.com
- app.launchdarkly.com

Incluir direcciones IP en una lista de permitidos

Si necesita incluir las direcciones IP en una lista de permitidos, para obtener una lista de todos los intervalos de direcciones IP actuales, consulte la lista de direcciones IP públicas de LaunchDarkly.

Puede usar esta lista para verificar que las configuraciones de su firewall se actualicen automáticamente de acuerdo con las actualizaciones de la infraestructura. Para obtener detalles sobre el estado actual de los cambios en la infraestructura, consulte la Página de estado de LaunchDarkly.

Requisitos del sistema para LaunchDarkly

Compruebe que las aplicaciones publicadas pueden comunicarse con estos servicios si el parámetro de túnel dividido está desactivado en Citrix ADC:

- Servicio de LaunchDarkly
- Servicio de escucha de APNs

Disposición para inhabilitar el servicio de LaunchDarkly

A partir de la versión 2205, puede inhabilitar el servicio de LaunchDarkly en la aplicación Citrix Workspace.

Para inhabilitar el servicio de LaunchDarkly, haga lo siguiente:

1. Vaya a la carpeta `<ICAROOT>/config/module.ini` y vaya a la sección LaunchDarkly.
2. Seleccione la entrada `EnableLaunchDarkly` e *inhabilítela*.

Continuidad del servicio

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) independientemente del estado de los servicios de la nube.

Para obtener información sobre los requisitos que permiten la continuidad del servicio en la aplicación Citrix Workspace, consulte Requisitos del sistema.

Para obtener más información, consulte la sección Continuidad del servicio de la documentación de Citrix Workspace.

Anclar el diseño de pantalla con varios monitores

A partir de la versión 2103, puede guardar la selección del diseño de pantalla con varios monitores. El diseño es la manera en que se muestra una sesión de escritorio. Anclarlo ayuda a reiniciar una sesión con el diseño seleccionado, lo que ofrece una mejor experiencia de usuario.

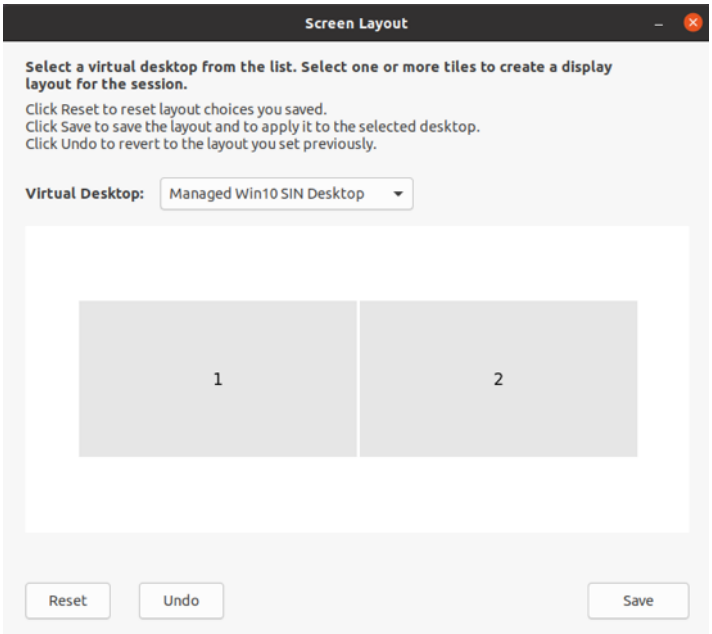
Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
      <key>ScreenPinEnabled</key>
      <value> true </value>
<!--NeedCopy-->
```

Solo después de agregar la clave anterior, podrá ver la opción **Diseño de pantalla** en el **indicador de aplicaciones**. Para obtener más información sobre el icono del indicador de aplicaciones, consulte Icono del indicador de aplicaciones.

Para seleccionar el diseño de la pantalla, haga clic en el icono del indicador de aplicaciones en la barra de tareas y seleccione **Diseño de pantalla**. Aparece el cuadro de diálogo **Diseño de pantalla**.

Si no, para abrir el cuadro de diálogo **Diseño de pantalla**, también puede presionar **Ctrl + M** cuando se encuentre en la ventana de autoservicio.



Seleccione un escritorio virtual en el menú desplegable. La selección del diseño se aplica solamente al escritorio que seleccione.

Seleccione uno o varios mosaicos para formar una selección rectangular del diseño. A continuación, la sesión se muestra según la selección del diseño.

Limitaciones:

- Al habilitar el anclaje de pantalla, se inhabilita la función para guardar el diseño durante las sesiones.
- Esta función solo se aplica a escritorios marcados como favoritos.

Categorías de las aplicaciones

Las categorías de aplicaciones permiten a los usuarios administrar colecciones de aplicaciones en la aplicación Citrix Workspace. Puede crear grupos de aplicaciones para lo siguiente:

- Aplicaciones compartidas entre diferentes grupos de entrega
- Aplicaciones utilizadas por un subconjunto de usuarios dentro de grupos de entrega.

Para obtener más información, consulte Crear un grupo de aplicaciones en la documentación de Citrix Virtual Apps and Desktops.

Protección de aplicaciones

> **RENUNCIA DE RESPONSABILIDADES**
>
> Las directivas de protección de aplicaciones funcionan filtrando el acceso a las funciones requeridas del sistema operativo subyacente. Se necesitan llamadas a API específicas para capturar pantallas o pulsaciones de teclas. Esta función significa que las directivas de protección de aplicaciones pueden proporcionar protección incluso contra herramientas de piratas informáticos personalizadas y diseñadas específicamente. Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de capturar pantallas y registrar pulsaciones de teclas. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

La protección de aplicaciones es una función adicional que proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops. La función restringe la posibilidad de que los clientes puedan verse amenazados por malware de registro de pulsaciones de teclas y malware de capturas de pantalla. La protección de aplicaciones evita la exfiltración de información confidencial, como credenciales de usuario e información confidencial que se muestran en la pantalla. La función evita que los usuarios y los atacantes hagan capturas de pantalla y usen registradores de pulsaciones de teclas para obtener y explotar información confidencial.

> **Notas:**
>
> - Esta función está disponible cuando la aplicación Citrix Workspace se instala mediante los paquetes tarball, Debian y Red Hat Package Manager (RPM). Además, x64 y armhf son las únicas arquitecturas compatibles.
> - Esta función está disponible en implementaciones locales de Citrix Virtual Apps and Desktops. También en implementaciones que utilizan Citrix Virtual Apps and Desktops Service con StoreFront.

La protección de aplicaciones requiere instalar una licencia adicional en el servidor de licencias. También debe haber presente una licencia de Citrix Virtual Desktops. Para obtener información sobre las licencias, consulte la sección **Configuración** de Citrix Virtual Apps and Desktops.

A partir de la versión 2108, la función de protección de aplicaciones es completamente funcional. La función de protección de aplicaciones está disponible en sesiones de escritorios y aplicaciones, y está habilitada de forma predeterminada. Sin embargo, debe configurar la función de protección de aplicaciones en el archivo `AuthManConfig.xml` para habilitarla en las interfaces del administrador de autenticación y de Self-Service Plug-in.

A partir de esta versión, puede iniciar recursos protegidos desde la aplicación Citrix Workspace mientras se ejecuta Mozilla Firefox.

A partir de la versión 2012, la función de protección de aplicaciones es una función experimental.

Requisito previo:

La protección de aplicaciones funciona mejor con estos sistemas operativos y GNOME Display Manager:

- Ubuntu 18.04 y Ubuntu 20.04 de 64 bits
- Debian 9 y Debian 10 de 64 bits
- CentOS 7 de 64 bits
- RHEL 7 de 64 bits
- Sistema operativo Raspberry Pi (Buster) con armhf de 32 bits (basado en Debian 10)

> **Nota:**
>
> Si utiliza una versión de la aplicación Citrix Workspace anterior a 2204, la función de protección de aplicaciones no es compatible con los sistemas operativos que utilizan `glibc` 2.34 o una versión posterior.
>
> Si instala la aplicación Citrix Workspace con la función de protección de aplicaciones habilitada en un SO que utiliza `glibc` 2.34 o una versión posterior, es posible que, al reiniciar el sistema, el SO no arranque. Para recuperarse de un error de arranque del SO, realice una de estas acciones:
>
> - Instale de nuevo el sistema operativo. Sin embargo, no admitimos la función de protección de aplicaciones en el sistema operativo que usa `glibc` 2.34 o una versión posterior.
> - Vaya al modo de recuperación del sistema operativo y desinstale la aplicación Citrix Workspace desde el terminal.
> - Arranque el sistema desde el SO en directo y quite el archivo `rm -rf /etc/ld.so.preload` del SO existente.

Instalación del componente de protección de aplicaciones:

Al instalar la aplicación Citrix Workspace con el paquete tarball, aparece el mensaje siguiente.

"¿Quiere instalar el componente de protección de aplicaciones? Advertencia: No puede inhabilitar esta función. Para inhabilitarla, debe desinstalar la aplicación Citrix Workspace. Para obtener más información, contacte con el administrador de sistemas. [default $INSTALLER_N]:"

Presione **Y** para instalar el componente de protección de aplicaciones.

De forma predeterminada, el componente de protección de aplicaciones no está instalado.

Reinicie la máquina para que los cambios surtan efecto. La protección de aplicaciones funciona como es debido solamente tras reiniciar la máquina.

Instalación del componente de protección de aplicaciones en paquetes RPM:

A partir de la versión 2104, la protección de aplicaciones se ofrece en la versión RPM de la aplicación Citrix Workspace.

Para instalar la protección de aplicaciones, haga esto:

1. Al instalar la aplicación Citrix Workspace.
2. Instale el paquete `ctxappprotection<version>.rpm` de protección de aplicaciones desde el instalador de la aplicación Citrix Workspace.
3. Reinicie el sistema para que los cambios surtan efecto.

Instalación del componente de protección de aplicaciones en paquetes Debian:

A partir de la versión 2101, la protección de aplicaciones se ofrece en la versión Debian de la aplicación Citrix Workspace.

Para una instalación silenciosa del componente de protección de aplicaciones, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
    install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

A partir de la versión 2106, la aplicación Citrix Workspace presenta una opción para configurar las funciones de protección contra el registro de tecleo y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-Service Plug-in.

Configuración de la protección de aplicaciones para el administrador de autenticación:

Vaya a `$ICAROOT/config/AuthManConfig.xml` y modifique el archivo de esta manera:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
    authmananti -A 1
     <key>AuthManAntiScreenCaptureEnabled</key>
     <value>true</value>
     <key>AuthManAntiKeyLoggingEnabled</key>
     <value>true </value>
```



```
6
7 <!--NeedCopy-->
```

Configuración de la protección de aplicaciones para la interfaz del Self-Service Plug-in:

Vaya a `$ICAROOT/config/AuthManConfig.xml` y modifique el archivo de esta manera:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
     protection -A 4
2 <!-- Selfservice App Protection configuration -->
3     <Selfservice>
4       <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
5       <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
6     </Selfservice>
7
8 <!--NeedCopy-->
```

Problemas conocidos:

- Al minimizar una pantalla protegida, la protección de aplicaciones continúa ejecutándose en segundo plano.

Limitación:

- A veces, no se pueden iniciar recursos protegidos cuando se está ejecutando una aplicación instalada desde Snap Store. Como solución temporal, identifique la aplicación que causa el problema en el archivo de registros de la aplicación Citrix Workspace. Luego, cierre la aplicación.
- Al intentar hacer una captura de pantalla de una ventana protegida, toda la pantalla, incluidas las aplicaciones no protegidas en segundo plano, se atenuaba.

Indicador de estado de la batería

Ahora el estado de la batería del dispositivo se muestra en el área de notificaciones de las sesiones de Citrix Desktop.

> **Nota:**
>
> A partir de la versión 2111, también se muestra el indicador de estado de la batería de los VDA de servidor.

El indicador de estado de la batería está habilitado de forma predeterminada.

Para inhabilitar el indicador de estado de la batería:

1. Vaya a la carpeta `<ICAROOT>/config/module.ini`.
2. Vaya a la sección `ICA 3.0`.
3. Configure esta opción: `MobileReceiver= Off`.

Programa para la mejora de la experiencia del usuario (CEIP)

Datos recopilados	Descripción	Para qué se utiliza
Datos de uso y configuración	El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información de uso y configuración de la aplicación Citrix Workspace para Linux y envía esos datos automáticamente a Google Analytics.	Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de la aplicación Citrix Workspace.

Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato con Citrix. Además, lo protege como se especifica en Citrix Services Security Exhibit disponible en el Centro de confianza de Citrix.

Citrix también utiliza Google Analytics para recopilar determinados datos de la aplicación Citrix Workspace como parte del programa CEIP. Puede revisar cómo gestiona Google los datos recopilados para Google Analytics.

Cancele el envío de datos de CEIP a Citrix y Google Analytics. Para esta actividad, hay una excepción para los datos recopilados para Google Analytics, que se indica con * en la segunda tabla de la sección siguiente. Haga lo siguiente para cancelar el envío de datos de CEIP a Citrix y Google Analytics:

1. Vaya a la carpeta <ICAROOT>/config/module.ini y vaya a la sección CEIP.
2. Seleccione la entrada EnableCeip y establézcala en Disable.

> **Nota:**
>
> Después de establecer la clave EnableCeip en Disable, puede inhabilitar el envío de los dos últimos elementos de datos CEIP recopilados por Google Analytics. Estos elementos de datos son la versión del sistema operativo y la versión de la aplicación Workspace. Para esta acción, vaya a esta sección y defina el valor como se sugiere:

Ubicación: <ICAROOT>/config/module.ini

Sección: GoogleAnalytics

Entrada: DisableHeartBeat

Valor: True

> **Nota:**
>
> No se recopilan datos de los usuarios de la Unión Europea (UE) ni del Espacio Económico Europeo (EEE) ni de Suiza ni del Reino Unido.

Elementos concretos de datos CEIP recopilados por Google Analytics:

Versión del sistema operativo*	Versión de la aplicación Workspace*	Nombre de la aplicación	Idioma de la aplicación Workspace
Método de inicio de sesiones	Versión del compilador	Plataforma de hardware	Configuración del almacén
Estado de inicio de las sesiones de Citrix Virtual Apps and Desktops	Configuración de la autenticación	Protocolo de conexión	Uso de la función Redirección de contenido del explorador
Detalles de la concesión de conexiones	Configuración de protección de aplicaciones		

Icono del indicador de aplicaciones

El indicador de aplicaciones se inicia cuando se abre la aplicación Citrix Workspace. Es un icono que está presente en el área de notificaciones. Con la introducción del indicador de aplicaciones, mejora el rendimiento del inicio de sesión de la aplicación Citrix Workspace para Linux.

Puede constatar la mejora del rendimiento en estos casos:

- Primer inicio de la aplicación Citrix Workspace
- Cerrar la aplicación y volver a iniciarla
- Salir de la aplicación y volver a iniciarla

> **Nota:**
>
> El paquete `libappindicator` es necesario para que el indicador de aplicaciones aparezca. Instale desde la web el paquete `libappindicator` adecuado para su distribución de Linux.

Proxy de ICA a X

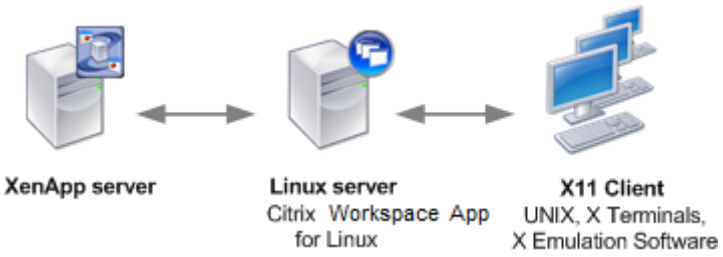
Puede utilizar una estación de trabajo que ejecuta la aplicación Citrix Workspace como servidor y redirigir la salida a otro dispositivo compatible con X11. Se recomienda realizar esta tarea para en-

tregar aplicaciones de Microsoft Windows a terminales X o estaciones de trabajo UNIX en las que la aplicación Citrix Workspace no está disponible.

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

Cuando se ejecuta la aplicación Citrix Workspace, se la 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. Puede ejecutar copias adicionales de la aplicación Citrix Workspace simultáneamente en un sistema. En este caso, cada aplicación Citrix Workspace envía sus datos a un dispositivo diferente.

En este gráfico se muestra un sistema con la aplicación Citrix Workspace 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 la aplicación Citrix Workspace en el servidor Linux que normalmente proporciona las aplicaciones X para los terminales X.
- Si quiere implementar estaciones de trabajo UNIX en las que la aplicación Citrix Workspace no está disponible, necesita tener un servidor adicional que actúe como proxy. Este servidor puede ser un PC con Linux.

El dispositivo final recibe las aplicaciones a través de X11 gracias al protocolo ICA. De forma predeterminada, puede utilizar la asignación de unidades solamente para acceder a las unidades en el proxy. Este parámetro 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 como proxy en la estación de trabajo y, a continuación, apuntar 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 de USB
- Redirección de tarjetas inteligentes
- Redirección de puertos COM
- No se transfiere audio al dispositivo X11, aunque el servidor que actúa como proxy admita audio.
- Las impresoras de los clientes no se transfieren al dispositivo X11. Acceda manualmente a la impresora de UNIX desde el servidor a través de la impresión LPD, o bien utilice una impresora de red.
- No se admite la redirección de entradas multimedia porque requiere una cámara web en la máquina que ejecuta la aplicación Citrix Workspace, donde el servidor actúa como proxy. Sin embargo, la redirección de salida multimedia se permite cuando `GStreamer` está instalado en el servidor que actúa como proxy (no comprobado).

Para iniciar la aplicación Citrix Workspace 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 hace de proxy, no es necesario establecer la variable de entorno **DISPLAY**.

3. En un símbolo del sistema del dispositivo local, escriba xhost <nombre del servidor proxy>
4. Compruebe si la aplicación Citrix Workspace está instalada en el directorio de instalación predeterminado. Si no está instalada, verifique que la variable de entorno ICAROOT esté configurada para que apunte al directorio de instalación real.
5. Ubique el directorio donde está instalada la aplicación Citrix Workspace. En la línea de comandos, escriba `selfservice &`.

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 otorguen recursos de Citrix de forma más eficiente para ofrecer un mejor rendimiento a los usuarios. Los siguientes tipos de URL pueden redirigirse:

- HTTP
- HTTPS
- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (versiones anteriores de Real Player)

La URL se abre mediante la aplicación del servidor cuando:

- La aplicación Citrix Workspace no tiene una aplicación adecuada
- La aplicación Citrix Workspace no puede acceder directamente al contenido

La redirección de contenido servidor-cliente se configura en el servidor. Esta funcionalidad está habilitada de forma predeterminada en la aplicación Citrix Workspace si la ruta incluye lo siguiente:

- RealPlayer
- Firefox, Mozilla o Netscape.

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

   La ruta es el directorio donde se encuentra el ejecutable del explorador. El comando es el nombre del ejecutable utilizado para gestionar las URL de exploradores redirigidas, junto a la URL enviada por el servidor. Por ejemplo:

   `$ICAROOT/nslaunch` Netscape, Firefox, Mozilla

   Este parámetro especifica lo siguiente:

   - Se ejecutará la utilidad `nslaunch` para insertar la URL en la ventana de un 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

   La ruta es el directorio donde se encuentra el ejecutable de RealPlayer. El comando es el nombre del ejecutable utilizado para gestionar las URL multimedia redirigidas, junto a la URL enviada por el servidor.
4. Guarde el archivo y ciérrelo.

> **Nota:**
>
> En el caso de los dos parámetros de ruta, 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 nombres de directorio adicionales como una lista separada por dos puntos. Si no se especifican estos parámetros, se utilizará la ruta $PATH actual del usuario.

Para borrar la redirección de contenido servidor-cliente desde Citrix Workspace:

1. Abra el archivo de configuración `module.ini`.
2. Cambie el ajuste `CREnabled` a `Off`.
3. Guarde el archivo y ciérrelo.

Conexión

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 latencia SpeedScreen**: La reducción de latencia SpeedScreen mejora el rendimiento en conexiones con latencia elevada. Para esta mejora, se proporciona una respuesta instantánea al usuario por los datos introducidos o a las acciones con el mouse. Use el Administrador de reducción de latencia SpeedScreen para habilitar esta función en el servidor. De forma predeterminada, esta función está inhabilitada para el teclado en la aplicación Citrix Workspace. Esta función solo está habilitada para el mouse en conexiones de alta latencia. Consulte la guía de referencia de OEM de la aplicación Citrix Workspace para Linux (en inglés).
- **Habilite la compresión de datos**: la compresión de datos reduce la cantidad de datos transferidos a través de la conexión. Esta configuración 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 audio y Compresión de imágenes** para habilitar esta función.
- **Reduzca el tamaño de la ventana**: cambie la dimensión de la ventana al tamaño utilizable más pequeño posible. En la comunidad, defina las opciones de sesión.
- **Reduzca la cantidad de colores**: reduzca la cantidad de colores a 256. En el sitio de Citrix Virtual Apps and Desktops o Citrix DaaS, configure las opciones de la sesión.
- **Reduzca la calidad de audio**: si la asignación de audio está habilitada, reduzca la calidad de audio al parámetro más bajo mediante la configuración de directiva de Citrix Calidad de audio.

Para obtener información sobre la solución de problemas, consulte Conexiones en la sección Solución de problemas.

Fuente

Suavizado de fuentes ClearType

El suavizado de fuentes ClearType mejora la calidad de las fuentes en pantalla más allá de la calidad disponible que permite ofrecer el suavizado de fuentes estándar o "anti-aliasing". El suavizado de fuentes ClearType se conoce también como presentación de fuentes de subpíxel. Puede activar o desactivar esta función.

También puede especificar el tipo de suavizado del siguiente modo:

1. Vaya a la sección [WFClient] del archivo de configuración correspondiente.
2. Modifique el siguiente parámetro:

   FontSmoothingType = número

   Donde el número puede ser uno de estos valores:

Valor	Comportamiento
0	Se usa la preferencia local existente en el dispositivo. El parámetro **FontSmoothingTypePref** define este valor.
1	Sin suavizado
2	Suavizado estándar
3	Suavizado ClearType (subpíxel horizontal)

Tanto el suavizado estándar como el suavizado ClearType pueden aumentar los requisitos de ancho de banda de la aplicación Citrix Workspace.

> **Importante:**
>
> El servidor puede configurar `FontSmoothingType` a través del archivo `ICA`. Este valor tiene prioridad sobre el valor que esté definido en [WFClient].

Si el servidor establece el valor en 0, este parámetro de [WFClient] determina la preferencia local:
FontSmoothingTypePref = número

Donde el número puede ser uno de estos valores:

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

Carpeta

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. Como resultado, estas carpetas permanecen fijas en diferentes tipos de servidores y configuraciones de comunidades de servidores. Esto es particularmente importante si, por ejemplo, un usuario móvil inicia 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:

Para habilitar la redirección de carpetas especiales, cree una entrada en el archivo module.ini y especifique las ubicaciones de las carpetas de la siguiente manera:

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

   [ClientDrive]

   SFRAllowed = True

   DocumentsFolder = documentos

   DesktopFolder = escritorio

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

   DesktopFolder = $HOME/.ICAClient/desktop

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

Asignación de unidades de cliente

La asignación de unidades del cliente permite redirigir letras de unidades del servidor de Citrix Virtual Apps and Desktops y Citrix DaaS a directorios existentes en el dispositivo del usuario local. Por ejemplo, la unidad H: de una sesión de usuario de Citrix se puede asignar a un directorio en el dispositivo del usuario local que ejecuta la aplicación Workspace.

La asignación de unidades de cliente puede hacer que cualquier directorio se monte en el dispositivo de usuario local. El dispositivo de usuario local incluye un CD-ROM, un DVD o un dispositivo de memoria USB, que están disponibles para el usuario durante la sesión. Además, el usuario local tiene permiso para acceder al dispositivo de usuario local. Cuando un servidor está configurado para permitir la asignación de unidades de cliente:

- Los usuarios pueden acceder a sus archivos almacenados localmente.
- Usar los archivos durante su sesión.
- Guardarlos de nuevo en una unidad local o en una unidad del servidor.

La aplicación Citrix Workspace admite la asignación de dispositivos del cliente para conexiones a servidores Citrix Virtual Apps and Desktops y Citrix DaaS. Esta función permite que una aplicación remota que se ejecuta en el servidor acceda a dispositivos conectados al dispositivo de usuario local. El usuario puede usar las aplicaciones y los recursos del sistema como si se ejecutaran localmente. Antes de utilizar estas funciones, verifique que el servidor admita la asignación de dispositivos del cliente.

> **Nota:**
>
> El modelo de seguridad de Linux con Seguridad Mejorada (SELinux - Security-Enhanced Linux) puede afectar al funcionamiento de la asignación de unidades del cliente y la redirección USB. Este modelo se aplica tanto a Citrix Virtual Apps and Desktops como a Citrix DaaS. Si se requieren estas funciones, inhabilite SELinux antes de configurarlas en el servidor.

Existen dos tipos de asignación de unidades disponibles:

- Asignación estática de unidades del cliente: Permite que los administradores asignen cualquier parte del sistema de archivos del dispositivo del usuario a una unidad especificada en el servidor cuando se inicia la sesión. Por ejemplo, se puede usar para asignar todos o una parte del

directorio principal o /tmp de un usuario. Luego, asigne los puntos de montaje de los dispositivos de almacenamiento masivo, como CD-ROM, DVD o dispositivos de memoria USB.

- Asignación dinámica de unidades del cliente: Supervisa los directorios en los que, por lo general, los dispositivos de almacenamiento masivo 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 la aplicación Citrix Workspace se conecta a Citrix Virtual Apps and Desktops o Citrix DaaS, 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 Citrix Virtual Apps and Desktops.

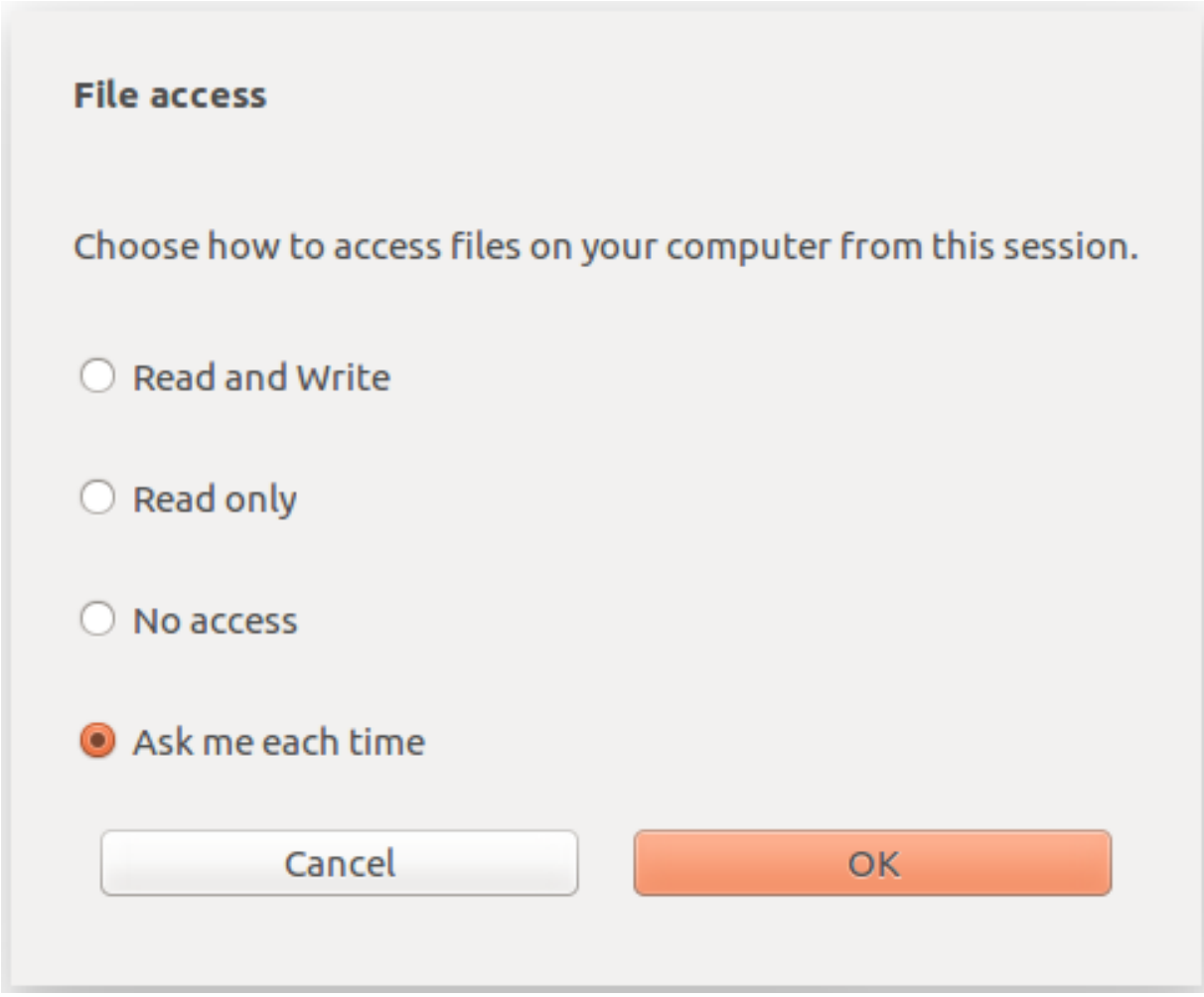
Los usuarios pueden asignar unidades mediante el cuadro de diálogo **Preferencias**.

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

Anteriormente, la configuración del acceso a archivos a través de CDM se aplicaba a todos los almacenes configurados.

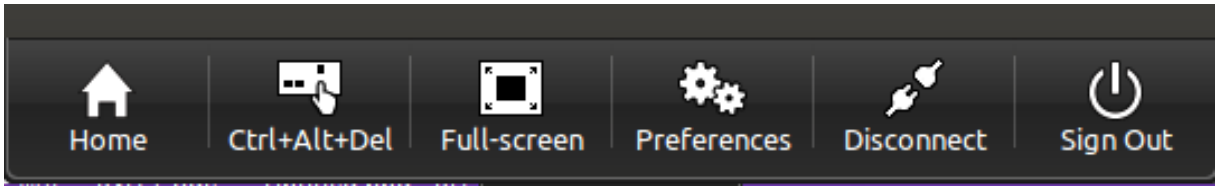
A partir de la versión 2012, la aplicación Citrix Workspace le permite configurar el acceso a archivos CDM por almacén.

> **Nota:**
>
> La configuración de acceso a archivos no es persistente en todas las sesiones cuando se utiliza Workspace para Web. De forma predeterminada, se utiliza la opción **Preguntarme cada vez**.

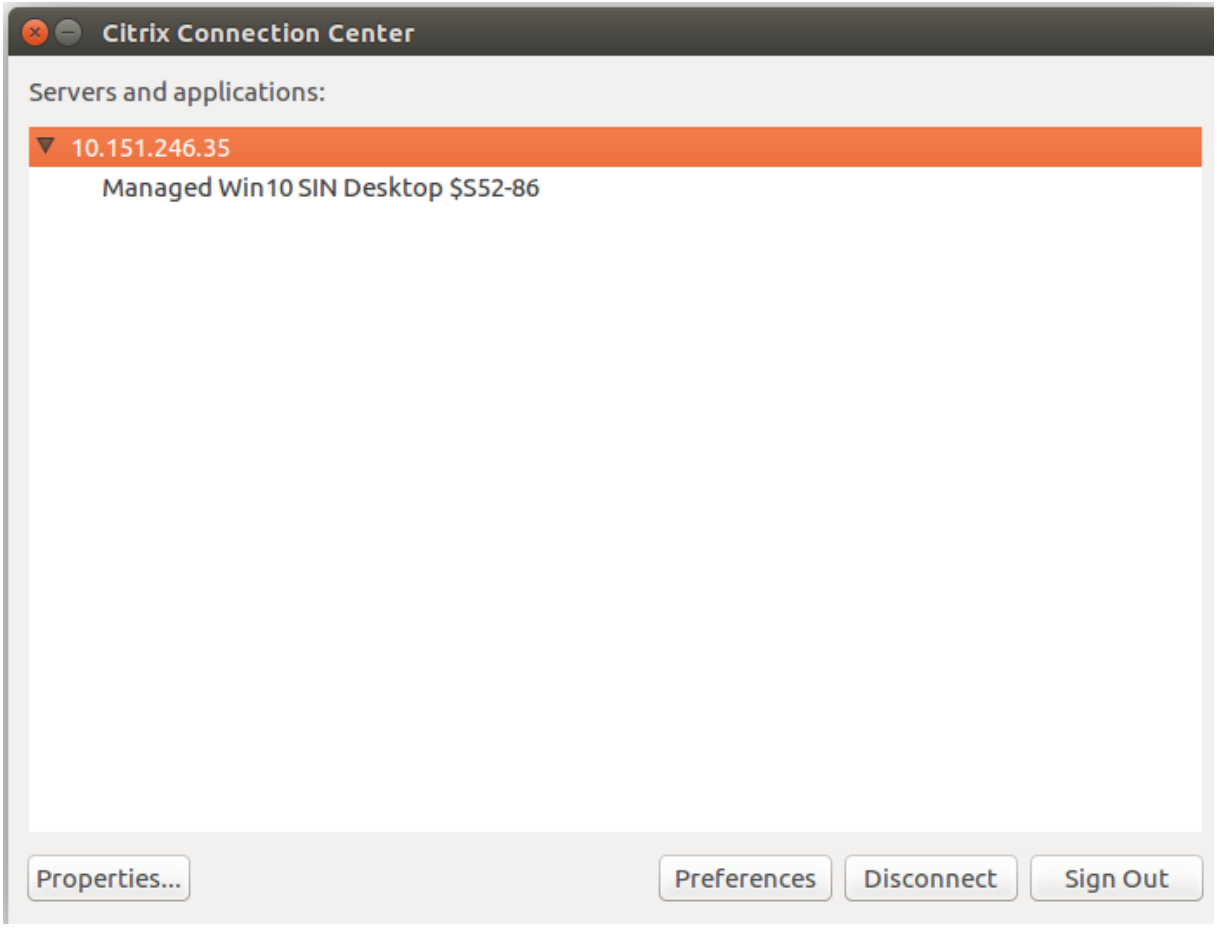


Puede utilizar el archivo `wfclient.ini` para configurar los atributos de la ruta asignada y el nombre de archivo. Utilice la GUI para establecer un nivel de acceso a archivos como se muestra en la captura de pantalla anterior.

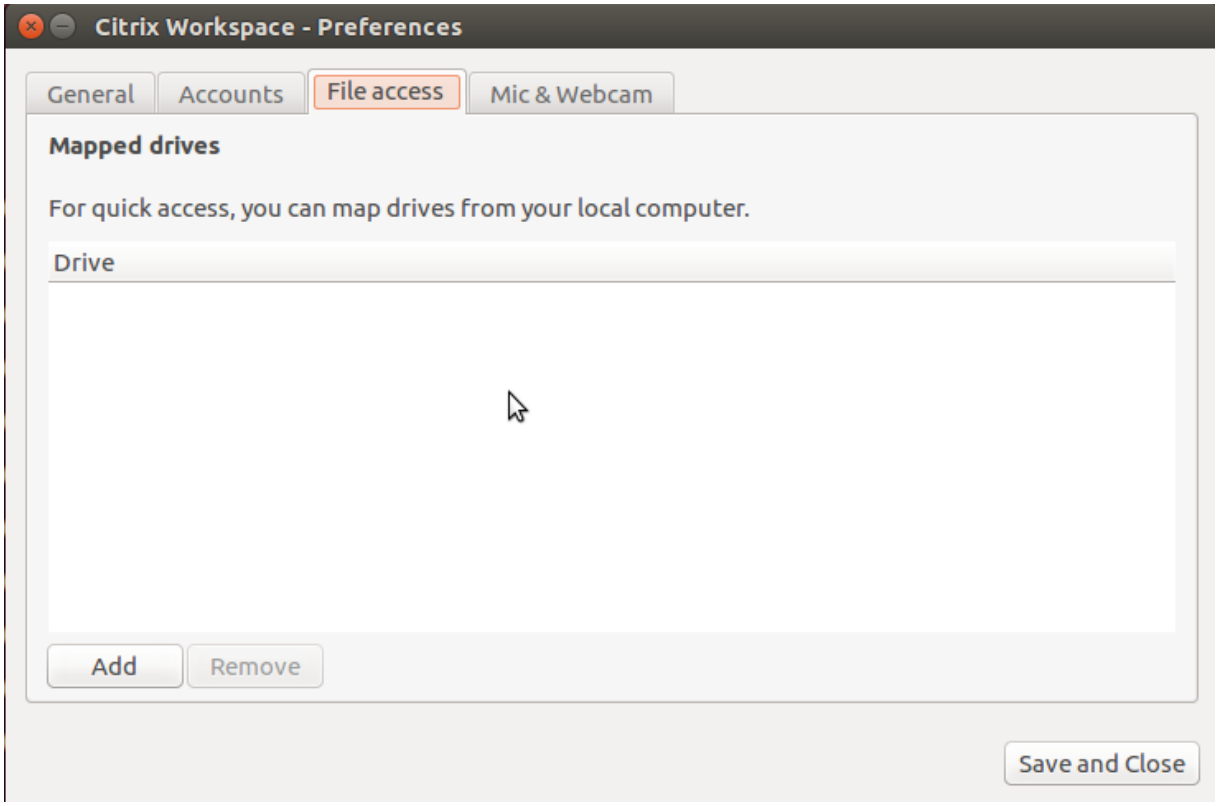
En una sesión de escritorio, para establecer un nivel de acceso a archivos, vaya a **Preferencias** > cuadro de diálogo **Acceso a archivos** desde Desktop Viewer.



En una sesión de aplicación, para establecer un nivel de acceso a archivos, abra el cuadro de diálogo **Acceso a archivos** desde la **Central de conexiones de Citrix**.



El cuadro de diálogo **Acceso a archivos** incluye el nombre de la carpeta asignada y su ruta.



El indicador del nivel de acceso ya no se admite en el archivo `wfclient.ini`.

Asignar impresoras del cliente

La aplicación Citrix Workspace admite 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, Citrix Virtual Apps and Desktops y Citrix DaaS permiten 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 perfectos 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. Sin embargo, esa configuración predeterminada puede crear inicios de sesión lentos en algunos entornos. En esa situación, quizá le interese 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, inhabilite la **directiva de ICA Conectar automáticamente puertos COM del cliente**.

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 la aplicación Workspace. En este caso, "todos los usuarios" se refiere a los primeros que usan el programa self-service después del cambio.

2. En la sección [WFClient] del archivo, escriba:

   ClientPrinterList=impresora1:impresora2:impresora3

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

3. Guarde el archivo y ciérrelo.

Asignación de una impresora local

La aplicación Citrix Workspace 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. Puede asignar manualmente impresoras del cliente en Citrix Virtual Apps and Desktops o Citrix DaaS 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 la aplicación Citrix Workspace, establezca una conexión de servidor e inicie sesión en un equipo que ejecute Citrix Virtual Apps and Desktops o Citrix DaaS.
2. En el menú Inicio, seleccione **Configuración > Impresoras**.
3. En el menú Archivo, seleccione **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. Por lo general, este valor es un nombre de impresora estándar, similar a los valores creados por Servicios de Escritorio remoto nativos, como "HP LaserJet 4 de nombre_cliente en sesión 3".

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

Audio

A partir de la versión 2112, se cambia el nombre del atributo `VdcamVersion4Support` del archivo `module.ini` a `AudioRedirectionV4`. A partir de la versión 2212, el valor predeterminado de `AudioRedirectionV4` se establece en **True**. Como resultado de ello:

- La biblioteca PulseAudio se utiliza para acceder a los dispositivos de audio y se admiten dispositivos extras.
- Más de una aplicación puede usar los dispositivos de audio en un momento dado.
- La aplicación Citrix Workspace muestra todos los dispositivos de audio locales que están disponibles en una sesión. En lugar de Citrix HDX Audio, los dispositivos de audio aparecen con sus respectivos nombres de dispositivo. Puede cambiar a cualquiera de los dispositivos disponibles de forma dinámica en una sesión.
- Las sesiones se actualizan dinámicamente al conectar o quitar dispositivos de audio.

Si establece el valor de `AudioRedirectionV4` en **False**:

- La biblioteca ALSA se utiliza para acceder a los dispositivos de audio y solo se admite un dispositivo.
- Aparece en la sesión el dispositivo de audio predeterminado con el nombre Citrix HDX Audio.
- Solo una aplicación puede usar el dispositivo Citrix HDX Audio.

Para establecer el valor de `AudioRedirectionV4` en **False**, haga lo siguiente:

1. Vaya a la carpeta <`ICAROOT`>/`config` y abra el archivo `module.ini`.
2. Vaya a la sección [ClientAudio] y agregue esta entrada:

   AudioRedirectionV4=False

3. Vuelva a iniciar la sesión para que los cambios surtan efecto.

Compatibilidad con la grabación de audio

A partir de la versión 2212, la funcionalidad de grabación de audio está habilitada de forma predeterminada. Los dispositivos para grabar audio aparecen cuando se inicia una sesión.

Para inhabilitar esta función, establezca el valor de `AllowAudioInput` en *False* en el archivo `wfclient.ini`.

> **Notas:**
>
> - La funcionalidad de redirección de audio mejorada está disponible de manera generalizada a partir de la versión 2212.
> - La opción **Micrófono y cámara web** del cuadro de diálogo **Preferencias** está inhabilitada de forma predeterminada. Para obtener información sobre cómo habilitar el micrófono y la cámara web, consulte Preferencias.
> - La aplicación Citrix Workspace versión 2010 aborda problemas para mejorar la funcionalidad ICA multisecuencia.

Limitaciones conocidas:

De forma predeterminada, el valor de `AudioRedirectionV4` se establece en **True**. Existe la siguiente limitación conocida cuando el valor de `AudioRedirectionV4` se establece en **True**:

- Si inicia una sesión desde la interfaz de línea de comandos con privilegios de “root”, es posible que el servidor de PulseAudio rechace la conexión al intentar conectarse a él. En este caso, los dispositivos de audio podrían empezar a utilizar la biblioteca ALSA, que solo admite dispositivos individuales.

Si establece el valor de `AudioRedirectionV4` en **False**, existen las siguientes limitaciones conocidas:

- En un VDA con Windows Server 2016, no se puede cambiar la selección del dispositivo de audio en una sesión. La selección se establece solo en la entrada y salida de audio predeterminada. Esta limitación se resuelve al establecer el valor `AudioRedirectionV4` en **True**.
- La redirección de dispositivos de audio no es compatible con dispositivos de audio Bluetooth. Esta limitación se resuelve al establecer el valor `AudioRedirectionV4` en **True**.
- Puede cambiar el dispositivo de audio predeterminado solo en los sistemas operativos Windows 10, Windows 7 y Windows 8. En los sistemas operativos de Windows Server, como Windows Server 2012, 2016 y 2019, no puede cambiar el dispositivo de audio predeterminado. Este problema se debe a una limitación de las sesiones de escritorio remoto de Microsoft.
- La redirección de dispositivos de audio no es compatible con dispositivos de audio HDMI. Esta limitación se resuelve al establecer el valor `AudioRedirectionV4` en **True**. Sin embargo, es posible que la aplicación Citrix Workspace muestre dispositivos de audio HDMI que no están conectados en una sesión.

Cuando el valor de `AudioRedirectionV4` es **False**, el dispositivo de audio predeterminado suele ser el dispositivo ALSA predeterminado que se configuró 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 quiera 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 los parámetros predeterminados.
2. Agregue esta opción y cree la sección si es necesario:

```
[ClientAudio]

AudioDevice = \<device\>
<!--NeedCopy-->
```

En esta sección, la información de dispositivo está ubicada en el archivo de configuración 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.

Mejora en la calidad del audio

Antes, el valor máximo del búfer de salida para reproducir audio sin problemas era de 200 ms en la aplicación Citrix Workspace. Debido a este conjunto de valores, se agregó una latencia de 200 ms en los casos de reproducción. Este valor máximo de búfer de salida también tenía un impacto en las aplicaciones de audio interactivo.

Con esta mejora, el valor máximo de búfer de salida se reduce a 50 ms en la aplicación Citrix Workspace. Como resultado, mejora la experiencia del usuario en la aplicación de audio interactivo. Además, el tiempo de ida y vuelta (RTT) se reduce en 150 ms.

A partir de la versión 2207, puede seleccionar el umbral de reproducción y el prebúfer de audio por pulsos adecuados para mejorar la calidad del audio. Para esta mejora, se agregan estos parámetros en la sección [ClientAudio] del archivo `module.ini`:

- `PlaybackDelayThreshV4`: Especificar el nivel inicial de búfer de salida en milisegundos. La aplicación Citrix Workspace intenta mantener este nivel de almacenamiento en búfer durante toda la sesión. El valor predeterminado de `PlaybackDelayThreshV4` es de 50 ms. Este parámetro solo es válido cuando `AudioRedirectionV4` se establece en **True**.
- `AudioTempLatencyBoostV4`: Cuando el procesamiento de audio sufre un pico repentino o no tiene un nivel suficiente para una red inestable, este valor aumenta el valor del búfer de salida. Este aumento en el valor del búfer de salida proporciona una calidad de audio fluida. Sin embargo, es posible que el audio se retrase un poco. El valor predeterminado de `AudioTempLatencyBoostV4` se establece en 100 ms. Este parámetro solo es válido cuando `AudioRedirectionV4` se establece en **True** y `AudioLatencyControlEnabled` en **True**. De forma predeterminada, el valor de `AudioLatencyControlEnabled` se establece en True.

De forma predeterminada, el valor de `AudioRedirectionV4` se establece en True. Para inhabilitar esta función, haga lo siguiente:

1. Vaya a la carpeta <`ICAROOT`>/`config` y abra el archivo module.ini.
2. Vaya a la sección [ClientAudio] y agregue esta entrada:

   AudioRedirectionV4=False
3. Vuelva a iniciar la sesión para que los cambios surtan efecto.

Función de eliminación de eco de audio mejorada

> **Nota:**
>
> A partir de la versión 2303, esta función está disponible de forma general para la aplicación Citrix Workspace.

A partir de esta versión, la aplicación Citrix Workspace admite la eliminación de eco. Esta función está diseñada para casos de usuario con audio en tiempo real y mejora la experiencia del usuario. La función de eliminación de eco opera con audio de calidad baja, calidad media y adaptable. Para obtener un rendimiento óptimo, Citrix recomienda usar audio adaptable.

De forma predeterminada, la función de eliminación de eco está inhabilitada. Durante los casos de usuario con audio en tiempo real, se recomienda activar la eliminación de eco si se utiliza el altavoz en lugar de los auriculares.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya a la carpeta <ICAROOT>/config y abra el archivo module.ini.
2. Vaya a la sección [ClientAudio] y actualice el valor del parámetro EnableEchoCancellation de la siguiente manera:

   EnableEchoCancellation =TRUE

Limitación:

Por diseño, la función de eliminación de eco está inhabilitada para proporcionar audio de alta calidad.

Adición de un mecanismo de búfer de vibración del lado del cliente [Technical Preview]

A partir de la versión 2212, la aplicación Citrix Workspace garantiza un audio fluido incluso cuando la latencia de la red fluctúa. De forma predeterminada, esta función está inhabilitada.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya al archivo de configuración /opt/Citrix/ICAClient/config/module.ini y modifíquelo.
2. Inhabilite el control de latencia de audio de la siguiente manera:

   ```
   `AudioLatencyControlEnabled = FALSE`
   ```

3. Habilite el búfer de vibración de la siguiente manera:

   ```
   `JitterBufferEnabled = TRUE`
   ```

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de

> compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Asignación de audio del cliente

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

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

Configure la asignación de audio del cliente a través de directivas. Para obtener más información, consulte la documentación de Citrix Virtual Apps and Desktops.

Audio adaptable

A partir de la versión 2109, la aplicación Citrix Workspace admite el audio adaptable. Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en los VDA. El audio adaptable optimiza los parámetros del entorno y sustituye los formatos de compresión de audio obsoletos para proporcionar una excelente experiencia de usuario. El audio adaptable está habilitado de forma predeterminada. Para obtener más información, consulte Audio adaptable.

A partir de la versión 2112, el audio adaptable funciona cuando se utiliza la entrega de audio del protocolo UDP (User Datagram Protocol).

Limitación conocida:

- El audio adaptable requiere procesadores CPU compatibles con Streaming SIMD Extensions (SSE) 4.x. La aplicación Citrix Workspace puede cerrarse cuando se usa audio adaptable con un procesador CPU no compatible con SSE 4.x.

Habilitar el audio UDP

El audio UDP puede mejorar la calidad de las llamadas telefónicas que se realizan a través de Internet. Utiliza UDP en lugar de TCP.

A partir de la versión 2112, el audio adaptable funciona cuando se utiliza la entrega de audio UDP. Además, a partir de esta versión, la aplicación Citrix Workspace admite el protocolo de seguridad Datagram Transport Layer Security (DTLS) para audio UDP. Como resultado, puede acceder al audio UDP a través de Citrix Gateway. De forma predeterminada, esta función está inhabilitada.

A partir de la versión 2202, la mejora para admitir audio UDP a través de Citrix Gateway está disponible de forma general para la aplicación Citrix Workspace.

Para habilitar el audio UDP:

1. Configure las siguientes opciones en la sección [ClientAudio] de module.ini:
   - Establezca `EnableUDPAudio` en **True**. De forma predeterminada, este valor está establecido en **False**, lo que inhabilita el audio UDP.
   - Especifique los números de puerto mínimo y máximo para el tráfico de audio UDP mediante `UDPAudioPortLow` y `UDPAudioPortHigh` respectivamente. De forma predeterminada, se utilizan los puertos que van de 16500 a 16509.
2. De forma predeterminada, el audio adaptable está habilitado en el VDA y admite audio UDP. Si inhabilitó el audio adaptable, configure los parámetros de audio del cliente y del servidor de esta manera para permitir el audio UDP. Como consecuencia, el audio resultante es de una calidad media (es decir, ni alta ni baja).

		Calidad de audio en el cliente	Calidad de audio en el cliente	Calidad de audio en el cliente
		Alto	Medio	Bajo
Calidad de audio en el servidor	Alto	Alto	Medio	Bajo
Calidad de audio en el servidor	Medio	Medio	Medio	Bajo
Calidad de audio en el servidor	Bajo	Bajo	Bajo	Bajo

Para habilitar el audio UDP mediante Citrix Gateway:

1. Vaya a la carpeta <`ICAROOT`>/`config` y abra el archivo `module.ini`.
2. Vaya a la sección [WFClient] y configure esta entrada:

   EnableUDPThroughGateway=True

3. Vaya a la sección [ClientAudio] y configure esta entrada:

   EnableUDPAudio=True

> **Nota:**
>
> Si usa la configuración de default.ica de StoreFront, el valor de `EnableUDPThroughGateway` establecido en la sección [Application] tiene prioridad sobre el valor establecido en el archivo `module.ini`. Sin embargo, puede establecer el valor `EnableUDPAudio` de la sección [ClientAudio] solo con el archivo `module.ini`. Además, no tiene prioridad sobre el valor establecido en la configuración de default.ica de StoreFront.

Limitaciones:

- El audio 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 audio se realiza mediante TCP.
- La prioridad del canal ICA puede afectar el audio UDP.

UDP en el cliente

1. Vaya al archivo `$ICAROOT/config/module.ini`.
2. Defina lo siguiente en la sección [ClientAudio]:

   EnableUDPAudio=True

   UDPAudioPortLow=int

   UDPAudioPortHigh=int
3. Defina lo siguiente en la sección [WFClient]:

   EnableUDPThroughGateway=True
4. Vaya al archivo `$HOME/.ICAClient/wfclient.ini`.
5. Defina lo siguiente en la sección [WFClient]:

   AllowAudioInput=True

   EnableAudioInput=true

   AudioBandWidthLimit=1

   > **Notas:**
   >
   > - Los valores establecidos para los atributos `AllowAudioInput`, `EnableAudioInput` y `AudioBandWidthLimit` de la sección [WFClient] se aplican tanto al audio UDP como al audio TCP.
   > - Si no se puede encontrar la carpeta `.ICAClient` (solo ocurre en la primera instalación e inicio), abra la aplicación Citrix Workspace y ciérrela. Esta acción crea la carpeta `.ICAClient`.

> - Cuando `AudioBandWidthLimit` se establece en 1, la calidad de audio del cliente es media.

6. Configure estas directivas en el Delivery Controller del dominio (DDC):
   - Establezca “Redirección de Windows Media” en “Prohibida”.
   - Establezca “Audio sobre UDP” en “Permitido”.
   - Establezca “Transporte de audio en tiempo real sobre UDP” en “Habilitado”.
   - Establezca “Calidad de audio” en “Media”.

Cómo cambiar la manera en la que se usa la aplicación Citrix Workspace

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, es posible que esta transferencia de archivos tarde mucho.
- **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, es posible que esta transferencia de archivos tarde mucho.
- **Evite reproducir contenido multimedia**. La reproducción de contenido multimedia utiliza una gran cantidad de ancho de banda y puede reducir el rendimiento.

USB

La compatibilidad con 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 después de habilitar manualmente la redirección automática por medio de los parámetros del archivo de configuración. La redirección automática de dispositivos USB está inhabilitada de forma predeterminada. Los dispositivos USB disponibles para comunicación remota incluyen los siguientes:

- Unidades flash
- Smartphones
- PDA
- Impresoras
- Escáneres
- Reproductores MP3
- Dispositivos de seguridad
- Tabletas

La redirección de USB requiere Citrix Virtual Apps and Desktops 7.6 o una versión posterior. Citrix Virtual Apps and Desktops y Citrix DaaS no ofrece la redirección de dispositivos USB de almacenamiento masivo y requiere una configuración especial para admitir dispositivos de audio. Para obtener más información, consulte la documentación de Citrix Virtual Apps 7.6.

Las funciones isócronas de los dispositivos USB (como cámaras web, micrófonos, altavoces y auriculares) se admiten en entornos LAN típicos de baja latencia o alta velocidad. Pero, por lo general, la redirección estándar de audio o cámara web es más adecuada.

Estos tipos de dispositivos se admiten directamente en una sesión de aplicaciones y escritorios virtuales, y por lo tanto no ofrecen la funcionalidad USB:

- Teclados
- Mouse
- Tarjetas inteligentes
- Auriculares con micro
- Cámaras web

> **Nota:**
>
> Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y mouse 3D) pueden configurarse para admitir USB. Para obtener información sobre cómo configurar reglas de directivas para otros dispositivos USB especializados, consulte CTX119722.

De manera predeterminada, existen ciertos tipos de dispositivos USB que no se admiten para la comunicación remota a través de Citrix Virtual Apps and Desktops o Citrix DaaS. Por ejemplo, un usuario puede tener una tarjeta de interfaz de red conectada a la placa del sistema mediante un dispositivo USB interno. Conectarse de forma remota a esta NIC no sería apropiado. De forma predeterminada, estos tipos de dispositivos USB no se admiten en aplicaciones ni escritorios virtuales:

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

Para actualizar la lista predeterminada de dispositivos USB disponibles para la comunicación remota, modifique el archivo `usb.conf` en la carpeta `$ICAROOT/`. Para obtener más información, consulte la sección “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 Citrix Virtual Apps and Desktops.

Funcionamiento de los USB

Cuando un usuario conecta un dispositivo USB, se confronta con la directiva USB. Y, si se permite, se redirige al escritorio virtual. Si la directiva predeterminada rechaza el dispositivo, solo estará disponible para el escritorio local.

Piense en un usuario que conecta un dispositivo USB en escritorios a los que se accede a través del modo Desktop Appliance. En este caso, ese dispositivo se redirige automáticamente al escritorio virtual después de habilitarse manualmente la redirección automática a través de los parámetros del archivo de configuración. La redirección automática de dispositivos USB está inhabilitada de forma predeterminada. Para configurar la redirección automática de dispositivos USB, haga lo siguiente:

1. Vaya al archivo de configuración `$Home/.ICAClient/wfclient.ini`.
2. Agregue la siguiente entrada:

   DesktopApplianceMode=True
3. Vaya al archivo de configuración `/opt/Citrix/ICAClient/usb.conf`.
4. Establezca cualquiera de las siguientes reglas de dispositivo:

   - CONNECT: Establezca la palabra clave “CONNECT” para habilitar la redirección automática de un dispositivo cuando se inicie una sesión.
   - ALLOW: Establezca la palabra clave “ALLOW” para permitir la redirección automática de un dispositivo solo después de que se inicie una sesión.
     Sin embargo, si se establece la palabra clave “CONNECT” o “ALLOW”, el dispositivo se redirige automáticamente cuando se desconecta y se conecta durante una sesión.

   Regla de dispositivo de ejemplo:
   CONNECT: vid=046D pid=0002 # Permitir un dispositivo específico por vid/pid
   ALLOW: vid=046D pid=0102 # Permitir un dispositivo específico por vid/pid

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 mediante el modo Desktop Appliance.

Limitación conocida:

Para la redirección de USB, es posible que las directivas definidas en el archivo `usb.conf` no funcionen y que los dispositivos USB no se redirijan a la sesión. Este problema se produce si hay más de 2000 caracteres en el archivo `usb.conf`. Como solución temporal, puede quitar los comentarios existentes de las directivas para reducir la cantidad de caracteres del archivo `usb.conf`.

Dispositivos de almacenamiento masivo

Imagine que un usuario se desconecta de un escritorio virtual cuando un dispositivo de almacenamiento masivo USB sigue conectado al escritorio local. En este caso, ese dispositivo no se redirige

al escritorio virtual cuando el usuario se vuelve a conectar. Para verificar que el dispositivo de almacenamiento masivo se redirige al escritorio virtual, el usuario debe retirar y volver a introducir el dispositivo después de reconectar.

> **Nota:**
>
> Si conecta un dispositivo de almacenamiento masivo en una estación de trabajo Linux configurada para rechazar el uso remoto de dispositivos de almacenamiento masivo USB, la aplicación Citrix Workspace no acepta el dispositivo. 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 dispositivos basados en Debian, puede hacerlo desde la barra de menú de Debian, en **Desktop > Preferences > Removable Drives and Media**. En la ficha **Storage**, en **Removable Storage**, desmarque la casilla de verificación **Browse removable media when inserted**.

A la hora de redirigir el dispositivo USB del cliente, tenga en cuenta estas notas.

> **Notas:**
>
> - Considere que la directiva de servidor para redirección de dispositivos USB del cliente está activada. En este caso, los dispositivos de almacenamiento masivo se dirigen como dispositivos USB, aunque la asignación de unidades del cliente esté activada.
> - La aplicación no admite la redirección de dispositivos compuestos para dispositivos USB.

Clases USB

Las reglas de directivas USB predeterminadas admiten estas clases de dispositivos USB:

- Audio (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 admiten 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. Es posible configurar una cámara para que utilice cualquiera de las clases desde los menús de configuración que proporciona la propia cámara.

Si una cámara aparece como un dispositivo de almacenamiento masivo, se utiliza la asignación de unidades del cliente y no se necesita el uso de 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 la funcionalidad 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 la funcionalidad USB.

  Importante: Se sabe que algunos virus se propagan en forma activa a través de todos los tipos de almacenamiento masivo. Piense bien si existe un requisito 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 uso de 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, y estos dispositivos generalmente se muestran como específicos del proveedor (clase ff).

Clases de dispositivos USB

Las reglas de directivas USB predeterminadas rechazan estas 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, los 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 mouse USB (clase 03, subclase 01, protocolo 2). Este parámetro se debe a que la mayoría de los teclados y mouse se manejan adecuadamente sin el uso de USB. Además, suele ser necesario utilizar estos dispositivos de forma local y remota cuando se conecta a 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 mediante la comunicación remota de la tarjeta inteligente y no se necesita la funcionalidad 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 ultraancha y Bluetooth.

  Es posible que algunos de estos dispositivos proporcionen acceso de red importante o conecten periféricos importantes, como mouse 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 al uso de USB.

Lista de dispositivos USB

Puede actualizar la gama de dispositivos USB disponibles para la conexión remota con los escritorios. Para actualizar dicha gama, modifique la lista de reglas predeterminadas del archivo `usb.conf` del dispositivo de 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 ofrecen al servidor. Las reglas en el servidor controlan los dispositivos que se aceptarán.

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

DENY: class=09 # Dispositivos del hub

DENY: class=03 subclass=01 # Dispositivo de arranque HID (teclados y mouse)

DENY: class=0b # Tarjeta inteligente

DENY: class=e0 # Controladores inalámbricos

DENY: class=02 # Control CDC y comunicaciones

DENY: class=03 # UVC (cámara web)

DENY: class=0a # Datos de CDC

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

Reglas de directivas USB

Sugerencia: Cuando cree 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 del archivo `usb.conf` que hay en el dispositivo de usuario adoptan el formato {ALLOW:|DENY:} seguido de un conjunto de expresiones basadas en valores para las siguientes etiquetas:

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

Al crear 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

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

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

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



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

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` en cada dispositivo de usuario, configure `DesktopApplianceMode = Boolean` de esta manera.

TRUE	Todos los dispositivos USB que ya estén conectados están disponibles al inicio. Los dispositivos están disponibles al inicio solo si no están prohibidos mediante una regla Denegar en las directivas USB del servidor (entrada de Registro) o del dispositivo del usuario (archivo de configuración de reglas de directivas).
FALSE	No hay dispositivos USB disponibles al inicio.

> **Nota:**
>
> Establezca la palabra clave “CONNECT” para habilitar la redirección automática de un dispositivo cuando se inicie una sesión. Además, establezca la palabra clave “ALLOW” para permitir la redirección automática de un dispositivo solo después de que se inicie una sesión. Sin embargo, si se establece la palabra clave CONNECT o ALLOW, el dispositivo se redirige automáticamente cuando se desconecta y se conecta durante una sesión.

Redirección de dispositivos USB compuestos

A partir de la versión 2207, la aplicación Citrix Workspace permite dividir dispositivos USB compuestos. Un dispositivo USB compuesto puede realizar más de una función. Esto se logra mediante la exposición de cada una de esas funciones desde interfaces diferentes. Ejemplos de dispositivos USB compuestos incluyen dispositivos HID que cuentan con entrada y salida de audio y vídeo.

Actualmente, la redirección de dispositivos USB compuestos solo está disponible en la sesión de escritorio. Los dispositivos divididos aparecen en Desktop Viewer.

Antes, cuando un dispositivo se desconectaba y conectaba durante una sesión, se redirigía automáticamente. Como resultado, se conectaba automáticamente al VDA. Con esta versión, debe habilitar

manualmente la redirección automática a través de los parámetros del archivo de configuración. La redirección automática de dispositivos USB compuestos está inhabilitada de forma predeterminada.

USB 2.1 y versiones posteriores admiten la noción de dispositivos USB compuestos donde varios dispositivos secundarios comparten una única conexión con el mismo bus USB. Estos dispositivos emplean un solo espacio de configuración y una conexión de bus compartida, donde se utiliza un número de interfaz único 00-ff para identificar cada dispositivo secundario. Esto no es lo mismo que un concentrador USB que proporciona un nuevo origen de bus USB para otros dispositivos USB con direcciones independientes para la conexión.

Los dispositivos compuestos encontrados en el dispositivo de punto final cliente se pueden reenviar al host virtual como una de estas dos opciones:

- Un solo dispositivo USB compuesto
- Un conjunto de dispositivos secundarios independientes (dispositivos divididos)

Cuando se reenvía un dispositivo USB compuesto, todo el dispositivo deja de estar disponible para el dispositivo de punto final. Esta acción el uso local del dispositivo para todas las aplicaciones del dispositivo de punto final, incluido el cliente Citrix Workspace necesario para ofrecer una experiencia remota con HDX optimizado.

Considere un dispositivo con auriculares USB con dispositivo de audio y un botón HID para el control de volumen y silencio. Si todo el dispositivo se reenvía mediante un canal USB genérico, el dispositivo deja de estar disponible para la redirección por el canal de audio con HDX optimizado. Sin embargo, puede obtener una experiencia óptima cuando el audio se envía a través del canal de audio con HDX optimizado, a diferencia del audio enviado mediante controladores de audio del lado del host a través de la comunicación remota por USB genérico. Esto es porque los protocolos de audio USB suelen provocar ruido.

También nota problemas cuando el teclado del sistema o el dispositivo al que apunta forman parte de un dispositivo compuesto con otras funciones integradas necesarias para admitir sesiones remotas. Cuando se reenvía un dispositivo compuesto completo, el teclado o el mouse del sistema dejan de funcionar en el dispositivo de punto final, excepto en la sesión o la aplicación del escritorio remoto.

Para resolver estos problemas, Citrix recomienda dividir el dispositivo compuesto y reenviar solo las interfaces secundarias que usan un canal USB genérico. Esto garantiza que los demás dispositivos secundarios estén disponibles para su uso en las aplicaciones del dispositivo de punto final del cliente, incluida la aplicación Citrix Workspace que ofrece una experiencia con HDX optimizado, al tiempo que permite el reenvío y la disposición de los dispositivos necesarios a la sesión remota.

Configurar la redirección automática de dispositivos USB compuestos

Antes, cuando un dispositivo se desconectaba y conectaba durante una sesión, se redirigía automáticamente. Como resultado, se conectaba automáticamente al VDA. Con esta versión, debe habilitar

manualmente la redirección automática a través de los parámetros del archivo de configuración. La redirección automática de dispositivos USB compuestos está inhabilitada de forma predeterminada.

Para configurar la redirección automática de dispositivos USB compuestos, haga lo siguiente:

1. Vaya al archivo de configuración $Home/.ICAClient/wfclient.ini.
2. Agregue la siguiente entrada:

   DesktopApplianceMode=True
3. Vaya al archivo de configuración /opt/Citrix/ICAClient/usb.conf.
4. Establezca cualquiera de las siguientes reglas de dispositivo:

   - CONNECT: Establezca la palabra clave "CONNECT" para habilitar la redirección automática de un dispositivo cuando se inicie una sesión.
   - ALLOW: Establezca la palabra clave "ALLOW" para permitir la redirección automática de un dispositivo solo después de que se inicie una sesión.

   Sin embargo, si se establece la palabra clave CONNECT o ALLOW, el dispositivo se redirige automáticamente cuando se desconecta y se conecta durante una sesión.

Regla de dispositivo de ejemplo:

CONNECT: vid=046d pid=0002 # Permitir un dispositivo específico por vid/pid‘

ALLOW: vid=046D pid=0102 # Permitir un dispositivo específico por vid/pid‘

Reglas de dispositivo:

Al igual que los dispositivos USB normales, los dispositivos compuestos para reenvío se seleccionan en función de las reglas de dispositivo establecidas en la configuración de la aplicación Citrix Workspace. La aplicación Citrix Workspace usa estas reglas para decidir los dispositivos USB para los que permitir o impedir el reenvío a la sesión remota.

Cada regla consta de una palabra clave de acción (Permitir, Conectar o Denegar), dos puntos (:) y cero o más parámetros de filtro que coinciden con dispositivos reales en el subsistema USB de los dispositivos de punto final. Estos parámetros de filtro corresponden a los metadatos descriptores del dispositivo USB que utiliza cada dispositivo USB para identificarse.

Las reglas de dispositivo son texto no cifrado con cada regla en una sola línea y un comentario opcional precedido de un carácter #. Las reglas se cotejan de arriba a abajo (orden de prioridad descendente). Se aplica la primera regla que coincida con la interfaz del dispositivo o la interfaz secundaria. Se ignoran las reglas subsiguientes que seleccionen el mismo dispositivo o interfaz.

Para modificar las reglas de dispositivo, haga lo siguiente:

1. Vaya al archivo /opt/Citrix/ICAClient/usb.conf.
2. Actualice las reglas del dispositivo según sea necesario.

Reglas de dispositivo de ejemplo:

```
ALLOW: vid=046D pid=0102 ## Allow a specific device by vid/pid

ALLOW: vid=0505 class=03 subclass=01 ## Allow any pid for vendor 0505 w/
subclass=01

DENY: vid=0850 pid=040C ## deny a specific device (including all child
devices)

DENY: class=03 subclass=01 prot=01 ## deny any device that matches all
filters

CONNECT: vid=0911 pid=0C1C ## Allow and auto-connect a specific device

ALLOW: vid=0286 pid=0101 split=01 ## Split this device and allow all
interfaces

ALLOW: vid=1050 pid=0407 split=01 intf=00,01 ## Split and allow only 2
interfaces

CONNECT: vid=1050 pid=0407 split=01 intf=02 ## Split and auto-connect
interface 2

DENY: vid=1050 pid=0407 split=1 intf=03 ## Prevent interface 03 from being
remoted
```

Puede usar cualquiera de estos parámetros de filtro para aplicar reglas a los dispositivos detectados:

Parámetro de filtro	Descripción
vid=xxxx	ID de proveedor del dispositivo USB (código hexadecimal de cuatro dígitos)
pid=xxxx	ID de producto del dispositivo USB (código hexadecimal de cuatro dígitos)
rel=xxxx	ID de versión del dispositivo USB (código hexadecimal de cuatro dígitos)
class=xx	Código de clase del dispositivo USB (código hexadecimal de dos dígitos)
subclass=xx	Código de subclase del dispositivo USB (código hexadecimal de dos dígitos)
prot=xx	Código de protocolo del dispositivo USB (código hexadecimal de dos dígitos)
split=1 (o split=0)	Seleccione un dispositivo compuesto que dividir (o no dividir)

Parámetro de filtro	Descripción
intf=xx[,xx,xx,…]	Seleccione un conjunto específico de interfaces secundarias de un dispositivo compuesto (lista separada por comas de códigos hexadecimales de dos dígitos)

Los seis primeros parámetros seleccionan los dispositivos USB a los que se debe aplicar la regla. Si algún parámetro no se especifica, la regla coteja dispositivos con CUALQUIER valor para ese parámetro.

El foro de implementadores de USB mantiene una lista de valores definidos de clase, subclase y protocolo en Defined Class Codes. USB-IF también conserva una lista de los ID de proveedores registrados. Puede comprobar los ID de proveedor, producto, versión e interfaz de un dispositivo específico con una herramienta gratuita como lsusb:

```
 <username@username>-ThinkPad-T470:/var/log$ lsusb

Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

Bus 002 Device 002: ID 0bda:0316 Realtek Semiconductor Corp. USB3.0-CRW

Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub

Bus 001 Device 005: ID 138a:0097 Validity Sensors, Inc.

Bus 001 Device 004: ID 5986:111c Acer, Inc Integrated Camera

Bus 001 Device 003: ID 8087:0a2b Intel Corp.

Bus 001 Device 006: ID 17ef:609b Lenovo Lenovo USB Receiver

Bus 001 Device 045: ID 1188:a001 Bloomberg L.P. Lenovo USB Receiver

Bus 001 Device 044: ID 1188:a301 Bloomberg L.P.

Bus 001 Device 043: ID 1188:a901 Bloomberg L.P. Keyboard Hub

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

<!--NeedCopy-->
```



```
| <username@username>-ThinkPad-T470:/var/log$ lsusb -t

/:  Bus 04.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 10000M

/:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M

/:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M

|__ Port 3: Dev 2, If 0, Class=Mass Storage, Driver=usb-storage, 5000M

/:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M

|__ Port 1: Dev 43, If 0, Class=Hub, Driver=hub/4p, 480M

    |__ Port 1: Dev 46, If 0, Class=Human Interface Device, Driver=usbhid, 12M

    |__ Port 4: Dev 45, If 0, Class=Human Interface Device, Driver=usbhid, 12M

    |__ Port 4: Dev 45, If 1, Class=Human Interface Device, Driver=usbhid, 12M

    |__ Port 2: Dev 44, If 3, Class=Audio, Driver=snd-usb-audio, 12M

    |__ Port 2: Dev 44, If 1, Class=Vendor Specific Class, Driver=, 12M

    |__ Port 2: Dev 44, If 4, Class=Audio, Driver=snd-usb-audio, 12M

    |__ Port 2: Dev 44, If 2, Class=Audio, Driver=snd-usb-audio, 12M

    |__ Port 2: Dev 44, If 0, Class=Human Interface Device, Driver=usbhid, 12M

|__ Port 4: Dev 6, If 1, Class=Human Interface Device, Driver=usbhid, 12M

|__ Port 4: Dev 6, If 2, Class=Human Interface Device, Driver=
```



```
          usbhid, 12M
34
35      |__ Port 4: Dev 6, If 0, Class=Human Interface Device, Driver=
          usbhid, 12M
36
37      |__ Port 7: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
38
39      |__ Port 7: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
40
41      |__ Port 8: Dev 4, If 1, Class=Video, Driver=uvcvideo, 480M
42
43      |__ Port 8: Dev 4, If 0, Class=Video, Driver=uvcvideo, 480M
44
45      |__ Port 9: Dev 5, If 0, Class=Vendor Specific Class, Driver=, 12M
          |
46
47  <!--NeedCopy-->
```

Cuando están presentes, los dos últimos parámetros solo se aplican a dispositivos USB compuestos. El parámetro de división determina si un dispositivo compuesto debe reenviarse como dispositivos divididos o como un solo dispositivo compuesto.

Split=1 indica que las interfaces secundarias seleccionadas de un dispositivo compuesto deben reenviarse como dispositivos divididos.
Split=0 indica que el dispositivo compuesto no se debe dividir.

> **Nota:**
>
> Si el parámetro de división se omite, se presupone que Split=0.

El parámetro intf selecciona las interfaces secundarias específicas del dispositivo compuesto al que debe aplicarse la acción. Si se omite, la acción se aplica a todas las interfaces del dispositivo compuesto.

Considere un dispositivo USB compuesto (por ejemplo, un teclado Bloomberg 4) con seis interfaces:

- Interfaz 0: Teclado Bloomberg 4 HID
- Interfaz 1: Teclado Bloomberg 4 HID
- Interfaz 2: Bloomberg 4 HID
- Interfaz 3: Canal de audio del teclado Bloomberg 4
- Interfaz 4: Canal de audio del teclado Bloomberg 4
- Interfaz 5: Canal de audio del teclado Bloomberg 4
- Las reglas sugeridas para este tipo de dispositivo son:

```
CONNECT: vid=1188 pid=9545 split=01 intf=00 ## Bloomberg 4 Keyboard HID

CONNECT: vid=1188 pid=9545 split=01 intf=01 ## Bloomberg 4 Keyboard HID
```



```
CONNECT: vid=1188 pid=9545 split=01 intf=02 ## Bloomberg 4 HID

DENY: vid=1188 pid=9545 split=01 intf=03 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=04 ## Bloomberg 4 Keyboard Audio
Channel

DENY: vid=1188 pid=9545 split=01 intf=05 ## Bloomberg 4 Keyboard Audio
Channel
```

Redirección de dispositivos USB compuestos con Citrix Viewer

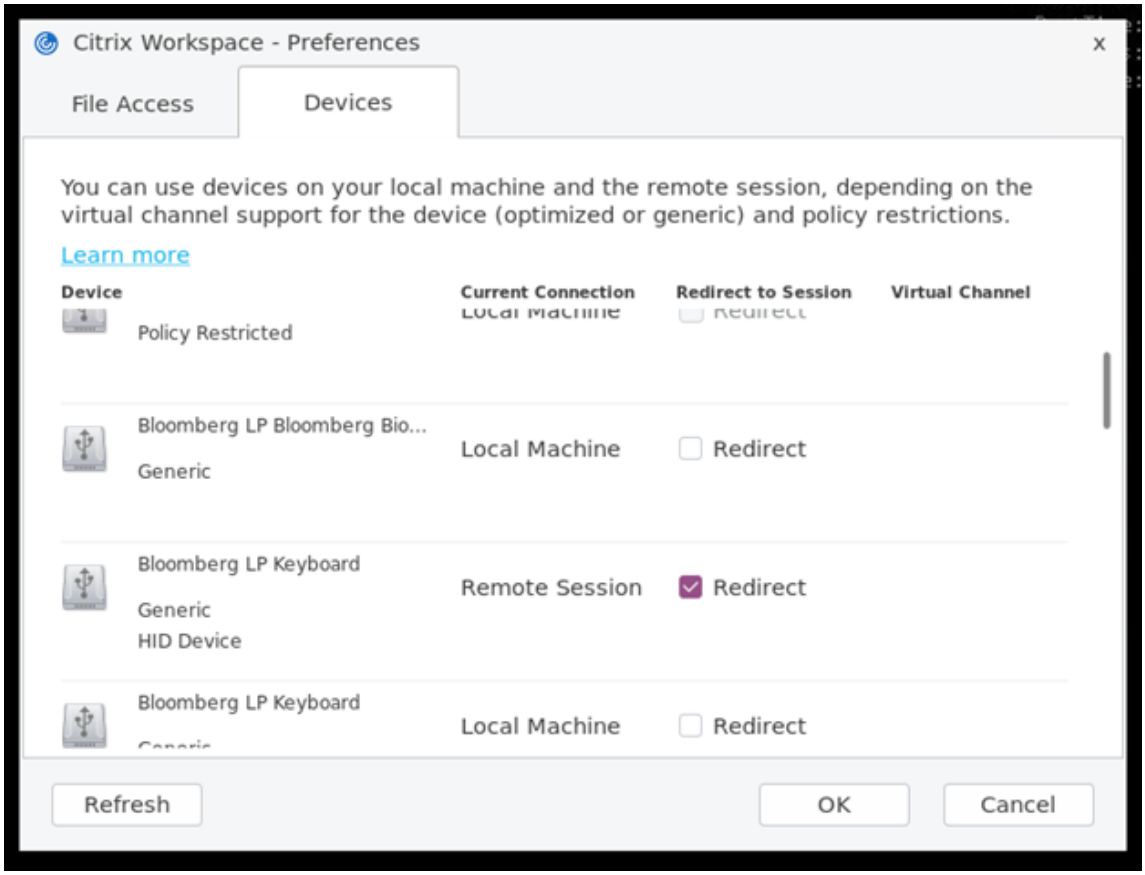
Para conectar los dispositivos USB desde la sección **Dispositivos**, haga lo siguiente:

1. En una sesión de escritorio, vaya a Desktop Viewer en **Dispositivos**.
   Aparecerán los dispositivos USB divididos.

2. Para conectar un dispositivo, seleccione el elemento de menú correspondiente.

Para conectar los dispositivos USB desde la sección **Preferencias**, haga lo siguiente:

1. Vaya a la sección **Preferencias > Dispositivos**.
   Aparecerán los dispositivos USB divididos.



2. Seleccione las casillas de verificación situadas junto a los dispositivos correspondientes.
3. Haga clic en **Aceptar**.

La configuración seleccionada se aplica a la conexión del dispositivo.

> **Nota:**
>
> Desactive el elemento de menú o las casillas de verificación situadas junto a los dispositivos para desconectar los dispositivos correspondientes.

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 algunos casos, es posible que se requiera que los usuarios conecten cámaras web a través de USB. Para conectar cámaras web por USB, inhabilite la compresión de vídeo de cámara web HDX RealTime.

Redirección de cámaras web

A continuación, se presentan algunos puntos sobre la redirección de cámaras web:

- La redirección de cámaras web es compatible con y sin RTME.
- La redirección de cámaras web funciona para aplicaciones de 32 bits y 64 bits. Por ejemplo, Skype, o GoToMeeting. Utilice un explorador de 32 o 64 bits para verificar la redirección de cámaras web online. Por ejemplo: www.webcamtests.com
- El uso de la cámara web es exclusivo de las aplicaciones. Por ejemplo, cuando Skype se ejecuta con una cámara web y usted inicia GoToMeeting, debe salir de Skype para usar la cámara web con GoToMeeting.

Redirección de cámaras web para aplicaciones de 64 bits [Technical Preview]

A partir de la versión 2111, la redirección de cámaras web está disponible en aplicaciones de 64 bits.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Requisitos del sistema

- Versión 0.1.x o 1.x del marco de trabajo `GStreamer`, en función de la versión actual instalada en el sistema.
- Versión de `ICAClient` posterior a 2106 si usa `GStreamer` 1.x
- Versión de `Gstreamer` y plug-ins:
  - `gstreamer1.0-plugins-base`
  - `gstreamer1.0-plugins-bad`
  - `gstreamer1.0-plugins-good`
  - `gstreamer1.0-plugins-ugly`
  - Biblioteca de `gstreamer1.0-vaapi plugin` y `libva`
  - Biblioteca x264

> **Nota:**
>
> La versión del plug-in de `GStreamer` debe coincidir con la versión del marco de trabajo `GStreamer`. Por ejemplo, si instala `Gstreamer` 1.2.4, la versión de todos los plug-ins de `Gstreamer` 1.x debe ser 1.2.4.

Configuración de redirección de cámaras web

Siga estos pasos para activar y configurar la función de redirección de cámaras web para aplicaciones de 64 bits en la aplicación Citrix Workspace para Linux.

Paso 1: Verifique la configuración de ICAClient

Establezca el valor de `AllowAudioInput` en **True** para habilitar la función de redirección de cámaras web. De forma predeterminada, este valor se establece en **True** durante la instalación de `ICAClient`.

Si el valor de `AllowAudioInput` se establece en **False**, haga lo siguiente para habilitar la función de redirección de cámaras web:

1. Vaya al archivo de configuración `~/.ICAClient/wfclient.ini` y modifíquelo.
2. Establezca el valor de `AllowAudioInput` en **True**.

   AllowAudioInput=True

Paso 2: Verifique la configuración del codificador Theora

Después de haber instalado correctamente `ICAClient` y haber establecido el valor de `AllowAudioInput` en **True**, de forma predeterminada se configura el codificador Theora. Este codificador es un codificador basado en software con un rendimiento aceptable. Sin embargo, este codificador solo admite aplicaciones de 32 bits en un VDA.

Haga lo siguiente para comprobar que el codificador Theora admite aplicaciones de 32 bits:

1. Instale Firefox de 32 bits en un VDA.
2. Acceda al sitio de pruebas de cámaras web en `https://webcamtests.com/`.

El codificador Theora no permite usar la redirección de cámaras web para aplicaciones de 64 bits en un VDA. Configure la opción del codificador H264 para que admita la función de redirección de cámaras web para aplicaciones de 64 bits en VDA.

Paso 3: Configure el codificador H264

El codificador H264 permite usar la redirección de cámaras web para aplicaciones de 64 bits en el VDA. Para habilitar el codificador H264, debe hacer lo siguiente:

1. Vaya al archivo de configuración `~/.ICAClient/wfclient.ini` y modifíquelo.
2. Establezca el valor de `HDXH264InputEnabled` en **True**.

   HDXH264InputEnabled=True

Haga lo siguiente para comprobar que el codificador H264 admite aplicaciones de 64 bits:

1. Instale Firefox de 64 bits en un VDA.
2. Acceda al sitio de pruebas de cámaras web en `https://webcamtests.com/`.

Paso 4: Verifique las dependencias del sistema

Después de configurar el codificador H264, si la función de redirección de cámaras web no admite aplicaciones de 64 bits en el VDA, verifique las dependencias del sistema.

La función de redirección de cámaras web para aplicaciones de 64 bits se basa en el marco de trabajo `GStreamer`. `ICAClient` usa la versión 0.1.x o 1.x del marco de trabajo `GStreamer` en función de la versión actual instalada en el sistema.

Paso 4.1: Verifique la versión de ICAClient

Compruebe si la versión de `ICAClient` es posterior a 2106 en caso de que utilice `GStreamer` 1.x. Es posible que las versiones anteriores de `ICAClient` fallen.

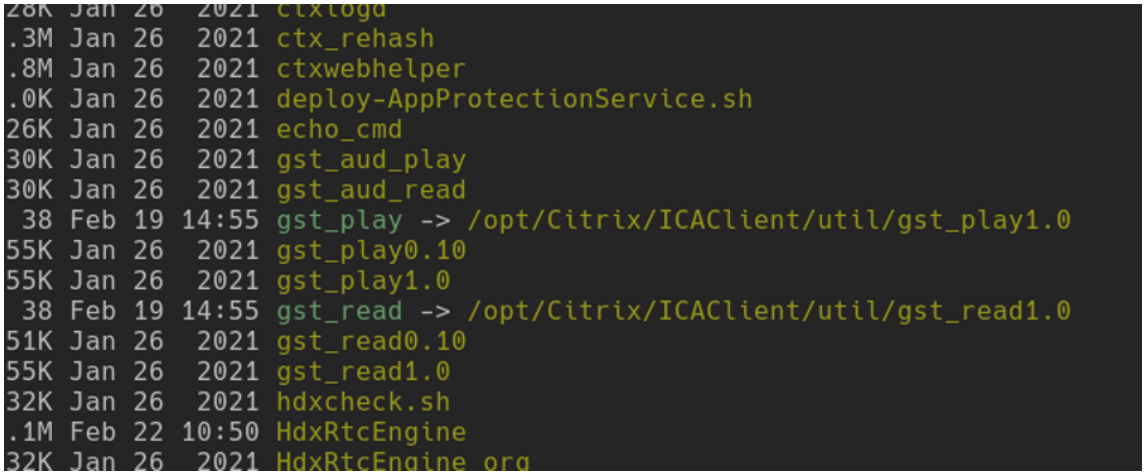
Siga estos pasos para verificar que la versión de `ICAClient` se basa en el marco de trabajo `GStreamer` instalado en su sistema:

1. Introduzca los siguientes comandos en una línea de comandos:

```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
ls -alh
<!--NeedCopy-->
```

2. Verifique si `gst_read symlink` está vinculado a `gst_read1.0` o `gst_read0.1.` como se muestra en esta imagen:



También puede ejecutar el script `workspaceappcheck.sh` en el directorio `util` y verificar el resultado de la sección que hace referencia a las dependencias de `GStreamer`.

Citrix recomienda usar una versión de `ICAClient` igual o posterior a 2106 y `GStreamer` 1.x.

Paso 4.2: Verifique la versión y los plug-ins de GStreamer

Además del marco de trabajo GStreamer 1.x, debe instalar estos plug-ins obligatorios:

- Gstreamer1.0-plugins-base
- Gstreamer1.0-plugins-bad
- Gstreamer1.0-plugins-good
- Gstreamer1.0-plugins-ugly
- Gstreamer1.0-vaapi plugin
- ibva library
- x264 library

Para obtener más información sobre cómo instalar los plugins anteriores, consulte la guía de instalación de GStreamer.

> **Nota:**
>
> La versión del plug-in de GStreamer debe coincidir con la versión del marco de trabajo GStreamer. Por ejemplo, si instala Gstreamer1.2.4, la versión de todos los plug-ins de Gstreamer1.x debe ser 1.2.4.

Ejecute este comando para comprobar la versión actual del marco de trabajo GStreamer:

```
gst-inspect-1.0 --gst-version
<!--NeedCopy-->
```

Para obtener información sobre la solución de problemas, consulte Cámara web en la sección Solución de problemas

Desenfoque de fondo para la redirección de cámaras web

A partir de la versión 2303, la aplicación Citrix Workspace para Linux permite el desenfoque de fondo para la redirección de cámaras web. Para habilitar esta función, lleve a cabo lo siguiente:

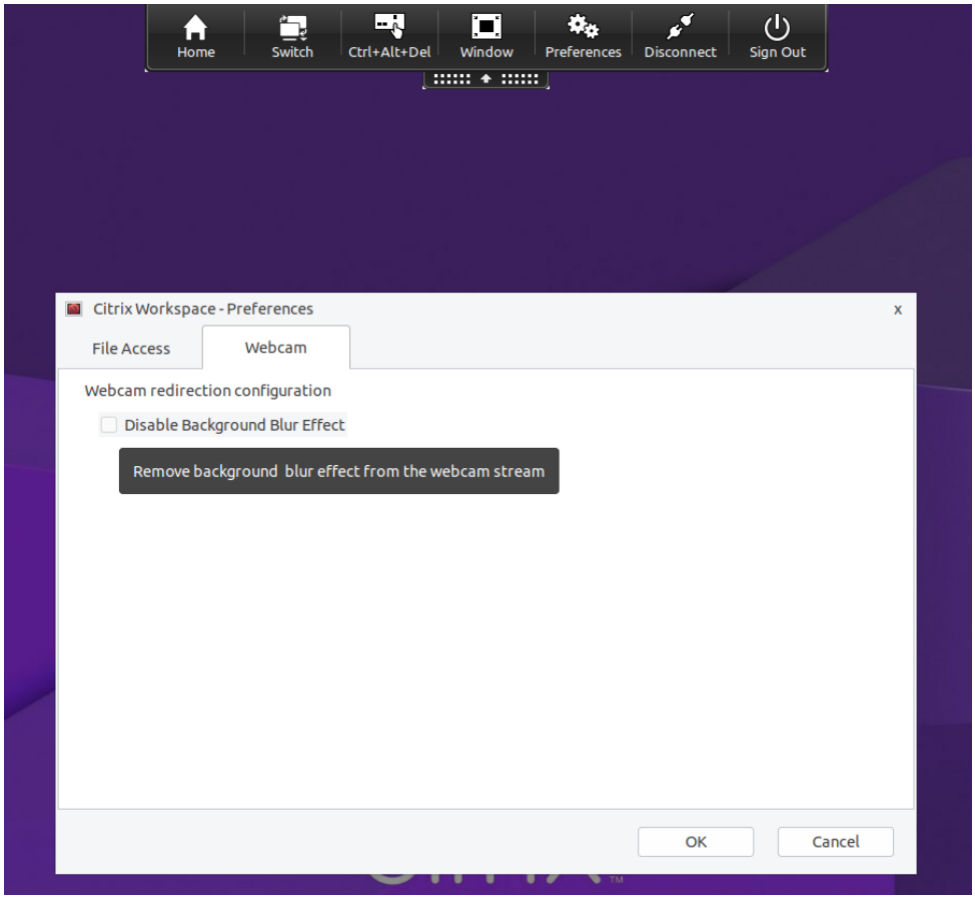
1. Vaya al archivo de configuración ~/.ICAClient/wfclient.ini.
2. Agregue esta entrada en el archivo wfclient.ini:

```
HDXWebCamEnableBackgndEffect=True
<!--NeedCopy-->
```

> **Nota:**
>
> El parámetro de esta configuración habilita el desenfoque de fondo para la función de redirección de cámaras web para clientes con y sin interfaz de usuario.

Para inhabilitar el desenfoque de fondo dentro de la sesión para la redirección de cámaras web mediante la interfaz gráfica de usuario:

1. Haga clic en **Preferencias** en **Desktop Viewer**. Aparecerá el cuadro de diálogo **Citrix Workspace - Preferencias**.
2. Haga clic en la ficha **Cámara web**. Aparecerá el siguiente cuadro de diálogo.



3. Marque la casilla **Inhabilitar efecto de desenfoque de fondo** para inhabilitar el desenfoque de fondo en la redirección de cámaras web.
4. Haga clic en **Aceptar**.

Xcapture

El paquete de la aplicación Citrix Workspace incluye una aplicación auxiliar, xcapture. Esta aplicación ayuda al intercambio de datos gráficos entre el portapapeles del servidor y las aplicaciones de X Window no conformes 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 conformes 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 Entrar (donde /opt/Citrix/ICAClient es el directorio en el que se instaló la aplicación Citrix Workspace).

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 quiere copiar y haga clic con el botón central del puntero.
   - Seleccione una región. Mantenga presionado el botón principal del puntero y arrastre el cursor para seleccionar el área que quiere 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.

Cursor

Compatibilidad con cursor de 32 bits [Technical Preview]

Anteriormente, cuando se utilizaba el cursor personalizado de 32 bits, podía aparecer un cuadro negro alrededor del mismo.

A partir de la versión 2212, la aplicación Citrix Workspace para Linux admite el cursor de 32 bits. De este modo se ha resuelto el problema del cuadro negro que aparecía alrededor del cursor.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Función para invertir el color del cursor

Antes, la aplicación Citrix Workspace mostraba un cursor punteado con el mismo color que el fondo blanco y negro de un texto. Como consecuencia, era difícil ubicar la posición del cursor.

A partir de la versión 2112, el color del cursor se invierte en función del color de fondo del texto. Así, puede ubicar fácilmente la posición del cursor en el texto. De forma predeterminada, esta función está inhabilitada.

Requisitos previos:

- Si `.ICAClient` ya está presente en la carpeta de inicio del usuario actual:

  Elimine el archivo `All_Regions.ini`.

  O bien:

  Para conservar el archivo `All_Regions.ini`, agregue estas líneas al final de la sección [Virtual Channels\Thinwire Graphics]:

  InvertCursorEnabled=

  InvertCursorRefreshRate=

  InvertCursorMode=

Si la carpeta `.ICAClient` no está presente, entonces es que indica una nueva instalación de la aplicación Citrix Workspace. En ese caso, se conserva la configuración predeterminada para la función.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya al archivo de configuración `$HOME/.ICAClient/wfclient.ini`.
2. Vaya a la sección [Thinwire3.0] y configure esta entrada:

   InvertCursorEnabled=True

> **Nota:**
>
> El cursor no se invierte cuando el valor de la directiva **Usar códec de vídeo para compresión** en Citrix Studio está establecido en `Do not use video codec`.

Puntero

Mouse relativo

La función del mouse relativo ofrece una opción para interpretar la posición del mouse 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 mouse relativo y no de un mouse absoluto.

> **Nota:**
>
> Esta función solo está disponible en sesiones que se ejecutan en Citrix Virtual Apps and Desktops 7.8 (o versiones posteriores) o Citrix DaaS. 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.

Este paso habilita la función, pero la mantiene inactiva hasta que usted la active. Para obtener más información sobre cómo habilitar funciones del mouse relativo, consulte la sección Valores alternativos del mouse relativo.

Para activar la función:

Introduzca Ctrl/F12.

Una vez que la función está habilitada, escriba Ctrl/F12 nuevamente para sincronizar la posición del puntero del servidor con el cliente. Las posiciones del puntero del servidor y del cliente no están sincronizadas cuando se utiliza el mouse 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 del mouse 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.
- RelativeMouse=4 Habilita o inhabilita la funcionalidad cuando se oculta o se muestra el puntero del mouse del lado del cliente. Este modo es adecuado para habilitar o inhabilitar automáticamente el mouse relativo para interfaces de aplicaciones de juego en primera persona.

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 la aplicación Citrix Workspace. Los valores de **RelativeMouseOnShift** y **RelativeMouseOffShift** establecen las teclas modificadoras para usarse, y se recogen en el título [Hotkey Shift States].

Teclado

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:
    - True significa que Ctrl+Alt+Fin pasa la combinación Ctrl+Alt+Supr al escritorio remoto.
    - False (valor predeterminado) significa que Ctrl+Alt+Entrar pasa la combinación Ctrl+Alt+Supr al escritorio remoto.

Redirección genérica

Configuración del teclado Bloomberg v4 a través de una redirección de USB genérico del lado del cliente:

Como requisito previo, la directiva debe habilitarse en el Domain Delivery Controller (DDC).

1. Busque el vid y el pid del teclado Bloomberg. Por ejemplo, en Debian y Ubuntu ejecute el siguiente comando:

    ```
    lsusb
    ```

2. Vaya a $ICAROOT y modifique el archivo usb.conf.
3. Agregue la siguiente entrada en el archivo usb.conf para que pueda realizarse la redirección del teclado Bloomberg a través de un USB y, a continuación, guarde el archivo.

    ALLOW: vid=1188 pid=9545

4. Reinicie el demonio `ctxusbd` en el cliente. Por ejemplo, en Debian y Ubuntu ejecute el siguiente comando:

    ```
    systemctl restart ctxusbd
    ```


5. Abra una sesión de cliente. Asegúrese de que el foco se encuentra en esa sesión mientras conecta el teclado Bloomberg v4 para su redirección.

Redirección de contenido del explorador web

Chromium Embedded Framework (CEF) para la redirección de contenido del explorador web

En versiones anteriores a la versión 1912, BCR utilizaba una superposición basada en WebkitGTK+ para generar el contenido. Sin embargo, en los clientes ligeros había problemas de rendimiento. A partir de la versión 1912, BCR utiliza una superposición basada en CEF. Esta funcionalidad enriquece la experiencia del usuario para la redirección de contenido de explorador web. Reduce la carga de red, el procesamiento de páginas y la generación de gráficos para el dispositivo de punto final.

A partir de la versión 2106, la redirección de contenido del explorador web basada en CEF es totalmente funcional. Esta función está activada de forma predeterminada.

Si es necesario, puede reemplazar el archivo `libffmpeg.so` proporcionado en el paquete de la aplicación Workspace por un archivo `libffmpeg.so` adecuado en la ruta `$ICAROOT/bcr/libffmpeg.so` que tenga los códecs necesarios.

> **Nota:**
>
> Esta función no está disponible en la plataforma armhf.

Habilitar la redirección de contenido del explorador web basada en CEF

Para habilitar la redirección de contenido del explorador web basada en CEF:

1. Vaya al archivo `$ICAROOT/config/All_Regions.ini`, donde $ICAROOT es el directorio de instalación predeterminado de la aplicación Citrix Workspace.
2. Vaya a la sección `[Client Engine\WebPageRedirection]` y configure esta entrada:

   UseCefBrowser=True

Problemas conocidos:

- Al establecer la opción `UseCefBrowser` en **True** en `~/.ICAClient/All_Regions.ini`, es posible que el IME de japonés, chino simplificado y coreano no funcione en los campos donde se pueda introducir texto. La aplicación Citrix Workspace para Linux no admite el IME de japonés, chino simplificado ni coreano cuando se utiliza Secure SaaS con el explorador integrado de Citrix.
- Al intentar iniciar una redirección de páginas web mediante redirección de contenido de explorador web basada en CEF, es posible que reciba un error de certificado desconocido. El problema se produce a partir de la versión 2106 de la aplicación Citrix Workspace.

Como solución temporal, ejecute este comando en el terminal para importar el certificado autofirmado en nssdb:

```
certutil -A -n "badssl.cer" -t "C,," -d ~/.pki/nssdb -i ~/
   Downloads/badssl.cer
<!--NeedCopy-->
```

Los argumentos de los comandos son:

- -A: Para agregar un certificado a la base de datos.
- -n: El nombre del certificado. Este argumento es opcional y se puede usar para agregar el apodo.
- "badssl.cer": El nombre del certificado que se exporta desde el sitio badssl.com.
- -t "C,," - -t es para TRUSTARGS y C es para el certificado de CA. Para obtener más información, consulte la documentación de Google.
- -d ~/.pki/nssdb: La ubicación de la base de datos.
- -i: Indica el archivo de entrada. Este argumento es para agregar la ubicación y el nombre del archivo de certificado.

Para obtener información sobre la redirección de contenido del explorador web, consulte Redirección de contenido de explorador web en la documentación del producto Citrix Virtual Apps and Desktops.

Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web

A partir de la versión 2303 de la aplicación Citrix Workspace, se le solicita que configure la ruta de almacenamiento de datos temporales para el explorador web basado en CEF. Para configurar la ruta, haga lo siguiente:

1. Vaya al archivo $ICAROOT/config/All_Regions.ini, donde $ICAROOT es el directorio de instalación predeterminado de la aplicación Citrix Workspace.
2. Vaya a la sección [Client Engline\WebPageRedirection] y agregue la siguiente entrada:

```
CefCachePath = <folder for CEF based BCR tmp files>
<!--NeedCopy-->
```

Reconexión automática

Este apartado describe la función de reconexión automática de clientes de HDX Broadcast. Citrix recomienda utilizar esta función en combinación con la función Fiabilidad de la sesión 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, la aplicación Citrix Workspace para Linux 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 Workspace 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 introducir 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 solo pueden volver a conectarse a sesiones desconectadas.

De forma predeterminada, la aplicación Citrix Workspace para Linux 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 de interrupciones de la red, compruebe que la función de fiabilidad de la sesión está habilitada tanto en el servidor como en el cliente, y que está configurada en Access Gateway.

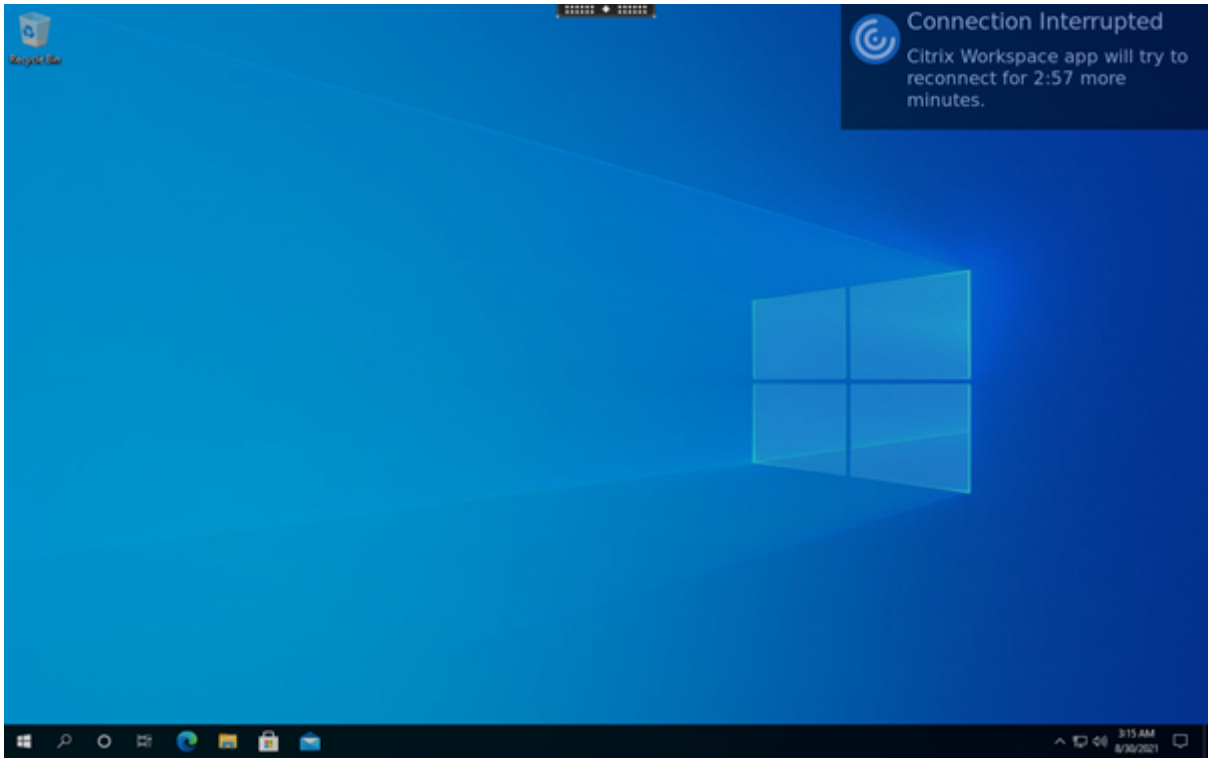
Para obtener instrucciones acerca de la configuración de la reconexión automática de clientes de HDX Broadcast, consulte la documentación de Citrix Virtual Apps and Desktops.

Fiabilidad de la sesión

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, es posible que los usuarios inalámbricos que pasen por un túnel pierdan 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.

Ahora puede ver los cambios en la pantalla cuando se inicia la fiabilidad de la sesión. Con esta mejora, la ventana de la sesión se atenúa y aparece un temporizador con una cuenta atrás que muestra el tiempo restante hasta el siguiente intento de reconexión.



> **Sugerencia**
>
> Puede modificar el brillo de la escala de grises utilizado para las sesiones inactivas mediante la directiva **Nivel de transparencia de la interfaz de usuario durante la reconexión**. De forma predeterminada, este valor está establecido en 80. El valor máximo es 100 (esto indica una ventana transparente) y el valor mínimo es 0 (esto indica una pantalla en negro).

Cuando la sesión se reconecta correctamente, desaparece el mensaje de notificación de la cuenta atrás. Puede interactuar con el escritorio como de costumbre.

A partir de la versión 2109, la notificación de fiabilidad de la sesión está habilitada de forma predeterminada.

Para inhabilitar esta mejora:

1. Vaya al archivo de configuración `/opt/Citrix/ICAClient/config/module.ini`.
2. En la sección [WFClient], modifique este parámetro:

```
SRNotification=False
```

> **Nota:**
>
> Esta función solo está disponible en Citrix Virtual Desktops.

Cuando se configuran la reconexión automática de clientes y la fiabilidad de la sesión, esta última tiene prioridad si se produce algún problema de conexión. La función Fiabilidad de la sesión intenta volver a establecer una conexión con la sesión existente. Puede llevar hasta 25 segundos detectar un

problema de conexión. Y luego transcurre un período configurable (el valor predeterminado es 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 Workspace no pueden anular la configuración del servidor.

> **Importante:**
>
> 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.

Uso de directivas de fiabilidad de la sesión

La configuración de directiva de conexiones de fiabilidad de la sesión habilita la fiabilidad de la sesión.

La configuración de directiva Tiempo de espera de fiabilidad de la sesión tiene un tiempo predeterminado de 180 segundos, o tres minutos. Si es necesario, puede ampliar el tiempo que la fiabilidad de la sesión mantiene abierta una sesión. No se le pedirá que vuelva a autenticarse.

> **Sugerencia**
>
> A medida que prolonga el tiempo que una sesión se mantiene abierta, es posible que se distraiga y se aleje de su dispositivo. Esta situación puede dejar la sesión accesible para usuarios no autorizados.

Las conexiones entrantes con la función de fiabilidad de la sesión utilizan el puerto 2598 a menos que cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.

Para obtener información sobre la configuración de directivas de fiabilidad de la sesión, consulte Configuraciones de la directiva Fiabilidad de la sesión.

> **Nota:**
>
> De forma predeterminada, la fiabilidad de sesión se habilita en el servidor. Para inhabilitar esta función, configure la directiva administrada por el servidor.

Rendimiento multimedia

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

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

> **Nota:**
>
> Citrix admite la coexistencia de RTOP con la aplicación Citrix Workspace para Linux versión 1901 y versiones posteriores con `GStreamer` 0.1.

Redirección de HDX MediaStream para Windows Media

La redirección de HDX MediaStream para Windows Media 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 multimedia en tiempo de ejecución en el dispositivo del usuario y no en el servidor. Como resultado, se reducen 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 audio WAV

La aplicación Citrix Workspace 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 admitidos
- 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 admitidos por `GStreamer` en un dispositivo de 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 de 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 el servidor no manipula los datos multimedia. Esta función requiere bibliotecas avanzadas multimedia de GStreamer en el dispositivo.

Para implementar la redirección de HDX MediaStream para Windows Media:

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 la aplicación Citrix Workspace para que, durante el proceso de instalación de la aplicación Citrix Workspace, este se configure para utilizar GStreamer.

   La mayoría de las distribuciones Linux incluyen GStreamer. También puede descargar GStreamer de http://gstreamer.freedesktop.org.

2. Para habilitar la obtención de contenido en el lado del cliente, instale los *plug-ins* 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 plug-in se encuentre instalado y funcione correctamente. Si gst-launch puede reproducir la dirección URL, el plug-in 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 la aplicación Citrix Workspace en el dispositivo, seleccione la opción de GStreamer si está utilizando el script tarball (este paso se completa 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 función 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. Puede volver al protocolo de playbin anterior para todas las funciones de MediaStream, excepto la obtención de contenido del lado del cliente. La función de obtención de contenido del lado del cliente sigue utilizando playbin2, con la opción SpeedScreenMMAEnablePlaybin2 de la sección Multimedia del archivo All-Regions.ini.
- La aplicación Citrix Workspace 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, GStreamer 0.10 se usa para la redirección de Windows Media de HDX MediaStream. GStreamer 1.0 solo se usa cuando GStreamer 0.10 no está disponible.
- Si quiere usar GStreamer 1.0, siga estos instrucciones:

1. Busque el directorio de instalación de los plug-ins de GStreamer. La ubicación de instalación de los plug-ins 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 la aplicación Citrix Workspace 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 la plataforma puede ser linuxx64, por ejemplo). Para obtener más información, consulte Instalar y configurar.
3. Instale libgstflatstm1.0.so mediante un vínculo simbólico en el directorio de plug-ins 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.

Habilitar GStreamer 1.x

En versiones anteriores a 1912, GStreamer 0.10 era la versión predeterminada admitida para la redirección multimedia. A partir de la versión 1912, puede configurar GStreamer 1.x como la versión predeterminada.

Limitaciones:

- Al reproducir un vídeo, es posible que rebobinar y avanzar no funcionen según lo previsto.
- Al iniciar la aplicación Citrix Workspace en dispositivos armhf, es posible que GStreamer 1.x no funcione según lo previsto.

Para instalar GStreamer 1.x

Instale el marco de trabajo GStreamer 1.x y los siguientes plug-ins desde https://gstreamer.freedesktop.org/documentation/installing/on-linux.html:

- Gstreamer-plugins-base
- Gstreamer-plugins-bad

- Gstreamer-plugins-good
- Gstreamer-plugins-ugly
- Gstreamer-libav

Para crear binarios localmente

En algunas distribuciones de SO de Linux (por ejemplo, SUSE y openSUSE), es posible que el sistema no encuentre los paquetes de GStreamer en la lista de fuentes predeterminada. En este caso, descargue el código fuente y cree todos los binarios localmente:

1. Descargue el código fuente desde https://gstreamer.freedesktop.org/src/.
2. Extraiga el contenido.
3. Vaya al directorio donde está disponible el paquete descomprimido.
4. Ejecute los comandos siguientes:

```
$sudo ./configure
$sudo make
$sudo make install
<!--NeedCopy-->
```

De forma predeterminada, los binarios generados están disponibles en */usr/local/lib/gstreamer-1.0/*.

Para obtener información sobre la solución de problemas, consulte el artículo CTX224988 de Knowledge Center.

Para configurar GStreamer 1.x

Para configurar GStreamer 1.x y usarlo con la aplicación Citrix Workspace, aplique esta configuración desde el símbolo del shell:

- $ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so.
- $ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play

Donde:

- ICACLIENT_DIR: Es la ruta de instalación de la aplicación Citrix Workspace para Linux.
- GST_PLUGINS_PATH: La ruta del plug-in de GStreamer. Por ejemplo, en una máquina Debian de 64 bits es */usr/lib/x86_64-linux-gnu/gstreamer-1.0/*.

Limitaciones:

- En versiones anteriores a la 2106, es posible que la redirección de cámaras web fallara y que la sesión se desconectara al usar GStreamer 1.15.1 o una versión posterior.

Redirección de HDX MediaStream para Flash

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 audio y vídeo de alta definición sin aumentar los requisitos de ancho de banda.

1. Compruebe 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 valor se establece en **Never**. Además, se presenta un cuadro de diálogo a los usuarios para preguntarles si quieren optimizar el contenido de Flash al conectarse a páginas web con dicho contenido.

   - **HDXFlashEnableServerSideContentFetching=Disabled**; **Enabled**

     Habilita o inhabilita la obtención de contenido en el servidor para la aplicación Citrix Workspace. De forma predeterminada, este valor está configurado como **Disabled**.

   - **HDXFlashUseServerHttpCookie=Disabled**; **Enabled**

     Habilita o inhabilita la redirección de cookies HTTP. De forma predeterminada, este valor está configurado como **Disabled**.

   - **HDXFlashEnableClientSideCaching=Disabled**; **Enabled**

     Habilita o inhabilita el almacenamiento en caché del cliente del contenido Web obtenido por la aplicación Citrix Workspace. De forma predeterminada, este valor está configurado como **Enabled**.

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

     Define el tamaño, en megabytes (MB), de la caché en el cliente. Este valor puede tener cualquier tamaño entre 25 MB 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 valor está establecido en **100**.

   - **HDXFlashServerSideContentCacheType=Persistent**: **Temporary**; **NoCaching**

     Define el tipo de almacenamiento en caché que utiliza la aplicación Citrix Workspace para el contenido que se obtiene en el servidor. De forma predeterminada, este valor está configurado como
     Persistent.

Nota: Este parámetro solo es necesario 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.

Compresión de vídeo de cámara web HDX RealTime

HDX RealTime proporciona una opción de compresión de vídeo de las cámaras web para mejorar la eficiencia del ancho de banda durante las videoconferencias. Esta opción garantiza que los usuarios disfruten de un rendimiento óptimo al usar aplicaciones como GoToMeeting con HDFaces o Skype Empresarial.

1. Compruebe que el dispositivo del usuario cumpla los requisitos de esta función.
2. Compruebe que el canal virtual `Multimedia` esté habilitado. Para habilitarlo, abra el archivo `$ICAROOT/config/module.ini` y compruebe que `MultiMedia`, en la sección [ICA3.0], esté establecido en `On`.
3. Para habilitar la entrada de audio, haga clic en **Usar mi micrófono y mi cámara web en la página Micrófono y cámara web** del cuadro de diálogo **Preferencias**.

Inhabilitar 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 algunos casos, es posible que se requiera que los usuarios conecten cámaras web a través de USB. Para realizar esta conexión, debe hacer lo siguiente:

- Inhabilitar la compresión de vídeo de cámara web HDX RealTime
- Habilitar la compatibilidad de USB para cámaras web

1. Agregar el parámetro siguiente en la sección [WFClient] del archivo INI apropiado:

   AllowAudioInput=False

   Para obtener más información, consulte Parámetros predeterminados.

2. Abra el archivo `usb.conf`, que normalmente está disponible en `$ICAROOT/usb.conf`.
3. Quite esta línea o conviértala en comentario:

   > DENY: class 0e # UVC (opción predeterminada a través de la compresión de vídeo de cámara web HDX RealTime)

4. Guarde el archivo y ciérrelo.

Función experimental de SaaS seguro con explorador Citrix incrustado

El acceso seguro a las aplicaciones SaaS ofrece una experiencia de usuario unificada en la entrega de aplicaciones SaaS publicadas a los usuarios. Las aplicaciones SaaS están disponibles con el inicio Single Sign-On. Ahora los administradores pueden proteger la red de la organización y los dispositivos de los usuarios finales frente al malware y las filtraciones de datos. Para esta protección, puede filtrar el acceso a sitios web y categorías de sitios web específicos.

La aplicación Citrix Workspace para Linux admite el uso de aplicaciones SaaS mediante Access Control Service. Este servicio permite a los administradores proporcionar una experiencia coherente, con Single Sign-On e inspección de contenido.

Requisito previo:

Compruebe que el paquete `libgtkglext1` esté disponible.

La entrega de aplicaciones SaaS desde la nube presenta los siguientes beneficios:

- Configuración simple: Fácil de operar, actualizar y consumir.
- Single Sign-On: Inicio de sesión sin complicaciones gracias a Single Sign-On.
- Plantilla estándar para aplicaciones diferentes: Configuración basada en plantillas para las aplicaciones de uso extendido.

> **Nota:**
>
> SaaS con Citrix Browser Engine solo se admite en plataformas x64 y x86 y no en hardware ArmHardFloatPort (armhf).

Para obtener información sobre cómo configurar aplicaciones SaaS con Access Control Services, consulte la documentación de Access Control.

Para obtener más información acerca de las aplicaciones SaaS con la aplicación Citrix Workspace, consulte Configuración de Workspace en la documentación más reciente de la aplicación Citrix Workspace para Windows.

H.264

La aplicación Citrix Workspace admite la presentación de gráficos H.264, incluidos gráficos HDX 3D Pro, proporcionados por los servidores de Citrix Virtual Apps and Desktops 7. Se utiliza la función de códec de compresión profunda, que se encuentra habilitada de forma predeterminada. Esta función ofrece un mejor rendimiento de las aplicaciones de gráficos de nivel profesional en redes WAN, comparado con el códec de JPEG existente.

> **Nota:**
>
> En H.264, la aplicación Citrix Workspace para Linux solo admite el formato YUV420 y no admite el formato YUV444.

Siga las instrucciones en este tema para inhabilitar esta función (y procesar gráficos mediante el códec de JPEG en su lugar). También puede inhabilitar el seguimiento de texto, pero, a su vez, mantener habilitado el códec de compresión profunda. Este parámetro ayuda a reducir los costes 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 funcionalidad, no use ninguna opción con pérdida en la directiva Calidad visual de Citrix Virtual Apps and Desktops o Citrix DaaS. Si lo hace, la codificación H.264 se inhabilita en el servidor y no funciona en la aplicación Citrix Workspace.

Para inhabilitar el códec de compresión profunda:

En el archivo `wfclient.ini`, establezca **H264Enabled** en **False**. Este parámetro también inhabilita el seguimiento de texto.

Para inhabilitar solo el seguimiento de texto:

Con la compatibilidad con códecs de compresión profunda habilitada, en el archivo `wfclient.ini`, establezca **TextTrackingEnabled** en **False**.

Mosaicos 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. Verifique que su biblioteca JPEG admite 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 `XSync` diferido.

Registros

En versiones anteriores, los archivos `debug.ini` y `module.ini` se utilizaban para configurar los registros.

A partir de la versión 2009, puede configurar los registros mediante uno de estos métodos:

- Interfaz de la línea de comandos
- Interfaz gráfica (GUI)

También a partir de la versión 2009, se elimina el archivo de configuración `debug.ini` del paquete de instalación de la aplicación Citrix Workspace.

Los registros capturan los detalles de implementación de la aplicación Citrix Workspace, los cambios de configuración y las actividades administrativas en una base de datos de registros. Un desarrollador externo puede aplicar este mecanismo de registro mediante el SDK de registro, que se incluye como parte del SDK de optimización de plataformas de la aplicación Citrix Workspace.

Puede utilizar la información de registro para:

- Diagnosticar y solucionar problemas técnicos que se produzcan después de cualquier cambio. El registro proporciona un rastro de los pasos seguidos.
- Ayudar en la administración de cambios y en el seguimiento de las configuraciones.
- Realizar informes sobre las actividades administrativas.

Si la aplicación Citrix Workspace está instalada con privilegios de usuario root, los registros se almacenan en `/var/log/citrix/ICAClient.log`. De lo contrario, los registros se almacenan en `${ HOME } /.ICAClient/logs/ICAClient.log`.

Cuando se instala la aplicación Citrix Workspace, se crea un usuario llamado `citrixlog` para gestionar la funcionalidad de los registros.

Interfaz de la línea de comandos

1. En el símbolo del sistema, vaya a la ruta `/opt/Citrix/ICAClient/util`.
2. Ejecute el siguiente comando para definir las preferencias de registro.

   ```
   ./setlog help
   ```

Se muestran todos los comandos disponibles.

En la tabla siguiente se enumeran varios módulos y sus valores de clase de seguimiento correspondientes. Utilice la tabla siguiente para un conjunto de valores de registro de línea de comandos específico:

Módulo	Clase del registro
Afirmaciones	LOG_ASSERT
Monitor de audio	TC_CM
BCR con CEF	TC_CEFBCR
Asignación de audio del cliente	TC_CAM
Central de conexiones	TC_CONNCENTER
Puerto de comunicación del cliente	TC_CCM
Asignación de unidades del cliente	TC_CDM
Clip	TC_CLIP

Módulo	Clase del registro
Asignación de impresoras del cliente	TC_CPM
Asignación de impresoras del cliente	TC_CPM
Fuente	TC_FONT
Fotograma	TC_FRAME
Abstracción de gráficos	TC_GA
Editor de métodos de entrada	TC_IME
IPC	TC_IPC
Asignación de teclado	TC_KEY
Controlador de licencias	TC_VDLIC
Contenido multimedia	TC_MMVD
Asignación de mouse	TC_MOU
MS Teams	TC_MTOP
Otras bibliotecas	TC_LIB
Controlador de protocolo	TC_PD
Almacén PNA	TC_PN
Registros de eventos estándar	LOG_CLASS
SRCC	TC_SRCC
Inicio de sesión SSPI	TC_CSM
Tarjeta inteligente	TC_SCARDVD
Autoservicio	TC_SS
Extensión de autoservicio	TC_SSEXT
StoreFrontLib	TC_STF
Controlador de transporte	TC_TD
Thinwire	TC_TW
Interfaz de ventana transparente	TC_TUI
Canal virtual	TC_VD
PAL	TC_VP
IU	TC_UI
UIDialogLibWebKit3	TC_UIDW3

Módulo	Clase del registro
UIDialogLibWebKit3_ext	TC_UIDW3E
Demonio USB	TC_CTXUSB
Controlador de fotogramas de vídeo	TC_VFM
WebKit	TC_WEBKIT
Controlador WinStation	TC_WD
`Wfica`	TC_NCS
Motor `Wfica`	TC_WENG
`Wfica` Shell	TC_WFSHELL
Ayudante web	TC_WH
Latencia cero	TC_ZLC

Interfaz gráfica (GUI)

Vaya a **Menú** > **Preferencias**. Aparecerá el cuadro de diálogo **Citrix Workspace - Preferencias**.

A niveles cada vez mayores de detalle de trazado, están disponibles los siguientes valores:

- Inhabilitado
- Solo error
- Normal
- Detallado

De forma predeterminada, la opción **Registros** se establece en **Solo error**.

Debido a la gran cantidad de datos que se pueden generar, es posible que el rastreo afecte de manera significativa al rendimiento de la aplicación Citrix Workspace. Solo se recomienda el nivel **Detallado** si es necesario para solucionar problemas.

Haga clic en **Guardar y cerrar** después de seleccionar el nivel de registro deseado. Los cambios se aplican dinámicamente en la sesión.

Haga clic en el icono de configuración situado junto al menú desplegable de opciones de **Registro**. Aparecerá el cuadro de diálogo **Preferencias de registro de Citrix**.

> **Nota:**
>
> Si elimina el archivo `ICAClient.log`, debe reiniciar el servicio de registros `ctxlogd`.

> Por ejemplo, si utiliza una instalación compatible con el sistema, ejecute el siguiente comando:
>
> `systemctl restart ctxlogd`.

Habilitar el registro en la versión 2006 y versiones anteriores:

Si tiene la versión 2006 o una anterior, habilite los registros mediante el procedimiento siguiente:

1. Descargue e instale la aplicación Citrix Workspace en su máquina Linux.
2. Defina la variable de entorno `ICAROOT` en la ubicación de instalación.

   Por ejemplo: `/opt/Citrix/ICAClient`.

   De forma predeterminada, la clase de rastreo `TC_ALL` está habilitada para proporcionar todos los rastreos.
3. Para recopilar registros de un módulo en concreto, abra el archivo `debug.ini` en `$ICAROOT` y agregue los parámetros de rastreo requeridos a la sección `[wfica]`.

   Agregue las clases de seguimiento con un símbolo “+”. Por ejemplo: `+TC_LIB`.

   Se pueden agregar diferentes clases separadas por barras verticales.
   Por ejemplo: `+TC_LIB|+TC_MMVD`.

En esta tabla se enumeran los módulos `wfica` y sus valores de clase de seguimiento correspondientes:

Módulo	Valor de traceClasses
Gráficos	TC_TW
EUEM	TC_EUEM
WFICA (inicio de sesiones)	TC_NCS
Impresión	TC_CPM
Secuencia de conexión: WD	TC_WD
Secuencia de conexión: PD	TC_PD
Secuencia de conexión: TD	TC_TD
Archivos relacionados con el proxy	TC_PROXY
Cámara web / controlador virtual multimedia	TC_MMVD
Controladores virtuales	TC_VD
Asignación de unidades del cliente	TC_CDM
Audio	TC_CAM
COM (puerto de comunicaciones)	TC_CCM

Módulo	Valor de traceClasses
Conexión directa	TC_TWI
Tarjeta inteligente	TC_SCARDVD

En esta tabla se enumeran los módulos de la central de conexiones y su valor de clase de seguimiento correspondientes:

Módulo	Valor de traceClasses
Central de conexiones	TC_CSM

En esta tabla se muestra el valor de clase de seguimiento de setWebHelper:

Valor de traceClasses
Establezca logSwitch en 1 (para habilitarlo) o 0 (para inhabilitarlo)
Ejemplo: logSwitch = 1

Solución de problemas:

Si `ctxlogd` deja de responder, los registros se rastrean en syslog.

Para obtener información sobre cómo obtener registros nuevos y actualizados en inicios posteriores, consulte Configuración de Syslog.

Configuración de Syslog

De forma predeterminada, todos los registros de syslog se guardan en /var/log/syslog. Para configurar la ruta y el nombre del archivo de registros, modifique esta línea en la sección [RULES] del archivo `/etc/rsyslog.conf`. Por ejemplo:

```
1 user.* -/var/log/logfile_name.log
```

Guarde los cambios y reinicie el servicio syslog mediante el comando:

```
sudo service rsyslog restart
```

Puntos que tener en cuenta:

- Para comprobar que hay disponible un nuevo syslog, elimine syslog y ejecute el comando: `sudo service rsyslog restart`.

- Para evitar mensajes duplicados, agregue **$RepeatedMsgReduction on** al principio del archivo `rsyslog.conf`.
- Para recibir registros, compruebe que la línea **$ModLoad imuxsock.so** no esté comentada al principio del archivo `rsyslog.conf`.

Registro remoto

Para habilitar el registro remoto:

- **Configuración del lado del servidor:** Quite las marcas de comentario en las siguientes líneas del archivo rsyslog.conf, presente en el servidor syslog:

  ```
  $ModLoad imtcp

  $InputTCPServerRun 10514
  ```

- **Configuración del lado del cliente:** Agregue esta línea en el archivo `rsyslog.conf` para reemplazar el host local por la IP del servidor remoto:

  ```
  *.* @@localhost:10514
  ```

Recopilar archivos de registros

Antes no había ninguna herramienta disponible para recopilar los archivos de registros en la aplicación Citrix Workspace. Los archivos de registros estaban presentes en diferentes carpetas. Había que recopilar manualmente archivos de registros de diferentes carpetas.

A partir de la versión 2109, la aplicación Citrix Workspace presenta la herramienta collectlog.py para recopilar archivos de registros de diferentes carpetas. Puede ejecutar la herramienta mediante la línea de comandos. Los archivos de registros se generan como un archivo de registros comprimido. Puede descargarlo desde el servidor local.

Requisitos previos

- Python3
- Requiere espacio extra para guardar los registros

A partir de la versión 2109, se agregan dos archivos nuevos para recopilar archivos de registros mediante la herramienta collectlog.py:

- Archivo `logcollector.ini`: Guarda el nombre y la ruta del archivo de registros.
- Archivo `collectlog.py`: Recopila los archivos de registros y los guarda como el archivo comprimido `cwalog_{ timestamp } .tar.gz`.

De forma predeterminada, el componente `[hdxteams]` se agrega al archivo `logcollector.ini` para recopilar archivos de registros para Microsoft Teams. Sin embargo, también puede agregar otros componentes al archivo `logcollector.ini` mediante este procedimiento:

1. Vaya al archivo `${ HOME } /.ICAClient/logs/ICAClient.log/logcollector.ini`.
2. Agregue el componente que necesite para recopilar archivos de registros en este ejemplo:

[nombre_componente]

log_name1 = “ruta_de_registros1”

log_name2 = “ruta_de_registros2”

Si tiene la versión 2109, recopile archivos de registros mediante este procedimiento:

1. Descargue e instale la aplicación Citrix Workspace en su máquina Linux.
2. En la línea de comandos, vaya a la ruta `/opt/Citrix/ICAClient/util`.
3. Ejecute este comando:
   `./collctlog.py -h`

   Aparece esta información del uso de comandos:

   ```
   usage: collect_log [-h] [-c CONFIG] [-a ARCHIVE]optional arguments: -h,
    --help show this help message and exit -c CONFIG, --config CONFIG The
   logcollector.ini path & file -a ARCHIVE, --archive ARCHIVE The archive
   path & file
   ```

4. Ejecute estos comandos según sea necesario:
   - `./collectlog.py`: Recopila archivos de registros mediante el archivo de configuración de la ruta predeterminada y los guarda como archivos de registros comprimidos en la ruta predeterminada.
   - `./collectlog.py -c /user_specified_path/logcollector.ini`: Recopila archivos de registros mediante el archivo de configuración de una ruta especificada por el usuario y los guarda como archivos de registros comprimidos en la ruta predeterminada.
   - `./collectlog.py -c /user_specified_path/logcollector.ini -a/another_user_spec /`: Recopila archivos de registros mediante el archivo de configuración de una ruta especificada por el usuario y los guarda como archivos de registros comprimidos en la ruta definida por el usuario.

   > **Nota:**
   >
   > La ruta predeterminada del archivo de configuración `logcollector.ini` es `/opt /Citrix/ICAClient/config/logcollector.ini`. La ruta predeterminada del archivo de registros comprimido es `/tmp`.

5. Vaya a la carpeta `/tmp` y recopile el archivo comprimido `cwalog_{ timestamp } .tar.gz`.

> **Nota:**
>
> Los archivos de registros se guardan en la carpeta `/tmp` con el nombre de archivo `cwalog_{`


```
timestamp } .tar.gz.
```

Optimización para Microsoft Teams

Optimización para Microsoft Teams de escritorio mediante Citrix Virtual Apps and Desktops o Citrix DaaS y la aplicación Citrix Workspace. La optimización para Microsoft Teams es similar a HDX Real-Time Optimization para Microsoft Skype Empresarial. La diferencia es que agrupamos todos los componentes necesarios para la optimización de Microsoft Teams en el VDA y en la aplicación Workspace para Linux.

La aplicación Citrix Workspace para Linux ofrece funciones de audio, vídeo y uso compartido de la pantalla con la optimización de Microsoft Teams.

> **Nota:**
>
> - La optimización de Microsoft Teams solo se ofrece en distribuciones x64 de Linux.
> - La optimización de Microsoft está disponible tanto en Citrix Virtual Apps and Desktops como en Citrix DaaS.
> - Para clientes ligeros que usan Dell Wyse, use el **Citrix Configuration Editor** para modificar parámetros del archivo `/var/.config/citrix/hdx_rtc_engine/config.json`. Para obtener más información, consulte la documentación de Dell.

Para obtener información sobre cómo habilitar los registros, siga los pasos mencionados indicados en Registros en Microsoft Teams.

Para obtener información sobre los requisitos del sistema, consulte Requisitos de la optimización de Microsoft Teams.

Para obtener más información, consulte Optimización para Microsoft Teams y Redirección de Microsoft Teams.

Mejora de la configuración de audio

Si Microsoft Teams configura las opciones de control automático de ganancias y supresión de ruido, la instancia de Microsoft Teams redirigida por Citrix respeta los valores tal y como se han configurado. De lo contrario, estas opciones están habilitadas de forma predeterminada. Sin embargo, a partir de la aplicación Citrix Workspace 2104, la opción de eliminación de eco está inhabilitada de forma predeterminada. A partir de la aplicación Citrix Workspace 2112, los administradores pueden cambiar los parámetros predeterminados para resolver problemas de audio (como voces robóticas, una CPU elevada que entrecorta el audio, etc.) de esta manera:

1. Vaya al archivo /var/.config/citrix/hdx_rtc_engine/config.json.
2. Configure estas opciones:
    - Valor de `EnableAEC` en 1 para habilitar la eliminación de eco y 0 para inhabilitarla

- Valor de EnableAGC en 1 para habilitar el control automático de ganancias y 0 para inhabilitarlo
- Valor de EnableNS en 1 para habilitar la supresión de ruido y 0 para inhabilitarla

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


      "EnableAEC":1,"EnableAGC":1,"EnableNS":1

 }

<!--NeedCopy-->
```

Una vez establecida la llamada, supervise el registro de webrpc, (/tmp/webrpc/<current date >/), en busca de estas entradas para verificar que los cambios surtieron efecto:

```
/tmp/webrpc/Wed_Feb__2_14_56_33_2022/webrpc.log:[040.025] Feb 02
   14:57:13.220 webrtcapi.NavigatorUserMedia Info: getUserMedia. audio
   constraints, aec=1, agc=1, ns=1
<!--NeedCopy-->
```

Estimador de rendimiento del codificador para Microsoft Teams

HdxRtcEngine es el motor de medios WebRTC integrado en la aplicación Citrix Workspace que gestiona la redirección de Microsoft Teams. HdxRtcEngine.exe puede estimar la mejor resolución de vídeo saliente (codificación) que la CPU del dispositivo de punto final puede mantener sin sobrecargarse. Los valores posibles son: 240p, 360p, 720p y 1080p.

El proceso de estimación de rendimiento utiliza código de macrobloque para determinar la mejor resolución que se puede lograr en ese dispositivo de punto final concreto. La negociación del códec durante la configuración de llamadas incluye la resolución más alta posible. La negociación del códec puede ser entre los pares o entre el par y el servidor de conferencias.

En esta tabla se muestran cuatro categorías de rendimiento para los dispositivos de punto final que tienen su propia resolución **máxima** disponible:

Rendimiento del dispositivo de punto final	Resolución máxima	Valor de clave del Registro
Rápido	1080p (1920x1080 16:9 @ 30 fps)	3
Medio	720p (1280x720 16:9 @ 30 fps)	2
Lento	360p (640x360 16:9 @ 30 fps o 640x480 4:3 @ 30 fps)	1
Muy lento	240p (320x180 16:9 @ 30 fps o 320x240 4:3 @ 30 fps)	0

Para establecer el valor de resolución de la codificación de los vídeos salientes (por ejemplo, en 360p), ejecute este comando en el terminal:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine

vim /var/.config/citrix/hdx_rtc_engine/config.json

{


    "OverridePerformance":1

 }

<!--NeedCopy-->
```

Registros en Microsoft Teams

Para habilitar los registros en Microsoft Teams:

1. Vaya al archivo `/opt/Citrix/ICAClient/debug.ini`.
2. Modifique la sección `[HDXTeams]` de la siguiente manera:

```
[HDXTeams]
; Retail logging for HDXTeams 0/1 = disabled/enabled
HDXTeamsLogSwitch = 1
; Debug logging; , It is in decreasing order
; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,
   LS_VERBOSE = 0
WebrtcLogLevel = 0
; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0
```



```
WebrpcLogLevel = 0

<!--NeedCopy-->
```

Los registros también se pueden habilitar al agregar esta línea al archivo config.json:

```
{

"WebrpcLogLevel": 0,"WebrtcLogLevel": 0
 }

<!--NeedCopy-->
```

Incorporar la dependencia de “libunwind-12 library” para llvm-12

A partir de la versión 2111, se agrega una dependencia nueva llamada “libunwind-12 library” para llvm-12. Sin embargo, de forma predeterminada, no existe en el repositorio original. Para instalar la biblioteca libunwind-12 manualmente en el repositorio, siga estos pasos:

1. Abra el terminal.
2. Introduzca esta línea para instalar el archivo de claves del repositorio `llvm`:

```
 wget -O - https://apt.llvm.org/llvm-snapshot.gpg.key|sudo apt-key
     add
<!--NeedCopy-->
```

3. Introduzca esta línea para configurar la lista de orígenes del repositorio `llvm`:

```
 sudo vim /etc/apt/sources.list
<!--NeedCopy-->
```

4. Agregue esta línea:

```
deb http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
deb-src http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
<!--NeedCopy-->
```

5. Ejecute este comando para instalar la biblioteca libunwind-12:

```
sudo apt-get update -y
sudo apt-get install libunwind-12
<!--NeedCopy-->
```


Limitar resoluciones de vídeo [Technical Preview]

Los administradores que tienen usuarios en dispositivos de punto final clientes de bajo rendimiento pueden optar por limitar las resoluciones de vídeos entrantes o salientes para reducir el impacto de la codificación y la decodificación de vídeo en dichos dispositivos. A partir de la aplicación Citrix Workspace 2303 para Linux, puede limitar estas resoluciones mediante las opciones de configuración del cliente.

> **Nota:**
>
> Los usuarios con resoluciones restringidas afectan a la calidad general del vídeo de las conferencias, ya que el servidor de Microsoft Teams se verá obligado a utilizar la resolución con el mínimo común denominador para todos los participantes de la conferencia.

Las restricciones de llamadas están inhabilitadas de forma predeterminada en el cliente con la aplicación Citrix Workspace 2303. Para habilitarlas, los administradores deben definir estas configuraciones del lado del cliente en el archivo `/var/.config/citrix/hdx_rtc_engine/config.json`:

```
{


        "EnableSimulcast": 1,

        "MaxOutgoingResolution" : 720,

        "MaxIncomingResolution" : 720,

        "MaxIncomingStreams" : 4,

        "MaxSimulcastLayers" : 2
<!--NeedCopy-->
```

Puede enviar sus comentarios sobre esta Technical Preview a través del formulario de Podio.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Configurar una interfaz de red preferida

Ahora, a partir de la versión 2303 de la aplicación Citrix Workspace, puede configurar una interfaz de red preferida para el tráfico de contenido multimedia. Con esta mejora, si tiene varias conexiones de red y el rendimiento de la predeterminada no es bueno, puede cambiar a otra red. Para habilitar esto, habilite esta mejora:

1. Vaya al archivo `/var/.config/citrix/hdx_rtc_engine/config.json`.
2. Vaya a esta sección:

```
1         mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3          vim /var/.config/citrix/hdx_rtc_engine/config.json
4
5         {
6
7
8              ” NetworkPreference” :1
9
10           }
11
12 <!--NeedCopy-->
```

3. Actualice el valor de “NetworkPreference:” con uno de estos valores según sea necesario:
   - 1: Ethernet
   - 2: Wi-Fi
   - 3: Móvil
   - 4: Vpn
   - 5: Bucle invertido
   - 6: Cualquiera

De forma predeterminada y si no se establece ningún valor, el motor de medios WebRTC elige la mejor ruta disponible.

Mejoras en la optimización de Microsoft Teams

- A partir de la versión 2101 de la aplicación Citrix Workspace:
  - El instalador de la aplicación Citrix Workspace incluye tonos de llamada de Microsoft Teams.
  - La salida de audio cambia automáticamente a los dispositivos de audio recién conectados y se establece un volumen de audio adecuado.
  - El proxy HTTP está disponible para la autenticación anónima.

- A partir de la versión 2103 de la aplicación Citrix Workspace, el códec de vídeo VP9 está inhabilitado de forma predeterminada.
- A partir de la versión 2104 de la aplicación Citrix Workspace, la función de eliminación de eco está inhabilitada de forma predeterminada. Le recomendamos no usar los altavoces y el micrófono integrados para las llamadas. Utilice unos auriculares en su lugar. Esta corrección tiene como objetivo resolver problemas de audio entrecortado detectados en clientes ligeros.
- A partir de la versión 2106 de la aplicación Citrix Workspace:
  - Antes, al hacer clic en **Compartir pantalla**, la vista previa de un monitor principal o predeterminado solo estaba disponible para el uso compartido de la pantalla.

    Con esta versión, se muestra una vista previa de todas las pantallas en el menú del selector de pantallas. Puede seleccionar una pantalla para compartirla en el entorno de VDA. Aparece un cuadrado rojo en el monitor seleccionado y una pequeña imagen del contenido de la pantalla seleccionada en el menú del selector de pantallas.

    En el modo integrado, puede seleccionar una de todas las pantallas para compartirla. Cuando Desktop Viewer cambia el modo de ventana (maximizada, restaurada o minimizada), la pantalla compartida se detiene.
- A partir de la versión 2112 de la aplicación Citrix Workspace:

  > **Nota:**
  >
  > Estas funciones están disponibles solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

  - **Solicitar control en Microsoft Teams**

    En esta versión, durante una llamada de Microsoft Teams, puede solicitar el control cuando un participante comparte la pantalla. Una vez que tenga el control, puede realizar selecciones, modificaciones u otras acciones en la pantalla compartida.

    Para tomar el control cuando se comparte una pantalla, haga clic en **Solicitar control** en la parte superior de la pantalla de Microsoft Teams. El participante de la reunión que comparte la pantalla puede aceptar o rechazar su solicitud.

    Mientras tenga el control, puede realizar selecciones, modificaciones y otras acciones en la pantalla compartida. Cuando haya terminado, haga clic en **Liberar control**.

    Limitaciones:

    * Los usuarios de un cliente Linux no pueden *dar* el control a otros usuarios. En otras palabras, después de que el usuario del cliente Linux comience a compartir

contenido, la opción **Dar control** no aparece en la barra de herramientas de uso compartido. Se trata de una limitación de Microsoft.

* La opción **Solicitar el control** no está disponible durante llamadas entre un usuario optimizado y un usuario en el cliente de escritorio de Microsoft Teams nativo en el dispositivo de punto final. Como solución temporal, los usuarios pueden unirse a una reunión para obtener la opción **Solicitar el control**.

– **Compatibilidad con e911 dinámico**

Con esta versión, la aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, proporciona la capacidad de:

* configurar y redirigir llamadas de emergencia
* notificar al personal de seguridad

La notificación se proporciona en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams que se ejecuta en el VDA.
La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. A partir de la aplicación Citrix Workspace 2112 para Linux, la optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum. Para que esta función esté disponible, la biblioteca LLDP debe incluirse en la distribución del sistema operativo del cliente ligero.

- A partir de la versión 2203 de la aplicación Citrix Workspace:

Chat y reuniones multiventana para Microsoft Teams

Con esta versión, puede usar varias ventanas para reuniones y chats en Microsoft Teams con la optimización de HDX en Citrix Virtual Apps and Desktops 2112 o una versión posterior. Puede separar las conversaciones o las reuniones de varias maneras. Para obtener detalles sobre la función de ventana emergente, consulte Microsoft Teams Pop-Out Windows for Chats and Meetings.

Si utiliza una versión anterior de la aplicación Citrix Workspace o Virtual Delivery Agent (VDA), recuerde que Microsoft retirará el código de las ventanas únicas en el futuro. Sin embargo, tendrá un mínimo de nueve meses después de que esta función esté generalmente disponible para actualizar VDA o la aplicación Citrix Workspace a una versión que admita varias ventanas (2203 o una versión posterior).

> **Nota:**
>
> Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, consulte

> CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

- A partir de la versión 2207 de la aplicación Citrix Workspace:

  Compatibilidad con timbre secundario:

  Puede utilizar la función de timbre secundario para seleccionar un dispositivo secundario en el que recibir la notificación de llamada entrante cuando Microsoft Teams está optimizado (Citrix HDX optimizado en Acerca de/Versión). Por ejemplo, considere que ha establecido un altavoz como timbre secundario y que su dispositivo de punto final está conectado a unos auriculares. En este caso, Microsoft Teams envía la señal de llamada entrante al altavoz aunque los auriculares sean el periférico principal para la llamada de audio. No se puede establecer un timbre secundario en los siguientes casos:

  - Cuando no se ha conectado a más de un dispositivo de audio
  - Si el periférico no está disponible (por ejemplo, auriculares Bluetooth)

  > **Nota:**
  >
  > Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Para saber cuándo implementa Microsoft la actualización, consulte el Plan de desarrollo de Microsoft 365. También puede consultar CTX253754 para obtener la actualización de la documentación y el anuncio.

- A partir de la versión 2207 de la aplicación Citrix Workspace:

  - **Uso compartido de aplicaciones habilitado:** A partir de la aplicación Citrix Workspace 2209 para Linux y Citrix Virtual Apps and Desktops 2109, puede compartir una aplicación mediante la función de compartir pantalla de Microsoft Teams.
  - **Mejoras en la compatibilidad con un nivel elevado de PPP:** Cuando la función de PPP elevado está habilitada y usa monitores 4K, las superposiciones de vídeo de Microsoft Teams están en la posición adecuada y tienen el tamaño correcto. Independientemente de los parámetros de la pantalla, como la disposición de uno o varios monitores, las superposiciones siempre aparecen correctamente y no se amplían ni aparecen en posiciones no deseadas. Para habilitar esta mejora, asegúrese de que el parámetro `DPIMatchingEnabled` del archivo de configuración `wfclient.ini` esté establecido en **True**. Para obtener más información, consulte Compatibilidad con la correspondencia de PPP.
  - **Actualización de la versión del SDK de WebRTC:** La versión de WebRTC que se utiliza para Microsoft Teams optimizado se actualizó a la versión M98.

- A partir de la versión 2212 de la aplicación Citrix Workspace:

  - **Compatibilidad con desenfoque y reemplazo de fondo para Teams optimizado por Citrix [Technical Preview]**

    Requisito previo:

Asegúrese de haber instalado wget.

Teams optimizado por Citrix en la aplicación Citrix Workspace para Linux ahora admite el desenfoque y el reemplazo de fondo. Para usar esta función, seleccione **More** > **Apply Background Effects** cuando esté en una reunión o en una llamada punto a punto (P2P).

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Canal virtual NetScaler App Experience (NSAP) disponible

Anteriormente disponible como una función experimental, la función de canal virtual NSAP está totalmente disponible a partir de la versión 2006. Todos los datos de HDX Insight se obtienen exclusivamente del canal virtual NSAP y se envían sin comprimir. Esta manera mejora la escalabilidad y el rendimiento de las sesiones. De forma predeterminada, el canal virtual NSAP está habilitado. Para inhabilitarlo, cambie el indicador VDNSAP `NSAP=Off` en el archivo module.ini.

Para obtener más información, consulte HDX Insight en la documentación de Linux Virtual Delivery Agent y HDX Insight en la documentación del servicio Citrix Application Delivery Management.

Persistencia del diseño en varios monitores

Esta función conserva la información sobre el diseño en el monitor de la sesión en los dispositivos de punto final. La sesión aparece en los mismos monitores configurados.

Requisito previo:

Esta función requiere lo siguiente:

- StoreFront 3.15 o una versión posterior.
- Si `.ICAClient` ya está presente en la carpeta de inicio del usuario actual:

  Elimine el archivo All_Regions.ini

  O bien

  Para conservar el archivo `All_Regions.ini`, agregue estas líneas al final de la sección [Client Engine\Application Launching]:

SubscriptionUrl=

PreferredWindowsBounds=

PreferredMonitors=

PreferredWindowState=

SaveMultiMonitorPref=

Si la carpeta `.ICAClient` no está presente, entonces es que indica una nueva instalación de la aplicación Citrix Workspace. En ese caso, se conserva la configuración predeterminada para la función.

Casos de uso

- Inicie una sesión en cualquier monitor en modo ventana y guarde la configuración. Cuando reinicie la sesión, aparecerá en el mismo modo, en el mismo monitor y en la misma posición.
- Inicie una sesión en cualquier monitor en modo de pantalla completa y guarde la configuración. Cuando reinicie la sesión, aparecerá en modo de pantalla completa en el mismo monitor.
- Estire y amplíe una sesión en modo ventana a varios monitores y luego cambie al modo de pantalla completa. La sesión continúa en pantalla completa en todos los monitores. Cuando reinicie la sesión, aparecerá en modo de pantalla completa, ampliada a todos los monitores.

> **Notas:**
>
> - El diseño de los elementos se sobrescribe con cada operación de guardado. Además, el diseño se guarda solo en el StoreFront activo.
> - Si inicia sesiones de escritorio adicionales desde el mismo StoreFront en diferentes monitores, guardar el diseño en una sesión guarda la información de diseño de todas las sesiones.

Guardar diseño

Para habilitar la función de guardar diseño:

1. Instale StoreFront 3.15 o una versión posterior (igual o posterior a 3.15.0.12) en un Delivery Controller (DDC) compatible.
2. Descargue la compilación de la aplicación Citrix Workspace para Linux 1808 o versiones posteriores desde la página Descargas y luego instálela en su máquina Linux.
3. Establezca la variable de entorno ICAROOT en la ubicación de instalación.
4. Compruebe si el archivo **All_Regions.ini** está presente en la carpeta **.ICAClient**. Si es así, elimínelo.

5. En el archivo **$ICAROOT/config/All_Regions.ini**, busque el campo – **SaveMultiMonitorPref**. De forma predeterminada, el valor de este campo es “true” (lo que significa que esta función está activada). Para desactivar esta función, establezca este campo en “false”.
   Si actualiza el valor **SaveMultiMonitorPref**, debe eliminar el archivo **All_Regions.ini** presente en la carpeta **.ICAClient** para evitar discrepancias de valores y un posible bloqueo de perfil. Establezca o desactive la marca **SaveMultiMonitorPref** antes de iniciar sesiones
6. Lance una nueva sesión de escritorio.
7. Haga clic en **Guardar diseño** en la barra de herramientas de Desktop Viewer para guardar el diseño de la sesión actual. Aparece una notificación en la parte inferior derecha de la pantalla, que indica que la operación se ha realizado correctamente.
   Cuando hace clic en Guardar diseño, el icono pasa a ser gris. Este cambio de color indica que la operación de guardado está en curso. Tras guardarse el diseño, el icono aparece como siempre.
8. Desconecte la sesión o ciérrela.
   Vuelva a iniciar la sesión. La sesión aparece en el mismo modo, en el mismo monitor y en la misma posición.

Limitaciones y casos no admitidos:

- No se admite el guardado de un diseño de sesión en modo ventana que abarca varios monitores, debido a limitaciones con el administrador de pantalla de Linux.
- En esta versión, no se admite el guardado de información de sesión en monitores con resolución variada, y guardarla podría dar lugar a un comportamiento impredecible.
- Implementaciones de clientes con almacenes adicionales de StoreFront

Uso de Citrix Virtual Desktops en monitores dobles

1. Seleccione Desktop Viewer y haga clic en la flecha hacia abajo.
2. Seleccione la opción **Ventana**.
3. Arrastre la pantalla Citrix Virtual Desktops entre los dos monitores. Verifique que aproximadamente la mitad de la pantalla esté presente en cada monitor.
4. En la barra de herramientas de Citrix Virtual Desktops, seleccione **Pantalla completa**.

   La pantalla se extiende ahora a ambos monitores.

Workspace Launcher

Citrix presenta Workspace Launcher (WebHelper) para iniciar aplicaciones y escritorios publicados.

Anteriormente, el plug-in del explorador provisto junto con la aplicación Citrix Workspace para Linux que permitía a los usuarios iniciar aplicaciones y escritorios publicados se basaba en NPAPI.

Como solución, Citrix presenta Workspace Launcher (WebHelper). Para habilitar esta función, configure StoreFront para enviar solicitudes a Workspace Launcher para detectar la instalación de la aplicación Citrix Workspace.

A partir de la versión 1901, Citrix Workspace Launcher es compatible con conexiones directas a StoreFront y Citrix Gateway. Esta función ayuda a iniciar el archivo ICA automáticamente y a detectar la instalación de la aplicación Citrix Workspace.

Para obtener más información sobre cómo configurar StoreFront, consulte **Solución - 2** > **a) Configuración de administrador** en el artículo del Knowledge Center CTX237727.

> **Nota:**
>
> Citrix Workspace Launcher actualmente funciona solo con conexiones directas a StoreFront. No se admite en otros casos, como en las conexiones a través de Citrix Gateway.

Inhabilitar el nuevo modo de interfaz de usuario web del espacio de trabajo

Cuando inicia la aplicación Citrix Workspace para Linux mediante un archivo ejecutable de autoservicio proveniente de proveedores de terceros de clientes ligeros, la aplicación puede dejar de responder debido al 100% de utilización de CPU.

Como solución temporal, para volver al antiguo modo de interfaz de usuario, puede hacer lo siguiente:

1. Elimine los archivos en caché con el comando:
   `rm -r ~/.ICAClient`
2. Vaya al archivo `$ICAROOT/config/AuthManconfig.xml`.
3. Cambie el valor de la clave `CWACapableEnabled` a “false”.
4. Inicie la aplicación Citrix Workspace para Linux. Podrá comprobar que el archivo ejecutable de autoservicio carga la IU anterior.

Sincronización de la distribución de teclado

La sincronización de la distribución del teclado le permite cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada. Después de habilitar esta función, la distribución del teclado del cliente se sincroniza automáticamente con las aplicaciones y escritorios virtuales.

A partir de la versión 2203, la aplicación Citrix Workspace ofrece estos tres modos de sincronización de la distribución del teclado:

- **Sincronizar solo una vez, cuando se inicia la sesión**: Según el valor de `KeyboardLayout` en el archivo wfclient.ini, la distribución del teclado del cliente se sincroniza con la del servidor cuando se inicia la sesión. Si el valor de `KeyboardLayout` es `0`, el teclado del sistema se sincroniza con el VDA. Si el valor de `KeyboardLayout` se establece en un idioma específico, el

teclado del idioma se sincroniza con el VDA. Los cambios que haga en la distribución del teclado del cliente durante la sesión no surtirán efecto inmediatamente. Para aplicar los cambios, cierre la sesión de la aplicación e inicie sesión de nuevo. El modo **Sincronizar solo una vez: al iniciarse la sesión** es la distribución de teclado predeterminada seleccionada para la aplicación Citrix Workspace.

- **Permitir sincronización dinámica**: Esta opción sincroniza la distribución del teclado del cliente con el servidor al cambiar la distribución del teclado del cliente.
- **No sincronizar**: Indica que el cliente utiliza la distribución del teclado presente en el servidor.

Requisito previo:

- Habilite la función de asignación de distribución de teclado Unicode en el Windows VDA. Para obtener más información, consulte el artículo CTX226335 de Knowledge Center.
- Habilite la función Sincronización de la distribución de teclado dinámico en Linux VDA. Para obtener más información, consulte Sincronización de la distribución del teclado dinámico
- La sincronización de la distribución del teclado depende de la biblioteca XKB.
- Al utilizar Windows Server 2016 o Windows Server 2019, vaya a la ruta `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme` del Registro, agregue un valor DWORD con nombre de clave `DisableKeyboardSync` y establezca su valor en `0`.
- Si `.ICAClient` ya está presente en la carpeta de inicio del usuario actual:

  Elimine el archivo All_Regions.ini

  O bien

  Para conservar el archivo `All_Regions.ini`, agregue estas líneas al final de la sección [Virtual Channels\Keyboard]:

  KeyboardSyncMode=

  KeyboardEventMode=

Configurar la distribución del teclado

La aplicación Citrix Workspace proporciona parámetros de configuración y de interfaz de usuario para habilitar tres modos distintos de sincronización de la distribución del teclado.

Para configurar la sincronización de la distribución del teclado mediante la interfaz gráfica de usuario:

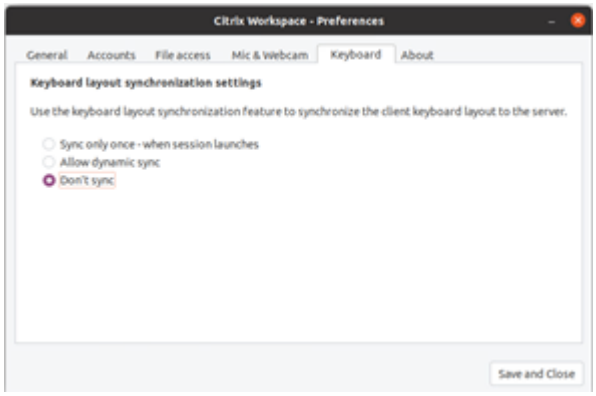
1. En el icono de la aplicación Citrix Workspace, en el área de notificaciones, seleccione **Preferencias**.

   O bien:

Abra el terminal, vaya a la ruta de instalación y ejecute este comando:

```
util/configmgr
```

Aparecerá el cuadro de diálogo **Citrix Workspace - Preferencias**.



2. Haga clic en la ficha **Teclado**.

   Aparecerá la página **Parámetros de sincronización de distribución del teclado**.

3. Seleccione una de estas opciones:

   - **Sincronizar solo una vez: cuando se inicia la sesión**: Indica que la distribución del teclado se sincroniza con el VDA solo una vez al iniciarse la sesión. El modo de entrada de texto del teclado Unicode es la opción recomendada para el modo **Sincronizar solo una vez: al iniciarse la sesión**.
   - **Permitir sincronización dinámica**: Indica que la distribución del teclado se sincroniza de manera dinámica con el VDA al cambiar el teclado del cliente en una sesión. El modo de entrada de texto del teclado Unicode es la opción recomendada para el modo **Permitir sincronización dinámica**.
   - **No sincronizar**: Indica que el cliente usa la distribución de teclado presente en el servidor, independientemente de la distribución de teclado que haya seleccionada en el cliente. El modo de entrada de texto del teclado Scancode es la opción recomendada para el modo **No sincronizar**. Debe asegurarse de que la distribución del teclado del cliente sea la misma que la distribución del teclado del VDA si selecciona Unicode para la opción **No sincronizar**.

4. Haga clic en **Guardar y Cerrar**.

Para configurar la sincronización de la distribución del teclado mediante los parámetros del archivo de configuración:

Modifique el archivo de configuración `wfclient.ini` para habilitar la distribución de teclado necesaria.

Sincronizar solo una vez: al iniciarse la sesión:

Con esta función habilitada, al iniciar una sesión, la distribución de teclado activa en el dispositivo cliente se sincroniza con la del VDA. Según el valor de `KeyboardLayout` del archivo `wfclient.ini`, la distribución del teclado del cliente se sincroniza con la del servidor cuando se inicia la sesión. Si el valor de `KeyboardLayout` es `0`, el teclado del sistema se sincroniza con el VDA. Si el valor de `KeyboardLayout` se establece en un idioma específico, el teclado del idioma se sincroniza con el VDA.

Para seleccionar este modo, haga lo siguiente:

1. Vaya al archivo de configuración `$HOME/.ICAClient/wfclient.ini`.
2. Agregue estas entradas:

```
KeyboardSyncMode=Once
KeyboardEventMode=Unicode/Scancode
<!--NeedCopy-->
```

El modo de entrada de texto del teclado Unicode es la opción recomendada para el modo **Sincronizar solo una vez: al iniciarse la sesión**.

Permitir sincronización dinámica:

Con esta función habilitada, cuando la distribución del teclado cambia en el dispositivo cliente durante una sesión, también cambia la distribución del teclado de la sesión.

Para seleccionar este modo, haga lo siguiente:

1. Vaya al archivo de configuración `$HOME/.ICAClient/wfclient.ini`.
2. Agregue estas entradas:

```
KeyboardSyncMode=Dynamic
KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
<!--NeedCopy-->
```

El modo de entrada de texto del teclado Unicode es la opción recomendada para el modo **Permitir sincronización dinámica**.

No sincronizar:

Con esta función habilitada, se utiliza la distribución del teclado del VDA, independientemente de la distribución del teclado que se seleccione en el dispositivo cliente.

Para seleccionar este modo, haga lo siguiente:

1. Vaya al archivo de configuración `$HOME/.ICAClient/wfclient.ini`.
2. Agregue estas entradas:

```
KeyboardSyncMode=No
```



```
KeyboardEventMode= Scancode (or KeyboardEventMode= Unicode)
<!--NeedCopy-->
```

El modo de entrada de texto del teclado Scancode es la opción recomendada para el modo **No sincronizar**. Debe asegurarse de que la distribución del teclado del cliente sea la misma que la distribución del teclado del VDA si configura Unicode para la opción **No sincronizar**.

> **Nota:**
>
> Cuando configurar `KeyboardSyncMode=""` (vacío) en el archivo `wfclient.ini`, el modo vuelve al comportamiento anterior. En el comportamiento anterior, la distribución del teclado se lee desde el archivo `$HOME/.ICAClient/wfclient.ini` y se envía al VDA junto con otra información del cliente cuando se inicia la sesión.

Modo de entrada de texto del teclado

Citrix recomienda este modo de entrada de texto del teclado para las diferentes opciones de sincronización de la distribución del teclado:

- Modo Scancode para la opción **No sincronizar**.
- Modo Unicode para **Permitir sincronización dinámica** y **Sincronizar solo una vez: al iniciarse la sesión**.

Puede cambiar la configuración de `KeyboardEventMode` en el archivo `wfclient.ini`. Sin embargo, para obtener un rendimiento óptimo, utilice los modos recomendados por Citrix para diferentes casos, teclados físicos y dispositivos cliente.

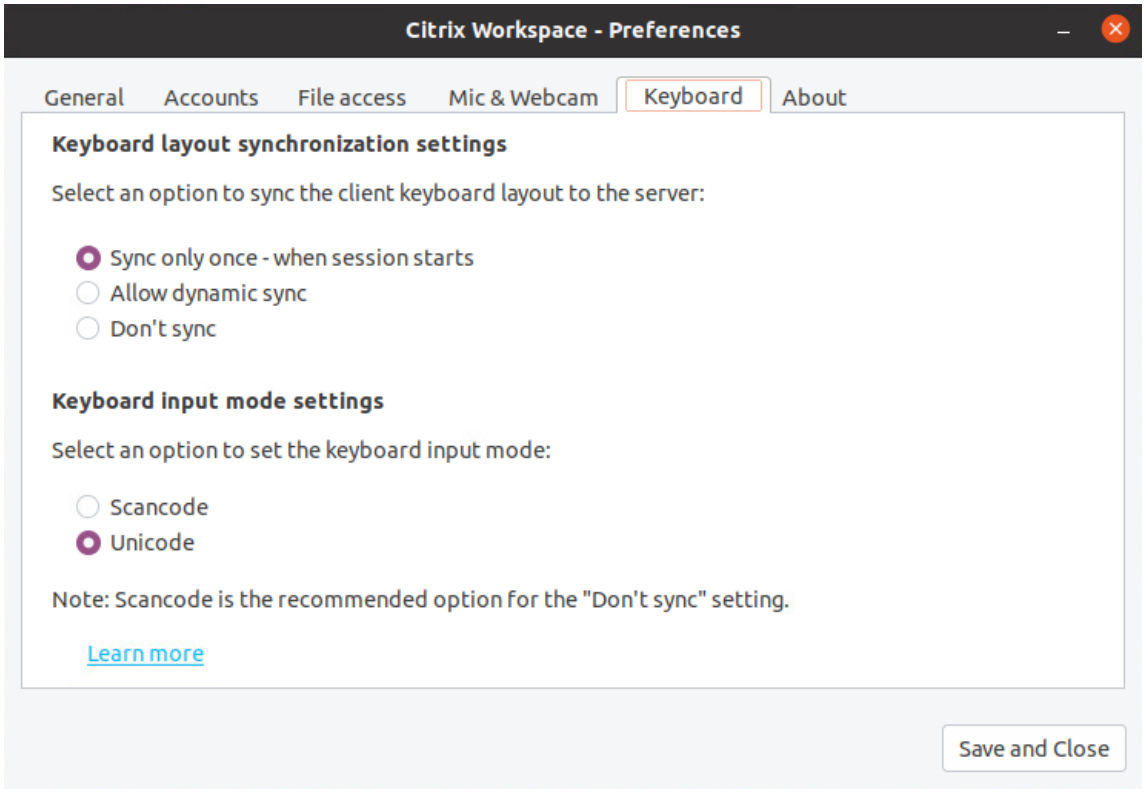
Mejoras en el modo de entrada del teclado [Technical Preview]

Antes solo podía habilitar diferentes modos de entrada del teclado al actualizar el valor de `KeyboardEventMode` en el archivo de configuración. No había ninguna opción de interfaz de usuario para seleccionar el modo de entrada del teclado.

A partir de la aplicación Citrix Workspace 2209, puede configurar diferentes modos de entrada del teclado desde la sección **Parámetros del modo de entrada de teclado** recientemente incorporada. Puede seleccionar **Scancode** o **Unicode** como modo de entrada del teclado.

Para configurar el modo de entrada del teclado mediante la GUI, haga lo siguiente:

1. En el icono de la aplicación Citrix Workspace, en el área de notificaciones, seleccione **Preferencias**.
   Aparecerá el cuadro de diálogo **Citrix Workspace - Preferencias**.
2. Haga clic en Teclado.
   Puede ver la sección **Parámetros del modo de entrada del teclado** recién agregada.



3. Seleccione una de estas opciones:

   - **Scancode**: Envía la posición de la tecla del teclado del lado del cliente al VDA, y el VDA genera el carácter correspondiente. Aplica la distribución del teclado del lado del servidor.
   - **Unicode**: Envía la tecla del teclado del lado del cliente al VDA, y el VDA genera el mismo carácter en el VDA. Aplica la distribución del teclado del lado del cliente.

   De forma predeterminada, los parámetros del modo de entrada del teclado están seleccionados como **Unicode**. Para obtener más información sobre el modo de entrada del teclado, consulte la sección **Configurar la distribución del teclado** de la documentación sobre la Sincronización de la distribución del teclado.

4. Haga clic en **Guardar y Cerrar**.

> **Nota:**
>
> Los cambios en la configuración del teclado surtirán efecto una vez que se haya conectado de nuevo a la aplicación. Si cambia el modo de entrada del teclado en la interfaz de usuario, el valor del parámetro `KeyboardEventMode` en el archivo `wfclient.ini` también se actualiza automáticamente.

Por ejemplo, considere una situación en la que utiliza una distribución de teclado internacional de EE. UU. y el VDA utiliza la distribución de teclado rusa.

Al seleccionar **Scancode** y presionar la tecla junto al bloqueo de mayúsculas, el scancode `1E` se envía al VDA. A continuación, el VDA usa `1E` para mostrar el carácter ф.

Si elige Unicode y presiona la tecla junto al bloqueo de mayúsculas, se envía el carácter a al VDA. Por lo tanto, aunque el VDA use la distribución del teclado ruso, el carácter a aparece en la pantalla.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Compatibilidad con distribuciones de teclado extendido [Technical Preview]

A partir de la versión 2209 de la aplicación Citrix Workspace, el modo de entrada de teclado Scancode admite estas distribuciones de teclado extendido:

- Teclado 106 japonés
- Teclados ABNT/ABNT2 portugueses
- Teclados multimedia

El modo de entrada de teclado Scancode admite las distribuciones de teclado extendidas junto con todos los modos de sincronización de distribución del teclado.

Esta funcionalidad está habilitada de forma predeterminada.

> **Nota:**
>
> Las Technical Previews están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción, y para darles la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

Distribución del teclado con Windows VDA y Linux VDA

Descripción del teclado del cliente Linux	Distribución del teclado del cliente Linux	Variante de teclado de cliente Linux	Se sincroniza con	ID de la configuración regional de Windows	Distribución del teclado de Windows VDA (ID)	Distribución del teclado de Linux VDA	Variante de teclado de Linux VDA
Árabe	ara	-	→	ar-SA	00000401	ara	-
Árabe (AZERTY)	ara	azerty	→	ar-DZ	00020401	ara	azerty
Alemán (Austria)	at	-	→	de-AT	00000407	at	-
Belga (ISO alt.)	be	iso-alternate	→	fr-BE	0000080c	be	iso-alternate
Belga	be	-	→	nl-BE	00000813	be	-
Búlgaro	bg	-	→	bg-BG	00030402	bg	-
Búlgaro (fonética tradicional)	bg	fonética	→	bg-BG	00040402	bg	fonética
Búlgaro (fonética moderna)	bg	bas_phonetic	→	bg-BG	00020402	bg	bas_phonetic
Portugués (Brasil)	br	-	→	pt-BR	00000416	br	-
Bielorruso	by	-	→	be-BY	00000423	by	-
Inglés (Canadá)	ca	eng	→	en-CA	00000409	ca	eng
Canadiense multilingüe	ca	multix	→	fr-CA	00011009	ca	multix
Francés (Canadá, antiguo)	ca	fr-legacy	→	fr-CA	00000c0c	ca	fr-legacy
Francés (Canadá)	ca	-	→	fr-CA	00001009	ca	-

Descripción del teclado del cliente Linux	Distribución del teclado del cliente Linux	Variante de teclado de cliente Linux	Se sincroniza con	ID de la configuración regional de Windows	Distribución del teclado de Windows VDA (ID)	Distribución del teclado de Linux VDA	Variante de teclado de Linux VDA
Francés (Suiza)	ch	fr	→	fr-CH	0000100c	ch	fr
Alemán (Suiza)	ch	-	→	de-CH	00000807	ch	-
Chino simplificado	cn	-	→	en-US	00000409	us	-
Checo	cz	-	→	cs-CZ	00000405	cz	-
Checo (QWERTY)	cz	qwerty	→	cs-CZ	00010405	cz	qwerty
Alemán	de	-	→	de-DE	00000407	de	-
Alemán (Macintosh)	de	mac	→	de-DE	00000407	de	mac
Danés	dk	-	→	da-DK	00000406	dk	-
Estonio	ee	-	→	et-EE	00000425	ee	-
Español (América Latina)	es	-	→	es-ES	0000040a	es	-
Español (Macintosh)	es	mac	→	es-ES	0000040a	es	mac
Finlandés	fi	-	→	fi-FI	0000040b	fi	-
Francés	fr	-	→	fr-FR	0000040c	fr	-
Francés (Macintosh)	fr	mac	→	fr-FR	0000040c	fr	mac

Descripción del teclado del cliente Linux	Distribución del teclado del cliente Linux	Variante de teclado de cliente Linux	Se sincroniza con	ID de la configuración regional de Windows	Distribución del teclado de Windows VDA (ID)	Distribución del teclado de Linux VDA	Variante de teclado de Linux VDA
Inglés (Reino Unido)	gb	-	→	en-GB	00000809	gb	-
Inglés (Macintosh)	gb	mac	→	en-GB	00000809	gb	mac
Inglés (Reino Unido, extendido, con teclas Win)	gb	extd	→	en-GB	00000452	gb	extd
Griego	gr	-	→	el-GR	00000408	gr	-
Croata	hr	-	→	hr-HR	0000041a	hr	-
Húngaro	hu	-	→	hu-HU	0000040e	hu	-
Irlandés	ie	-	→	en-IE	00001809	ie	-
Hebreo	il	-	→	he-IL	0002040d	il	-
Inglés (India, con rupia)	in	eng	→	en-IN	00004009	in	eng
Iraquí	iq	-	→	ar-IQ	00000401	iq	-
Islandés	is	-	→	is-IS	0000040f	is	-
Italiano	it	-	→	it-IT	00000410	it	-
Japonés	jp	-	→	en-US	00000409	us	-
Japonés (Macintosh)	jp	mac	→	en-US	00000409	us	mac
Coreano	kr	-	→	en-US	00000409	us	-

Descripción del teclado del cliente Linux	Distribución del teclado del cliente Linux	Variante de teclado de cliente Linux	Se sincroniza con	ID de la configuración regional de Windows	Distribución del teclado de Windows VDA (ID)	Distribución del teclado de Linux VDA	Variante de teclado de Linux VDA
Español (América Latina)	latam	-	→	es-MX	0000080a	latam	-
Lituano	lt	-	→	lt-LT	00010427	lt	-
Lituano (IBM LST 1205-92)	lt	ibm	→	lt-LT	00000427	lt	ibm
Lituano (estándar)	lt	std	→	lt-LT	00020427	lt	std
Letón	lv	-	→	lv-LV	00020426	lv	-
Noruego	no	-	→	nb-NO	00000414	no	-
Polaco	pl	-	→	pl-PL	00000415	pl	-
Polaco (QWERTZ)	pl	qwertz	→	pl-PL	00010415	pl	qwertz
Portugués	pt	-	→	pt-PT	00000816	pt	-
Portugués (Macintosh)	pt	mac	→	pt-PT	00000816	pt	mac
Rumano (estándar)	ro	std	→	ro-RO	00010418	ro	std
Serbio	rs	-	→	sr-Cyrl-RS	00000c1a	rs	-
Serbio (latino)	rs	latin	→	sr-Latn-RS	0000081a	rs	latin
Ruso	ru	-	→	ru-RU	00000419	ru	-

Descripción del teclado del cliente Linux	Distribución del teclado del cliente Linux	Variante de teclado de cliente Linux	Se sincroniza con	ID de la configuración regional de Windows	Distribución del teclado de Windows VDA (ID)	Distribución del teclado de Linux VDA	Variante de teclado de Linux VDA
Ruso (máquina de escribir)	ru	typewriter	→	ru-RU	00010419	ru	typewriter
Ruso (Macintosh)	ru	mac	→	ru-RU	00000419	ru	mac
Sueco	se	-	→	sv-SE	0000041d	se	-
Sueco (Macintosh)	se	mac	→	sv-SE	0000041d	se	mac
Esloveno	si	-	→	sl-SI	00000424	si	-
Eslovaco	sk	-	→	sk-SK	0000041b	sk	-
Eslovaco (QWERTY)	sk	qwerty	→	sk-SK	0001041b	sk	qwerty
Tailandés	th	-	→	th-TH	0000041e	th	-
Tailandés (Pattachote)	th	pat	→	th-TH	0001041e	th	pat
Tayiko	tj	-	→	tg-Cyrl-TJ	00000428	tj	-
Turco	tr	-	→	tr-TR	0000041f	tr	-
Turco (F)	tr	f	→	tr-TR	0001041f	tr	f
Chino tradicional	tw	-	→	en-US	00000409	us	-
Ucraniano	ua	-	→	uk-UA	00000422	ua	-
Inglés (EE. UU.)	us	-	→	en-US	00000409	us	-

Descripción del teclado del cliente Linux	Distribución del teclado del cliente Linux	Variante de teclado de cliente Linux	Se sincroniza con	ID de la configuración regional de Windows	Distribución del teclado de Windows VDA (ID)	Distribución del teclado de Linux VDA	Variante de teclado de Linux VDA
Inglés (Macintosh)	us	mac	→	en-US	00000409	us	mac
Inglés (Dvorak)	us	dvorak	→	en-US	00010409	us	dvorak
Inglés (Dvorak, para zurdos)	us	dvorak-l	→	en-US	00030409	us	dvorak-l
Inglés (Dvorak, para diestros)	us	dvorak-r	→	en-US	00040409	us	dvorak-r
Inglés (EE. UU., internacional, con teclas inactivas)	us	intl	→	nl-NL	00020409	us	intl
Vietnamita	vn	-	→	vi-VN	0000042a	vn	-

Distribución del teclado VDA

La función de distribución del teclado VDA ayuda en el uso de esta distribución, independientemente de los parámetros de la distribución del teclado del cliente. Es compatible con los siguientes tipos de teclado: PC/XT 101, 102, 104, 105, 106.

Para utilizar la distribución del teclado en el lado del servidor:

1. Inicie el archivo wfclient.ini.
2. Cambie el valor del atributo `KeyboardLayout` de la siguiente manera:

   ```
   KeyboardLayout=(Server Default)
   ```


El valor predeterminado del atributo `KeyboardLayout` es (User Profile).

3. Vuelva a iniciar la sesión para que los cambios surtan efecto.

Asociación de tipos de archivos

Una instancia de Citrix Virtual Apps Services también puede publicar un archivo, en lugar de una aplicación o un escritorio. Este proceso se denomina publicación de contenido y permite que pnabrowse abra el archivo publicado.

Existe una limitación en el tipo de archivos que reconoce la aplicación Citrix Workspace. Solo cuando una aplicación publicada está asociada al tipo de archivo del archivo publicado:

- El sistema reconoce el tipo de archivo del contenido publicado
- Los usuarios pueden ver el archivo a través de la aplicación Citrix Workspace

Por ejemplo, para ver un archivo Adobe PDF publicado a través de la aplicación Citrix Workspace, debe publicarse una aplicación como Adobe PDF Viewer. A menos que se publique una aplicación adecuada, los usuarios no podrán ver el contenido publicado.

Para habilitar la asociación de tipos de archivo del lado del cliente:

1. Verifique que la aplicación que quiere asociar sea una aplicación favorita o suscrita.
2. Para obtener la lista de aplicaciones publicadas y la URL del servidor, ejecute los comandos:

```
./util/storebrowse -l

./util/storebrowse -S <StoreFront URL>
<!--NeedCopy-->
```

3. Ejecute el comando ./util/ctx_app_bind con la siguiente sintaxis:

   `./util/ctx_app_bind [-p] example_file|MIME-type published-application [server|server-URI]`

   Por ejemplo:
   `./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.bvt.local/citrix/store/discovery`

4. Compruebe que el archivo que está intentando abrir esté habilitado para la asignación de unidades de cliente (CDM).
5. Haga doble clic en el archivo para abrirlo mediante la aplicación asociada.

Asociar una aplicación publicada a tipos de archivo

La aplicación Citrix Workspace para Android lee y aplica los parámetros configurados por los administradores en Citrix Studio.

Requisito previo:

Debe conectarse al servidor del almacén donde está configurada la asociación de tipos de archivo (FTA).

Para vincular una extensión de nombre de archivo a una aplicación Citrix Workspace para Linux:

1. Publique la aplicación.
2. Inicie sesión en Citrix Studio.
3. Haga clic con el botón secundario en la aplicación y seleccione **Propiedades**.
4. Seleccione **Ubicación**.
5. Agregue "%**" al campo de argumento de la línea de comandos (opcional) para omitir la validación de líneas de comandos y, a continuación, haga clic en Aceptar.
6. Haga clic con el botón secundario en la aplicación y seleccione **Propiedades**.
7. Seleccione **Asociación de tipos de archivo**.
8. Seleccione las extensiones que quiere que Citrix Workspace asocie con la aplicación.
9. Haga clic en **Aplicar** y en **Actualizar tipos de archivo**.
10. Siga los pasos indicados en Asociación de tipos de archivo para habilitar la asociación de tipos de archivo en el lado del cliente.

> **Nota:**
>
> La asociación de tipos de archivo de StoreFront debe estar activada. De forma predeterminada, la asociación de tipos de archivo está habilitada.

Compatibilidad con Citrix Analytics

A partir de la versión 2006, la aplicación Citrix Workspace se actualiza para transmitir datos a Citrix Analytics Service de las sesiones ICA que inicie desde un explorador web.

Para obtener más información sobre cómo utiliza esta información Citrix Analytics, consulte Self-Service Search for Performance y Self-service search for Virtual Apps and Desktops.

La aplicación Citrix Workspace para Linux está diseñada para transmitir registros de forma segura a Citrix Analytics cuando la aplicación desencadena ciertos eventos. Los registros se analizan y almacenan en los servidores de Citrix Analytics cuando está habilitado. Para obtener más información sobre Citrix Analytics, consulte Citrix Analytics.

Interfaz de usuario transparente

El protocolo ICA de Citrix utiliza el protocolo de canal virtual [TUI VC] para interfaces de usuario transparentes con el objetivo de transmitir datos entre servidores de Citrix Virtual Apps and Desktops o Citrix DaaS y servidores host. El protocolo TUI transmite mensajes de componentes de interfaz de usuario [IU] para conexiones remotas.

La aplicación Citrix Workspace para Linux admite la función TUI VC. Esta función ayuda al cliente a recibir los paquetes TUI enviados por el servidor, y el cliente puede acceder a los componentes relacionados con la IU. Esta funcionalidad le ayuda a controlar la visualización de la pantalla superpuesta predeterminada. Puede activar y desactivar el indicador `VDTUI` en el archivo `module.ini`: `VDTUI - On/Off`

A partir de la versión 1912, el indicador **VDTUI** se **activa** de forma predeterminada. Por eso, el cuadro de diálogo "Iniciando \<aplicación\>" ya no aparece al iniciar una aplicación. En su lugar, aparece el cuadro de diálogo "Conectando \<aplicación\>" con una barra de progreso. El cuadro de diálogo también muestra el progreso del inicio de la aplicación. Sin embargo, si **desactiva** el indicador, el cuadro de diálogo "Iniciando \<aplicación\>" se muestra en la parte superior de otras ventanas de la aplicación, con lo que oculta la solicitud de inicio de sesión.

Para obtener más información sobre los canales virtuales, consulte Canales virtuales de Citrix ICA en la documentación de Citrix Virtual Apps and Desktops.

Autenticarse

May 9, 2023

A partir de la aplicación Citrix Workspace 2012, puede ver el cuadro de diálogo de autenticación dentro de la aplicación Citrix Workspace y los detalles del almacén en la pantalla de inicio de sesión. Esto proporciona una experiencia mejor.

Los tokens de autenticación se cifran y se almacenan para que no tenga que introducir credenciales de nuevo cuando se reinicie el sistema o la sesión.

> **Nota:**
>
> Esta mejora de la autenticación solo se aplica a implementaciones en la nube.

Requisito previo:

Instale la biblioteca `libsecret`.

Esta función está habilitada de manera predeterminada.

Mejora de la autenticación para Storebrowse

> **Nota:**
>
> A partir de la versión 2205, esta función está disponible de forma general para la aplicación Citrix Workspace.

A partir de la versión 2203, el cuadro de diálogo de autenticación está presente en la aplicación Citrix Workspace, y los detalles del almacén se muestran en la pantalla de inicio de sesión para mejorar la experiencia de usuario. Los tokens de autenticación se cifran y se almacenan para que no tenga que introducir credenciales de nuevo cuando se reinicie el sistema o la sesión.

La mejora de la autenticación permite usar storebrowse para estas operaciones:

- `Storebrowse -E`: Muestra los recursos disponibles.
- `Storebrowse -L`: Inicia una conexión con un recurso publicado.
- `Storebrowse -S`: Enumera los recursos suscritos.
- `Storebrowse -T`: Cierra todas las sesiones del almacén especificado.
- `Storebrowse -Wr`: Conecta de nuevo las sesiones desconectadas, pero todavía activas, del almacén especificado. La opción [r] conecta de nuevo todas las sesiones desconectadas.
- `storebrowse -WR`: Conecta de nuevo las sesiones desconectadas, pero todavía activas, del almacén especificado. La opción [R] conecta de nuevo todas las sesiones activas y desconectadas.
- `Storebrowse -s`: Suscribe el recurso especificado de un almacén.
- `Storebrowse -u`: Cancela la suscripción del recurso especificado de un almacén.
- `Storebrowse -q`: Inicia una aplicación mediante la URL directa. Este comando solo funciona para almacenes de StoreFront.

> **Nota:**
>
> - Puede seguir utilizando los comandos de storebrowse restantes como se usaban antes (con AuthManagerDaemon).
> - La mejora de la autenticación solo se aplica a las implementaciones de la nube.
> - Con esta mejora, se admite la función de inicio de sesión persistente.

Mejora de la autenticación para la configuración de Storebrowse

De forma predeterminada, la función de mejora de la autenticación está inhabilitada.

Si gnome-keyring no está disponible, el token se almacena en la memoria del proceso de autoservicio.

Para forzar el almacenamiento del token en la memoria, siga estos pasos para inhabilitar gnome-keyring:

1. Vaya a `/opt/Citrix/ICAClient/config/AuthmanConfig.xml`.
2. Agregue la siguiente entrada:


```
<GnomeKeyringDisabled>true</GnomeKeyringDisabled>
<!--NeedCopy-->
```

Tarjeta inteligente

Para configurar la compatibilidad con tarjetas inteligentes en la aplicación Citrix Workspace para Linux, debe configurar el servidor de StoreFront a través de la consola de StoreFront.

La aplicación Citrix Workspace admite lectores de tarjetas inteligentes compatibles con los controladores PCSC-Lite y PKCS #11. Ahora, la aplicación Citrix Workspace busca `opensc-pkcs11.so` en una de las ubicaciones estándares de forma predeterminada.

La aplicación Citrix Workspace puede encontrar `opensc-pkcs11.so` en una ubicación no estándar u otro controlador de `PKCS\##11`. Puede almacenar la ubicación respectiva mediante este procedimiento:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Busque la línea <key>PKCS11module</key> y agregue la ubicación del controlador al elemento <value> que hay justo después de la línea.

> **Nota:**
>
> Si indica un nombre de archivo para la ubicación del controlador, la aplicación Citrix Workspace va a ese archivo en el directorio `$ICAROOT/PKCS\ ##11`. También puede usar una ruta absoluta que comience por "/".

Después de extraer una tarjeta inteligente, debe configurar el comportamiento de la aplicación Citrix Workspace. Para ello, siga estos pasos para actualizar `SmartCardRemovalAction`:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Busque la línea <key>SmartCardRemovalAction</key> y agregue `noaction` o `forcelogoff` al elemento <value> 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 extraer la tarjeta inteligente.

La acción `forcelogoff` borra todas las credenciales y todos los tokens que hubiera en StoreFront al extraer la tarjeta inteligente.

Habilitar la compatibilidad con tarjetas inteligentes

La aplicación Citrix Workspace admite varios lectores de tarjetas inteligentes si la tarjeta inteligente está habilitada tanto en el servidor como en la aplicación Citrix Workspace.

Puede usar tarjetas inteligentes con estos fines:

- Autenticación de inicio de sesión con tarjeta inteligente: Le autentica en servidores de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).
- Compatibilidad con aplicaciones de tarjetas inteligente: Permite que las aplicaciones publicadas compatibles con tarjetas inteligentes puedan acceder a dispositivos de tarjetas inteligentes locales.

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

La compatibilidad con 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.
- Instale el controlador apropiado para su tarjeta inteligente.
- Instale el paquete PC/SC Lite.
- Debe instalar y ejecutar el demonio `pcscd`, lo que proporciona al middleware acceso mediante PC/SC a las tarjetas inteligentes.
- En un sistema de 64 bits, las versiones de 32 y 64 bits del paquete "libpscslite1" deben estar presentes.

Para obtener más información sobre cómo configurar la compatibilidad con tarjetas inteligentes en los servidores, consulte Tarjetas inteligentes en la documentación de Citrix Virtual Apps and Desktops.

Mejora en la compatibilidad con tarjetas inteligentes

> **Nota:**
>
> Esta función está generalmente disponible en la aplicación Citrix Workspace.

A partir de la versión 2112, la aplicación Citrix Workspace admite la funcionalidad Plug and Play para el lector de tarjetas inteligentes.

Al insertar una tarjeta inteligente, el lector de tarjetas inteligentes detecta la tarjeta inteligente en el servidor y en el cliente.

Puede conectar y usar directamente distintas tarjetas al mismo tiempo, y todas se detectan.

Requisitos previos:

Instale la biblioteca `libpcscd` en el cliente Linux.

> **Nota:**
>
> Es posible que esta biblioteca se instale de forma predeterminada en las versiones recientes de la mayoría de las distribuciones de Linux. Sin embargo, es posible que deba instalar la biblioteca `libpcscd` en versiones anteriores de algunas distribuciones de Linux, como Ubuntu 1604.

Para inhabilitar esta mejora:

1. Vaya a la carpeta <ICAROOT>/config/module.ini.
2. Vaya a la sección SmartCard.
3. Configure esta opción: DriverName=VDSCARD.DLL.

Compatibilidad con nuevas tarjetas PIV

A partir de la versión 2303, la aplicación Citrix Workspace admite estas tarjetas nuevas de verificación de identificación personal (PIV):

- Tarjeta inteligente IDEMIA de nueva generación
- Tarjeta inteligente TicTok de DELL

Optimización del rendimiento del controlador de tarjetas inteligentes

La versión 2303 de la aplicación Citrix Workspace incluye correcciones y optimizaciones relacionadas con el rendimiento para el controlador de tarjetas inteligentes VDSCARDV2.DLL. Estas mejoras ayudan a superar a la versión 1 VDSCARD.DLL.

Compatibilidad con autenticación de varios factores (nFactor)

La autenticación de varios factores mejora la seguridad de las aplicaciones porque requiere que los usuarios proporcionen pruebas de identidad adicionales para obtener acceso.

La autenticación de varios factores hace que el administrador pueda configurar los pasos de autenticación y los formularios de recopilación de credenciales asociados.

La aplicación Citrix Workspace nativa admite este protocolo a partir de la funcionalidad de formularios de inicio de sesión ya implementada para StoreFront. Las páginas de inicio de sesión web de los servidores virtuales de Citrix Gateway y Traffic Manager también utilizan este protocolo.

Para obtener más información, consulte SAML authentication y Multi-Factor (nFactor) authentication en la documentación de Citrix ADC.

Compatibilidad con la autenticación mediante FIDO2 en sesiones HDX

> **Nota:**
>
> A partir de la versión 2303, esta función está disponible de forma general para la aplicación Citrix Workspace.

Con esta versión, puede autenticarse dentro de una sesión de HDX mediante claves de seguridad FIDO2 sin contraseña. Las claves de seguridad FIDO2 ofrecen un modo intuitivo de autenticación para

empleados corporativos en aplicaciones o escritorios compatibles con FIDO2 sin necesidad de introducir un nombre de usuario o una contraseña. Para obtener más información sobre FIDO2, consulte Autenticación FIDO2.

> **Nota:**
>
> Si utiliza el dispositivo FIDO2 mediante la redirección de USB, quite la regla de redirección de USB de su dispositivo FIDO2 del archivo `usb.conf` de la carpeta `$ICAROOT/`. Esta actualización le ayuda a cambiar al canal virtual FIDO2.

De forma predeterminada, la autenticación FIDO2 está inhabilitada. Para habilitar la autenticación FIDO2, haga lo siguiente:

1. Vaya al archivo `<ICAROOT>/config/module.ini`.
2. Vaya a la sección `ICA 3.0`.
3. Defina `FIDO2= On`.

Esta función admite actualmente autenticadores móviles (solo USB) con código PIN y funciones táctiles. Puede configurar la autenticación basada en claves de seguridad FIDO2. Para obtener información sobre los requisitos previos y el uso de esta función, consulte Autorización local y autenticación virtual mediante FIDO2.

Al acceder a una aplicación o un sitio web que admite FIDO2, aparece un mensaje que solicita acceso a la clave de seguridad. Si ya registró su clave de seguridad con un PIN (como mínimo, 4 caracteres, y como máximo, 64), debe introducir el PIN al iniciar sesión.

Si ya registró su clave de seguridad sin un PIN, solo tiene que tocar la clave de seguridad para iniciar sesión.

Limitación:

Es posible que no pueda registrar el segundo dispositivo en una misma cuenta mediante la autenticación FIDO2.

Proteger comunicaciones

January 18, 2023

Para proteger la comunicación entre el sitio y la aplicación Citrix Workspace, se pueden integrar las conexiones de la aplicación Citrix Workspace a través de tecnologías de seguridad como Citrix Gateway.

> **Nota:**
>
> Citrix recomienda utilizar Citrix Gateway entre los servidores de StoreFront y los dispositivos de

> los usuarios.

- 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 utiliza la aplicación Citrix Workspace 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 la dirección externa.
- Servidor de confianza.
- Solo para implementaciones de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service; no se aplica a XenDesktop 7): Un servidor proxy SOCKS o un servidor proxy seguro (también conocido como servidor proxy de seguridad, servidor proxy HTTPS o servidor proxy de túnel Transport Layer Security o TLS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre la aplicación Citrix Workspace y los servidores. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.
- Solo para implementaciones de Citrix Virtual Apps and Desktops o Citrix DaaS: Soluciones Citrix Secure Web Gateway o Traspaso SSL con protocolos TLS. Se admite de la versión 1.0 a la versión 1.2 de TLS.

Citrix Gateway

Citrix Gateway (anteriormente Access Gateway) protege las conexiones a los almacenes de StoreFront. Además, permite a los administradores controlar, de manera detallada, el acceso de los usuarios a los escritorios y las aplicaciones.

Para conectarse a escritorios y aplicaciones a través de Citrix Gateway:

1. Especifique la URL de Citrix Gateway que el administrador proporciona de una de las siguientes maneras:
   - 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 quiere 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, si quiere, un almacén concreto:

   - Para conectar con el primer almacén que encuentre la aplicación Citrix Workspace, use una URL con, por ejemplo, el formato: https://gateway.company.com.
   - Para conectar con un almacén específico, use una URL con, por ejemplo, el formato: https://gateway.company.com?<storename>. Esta dirección URL dinámica no tiene el formato estándar; no incluya = (el signo igual) en la URL. Si quiere establecer una conexión a un

almacén concreto mediante storebrowse, puede que se necesiten comillas alrededor de la dirección URL en el comando storebrowse.

2. Cuando se le solicite, conéctese al almacén (a través de la puerta de enlace) con su nombre de usuario, contraseña y token de seguridad. Para obtener más información sobre este paso, consulte la documentación de Citrix Gateway.

   Una vez completado el proceso de autenticación, se muestran los escritorios y las aplicaciones.

Servidor proxy

Los servidores proxy se utilizan para limitar el acceso entrante y saliente de la red, y para gestionar conexiones entre la aplicación Citrix Workspace y los entornos de Citrix Virtual Apps and Desktops o Citrix DaaS.

La aplicación Citrix Workspace admite el protocolo SOCKS, junto con lo siguiente:

- Citrix Secure Web Gateway y el Traspaso SSL de Citrix, el protocolo de proxy seguro
- Autenticación de desafío/respuesta de Windows NT (NTLM).

Para configurar el proxy de modo que inicie un escritorio, haga lo siguiente:

1. Vaya al archivo de configuración `~/.ICAClient/All_Regions.ini`.
2. Actualice estos atributos:
   a) Actualice `ProxyType`. Puede usar `SocksV5` como `ProxyType`.
   b) Actualice `ProxyHost`. Puede agregar `ProxyHost` en este formato:

      `<IP>:<PORT>`. Por ejemplo: “10.122.122.122:1080”.

> **Nota:**
>
> - Para usar el proxy, inhabilite EDT. Para inhabilitar EDT, *desactive* el atributo `HDXoverUDP` en la sección `[Network\UDT]` del archivo de configuración `~/.ICAClient/All_Regions.ini`.
> - Para garantizar una conexión segura, habilite TLS.

Servidor proxy seguro

La configuración de conexiones para utilizar el protocolo de proxy seguro también habilita 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.

> **Importante:**
>
> La compatibilidad con NTLM requiere las bibliotecas OpenSSL 1.1.1d y libcrypto.so. Instale las

> bibliotecas en el dispositivo del usuario. Estas bibliotecas se incluyen a menudo en las distribuciones de Linux. También puede descargarlas desde http://www.openssl.org/.

Secure Web Gateway y SSL

Puede integrar la aplicación Citrix Workspace con los servicios Citrix Secure Web Gateway o servicio de Traspaso SSL. La aplicación Citrix Workspace admite el protocolo TLS. TLS (Transport Layer Security) 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.

Secure Web Gateway

Puede usar Citrix Secure Web Gateway en modo normal o modo de traspaso para proporcionar un canal de comunicaciones seguro entre la aplicación Citrix Workspace y el servidor. Si utiliza Secure Web Gateway en modo **normal**, la aplicación Citrix Workspace no requiere ninguna configuración.

Si se instala Citrix Secure Web Gateway Proxy en un servidor de una red segura, se puede utilizar Citrix Secure Web Gateway Proxy en modo de traspaso (Relay). Si se utiliza el modo de traspaso, el servidor de Citrix Secure Web Gateway funciona como un proxy y es necesario configurar la aplicación Citrix Workspace para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor de Citrix Secure Web Gateway.
- El número de puerto del servidor de Citrix Secure Web Gateway.

> **Nota:**
>
> La versión 2.0 de Citrix Secure Web Gateway no ofrece el modo de traspaso.

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

- Nombre de host
- Dominio intermedio
- Dominio superior

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

Traspaso SSL

De forma predeterminada, el Traspaso SSL Citrix utiliza el puerto TCP 443 en el servidor de Citrix Virtual Apps and Desktops o Citrix DaaS 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 la aplicación Citrix Workspace 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

Para obtener más información sobre la configuración y el uso del Traspaso SSL para proteger la instalación, consulte la documentación de Citrix Virtual Apps.

TLS

Antes, la versión mínima de TLS admitida era 1.0, y la versión máxima de TLS admitida era 1.2. A partir de la versión 2203, la versión máxima de TLS admitida es 1.3.

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

- MinimumTLS=1.1
- MaximumTLS=1.3

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

> **Notas:**
>
> - Estos valores se leen en el momento de iniciar los programas. Si los cambia después de haber iniciado self-service o storebrowse, debe escribir: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.
> - La aplicación Citrix Workspace para Linux no permite usar el protocolo SSLv3.
> - TLS 1.0/1.1 solo funciona con la versión anterior de VDI o Citrix Gateway que los admitan.

Para seleccionar el conjunto de cifrado, agregue la siguiente opción de configuración en la sección [WFClient]:

- SSLCiphers=GOV

Este es el valor predeterminado. Otros valores reconocidos son COM y ALL.

> **Nota:**
>
> Al igual que con la configuración de la versión de TLS, si cambia esta configuración después de

> haber iniciado self-service o storebrowse, debe escribir:
> **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

Actualización de CryptoKit

La versión 14.2 de CryptoKit está integrada en la versión 1.1.1d de OpenSSL.

Actualización criptográfica

Esta función es un cambio importante en el protocolo de comunicación segura. Los conjuntos de cifrado con el prefijo TLS_RSA_ que no ofrecen confidencialidad directa se consideran débiles.

Los conjuntos de cifrado TLS_RSA_ se han eliminado por completo. En su lugar, se admiten los conjuntos de cifrado avanzados TLS_ECDHE_RSA_.

Si su entorno no está configurado con los conjuntos de cifrado TLS_ECDHE_RSA_, los inicios de sesión clientes no se admiten debido a cifrados débiles. Para la autenticación de clientes, se admiten claves RSA de 1536 bits.

Se admiten los siguientes conjuntos de cifrado avanzado:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

DTLS v1.0 admite los siguientes conjuntos de cifrado:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

DTLS v1.2 admite los siguientes conjuntos de cifrado:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

TLS 1.3 admite los siguientes conjuntos de cifrado:

- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_AES_256_GCM_SHA384 (0x1302)

> **Nota:**
>
> A partir de la versión 1903 y posteriores, DTLS se admite en Citrix Gateway 12.1 y versiones posteriores. Para obtener información sobre los conjuntos de cifrado compatibles con DTLS para Citrix Gateway, consulte Compatibilidad con el protocolo DTLS.

Conjuntos de cifrado

Para habilitar diferentes conjuntos de cifrado, cambie el valor del parámetro `SSLCiphers` a `ALL`, `COM` o `GOV`. De forma predeterminada, la opción está establecida en `ALL` en el archivo `All_Regions.ini` del directorio `$ICAROOT/config`.

ALL, GOV y COM proporcionan los siguientes conjuntos de conjuntos de cifrado:

- ALL
  - Están disponibles los 3 conjuntos de cifrado.
- GOV
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- COM
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Para obtener información sobre la solución de problemas, consulte Conjuntos de cifrado.

Los conjuntos de cifrado con el prefijo TLS_RSA_ no ofrecen confidencialidad directa. Estos conjuntos de cifrado ya son obsoletos en la industria. Sin embargo, por compatibilidad con versiones anteriores de Citrix Virtual Apps and Desktops o Citrix DaaS, la aplicación Citrix Workspace dispone de una opción para utilizar estos conjuntos de cifrado.

Para una mayor seguridad, establezca el indicador `Enable\\_TLS\\_RSA\\_` en **False**.

A continuación, dispone de la lista de conjuntos de cifrado retirados:

- TLS_RSA_AES256_GCM_SHA384
- TLS_RSA_AES128_GCM_SHA256
- TLS_RSA_AES256_CBC_SHA256
- TLS_RSA_AES256_CBC_SHA
- TLS_RSA_AES128_CBC_SHA
- TLS_RSA_3DES_CBC_EDE_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

> **Nota:**
>
> Los dos últimos conjuntos de cifrado utilizan el algoritmo RC4 y se han retirado porque no son seguros. El conjunto de cifrado TLS_RSA_3DES_CBC_EDE_SHA también se puede considerar retirado. Puede usar estos indicadores para aplicar todos estos elementos retirados.

Para obtener información sobre la configuración de DTLS 1.2, consulte la sección Transporte adaptable de la documentación de Citrix Virtual Apps and Desktops.

Requisito previo:

Si utiliza la versión 1901 o una anterior, siga estos pasos:

Si `.ICAClient` ya está presente en el directorio de inicio del usuario actual:

- Elimine el archivo `All\\_Regions.ini`.

O bien:

- Para conservar el archivo `AllRegions.ini`, agregue las siguientes líneas al final de la sección [Network\SSL]:
  - Enable_RC4-MD5=
  - Enable_RC4_128_SHA=
  - Enable_TLS_RSA_=

Si la carpeta `.ICAClient` no está presente en la carpeta particular del usuario actual, indica una nueva instalación de la aplicación Citrix Workspace. En ese caso, se conserva la configuración predeterminada para la funcionalidad.

En la tabla siguiente se enumeran los conjuntos de cifrado en cada grupo:
Tabla 1: Tabla de compatibilidad de los conjuntos de cifrado

> **Nota:**
>
> Todos los conjuntos de cifrado anteriores cumplen con FIPS y SP800-52. Los dos primeros están permitidos solo para conexiones (D)TLS1.2. Consulte **Tabla 1: Tabla de compatibilidad de los conjuntos de cifrado** para obtener una representación completa de la compatibilidad con los conjuntos de cifrado.

Certificados

Cuando utiliza un almacén con autenticación SAML (con el protocolo AUTHv3), aparece el siguiente mensaje de error: “Unacceptable TLS Certificate”.

El problema se produce cuando se utiliza la aplicación Citrix Workspace 1906 y versiones posteriores. Para obtener instrucciones sobre la solución de problemas, consulte los siguientes artículos en Knowledge Center.

- CTX260336
- CTX231524
- CTX203362

Si el servidor de StoreFront no consigue proporcionar los certificados intermedios que coincidan con el certificado que está utilizando, o si instala certificados intermedios para admitir usuarios de tarjetas inteligentes, siga estas instrucciones antes de agregar un almacén de StoreFront:

1. Obtenga uno o varios certificados intermedios por separado en formato PEM.

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

2. Como el usuario que instala el paquete (normalmente root):
   a) Copie uno o varios archivos a $ICAROOT/keystore/intcerts.
   b) Ejecute el siguiente comando como usuario que instaló el paquete:

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

Si autentica un certificado de servidor emitido por una entidad de certificación, pero que no goza de la confianza de los dispositivos de usuario, siga estas instrucciones antes de agregar un almacén de StoreFront:

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

Mejora del protocolo HDX Enlightened Data Transport (EDT)

En versiones anteriores, al establecer `HDXoverUDP` en `Preferred`, el transporte de datos por EDT se utiliza como transporte principal, y TCP queda como opción de emergencia.

A partir de la versión 2103 de la aplicación Citrix Workspace, cuando la fiabilidad de la sesión está habilitada, se intentan EDT y TCP en paralelo en los siguientes casos::

- Conexión inicial
- Reconexión de fiabilidad de la sesión
- Reconexión automática de clientes

Esta mejora reduce el tiempo de conexión cuando se prefiere EDT. No obstante, el transporte UDP subyacente necesario no está disponible y se debe utilizar TCP.

De forma predeterminada, después de recurrir a TCP, el transporte adaptable vuelve a intentar utilizar EDT cada cinco minutos.

Detección de MTU en Enlightened Data Transport (EDT)

La aplicación Citrix Workspace versión 2109 permite la detección de unidades de transmisión máxima (MTU) en Enlightened Data Transport (EDT). Aumenta la fiabilidad y la compatibilidad del protocolo

EDT y mejora la experiencia de usuario.

Para obtener más información, consulte la sección Detección de MTU en EDT de la documentación de Citrix Virtual Apps and Desktops.

Compatibilidad con IPv6 de EDT

A partir de la versión 2203 de la aplicación Citrix Workspace, se admite EDT IPv6.

> **Nota:**
>
> IPv6 es compatible con TCP y EDT. Sin embargo, IPv6 no se admite en TCP por TLS y en EDT por DTLS.

Storebrowse

January 18, 2023

Storebrowse es una utilidad ligera de línea de comandos que interactúa entre el cliente y el servidor. Con la utilidad storebrowse, los administradores pueden automatizar las siguientes operaciones cotidianas:

- Agregar un almacén.
- Producir una lista de las aplicaciones y los escritorios publicados desde un almacén configurado.
- Suscribir y cancelar la suscripción de aplicaciones y escritorios de un almacén configurado.
- Habilitar e inhabilitar accesos directos para aplicaciones y escritorios publicados.
- Iniciar aplicaciones publicadas.
- Volver a conectarse a sesiones desconectadas.

La utilidad storebrowse suele estar disponible en la carpeta `/util`. Puede encontrarla en la ubicación de la instalación. Por ejemplo: `/opt/Citrix/ICAClient/util`.

Requisitos previos

La utilidad storebrowse requiere el paquete de biblioteca **libxml2**.

Iniciar aplicaciones y escritorios publicados

Hay dos formas de iniciar un recurso:

- Puede utilizar los comandos de la línea de comandos y de storebrowse.
- Puede utilizar la interfaz de usuario para iniciar recursos.

En este artículo se describen los comandos de storebrowse.

Mejora de Storebrowse para la continuidad del servicio

Antes, los archivos de concesión de conexiones de Workspace se sincronizaban con archivos disponibles en el servidor remoto solamente si se conectaba mediante Self-Service Plug-in. Como resultado, la función de continuidad del servicio no estaba disponibles al iniciar aplicaciones o sesiones de escritorio mediante storebrowse. La mayoría de los proveedores externos de clientes ligeros utilizan storebrowse para conectarse a la plataforma Workspace, y la función de continuidad del servicio no estaba habilitada para ellos.

A partir de la versión 2109 de la aplicación Citrix Workspace, los archivos de concesión de conexiones de Workspace también se sincronizan con archivos disponibles en el servidor remoto al conectarse mediante storebrowse. Esta función ayuda a los proveedores externos de clientes ligeros a acceder a Workspace incluso cuando no hay conexión.

> **Nota:**
>
> - Esta mejora solo está disponible cuando la continuidad del servicio está habilitada en implementaciones en la nube. Para obtener más información, consulte la sección Configurar la continuidad del servicio de la documentación de Citrix Workspace.

Uso de comandos

En la siguiente sección se detallan los comandos de storebrowse que puede utilizar desde la utilidad storebrowse.

Agregar un almacén

`-a, --addstore`

Descripción:

Agrega un almacén con detalles sobre la puerta de enlace, la baliza y el proceso de demonio ServiceRecord. Este comando devuelve la URL completa del almacén. Aparece un error si no se puede agregar un almacén.

Ejemplo de comando en StoreFront:

Comando:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

Ejemplo:

```
./storebrowse -a https://my.firstexamplestore.net
```


> **Nota:**
>
> Puede agregar varios almacenes mediante la utilidad storebrowse.

Ayuda

`-?, -h, --help`

Descripción:

Ofrece información detallada sobre el uso de la utilidad storebrowse

Enumerar almacenes

`-l --liststore`

Descripción:

Muestra los almacenes que ha agregado.

Ejemplo de comando en StoreFront:

`./storebrowse -l`

Enumerar

`-E --enumerate`

Descripción:

Muestra los recursos disponibles. De forma predeterminada, aparecen los siguientes valores:

- Resource name
- Nombre simplificado
- Carpeta del recurso

Para ver más información, adjunte el comando `-M --details` al comando `-E`.

> **Nota:**
>
> Al ejecutar el comando **-E**, aparece una ventana de autenticación si antes no proporcionó sus credenciales.

Escriba toda la URL del almacén según lo indicado por **-liststore**.

Ejemplo de comando de StoreFront:

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Suscrito

`-S --subscribed`

Descripción:

Enumera los recursos suscritos. De forma predeterminada, aparecen los siguientes valores:

- Resource name
- Nombre simplificado
- Carpeta del recurso

Para ver más información, adjunte el comando `-M --details` al comando `-E`.

Ejemplo de comando de StoreFront:

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

Detalles

`-M --details`

Descripción:

Este comando devuelve varios atributos de las aplicaciones publicadas. Este comando suele utilizarse con los comandos **-E** y **-S**. Este comando toma un argumento que es la suma de los números correspondientes a los detalles requeridos:

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)

- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

> **Notas:**
>
> - Para crear entradas de menú para aplicaciones suscritas, utilice el argumento CreateShortcuts(0x100000) con los comandos **-S**, **-s** y **-u**.
> - Para eliminar todas las entradas de menú, utilice RemoveShortcuts(0x200000) con el comando **-S**.

Ejemplo de comando de StoreFront:

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

En el ejemplo de comando anterior, 0x264 es la combinación de DisplayName(0x200), AppIsDisabled(0x40), AppIsDesktop(0x20) y SoundType(0x4). El resultado muestra los recursos suscritos y sus detalles.

Puede utilizar el comando **-M** para enumerar los recursos con los detalles necesarios:

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

> **Notas:**
>
> - Puede expresar los valores en formato decimal o hexadecimal. Por ejemplo, 512 para 0x200.
> - Cuando algunos de los detalles no están disponibles a través de storebrowse, el valor resultante es cero.

Suscribir

```
-s --subscribe
```

Descripción:

Suscribe el recurso especificado de un almacén.

Ejemplo de comando de StoreFront:

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

Cancelar suscripción

```
-u --unsubscribe
```


Descripción:

Cancela la suscripción del recurso especificado de un almacén.

Ejemplo de comando de StoreFront:

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

Inicio

```
-L --launch
```

Descripción:

Inicia una conexión con un recurso publicado. A continuación, la utilidad se cierra automáticamente, lo que deja una sesión conectada correctamente.

Ejemplo de comando de StoreFront:

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

Iconos

```
-i --icons
```

Descripción:

Este comando obtiene iconos de escritorio y aplicación en formato PNG. Este comando se utiliza con los comandos **-E** o **-S**.

Para obtener iconos de tamaños y profundidades requeridos, utilice el método del argumento best o del argumento size.

Argumento best

Con el método del argumento best, puede obtener los iconos del mejor tamaño disponibles en el servidor. Más tarde, puede ajustar los iconos a los tamaños requeridos. El método del argumento best es la forma más eficiente de almacenar, aplicar ancho de banda y simplificar la creación de scripts. Los archivos se guardan en formato <nombre del recurso>.PNG.

Argumento size

Para obtener iconos de tamaños y profundidades especificados, utilice el método del argumento size. Aparece un error si el servidor no puede obtener iconos de un tamaño o una profundidad determinados.

El argumento size tiene la forma WxB, donde:

- **W** es el ancho de los iconos. Todos los iconos son cuadrados, por lo que solo se necesita un valor para especificar el tamaño.
- **B** es la profundidad de color. Es decir, la cantidad de bits por píxel.

> **Nota:**
>
> El valor **W** es obligatorio. El valor **B** es opcional.

Si deja los valores sin especificar, aparecerán iconos de todas las profundidades de imagen disponibles. Los archivos se guardan en el formato <nombre del recurso>_WxWxB.png.

Los dos métodos guardan iconos en formato **PNG** para cada recurso que devuelven los comandos **-E** o **-S**.

Los iconos se almacenan en la carpeta **.ICAClient/cache/icons**.

Ejemplo de comando de StoreFront:

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

Reconectar sesión

`-W [r|R] --reconnect [r|R]`

Descripción:

Vuelve a conectar las sesiones desconectadas pero todavía activas del almacén especificado. La opción [r] conecta de nuevo todas las sesiones desconectadas. La opción [R] conecta de nuevo todas las sesiones activas y desconectadas.

Ejemplo de comando de StoreFront:

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

Desconectar sesión

`-WD --disconnect`

Descripción:

Desconecta todas las sesiones del almacén especificado.

Ejemplo de comando de StoreFront:

```
./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery
```

Cerrar sesión

```
-WT --terminate
```

Descripción:

Cierra todas las sesiones del almacén especificado.

Ejemplo de comando de StoreFront:

```
./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery
```

Versión

```
-v --version
```

Descripción:

Muestra la versión de la utilidad storebrowse.

Ejemplo de comando de StoreFront:

```
./storebrowse -v
```

Directorio raíz

```
-r --icaroot
```

Descripción:

Especifica el directorio raíz donde está instalada la aplicación Citrix Workspace para Linux. Si no se especifica, el directorio raíz se determina durante la ejecución.

Ejemplo de comando de StoreFront:

```
./storebrowse -r /opt/Citrix/ICAClient
```

Nombre de usuario, contraseña, dominio

```
-U --username, -P --password, -D --domain
```

Descripción:

Pasa el nombre de usuario, la contraseña y los detalles del dominio al servidor. Este método solo funciona con almacenes PNA. Los almacenes de StoreFront ignoran este comando. Los detalles no se almacenan en la caché. Introduzca los detalles con cada comando.

Ejemplo de comando de StoreFront:

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U
 user1 -P password -D domain-name
```

Eliminar almacén

```
-d --deletestore
```

Descripción:

Cancela el registro de un almacén con el demonio de ServiceRecord.

Ejemplo de comando de StoreFront:

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Configurar autoservicio

```
-c --configselfservice
```

Descripción:

Obtiene y configura los parámetros de interfaz de usuario de autoservicio que se guardan en Store-Cache.ctx. Toma un argumento con el formato <entrada[=valor]>. Si solo está presente la entrada, se imprime el valor actual del parámetro. Sin embargo, si hay un valor presente, el valor se utiliza para configurar el parámetro.

Ejemplo de comando de StoreFront:

```
./storebrowse -c SharedUserMode=True
```

Agregar archivo CR

```
-C --addcr
```

Descripción:

Lee el archivo de Citrix Receiver (CR) proporcionado y le solicita que agregue cada almacén. El resultado es el mismo que el del comando **-a**, pero tiene más de un almacén, y estos están separados en líneas nuevas.

Ejemplo de comando de StoreFront:

```
./storebrowse -C <path to CR file>
```


Sincronizar archivos de concesión de conexiones

```
-o --synclease
```

Descripción:

Comienza a sincronizar los archivos de concesión de conexiones de Workspace con los archivos disponibles en el servidor remoto para el almacén especificado. Este comando ayuda a actualizar el almacén predeterminado y activa la sincronización de archivos de concesión. Aparece un error si la continuidad del servicio está inhabilitada.

Comando:

```
./storebrowse -o *URL of Store *
```

Ejemplo de comando de StoreFront:

```
./storebrowse -o https://my.firstexamplestore.net
```

Cerrar el demonio de storebrowse

```
-K --killdaemon
```

Descripción:

Cierra el demonio de storebrowse. Como consecuencia, se borran todas las credenciales y todos los tokens.

Ejemplo de comando de StoreFront:

```
./storebrowse -K
```

Enumerar códigos de error

```
-e --listerrorcodes
```

Descripción:

Enumera los códigos de error registrados.

Ejemplo de comando de StoreFront:

```
./storebrowse -e
```

Puerta de enlace del almacén

```
-g --storegateway
```

Descripción:

Establece la puerta de enlace predeterminada para un almacén que ya está registrado en el demonio de ServiceRecord.

Ejemplo de comando de StoreFront:

```
./storebrowse -g "<unique gateway name>" https://my.firstexamplestore.net/Citrix/Store/discovery
```

> **Nota:**
>
> El nombre exclusivo de la puerta de enlace debe estar en la lista de puertas de enlace del almacén especificado.

Inicio rápido

`-q, --quicklaunch`

Descripción:

Inicia una aplicación mediante la URL directa. Este comando solo funciona para almacenes de StoreFront.

Ejemplo de comando de StoreFront:

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Convertir en demonio

`-n --nosingleshot`

Descripción:

Siempre convierte el proceso storebrowse en demonio.

Ejemplo de comando de StoreFront:

```
./storebrowse -n
```

Parámetros de archivo

`-F --fileparam`

Descripción:

Inicia un archivo con la ruta de acceso del archivo y el recurso especificados.

Ejemplo de comando de StoreFront:


```
./storebrowse -F “<path to file>” -L <Resource Name> <https://my.firstexamplestore
.net/Citrix/Store/discovery>
```

Flujo de trabajo

En este artículo se muestra un sencillo flujo de trabajo sobre cómo iniciar una aplicación mediante los comandos de storebrowse:

1. `./storebrowse -a https://my.firstexamplestore.net`

   Agrega un almacén y proporciona la URL completa de dicho almacén. Tome nota de la URL completa porque se utiliza en los comandos posteriores.

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

   Enumera todas las aplicaciones y escritorios publicados. Introduzca sus credenciales en la ventana emergente que aparece para el almacén registrado.

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

   Inicia el recurso. Tome el valor de Resource_Name del resultado del comando anterior.

4. `./storebrowse -K`

   Este comando borra las credenciales introducidas anteriormente y cierra el proceso de demonio de storebrowse. Si no menciona explícitamente este comando, el proceso storebrowse se cierra una hora después.

Solución de problemas

February 21, 2023

En este artículo se proporciona información para ayudar a los administradores a solucionar problemas con la aplicación Citrix Workspace.

Conexión

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

Inicio de ICA en Fedora 29/30

Es posible que ICA no se pueda iniciar en Fedora 29/30. Como solución temporal, siga estos pasos:

1. Instale `compat-openssl10` con el comando.

   ```
   sudo yum install compat-openssl10.x86_64
   ```

2. Establezca la variable de entorno en `~/.bashrc` para carga en cada sesión. Esta acción apunta a la biblioteca `libcrypto` antigua.

   ```
   export LD_PRELOAD=/lib64/libcrypto.so.1.0.2o
   ```

> **Nota:**
>
> La aplicación Citrix Workspace funciona bien en el servidor X.Org, en comparación con el compositor Wayland. Para las distribuciones que tienen Wayland como protocolo de gráficos predeterminado, quite la marca de comentario de cualquiera de las siguientes opciones:
>
> `WaylandEnable=false` en `/etc/gdm/custom.conf` o en `/etc/gdm3/custom.conf`
>
> Cierre sesión e inicie sesión de nuevo para apuntar al servidor de X.Org.

Sesión de escritorio o recurso publicado

Al establecer una conexión con un servidor de Windows, si aparece un cuadro de diálogo con el mensaje “Connecting to server…”, pero luego no aparece ninguna 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.

Reconexión de sesión

Es posible que la conexión falle al conectarse de nuevo a una sesión con una profundidad de color superior a la que requiere la aplicación Citrix Workspace. Este error se produce cuando se agota la memoria disponible en el servidor.

Si la reconexión falla, la aplicación Citrix Workspace intenta utilizar la profundidad de color original. En caso contrario, el servidor intenta iniciar una sesión nueva con la profundidad de color solicitada, con lo que deja la sesión original en estado desconectado. Es posible que la segunda conexión falle si sigue faltando memoria en el servidor.

Nombre completo de Internet

Citrix recomienda configurar el DNS (servidor de nombres de dominio) en la red. Esta configuración le permite resolver los nombres de los servidores a los que quiere conectarse. Si el servidor DNS no está configurado, quizás no sea posible resolver el nombre de un servidor en una dirección IP. Como alternativa, puede especificar el servidor por su dirección IP, en lugar de hacerlo por su nombre. Las conexiones TLS requieren un nombre de dominio completo, no una dirección IP.

Error de detección de proxy

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 este comando, donde host name 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 ...;
```

Sesiones lentas

Si una sesión no se inicia hasta que mueva el mouse, puede que haya un problema con la generación del número aleatorio en el kernel de Linux. Como solución temporal, ejecute un demonio que genere entropía, como `rngd` (que está basado en hardware) o `haveged` (de Magic Software).

Conjuntos de cifrado

Si su conexión falla con la nueva función de cifrado:

1. Puede utilizar varias herramientas para comprobar los conjuntos de cifrado que admite su servidor, donde se incluyen:
   - `Ssllabs.com` (requiere que el servidor tenga acceso a Internet)
   - `sslyze` (`https://github.com/nabla-c0d3/sslyze`)
2. En Linux Client WireShark, busque el paquete (Client Hello, Server Hello) con el filtro (ip.addr == `VDAIPAddress`) para encontrar la sección SSL. El resultado tiene los conjuntos de cifrado enviados por el cliente y aceptados por el servidor.

Citrix Optimization SDK incorrecto

El paquete Citrix Optimization SDK incluye una versión incorrecta de `UIDialogLibWebKit.so`. Como solución temporal, haga lo siguiente:

1. Descargue la versión 18.10 del paquete del SDK de Citrix Optimization de la página Descargas.

a) Vaya a la ruta CitrixPluginSDK/UIDialogLib/GTK:

```
cd CitrixPluginSDK/UIDialogLib/GTK
```

b) Elimine todos los archivos objeto:

```
rm -rf *.o
```

c) Vaya a la carpeta WebKit:

```
cd ../WebKit
```

d) Retire el UIDialogLibWebKit.so existente:

```
rm -rf UIDialogLibWebKit.so
```

e) Utilice el siguiente comando en el directorio WebKit:

```
make all
```

Se genera el nuevo UIDialogLibWebKit.so.

f) Copie la nueva biblioteca en el directorio **$ICAROOT/lib**.

Conjuntos de cifrado débiles para las conexiones SSL

Al establecer una conexión TLS, la aplicación Citrix Workspace ofrece de forma predeterminada una serie de conjuntos de cifrado avanzados y restringidos.

Si se conecta a un servidor que requiere un conjunto de cifrado más antiguo, establezca la opción de configuración `SSLCiphers=ALL` en la sección [WFClient\] de un archivo de configuración.

Se admiten los siguientes conjuntos de cifrado avanzado:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028), ALL, GOV
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013), ALL, COM

Pérdida de conexión

Al usar el protocolo EDT, es posible que aparezca este mensaje de error: La conexión con "…" se ha perdido. Este problema puede ocurrir si la conexión pasa a través de un enrutador con una unidad de transmisión máxima para EDT que es inferior al valor predeterminado de 1500 bytes. Haga lo siguiente:

- Defina `edtMSS=1000` en un archivo de configuración.

Errores de conexión

Los errores de conexión pueden producir varios diálogos de error diferentes. Por ejemplo:

- "Error in connection: A protocol error occurred while communicating with the Authentication Service"
- "The Authentication Service cannot be contacted"
- "Your account cannot be added using this server address"

Estos errores pueden deberse a varios problemas, por ejemplo:

- Cuando el equipo local y el equipo remoto no pueden negociar un protocolo TLS común. Para obtener más información, consulte TLS.
- Cuando el equipo remoto requiere un conjunto de cifrado más antiguo para una conexión TLS. En este caso, puede establecer la opción de configuración `SSLCiphers=ALL` en la sección `\[WFClient\]` de un archivo de configuración y ejecutar `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` antes de reiniciar la conexión.
- Cuando el equipo remoto no pide el certificado de cliente de la manera apropiada. IIS solo debe **aceptar** o **solicitar** certificados para Citrix, Authentication y Certificate.
- Otros problemas.

Conexiones con ancho de banda reducido

Citrix recomienda utilizar la versión más reciente de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) en el servidor. Igualmente, use la aplicación Citrix Workspace más reciente en el dispositivo del usuario.

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

- **Configure la conexión de la aplicación Citrix Workspace**: La configuración de las conexiones de la aplicación Citrix Workspace puede reducir el ancho de banda que ICA requiere y, así, mejorar el rendimiento.
- **Cambie la forma en que se utiliza la aplicación Citrix Workspace**: Cambiar la forma en que se utiliza la aplicación Citrix Workspace 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 la aplicación Citrix Workspace para Linux y Citrix Virtual Apps and Desktops o Citrix DaaS**: Citrix aumenta y mejora constantemente el rendimiento en cada versión, y muchas funcionalidades de rendimiento requieren la versión más reciente de la aplicación Citrix Workspace y el software de servidor.

Pantalla

Pantalla partida

El problema de pantalla partida se produce cuando dos o más fotogramas distintos aparecen en pantalla al mismo tiempo, en bloques horizontales. Este problema se ve principalmente en áreas grandes de contenido que cambia rápidamente en la pantalla.

Se evita este artefacto cuando se capturan datos en el VDA. Este artefacto no se da cuando los datos se pasan al cliente. Sin embargo, X11 (el subsistema de gráficos de Linux/Unix) no proporciona una forma consistente de dibujar en la pantalla para evitar el artefacto.

Para evitar la pantalla partida, Citrix recomienda el enfoque estándar, que sincroniza el dibujo de la aplicación con el dibujo de la pantalla. Es decir, esperar a que `vsvnc` inicie el dibujo del fotograma siguiente. Según el hardware gráfico del cliente y el administrador de ventanas que utilice, están disponibles los dos grupos de soluciones siguientes para evitar que la pantalla se parta:

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

Parámetros de GPU de X11

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

```
Section "Device"

 Identifier    "Intel Graphics"
 Driver        "intel"
 Option        "AccelMethod" "sna"
 Option        "TearFree" "true"

 EndSection
```

Para gráficos de NVIDIA, busque en la carpeta xorg.conf.d el archivo que incluya 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 ejem-

> plo: /etc/X11/xorg.conf.d o /user/share/X11/xorg.conf.d.

Administradores de composición

Use lo siguiente:

- Compiz (integrado en Ubuntu Unity). Instale el administrador de parámetros “CompizConfig Settings Manager”.

  Ejecute “CompizConfig Settings Manager”.

  En **General** > **Composition**, desmarque la casilla **Undirect Fullscreen Windows**.

> **Nota:**
>
> Utilice “CompizConfig Settings Manager” con atención, 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 principal de Compton para ver todos los detalles. Por ejemplo, ejecute el comando:

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

Entradas de teclado incorrectas

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

Redibujado excesivo

Algunos administradores de ventanas informan continuamente de la posición nueva de las ventanas integradas 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

La aplicación Citrix Workspace crea iconos de ventanas que son compatibles con la mayoría de los administradores de ventanas. Sin embargo, estos iconos no son totalmente compatibles con la convención de comunicaciones entre clientes de X.

Compatibilidad total de iconos

Para ofrecer una compatibilidad total de iconos:

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

Color del 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 el archivo y ciérrelo.

Flash de color

Cuando mueva el puntero en una ventana de conexión, o fuera de ella, los colores de la ventana fuera de foco comienzan a parpadear. Este problema es una limitación conocida cuando se utiliza X Windows System con presentaciones en PseudoColor. De ser posible, utilice una profundidad de color mayor para la conexión afectada.

Cambios de color en presentaciones en color verdadero

Los usuarios tienen la opción de utilizar 256 colores cuando se conectan a un servidor. En esta opción se asume que el hardware del vídeo admite paletas, 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 este recurso es costosa en tiempo y en tráfico de red. Para reducir este coste, la aplicación Citrix Workspace almacena en búfer los cambios rápidos de la paleta y actualiza la paleta real solamente cada pocos segundos.

Pantalla incorrecta

La aplicación Citrix Workspace utiliza la codificación de caracteres EUC-JP o UTF-8 para los caracteres japoneses, mientras que el servidor utiliza la codificación de caracteres SJIS. La aplicación Citrix Workspace no traduce entre estos grupos de caracteres. Este problema puede provocar problemas de visualización de:

- Archivos que se guardan en el servidor y se ven localmente
- Archivos que se guardan 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.

Extensión de sesión

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 monitores adicionales.

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, admite varios monitores para los monitores intersecados.

> **Importante:**
>
> Span no tiene ningún efecto en sesiones de ventanas integradas o normales (incluidas aquellas sesiones 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`. Si `h` es el valor completo de la opción, wfica se cierra.

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

> **Precaución:**
>
> - No se recomienda usar esta opción. Debe considerarse como última opción y solo utilizarse con administradores de ventanas que presenten dificultades de uso.
> - El administrador de ventanas no ve la ventana de la sesión; además, la ventana no tiene icono y no se puede volver a apilar.
> - Solo se podrá quitar finalizando la sesión.

Si se especifica `a`, la aplicación Citrix Workspace intenta crear una sesión que cubra todos los monitores.

La aplicación Citrix Workspace supone que el resto del valor de la opción -span es una lista de números de monitores.

- Un solo valor selecciona un monitor específico.
- Si hay dos valores, se seleccionan los monitores de las esquinas superior izquierda e inferior derecha del área requerida.
- Si hay cuatro valores, se especifican los monitores de los bordes superior, inferior, izquierdo y derecho del área.

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

El siguiente comando se puede utilizar para probar la función del administrador de ventanas:
`xprop -root | grep \\_NET\\_WM\\_FULLSCREEN\\_MONITORS`

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

Para crear una sesión que abarque monitores adicionales 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\[,y,z\]\]\]
   ```

   Los valores w, x, y z son números de monitor del paso 1 de las etapas anteriores. El valor único w indica un monitor específico. Los valores w y x especifican los monitores de las esquinas superior izquierda e inferior derecha del área requerida. Los cuatro valores w, x, y y z especifican monitores en los bordes superior, inferior, izquierdo y derecho del área.

   > **Importante:**
   >
   > - Defina la variable WFICA_OPTS antes de iniciar el autoservicio a través de un explorador web. Para definir esta variable, modifique 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"
   >   ```


> - Este cambio afecta tanto a las sesiones de aplicaciones virtuales como a las de escritorios virtuales.
> - Si ha iniciado self-service o storebrowse, quite los procesos que se iniciaron para que la nueva variable de entorno surta efecto. Quítelos con:
>
> ```
> killall AuthManagerDaemon ServiceRecord storebrowse
> ```

Aplicaciones locales

Es posible que no pueda salir de una sesión a pantalla completa para utilizar aplicaciones locales u otras sesiones. Este problema 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.

Como solución temporal, 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. Esta solución temporal inhabilita la función de transparencia de teclado. Sin embargo, es posible que deba superditar el archivo ICA. Para ello, **agregue este parámetro** al archivo All_regions.ini.

Cámara web

Actualizar la cámara web predeterminada

Por ahora, la redirección de cámaras web en la aplicación Citrix Workspace para Linux solo admite una cámara web a la vez. La cámara web predeterminada seleccionada se asigna a la ruta del dispositivo `/dev/video0`, que es, generalmente, la cámara web integrada en equipos portátiles.

Para enumerar todos los dispositivos con funcionalidad de vídeo del sistema, debe instalar las herramientas v4l con el siguiente comando:

```
sudo apt-get install v4l-util
<!--NeedCopy-->
```

Enumere los dispositivos de vídeo con el siguiente comando:

```
v4l2-ctl --list-devices
<!--NeedCopy-->
```

Es posible que reciba un resultado como el siguiente:

```
user@user-pc:~ $ v4l2-ctl --list-devices
UVC Camera (046d:09a6) (usb-0000:00:14.0-1):
    /dev/video2
```



```
    /dev/video3
    /dev/media1
Integrated Camera: Integrated C (usb-0000:00:14.0-8):
    /dev/video0
    /dev/video1
    /dev/media0
<!--NeedCopy-->
```

Según el ejemplo anterior, hay dos cámaras web. Puede usar cualquiera de ellas. Citrix recomienda usar el primer índice. Hay un problema conocido con Ubuntu, por lo que es posible que aparezcan varios índices para una cámara web. En este ejemplo, puede usar /dev/video0 y /dev/video2.

Para configurar otra captura de vídeo como predeterminada, haga lo siguiente:

1. Vaya al archivo de configuración ~/.ICAClient/wfclient.ini y modifíquelo.
2. En la sección [WFClient], agregue este parámetro.

   HDXWebCamDevice=<device path>

Por ejemplo, agregue HDXWebCamDevice=/dev/video2 para configurar la cámara web asignada a /dev/video2 en un sistema.

Prestaciones para pruebas

En el cliente, el módulo de redirección de cámaras web se puede utilizar en varios modos para probar componentes aislados en las condiciones del entorno del cliente.

Modo de producción y depuración

Este modo compara la visualización de vídeo en el lado del VDA y los búferes reales que el codificador produce en el lado del cliente. Permite probar todo el proceso.

Para habilitar este modo:

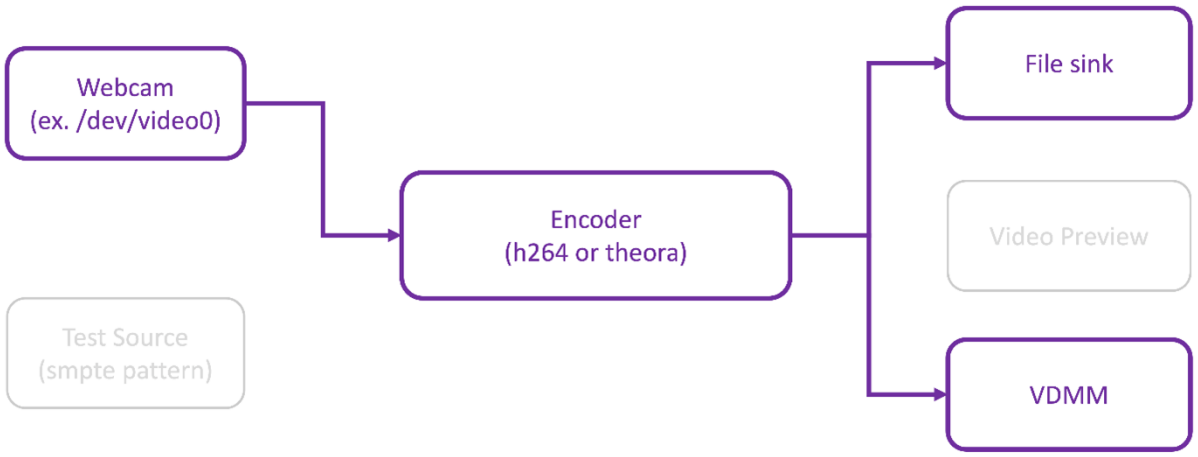
1. Vaya al archivo de configuración ~/.ICAClient/wfclient.ini y modifíquelo.
2. Establezca el valor de HDXWebcamDebug en **True**.

   HDXWebcamDebug = True

Una vez habilitado este modo, el codificador genera estos archivos con los búferes, según el codificador utilizado:

- Para el codificador H264: /tmp/file_mode_buffers.h264
- Para el codificador Theora: /tmp/file_mode_buffers.theora

Este diagrama describe el modo de producción y depuración:



Modo probador de cámaras web

Este modo le permite probar la cámara web aislada del resto de los elementos del proceso.

```
./gst_read --buffers | -b BUFFERS_AMOUNT  [ --input_device | -i
   WEBCAM_DEVICE; default=/dev/video0]
<!--NeedCopy-->
```

Para habilitar el modo probador de cámaras web, ejecute los siguientes comandos desde la línea de comandos:

```
   cd /opt/Citrix/ICAClient/util
   <!--NeedCopy-->
```

```
   `$./gst_read -b 100 /dev/video0
   <!--NeedCopy-->
```

Después de habilitar este modo, aparece una vista previa de vídeo y se crea este archivo con los búferes sin procesar de la cámara web:

/tmp/wewbcam_buffers.buff

El único cambio requerido para el modo probador de cámaras web son las opciones `--buffers (-b)`. También puede especificar el dispositivo de cámara web que quiere probar. Por ejemplo, observe lo siguiente:

- ./gst_read -buffers 150
- ./gst_read –buffers 100 –input_device /dev/video2

Este diagrama describe el modo probador de cámaras web:

Modo probador de codificadores

Este modo le permite probar el codificador aislado del proceso.

```
./gst_read --output_file | -o FILE_NAME [ --buffers | -b BUFFER_AMOUNT;
    default=10 0 ]  [ --enableH264  | -e ]
<!--NeedCopy-->
```

Para habilitar el modo probador de codificadores, ejecute los siguientes comandos desde la línea de comandos:

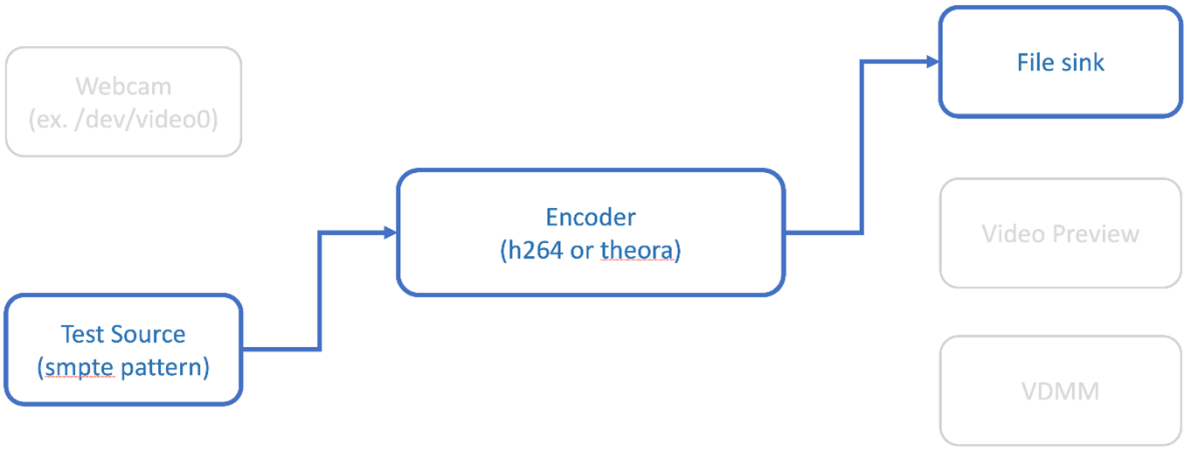
```
cd /opt/Citrix/ICAClient/util
<!--NeedCopy-->
```

```
./gst_read -o ~/file_buffers.h264 -e
 <!--NeedCopy-->
```

El único cambio requerido para este modo son las opciones `--output_file (-o)`. También puede probar los codificadores Theora o H264 y el búfer que se generaría. Por ejemplo, observe lo siguiente:

- For H264: ./gst_read –output_file ~/file_buffers.h264 –buffers 200 –enableH264
- For Theora: ./gst_read -o ~/file_buffers.theora -b 100

Este diagrama describe el modo probador de codificadores:



Codificador de software H264

Si el codificador H264 basado en software no funciona correctamente, debe verificar sus dependencias mediante estos pasos:

1. Verifique si el plug-in de `GStreamer` de x264 esté en el sistema como parte de `gstreamer-plugins-ugly`. Si está disponible en la biblioteca `libgstx264.so`, ejecute este comando para verificarlo:

```
gst-inspect-1.0 x264
<!--NeedCopy-->
```

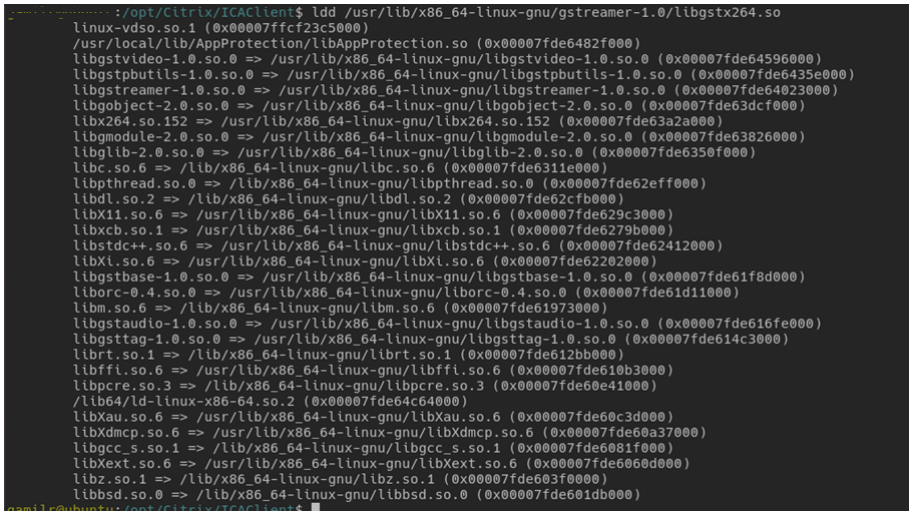
```
:/opt/Citrix/ICAClient$ gst-inspect-1.0 x264
Plugin Details:
  Name                     x264
  Description              libx264-based H264 plugins
  Filename                 /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
  Version                  1.14.5
  License                  GPL
  Source module            gst-plugins-ugly
  Source release date      2019-05-29
  Binary package           GStreamer Ugly Plugins (Ubuntu)
  Origin URL               https://launchpad.net/distros/ubuntu/+source/gst-plugins-ugly1.0

  x264enc: x264enc

  1 features:
  +-- 1 elements
```

2. Ejecute este comando para verificar las dependencias de la biblioteca `libgstx264.so`:

```
ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
<!--NeedCopy-->
```

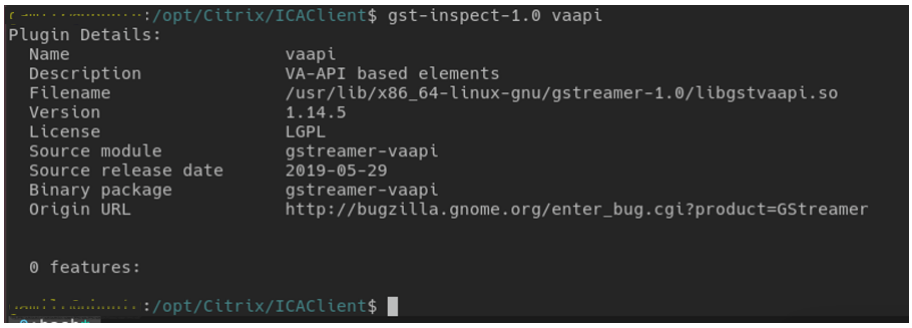
Si el archivo `libgstx264.so` no está presente, debe instalar los plug-ins “Ugly” de GStreamer con el siguiente comando:

```
sudo apt-get install gstreamer1
0-plugins-ugly
<!--NeedCopy-->
```

Codificador de hardware H264

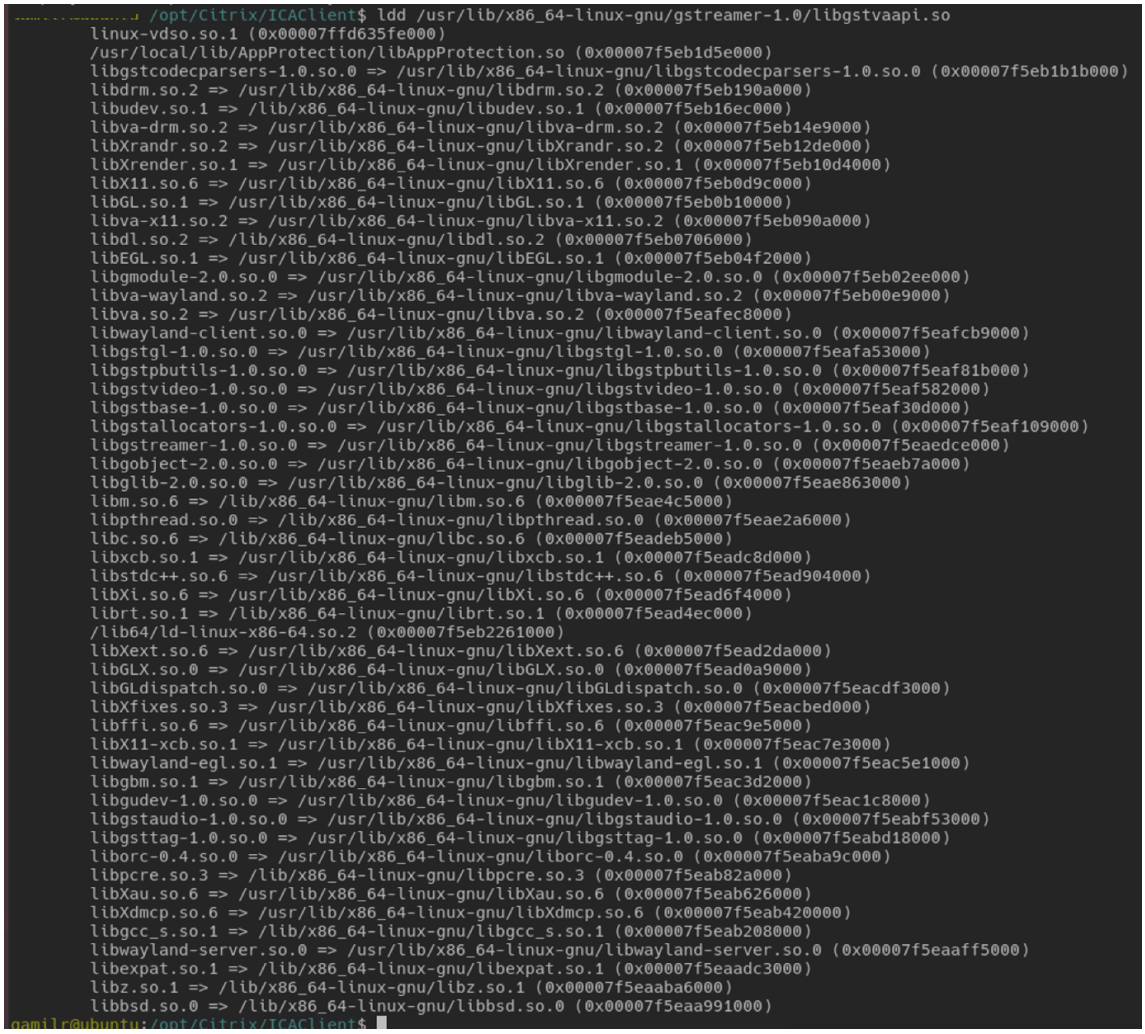
1. Verifique que el plug-in de `vaapi GStreamer` esté en el sistema como parte de `gstreamer1.0-vaapi`. Si está disponible en la biblioteca `libgstvaapi.so`, ejecute este comando para verificarlo:

   ```
   gst-inspect-1.0 vaapi
   <!--NeedCopy-->
   ```

2. Ejecute este comando para verificar las dependencias de la biblioteca libgstvaapi.so:

   ```
   ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
   <!--NeedCopy-->
   ```

3. Resuelva las dependencias que falten.

Para instalar y configurar `vaapi`, siga la guía de instalación de `GStreamer vappi`.

Recopilar marcos de trabajo GStreamer internos y registros de gst_read

Como alternativa a los registros de `ICAClient` normales, debe recopilar los registros del módulo `gst_read`.

Haga lo siguiente para recopilar los registros:

1. Abra un terminal y ejecute los siguientes comandos:

```
export GST_DEBUG=2, gst_read_debug:6
<!--NeedCopy-->
```

```
export GST_DEBUG_FILE=~/gst_read.log
<!--NeedCopy-->
```


> **Nota:**
>
> Esta variable establece el nivel de captura de registros y el archivo donde almacenarlos. En este caso, establecemos el nivel 2 para el marco de trabajo `GStreamer` y el nivel 7 para el módulo `gst_read`. Para obtener más información, consulte este documento. Solo se recomienda establecer niveles de error y advertencia para el marco de trabajo interno `GStreamer` y el nivel de registro para `gst_read`.

2. Descargue un archivo ICA de un VDA válido.
3. En el mismo terminal, ejecute este comando para iniciar una sesión de VDA:

```
cd /opt/Citrix/ICAClient
<!--NeedCopy-->
```

```
./wfica   <ICA file path>/vda.ica
<!--NeedCopy-->
```

El archivo `gst_read.log` se genera con el marco de trabajo interno `GStreamer` y los registros de `gst_read`.

Inspecciones de los procesos de GStreamer

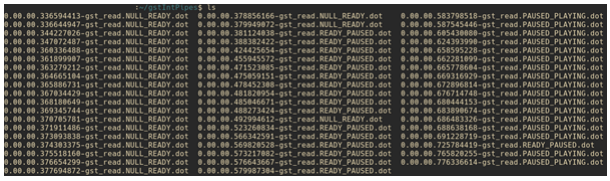
Para ver los procesos reales que crea el marco de trabajo `GStreamer`, haga lo siguiente:

1. Cree una carpeta para almacenar los archivos DOT. Por ejemplo: `gstIntPipes`.
2. Abra un terminal y exporte `GST_DEBUG_DUMP_DOT_DIR=<Absolute path>/gstIntPipes`. Esta variable indica dónde `GStreamer` almacena los archivos DOT.
3. Descargue un archivo ICA de un VDA válido.
4. En el mismo terminal, ejecute estos comandos para iniciar una sesión de VDA:

```
cd /opt/Citrix/ICAClient/
<!--NeedCopy-->
```

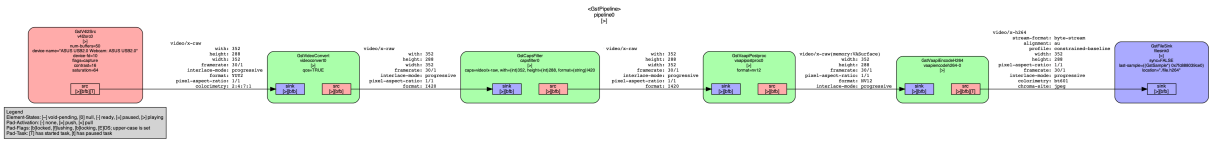
```
./wfica <ICA file path>/vda.ica
<!--NeedCopy-->
```

5. El directorio `gstIntPipes` incluye los archivos DOT. `GStreamer` genera un archivo DOT para cada cambio de estado en el proceso. Como resultado, puede inspeccionar todos los procesos creados. A continuación se muestra un ejemplo del conjunto de archivos DOT:

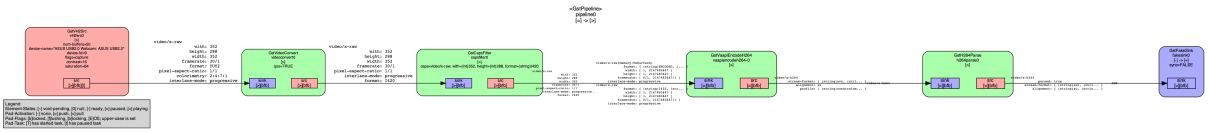


6. Instale una utilidad de archivos DOT para ver una representación visual de los procesos. Por ejemplo, Graphviz. Estas imágenes son ejemplos de un proceso bien y mal creado:

Proceso creado correctamente:



El proceso no se puede vincular:



> **Nota:**
>
> Para ampliar las imágenes anteriores o cualquier otra imagen, haga clic con el botón secundario en la imagen, seleccione **Open image in new tab** y amplíe la vista del explorador web según sea necesario.

Como se muestra en la imagen anterior, el segundo proceso no puede vincular el elemento `GstCapsFilter` y el elemento `GstVaapiEncodeH264`. Las prestaciones nunca se negocian por completo. Para obtener más información, consulte este documento.

Script de diagnóstico del sistema para la redirección de cámaras web

Proporcionamos un script, `helios_troubleshooting.sh`, para verificar si la configuración y las dependencias del sistema son adecuadas para admitir la redirección de cámaras web.

Haga lo siguiente para ejecutar el script:

1. Haga clic en helios_troubleshooting.sh para descargar el script.
2. Abra el terminal de su máquina Linux.
3. Escriba `helios_troubleshooting.sh --help` o `helios_troubleshooting.sh -h` para ver los argumentos de la línea de comandos compatibles.
4. Escriba una de estas opciones:
    - `helios_troubleshooting.sh -s` o `helios_troubleshooting.sh -static`: Use este comando para realizar una comprobación estática del archivo de configuración.

- `helios_troubleshooting.sh -d` o `helios_troubleshooting.sh -dynamic`: Use este comando para realizar una comprobación estática y dinámica, y comprobar la cámara web y los codificadores de un proceso de GStreamer.

Se muestran la configuración y las dependencias del sistema.

Explorador web

Explorador local

Al hacer clic en un enlace durante una sesión de Windows, el contenido aparece en un explorador local. La redirección de contenido servidor-cliente está habilitada en wfclient.ini. Esta redirección provoca que se ejecute una aplicación local. Para inhabilitar la redirección de contenido entre servidor y cliente, consulte Redirección de contenido servidor-cliente.

Acceso a los recursos publicados

Cuando accede a recursos publicados, el explorador le pide que guarde un archivo. Los exploradores web distintos de Firefox y Chrome pueden requerir cierta configuración para poder conectar con un recurso publicado. Sin embargo, al intentar acceder a un recurso con un clic en su icono en la página, el explorador web le solicitará guardar el archivo ICA.

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`.

Explorador Firefox

Cuando inicie escritorios o aplicaciones en Firefox, si la página no responde, pruebe a habilitar el plug-in ICA.

Plug-in ICA en Firefox

Cuando el plug-in ICA está habilitado en Firefox, es posible que no se inicien ni las sesiones de escritorio ni las sesiones de aplicación En este caso, pruebe a inhabilitar el plug-in ICA.

Errores de configuración

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 modificó incorrectamente o está dañado.

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

El archivo de configuración se modificó 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 modificado 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 base de datos de la conexión.

E_PNAGENT_FILE_UNREADABLE. No se puede leer el archivo Citrix Virtual Apps "…": No existe tal archivo o directorio.

O bien:

No se puede leer el archivo de Citrix Virtual Apps "…": permiso denegado.

Está intentando acceder a un recurso a través de un menú o un elemento de escritorio, pero el archivo de Citrix Virtual Apps and Desktops o Citrix DaaS 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 icono del escritorio o del elemento del menú.
- Compruebe el archivo de Citrix Virtual Apps and Desktops o Citrix DaaS al que hace referencia 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. De lo 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 este archivo 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 este archivo en el servidor o vuelva a configurar el explorador.

Error de detección de proxy: No se admite JavaScript.

Falta el archivo ejecutable PAC o el archivo de texto pac.js. Vuelva a instalar la aplicación Citrix Workspace.

Error de detección de proxy: Error de JavaScript.

El archivo PAC incluye JavaScript no válido. Corrija el archivo PAC en el servidor. Consulte también 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 este archivo en el servidor o vuelva a configurar el explorador.

Otros

Problemas de conexión

Es posible que también encuentre estos problemas.

Cerrar una sesión

Para saber si el servidor ha indicado a la aplicación Citrix Workspace que cierre una sesión, use el programa *wfica*. Este programa registra cuándo recibe un comando para finalizar la sesión desde el servidor.

Para grabar esta información en el sistema de syslog, agregue *SyslogThreshold* con el valor 6 a la sección [WFClient] del archivo de configuración. Este parámetro 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 tener *wfica*, envíe la información a la salida de "standard error" y agregue *PrintLogThreshold* con el valor 6 a la sección [WFClient]. El valor predeterminado de *PrintLogThreshold* es 0 (=LOG_EMERG).

Para obtener más información sobre cómo iniciar sesión, consulte Captura de registros y, para obtener más información sobre la configuración de syslog, consulte Configuración de Syslog.

Parámetros del archivo de configuración

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.

Aplicaciones publicadas

Si tiene problemas al ejecutar una aplicación publicada que accede a un puerto serie, es posible que 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 está bloqueando el puerto serie. En cuanto a bloqueos del tipo UUCP, puede que se haya dejado un archivo de bloqueo después de que la aplicación finalice. La ubicación de estos archivos de bloqueo depende del sistema operativo que utilice.

Inicio de la aplicación Citrix Workspace

Si la aplicación Citrix Workspace no se inicia, aparece el mensaje de error "Application default file could not be found or is out of date". Eso puede ocurrir porque la variable de entorno ICAROOT no se definió correctamente. Esta variable es un requisito si instaló la aplicación Citrix Workspace 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 está definida correctamente, intente iniciar la aplicación Citrix Workspace 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 la aplicación Citrix Workspace en la ubicación predeterminada. Para obtener más información sobre cómo instalar la aplicación Citrix Workspace, consulte Instalar y configurar.

  Si la aplicación Citrix Workspace se ha instalado anteriormente en la ubicación predeterminada, elimine el directorio `/opt/Citrix/ICAClient` o `$HOME/ICAClient/platform` antes de volver a instalarla.

Citrix CryptoKit (anteriormente, SSLSDK)

Para encontrar el número de versión de Citrix CryptoKit (anteriormente SSLSDK) o de OpenSSL que se está utilizando, puede utilizar este comando:

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

También puede ejecutar este comando en AuthManagerDaemon o en PrimaryAuthManager.

Teclas de acceso rápido

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. Este parámetro asigna la combinación de teclas local Alt+Ctrl+F1 en Alt+F1:
  - Cambie Hotkey1Shift=Ctrl+Mayús por Hotkey1Shift=Alt+Ctrl.
- El modo directo en el teclado envía todas las combinaciones de teclas directamente al servidor. 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.

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.

Teclado japonés

Para configurar el uso del teclado japonés, actualice esta entrada en el archivo de configuración wfclient.ini:

KeyboardLayout=Japanese (JIS)

Teclado ABNT2

Para configurar el uso del teclado ABNT2, actualice esta entrada en el archivo de configuración wfclient.ini:

KeyboardLayout=Brazilian (ABNT2)

Teclado local

Si algunas teclas del teclado local no funcionan de la manera prevista, elija la mejor distribución de servidores de la lista que hay en $ICAROOT/config/module.ini.

Reproductor de Windows Media

Es posible que la aplicación Citrix Workspace no tenga los plug-ins de GStreamer para gestionar un formato solicitado. Normalmente, este problema hace que el servidor solicite un formato distinto. Algunas veces, la comprobación inicial de plug-ins adecuados indica, incorrectamente, que sí existen. Este problema debería detectarse y muestra un cuadro de diálogo de error en el servidor para indicar que el Reproductor de Windows Media encontró un problema al reproducir el archivo. Reproducir el archivo de nuevo dentro de la sesión suele funcionar porque la aplicación Citrix Workspace rechaza el formato. Por eso, el servidor solicita otro formato u ofrece los medios él mismo.

En algunas circunstancias, el hecho de que no haya plug-ins adecuados no se detecta y el archivo no se reproduce correctamente, a pesar de que el indicador de progreso se mueve como es debido 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 autoservicio 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 al plug-in que falta, o el tipo MIME que debe 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. Este parámetro 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 es posible instalar un plug-in GStreamer para descifrarlo.

Configuración 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=device

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

LastComPortNum=2

ComPort1=device1

ComPort2=device2

Errores

Este tema incluye una lista de otros mensajes de error comunes que pueden aparecer al utilizar la aplicación Citrix Workspace.

Ha ocurrido un error. El código del error es 11 (E_MISSING_INI_SECTION). Consulte la documentación. Cerrándose.

Al ejecutar la aplicación Citrix Workspace desde la línea de comandos, este error normalmente significa que la descripción otorgada en la línea de comandos no se ha encontrado en el archivo appsrv.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.

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.

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 falten datos en estos archivos: "…".

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

Información de diagnóstico

Si tiene problemas con la aplicación Citrix Workspace, 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 la aplicación Citrix Workspace:

1. En el directorio de instalación, escriba util/lurdump. Se recomienda que haga esta modificación en una sesión abierta y, si es posible, mientras el problema siga activo.

   Se genera un archivo que ofrece información de diagnóstico detallada, la cual incluye detalles de la versión, el contenido de los archivos de configuración de la aplicación Citrix Workspace 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.

Solución de problemas en las conexiones con recursos

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

- Cerrar aplicaciones.
- Cerrar la sesión. Este paso finaliza la sesión y cierra todas las aplicaciones que hubiera abiertas.
- Desconectarse de una sesión. Este paso 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.

SDK y API

January 18, 2023

Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) admite la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para canales virtuales adicionales que usan el protocolo ICA.

Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores de Citrix Virtual Apps and Desktops o Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

Si quiere escribir controladores virtuales para otras plataformas cliente, póngase en contacto con el equipo de Asistencia técnica de Citrix.

El Virtual Channel SDK ofrece:

- La API para Citrix Virtual Driver (VDAPI), que se usa con las funciones de canal virtual en el SDK de WFAPI (Citrix Server API SDK) para crear nuevos canales virtuales. La función de canales virtuales proporcionada por VDAPI está diseñada para simplificar 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 WFAPI para escribir la parte del lado del servidor del canal virtual.

Para obtener más información, consulte Citrix Virtual Channel SDK para la aplicación Citrix Workspace para Linux.

Referencia de línea de comandos

Para obtener información sobre las referencias y los parámetros de la línea de comandos, consulte Referencia de comandos de la aplicación Citrix Workspace para Linux.

SDK de optimización de plataforma

Como parte de la iniciativa de HDX SoC para la aplicación Citrix Workspace para Linux, presentamos el "SDK de optimización de plataforma".

Este SDK permite un ecosistema de dispositivos de bajo coste, bajo consumo y alto rendimiento con factores de forma innovadores.

Los desarrolladores pueden usar el SDK de optimización de plataforma para mejorar el rendimiento de los dispositivos basados en Linux. Este SDK permite a los desarrolladores crear extensiones de plug-in para el componente del motor ICA (`wfica`) de la aplicación Citrix Workspace. Los plug-ins se crean como bibliotecas que se pueden compartir y `wfica` carga estas bibliotecas de forma dinámica.

Estos plug-ins pueden ayudarle a optimizar el rendimiento de los dispositivos Linux, mediante la habilitación de las siguientes funciones:

- Proporcionar la descodificación acelerada de datos JPEG y H.264 que se utilizan para dibujar la imagen de la sesión
- Controlar la asignación de memoria utilizada para dibujar la imagen de la sesión
- Mejorar el rendimiento, tomando el control del dibujo de bajo nivel de la imagen de la sesión
- Proporcionar servicios de salida de gráficos y entradas de usuario para entornos de sistema operativo que no admiten X11

Para obtener más información, consulte Aplicación Citrix Workspace para Linux - Platform Optimization SDK.

Referencia para parámetros ICA

January 18, 2023

En el archivo de referencia para parámetros ICA se ofrecen listas de parámetros de Registro y parámetros de archivos ICA, lo que permite a los administradores personalizar el comportamiento de la aplicación Citrix Workspace. También puede usar la Referencia para parámetros ICA a fin de solucionar problemas relacionados con un comportamiento inesperado de la aplicación Citrix Workspace.

Referencia para parámetros ICA (descarga en PDF)

