

Guía de instalación y configuración de VMware Horizon Client para Linux

Marzo de 2020

VMware Horizon Client for Linux 5.4

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

<https://docs.vmware.com/es/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2012-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Guía de instalación y configuración de VMware Horizon Client para Linux 6

1 Requisitos del sistema 7

- Requisitos del sistema para sistemas cliente Linux 7
- Requisitos del sistema para las funciones de Horizon Client 9
 - Requisitos para la autenticación con tarjetas inteligentes 9
 - Requisitos del sistema para el redireccionamiento del puerto serie 12
 - Requisitos para usar Redireccionamiento de contenido URL 13
 - Requisitos del sistema para la función Audio/vídeo en tiempo real 14
 - Requisitos del sistema para la función de redireccionamiento del escáner 15
 - Requisitos del sistema para el redireccionamiento multimedia (MMR) 16
 - Requisitos para usar el redireccionamiento URL de Flash 18
 - Requisitos del sistema para el redireccionamiento multimedia HTML5 19
 - Requisitos de la función Session Collaboration 20
- Requisitos para usar Skype Empresarial con Horizon Client 21
- Sistemas operativos del escritorio compatibles 21

2 Instalación 23

- Preparar el servidor de conexión para Horizon Client 23
- Opciones de instalación 25
- Instalar o actualizar Horizon Client para Linux desde la página de descargas de productos de VMware 28
 - Opciones de instalación de la línea de comandos del cliente Linux 30
 - Habilitar la función de impresión virtual en un cliente Linux 33

3 Configurar Horizon Client para usuarios finales 35

- Opciones de configuración comunes 35
- Utilizar los archivos de configuración y la interfaz de línea de comandos de vmware-view 36
 - Opciones de la línea de comandos y configuración de Horizon Client 37
- Utilizar URI para configurar Horizon Client 57
 - Sintaxis para crear URI de vmware-view 57
 - Ejemplos de URI vmware-view 61
- Configurar las opciones de VMware Blast 64
- Configurar el uso compartido de datos de Horizon Client 66
 - Datos de Horizon Client recopilados por VMware 67
- Configurar el modo de comprobación de certificados para usuarios finales 69
- Configurar las opciones de TLS avanzadas 70
- Configurar teclas específicas y combinaciones de teclas para enviarlas al sistema local 71

- Utilizar FreeRDP para las conexiones RDP 73
 - Instalar y configurar FreeRDP 75
- Habilitar el modo compatible con FIPS 76
- Configurar la caché de imágenes del lado del cliente PCoIP 77

4 Administrar las conexiones de las aplicaciones publicadas y los escritorios remotos 79

- Conectarse a una aplicación publicada o a un escritorio remoto 79
- Conectarse a aplicaciones públicas mediante acceso sin autenticar 82
- Compartir el acceso a unidades y carpetas locales con el Redireccionamiento de unidades cliente 83
 - Compartir carpetas editando un archivo de configuración 86
- Configurar el modo de comprobación del certificado en Horizon Client 86
- Cambiar los escritorios remotos o las aplicaciones publicadas 88
- Cerrar sesión o desconectarse 89

5 Utilizar una aplicación o un escritorio de Microsoft Windows en un sistema Linux 90

- Matriz de compatibilidad de funciones para clientes Linux 90
- Idiomas admitidos 94
- Teclados y monitores 94
 - Utilizar la función Ajuste de escala de la pantalla 97
 - Usar la sincronización PPP 98
 - Seleccionar monitores específicos para mostrar las aplicaciones publicadas 99
 - Configurar la sincronización de las teclas de bloqueo 100
- Mejorar el rendimiento del mouse en escritorios remotos 101
- Uso del redireccionamiento USB para conectar dispositivos USB 102
 - Limitaciones del redireccionamiento USB 105
- Usar el redireccionamiento del puerto serie 106
- Usar escáneres 108
- Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos 110
 - Cuándo se puede utilizar una cámara web con la función Audio/vídeo en tiempo real 110
 - Seleccionar un micrófono predeterminado en un sistema cliente Linux 111
 - Seleccionar una cámara web o un micrófono preferidos en un sistema cliente Linux 112
- Usar la función de redireccionamiento de contenido URL 115
- Compartir sesiones de escritorios remotos 116
 - Invitar a un usuario a que se una a una sesión de escritorio remoto 116
 - Administrar una sesión de escritorio remoto compartida 118
 - Unirse a una sesión de escritorio remoto 119
- Usar varias sesiones de una aplicación publicada desde dispositivos cliente diferentes 121
- Usar la función de aplicación remota 121
- Guardar documentos en una aplicación publicada 122

Imprimir desde un escritorio remoto	122
Establecer las preferencias de impresión para la función de impresión virtual	122
Establecer las preferencias de impresión para la función VMware Integrated Printing	124
Imprimir desde un escritorio remoto a una impresora USB local	125
Copiar y pegar texto	126
Configurar el tamaño de la memoria del portapapeles cliente	126
Registrar la actividad de copiar y pegar	127
6 Configurar el redireccionamiento USB en el cliente	129
Requisitos del sistema para la función de redireccionamiento USB	129
Archivos de registro específicos de dispositivos USB	129
Establecer las propiedades de configuración USB	130
Familias de dispositivos USB	135
7 Solucionar problemas relacionados con Horizon Client	137
Reiniciar un escritorio remoto	137
Restablecer aplicaciones publicadas o escritorios remotos	138
Desinstalar Horizon Client para Linux	139
Recopilar información de registro de Horizon Client	140
Problemas con la entrada de teclado	141
Conexión a un servidor en el modo Workspace ONE	141

Guía de instalación y configuración de VMware Horizon Client para Linux

Este documento, *Guía de instalación y configuración de VMware Horizon Client para Linux*, proporciona información sobre cómo instalar, configurar y utilizar el software VMware Horizon[®] Client[™] en un sistema cliente Linux.

Este documento incluye información sobre los requisitos del sistema e instrucciones para instalar y usar Horizon Client para Linux.

Nota Este documento no incluye instrucciones para instalar el sistema operativo Linux en un sistema cliente. Para obtener más información sobre la instalación de Linux, consulte las instrucciones del fabricante de su distribución Linux.

Esta información está destinada a administradores que deban configurar una implementación de Horizon que incluya sistemas cliente Linux. La información está destinada a administradores de sistemas con experiencia, que estén familiarizados con la tecnología de máquinas virtuales y operaciones de centros de datos.

Nota Este documento se aplica a la mayoría de Horizon Client para Linux de VMware. Además, varios partners de VMware ofrecen dispositivos de cliente ligero y cero para implementaciones de Horizon. El proveedor determina las funciones que están disponibles para cada dispositivo cliente ligero o cero y los sistemas operativos admitidos (el modelo y la configuración que una empresa elije usar). Para obtener más información acerca de los proveedores y los modelos de estos dispositivos cliente, consulte la [Guía de compatibilidad de VMware](#) en el sitio web de VMware.

Requisitos del sistema

1

Los sistemas cliente deben cumplir ciertos requisitos de software y hardware.

Este capítulo incluye los siguientes temas:

- [Requisitos del sistema para sistemas cliente Linux](#)
- [Requisitos del sistema para las funciones de Horizon Client](#)
- [Requisitos para usar Skype Empresarial con Horizon Client](#)
- [Sistemas operativos del escritorio compatibles](#)

Requisitos del sistema para sistemas cliente Linux

El dispositivo Linux en el que instala Horizon Client y los periféricos que usa deben cumplir ciertas configuraciones del sistema que VMware probó y soporta oficialmente.

Nota Estos requisitos del sistema se aplican a Horizon Client para Linux de VMware. Además, varios partners de VMware ofrecen dispositivos de cliente ligero y cero para implementaciones de Horizon 7. El proveedor y el modelo de cada dispositivo cliente ligero o cero y la configuración que decide usar una empresa determinan las características que estarán disponibles en cada dispositivo cliente y los sistemas operativos admitidos. Para obtener más información acerca de los proveedores y los modelos de estos dispositivos cliente, consulte la [Guía de compatibilidad de VMware](#) en el sitio web de VMware.

Arquitectura

i386, x86_64 y ARM

Memoria

Al menos 2 GB de RAM

Sistema operativo

Horizon Client para Linux se probó en los siguientes sistemas operativos para esta versión.

Sistema operativo	Versión
Ubuntu de 32 bits	16.04
Ubuntu de 64 bits	16.04, 18.04
Red Hat Enterprise Linux (RHEL) de 64 bits	7.7, 8

Nota En los sistemas RHEL 8, Horizon Client solo admite el protocolo de servidor de visualización X11. No se admite el protocolo de servidor de visualización Wayland.

Requisito de OpenSSL

Horizon Client necesita una versión específica de OpenSSL. La versión correcta se descarga y se instala de forma automática.

Servidor de conexión de Horizon, servidor de seguridad y Horizon Agent

Versión de mantenimiento más reciente de Horizon 6.2.x y versiones posteriores

Si los sistemas cliente se conectan desde fuera del firewall corporativo, es recomendable utilizar un servidor de seguridad. Con un servidor de seguridad, los sistemas cliente no necesitan una conexión VPN.

Protocolo de visualización

- VMware Blast (requiere Horizon Agent 7.0 o una versión posterior)
- PCoIP
- RDP

Resolución de pantalla en el sistema cliente

Mínima: 1024 x 768 píxeles

Requisitos de hardware para VMware Blast y PCoIP

- Procesador basado en x86 o x64 con extensiones SSE2 y una velocidad de procesador igual o superior a 800 MHz
- RAM disponible superior a la que se indica en los requisitos del sistema para admitir varias configuraciones de monitor. Utilice la siguiente fórmula como guía general:

$$20 \text{ MB} + (24 * (\# \text{ monitors}) * (\text{monitor width}) * (\text{monitor height}))$$

Como guía general, puede utilizar los siguientes cálculos:

```
1 monitor: 1600 x 1200: 64 MB
2 monitors: 1600 x 1200: 128 MB
3 monitors: 1600 x 1200: 256 MB
```


Requisitos de hardware para RDP

- Procesador basado en x86 o x64 con extensiones SSE2 y una velocidad de procesador igual o superior a 800 MHz
- 128 MB de RAM

Requisitos de software para Microsoft RDP

Utilice la versión disponible de rdesktop más actualizada.

Requisitos de software para FreeRDP

Si tiene previsto utilizar una conexión RDP a escritorios de Horizon y prefiere usar un cliente FreeRDP para la conexión, deberá instalar la versión correcta de FreeRDP y las revisiones correspondientes. Consulte [Instalar y configurar FreeRDP](#).

Otros requisitos de software

Horizon Client también tiene otros requisitos de software en función de la distribución Linux que utilice. Permita el asistente de instalación de Horizon Client para buscar dependencias y compatibilidades de bibliotecas en su sistema. La siguiente lista de requisitos solo se aplica a las distribuciones Ubuntu.

- `libudev.so.0`

Nota A partir de Horizon Client 4.2, se requiere `libudev0` para ejecutar Horizon Client. De forma predeterminada, `libudev0` no está instalado en algunos sistemas.

- Para admitir los tiempos de espera de las sesiones inactivas: `libXsso.so.1`.
- Para admitir el redireccionamiento de URL Flash: `libexpat.so.1`. El archivo `libexpat.so.0` ya no es necesario.
- Para mejorar el rendimiento a la hora de utilizar varios monitores, habilite Xinerama.

Requisitos del sistema para las funciones de Horizon Client

Las funciones de Horizon Client tienen requisitos específicos de hardware y de software.

Requisitos para la autenticación con tarjetas inteligentes

Los dispositivos cliente que utilizan una tarjeta inteligente para la autenticación del usuario deben cumplir ciertos requisitos.

Requisitos de hardware y de software del cliente

Cada dispositivo cliente que utilice una tarjeta inteligente para la autenticación del usuario debe contar con el software y el hardware especificados a continuación.

- Horizon Client
- Lector de tarjeta inteligente compatible

- Controlador del lector de tarjeta inteligente
- Controlador de tarjeta inteligente
- Controladores de aplicaciones específicos para el producto

Los usuarios que se autentican con tarjetas inteligentes deben usar un tipo de tarjeta inteligente compatible con el middleware correspondiente, tal como se describe en la siguiente sección. Cada tarjeta inteligente también debe contener un certificado de usuario.

Requisitos para el middleware y el tipo de tarjeta inteligente

Horizon Client es compatible con las siguientes combinaciones de tarjetas inteligentes y middleware de tarjeta inteligente.

Tipo de tarjeta inteligente	Fabricante	Middleware del cliente	Middleware del agente
Tarjeta de verificación de identidad personal (PIV)	NIST	Módulo PKCS11 de OpenSC	ActivClient 7.x
Tarjeta IDprime .NET	Gemalto	Biblioteca Gemalto .NET PKCS11 (libgtop11dotnet.so)	Minicontrolador Gemalto .NET

Requisitos de software para aplicaciones publicadas y escritorios remotos

Un administrador de Horizon debe instalar controladores de aplicaciones específicos para cada producto en el host RDS o en los escritorios virtuales.

Habilitar el cuadro de texto de sugerencia de nombre de usuario en Horizon Client

En algunos entornos, los usuarios pueden usar un certificado de tarjeta inteligente único para autenticar varias cuentas de usuario. Los usuarios escriben su nombre en el cuadro de texto **Sugerencia de nombre de usuario** cuando inician sesión con una tarjeta inteligente.

Para que el cuadro de texto **Sugerencia de nombre de usuario** aparezca en el cuadro de diálogo de inicio de sesión de Horizon Client, debe habilitar la función de sugerencia del nombre de usuario de la tarjeta inteligente en el servidor de conexión. Dicha función es compatible únicamente con servidores y agentes con Horizon 7 versiones 7.0.2 y posteriores. Para obtener más información sobre cómo habilitar la función de sugerencias de nombre de usuario de la tarjeta inteligente, consulte el documento *Administración de VMware Horizon Console*.

Si el entorno usa un dispositivo Unified Access Gateway en lugar de un servidor de seguridad para el acceso externo seguro, debe configurar el dispositivo Unified Access Gateway para que admita la función de sugerencias de nombre de usuario de la tarjeta inteligente. Dicha función es compatible únicamente con Unified Access Gateway 2.7.2 y versiones posteriores. Para obtener más información sobre cómo habilitar la función de sugerencias de nombre de usuario de la tarjeta inteligente en Unified Access Gateway, consulte el documento *Implementación y configuración de Unified Access Gateway*.

Horizon Client sigue admitiendo certificados de tarjetas inteligentes de una cuenta única, aunque la función de sugerencias de nombre de usuario de la tarjeta inteligente está habilitada.

Requisitos adicionales para la autenticación con tarjetas inteligentes

Además de cumplir los requisitos de las tarjetas inteligentes en los sistemas Horizon Client, otros componentes de Horizon deben cumplir ciertos requisitos de configuración para ser compatibles con las tarjetas inteligentes.

Servidor de conexión y hosts del servidor de seguridad

Un administrador debe agregar todos los certificados de entidad de certificación (CA) aplicables a todos los certificados de usuario de confianza en un archivo del almacén de confianza del servidor en el servidor de conexión o en el host del servidor de seguridad. Estos certificados incluyen certificados raíz y, si una entidad de certificación intermedia expide el certificado de tarjeta inteligente del usuario, también se deben incluir los certificados intermedios.

Para obtener más información sobre cómo configurar el servidor de conexión de forma que admita el uso de tarjetas inteligentes, consulte el documento *Administración de VMware Horizon Console*.

Active Directory

Para obtener más información sobre las tareas que puede que tengan que llevar a cabo los administradores en Active Directory para implementar la autenticación con tarjeta inteligente, consulte el documento *Administración de VMware Horizon Console*.

Configurar Horizon Client para la autenticación con tarjeta inteligente

Puede realizar una configuración en varios pasos para utilizar una tarjeta inteligente en Horizon Client.

Requisitos previos

- Instale Horizon Client.
- (Opcional) Para que el campo **Sugerencia de nombre de usuario** aparezca en el cuadro de diálogo de inicio de sesión de Horizon Client, habilite la función de sugerencia del nombre de usuario de la tarjeta inteligente en el servidor de conexión. Para obtener más información, consulte el apartado sobre cómo configurar la autenticación con tarjeta inteligente en el documento *Administración de VMware Horizon Console*.

Procedimiento

- 1 Cree la carpeta `/usr/lib/vmware/view/pkcs11`.

- 2 Cree un vínculo simbólico a la biblioteca pkcs11, que se utiliza para la autenticación con tarjeta inteligente.

Por ejemplo, ejecute el siguiente comando:

```
sudo ln -s /usr/lib64/pkcs11/opensc-pkcs11.so
        /usr/lib/vmware/view/pkcs11/libopenscpkcs11.so
```

Nota Asegúrese de que el nombre del vínculo simbólico de la biblioteca opensc-pkcs11 comienza por lib.

Requisitos del sistema para el redireccionamiento del puerto serie

Con la función de redireccionamiento del puerto serie, los usuarios finales pueden redireccionar puertos serie (/dev/ttyS) conectados de forma local, como puertos RS232 integrados o adaptadores de USB a puertos serie, a sus escritorios remotos. Para admitir el redireccionamiento del puerto serie, la implementación de Horizon debe cumplir ciertos requisitos de software y hardware.

Escritorios publicados en hosts RDS

El host RDS que aloja escritorios publicados debe tener instalado Horizon Agent 7.6 o una versión posterior con la opción Redireccionamiento de puerto serie seleccionada. De manera predeterminada, esta opción de configuración no está seleccionada.

Los escritorios publicados admiten los siguientes sistemas operativos.

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

No es necesario instalar los controladores de los dispositivos del puerto serie en el host RDS.

Escritorios virtuales

Los escritorios virtuales deben tener instalado Horizon Agent 7.9 o una versión posterior con la opción de configuración Redireccionamiento de puerto serie seleccionada. De manera predeterminada, esta opción de configuración no está seleccionada.

Los escritorios virtuales admiten los siguientes sistemas operativos.

- Windows 7
- Windows 10

No es necesario instalar los controladores de los dispositivos del puerto serie en escritorio virtuales.

Equipo con Horizon Client o dispositivo de acceso del cliente

Se puede usar la función de redireccionamiento del puerto serie en los sistemas Linux que se admiten en esta versión. Los controladores del puerto serie necesarios deben estar

instalados y este puerto debe estar operativo. El redireccionamiento del puerto serie está disponible en Horizon Client 4.9 y versiones posteriores.

Sesiones anidadas

La función Redireccionamiento de puerto serie se admite en aplicaciones publicadas que se inician desde Horizon Client en escritorios publicados (sesiones anidadas). Horizon Client 4.10 o una versión posterior debe estar instalado en los escritorios publicados.

La función Redireccionamiento de puerto serie tiene las siguientes limitaciones cuando se utiliza en una sesión anidada.

- El número de usuarios simultáneos es limitado.
- Los usuarios deben usar versiones coincidentes de cliente y agente (por ejemplo, Horizon Client 5.1 y Horizon Agent 7.9).

Protocolos de visualización

- VMware Blast (requiere Horizon Agent 7.0 o una versión posterior)
- PCoIP (requiere Horizon Agent 7.9 o versiones posteriores)

Requisitos para usar Redireccionamiento de contenido URL

Gracias a la función Redireccionamiento de contenido URL, es posible redireccionar el contenido URL de un equipo cliente a una aplicación publicada o un escritorio remoto (redireccionamiento de cliente a agente), o bien de una aplicación publicada o un escritorio remoto al equipo cliente (redireccionamiento de agente a cliente).

Por ejemplo, un usuario final puede hacer clic en un vínculo en el navegador Firefox nativo del cliente y que se abra en el navegador Internet Explorer remoto, o bien puede hacer clic en un vínculo en navegador Internet Explorer remoto y que se abra en el navegador Firefox nativo de la máquina cliente. Se puede configurar un amplio número de protocolos para el redireccionamiento, entre los que se incluyen HTTP, mailto y callto.

Navegadores web

Puede escribir una URL o hacer clic en ella en los siguientes navegadores y redireccionar esa URL.

- Firefox 50.0 o posterior

Sistema cliente

Para usar la función Redireccionamiento de contenido URL con el navegador Firefox, debe habilitar la extensión de redireccionamiento URL de VMware Horizon para Firefox. Para obtener información, consulte el tema "Instalar y habilitar la extensión de redireccionamiento de URL de VMware Horizon para Firefox en Linux" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

La primera vez que se redirija una URL desde el navegador Firefox en el cliente Linux, se le solicitará al usuario que abra la URL en Horizon Client. El usuario deberá seleccionar

VMware Horizon Client y hacer clic en **Abrir vínculo**, o no se producirá el redireccionamiento de URL. Si selecciona la casilla **Recordar mi elección para todos los vínculos de vmware-view** (opción recomendada), este mensaje no volverá a aparecer.

Escritorio remoto o aplicación publicada

Un administrador de Horizon debe habilitar el Redireccionamiento de contenido URL si Horizon Agent está instalado. Para obtener más información, consulte los documentos *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

El administrador de Horizon también debe configurar las opciones que especifican cómo Horizon Client redirecciona el contenido URL del cliente a una aplicación publicada o un escritorio remoto, o bien cómo Horizon Agent redirecciona el contenido URL de una aplicación publicada o un escritorio remoto al cliente. Para obtener toda la información, consulte el tema sobre cómo configurar el redireccionamiento de contenido URL en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Requisitos del sistema para la función Audio/vídeo en tiempo real

Audio/vídeo en tiempo real funciona con dispositivos de audio analógicos, dispositivos de audio USB y cámaras web estándar. La función también funciona con aplicaciones de conferencias estándar. Para que esta función sea compatible, la implementación de Horizon debe cumplir ciertos requisitos de software y hardware.

Escritorios virtuales

Para utilizar la función Audio/vídeo en tiempo real con escritorios virtuales, se debe instalar View Agent 6.2.x o una versión posterior, o bien Horizon Agent 7.0 o una versión posterior.

Si se utiliza Microsoft Teams con Audio/vídeo en tiempo real, VMware recomienda que los escritorios virtuales tengan un mínimo de 4 vCPU y 4 GB de RAM.

Aplicaciones y escritorios publicados

Para usar la función Audio/vídeo en tiempo real con las aplicaciones y los escritorios publicados, Horizon Agent 7.0.2 o una versión posterior debe estar instalado en el host RDS.

Equipo con Horizon Client o dispositivo de acceso del cliente

- La función Audio/vídeo en tiempo real es compatible con los dispositivos x86 y x64. Esta función no es compatible con procesadores ARM. El sistema cliente debe cumplir los requisitos mínimos de hardware que se indican a continuación.

Resolución	Velocidad de fotogramas	CPU	Memoria necesaria
320 x 240	15 FPS	2 núcleos, 1800 MHz	105 MB
640 x 480	15 FPS	2 núcleos, 2700 MHz	150 MB
1280 x 720	15 FPS	4 núcleos, 3400 MHz	210 MB

- Horizon Client necesita las siguientes bibliotecas:
 - Video4Linux2
 - libv4l
 - Pulse Audio

El archivo de complemento (/usr/lib/pcoip/vchan_plugins/libviewMMDevRedir.so) tiene las siguientes dependencias:

```
libuuid.so.1
libv4l2.so.0
libspeex.so.1
libudev0
libtheoradec.so.1
libtheoraenc.so.1
libv4lconvert.so.0
libjpeg.so.8
```

Todos estos archivos deben encontrarse en el sistema cliente. De lo contrario, la función Audio/vídeo en tiempo real no funcionará. Tenga en cuenta que estas dependencias complementan a las que se necesitan para el propio Horizon Client.

- Los controladores del dispositivo de audio y de cámara web deben estar instalados, y el dispositivo de audio y de cámara web debe estar operativo en el equipo cliente. No es necesario que instale los controladores del dispositivo en la máquina donde está instalado el agente.

Protocolos de visualización

- PCoIP
- VMware Blast (requiere Horizon Agent 7.0 o una versión posterior)

Requisitos del sistema para la función de redireccionamiento del escáner

Los usuarios finales pueden escanear información en los escritorios remotos con escáneres conectados a los sistemas cliente locales. Pueden controlar la configuración del escáner mediante las opciones de la interfaz del escritorio remoto. Para usar esta función, los escritorios remotos y los equipos cliente deben cumplir ciertos requisitos de sistema.

Escritorios remotos

Los escritorios remotos deben tener instalado Horizon Agent 7.8 o versiones posteriores, con la opción de configuración Redireccionamiento del escáner, en las máquinas virtuales de plantilla o principal o los hosts RDS. En escritorios Windows y sistemas operativos invitados Windows Server, la opción de configuración Redireccionamiento del escáner de Horizon Agent no está seleccionada de forma predeterminada.

Para obtener más información sobre los sistemas operativos invitados que pueden utilizarse con escritorios virtuales y con hosts RDS, así como para obtener información sobre la configuración del redireccionamiento del escáner en escritorios remotos, consulte "Configurar Redireccionamiento de escáner" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Equipo con Horizon Client o dispositivo de acceso del cliente

El equipo cliente debe estar conectado a un escáner compatible con el estándar de interfaz de escáneres SANE. Los controladores del escáner SANE deben estar instalados y este dispositivo debe estar operativo en el equipo cliente. No es necesario que instale los controladores del escáner en el sistema operativo del escritorio remoto donde está instalado el agente.

Estándar del escáner

SANE

Protocolos de visualización

- PCoIP
- VMware Blast

El redireccionamiento del escáner no se admite en las sesiones de escritorio RDP.

Requisitos del sistema para el redireccionamiento multimedia (MMR)

Con el redireccionamiento multimedia (MMR), la transmisión multimedia se descodifica en el sistema cliente. El sistema cliente reproduce el contenido multimedia, por lo que reduce la carga en el host ESXi.

Escritorios remotos

- Los escritorios virtuales deben tener instalado View Agent 6.2.X o Horizon Agent 7.0 (o versiones posteriores).
- Los escritorios publicados deben tener instalados en el host RDS View Agent 6.2.x o Horizon Agent 7.0 (o versiones posteriores).

Para obtener más información sobre los requisitos del sistema operativo y otros requisitos de software, así como las opciones de configuración, consulte los temas sobre Redireccionamiento multimedia de Windows Media en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Equipo con Horizon Client o dispositivo de acceso del cliente

Como MMR descarga el procesamiento multimedia del servidor al cliente, este último debe tener los siguientes requisitos mínimos de hardware.

Procesador:	Intel Pentium 4 o AMD Athlon de doble núcleo
Velocidad del procesador:	1.5 GHz para uso común o 1.8 GHz para Full HD

Memoria: 2 GB de RAM

Adaptador de vídeo: Hardware acelerado

Debe instalar una de las siguientes bibliotecas para evitar problemas relacionados con la reproducción de vídeos:

- Biblioteca GStreamer core library y gstreamer-ffmpeg 0.10
- Biblioteca de núcleo de GStreamer y fluendo 0.10

En clientes ligeros Dell Wyse, es posible que la reproducción de vídeos no funcione en la biblioteca fluendo preinstalada. Para resolver este problema, póngase en contacto con el soporte técnico de Dell para obtener la última versión de la biblioteca fluendo.

Formatos de medios compatibles

Formatos de medios que admite Windows Media Player; por ejemplo: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8 y 9; WMA; AVI; ACE; MP3; WAV.

La versión 7.9 y posteriores de Horizon 7 admiten MMS y RTSP.

El formato MP3 no es compatible cuando se utiliza MMS y RTSP.

Nota El contenido protegido con DRM no se redirige a través de MMR de Windows Media.

Marco de GStreamer

Configure el entorno de GStreamer de manera que el marco se componga de la tarjeta gráfica, de la API de aceleración de hardware y del complemento de GStreamer que permite el correcto funcionamiento de GStreamer. [Tabla 1-1. Configuración del marco de GStreamer](#) muestra las diferentes combinaciones de opciones posibles. Para obtener el mejor entorno posible, configure el entorno de GStreamer siguiendo la información de [Tabla 1-1. Configuración del marco de GStreamer](#) para las tarjetas gráficas Intel y NVIDIA.

Tabla 1-1. Configuración del marco de GStreamer

Tarjeta gráfica (con controlador)	API de aceleración de hardware	Complemento de GStreamer
NVIDIA	VDP AU (libvdpau.so)	vdpau
Intel	VA API (libvaapi.so)	gstreamer-vaapi
--	OpenMax	gst-omx
--	DCE	gstreamer-ducati
AMD	OVD/UVD	No disponible

Para obtener información más detallada, consulte <https://gstreamer.freedesktop.org/documentation/tutorials/playback/hardware-accelerated-video-decoding.html>.

MMR no está habilitado de forma predeterminada. Para habilitarlo, debe establecer la opción de configuración `view.enableMMR`. Si desea obtener más información, consulte [Opciones de la línea de comandos y configuración de Horizon Client](#).

Requisitos para usar el redireccionamiento URL de Flash

Al enviar el contenido Flash directamente desde Adobe Media Server a endpoints cliente, disminuye la carga en el host ESXi del centro de datos y se elimina el enrutamiento adicional de dicho centro, además de reducir el ancho de banda necesario para transmitir al mismo tiempo vídeos en directo a varios endpoints cliente.

La función de redireccionamiento URL de Flash usa un script JavaScript que el administrador de una página web incrustó en la misma. Cuando un usuario del escritorio remoto haga clic en el vínculo URL designado desde una página web, el script intercepta y realiza un redireccionamiento de ShockWave File (SWF) desde la sesión del escritorio remoto al endpoint cliente. A continuación, el endpoint abre un VMware Flash Projector local fuera de la sesión del escritorio virtual y reproduce la secuencia de medios de forma local. Tanto la multidifusión como la unidifusión son compatibles.

La función de redireccionamiento URL de Flash solo está disponible cuando la versión correcta del software agente está instalada. Esta función se incluye en el software del agente.

Para usar la función de redireccionamiento URL de Flash, debe configurar la página web y los dispositivos cliente. Los sistemas cliente deben cumplir los siguientes requisitos de software.

- Esta función solo es compatible con PCoIP. Esta función no es compatible con procesadores ARM.
- Los sistemas cliente deben tener conectividad IP con el servidor Adobe Web que aloja ShockWave File (SWF) que inicia la transmisión multidifusión o unidifusión. Si es necesario, configure el firewall para abrir los puertos apropiados para permitir que los dispositivos cliente accedan a este servidor.
- Los sistemas cliente deben tener instalado el complemento Flash apropiado.
 - a Instale el archivo `libexpat.so.1` o compruebe que este archivo ya está instalado.
Asegúrese de que este archivo esté instalado en el directorio `/usr/lib` o `/usr/local/lib`.
 - b Instale el archivo `libflashplayer.so` o compruebe que este archivo ya esté instalado.
Asegúrese de que el archivo esté instalado en el directorio del complemento Flash apropiado para el sistema operativo Linux.
 - c Instale la aplicación `wget` o compruebe que ya esté instalada.

Para obtener una lista de los requisitos de los escritorios remotos del redireccionamiento URL de Flash e instrucciones sobre cómo configurar una página web para proporcionar transmisiones multidifusión o unidifusión, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Requisitos del sistema para el redireccionamiento multimedia HTML5

Horizon Agent, Horizon Client, los escritorios remotos y los sistemas cliente en los que instala los software agente y cliente deben cumplir ciertos requisitos para admitir la función Redireccionamiento multimedia HTML5.

Con el Redireccionamiento multimedia HTML5, si un usuario final utiliza los navegadores Google Chrome o Microsoft Edge en un escritorio remoto, el contenido multimedia HTML5 se envía al sistema cliente. El sistema cliente reproduce el contenido multimedia, lo que reduce la carga del host ESXi y el usuario final disfruta de una experiencia mejorada de audio y vídeo.

Escritorio remoto

- Los escritorios virtuales deben tener instalado Horizon Agent 7.3.2 o una versión posterior para Chrome, o Horizon Agent 7.5 o una versión posterior para Edge, con la opción de configuración personalizada Redireccionamiento multimedia HTML5 seleccionada. De forma predeterminada, esta opción no está seleccionada. A partir de Horizon Agent 7.10, se elimina la opción de configuración personalizada del redireccionamiento multimedia HTML5, que estará instalado de forma predeterminada. Consulte los temas sobre cómo instalar Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7*.
- Los hosts RDS para los escritorios publicados deben tener instalado Horizon Agent 7.3.2 o una versión posterior con la opción de configuración personalizada Redireccionamiento multimedia HTML5 seleccionada. De forma predeterminada, esta opción no está seleccionada. A partir de Horizon Agent 7.10, se elimina la opción de configuración personalizada del redireccionamiento multimedia HTML5, que estará instalado de forma predeterminada. Consulte los temas sobre cómo instalar Horizon Agent en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Los ajustes de directiva de grupo Redireccionamiento multimedia HTML5 deben estar configurados en el servidor de Active Directory. Consulte los temas sobre cómo configurar el Redireccionamiento multimedia HTML5 en el documento *Configurar funciones de escritorios remotos en Horizon 7*.
- El navegador Chrome o el navegador Edge debe estar instalado.
- La extensión Redireccionamiento multimedia HTML5 de VMware Horizon debe estar instalada en el navegador Chrome o Edge. Consulte los temas sobre cómo configurar el Redireccionamiento multimedia HTML5 en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Sistema cliente

- La opción de configuración personalizada Redireccionamiento multimedia HTML5 debe estar seleccionada cuando instale Horizon Client. Esta opción está seleccionada de manera predeterminada.
- El sistema cliente debe tener instalada la versión 2.14 de glibc (biblioteca de C de GNU) o una posterior.

Protocolo de visualización para la sesión remota

- PCoIP
- VMware Blast

Limitaciones

La función Redireccionamiento multimedia HTML5 tiene las siguientes limitaciones.

- No se admite la función de mouse relativo de Horizon Client.
- No se puede usar la función **Silenciar sitio** (navegador Chrome) o **Silenciar pestaña** (navegador Edge) para silenciar el contenido de vídeo redireccionado.
- Para utilizar el redireccionamiento multimedia HTML5 de Chrome en un sistema cliente Linux, abra como máximo un navegador Chrome publicado por un host RDS. El redireccionamiento multimedia HTML5 no funciona correctamente si se abre un navegador Chrome adicional publicado por otro host RDS.
- Si el rendimiento es lento al reproducir contenido multimedia redireccionado en un sistema cliente Linux que utiliza hardware de cliente ligero de menor capacidad, puede optimizar el rendimiento del sistema como se describe a continuación. Agregue la entrada `disableGPU.html5mmr=true` a uno de los tres archivos de configuración siguientes. Estos archivos de configuración se procesan en este orden:

- a `/usr/lib/vmware/config`
- b `/etc/vmware/config`
- c `~/.vmware/config`

Requisitos de la función Session Collaboration

Con la función Session Collaboration, los usuarios pueden invitar a otros usuarios a que se unan a una sesión de escritorio remoto existente. Para admitir la función Session Collaboration, la implementación de Horizon debe cumplir ciertos requisitos.

Colaboradores de sesión

Para unirse a una sesión colaborativa, un usuario debe tener Horizon Client 4.7 para Windows, Mac o Linux instalado en el sistema cliente, o bien usar la versión 4.7 de HTML Access o una posterior.

Escritorios remotos Windows

- Se debe instalar Horizon Agent 7.4 o una versión posterior en el escritorio virtual Windows o en el host RDS para los escritorios publicados.
- Debe habilitarse la función Session Collaboration en el nivel de granja o grupo de escritorios. Para obtener más información sobre cómo habilitar la función Session

Collaboration en los grupos de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7*. Para obtener más información sobre cómo habilitar la función Session Collaboration en una granja, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Puede utilizar la configuración de directiva de grupo de Horizon Agent para configurar la función Session Collaboration. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Escritorios remotos Linux

Para conocer los requisitos que se aplican a los escritorios remotos Linux, consulte el documento *Configurar escritorios de Horizon 7 for Linux*.

Servidor de conexión

Para usar la función Session Collaboration, la instancia del servidor de conexión debe usar una licencia empresarial.

Protocolos de visualización

VMware Blast

La función Session Collaboration no admite las sesiones de aplicaciones publicadas.

Requisitos para usar Skype Empresarial con Horizon Client

Los usuarios finales pueden ejecutar Skype Empresarial en un escritorio virtual sin que afecte de forma negativa a la infraestructura virtual ni sobrecargue la red. Durante las llamadas de audio y vídeo de Skype, todos los procesos de medios tienen lugar en la máquina cliente en lugar de en el escritorio virtual.

Para utilizar esta función, debe instalar VMware Virtualization Pack para Skype Empresarial en el equipo cliente durante la instalación de Horizon Client para Linux. Para obtener información, consulte [Opciones de instalación](#).

El administrador de Horizon también debe instalar la función VMware Virtualization Pack para Skype Empresarial en el escritorio virtual si Horizon Agent está instalado. Para obtener información sobre cómo instalar Horizon Agent, consulte el documento *Configurar escritorios virtuales en Horizon 7*.

Para conocer todos los requisitos, consulte "Configurar Skype Empresarial" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Sistemas operativos del escritorio compatibles

Un administrador de Horizon crea máquinas virtuales que tienen un sistema operativo invitado e instala el software agente en el sistema operativo invitado. Los usuarios finales pueden iniciar sesión en esas máquinas virtuales desde un dispositivo cliente.

Para obtener una lista de los sistemas operativos invitados Windows compatibles, consulte el documento *Instalación de Horizon 7*.

También se admiten algunos sistemas operativos invitados Linux. Para obtener información sobre los requisitos del sistema, la configuración de las máquinas virtuales Linux y una lista de las funciones compatibles, consulte el documento *Configurar escritorios de Horizon 7 for Linux*.

El proceso de instalación de Horizon Client es similar al de otras aplicaciones.

Este capítulo incluye los siguientes temas:

- [Preparar el servidor de conexión para Horizon Client](#)
- [Opciones de instalación](#)
- [Instalar o actualizar Horizon Client para Linux desde la página de descargas de productos de VMware](#)

Preparar el servidor de conexión para Horizon Client

Antes de que los usuarios finales se puedan conectar a un servidor y acceder a una aplicación publicada o un escritorio remoto, un administrador de Horizon debe configurar ciertas opciones del servidor de conexión.

Unified Access Gateway y servidores de seguridad

- Si la implementación de Horizon incluye un dispositivo de Unified Access Gateway, configure el servidor de conexión para que funcione con Unified Access Gateway. Consulte el documento *Implementación y configuración de Unified Access Gateway*. Los dispositivos de Unified Access Gateway tienen la misma función que los servidores de seguridad.
- Si la implementación de Horizon incluye un servidor de seguridad, compruebe que esté utilizando las últimas versiones de mantenimiento del servidor de conexión 6.2.x y del servidor de seguridad 6.2.x o versiones posteriores. Para obtener más información, consulte el documento de instalación de su versión de Horizon.

Conexión de túnel de seguro

Si tiene pensado utilizar una conexión de túnel seguro para dispositivos cliente y si la conexión segura está configurada con un nombre de host DNS para la instancia de un servidor de conexión o un servidor de seguridad, compruebe que el dispositivo cliente pueda resolver este nombre DNS.

Grupos de escritorios y aplicaciones

- Compruebe que se creó un grupo de aplicaciones o de escritorios y que la cuenta de usuario que tiene pensado utilizar tiene autorización para acceder al grupo. Para obtener más información, consulte los documentos *Configurar escritorios virtuales en Horizon 7* y *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Autenticación de usuarios

- Para proporcionar a los usuarios finales acceso sin autenticar a las aplicaciones publicadas en Horizon Client, debe habilitar esta función en la instancia del servidor de conexión. Para obtener más información, consulte los temas relacionados con el acceso sin autenticar en el documento *Administración de VMware Horizon Console*.
- Para usar una autenticación en dos fases, como las autenticaciones RSA SecurID o RADIUS, con Horizon Client, debe habilitar la función de autenticación en dos fases para la instancia del servidor de conexión. A partir de la versión 7.11 de Horizon 7, puede personalizar las etiquetas de la página de inicio de sesión de la autenticación de RADIUS. A partir de Horizon 7 versión 7.12, puede configurar la autenticación en dos fases para que se ejecute después de agotar el tiempo de espera de una sesión remota. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento *Administración de VMware Horizon Console*.
- Para ocultar la URL del servidor en Horizon Client, habilite la opción global **Ocultar la información del servidor en la interfaz de usuario del cliente**. Esta opción está disponible en Horizon 7 versión 7.1 y versiones posteriores. Para obtener más información, consulte el documento *Administración de VMware Horizon Console*.
- Para ocultar el menú desplegable **Dominio** en Horizon Client, habilite la opción global **Ocultar la lista de dominios en la interfaz de usuario del cliente**. Esta opción está disponible en Horizon 7 versión 7.1 y versiones posteriores. A partir de Horizon 7 versión 7.8, está habilitada de forma predeterminada. Para obtener más información, consulte el documento *Administración de VMware Horizon Console*.
- Para enviar la lista de dominios a Horizon Client, habilite a la opción global **Enviar lista de dominios** en Horizon Console. Esta opción está disponible a partir de Horizon 7 versión 7.8 y está deshabilitada de forma predeterminada. Las versiones anteriores de Horizon 7 envían la lista de dominios. Para obtener más información, consulte el documento *Administración de VMware Horizon Console*.

En la siguiente tabla se muestra cómo las opciones globales **Enviar lista de dominios:** y **Ocultar la lista de dominios en la interfaz de usuario del cliente** determinan la forma en la que los usuarios pueden iniciar sesión en el servidor.

Opción Enviar lista de dominios	Opción Ocultar la lista de dominios en la interfaz de usuario del cliente	Cómo inician sesión los usuarios
Deshabilitado (opción predeterminada)	Habilitado	El menú desplegable Dominio está oculto. Los usuarios deben introducir uno de los siguientes valores en el cuadro de texto Nombre de usuario . <ul style="list-style-type: none"> ■ Nombre de usuario (no se permite en varios dominios) ■ <i>dominio\usuario</i> ■ <i>usuario@dominio.com</i>
Deshabilitado (opción predeterminada)	Deshabilitado	Si se configura un dominio predeterminado en el cliente, el dominio predeterminado aparecerá en el menú desplegable Dominio . Si el cliente no conoce un dominio predeterminado, aparecerá *DefaultDomain* en el menú desplegable Dominio . Los usuarios deben introducir uno de los siguientes valores en el cuadro de texto Nombre de usuario . <ul style="list-style-type: none"> ■ Nombre de usuario (no se permite en varios dominios) ■ <i>dominio\usuario</i> ■ <i>usuario@dominio.com</i>
Habilitado	Habilitado	El menú desplegable Dominio está oculto. Los usuarios deben introducir uno de los siguientes valores en el cuadro de texto Nombre de usuario . <ul style="list-style-type: none"> ■ Nombre de usuario (no se permite en varios dominios) ■ <i>dominio\usuario</i> ■ <i>usuario@dominio.com</i>
Habilitado	Deshabilitado	Los usuarios pueden introducir un nombre de usuario en el cuadro de texto Nombre de usuario y, a continuación, seleccionar un dominio en el menú desplegable Dominio . También pueden introducir uno de los siguientes valores en el cuadro de texto Nombre de usuario . <ul style="list-style-type: none"> ■ <i>dominio\usuario</i> ■ <i>usuario@dominio.com</i>

Opciones de instalación

Durante el proceso de instalación de Horizon Client, se le solicitará que confirme la instalación de componentes opcionales. La acción predeterminada es instalar todos los componentes.

La siguiente tabla proporciona un breve resumen de cada componente opcional.

Tabla 2-1. Opciones de instalación de Horizon Client para Linux

Opción	Descripción
Redirecciónamiento de unidades cliente	<p>Permite a los usuarios compartir carpetas y unidades en el equipo cliente con aplicaciones y escritorios remotos. Las unidades pueden incluir unidades montadas y dispositivos de almacenamiento USB.</p> <p>Los archivos de componentes se instalan en <code>/usr/lib/vmware/view/vdpService/</code>.</p>
Redirecciónamiento multimedia HTML5 (HTML5MMR)	<p>Redirige el contenido multimedia HTML5 desde un navegador Google Chrome o Microsoft Edge en el escritorio hasta la máquina cliente, donde se procesa.</p>
Redirecciónamiento multimedia (MMR)	<p>Redirige la transmisión multimedia desde el escritorio al equipo cliente, donde esta se procesa.</p> <p>El archivo de componente se instala en <code>/usr/lib/vmware/view/vdpService/</code>.</p>
Audio/vídeo en tiempo real	<p>Redirige los dispositivos de audio y de cámara web que están conectados al sistema cliente para que se puedan usar en el escritorio remoto.</p> <p>El archivo de componente se instala en <code>/usr/lib/pcoip/vchan_plugins/</code>.</p>
Redirecciónamiento de escáner	<p>Permite a los usuarios escanear datos en escritorios remotos con escáneres que cumplan el estándar SANE conectados a sus sistemas cliente locales. Los usuarios no tienen que instalar controladores adicionales en los escritorios remotos.</p> <p>Si permite que el instalador de Horizon Client registre e inicie los servicios instalados después de completar la instalación, el demonio de redirecciónamiento de escáner se ejecutará automáticamente. Si no es así, puede iniciar el demonio del redirecciónamiento de escáner de forma manual ejecutando el siguiente comando.</p> <pre># sudo /etc/init.d/ftscanhv start</pre> <p>El redirecciónamiento de escáner requiere que los escritorios remotos tengan instalado Horizon Agent 7.8 o versiones posteriores, con la opción de configuración Redirecciónamiento de escáner, en las máquinas virtuales de plantilla o principal o los hosts RDS. Además, esta función requiere el protocolo de visualización VMware Blast o PCoIP.</p> <p>Tras la instalación, puede establecer la configuración de directiva de grupo de esta función siguiendo las instrucciones especificadas en la sección "Configurar el redirecciónamiento de escáner" del documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>
Función de aplicación remota	<p>Con esta función, los usuarios pueden interactuar con una aplicación que se ejecuta en un escritorio remoto como si fuera una aplicación de ejecución local.</p>
Redirecciónamiento del puerto serie	<p>Permite a los usuarios finales redirigir puertos serie conectados localmente, como los puertos RS-232 integrados (<code>/dev/ttySxx</code>) o los adaptadores de USB a puerto serie (<code>/dev/ttyUSBxx</code>), a sus escritorios remotos. Si permite que el instalador de Horizon Client registre e inicie los servicios instalados después de completar la instalación, el demonio del puerto serie se ejecutará automáticamente. Si no es así, puede iniciar el demonio del puerto serie de forma manual ejecutando el siguiente comando.</p> <pre># sudo /etc/init.d/ftsprhv start</pre> <p>Para que un dispositivo adaptador de USB a puerto serie esté disponible para el redirecciónamiento de puertos serie, desmarque Conectar dispositivo USB > Conectar automáticamente al inicio y Conectarse automáticamente al insertar el dispositivo y asegúrese de que el dispositivo adaptador de USB a puerto serie no esté seleccionado en el menú Conectar dispositivo USB.</p>

Tabla 2-1. Opciones de instalación de Horizon Client para Linux (continuación)

Opción	Descripción
Tarjeta inteligente	<p>Permite al usuario autenticarse con tarjetas inteligentes cuando usan los protocolos de visualización VMware Blast o PCoIP. Aunque esta opción está seleccionada en el instalador cliente de forma predeterminada, no está seleccionada de forma predeterminada cuando ejecuta el instalador de Horizon Agent en el escritorio remoto.</p> <p>La tarjeta inteligente es compatible con escritorios remotos que se implementan en equipos de un solo usuario y en hosts RDS.</p> <p>Los archivos de componentes se instalan en <code>/usr/lib/pcoip/vchan_plugins/</code>.</p>
Redireccionamiento USB	<p>Proporciona a los usuarios acceso a dispositivos USB conectados de forma local en las aplicaciones y los escritorios.</p> <p>El redireccionamiento USB es compatible con las aplicaciones y los escritorios remotos que se implementan en equipos de un solo usuario.</p> <p>Los archivos de componentes se instalan en <code>/usr/lib/vmware/view/usb/</code>. Si permite que el instalador registre e inicie los servicios instalados después de completar la instalación, el demonio del árbitro USB, <code>vmware-USBArbitrator</code>, se ejecutará automáticamente. Si no es así, puede iniciar el demonio de forma manual ejecutando el siguiente comando:</p> <pre># sudo /etc/init.d/vmware-USBArbitrator start</pre> <p>Nota Puede usar la configuración de la directiva de grupo si desea deshabilitar el redireccionamiento USB para usuarios específicos. Para obtener más información, consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>
Impresión virtual	<p>Permite a los usuarios imprimir en cualquier impresora disponible en los equipos cliente. Los usuarios no tienen que instalar controladores adicionales en los escritorios remotos.</p> <p>Los archivos de componentes se instalan en <code>/usr/lib/vmware/view/virtualPrinting/</code>. Después de instalar al cliente, si permite que el instalador registre e inicie los servicios instalados después de la instalación, no será necesario configurar esta función manualmente. En caso contrario, puede configurar y habilitar esta función según las instrucciones disponibles en Habilitar la función de impresión virtual en un cliente Linux.</p> <p>La función Impresión virtual es compatible con los siguientes escritorios remotos y las siguientes aplicaciones publicadas:</p> <ul style="list-style-type: none"> ■ Escritorios que se implementan en máquinas de usuario único. ■ Escritorios que se implementan en hosts RDS, donde los hosts RDS son máquinas virtuales. ■ Aplicaciones remotas, proporcionadas por hosts RDS. ■ Aplicaciones remotas que se inician desde Horizon Client dentro de los escritorios remotos (sesiones anidadas).

Tabla 2-1. Opciones de instalación de Horizon Client para Linux (continuación)

Opción	Descripción
VMware Horizon(R) Virtualization Pack para Skype Empresarial	<p>Permita que los usuarios ejecuten Skype Empresarial en un escritorio virtual sin que afecte de forma negativa a la infraestructura virtual ni sobrecargue la red. Durante las llamadas de voz y las videollamadas de Skype, todos los procesos multimedia tienen lugar en el sistema cliente Linux, en lugar de producirse en el escritorio virtual.</p> <p>El archivo de componente se instala en <code>/usr/lib/vmware/mediaprovider</code>.</p>
VMware Integrated Printing	<p>Permite a los usuarios imprimir en impresoras locales o de red desde un escritorio remoto de Windows sin tener que instalar controladores de impresora adicionales en el escritorio remoto. Además de instalar esta opción en el sistema cliente, debe habilitar la opción VMware Integrated Printing en el instalador de Horizon Agent y establecer directivas que controlen el comportamiento de la impresión virtual.</p> <p>Para obtener información sobre cómo instalar Horizon Agent, consulte el documento <i>Configurar escritorios virtuales en Horizon 7</i> o <i>Configurar aplicaciones y escritorios publicados en Horizon 7</i>. Para obtener más información sobre cómo configurar directivas, consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>

Instalar o actualizar Horizon Client para Linux desde la página de descargas de productos de VMware

Es posible descargar y ejecutar un paquete de instalación de Horizon Client desde la página de descargas de VMware. Este instalador contiene módulos para funciones como redireccionamiento USB, impresión virtual, Audio/vídeo en tiempo real, tarjeta inteligente y redireccionamiento de la unidad cliente.

Nota En la mayoría de distribuciones Linux, el paquete de instalación de Horizon Client inicia un asistente GUI. También puede ejecutar el instalador con la opción `--console` para iniciar el asistente de la línea de comandos.

Requisitos previos

- Compruebe que el sistema cliente ejecute un sistema operativo compatible. Consulte [Requisitos del sistema para sistemas cliente Linux](#).
- Familiarícese con las opciones de instalación. Consulte [Opciones de instalación](#).
- Compruebe que tenga acceso raíz en el sistema cliente.
- Compruebe que VMware Workstation no esté instalado en el sistema cliente.
- Si tiene pensado usar el protocolo de visualización RDP para conectarse a un escritorio de View, compruebe que tenga instalado el cliente RDP apropiado. Consulte [Requisitos del sistema para sistemas cliente Linux](#).
- Desinstale las versiones anteriores del software Horizon Client. Consulte [Desinstalar Horizon Client para Linux](#).

- Si tiene pensado usar el instalador de la línea de comandos, familiarícese con las opciones de instalación de la línea de comandos de Linux. Consulte [Opciones de instalación de la línea de comandos del cliente Linux](#).
- Confirme que la versión 2.x de Python esté instalada en el sistema cliente. Si el sistema no tiene el paquete Python 2.x, ejecute el comando necesario para instalarlo.
- Si utiliza un cliente ligero, confirme que tiene instalado libgtk 3.14 o una versión posterior en el sistema. Si es necesario, obtenga la versión 3.14 o una posterior de la biblioteca libgtk e instálela en el sistema cliente ligero.

Como parte del proceso de instalación, el instalador ejecuta un análisis de las bibliotecas del sistema para determinar si el sistema es compatible con Horizon Client, aunque puede omitir este análisis si lo desea.

Procedimiento

- 1 En el sistema cliente Linux, descargue el archivo instalador desde la página de descargas de productos de Horizon Client, disponible en Horizon Client <http://www.vmware.com/go/viewclients>.

El nombre del archivo es `VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`, donde `x.x.x` es el número de la versión, `yyyyyyy` es el número de compilación y `arch` es `x86` o `x64`.

- 2 Abra una ventana de terminal, cambie los directorios al directorio que contiene el archivo de instalación y ejecute el instalador mediante el comando apropiado.

Opción	Comando
Para el asistente GUI, si tiene configurados permisos ejecutables	<code>sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle</code>
Para el asistente GUI, si no tiene configurados permisos ejecutables	<code>sudo sh ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle</code>
Para el instalador de la línea de comandos	<code>sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console</code>

El asistente de instalación aparecerá y le solicitará que acepte el contrato de licencia para el usuario final.

- 3 Para finalizar la instalación, siga los mensajes.

Importante Se le solicitará que permita al instalador registrarse o iniciar los servicios instalados después de la instalación. Si permite que el instalador complete estas tareas, tiene que iniciar los servicios de redireccionamiento USB de forma manual cada vez que reinicie y no es necesario habilitar manualmente la función de impresión virtual.

- 4 Cuando la instalación se complete, especifique si desea realizar un análisis de compatibilidad en las bibliotecas de las que dependen varios componentes de las funciones.

El análisis del sistema muestra un valor del resultado de las compatibilidades de las bibliotecas.

Valor del resultado	Descripción
Correcto	Se encontraron todas las bibliotecas necesarias.
Con error	No se encuentra la biblioteca especificada.

Resultados

La información del registro de instalación se guarda en `/tmp/vmware-root/vmware-installer-pid.log`.

Pasos siguientes

Inicie Horizon Client y compruebe que pueda iniciar sesión en el escritorio virtual correcto.

Consulte [Conectarse a una aplicación publicada o a un escritorio remoto](#).

Opciones de instalación de la línea de comandos del cliente Linux

Puede usar las opciones de instalación de la línea de comandos para instalar Horizon Client en un sistema Linux.

Instale Horizon Client silenciosamente usando la opción `--console` junto con otras opciones de la línea de comandos, así como la configuración de la variable del entorno. La instalación silenciosa le permite implementar los componentes de View correctamente en una empresa de gran tamaño.

La siguiente tabla muestra las opciones que puede usar cuando ejecute el archivo instalador `VMware-Horizon-Client-x.x.x-yyyyyy.arch.bundle.bundle`.

Tabla 2-2. Opciones de instalación de la línea de comandos en Linux

Opción	Descripción
<code>--help</code>	Muestra información de uso.
<code>--console</code>	Le permite usar el instalador de la línea de comandos en una ventana de terminal.
<code>--custom</code>	Muestra todas preguntas de instalación, incluso si las respuestas predeterminadas se generan por script, como, por ejemplo, al usar las opciones <code>--set-setting</code> . La opción predeterminada es <code>--regular</code> , que muestra únicamente las preguntas que no tienen una respuesta predeterminada.
<code>--eulas-agreed</code>	Acepta el acuerdo de licencia del usuario final.
<code>--gtk</code>	Abre el instalador de VMware basado en GUI, que es la opción predeterminada. Si GUI no se puede mostrar o cargar por alguna razón, se usa el modo de consola.

Tabla 2-2. Opciones de instalación de la línea de comandos en Linux (continuación)

Opción	Descripción
<code>--ignore-errors o -I</code>	Permite que continúe la instalación, aunque se produzca un error en uno de los scripts del instalador. Como la sección que tiene un error no se completa, es posible que el componente no se configure correctamente.
<code>--regular</code>	Muestra las preguntas de instalación que no se respondieron o que son necesarias. Esta es la opción predeterminada.
<code>--required</code>	Muestra la solicitud del contrato de licencia y, a continuación, comienza a instalar el cliente. La opción predeterminada es <code>--regular</code> , que muestra únicamente las preguntas que no tienen una respuesta predeterminada.
<code>--set-setting vmware-horizon-html5mmr html5mmrEnable yes</code>	Instala el componente de redireccionamiento multimedia HTML5.
<code>--set-setting vmware-horizon-integrated-printing vmipEnable yes</code>	Instala el componente VMware Integrated Printing.
<code>--set-setting vmware-horizon-media-provider mediaproviderEnable yes</code>	Instala el componente VMware Horizon Virtualization Pack para Skype Empresarial.
<code>--set-setting vmware-horizon-mmrm mmrEnable yes</code>	Instala la función de redireccionamiento multimedia (MMR).
<code>--set-setting vmware-horizon-rtav rtavEnable yes</code>	Instala el componente Audio/vídeo en tiempo real.
<code>--set-setting vmware-horizon-scannerclient scannerEnable yes</code>	Instala la función de redireccionamiento de escáner.
<code>--set-setting vmware-horizon-serialportclient serialportEnable yes</code>	Instala la función de redireccionamiento de puerto serie.
<code>--set-setting vmware-horizon-smartcard smartcardEnable yes</code>	Instala el componente de la tarjeta inteligente.
<code>--set-setting vmware-horizon-tsdr tsdrEnable yes</code>	Instala la función de redireccionamiento de la unidad cliente.
<code>--set-setting vmware-horizon-usb usbEnable yes</code>	Instala la función de redireccionamiento USB.
<code>--set-setting vmware-horizon-virtual-printing tpEnable yes</code>	Instala la función Impresión virtual.
<code>--stop-services</code>	No se registra ni inicia los servicios instalados.

Además de las opciones que aparecen en la tabla, puede establecer las siguientes variables del entorno.

Tabla 2-3. Opciones de instalación de variables del entorno de Linux

Variable	Descripción
TERM=dumb	Muestra una interfaz de usuario de texto básica.
VMWARE_EULAS_AGREED=yes	Le permite aceptar silenciosamente el Contrato de licencia para el usuario final del producto.
VMIS_LOG_LEVEL= <i>valor</i>	<p>Use uno de los siguientes valores para <i>valor</i>:</p> <ul style="list-style-type: none"> ■ NOTSET ■ DEBUG ■ INFO ■ WARNING ■ ERROR ■ CRITICAL <p>La información de los registros se almacena en <code>/tmp/vmware-root/vmware-installer-<i>pid</i>.log</code>.</p>

Ejemplo: Comandos de instalación silenciosa

A continuación, se muestra un ejemplo de cómo instalar Horizon Client silenciosamente y, en cada componente, el ejemplo especifica si instalarlo.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \
./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console \
--set-setting vmware-horizon-usb usbEnable no \
--set-setting vmware-horizon-virtual-printing tpEnable yes \
--set-setting vmware-horizon-smartcard smartcardEnable no\
--set-setting vmware-horizon-rtav rtavEnable yes \
--set-setting vmware-horizon-tsdr tsdrEnable yes
--set-setting vmware-horizon-scannerclient scannerEnable yes
--set-setting vmware-horizon-serialportclient serialportEnable yes
--set-setting vmware-horizon-mmrm mmrEnable yes
--set-setting vmware-horizon-media-provider mediaproviderEnable yes
```

El siguiente ejemplo muestra cómo realizar una instalación silenciosa de Horizon Client con la configuración predeterminada.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \
./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console --required
```


Habilitar la función de impresión virtual en un cliente Linux

El paquete de instalación para Horizon Client 3.2 y versiones posteriores incluye un componente de impresión virtual. Si cuenta con Horizon Client 3.2, debe crear un archivo de configuración y establecer algunas variables de entorno para habilitar la función.

La función de impresión virtual permite a los usuarios finales utilizar impresoras locales o de red desde un escritorio remoto sin que sea necesario que los controladores de impresión estén instalados en el escritorio remoto.

Importante Normalmente, no es necesario realizar este procedimiento si tiene Horizon Client 3.4 o una versión posterior ya que puede especificar, durante la instalación del cliente, que el instalador debe registrar e iniciar los servicios instalados después del proceso de instalación. Cuando el usuario inicie el cliente, se creará automáticamente un archivo de configuración que se ubica en el directorio home del usuario.

Requisitos previos

Debe usar el paquete de instalación proporcionado por VMware para instalar Horizon Client 3.2 o posterior. El componente de impresión virtual se instala de forma predeterminada.

Procedimiento

- 1 Abra una ventana de terminal e introduzca un comando para crear una carpeta denominada `.thnucInt` en el directorio home.

```
$ mkdir ~/.thnucInt/
```

Nota Dado que este archivo se crea en un directorio de inicio específico del usuario, es necesario que se cree el archivo para cada usuario que utilice el sistema cliente Linux.

- 2 Use un editor de texto para crear un archivo de configuración denominado `thnucInt.conf` en la carpeta `~/.thnucInt` y agregue el siguiente texto al archivo:

```
autoupdate = 15
automap = true
autoid = 0
updatecount = 1
editcount = 0

connector svc {
    protocol = listen
    interface = /home/user/.thnucInt/svc
    setdefault = true
}
```

En este texto, sustituya el nombre de usuario por *user*.

- 3 Guarde y cierre el archivo.

- 4 Introduzca un comando para iniciar el proceso `thnucInt`.

```
$ thnucInt -fg
```

- 5 Introduzca los comandos para establecer las variables del entorno destinadas a los componentes de impresión virtual.

```
$ export TPCLIENTADDR=/home/user/.thnucInt/svc  
$ export THNURDPIMG=/usr/bin/thnurdp
```

- 6 Para iniciar Horizon Client, es necesario que inicie el proceso `vmware-view`.

Las impresoras que suelen aparecer en el cliente ahora están redireccionadas para que aparezcan en el cuadro de diálogo Imprimir del escritorio remoto.

- 7 (opcional) Si en algún momento desea deshabilitar esta función, siga estos pasos:

- a Introduzca un comando para detener el proceso `thnucInt`.

```
$ killall thnucInt
```

- b Desconéctese del escritorio remoto y vuelva a conectarse al escritorio.

Las impresoras ya no estarán redirigidas.

Configurar Horizon Client para usuarios finales

3

La configuración de Horizon Client para usuarios finales puede incluir la construcción de los URI, la modificación de las opciones avanzadas de TLS/SSL, la configuración del modo de verificación del certificado, de combinaciones de teclas y teclas específicas así como de las opciones del protocolo de visualización y la habilitación del modo compatible con FIPS.

Este capítulo incluye los siguientes temas:

- [Opciones de configuración comunes](#)
- [Utilizar los archivos de configuración y la interfaz de línea de comandos de vmware-view](#)
- [Utilizar URI para configurar Horizon Client](#)
- [Configurar las opciones de VMware Blast](#)
- [Configurar el uso compartido de datos de Horizon Client](#)
- [Configurar el modo de comprobación de certificados para usuarios finales](#)
- [Configurar las opciones de TLS avanzadas](#)
- [Configurar teclas específicas y combinaciones de teclas para enviarlas al sistema local](#)
- [Utilizar FreeRDP para las conexiones RDP](#)
- [Habilitar el modo compatible con FIPS](#)
- [Configurar la caché de imágenes del lado del cliente PCoIP](#)

Opciones de configuración comunes

Horizon Client proporciona varios mecanismos de configuración que simplifican la experiencia de selección de escritorios remotos y de inicio de sesión para los usuarios finales, además de implementar las directivas de seguridad.

La siguiente tabla muestra solo algunas de las opciones de configuración que puede establecer de una o varias formas.

Tabla 3-1. Opciones de configuración comunes

Configuración	Mecanismos de configuración
Dirección de servidor	URI, propiedad del archivo de configuración y línea de comandos
Nombre de usuario de Active Directory	URI, propiedad del archivo de configuración y línea de comandos
Nombre de dominio	URI, propiedad del archivo de configuración y línea de comandos
Nombre para mostrar del escritorio remoto	URI, propiedad del archivo de configuración y línea de comandos
Tamaño de la ventana	URI, propiedad del archivo de configuración y línea de comandos
Protocolo de visualización	URI, propiedad del archivo de configuración y línea de comandos
Configurar la comprobación del certificado	Propiedad del archivo de configuración
Configurar protocolos TLS y algoritmos criptográficos	Propiedad del archivo de configuración, línea de comandos

Utilizar los archivos de configuración y la interfaz de línea de comandos de vmware-view

Puede configurar Horizon Client con opciones de línea de comandos o propiedades equivalentes de un archivo de configuración.

Puede utilizar la interfaz de línea de comandos de `vmware-view` o establecer propiedades en archivos de configuración para definir los valores predeterminados que sus usuarios verán en Horizon Client o para evitar que algunos cuadros de diálogo soliciten información a los usuarios. También puede especificar las opciones que no quiera que cambien los usuarios.

Orden de procesamiento de las opciones de configuración

Cuando se inicia Horizon Client, las opciones de configuración se procesan desde varias ubicaciones en el siguiente orden:

- 1 `/etc/vmware/view-mandatory-config`
- 2 Argumentos de la línea de comandos
- 3 `~/.vmware/view-preferences`
- 4 `/etc/vmware/view-default-config`

Nota Debe crear manualmente los archivos `/etc/vmware/view-default-config` y `/etc/vmware/view-mandatory-config`. Después de iniciar Horizon Client, se generará automáticamente el archivo `~/.vmware/view-preferences`.

Si una opción se define en varias ubicaciones, el valor que se utiliza es el que se obtiene de la última lectura de la opción de línea de comandos o del archivo. Por ejemplo, para especificar opciones que anulen las preferencias del usuario, establezca propiedades en el archivo `/etc/vmware/view-mandatory-config`.

Para establecer valores predeterminados que los usuarios puedan cambiar, utilice el archivo `/etc/vmware/view-default-config`. Una vez que el usuario cambie una opción, las opciones que se hayan cambiado se guardarán en el archivo `~/.vmware/view-preferences` al salir de Horizon Client.

Propiedades que evitan que los usuarios cambien las opciones predeterminadas

En muchas propiedades, puede establecer una propiedad `view.allow` correspondiente que controle si los usuarios tienen permiso para cambiar la opción. Por ejemplo, si asigna el valor "FALSE" a la propiedad `view.allowDefaultBroker` en el archivo `/etc/vmware/view-mandatory-config`, los usuarios no podrán cambiar el nombre del servidor cuando se conecten con Horizon Client.

Sintaxis para utilizar la interfaz de línea de comandos

Utilice el siguiente formato del comando `vmware-view` en una ventana de terminal.

```
vmware-view [command-line-option [argument]] ...
```

De forma predeterminada, el comando `vmware-view` se encuentra en el directorio `/usr/bin`.

Puede utilizar tanto el formato corto como el largo del nombre de la opción, aunque no todas las opciones tienen un formato corto. Por ejemplo, para especificar el dominio, puede utilizar `-d` (formato corto) o `--domainName=` (formato largo). Es posible que utilice el formato largo para que un script tenga un lenguaje más natural.

Puede utilizar la opción `--help` para obtener una lista de información de uso y opciones de línea de comandos.

Importante Si necesita utilizar un proxy, utilice la siguiente sintaxis:

```
http_proxy=proxy_server_URL:port https_proxy=proxy_server_URL:port vmware-view options
```

Esta solución alternativa es necesaria porque debe borrar las variables de entorno que se establecieron anteriormente para el proxy. Si no realiza esta acción, la opción de excepción de proxy no se aplicará en Horizon Client. Debe configurar una excepción de proxy para la instancia del servidor de conexión de View.

Opciones de la línea de comandos y configuración de Horizon Client

Para su comodidad, casi todas las opciones de configuración cuentan con una propiedad `key=value` y un nombre de la opción de la línea de comandos correspondiente. En algunas opciones, existe una opción de la línea de comandos pero no una propiedad correspondiente

que pueda establecer en un archivo de configuración. En otras opciones, debe establecer una propiedad porque no existe ninguna línea de comandos disponible.

Importante Algunas opciones de la línea de comandos y de las claves de configuración están disponibles únicamente con la versión de Horizon Client proporcionada por proveedores de terceros. Para obtener más información sobre los partners del cliente ligero o del cliente cero, consulte la *Guía de compatibilidad de VMware* en <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm>.

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client

Clave de configuración	Opción de línea de comandos	Descripción
view.allMonitors	--allmonitors	Oculto la sistema operativo del host y abre Horizon Client en modo de pantalla completa en todos los monitores que están conectados al sistema cliente cuando se inicia Horizon Client. Si establece la clave de configuración, especifique "TRUE" o "FALSE" . El valor predeterminado es "FALSE" .
view.allowDefaultBroker	-l, --lockServer	Si usa esta opción de la línea de comandos o configura la propiedad como "FALSE" , se deshabilitará el cuadro de texto Servidor , a menos que el cliente no se haya conectado nunca a un servidor, y no se haya especificado ninguna dirección de servidor en la línea de comandos ni en el archivo de preferencias. Por ejemplo: <pre>--lockServer -s view.company.com</pre>
view.allowEnableHEVC	Ninguno	Si se establece "FALSE" para esta propiedad, el cliente no podrá cambiar la opción Permitir decodificación de vídeo de alta eficacia (HEVC) en la ventana Configuración de VMware Horizon Blast.
view.autoConnectBroker	Ninguna	Se conecta automáticamente al último servidor utilizado, a menos que se establezca la propiedad de configuración view.defaultBroker o se use la opción de línea de comandos --serverURL=. Especifique "TRUE" o "FALSE" . El valor predeterminado es "FALSE" . Si se establece esta propiedad y la propiedad view.autoConnectDesktop en "TRUE" , esta acción es equivalente a establecer la propiedad view.nonInteractive en "TRUE" .

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.autoConnectDesktop	Ninguna	<p>Se conecta automáticamente al último escritorio remoto utilizado, a menos que se establezca la propiedad de configuración view.defaultDesktop o se use la opción de línea de comandos --desktopName=.</p> <p>Especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p> <p>Si se establece esta propiedad y la propiedad view.autoConnectBroker en "TRUE", esta acción es equivalente a establecer la propiedad view.nonInteractive en "TRUE".</p>
view.autoDisconnectEmptyAppSession	Ninguna	<p>Cuando se establece en "TRUE" (valor predeterminado), si la sesión de la aplicación se vacía porque el usuario cierra todas las aplicaciones, se mostrará un mensaje para el usuario final. Este mensaje le solicita al usuario que elija si desea desconectar la sesión vacía o mantenerla en ejecución. Si se establece en "FALSE", las sesiones se cierran según la opción del tiempo de espera utilizada en Horizon Console, que de forma predeterminada se desconectará después de un minuto.</p>
view.autoHideToolbar	Ninguna	<p>Especifica si la barra de herramientas se oculta o se ancla automáticamente de forma predeterminada. Especifique "TRUE" para ocultar la barra de tareas automáticamente. El valor predeterminado es "FALSE".</p> <p>Esta opción también se puede configurar iniciando Horizon Client, seleccionando Archivo > Preferencias en la barra de menús y, a continuación, seleccionando la casilla de verificación Ocultar automáticamente la barra de herramientas.</p>
view.BENITServerConnectionMode	Ninguna	<p>Establece el modo de conexión que se usa al conectarse a un servidor. Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> ■ "T" para forzar una única conexión TCP. ■ "U" para forzar una única conexión UDP. ■ "4" para forzar una conexión con una dirección IPv4. ■ "T4" para forzar únicamente una conexión TCP y usar una dirección IPv4. ■ "U4" para forzar solo una conexión UDP y usar una dirección IPv4. ■ "bypass" para usar el modo de conexión BEAT heredado.

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.BENITTcpConnectCount	Ninguna	<p>Utilice este valor al conectarse desde una red con un gran porcentaje de pérdida de paquetes (superior al 20 %). Establezca el valor predeterminado a 12.</p> <p>Importante Utilice siempre esta opción con la clave de configuración <code>view.BENITUdpSendCount</code>.</p>
view.BENITUdpSendCount	Ninguna	<p>Utilice este valor al conectarse desde una red con un gran porcentaje de pérdida de paquetes (superior al 20 %). Establezca el valor predeterminado a 12.</p> <p>Importante Utilice siempre esta opción con la clave de configuración <code>view.BENITTcpConnectCount</code>.</p>
view.defaultAppHeight	Ninguna	<p>Especifica la altura predeterminada, en píxeles, de la ventana de las aplicaciones publicadas. Use esta propiedad y <code>view.defaultAppWidth</code> cuando especifique un tamaño de escritorio personalizado (la propiedad <code>view.defaultAppSize</code> está establecida en "5"). El valor predeterminado es "480".</p>
view.defaultAppWidth	Ninguna	<p>Especifica el ancho predeterminado, en píxeles, de la ventana de las aplicaciones publicadas. Use esta propiedad y <code>view.defaultAppHeight</code> cuando especifique un tamaño de escritorio personalizado (la propiedad <code>view.defaultAppSize</code> está establecida en "5"). El valor predeterminado es "640".</p>
view.defaultBroker	-s, --serverURL=	<p>Agrega el nombre que especificó en el cuadro de texto Servidor de Horizon Client. Especifique un nombre de dominio completo. También puede especificar un número de puerto si no utiliza el puerto 443 predeterminado.</p> <p>De forma predeterminada, se usará el último valor utilizado.</p> <p>Por ejemplo:</p> <pre>--serverURL=https://view.company.com -s view.company.com --serverURL=view.company.com:1443</pre>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.defaultDesktop	-n, --desktopName=	<p>Especifica el escritorio remoto que se usará cuando autoConnectDesktop se configura como "TRUE" y el usuario tiene acceso a varios escritorios remotos.</p> <p>El valor especificado es el nombre que aparece en el cuadro de diálogo Seleccionar escritorio. El nombre suele ser el nombre del grupo de escritorios.</p>
view.defaultDesktopHeight	Ninguna	<p>Especifica la altura predeterminada, en píxeles, de la ventana del escritorio remoto. Use esta propiedad y view.defaultDesktopWidth cuando especifique un tamaño de escritorio personalizado (la propiedad view.defaultDesktopSize está establecida en "5").</p>
view.defaultDesktopSize	--desktopSize=	<p>Establece el tamaño predeterminado de la ventana del escritorio remoto:</p> <ul style="list-style-type: none"> ■ Para usar todos los monitores, establezca la propiedad en "1" o bien utilice el argumento de la línea de comandos "all". ■ Para usar el modo de pantalla completa en un monitor, establezca la propiedad en "2" o bien utilice el argumento de la línea de comandos "full". ■ Para usar una ventana grande, establezca la propiedad en "3" o bien utilice el argumento de la línea de comandos "large". ■ Para usar una ventana pequeña, establezca la propiedad en "4" o bien utilice el argumento de la línea de comandos "small". ■ Para configurar un tamaño personalizado, establezca la propiedad en "5" y, a continuación, establezca también las propiedades view.defaultDesktopWidth y view.defaultDesktopHeight. De forma alternativa, especifique en píxeles el ancho y el alto en la línea de comandos de esta forma: "anchoxalto". <p>Por ejemplo:</p> <pre>--desktopSize="1280x800" --desktopSize="all"</pre>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.defaultDesktopWidth	Ninguna	<p>Especifica el ancho predeterminado, en píxeles, de la ventana del escritorio remoto. Use esta propiedad y view.defaultDesktopHeight cuando especifique un tamaño de escritorio personalizado (la propiedad view.defaultDesktopSize está establecida en "5").</p>
view.defaultDomain	-d, --domainName=	<p>Establece el nombre de dominio que usa Horizon Client en todas las conexiones y agrega el nombre de dominio que especificó en el cuadro de texto Nombre de dominio en el cuadro de diálogo de autenticación.</p>
view.defaultLogLevel	Ninguna	<p>Establece el nivel de los registros de Horizon Client. Establezca la propiedad en uno de los siguientes valores:</p> <ul style="list-style-type: none"> ■ En "0", se incluyen todos los eventos de registro. ■ En "1", se incluyen los eventos a nivel de seguimiento y los eventos capturados de las opciones 2 a 6. ■ En "2", se incluyen los eventos de depuración y los eventos capturados de las opciones 3 a 6. ■ En "3" (predeterminado), se incluyen los eventos a nivel de información y los eventos capturados de las opciones 4 a 6. ■ En "4", se incluyen los eventos graves, de aviso y de error. ■ En "5", se incluyen los eventos graves y de error. ■ En "6", se incluyen los eventos graves. <p>El valor predeterminado es "3".</p>
view.defaultPassword	-p "-", --password="-"	<p>Para las conexiones rdesktop, VMware Blast y PCoIP, especifique siempre "-" para que la contraseña se lea desde stdin.</p> <p>Establece la contraseña que utiliza Horizon Client para todas las conexiones y, si el servidor acepta la autenticación de la contraseña, agrega la contraseña del cuadro de texto Contraseña del cuadro de diálogo de autenticación.</p> <p>Nota No puede usar una contraseña en blanco. Es decir, no puede especificar <code>--password=""</code>.</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.defaultProtocol	--protocol=	<p>Especifica el protocolo de visualización que se usará. Especifique "PCOIP", "BLAST" o "RDP". Estos valores distinguen entre mayúsculas y minúsculas. Por ejemplo, si introduce rdp, el protocolo que se usa es el predeterminado. Este se especifica en Horizon Console, en la configuración del grupo.</p> <p>Si usa RDP y desea usar FreeRDP en lugar de rdesktop, debe utilizar también la opción rdpClient.</p>
view.defaultUser	-u, --userName=	<p>Establece el nombre de usuario que utiliza Horizon Client en todas las conexiones y agrega el nombre de usuario que especificó en el cuadro de texto Nombre de usuario del cuadro de diálogo de autenticación.</p> <p>En el modo de quiosco, el nombre de la cuenta se puede basar en la dirección MAC del cliente o puede comenzar con una cadena de prefijo reconocido, como custom-.</p>
view.enableDataSharing	Ninguna	<p>Especifica si Horizon Client tiene permiso para compartir datos anónimos en el sistema cliente.</p> <p>Establezca el valor "TRUE" o "FALSE". El valor predeterminado es "TRUE".</p>
view.enableDisplayScaling	Ninguna	<p>Especifica si la función de ajuste de escala de la pantalla está habilitada en todos los escritorios remotos. Establezca el valor "TRUE" o "FALSE". Cuando esta opción está configurada como "FALSE", la función de ajuste de escala de la pantalla se deshabilita en todos los escritorios remotos. Si esta opción no está configurada o se establece como "TRUE", (la opción predeterminada), el ajuste de escala de la pantalla está habilitado en todos los escritorios remotos.</p>
view.enableH264	Ninguna	<p>Habilita o deshabilita la decodificación H.264. Especifique "TRUE" o "FALSE". El valor predeterminado es "TRUE". Si desea obtener más información, consulte Configurar las opciones de VMware Blast.</p>
view.enableHEVC	Ninguna	<p>Habilita o deshabilita la decodificación HEVC. Especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE". Si desea obtener más información, consulte Configurar las opciones de VMware Blast.</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.enableMMR	Ninguna	Habilita o deshabilita el redireccionamiento multimedia (MMR). Especifique "TRUE" o "FALSE" . El valor predeterminado es "FALSE" .
view.enableRelativeMouse	Ninguna	Especifica si se fuerza que se habilite o deshabilite la función de mouse relativo de Horizon Client para la sesión actual de escritorio remoto. Si establece la clave de configuración, especifique "1" para forzar la habilitación de la función y "0" para forzar su deshabilitación. Los valores diferentes a estos no son válidos y se ignorarán. No se puede editar el valor especificado durante la sesión actual de escritorio remoto. Si el escritorio remoto no admite el mouse relativo, no se usará esta opción. Si esta opción no está configurada (opción predeterminada), los usuarios finales pueden habilitar y deshabilitar la función de mouse relativo usando Conexión > Habilitar mouse relativo en la barra de menú de Horizon Client.
view.fullScreen	--fullscreen	Oculto el sistema operativo del host y abre Horizon Client en modo de pantalla completa en un monitor. Esta opción no afecta al modo de pantalla de la sesión del escritorio remoto. Si establece la clave de configuración, especifique "TRUE" o "FALSE" . El valor predeterminado es "FALSE" .

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.kbdLayout	-k, --kbdLayout=	<p>Especifica qué configuración local usar en la distribución del teclado.</p> <p>Nota rdesktop usa códigos de configuración local, como "fr" y "de", mientras que freerdp usa los ID de distribución de teclado. Para obtener una lista de estos ID, use el siguiente comando:</p> <pre>xfreerdp --kbd-list</pre> <p>A continuación, se incluye un ejemplo del uso de la opción de la línea de comandos para rdesktop:</p> <pre>--kbdLayout="en-us" -k "fr"</pre> <p>A continuación, se incluye un ejemplo del uso de la opción de la línea de comandos para freerdp:</p> <pre>-k "0x00010407"</pre>
view.kioskLogin	--kioskLogin	<p>Especifica que Horizon Client se autentica mediante una cuenta de modo de quiosco.</p> <p>Si establece la clave de configuración, especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p> <p>Consulte el ejemplo de modo de quiosco que aparece tras esta tabla.</p>
Ninguno	--launchMinimized	<p>Inicia Horizon Client en modo minimizado. La ventana Horizon Client permanece minimizada y oculta en segundo plano mientras se inicia la aplicación publicada o el escritorio remoto especificados por el usuario.</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.monitors	<code>--monitors= <i>lista numerada</i></code>	<p>Le permite especificar los monitores adyacentes que utilizará para Horizon Client. Use <code>--allmonitors</code> (o <code>view.allMonitors</code>) para especificar que desea usar la pantalla completa en todos los monitores y <code>--monitors=lista numerada</code> para especificar el subconjunto de monitores que se usará.</p> <p>En el siguiente ejemplo se muestra cómo especificar el primer y el segundo monitor en una configuración en la que se establecen tres monitores horizontalmente uno junto al otro:</p> <pre>--allmonitors --monitors="1,2" `</pre> <p>Para ayudar a distinguir qué monitor físico está asociado a un icono de monitor en Horizon Client, aparece un rectángulo en la esquina superior izquierda del monitor físico que especificó que se debía utilizar. Este rectángulo tendrá el color y el número que utiliza el icono del monitor seleccionado.</p>
view.noMenuBar	<code>--nomenubar</code>	<p>Suprime la barra de menús de Horizon Client cuando el cliente está en modo de pantalla completa, por lo que el usuario no puede acceder a las opciones del menú para desconectarse de un escritorio remoto, restablecerlo o cerrar sesión en él. Utilice esta opción cuando configure el modo de quiosco.</p> <p>Si establece la clave de configuración, especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.nonInteractive	-q, --nonInteractive	<p>Oculto a los usuarios finales los pasos de la interfaz de usuario que no son necesarios al omitir las pantallas que se especifican en la línea de comandos o en las propiedades de configuración.</p> <p>Si establece la clave de configuración, especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p> <p>Si se establece esta propiedad en "TRUE", esta acción es equivalente a establecer las propiedades view.autoConnectBroker y view.autoConnectDesktop en "TRUE".</p> <p>Por ejemplo:</p> <pre>--nonInteractive --serverURL="https:// view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"</pre>
view.once	--once	<p>Especifica que no desea que Horizon Client vuelva a intentar la conexión si se produce un error.</p> <p>Especifique esta opción si utiliza el modo de quiosco y utilice el código de salida para solucionar el error. De lo contrario, puede resultar difícil eliminar el proceso vmware-view de forma remota.</p> <p>Si establece la clave de configuración, especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p>
view.rdesktopOptions	--rdesktopOptions=	<p>(Disponible si usa el protocolo de visualización Microsoft RDP). Especifica opciones de la línea de comandos para reenviarlas a la aplicación rdesktop. Para obtener más información acerca de las opciones rdesktop, consulte la documentación sobre dichas opciones.</p> <p>Por ejemplo:</p> <pre>--rdesktopOptions="-f -m"</pre>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
Ninguna	<code>-r, --redirect=</code>	<p>(Disponible si usa el protocolo de visualización Microsoft RDP). Especifica un dispositivo local para que rdesktop redireccione al escritorio remoto.</p> <p>Especifique la información del dispositivo que desea transferir a la opción <code>-r</code> de rdesktop. Puede establecer varias opciones de dispositivos en un único comando.</p> <p>Por ejemplo:</p> <pre>--redirect="sound:off"</pre>
<code>view.rdpClient</code>	<code>--rdpclient=</code>	<p>(Disponible si usa el protocolo de visualización Microsoft RDP). Especifica el tipo de cliente RDP que se usará. El predeterminado es <code>rdesktop</code>. Para usar FreeRDP en su lugar, especifique <code>xfreerdp</code>.</p> <p>Nota Para usar FreeRDP, debe tener instalada la versión adecuada de FreeRDP y las revisiones correspondientes. Si desea obtener más información, consulte Instalar y configurar FreeRDP.</p>
Ninguna	<code>--save</code>	<p>Guarda el nombre de usuario y de dominio que se usó la última vez para iniciar sesión correctamente, por lo que no será necesario que los introduzca la próxima vez que se le soliciten las credenciales de inicio de sesión.</p>
<code>view.sendCtrlAltDelToLocal</code>	Ninguna	<p>(Disponible si usa el protocolo de visualización VMware Blast o PCoIP). Cuando se establece como "TRUE", envía la combinación de teclas <code>Ctrl+Alt+Supr</code> al sistema cliente en lugar de abrir un cuadro de diálogo para solicitar al usuario que se desconecte del escritorio remoto. El valor predeterminado es "FALSE".</p> <p>Nota Si usa el protocolo de visualización Microsoft RDP, puede realizar esta función con la opción <code>-K</code>, por ejemplo, <code>vmware-view -K</code>.</p> <p>Esta opción tiene la misma prioridad que la configuración del archivo <code>/etc/vmware/view-keycombos-config</code>.</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.sendCtrlAltDelToVM	Ninguna	(Disponible si usa el protocolo de visualización VMware Blast o PCoIP). Cuando se establece como "TRUE" , envía la combinación de teclas Ctrl+Alt+Supr al escritorio remoto en lugar de abrir un cuadro de diálogo para solicitar al usuario que se desconecte del escritorio remoto. El valor predeterminado es "FALSE" . Esta opción tiene más prioridad que la configuración del archivo <code>/etc/vmware/view-keycombos-config</code> .
view.sendCtrlAltInsToVM	Ninguna	(Disponible si usa los protocolos de visualización VMware Blast o PCoIP). Si está configurada como "TRUE" , envía la combinación de teclas Ctrl+Alt+Insert al escritorio virtual en lugar de enviar la combinación Ctrl+Alt+Supr. El valor predeterminado es "FALSE" . Nota Para usar esta función, también debe establecer la configuración de directiva de grupo del agente Usar una tecla alternativa para enviar la secuencia de aviso de seguridad , disponible en el archivo de plantilla <code>pcoip.adm</code> . Para obtener más información, consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> . Esta opción tiene menos prioridad que la configuración del archivo <code>/etc/vmware/view-keycombos-config</code> .
view.shareRemovableStorage	Ninguna	Cuando se establece en "TRUE" , habilita la opción Permitir acceso a almacenamiento extraíble . El valor predeterminado es "TRUE" .
view.skipCRLRevocationCheck	--skipCRLRevocationCheck	De forma predeterminada, al conectarse a un servidor, Horizon Client comprueba y descarga la lista de revocación de certificados (CRL) del servidor. Esta opción de la línea de comandos indica a Horizon Client que detenga la comprobación de la CRL durante las conexiones. Si establece la clave de configuración, especifique "TRUE" para dejar de comprobar la CRL. El valor predeterminado es "FALSE" .

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.sslCipherString	--sslCipherString=	<p>Configura la lista de cifrado para restringir el uso de ciertos algoritmos criptográficos antes de establecer una conexión SSL cifrada.</p> <p>Para obtener una lista de cadenas de cifrado, consulte http://www.openssl.org/docs/apps/ciphers.html.</p> <p>El valor predeterminado de Horizon Client es "!"aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES".</p>
view.sslProtocolString	--sslProtocolString=	<p>Configura la lista de cifrado para restringir el uso de ciertos protocolos criptográficos antes de establecer una conexión SSL cifrada.</p> <p>Los protocolos admitidos son TLSv1.1 y TLSv1.2. La lista de cifrado consiste en una o varias cadenas de protocolos separadas por dos puntos. Estas cadenas no distinguen entre mayúsculas y minúsculas.</p> <p>El valor predeterminado es "TLSv1.1:TLSv1.2".</p>
view.sslVerificationMode	Ninguna	<p>Establece el modo de verificación del certificado del servidor.</p> <p>Especifique "1" para rechazar conexiones si se produce un error en el certificado al comprobar las verificaciones, "2" para mostrar una advertencia pero permitiendo que las conexiones usen un certificado autofirmado o "3" para permitir conexiones no verificables. Si especifica "3", no se realizarán comprobaciones de verificación. El valor predeterminado es "2".</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.UnauthenticatedAccessEnabled	--unauthenticatedAccessEnabled	<p>Si está establecida en "TRUE", la función Acceso sin autenticar está habilitada de forma predeterminada. La opción Iniciar sesión de forma anónima con Acceso sin autenticar aparece visible en la interfaz de usuario y está marcada como seleccionada.</p> <p>Si está establecida en "FALSE", la función Acceso sin autenticar está deshabilitada. La opción Iniciar sesión de forma anónima con Acceso sin autenticar está oculta y desmarcada.</p> <p>Cuando está establecida en " ", la función Acceso sin autenticar está deshabilitada y la opción Iniciar sesión de forma anónima con Acceso sin autenticar se puede ver en la interfaz de usuario y está desmarcada.</p> <p>Si establece la clave de configuración, especifique "TRUE" o "FALSE".</p> <p>Por ejemplo:</p> <pre>-- unauthenticatedAccessEnabled="TRUE"</pre>
view.UnauthenticatedAccessAccount	--unauthenticatedAccessAccount	<p>Especifica la cuenta que se utilizará cuando unauthenticatedAccessEnabled esté establecido en "TRUE".</p> <p>Si la unauthenticatedAccessEnabled está establecida en "FALSE", esta configuración se ignorará.</p> <p>En el siguiente ejemplo se muestra cómo utilizar esta opción de la línea de comandos con la cuenta de usuario anonymous1:</p> <pre>-- unauthenticatedAccessAccount='anonymous1'</pre>
view.usbAutoConnectAtStartup	--usbAutoConnectAtStartup=	<p>Redirecciona los dispositivos USB automáticamente a un escritorio remoto o aplicación publicada si los dispositivos USB se introducen en el sistema host antes de que se conecte el escritorio o la aplicación.</p> <p>Especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
view.usbAutoConnectOnInsert	--usbAutoConnectOnInsert=	<p>Redirecciona los dispositivos USB automáticamente a un escritorio remoto o una aplicación publicada cuando los dispositivos USB se introducen en el sistema host después de que se conecte el escritorio o la aplicación. Especifique "TRUE" o "FALSE". El valor predeterminado es "FALSE".</p>
view.xfreerdpOptions	--xfreerdpOptions=	<p>(Disponible si usa el protocolo de visualización Microsoft RDP). Especifica opciones de la línea de comandos para reenviarlas al programa xfreerdp. Para obtener más información acerca de las opciones xfreerdp, consulte la documentación sobre dichas opciones xfreerdp.</p> <p>Nota Para usar FreeRDP, debe tener instalada la versión adecuada de FreeRDP y las revisiones correspondientes. Si desea obtener más información, consulte Instalar y configurar FreeRDP.</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
Ninguna	<code>--useExisting</code>	<p>Le permite iniciar varias aplicaciones publicadas y escritorios remotos desde una sesión única. Cuando se especifica esta opción, Horizon Client determina si ya hay una sesión conectada a la misma URL del servidor. Si es así, Horizon Client utiliza esa sesión en lugar de iniciar una nueva.</p> <p>Si hay una sesión conectada a otra URL del servidor, Horizon Client se desconecta de esa sesión e inicia una sesión conectada a la nueva URL del servidor. Si existen varias sesiones con la misma URL de servidor, Horizon Client se desconecta de la sesión más antigua antes de crear la nueva.</p> <p>En el siguiente ejemplo, el usuario 1 inicia la aplicación Calculadora y se crea una nueva sesión.</p> <pre>vmware-view -serverURL view.mycompany.com -userName user1 -password 'secret' -domainName domain -appName Calculator</pre> <p>En el ejemplo siguiente, el usuario 1 inicia la aplicación Paint con la misma URL de servidor, por lo que se utiliza la misma sesión.</p> <pre>vmware-view -serverURL view.mycompany.com -userName user1 -password 'secret' -domainName domain -appName Paint -- useExisting</pre> <p>En el ejemplo siguiente, el usuario 1 inicia la aplicación Calculadora con una URL de servidor diferente. Horizon Client se desconecta de la primera sesión con view.mycompany.com e inicia una nueva sesión con horizon.mycompany.com.</p> <pre>vmware-view -serverURL horizon.mycompany.com -userName user1 -password 'secret' -domainName domain -appName Calculator --useExisting</pre>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
Ninguna	<code>--enableNla</code>	<p>(Se aplica si utiliza FreeRDP para las conexiones RDP). Habilita la autenticación a nivel de red (NLA). Debe utilizar esta opción y la opción <code>--ignore-certificate</code>. Si desea obtener más información, consulte Utilizar FreeRDP para las conexiones RDP.</p> <p>Si utiliza FreeRDP, NLA estará desactivado de forma predeterminada.</p> <p>Debe tener instalada la versión adecuada de FreeRDP y las revisiones correspondientes. Si desea obtener más información, consulte Instalar y configurar FreeRDP.</p> <p>Nota El programa <code>rdesktop</code> no es compatible con NLA.</p>
Ninguna	<code>--printEnvironmentInfo</code>	<p>Muestra información sobre el entorno de un dispositivo cliente, incluidos el nombre de dominio, el nombre de equipo, la dirección MAC y la dirección IP.</p> <p>En el modo de quiosco, puede crear una cuenta para el cliente en función de la dirección MAC. Para mostrar la dirección MAC, use esta opción con la opción <code>-s</code>.</p> <p>Por ejemplo:</p> <pre>--printEnvironmentInfo -s view.company.com</pre>
Ninguna	<code>--usb=</code>	<p>Especifica las opciones que se usarán para el redireccionamiento USB. Si desea obtener más información, consulte Requisitos del sistema para la función de redireccionamiento USB.</p>
Ninguna	<code>--version</code>	<p>Muestra la información de la versión de Horizon Client.</p>

Tabla 3-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (continuación)

Clave de configuración	Opción de línea de comandos	Descripción
Ninguno	--tokenUserName	<p>Para la autenticación de RSA SecurID o RADIUS, especifica el nombre de usuario del token. Si no utiliza esta opción, o si la opción está vacía, se utilizará el nombre de usuario de Active Directory.</p> <p>Para especificar el código de acceso de autenticación de RADIUS o RSA SecurID, utilice la opción --passcode.</p> <p>En el siguiente ejemplo se muestra cómo utilizar la opción -q para iniciar sesión sin la interacción del usuario en Horizon Client. Si no especifica la opción -q, la página de inicio de sesión de RSA SecurID o RADIUS aparecerá en Horizon Client.</p> <pre>vmware-view -- serverURL='12.345.67.89' -q --tokenUserName='pwduser' -- userName=' johndoe' --password='password' -- domainName='mydomain' --passcode='passcode'</pre>
Ninguno	--passcode	<p>Especifica el código de acceso para la autenticación RSA SecurID o RADIUS. El código de acceso solo se puede usar una vez.</p> <p>Utilice esta opción junto con la opción --tokenUserName.</p>

Ejemplo: Ejemplo de modo de quiosco

Entre los usuarios del modo de quiosco, se pueden incluir clientes en estaciones de registros de líneas aéreas, estudiantes en clases o bibliotecas, personal sanitario en estaciones de trabajo en las que se introducen información médica o clientes en puntos de autoservicio. Las cuentas están asociadas con dispositivos cliente en lugar de con usuarios, ya que los usuarios no necesitan iniciar sesión para usar el dispositivo cliente o el escritorio remoto. Aun así, se les solicitará a los usuarios que proporcionen credenciales de autenticación en algunas aplicaciones.

Para configurar el modo de quiosco, debe usar la interfaz de la línea de comandos `vdmadmin` en la instancia de Horizon Connection Server y realizar varios procedimientos que aparecen en el capítulo sobre el modo de quiosco del documento *Administración de Horizon 7*. Tras configurar el modo de quiosco, puede usar el comando `vmware-view` en un cliente Linux para conectarse a un escritorio remoto en modo de quiosco.

Para conectarse a escritorios remotos desde clientes Linux en modo de quiosco, debe incluir como mínimo las siguientes claves de configuración u opciones de la línea de comandos.

Clave de configuración	Opciones de la línea de comandos equivalentes
view.kioskLogin	--kioskLogin
view.nonInteractive	-q, --nonInteractive
view.fullScreen	--fullscreen
view.noMenuBar	--nomenubar
view.defaultBroker	-s, --serverURL=

El modo de quiosco no admite la omisión de estas opciones de configuración. Si Horizon Connection Server se configura de forma que sea necesario un nombre de usuario de quiosco no predeterminado, también debe configurar la propiedad `view.defaultUser` o utilizar las opciones de la línea de comandos `-u` o `--userName=`. Si no es necesario un nombre de usuario no predeterminado y no necesita especificar un nombre de usuario, Horizon Client puede derivarse y utilizar el nombre de usuario de quiosco predeterminado.

Nota Si configura la clave de configuración de `view.sslVerificationMode`, configúrela en el archivo `/etc/vmware/view-mandatory-config`. Cuando se ejecuta el cliente en modo de quiosco, no aparece en el archivo `view-preferences`.

El comando que se muestra en este ejemplo ejecuta Horizon Client en un sistema cliente Linux y cuenta con la siguientes características:

- El nombre de la cuenta del usuario se establece en función de la dirección MAC del cliente.
- Horizon Client se ejecuta en pantalla completa sin una barra de menús de Horizon Client.
- Los usuarios se conectan automáticamente a la instancia de Horizon Connection Server y al escritorio remoto especificados sin tener que introducir sus credenciales de inicio de sesión.
- Si se produce un error de conexión, en función del código de error que se devuelva, se puede ejecutar un script o puede solventar el error un programa de supervisión de quiosco. Como resultado, por ejemplo, el sistema cliente podría mostrar una pantalla de fuera de servicio o podría esperar durante cierto tiempo antes de intentar conectarse de nuevo a Horizon Connection Server.

```
./vmware-view --kioskLogin --nonInteractive --once --fullscreen --nomenubar
--serverURL="server.mycompany.com" --userName="CM-00:11:22:33:44:55:66:77" --password="mypassword"
```

Importante Si se configuró un mensaje previo al inicio de sesión para que aparezca antes de permitir que Horizon Client se conecte a un escritorio remoto, el usuario debe confirmar el mensaje antes de que se le permita acceder al escritorio. Para evitar este problema, utilice Horizon Console para deshabilitar los mensajes previos al inicio de sesión.

Utilizar URI para configurar Horizon Client

Puede utilizar identificadores uniformes de recursos (URI) para crear páginas web o vínculos de correos electrónicos para que los usuarios finales puedan hacer clic para iniciar Horizon Client, conectarse a un servidor o abrir un escritorio remoto o una aplicación publicada.

Para ello, deberá crear URI que ofrezcan toda la información (o parte de ella) que se indica a continuación para que los usuarios finales no tengan que proporcionarla.

- Dirección de servidor
- Número de puerto para el servidor de conexión
- Nombre de usuario de Active Directory
- Nombre de dominio
- Nombre para mostrar del escritorio remoto o la aplicación publicada
- Tamaño de la ventana
- Acciones (como restablecer e iniciar o cerrar sesión)
- Protocolo de visualización

Para crear un URI, deberá utilizar el esquema URI `vmware-view` con la ruta y las partes de consulta específicas de Horizon Client.

Si desea usar los URI para iniciar Horizon Client, Horizon Client debe estar instalado en los equipos cliente.

Sintaxis para crear URI de vmware-view

La sintaxis de URI incluye el esquema URI `vmware-view`, una parte de la ruta que se utiliza para especificar el escritorio remoto o la aplicación publicada y, de forma opcional, una consulta que se utiliza para indicar acciones de la aplicación publicada, el escritorio remoto u opciones de configuración.

Especificación de URI

Al crear un URI, básicamente está llamando a `vmware-view` con la cadena completa de URI de Horizon como un argumento.

Utilice la siguiente sintaxis para crear los URI e iniciar Horizon Client.

```
vmware-view://[authority-part]/[path-part][?query-part]
```

El único elemento necesario es el esquema URI, `vmware-view`. Como el nombre del esquema distingue entre mayúsculas y minúsculas en algunas versiones de ciertos sistemas operativos cliente, escriba `vmware-view`.

Importante En todas las partes, se deben codificar primero los caracteres que no sean-ASCII según UTF-8 [STD63]. A continuación, cada octeto de la secuencia UTF-8 correspondiente se debe codificar con porcentaje para representarse como caracteres URI.

Para obtener información sobre la codificación de caracteres ASCII, consulte la referencia de codificación de URL de <http://www.utf8-chartable.de/>.

authority-part

La dirección del servidor y, de manera opcional, un nombre de usuario, un número de puerto no predeterminado o ambos. Los nombres de los servidores no admiten guiones bajos (_). Los nombres de servidor deben adaptarse a la sintaxis de DNS.

Para especificar un nombre de usuario, utilice la siguiente sintaxis.

```
user1@server-address
```

No puede especificar una dirección UPN, que incluye el dominio. Para especificar el dominio, puede utilizar la parte de la consulta `domainName` en la URI.

Para especificar un número de puerto, utilice la siguiente sintaxis.

```
server-address:port-number
```

path-part

El nombre para mostrar del escritorio remoto o de la aplicación publicada. El nombre para mostrar se especifica en Horizon Console cuando se crea el grupo de escritorios o de aplicaciones. Si el nombre para mostrar contiene un espacio, utilice el mecanismo de codificación `%20` para representar el espacio.

Opcionalmente, puede especificar un identificador de aplicación o de escritorio, que es una cadena de ruta que incluye el identificador del grupo de aplicaciones o escritorios. Para buscar un identificador de escritorio o aplicaciones, abra el Editor ADSI en el host del servidor de conexión, vaya a `DC=vdi,dc=vmware,dc=int` y seleccione el nodo `OU=Applications`. Se mostrarán todos los grupos de aplicaciones y escritorios. El atributo `distinguishedName` especifica el valor del identificador ID. Debe codificar el valor del identificador antes de

especificarlo en un URI (por ejemplo, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

Nota Varios escritorios remotos o aplicaciones publicadas pueden tener el mismo nombre para mostrar, pero el identificador de cada aplicación y cada escritorio son únicos. Para especificar un escritorio remoto o una aplicación publicada en particular, utilice el identificador de la aplicación o el escritorio en lugar del nombre para mostrar.

query-part

Las opciones de configuración que se usarán o las acciones que realizarán las aplicaciones publicadas o los escritorios remotos. Las consultas no distinguen entre mayúsculas y minúsculas. Para utilizar varias consultas, utilice el signo et (&) entre ellas. Si existe algún conflicto en las consultas, Horizon Client usa la última consulta de la lista. Utilice la siguiente sintaxis.

```
query1=value1[&query2=value2. . .]
```

Consultas admitidas

Se admiten las siguientes consultas para este tipo de Horizon Client. Si va a crear URI para varios tipos de cliente, como clientes de escritorio y clientes móviles, consulte la guía de instalación y configuración para cada tipo de sistema cliente de la lista de consultas admitidas.

action

Tabla 3-3. Valores que se pueden utilizar con la consulta action

Valor	Descripción
browse	Muestra una lista de las aplicaciones publicadas y los escritorios remotos disponibles y alojados en el servidor especificado. No tendrá que especificar un escritorio remoto ni una aplicación publicada al utilizar esta acción.
start-session	Abre la aplicación publicada o el escritorio remoto especificados. Si no se proporciona ninguna consulta action y se facilita el nombre de la aplicación publicada o del escritorio remoto, start-session es la acción predeterminada.
reset	Apaga y reinicia la aplicación publicada o el escritorio remoto especificados. Se pierden los datos que no se hayan guardado. La acción de reiniciar un escritorio remoto es equivalente a pulsar el botón Reiniciar en un equipo físico.
restart	Apaga y reinicia el escritorio remoto especificado. Reiniciar un escritorio remoto es el equivalente del comando de reinicio del sistema operativo Windows. El sistema operativo suele solicitar al usuario que guarde los datos que no se guardarán antes de reiniciar.
logout	Cierra la sesión del usuario en el sistema operativo invitado del escritorio remoto. Si especifica una aplicación publicada, la acción se ignorará o el usuario final verá el mensaje de error "Acción de URI no válida".

args

Especifica los argumentos de la línea de comandos que se agregan cuando se inicia la aplicación publicada. Utilice la sintaxis `args=value`, en el que *value* es una cadena. Utilice la codificación con porcentajes para los siguientes caracteres:

- Para los dos puntos (:), utilice **%3A**.
- Para una barra diagonal inversa (\), utilice **%5C**.
- Para un espacio (), utilice **%20**.
- Para unas comillas dobles ("), use **%22**.

Por ejemplo, para especificar el nombre de archivo "My new file.txt" para la aplicación Notepad++, utilice **%22My%20new%20file.txt%22**.

appProtocol

Para las aplicaciones publicadas, los valores válidos son **PCOIP** y **BLAST**. Por ejemplo, para especificar PCoIP, utilice la sintaxis **appProtocol=PCOIP**.

desktopLayout

Establece el tamaño de la ventana del escritorio remoto. Para utilizar esta consulta, debe establecer la consulta *action* en **start-session** o no tener ninguna consulta *action*.

Tabla 3-4. Valores válidos para la consulta desktopLayout

Valor	Descripción
fullscreen	Pantalla completa en un monitor. Este valor es el predeterminado.
multimonitor	Pantalla completa en todos los monitores.
windowLarge	Ventana grande.
windowSmall	Ventana pequeña.
WxH	Resolución personalizada, en la que puede especificar el ancho y el alto en píxeles. Un ejemplo de sintaxis es desktopLayout=1280x800 .

desktopProtocol

Para los escritorios remotos, los valores válidos son **RDP**, **PCOIP** y **BLAST**. Por ejemplo, para especificar PCoIP, utilice la sintaxis **desktopProtocol=PCOIP**.

domainName

Especifica el nombre de dominio NETBIOS asociado al usuario que se conecta a la aplicación publicada o al escritorio remoto. Por ejemplo, puede usar `mycompany` en lugar de `mycompany.com`.

launchMinimized

Inicia Horizon Client en modo minimizado. La ventana Horizon Client permanece minimizada y oculta en segundo plano mientras se inicia la aplicación publicada o el escritorio remoto especificados por el usuario. La sintaxis es **launchMinimized=true**. El valor predeterminado es **false**.

useExisting

Si a esta opción se le asigna el valor **true**, solo se podrá ejecutar una instancia de Horizon Client. Si los usuarios intentan conectarse a un segundo servidor, deberán cerrar sesión en el primero, lo que provocará que las sesiones de aplicaciones publicadas y escritorios remotos se desconecten. Si a esta opción se le asigna el valor **false**, se podrán ejecutar varias instancias de Horizon Client y los usuarios se podrán conectar a varios servidores a la vez. El valor predeterminado es **true**. Un ejemplo de sintaxis es **useExisting=false**.

unauthenticatedAccessEnabled

Si esta opción está establecida como **true**, la función Acceso sin autenticar está habilitada de forma predeterminada. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** aparece seleccionada y visible en la interfaz de usuario. Si esta opción está establecida como **false**, la función Acceso sin autenticar está deshabilitada. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está desmarcada y oculta. Cuando esta opción está establecida como "", la función Acceso sin autenticar está deshabilitada y la opción **Iniciar sesión de forma anónima con Acceso sin autenticar** se puede ver en la interfaz de usuario y está desmarcada. Un ejemplo de sintaxis es **unauthenticatedAccessEnabled=true**.

unauthenticatedAccessAccount

Si la función Acceso sin autenticar está habilitada, configura la cuenta que se usará. Si la función Acceso sin autenticar está deshabilitada, esta consulta se ignora. Un ejemplo de sintaxis con la cuenta de usuario **anonymous1** es **unauthenticatedAccessAccount=anonymous1**.

Ejemplos de URI vmware-view

Puede usar el esquema URI **vmware-view** para crear botones o vínculos de hipertexto, e incluir estos vínculos en un correo electrónico o en una página web. Por ejemplo, un usuario final puede hacer clic en un vínculo URI para iniciar un escritorio remoto con las opciones de inicio que especifique.

Ejemplos de sintaxis de URI

Cada ejemplo de URI aparece con una descripción sobre qué es lo que el usuario final ve después de hacer clic en el vínculo del URI.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. El cuadro de diálogo de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio remoto cuyo nombre para mostrar es `Escritorio primario` y el usuario inicia sesión en el sistema operativo cliente.

Nota En este ejemplo, se utilizan el protocolo de visualización y el tamaño de ventana predeterminados. El protocolo de visualización predeterminado es PCoIP y el tamaño predeterminado de la ventana es pantalla completa.

Es posible cambiar estos valores predeterminados. Consulte [Utilizar los archivos de configuración y la interfaz de línea de comandos de vmware-view](#).

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. El cuadro de diálogo de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Después de iniciar sesión correctamente, el cliente se conectará al escritorio remoto que tiene el identificador de escritorio `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (valor codificado `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Este URI tiene el mismo efecto que el ejemplo anterior, excepto que usa el puerto 7555 no predeterminado para la instancia del servidor de conexión. (El puerto predeterminado es 443). Dado que se proporciona el identificador del escritorio remoto, este se abre aunque la acción `start-session` no se incluya en el URI.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCoIP`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. En el cuadro de diálogo de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con `fred`. El usuario debe proporcionar el nombre de dominio y la contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio remoto cuyo nombre para mostrar es `Escritorio de finanzas` y el usuario inicia sesión en el sistema operativo cliente. La conexión utiliza el protocolo de visualización PCoIP.

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. En el cuadro de diálogo de inicio de sesión, el usuario debe proporcionar el nombre de usuario, de dominio y la contraseña. Después de iniciar sesión correctamente, el cliente se conecta a la aplicación publicada que tiene el nombre para mostrar `Calculadora`. La conexión utiliza el protocolo de visualización VMware Blast.

6 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. En el cuadro de diálogo de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con `fred` y el cuadro de texto **Dominio** se rellena con `mycompany`. El usuario solo debe proporcionar una contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio remoto cuyo nombre para mostrar es `Escritorio de finanzas` y el usuario inicia sesión en el sistema operativo cliente.

7 `vmware-view://view.mycompany.com/`

Horizon Client se inicia y se muestra la solicitud de inicio de sesión para que el usuario se conecte al servidor `view.mycompany.com`.

8 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. El cuadro de diálogo de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, Horizon Client muestra un cuadro de diálogo que le solicita al usuario que confirme la operación para restablecer el `Escritorio primario`.

Nota Esta acción solo está disponible si Horizon Administrator habilitó la función de restablecimiento para el escritorio remoto.

9 `vmware-view://view.mycompany.com/Primary%20Desktop?action=restart`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. El cuadro de diálogo de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, Horizon Client muestra un cuadro de diálogo que le solicita al usuario que confirme la operación para restablecer el `Escritorio primario`.

Nota Esta acción solo está disponible si Horizon Administrator habilitó la función de restablecimiento para el escritorio remoto.

10 `vmware-view://`

Horizon Client se inicia y aparece la página en la que el usuario tiene que introducir la dirección de un servidor.

11 `vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22`

Inicia Notepad++ en el servidor `10.10.10.10` y envía el argumento `My new file.txt` al comando del inicio de la aplicación publicada. El nombre del archivo aparece entre comillas dobles porque contiene espacios.

12 `vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt`

Inicia Notepad++ 12 en el servidor 10.10.10.10 y envía el argumento `a.txt b.txt` al comando del inicio de la aplicación publicada. Dado que los argumentos no están entre comillas, un espacio separa los nombres de los archivos y ambos archivos se abren de forma independiente en Notepad++.

Nota Las aplicaciones publicadas pueden utilizar los argumentos de la línea de comandos de forma diferente. Por ejemplo, si envía el argumento `a.txt b.txt` a WordPad, este último solo abrirá un archivo, `a.txt`.

13 `vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1`

Horizon Client se inicia y se conecta al servidor `view.mycompany.com` utilizando la cuenta de usuario **anonymous1**. Se inicia la aplicación Bloc de notas sin solicitar al usuario que proporcione las credenciales de inicio de sesión.

Ejemplos de códigos HTML

Si lo desea, puede utilizar los URI para hacer que los botones y los vínculos de hipertexto se incluyan en correos electrónicos o en páginas web. Los siguientes ejemplos muestran cómo usar el URI en el primer ejemplo de URI para codificar un vínculo de hipertexto etiquetado como **Test Link** y un botón etiquetado como **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Configurar las opciones de VMware Blast

Puede configurar las opciones de VMware Blast para las sesiones de aplicaciones publicadas y escritorios remotos que utilizan el protocolo de visualización VMware Blast.

Puede permitir la decodificación H.264 y la codificación de vídeo de alta eficacia (HEVC). H.264 es un estándar del sector para la compresión de vídeo, que es el proceso de convertir vídeo digital en un formato que ocupe menos cuando se almacene o se transmita. Cuando se permite la decodificación H.264, también puede permitir una mayor fidelidad del color. Esta función no es compatible con procesadores ARM.

La resolución máxima que se admite depende de la capacidad de la unidad de procesamiento gráfico (GPU) en el cliente. Una GPU que puede admitir 4K de resolución para JPEG/PNG, es posible que no admita esta misma resolución para H.264.

La decodificación H.264 es compatible en las GPU de AMD, NVIDIA e Intel. La decodificación H.264 requiere que la biblioteca gráfica OpenGL 3.2 o una versión posterior esté instalada para las GPU de AMD y NVIDIA.

Si tiene pensado usar la decodificación H.264 con una GPU de NVIDIA, instale VDPAU (API para decodificación y presentación de vídeos para UNIX). VDPAU ya no se incluye con el controlador NVIDIA más reciente y debe instalarse de forma independiente.

Para usar H.264 con una GPU de Intel, se necesitan el controlador VA API de Intel y las bibliotecas VA-API de GLX. Al ejecutar el comando `va-info`, se muestran los perfiles H.264.

Si su entorno utiliza un servidor proxy, puede especificar si desea permitir conexiones de VMware Blast con un servidor proxy del sistema operativo.

Para los servidor proxy SSL, también debe configurar la comprobación de certificados para las conexiones secundarias a través de servidores proxy SSL. Si desea obtener más información, consulte [Configurar el modo de comprobación del certificado en Horizon Client](#).

Puede configurar las opciones de VMware Blast antes o después de conectarse a un servidor.

Requisitos previos

- Para usar la decodificación H.264, debe estar instalada la versión 7.0 o posterior de Horizon Agent.
- Para aumentar la fidelidad del color cuando se permita la decodificación H.264, se debe instalar Horizon Agent 7.4 o una versión posterior.
- Para utilizar la codificación de vídeo de alta eficacia (HEVC), debe tener instalado Horizon Agent 7.7 o una versión posterior. Para aumentar la precisión del color con YUV 4:4:4, se debe instalar Horizon Agent 7.11 o una versión posterior. Además, el sistema cliente debe tener una GPU que admita la decodificación HEVC.

Según la versión de Horizon Agent que esté instalada, un administrador de Horizon puede usar la configuración de directiva de grupo del agente para habilitar o deshabilitar las funciones de VMware Blast, incluidas la alta precisión de color HEVC y H.264. Para obtener información, consulte "Configuración de directivas de VMware Blast" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Procedimiento

- 1 Inicie Horizon Client.
- 2 Seleccione **Archivo > Configurar VMware Blast** en la barra de menús.
- 3 Para permitir la decodificación H.264 en Horizon Client, seleccione la casilla de verificación **Permitir la decodificación H.264**.
 - Cuando esta opción está seleccionada (la opción predeterminada) y la GPU cliente tenga un decodificador de hardware H.264, Horizon Client usa un decodificador de hardware H.264 4.2.0.

- Cuando esta opción está seleccionada, si la GPU cliente no tiene ningún decodificador de hardware H.264 y la función para aumentar la fidelidad del color no se admite, Horizon Client usa el decodificador de software H.264 4.2.0.
 - Cuando se desmarca esta opción, Horizon Client usa la descodificación JPG/PNG.
- 4 Si desea permitir que se aumente la fidelidad del color cuando se permita la decodificación H.264 en Horizon Client, seleccione la casilla de verificación **Permitir alta precisión de color (disminuye el rendimiento y la duración de la batería)**.
- Cuando esta opción está seleccionada, Horizon Client usa el decodificador de software H.264 4.4.4, independientemente de si la GPU cliente cuenta con un decodificador de hardware H.264. Esta opción puede reducir el rendimiento y la duración de la batería. Esta función está deshabilitada de forma predeterminada.
- 5 Para permitir HEVC, seleccione la casilla **Permitir decodificación de vídeo de alta eficacia (HEVC)**.
- Cuando esta opción está seleccionada, el rendimiento y la calidad de imagen mejoran si la máquina cliente tiene una GPU que admite la descodificación HEVC. Esta función está deshabilitada de forma predeterminada.
- Si selecciona esta opción, pero el equipo cliente no tiene una GPU que admita la decodificación HEVC, Horizon Client usará la decodificación H.264 en su lugar.
- 6 Para permitir conexiones de VMware Blast a través de un servidor proxy, active la casilla de verificación **Permitir que las conexiones de Blast utilicen la configuración de proxy del sistema operativo**.
- 7 Haga clic en **Aceptar** para guardar los cambios.

Resultados

Se efectuarán los cambios la próxima vez que un usuario se conecte a una aplicación publicada o un escritorio remoto y seleccione el protocolo de visualización VMware Blast. Los cambios no afectan a las sesiones VMware Blast existentes.

Configurar el uso compartido de datos de Horizon Client

Si un administrador de Horizon decidió participar en el programa de mejora de la experiencia de cliente (CEIP), VMware recopila y recibe datos anónimos de los sistemas cliente a través del servidor de conexión. Puede decidir si quiere compartir los datos de este cliente con el servidor de conexión.

Para obtener más información sobre cómo configurar Horizon para que se una a CEIP, consulte el documento *Administración de VMware Horizon Console*.

El uso compartido de datos está habilitado de forma predeterminada en Horizon Client. La clave de configuración `view.enableDataSharing` está establecida inicialmente como "TRUE" en el archivo `~/.vmware/view-preferences`. Debe configurar la opción de uso compartido de datos antes de conectarse a un servidor. La opción se aplica a todos los servidores. No puede cambiar la opción de uso compartido de datos de Horizon Client después de conectarse a un servidor.

Procedimiento

- 1 Seleccione **Archivo > Configurar el uso compartido de datos** en la barra de menú.
- 2 Seleccione o desmarque la casilla de verificación **Permitir el uso compartido de datos**.
- 3 Haga clic en **Aceptar** para guardar los cambios.

Su preferencia se almacena con la clave de configuración de `view.enableDataSharing` del archivo de configuración `~/.vmware/view-preferences`.

Datos de Horizon Client recopilados por VMware

Si un administrador de Horizon ha decidido participar en el programa de mejora de la experiencia de cliente y el uso compartido de datos está habilitado en el sistema cliente, VMware recopila datos sobre el sistema cliente.

VMware recopila datos sobre los sistemas cliente para priorizar la compatibilidad entre el hardware y el software. Si su administrador de Horizon decidió participar en el programa de mejora de la experiencia de cliente, VMware recopila datos anónimos acerca de la implementación para responder mejor a los requisitos del cliente. VMware no recopila información que identifique a su organización. La información de Horizon Client se envía primero a la instancia del servidor de conexión y después a VMware, junto con los datos del servidor de conexión, los grupos de escritorios y los escritorios remotos.

La información se cifra cuando está en tránsito hacia la instancia del servidor de conexión. La información del sistema cliente se registra sin cifrar en un directorio específico del usuario. Los registros no contienen información de identificación personal.

Un administrador de Horizon puede decidir si desea participar en el programa de mejora de la experiencia de cliente de VMware cuando se esté instalando el servidor de conexión o puede hacerlo configurando una opción en Horizon Console después de la instalación.

Tabla 3-5. Datos recopilados de las instancias de Horizon Client para el programa de mejora de la experiencia de cliente

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Compañía que desarrolló la aplicación Horizon Client	No	VMware
Nombre de producto	No	VMware Horizon Client
Versión del producto del cliente	No	(El formato es <code>x.x.x-yyyyyy</code> , donde <code>x.x.x</code> es el número de la versión cliente e <code>yyyyyy</code> es el número de compilación).

Tabla 3-5. Datos recopilados de las instancias de Horizon Client para el programa de mejora de la experiencia de cliente (continuación)

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Arquitectura binaria del cliente	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ i386 ■ x86_64 ■ arm
Nombre de compilación del cliente	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Sistema operativo del host	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Compilación 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Kernel del sistema operativo del host	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ desconocido (para la Tienda Windows)
Arquitectura del sistema operativo del host	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ x86_64 ■ i386 ■ armv71 ■ ARM
Modelo de sistema del host	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Estación de trabajo Dell Inc. Precision T3400 (A04 03/21/2008)
CPU de sistema del host	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ desconocido (para iPad)

Tabla 3-5. Datos recopilados de las instancias de Horizon Client para el programa de mejora de la experiencia de cliente (continuación)

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Número de núcleos en el procesador del sistema del host	No	Por ejemplo: 4
MB de memoria en el sistema del host	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ 4096 ■ desconocido (para la Tienda Windows)
Número de dispositivos USB conectados	No	2 (el redireccionamiento de dispositivos USB es compatible solo con los clientes Linux, Windows y Mac).
Número máximo de conexiones simultáneas de dispositivos USB	No	2
ID del proveedor del dispositivo USB	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID del producto del dispositivo USB	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Data Traveler ■ Controlador para juegos ■ Unidad de almacenamiento ■ Mouse inalámbrico
Familia de dispositivos USB	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Seguridad ■ Dispositivo de interfaz de usuario ■ Imágenes
Recuento del uso del dispositivo USB	No	(Número de veces que se compartió el dispositivo)

Configurar el modo de comprobación de certificados para usuarios finales

Puede configurar el modo de comprobación de certificados para usuarios finales. Por ejemplo, puede configurar que la verificación completa siempre se realice. La comprobación del certificado se aplica a las conexiones TLS entre un servidor y Horizon Client.

Puede configurar una de las siguientes estrategias de verificación de certificados para los usuarios finales.

- Los usuarios finales pueden seleccionar el modo de comprobación de certificados en Horizon Client.
- (Sin verificación) No se comprueban los certificados.
- (Advertir) Si el servidor presenta un certificado autofirmado, se le advierte a los usuarios finales. Los usuarios pueden determinar si desean permitir este tipo de conexión.

- (Seguridad completa) Se realiza una verificación completa y se rechazan las conexiones que dicha verificación no apruebe.

Si utiliza un servidor proxy SSL para inspeccionar el tráfico enviado desde el entorno de cliente a Internet, puede configurar la comprobación de certificados para las conexiones secundarias a través del servidor proxy SSL. Esta función se aplica tanto a la puerta de enlace segura Blast como a las conexiones de túnel seguro. También puede permitir el uso del servidor proxy para las conexiones de VMware Blast.

Para obtener más información sobre los tipos de comprobaciones de certificados que se pueden llevar a cabo, consulte [Configurar el modo de comprobación del certificado en Horizon Client](#).

Puede establecer los ajustes del servidor proxy y el modo de comprobación del certificado predeterminado configurando las propiedades del archivo `/etc/vmware/view-mandatory-config`.

Para establecer el modo de comprobación del certificado predeterminado, establezca uno de los siguientes valores para la propiedad `view.sslVerificationMode`.

- **1** implementa Full Verification.
- **2** implementa Warn If the Connection May Be Insecure.
- **3** implementa No Verification Performed.

Para configurar el modo de comprobación del certificado de forma que los usuarios finales no puedan cambiarlo, establezca el valor **"False"** para la propiedad `view.allowSslVerificationMode`. Para establecer esta propiedad desde la línea de comandos, consulte [Opciones de la línea de comandos y configuración de Horizon Client](#).

Para configurar el ajuste **Permitir conexión a través de un proxy SSL** de forma que los usuarios finales no puedan cambiarlo, establezca el valor **"False"** para la clave `view.allowAllowSslProxy`.

Para establecer el valor predeterminado del ajuste **Permitir conexión a través de un proxy SSL**, configure la propiedad `view.allowSslProxy`. **"True"** la habilita y **"False"** la deshabilita.

Para establecer el valor predeterminado para el ajuste **Permitir que las conexiones de Blast utilicen la configuración de proxy del sistema operativo**, configure la propiedad `view.allowBlastProxy`. **"True"** la habilita y **"False"** la deshabilita.

Para configurar el ajuste **Permitir que las conexiones de Blast utilicen la configuración de proxy del sistema operativo** de forma que los usuarios finales no puedan cambiarlo, establezca el valor **"False"** para la clave `view.allowAllowBlastProxy`.

Configurar las opciones de TLS avanzadas

Puede seleccionar los protocolos de seguridad y los algoritmos criptográficos que se utilizan para cifrar la comunicación entre Horizon Client y los servidores, y entre Horizon Client y el agente en un escritorio remoto.

Estas opciones también se utilizan para cifrar el canal USB (comunicación entre el demonio del servicio USB y el agente).

Con la configuración predeterminada, los paquetes de cifrado usan AES de 128 o 256 bits, eliminan los algoritmos DH anónimos y, a continuación, ordenan la lista de cifrado actual de acuerdo con la longitud de la clave del algoritmo de cifrado.

De forma predeterminada, TLS v1.1 y TLS v1.2 están habilitados. No se admiten SSL v2.0, SSL v3.0 ni TLS v1.0.

Si configura un protocolo de seguridad para Horizon Client que no está habilitado en el servidor al que el cliente se conecta, se produce un error TLS y de conexión.

Importante Al menos uno de los protocolos que habilita en Horizon Client también debe estar habilitado en el escritorio remoto o los dispositivos USB no se podrán redireccionar a dicho escritorio.

En el sistema cliente, puede usar las propiedades del archivo de configuración o las opciones de la línea de comandos para la siguiente configuración:

- Para usar las propiedades del archivo de configuración, utilice las propiedades `view.sslProtocolString` y `view.sslCipherString`.
- Para usar las opciones de la configuración de la línea de comandos, use las opciones `--sslProtocolString` y `--sslCipherString`.

Para obtener más información, consulte [Utilizar los archivos de configuración y la interfaz de línea de comandos de vmware-view](#) y busque el nombre de la opción y de la propiedad en la tabla que aparece en [Opciones de la línea de comandos y configuración de Horizon Client](#).

Configurar teclas específicas y combinaciones de teclas para enviarlas al sistema local

Tanto con Horizon Client, si utiliza PCoIP, como con Horizon Client 4.0, si utiliza VMware Blast o PCoIP, puede crear un archivo `view-keycombos-config` para especificar las teclas individuales y las combinaciones de teclas que no se deben enviar al escritorio remoto.

Cuando trabaje en un escritorio remoto, es posible que prefiera tener algunas teclas o combinaciones controladas por el sistema cliente local. Por ejemplo, es posible que quiera usar una combinación de teclas determinada para iniciar el protector de pantalla en su equipo cliente. Puede crear un archivo ubicado en `/etc/vmware/view-keycombos-config` y especificar las combinaciones de teclas y las teclas individuales.

Coloque cada tecla o combinación de teclas en una línea nueva con el formato siguiente:

```
<modName> scanCodescanCode
```

El primer ejemplo es de una combinación de teclas. El segundo es un ejemplo de una tecla individual. El valor `scanCode` es el código de tecla del teclado, expresado en hexadecimal.

En este ejemplo, *modName* es una de las cuatro teclas modificadoras: `ctrl`, `alt`, `mayús` y `super`. La tecla `Super` es específica de cada teclado. Por ejemplo, la tecla `Super` suele ser la tecla `Windows` en un teclado `Microsoft Windows`. Sin embargo, corresponde a la tecla `Comando` en un teclado `Mac OS X`. También puede usar `<any>` como comodín de *modName*. Por ejemplo, `<any>0x153` especifica todas las combinaciones de la tecla `Suprimir`, incluida esta tecla individual en el teclado de los Estados Unidos. El valor que use para *modName* no distingue entre mayúsculas y minúsculas.

Especificar el código de tecla

El valor *scanCode* debe estar en formato hexadecimal. Para determinar el código que se debe utilizar, abra el archivo del idioma y del teclado apropiados en el directorio `lib/vmware/xkeymap` del sistema cliente. Además de los códigos que aparecen en este archivo, también puede usar los siguientes códigos:

Tabla 3-6. Teclas multimedia

Nombre de la tecla	Código de tecla
PISTA_ANTERIOR	0x110
PISTA_SIGUIENTE	0x119
SILENCIAR	0x120
CALCULADORA	0x121
REPRODUCIR_PAUSA	0x122
DETENER	0x124
BAJAR_VOLUMEN	0x12e
SUBIR_VOLUMEN	0x130
INICIO_EN_EXPLORADOR	0x132
BUSCAR_EN_EXPLORADOR	0x165
FAVORITOS_EN_EXPLORADOR	0x166
ACTUALIZAR_EN_EXPLORADOR	0x167
DETENER_EN_EXPLORADOR	0x168
ADELANTE_EN_EXPLORADOR	0x169
ATRÁS_EN_EXPLORADOR	0x16A
EQUIPO	0x16B
CORREO	0x16C
SELECCIÓN_DE_MEDIOS	0x16D

Tabla 3-7. Teclas Hangul y Hanja

Nombre de la tecla	Código de tecla
HANGUL_ES	0x72
HANJA_ES	0x71

Tabla 3-7. Teclas Hangul y Hanja (continuación)

Nombre de la tecla	Código de tecla
HANGUL_KO	0x172
HANJA_KO	0x171
HANGUL	0xF2
HANJA	0xF1

Tabla 3-8. Teclas de alimentación, de reanudación y de suspensión

Nombre de la tecla	Código de tecla
SUSPENDER_SISTEMA	0x15F
REANUDAR_SISTEMA	0x163
ALIMENTACIÓN_SISTEMA	0x15e

La siguiente lista muestra los contenidos de ejemplo en un archivo `/etc/vmware/view-keycombos-config`. El carácter `#` precede a los comentarios de códigos.

```
<ctrl>0x152      #block ctrl-insert
<alt>15          #block alt-tab
<Ctrl><Alt>0x153 #block ctrl-alt-del
<any>0x137       #block any combinations of the Print key
0x010            #block the individual Q key in a US English keyboard
                  #or block the individual A key in a French keyboard
0x03b            #block the individual F1 key
0x04f            #block the individual 1 key in a numeric keypad
```

Utilizar FreeRDP para las conexiones RDP

Si tiene previsto utilizar RDP en lugar de VMware Blast o PCoIP para las conexiones a escritorios de View, puede utilizar un cliente `rdesktop` o `xfreerdp`, la implementación de software libre del protocolo de escritorio remoto (RDP), lanzada bajo la licencia de Apache.

Dado que el programa `rdesktop` ya no se desarrolla de forma activa, Horizon Client también puede ejecutar el archivo `xfreerdp` si su equipo Linux tiene la versión y las revisiones necesarias de FreeRDP.

Importante Si tiene previsto conectarse a aplicaciones o escritorios remotos en un host de Microsoft RDS y dicho host está configurado con el modo de licencia por dispositivo, deberá utilizar `xfreerdp` o bien cambiar el modo de licencia al modo de licencia por usuario. La razón es que el modo de licencia por dispositivo necesita que el cliente RDP proporcione un ID de cliente y `rdesktop` no proporciona dicho ID, mientras que `xfreerdp` sí.

Debe tener instalada la versión adecuada de FreeRDP, junto con las revisiones correspondientes. Si desea obtener más información, consulte [Instalar y configurar FreeRDP](#).

Sintaxis general

Puede utilizar la interfaz de línea de comandos de `vmware-view` o algunas propiedades de archivos de configuración para especificar opciones para `xfreerdp`, del mismo modo que para `rdesktop`.

- Para especificar que Horizon Client debe ejecutar `xfreerdp` en lugar de `rdesktop`, utilice la opción de línea de comandos o la clave de configuración adecuadas.

Opción de línea de comandos: `--rdpclient="xfreerdp"`

Clave de configuración: `view.rdpClient="xfreerdp"`

- Para especificar opciones y enviarlas al programa `xfreerdp`, utilice la opción de línea de comandos o la clave de configuración adecuadas e indique las opciones de FreeRDP.

Opción de línea de comandos: `--xfreerdpOptions`

Clave de configuración: `view.xfreerdpOptions`

Para obtener más información sobre cómo utilizar los archivos de configuración y la interfaz de línea de comandos de `vmware-view`, consulte [Utilizar los archivos de configuración y la interfaz de línea de comandos de vmware-view](#).

Sintaxis de la autenticación a nivel de red

Muchas opciones de configuración del programa `rdesktop` son las mismas que las del programa `xfreerdp`. Una diferencia importante es que `xfreerdp` es compatible con la autenticación a nivel de red (NLA). Esta autenticación está desactivada de forma predeterminada. Debe utilizar la siguiente opción de línea de comandos para activar la autenticación a nivel de red:

```
--enableNla
```

Asimismo, debe agregar la opción `/cert-ignore` para que el proceso de verificación de certificados se realice correctamente. A continuación, se indica un ejemplo de la sintaxis correcta:

```
vmware-view --enableNla --rdpclient=xfreerdp --xfreerdpOptions="/p:password /cert-ignore /u:user-name /d:domain-name /v:server"
```

Si la contraseña contiene caracteres especiales, codifíquelos (por ejemplo: `\$`).

Sintaxis específica para utilizar FreeRDP con Horizon Client

Tenga en cuenta las siguientes directrices:

- Debe codificar los caracteres especiales que suele colocar entre comillas. Por ejemplo, el siguiente comando no funciona porque el carácter especial `$` de `pa$$word` no se codificó:

```
(incorrecto) vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa$$word' /u:'crt\nadministrator'"
```

En su lugar, deberá utilizar:

```
(correcto) vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa\$\$word' /u:'crt
\administrator'"
```

- Si los usuarios finales utilizan una implementación del tipo sesión en sesión de Horizon Client, deberá utilizar la opción `/rfx`. Un ejemplo de implementación de tipo sesión en sesión es aquella en la que un usuario final se conecta a Horizon Client en un cliente ligero, de modo que la interfaz de Horizon Client es la única que el usuario final ve. A continuación, este inicia una versión anidada de Horizon Client para usar una aplicación remota proporcionada por un host RDS. En casos como este, si no utiliza la opción `/rfx`, el usuario final no podrá ver los iconos de aplicaciones y escritorios remotos en la ventana de selección de aplicaciones y escritorios del cliente anidado.

Instalar y configurar FreeRDP

Para usar un cliente FreeRDP para las conexiones RDP con escritorios View, el equipo Linux debe incluir la versión necesaria de FreeRDP.

Para obtener una lista de paquetes de los que depende `xfreerdp` en Ubuntu, vaya a <https://github.com/FreeRDP/FreeRDP/wiki/Compilation>.

Requisitos previos

En el equipo cliente Linux, descargue FreeRDP 1.1 desde GitHub, en <https://github.com/FreeRDP/FreeRDP>.

Procedimiento

- 1 Conéctelo con el archivo denominado `freerdp-1.1.0.patch`, usando los siguientes comandos:

```
cd /client-installation-directory/patches/FreeRDP-stable-1.1
patch -p1 < freerdp-1.1.0.patch
patch -p1 < freerdp-1.1.0-tls.patch
```

En este caso, *client-installation-directory* es la ruta de `VMware-Horizon-View-Client-x.x.x-yyyyyy.i386`, donde *x.x.x* es el número de versión y *yyyyyy* es el número de compilación. El archivo `freerdp-1.1.0-tls.patch` habilita la conexión TLSv1.2 en `xfreerdp`. Si instaló VMware Horizon Client para Linux, los archivos `freerdp-1.1.0.patch` y `freerdp-1.1.0-tls.patch` se encuentran en el directorio `/usr/share/doc/vmware-horizon-client/patches`. Para obtener más información sobre el archivo `freerdp-1.1.0.patch`, consulte el archivo `README.patches` en el mismo directorio *client-installation-directory/patches*.

- 2 Ejecute el siguiente comando:

```
cmake -DWITH_SSE2=ON -DWITH_PULSEAUDIO=ON -DWITH_PCSC=ON -DWITH_CUPS=ON .
```

- 3 Ejecute el siguiente comando:

```
make
```

- 4 Ejecute el siguiente comando, que instalará el archivo binario xfreerdp compilado en un directorio de ejecución de PATH para que Horizon Client pueda iniciar el programa al ejecutar xfreerdp:

```
sudo make install
```

- 5 (opcional) Compruebe que el módulo de impresión virtual se pueda cargar correctamente.
 - a Para comprobar que FreeRDP 1.1 pueda cargar tprdp.so, ejecute el siguiente comando:

```
sudo ln -s /usr/lib/vmware/rdpvcbridge/tprdp.so /usr/local/lib/i386-linux-gnu/freerdp/tprdp-client.so
```

- b Para iniciar Horizon Client con la función de impresión virtual habilitada, ejecute el siguiente comando:

```
vmware-view --rdpclient=xfreerdp --xfreerdpOptions='/cert-ignore /vc:tprdp'
```

Nota La función de impresión virtual está disponible si usa VMware Blast o PCoIP.

Habilitar el modo compatible con FIPS

Puede habilitar el modo compatible con FIPS (Estándar federal de procesamiento de información) para que el cliente use algoritmos criptográficos conformes a FIPS cuando se comunique con escritorios remotos.

Nota En el modo compatible con FIPS, Horizon Client para Linux implementa un módulo cifrado que está diseñado conforme a los requisitos del estándar FIPS 140-2. Este módulo se validó en los entornos operativos que aparecen en el certificado CMVP #2839 y se trasladó a esta plataforma. Sin embargo, todavía no se completaron en el plan del producto los requisitos de pruebas de CMVP y de CAVP diseñados para incluir nuevos entornos operativos en los certificados CMVP y CAVP NIST de VMware.

Importante Si habilita el modo compatible con FIPS en el cliente, el escritorio remoto también debe tener el modo FIPS habilitado. No se admite el modo mixto, en el que solo el cliente o solo el escritorio tienen el modo compatible con FIPS habilitado.

Para habilitar el modo compatible con FIPS, realice los siguientes cambios en la configuración:

- 1 Edite /etc/vmware/config y agregue las siguientes líneas:

```
usb.enableFIPSMODE = "TRUE"
mks.enableFIPSMODE = "TRUE"
```

- 2 Edite /etc/vmware/view-mandatory-config y agregue la siguiente línea:

```
View.fipsMode = "TRUE"
```

3 Edite `/etc/teradici/pcoip_admin.conf` y agregue la siguiente línea:

```
pcoip.enable_fips_mode = 1
```

Configurar la caché de imágenes del lado del cliente PCoIP

La caché de imágenes del lado del cliente PCoIP almacena contenidos de imagen en el cliente para evitar una retransmisión. Esta función está habilitada de forma predeterminada para reducir el uso del ancho de banda.

La caché de imagen PCoIP captura la redundancia espacial así como la temporal. Por ejemplo, cuando se desplaza hacia abajo en un documento PDF, el contenido nuevo aparece desde la parte inferior de la ventana y el contenido antiguo desaparece desde la parte superior de la ventana. Todo el contenido restante se mantiene constante y se mueve hacia arriba. La caché de imágenes PCoIP es capaz de detectar esta redundancia espacial y temporal.

Debido a que durante el desplazamiento, la información mostrada que se envía al dispositivo cliente es una secuencia de índices de caché, utilizando la caché de imágenes se ahorra una cantidad significativa de ancho de banda. Este desplazamiento eficiente tiene beneficios en LAN y a través de WAN.

- En LAN, donde el ancho de banda está relativamente sin restringir, con el almacenamiento caché de imágenes del lado del cliente se proporciona un ahorro significativo de ancho de banda.
- A través de WAN, para mantenerse dentro del ancho de banda restringido disponible, la acción de desplazarse suele degradarse a menos que se use la caché del lado del cliente. En esta situación, el almacenamiento caché del lado del cliente permite ahorrar ancho de banda y garantiza una experiencia de desplazamiento suave y con una buena respuesta.

De forma predeterminada, esta función está habilitada, por lo que el cliente almacena partes de la pantalla que se transmitió previamente. El tamaño predeterminado de la caché es 250 MB. Un tamaño mayor de caché reduce el uso del ancho de banda, pero requiere más memoria en el cliente. Un tamaño menor de caché consume más ancho de banda. Por ejemplo, un cliente ligero con poca memoria necesita un tamaño menor de caché.

Establecer la propiedad de configuración

Para configurar el tamaño de caché, puede establecer la propiedad `pcoip.image_cache_size_mb`. Por ejemplo, la siguiente configuración establece el tamaño de caché en 50 MB:

```
pcoip.image_cache_size_mb = 50
```

Use un espacio antes y después del signo igual (=).

Si especifica un valor menor a la cantidad de la memoria disponible dividida entre 2, el valor se redondea al múltiplo de 10 más próximo. El valor mínimo es 50. Se ignorará cualquier valor que sea menor de 50.

Si especifica un valor superior a la cantidad de memoria disponible dividida entre 2, el valor se establece en la cantidad de memoria disponible dividida entre 2 y se redondea al múltiplo de 10 más próximo.

Puede establecer esta propiedad en todos los archivos. Cuando se inicia Horizon Client, la configuración se procesa desde varias ubicaciones en el siguiente orden:

- 1 /etc/teradici/pcoip_admin_defaults.conf
- 2 ~/.pcoip.rc
- 3 /etc/teradici/pcoip_admin.conf

Si una configuración se define en varias ubicaciones, el valor que se usa es el que se obtiene de la última lectura de archivo.

Nota Puede configurar la siguiente propiedad para que muestre una indicación visual que notifique que la caché de imágenes está funcionando:

```
pcoip.show_image_cache_hits = 1
```

Con esta configuración, verá un rectángulo alrededor de cada mosaico (32 x 32 píxeles) de una imagen que provenga de la caché de imágenes.

Administrar las conexiones de las aplicaciones publicadas y los escritorios remotos

4

Los usuarios finales pueden utilizar Horizon Client para conectarse a un servidor, iniciar o cerrar sesión en escritorios remotos y utilizar aplicaciones publicadas. Para solucionar problemas, los usuarios finales también pueden reiniciar y restablecer los escritorios remotos y restablecer las aplicaciones publicadas.

Según el modo en que configure las directivas, los usuarios finales podrán realizar varias operaciones en los escritorios remotos y las aplicaciones publicadas.

Este capítulo incluye los siguientes temas:

- [Conectarse a una aplicación publicada o a un escritorio remoto](#)
- [Conectarse a aplicaciones públicas mediante acceso sin autenticar](#)
- [Compartir el acceso a unidades y carpetas locales con el Redireccionamiento de unidades cliente](#)
- [Configurar el modo de comprobación del certificado en Horizon Client](#)
- [Cambiar los escritorios remotos o las aplicaciones publicadas](#)
- [Cerrar sesión o desconectarse](#)

Conectarse a una aplicación publicada o a un escritorio remoto

Después de iniciar sesión en un servidor, puede conectarse a las aplicaciones publicadas y a los escritorios remotos que esté autorizado a utilizar.

Antes de que los usuarios finales obtengan acceso a las aplicaciones y los escritorios remotos, pruebe que puede conectarse a una aplicación o a un escritorio remotos desde un dispositivo cliente. Debe especificar un servidor y proporcionar las credenciales de su cuenta de usuario.

Para usar aplicaciones remotas, debe conectarse a la versión 6.0 o posterior del servidor de conexión.

Requisitos previos

- Obtenga las credenciales de inicio de sesión, como un nombre de usuario y contraseña, el nombre de usuario y el código de acceso de RSA SecurID, las credenciales de autenticación de RADIUS o el número de identificación personal de la tarjeta inteligente (PIN).
- Obtenga el nombre de dominio NETBIOS para iniciar sesión. Por ejemplo, puede usar `mycompany` en lugar de `mycompany.com`.
- Realice las tareas administrativas descritas en [Preparar el servidor de conexión para Horizon Client](#).
- Si se encuentra fuera de la red corporativa y necesita una conexión VPN para acceder a aplicaciones publicadas y escritorios remotos, verifique que el dispositivo cliente esté configurado para utilizar una conexión VPN y establezca esa conexión.
- Compruebe que tiene un nombre de dominio completo (FQDN) del servidor que proporciona acceso a la aplicación publicada o al escritorio remoto. Los nombres de los servidores no admiten guiones bajos (_). Si el puerto no es 443, también necesita el número de puerto.
- Si tiene pensado usar el protocolo de visualización RDP para conectarse a un escritorio remoto, compruebe que el ajuste de la directiva de grupo agente AllowDirectRDP está habilitado. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Procedimiento

- 1 Abra una ventana de terminal e introduzca **vmware-view**, o bien busque las aplicaciones de **VMware Horizon Client** y haga doble clic en el icono.
- 2 Si se le solicitan las credenciales de RSA SecurID o las credenciales de autenticación de RADIUS, introdúzcalas y haga clic en **Iniciar sesión**.
- 3 Si se le solicita un nombre de usuario y una contraseña, introduzca las credenciales de Active Directory.
 - a Escriba el nombre y la contraseña de un usuario que tenga autorización para utilizar al menos un grupo de escritorios o de aplicaciones.

Si el menú desplegable **Dominio** está deshabilitado, deberá introducir el nombre de usuario con el formato **dominio\nombredeusuario** o **nombredeusuario@dominio.com**.
 - b (Opcional) Seleccione un valor de dominio en el menú desplegable **Dominio**.
 - c Haga clic en **Inicio de sesión**.

- 4 (opcional) Si desea configurar las opciones de visualización para un escritorio remoto, haga clic con el botón secundario en el icono de escritorio remoto y seleccione **Configuración**.

Opción	Acción
Seleccionar un protocolo de visualización	Si un administrador de Horizon lo permitió, use el menú desplegable Conectar a través de para seleccionar el protocolo de visualización. Para usar VMware Blast, debe estar instalada la versión 7.0 o posterior de Horizon Agent.
Seleccionar un diseño de visualización	Use el menú desplegable Pantalla para seleccionar un tamaño de ventana o para usar varios monitores.

- 5 (opcional) Para marcar una aplicación publicada o un escritorio remoto como favorito, haga clic con el botón secundario en el icono de la aplicación publicada o el escritorio remoto y seleccione **Marcar como favorito** en el menú contextual que aparece.

Aparece un icono de estrella en la esquina superior derecha del nombre de la aplicación publicada o del escritorio remoto. La próxima vez que inicie sesión, puede hacer clic en el botón **Mostrar favoritos** para encontrar rápidamente esta aplicación o este escritorio.

- 6 Haga doble clic en una aplicación o un escritorio remoto a los que desee conectarse.

Si va a conectarse a un escritorio remoto basado en una sesión, alojada en un host de Microsoft RDS y si el escritorio ya está configurado para usar un protocolo de visualización diferente, no podrá conectarse inmediatamente. Para poder establecer una conexión con el protocolo que seleccionó, se le pedirá que utilice el protocolo que está establecido o bien que cierre la sesión en el sistema operativo remoto.

Resultados

La ventana del cliente se mostrará cuando se haya conectado.

Si se produce un error en el proceso de autenticación del servidor de conexión o el cliente no puede conectarse a la aplicación o el escritorio remoto, realice las siguientes tareas:

- Verifique que el certificado de seguridad del servidor de conexión funcione correctamente. Si no es así, en Horizon Console, podría ver también que no es posible obtener acceso a View Agent o Horizon Agent en los escritorios. Estos síntomas indican problemas de conexión adicionales provocados por problemas con el certificado.
- Verifique que las etiquetas definidas en la instancia del servidor de conexión permiten el establecimiento de conexiones desde este usuario. Consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Verifique que el usuario esté autorizado a obtener acceso a esta aplicación o a este escritorio. Consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7* o *Configurar escritorios virtuales en Horizon 7*.
- Si usa el protocolo de visualización RDP para conectarse a un escritorio remoto, verifique que el sistema operativo remoto permita las conexiones de escritorio remoto.

Conectarse a aplicaciones públicas mediante acceso sin autenticar

Puede conectarse a aplicaciones públicas mediante una cuenta de acceso sin autenticar con Horizon Client.

Antes de que el usuario final acceda a sus aplicaciones publicadas con acceso sin autenticar, compruebe que puede conectarse a las aplicaciones publicadas desde un dispositivo cliente mediante una cuenta de usuario de acceso sin autenticar.

Requisitos previos

- Compruebe que el servidor de conexión de Horizon 7 7.1 o versiones posteriores está configurado para acceso sin autenticar.
- Compruebe que se crearon sus usuarios de acceso sin autenticar en Horizon Console. Si el usuario sin autenticar predeterminado es el único usuario de acceso sin autenticar, Horizon Client se conecta al servidor de conexión con el usuario predeterminado.

Procedimiento

- 1 Abra una ventana de terminal e introduzca **vmware-view**, o bien busque las aplicaciones de **VMware Horizon Client** y haga doble clic en el icono.
- 2 En la pantalla de inicio de Horizon Client, seleccione **Archivo > Iniciar sesión de forma anónima con Acceso sin autenticar** en la barra de menús si dicha opción no estuviera seleccionada.
- 3 Conéctese al servidor de conexión que está configurado para acceso sin autenticar.
 - Si aún no se agregó el servidor que necesita, haga doble clic en el botón **+ Agregar servidor** o haga clic en el botón **Servidor nuevo** de la barra de menús. A continuación, introduzca el nombre del servidor de conexión o un servidor de seguridad y haga clic en **Conectar**.
 - Si el servidor que necesita aparece en la pantalla de inicio de Horizon Client, haga clic con el botón secundario en el icono del servidor y seleccione **Conectar** en el menú contextual.

Es posible que se muestre un mensaje que debe confirmar antes de que aparezca el cuadro de diálogo de inicio de sesión.

- 4 En el cuadro de diálogo Acceso al servidor, especifique la cuenta de acceso sin autenticar que desea utilizar.
 - a Seleccione una cuenta de usuario de las que aparecen en el menú desplegable de cuentas de acceso sin autenticar.

Junto a la cuenta de usuario predeterminada se muestra **(predeterminada)**.
 - b (Opcional) Haga clic en **Usar siempre esta cuenta** si desea omitir el cuadro de diálogo Acceso al servidor la próxima vez que se conecte al servidor.
 - c Haga clic en **Aceptar**.

Se mostrará la ventana para seleccionar una aplicación, en la que se mostrarán las aplicaciones publicadas que la cuenta de acceso sin autenticar está autorizada a utilizar.

Nota Si seleccionó la opción **Usar siempre esta cuenta** durante un inicio de sesión anterior de acceso sin autenticar, no se le solicitará que la cuenta se utilice para la sesión de acceso sin autenticar. Para desmarcar esta opción, haga clic con el botón secundario en el icono del servidor en la pantalla de inicio de Horizon Client y seleccione **Olvidar la cuenta de Acceso sin autenticar guardada** en el menú contextual.

- 5 Para iniciar una aplicación, haga doble clic en su icono.

Se mostrará la ventana de la aplicación.

- 6 Salga de la aplicación cuando termine de utilizarla.

Se mostrará el cuadro de diálogo Desconectarse de la sesión, en el que se le preguntará si desea desconectarse del servidor.

Resultados

Si se agota el tiempo de espera de la sesión especificado por su administrador de Horizon, la sesión se desconecta automáticamente del servidor.

Compartir el acceso a unidades y carpetas locales con el Redireccionamiento de unidades cliente

Con la función Redireccionamiento de unidades cliente, puede compartir carpetas y unidades del sistema cliente local con escritorios remotos y aplicaciones publicadas.

Las unidades compartidas pueden incluir unidades asignadas y dispositivos de almacenamiento USB.

La función de redireccionamiento de unidades cliente no admite el uso compartido de Microsoft OneDrive, Google Drive ni el almacenamiento de archivos empresariales.

En un escritorio remoto Windows, las unidades y las carpetas compartidas aparecen en la carpeta **Este equipo** o en **Equipo**, según la versión del sistema operativo Windows. En una aplicación publicada, como el Bloc de notas, puede explorar y abrir un archivo que se encuentre en una unidad o carpeta compartida.

La función de redireccionamiento de unidades cliente requiere que se encuentren instalados los archivos de biblioteca siguientes. Es posible que estos archivos de biblioteca no se encuentren instalados de forma predeterminada en algunos equipos cliente ligeros.

- libsigc-2.0.so.0
- libglibmm-2.4.so.1

La configuración del redireccionamiento de unidades cliente se aplica a todos los escritorios remotos y las aplicaciones publicadas.

Requisitos previos

Para compartir carpetas y unidades con una aplicación publicada o un escritorio remoto, es necesario que un administrador de Horizon habilite la función Redireccionamiento de unidades cliente. Esta tarea implica habilitar la opción **Redireccionamiento de unidades cliente** del agente. También puede incluir directivas de configuración o ajustes de registro para controlar el comportamiento del redireccionamiento de unidades cliente. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Con Horizon Agent 7.9 y versiones posteriores, puede incluir o excluir carpetas en dispositivos que tengan ID de proveedor y de producto especificados para que no sean redirigidas mediante la configuración de la directiva de grupo **Incluir un dispositivo Vid/Pid** y **Excluir un dispositivo Vid/Pid**. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Procedimiento

- 1 Abra el cuadro de diálogo Configuración con el panel Compartir abierto.

Opción	Descripción
En la ventana para seleccionar la aplicación y el escritorio	Haga clic con el botón secundario en el icono de una aplicación publicada o un escritorio remoto, seleccione Configuración y haga clic en Compartir . Otro método consiste en seleccionar Conexión > Configuración en la barra de menús y hacer clic en Compartir .
En el cuadro de diálogo Compartir cuando se conecta a un escritorio remoto o una aplicación publicada	Haga clic en Permitir para compartir su directorio de inicio, o en Denegar para no hacerlo.
En un escritorio remoto	Seleccione Conexión > Configuración en la barra de menús y haga clic en Compartir .

- 2 Configure el redireccionamiento de unidades cliente.

Opción	Acción
Compartir una unidad o carpeta específica con aplicaciones publicadas o escritorios remotos	Haga clic en el botón Agregar , desplácese hasta la carpeta o unidad que desee compartir, selecciónela, y haga clic en Aceptar . Nota Si un dispositivo USB ya está conectado a un escritorio remoto o a una aplicación publicada con la función de redireccionamiento USB, no puede compartir ninguna carpeta del dispositivo USB.
Dejar de compartir una carpeta o unidad específica	En la lista Carpeta, seleccione la carpeta o unidad y haga clic en el botón Eliminar .
Permitir que las aplicaciones publicadas y los escritorios remotos obtengan acceso a los archivos de su directorio de inicio	Seleccione la casilla de verificación Compartir su carpeta de inicio: directorio de inicio .

Opción	Acción
Compartir dispositivos de almacenamiento USB con aplicaciones publicadas y escritorios remotos	<p>Seleccione la casilla de verificación Permitir acceso a almacenamiento extraíble. La función de redireccionamiento de unidades cliente comparte todos los dispositivos de almacenamiento USB insertados en el sistema cliente y todas las unidades externas FireWire y Thunderbolt conectadas automáticamente. No es necesario seleccionar un dispositivo específico para que se comparta.</p> <hr/> <p>Nota No se compartirán los dispositivos de almacenamiento que ya se encuentren conectados a una aplicación publicada o a un escritorio remoto con la función de redireccionamiento USB.</p> <hr/> <p>Si esta casilla de verificación no está seleccionada, puede usar la función de redireccionamiento USB para conectar dispositivos de almacenamiento USB a aplicaciones publicadas y escritorios remotos.</p>
No mostrar el cuadro de diálogo Compartir al conectarse a una aplicación publicada o a un escritorio remoto	<p>Seleccione la casilla de verificación No mostrar el cuadro de diálogo al conectarse a un escritorio o una aplicación.</p> <p>Si esta casilla no está marcada, el cuadro de diálogo Compartir aparece la primera vez que se conecta a un escritorio remoto o una aplicación publicada. Por ejemplo, si inicia sesión en un servidor y se conecta a un escritorio remoto, se mostrará el cuadro de diálogo Compartir. Si a continuación se conecta a otro escritorio remoto o aplicación publicada, no se muestra el cuadro de diálogo. Para que se muestre el cuadro de diálogo de nuevo, deberá desconectarse del servidor e iniciar sesión otra vez.</p>

Pasos siguientes

Compruebe que puede ver las carpetas compartidas desde la aplicación publicada o el escritorio remoto.

- En un escritorio remoto Windows, abra Explorador de archivos y consulte la carpeta **Este equipo** o abra Explorador de archivos y consulte la carpeta **Equipo**, según la versión del sistema operativo Windows.
- En una aplicación publicada, seleccione **Archivo > Abrir** o **Archivo > Guardar como** y desplácese a la carpeta o la unidad.

Las carpetas y las unidades que seleccionó para el uso compartido pueden usar una o varias de las siguientes convenciones de nomenclatura.

Convención de nomenclatura	Ejemplo
<i>nombre_de_carpeta</i> en <i>nombre_de_escritorio</i>	jsmith en JSMITH W03
<i>nombre_de_carpeta</i> (<i>número_de_unidad</i> :)	jsmith (Z:)
<i>nombre_de_carpeta</i> en el <i>nombre_de_escritorio</i> (<i>número_de_unidad</i> :)	jsmith en JSMITH W03 (Z:).

En algunas versiones de Horizon Agent, una carpeta redireccionada puede tener dos entradas, tal como aparece en **Dispositivos y unidades y Ubicaciones de red** en Windows 10, y pueden aparecer ambas entradas al mismo tiempo. Si ya se están utilizando todas las etiquetas de volumen (desde A: hasta Z:), las carpetas redirigidas solo tienen una entrada.

Compartir carpetas editando un archivo de configuración

Además de compartir carpetas a través del cuadro de diálogo Configuración, también puede compartirlas editando un archivo de configuración.

Procedimiento

- 1 Cree un archivo de configuración denominado `config` si no existe en ninguna de las siguientes ubicaciones:

- `$HOME/.vmware/`
- `/usr/lib/vmware/`
- `/etc/vmware/`

- 2 Agregue la siguiente línea en cada carpeta que desea compartir:

```
tsdr.share=Ruta de carpeta
```

Por ejemplo, para compartir las carpetas `/` y `/home/user1`, cree el archivo `/etc/vmware/config` y agregue las siguientes líneas:

```
tsdr.share=/
tsdr.share=/home/user1
```

Resultados

Las carpetas que se comparten en un archivo de configuración no aparecen en el panel Compartir del cuadro de diálogo Configuración. Puede editar el archivo de configuración para dejar de compartir carpetas o para compartir carpetas adicionales.

Configurar el modo de comprobación del certificado en Horizon Client

La comprobación del certificado del servidor se aplica a conexiones entre Horizon Client y un servidor. Un certificado es una manera de identificación digital, similar al pasaporte o al permiso de conducir.

La comprobación de certificados del servidor incluye las siguientes comprobaciones:

- ¿El certificado persigue otro objetivo que no sea verificar la identidad del remitente y el cifrado de las comunicaciones del servidor? Es decir, ¿es el tipo de certificado correcto?
- ¿Expiró el certificado o solo será válido en el futuro? Es decir, ¿el certificado es válido según el reloj del equipo?

- ¿El nombre común del certificado coincide con el nombre de host del servidor que lo envía? Se produce un error de coincidencia cuando un equilibrador de carga redirecciona Horizon Client a un servidor que tiene un certificado que no coincide con el nombre de host introducido en Horizon Client. También puede producirse un error de coincidencia si introduce una dirección IP distinta al nombre de host en el cliente.
- ¿El certificado está firmado por una entidad de certificación desconocida o que no es de confianza? Los certificados autofirmados no son certificados de confianza. Para superar esta comprobación, la cadena de confianza del certificado debe especificar la raíz en el almacén de certificados local del dispositivo.

Para obtener información sobre cómo distribuir un certificado raíz autofirmado que los usuarios puedan instalar en sus sistemas cliente de Linux, consulte la documentación de Ubuntu.

Horizon Client utiliza los certificados con formato PEM almacenados en el directorio `/etc/ssl/certs` del sistema cliente. Para obtener información sobre cómo importar un certificado raíz almacenado en esta ubicación, consulte "Importar un certificado en la base de datos de entidades de certificación de todo el sistema" en el documento incluido en la página <https://help.ubuntu.com/community/OpenSSL>.

Puede establecer el modo de comprobación del certificado si un administrador de Horizon lo permitió. Para establecer el modo de comprobación del certificado, inicie Horizon Client y seleccione **Archivo > Preferencias** en la barra de menú. Puede seleccionar una de las siguientes opciones.

- **No conectarse nunca a servidores que no sean de confianza.** Con esta opción, no puede conectarse al servidor si alguna comprobación del certificado falla. Aparece un mensaje de error con las comprobaciones que han fallado.
- **Advertirme antes de conectarme a servidores que no sean de confianza.** Con esta opción, puede hacer clic en **Continuar** para ignorar la advertencia si falla alguna comprobación de certificado porque el servidor usa un certificado autofirmado. En lo que respecta a los certificados autofirmados, el nombre del certificado no tiene que coincidir con el nombre del servidor que introdujo en Horizon Client. También puede recibir una advertencia si el certificado expiró.
- **No comprobar los certificados de identidad de los servidores.** Esta opción significa que no se ha llevado a cabo ninguna comprobación del certificado.

En Horizon Client, puede configurar el modo predeterminado de comprobación de certificados e impedir que los usuarios finales lo cambien. Si desea obtener más información, consulte [Configurar el modo de comprobación de certificados para usuarios finales](#).

Usar un servidor proxy SSL

Si utiliza un servidor proxy SSL para inspeccionar el tráfico enviado desde el entorno de cliente a Internet, habilite el ajuste **Permitir conexión a través de un proxy SSL**. Esta opción permite la comprobación del certificado en conexiones secundarias a través de un servidor proxy SSL y se aplica tanto a la puerta de enlace segura Blast como a las conexiones de túnel seguro. Si utiliza

un servidor proxy SSL y habilita la comprobación del certificado, pero no habilita el ajuste **Permitir conexión a través de un proxy SSL**, se producirá un error en las conexiones debido a que las huellas digitales no coinciden. El ajuste **Permitir conexión a través de un proxy SSL** no estará disponible si se habilita la opción **No comprobar los certificados de identidad de los servidores**. Si la opción **No comprobar los certificados de identidad de los servidores** está habilitada, Horizon Client no verificará el certificado ni la huella digital, y siempre se permitirá el proxy SSL.

Para permitir las conexiones de VMware Blast a través de un servidor proxy, consulte [Configurar las opciones de VMware Blast](#).

Cambiar los escritorios remotos o las aplicaciones publicadas

Si está conectado a un escritorio remoto, puede cambiar a otro. También puede conectarse a una aplicación publicada mientras está conectado a un escritorio remoto.

Procedimiento

- ◆ Seleccione una aplicación o un escritorio remotos desde el mismo servidor o desde uno diferente.

Opción	Acción
Elegir un escritorio o una aplicación diferentes en el mismo servidor	<p>Realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> ■ Si inició sesión en un escritorio remoto y desea cambiar a otra aplicación o escritorio remotos que estén en ejecución en su cliente, seleccione el escritorio o la aplicación en el menú de View. ■ Si inició sesión en una aplicación o escritorio remotos y desea cambia a otro que no esté en ejecución, seleccione Archivo > Volver a la lista de aplicaciones y de escritorios en la barra de menú e inicie la aplicación o el escritorio desde la ventana de selección. ■ En la ventana para seleccionar una aplicación o un escritorio, haga doble clic en el icono del otro escritorio o aplicación. Este escritorio o esta aplicación se abre en una ventana nueva, de forma que aparecerán varias ventanas abiertas y podrá cambiar de una a otra.
Elegir otro escritorio u otra aplicación en un servidor diferente	<p>Realice cada una de las siguientes acciones:</p> <ul style="list-style-type: none"> ■ Si quiere mantener la aplicación o el escritorio abiertos y conectarse también a una aplicación o a un escritorio remotos en otro servidor, inicie una nueva instancia de Horizon Client y conéctela al otro escritorio o aplicación. ■ Si quiere cerrar el escritorio actual y conectarse a un escritorio en otro servidor, diríjase a la ventana para seleccionar un escritorio, haga clic en el icono Desconectar situado en la esquina superior izquierda de la ventana y confirme que desea cerrar sesión en el servidor. Se desconectará del servidor actual y de todas las sesiones del escritorio o de las aplicaciones abiertas. Entonces podrá conectarse a un servidor diferente.

Cerrar sesión o desconectarse

Si se desconecta de un escritorio remoto sin cerrar sesión, las aplicaciones de dicho escritorio pueden permanecer abiertas. También puede desconectarse de un servidor y dejar las aplicaciones publicadas ejecutándose.

Puede cerrar sesión en un escritorio remoto, aunque no tenga ningún escritorio abierto. Esta función tiene el mismo resultado que si envía la secuencia Ctrl+Alt+Supr al escritorio remoto y luego hace clic en **Cerrar sesión**.

Procedimiento

- ◆ Desconectarse sin cerrar sesión.

Opción	Acción
Salir también de Horizon Client	Haga clic en el botón Cerrar situado en la esquina de la ventana o seleccione Archivo > Salir en la barra de menú.
Seleccionar un escritorio remoto diferente del mismo servidor	Seleccione Escritorio > Desconectar en la barra de menú.
Seleccionar un escritorio remoto diferente en un servidor diferente	Seleccione Archivo > Desconectarse del servidor en la barra de menú.

Nota Un administrador de Horizon puede establecer que los escritorios cierren sesión de forma automática cuando se desconecten. En ese caso, se detendrán todas las aplicaciones abiertas en el escritorio remoto.

- ◆ Cerrar sesión y desconectarse desde un escritorio remoto.

Opción	Acción
Desde el escritorio remoto	Utilice el menú Inicio de Windows para cerrar sesión.
En la barra de menú	<p>Seleccione Escritorio > Desconectar y cerrar sesión.</p> <p>Si utiliza este procedimiento, los archivos que estén abiertos en el escritorio remoto se cierran sin guardar.</p>

- ◆ Cerrar sesión cuando no tenga ningún escritorio remoto abierto.
 - Desde la pantalla de inicio con combinaciones de teclas de los escritorios, seleccione el escritorio y, a continuación, **Escritorio > Cerrar sesión** en la barra de menú.
 - Introduzca las credenciales para acceder al escritorio remoto si se le solicitan.

Si utiliza este procedimiento, los archivos que estén abiertos en el escritorio remoto se cierran sin guardar.

Utilizar una aplicación o un escritorio de Microsoft Windows en un sistema Linux

5

Horizon Client para Linux proporciona un entorno de aplicaciones y escritorios personalizado y sencillo. Los usuarios finales pueden acceder a dispositivos USB y de otro tipo conectados al equipo local, enviar documentos a las impresoras que este equipo pueda detectar, autenticarse con tarjetas inteligentes y usar varios monitores.

Este capítulo incluye los siguientes temas:

- [Matriz de compatibilidad de funciones para clientes Linux](#)
- [Idiomas admitidos](#)
- [Teclados y monitores](#)
- [Mejorar el rendimiento del mouse en escritorios remotos](#)
- [Uso del redireccionamiento USB para conectar dispositivos USB](#)
- [Usar el redireccionamiento del puerto serie](#)
- [Usar escáneres](#)
- [Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos](#)
- [Usar la función de redireccionamiento de contenido URL](#)
- [Compartir sesiones de escritorios remotos](#)
- [Usar varias sesiones de una aplicación publicada desde dispositivos cliente diferentes](#)
- [Usar la función de aplicación remota](#)
- [Guardar documentos en una aplicación publicada](#)
- [Imprimir desde un escritorio remoto](#)
- [Copiar y pegar texto](#)

Matriz de compatibilidad de funciones para clientes Linux

Cuando planifique el protocolo de visualización y las funciones que estarán disponibles para el usuario final, utilice la siguiente información para determinar qué sistemas operativos cliente admiten cada función.

Tabla 5-1. Funciones que admiten los escritorios virtuales de Windows

Función	Escritorio de Windows 7	Escritorio de Windows 8.x	Escritorio de Windows 10	Escritorios Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019
Redireccionamiento USB	X	X	X	X
Audio/vídeo en tiempo real (RTAV)	X	X	X	X
Redireccionamiento del escáner	X	X	X	X
Redireccionamiento del puerto serie	X		X	
Protocolo de visualización RDP	X	X	X	X
Protocolo de visualización PCoIP	X	X	X	X
Protocolo de visualización VMware Blast	X	X	X	X
Administración de identidades				
Redireccionamiento multimedia (MMR) de Windows Media	X	X	X	
Redireccionamiento multimedia HTML5	X	X	X	X
Impresión basada en ubicación	X	X	X	X
Impresión virtual	X	X	X	X
VMware Integrated Printing	X	X	X	X
Tarjetas inteligentes	X	X	X	X
RSA SecurID o RADIUS	X	X	X	X
Single Sign-On	X	X	X	X
Varios monitores	X	X	X	X
Redireccionamiento de unidades cliente	X	X	X	X

Los escritorios de Windows Server 2016 necesitan Horizon Agent 7.0.2 o una versión posterior.

VMware Blast requiere Horizon Agent 7.0 o una versión posterior.

El redireccionamiento multimedia HTML5 requiere Horizon Agent 7.3.2 o versiones posteriores para Chrome, o Horizon Agent 7.5 o versiones posteriores para Edge.

Compatibilidad de funciones para escritorios publicados en hosts RDS

Los hosts RDS son equipos servidor con Servicios de Escritorio remoto de Windows y View Agent o Horizon Agent instalados. Varios usuarios pueden tener sesiones de escritorio remoto simultáneas en un host RDS. Un host RDS puede ser un equipo físico o una máquina virtual.

Nota En la tabla siguiente se incluyen solo filas con las funciones que son compatibles. Cuando el texto especifica una versión mínima de View Agent, el texto "y posterior" incluye Horizon Agent 7.0.x y posterior.

Tabla 5-2. Funciones compatibles con los hosts RDS

Función	Host RDS con Windows Server 2012 R2	Host RDS con Windows Server 2016	Host RDS con Windows Server 2019
RSA SecurID o RADIUS	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Redireccionamiento del puerto serie	Horizon Agent 7.6 y posterior	Horizon Agent 7.6 y posterior	Horizon Agent 7.6 y posterior
Tarjeta inteligente	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Single Sign-On	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Protocolo de visualización RDP	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Protocolo de visualización PCoIP	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Protocolo de visualización VMware Blast	Horizon Agent 7.0 y posterior	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
HTML Access	X (solo máquina virtual)	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Redireccionamiento multimedia (MMR) de Windows Media	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Redireccionamiento multimedia HTML5	Horizon Agent 7.3.2 o versiones posteriores	Horizon Agent 7.3.2 o versiones posteriores	Horizon Agent 7.3.2 o versiones posteriores
Redireccionamiento USB	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Redireccionamiento de unidades cliente	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior

Tabla 5-2. Funciones compatibles con los hosts RDS (continuación)

Función	Host RDS con Windows Server 2012 R2	Host RDS con Windows Server 2016	Host RDS con Windows Server 2019
Impresión virtual	De View Agent 6.2.x a Horizon Agent 7.6 (solo máquinas virtuales) Horizon Agent 7.7 y posterior (máquina virtual y máquina física)	Horizon Agent de 7.0.2 a Horizon Agent 7.6 (solo máquinas virtuales) Horizon Agent 7.7 y posterior (máquina virtual y máquina física)	Horizon Agent 7.7 y posterior
VMware Integrated Printing	Horizon Agent 7.9 o posterior	Horizon Agent 7.9 o posterior	Horizon Agent 7.9 o posterior
Impresión basada en ubicación	De View Agent 6.2.x a Horizon Agent 7.6 (solo máquinas virtuales) Horizon Agent 7.7 y posterior (máquina virtual y máquina física)	Horizon Agent de 7.0.2 a Horizon Agent 7.6 (solo máquinas virtuales) Horizon Agent 7.7 y posterior (máquina virtual y máquina física)	Horizon Agent 7.7 y posterior
Varios monitores	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Audio/vídeo en tiempo real (RTAV)	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.3 y posterior	Horizon Agent 7.7 y posterior

Para obtener información sobre qué ediciones de cada sistema operativo invitado son compatibles, consulte el documento *Instalación de Horizon 7*.

Limitaciones en funciones específicas

Las funciones que son compatibles en escritorios Windows con Horizon Client para Linux tienen las siguientes restricciones.

Tabla 5-3. Requisitos para funciones específicas

Función	Requisitos
Audio/vídeo en tiempo real	Son necesarios los protocolos de visualización VMware Blast o PCoIP.
Impresión virtual e impresión según ubicación para escritorios de RDS (en hosts RDS de máquinas virtuales) y aplicaciones remotas	Son necesarios los protocolos de visualización VMware Blast o PCoIP.
VMware Integrated Printing	Requiere Horizon Agent 7.9 o una versión posterior.
Redireccionamiento multimedia HTML5	Son necesarios los protocolos de visualización VMware Blast o PCoIP.

Tabla 5-3. Requisitos para funciones específicas (continuación)

Función	Requisitos
Redireccionamiento USB	Son necesarios los protocolos de visualización VMware Blast o PCoIP.
Redireccionamiento de escáner	Son necesarios los protocolos de visualización VMware Blast o PCoIP.

Nota También puede utilizar Horizon Client para acceder de forma segura a aplicaciones remotas basadas en Windows además de escritorios remotos. Cuando seleccione una aplicación en Horizon Client, se abrirá una ventana de dicha aplicación en el dispositivo del cliente final y la aplicación se verá y se comportará como si estuviera instalada localmente.

Nota El proveedor y el modelo de cada dispositivo cliente ligero y la configuración que decide usar una empresa determinan las características que estarán disponibles en el dispositivo. Para obtener más información sobre modelos de dispositivos de cliente ligeros, consulte la *Guía de compatibilidad de VMware* en <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm>.

Para ver las descripciones de estas funciones y sus limitaciones, consulte el documento acerca de *cómo planificar Horizon 7*.

Compatibilidad de funciones para los escritorios de Linux

Los sistemas operativos invitados Linux son compatibles. Si desea obtener una lista de los sistemas operativos Linux compatibles e información sobre las funciones admitidas, consulte el documento *Configurar escritorios de Horizon 7 for Linux*.

Idiomas admitidos

La interfaz de usuario y la documentación están disponibles en inglés, japonés, francés, alemán, chino simplificado, chino tradicional, coreano y español.

Teclados y monitores

Es posible utilizar varios monitores y todos los tipos de teclados con un escritorio remoto. Algunas opciones permiten disfrutar de la mejor experiencia de usuario posible.

Prácticas recomendadas para usar varios monitores

A continuación, le presentamos recomendaciones para usar correctamente varios monitores con un escritorio remoto:

- Defina el monitor principal como el que ocupa la posición inferior izquierda.
- Habilite Xinerama. Si no habilita esta extensión, la pantalla principal no se identificará correctamente.

- La barra de menú aparece en el monitor que ocupa la posición superior izquierda. Por ejemplo, si tiene dos monitores lado a lado y la parte superior del monitor de la izquierda está por debajo de la parte superior del monitor de la derecha, la barra de menú aparece en el monitor de la derecha porque ese es el monitor que está situado más arriba y a la izquierda.

- Puede usar hasta cuatro monitores si cuenta con suficiente RAM de vídeo.

Si desea usar más de dos monitores para mostrar el escritorio remoto en un sistema cliente Ubuntu, debe configurar el ajuste `kernel.shmmax` correctamente. Use la siguiente fórmula:

max horizontal resolution X max vertical resolution X max number of monitors X 4

Por ejemplo, al configurar de forma manual `kernel.shmmax` a 65536000 puede usar cuatro monitores con una resolución de pantalla de 2560x1600.

- Horizon Client utiliza la configuración del monitor que se encuentra en uso cuando se inicia Horizon Client. Si cambia un monitor de modo horizontal a vertical o si conecta un monitor adicional en el sistema cliente mientras se ejecuta Horizon Client, debe reiniciar Horizon Client para utilizar la nueva configuración del monitor.

Horizon Client es compatible con las siguientes configuraciones del monitor:

- Si utiliza dos monitores, no es necesario que se encuentren en el mismo modo. Por ejemplo, si usa un portátil conectado a un monitor externo, este puede presentar una orientación vertical u horizontal.
- Si tiene una versión de Horizon Client anterior a la 4.0 y utiliza más de dos monitores, estos deberán estar en el mismo modo y tener la misma resolución de pantalla. Esto significa que si usa tres monitores, todos ellos deberán estar en modo horizontal o vertical y usar la misma resolución de pantalla.
- Los monitores pueden estar colocados uno al lado del otro, apilados de 2 en 2 o de forma vertical solo si está usando dos monitores.
- Si especifica que desea usar todos los monitores y utiliza los protocolos de visualización VMware Blast o PCoIP, puede especificar un subgrupo de monitores adyacentes. Para ello, haga clic con el botón secundario en la ventana de selección del escritorio, seleccione **Pantalla completa - Todos los monitores** en el menú desplegable **Pantalla** y, a continuación, haga clic para seleccionar los monitores que desea usar.

Nota Si tiene un sistema cliente Ubuntu, debe seleccionar el monitor situado en la parte superior izquierda como uno de los monitores. Por ejemplo, si tiene cuatro monitores agrupados 2x2, deberá seleccionar los dos monitores de la parte superior o los dos situados más a la izquierda.

Resolución de pantalla

Tenga en cuenta las siguientes instrucciones cuando configure la resolución de pantalla:

- Si abre un escritorio remoto en un monitor secundario y, a continuación, cambia la resolución de pantalla en dicho monitor, el escritorio remoto se trasladará al monitor principal.

- En el caso de PCoIP, si utiliza dos monitores, puede ajustar la resolución de cada monitor de forma separada, con una resolución de hasta 2560x1600 por pantalla. Si utiliza más de dos monitores, estos deben tener la misma resolución de pantalla.
- Gracias a los protocolos de visualización VMware Blast o PCoIP, se admite una resolución de pantalla de escritorio remoto de 4K (3840 x 2160). El número de pantallas 4K que se admite depende de la versión de hardware de la máquina virtual de escritorio y la versión de Windows.

Versión de hardware	Versión de Windows	Número de pantallas 4K admitidas
10 (compatible con ESXi 5.5.x)	7, 8, 8.x, 10	1
11 (compatible con ESXi 6.0)	7 (funciones de representación 3D y Windows Aero deshabilitadas)	3
11	7 (función de representación 3D habilitada)	1
11	8, 8.x, 10	1
13 o 14	7, 8, 8.x, 10 (función de representación 3D habilitada)	1
13 o 14	7, 8, 8.x, 10	4

Para obtener el mejor rendimiento, la máquina virtual debe disponer al menos de 2 GB de RAM y 2 CPU virtuales. Esta función puede requerir buenas condiciones de red, como un ancho de banda de 1000 Mbps con una baja latencia de red y una reducida tasa de pérdida de paquetes.

Nota Cuando la resolución de pantalla del escritorio remoto se establece en 3840 x 2160 (4K), es posible que los elementos de la pantalla se muestren más pequeños; asimismo, es posible que no pueda usar el cuadro de diálogo de resolución de pantalla para hacer que el texto y otros elementos se muestren más grandes.

- En el caso de RDP, si cuenta con varios monitores, no puede ajustar la resolución de cada monitor de forma independiente.

Limitaciones del teclado

Por lo general, los teclados funcionan con un escritorio remoto igual que con un equipo físico. A continuación aparece una lista de las limitaciones con las que se podría encontrar, según el tipo de periféricos y de software de su sistema cliente:

- Si usa el protocolo de visualización PCoIP y desea que el escritorio remoto detecte qué asignación de teclado usa el sistema cliente como, por ejemplo, un teclado japonés o un teclado alemán, debe configurar un GPO en Horizon Agent. Utilice la directiva para **activar la**

sincronización del PColP del idioma de entrada predeterminado del usuario, disponible como parte del archivo de plantilla ADM de variables de la sesión PColP de View. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

- Es posible que no funcionen algunas teclas multimedia de un teclado multimedia. Por ejemplo, es posible que no funcionen la tecla Música o la tecla Mi equipo.
- Si se conecta a un escritorio a través de RDP y cuenta con el administrador de ventanas Fluxbox, el teclado puede dejar de funcionar después de un periodo de inactividad (si se ejecuta un protector de pantalla en el escritorio remoto).

Independientemente de qué administrador de ventanas utilice, es recomendable desactivar el protector de pantalla en escritorios remotos y no especificar el tiempo de suspensión.

Utilizar la función Ajuste de escala de la pantalla

Los usuarios con problemas en la vista o que tengan pantallas de alta resolución, como monitores 4K, suelen ajustar la escala de la pantalla estableciendo el porcentaje de los puntos por pulgada del sistema cliente por encima del 100 %. La configuración de PPP controla el tamaño del texto, de las aplicaciones y los iconos. Una configuración de PPP más baja hace que aparezcan con un tamaño menor y una configuración más elevada hace que aparezcan con mayor tamaño. Con la función de ajuste de escala de la pantalla y los escritorios remotos permiten ajustar la escala de la máquina cliente para mostrarse en tamaño normal en lugar de muy pequeños.

Nota La función Ajuste de escala de PPP no se admite en dispositivos Raspberry Pi y no funciona con aplicaciones publicadas.

En una configuración de varios monitores, usar la escala de la pantalla no afecta el número de monitores y a las resoluciones máximas que admite Horizon Client. Cuando el ajuste de escala de la pantalla se admita y se esté utilizando, la escala se basará en el ajuste de PPP del sistema.

Este procedimiento describe cómo usar uno de los archivos de configuración para habilitar o deshabilitar el ajuste de escala de la pantalla para todos los escritorios remotos.

Procedimiento

- 1 Abra el archivo de configuración `~/.vmware/view-preferences`, `/etc/vmware/view-default-config` o `/etc/vmware/view-mandatory-config` en un editor de texto.
- 2 Establezca la clave de configuración `view.enableDisplayScaling`.

Establezca el valor **"TRUE"** o **"FALSE"**. Cuando esta opción está configurada como **"FALSE"**, la función de ajuste de escala de la pantalla se deshabilita en todos los escritorios remotos. Si esta opción no está configurada o se establece como **"TRUE"**, (la opción predeterminada), el ajuste de escala de la pantalla está habilitado en todos los escritorios remotos.

- 3 Guarde los cambios y cierre el archivo.

Usar la sincronización PPP

La función Sincronización de PPP garantiza que la configuración de PPP en una aplicación publicada o un escritorio remoto coincida con la del sistema cliente.

Nota No se admite la función Sincronización de PPP en dispositivos Raspberry Pi.

Cuando la función Sincronización PPP y la función Ajuste de escala de la pantalla están habilitadas, en todo momento solo tiene efecto una de las dos funciones. La escala de la pantalla tiene lugar únicamente cuando la sincronización de PPP aún no se realizó (esto es, antes de que la configuración PPP del escritorio remoto coincida con la configuración PPP del sistema cliente), y se detiene después de que coincidan ambas configuraciones.

La opción de la directiva de grupo **Sincronización de PPP** determina si la función Sincronización de PPP está habilitada. Esta función está habilitada de forma predeterminada. Con la sincronización de PPP, se cambia el valor de PPP en la sesión remota para que coincida con el valor de PPP del equipo cliente cuando se conecte a un escritorio remoto o aplicación publicada. Para usar la función Sincronización de PPP, se necesita Horizon Agent 7.0.2 o una versión posterior.

Si la opción de la directiva de grupo **Sincronización de PPP por conexión** está habilitada además de la opción de la directiva de grupo **Sincronización de PPP**, la sincronización de PPP estará disponible cuando vuelva a conectarse a un escritorio remoto. Esta función está deshabilitada de forma predeterminada. Para usar la función Sincronización de PPP por conexión, se necesita Horizon Agent 7.8 o una versión posterior.

Para obtener más información sobre las opciones de las directivas de grupo **Sincronización de PPP** y **Sincronización de PPP por conexión**, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

En escritorios virtuales, la función Sincronización de PPP es compatible con los siguientes sistemas operativos invitados:

- Windows 7 de 64 o 32 bits
- Windows 8.x de 64 o 32 bits
- Windows 10 de 64 o 32 bits
- Windows Server 2012 R2 configurado como escritorio
- Windows Server 2016 configurado como escritorio
- Windows Server 2019 configurado como escritorio

Para aplicaciones y escritorios publicados, la función Sincronización PPP es compatible con los siguientes hosts RDS:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

En escritorios virtuales, la función Sincronización de PPP por conexión es compatible con los siguientes sistemas operativos invitados:

- Windows 10 1607 y versiones posteriores
- Windows Server 2016 y versiones posteriores (como escritorio)

La función Sincronización de PPP por conexión no se admite en escritorios publicados ni aplicaciones publicadas.

A continuación le mostramos algunos consejos para usar la función Sincronización de PPP.

- Si cambia el ajuste de PPP en el sistema cliente, pero no se cambia en el escritorio remoto, es posible que tenga que cerrar la sesión y volver a iniciarla para que quede constancia en Horizon Client del nuevo ajuste de PPP en el sistema cliente.
- Si inicia una sesión remota en un sistema cliente que tenga una configuración PPP de más del 100 % y utiliza la misma sesión en otro sistema cliente que tenga una configuración PPP diferente de más del 100 %, es posible que tenga que cerrar la sesión remota y volver a iniciarla en el segundo sistema cliente para hacer que la sincronización de PPP funcione en dicho sistema.
- Si un administrador de Horizon cambia el valor configurado para la directiva de grupo **Sincronización de PPP** para Horizon Agent, debe cerrar sesión y volver a iniciarla para que se aplique la nueva configuración.

Seleccionar monitores específicos para mostrar las aplicaciones publicadas

Si tiene dos monitores o más, puede seleccionar los monitores en los que se mostrarán las ventanas de la aplicación publicada. Por ejemplo, si dispone de tres monitores, puede especificar que la ventana de la aplicación publicada solo aparezca en dos de esos monitores.

Puede seleccionar hasta cuatro monitores contiguos. Los monitores pueden estar uno junto al otro, o bien apilados verticalmente. Por ejemplo, puede configurar dos filas de dos monitores cada una.

Nota Para las pantallas 4K, se aplican las siguientes restricciones:

- Para una aplicación publicada en un host RDS, puede seleccionar hasta cuatro monitores adyacentes.
 - Para una aplicación publicada en un escritorio alojado en RDS, puede seleccionar hasta tres monitores adyacentes.
-

Requisitos previos

Debe tener al menos dos monitores.

Procedimiento

- 1 Inicie Horizon Client y conéctese a un servidor.

- 2 Haga clic en el botón **Configuración** (icono de rueda dentada) situado en la esquina superior derecha de la ventana de selección de aplicaciones y escritorios.
- 3 Seleccione **Aplicaciones** en el panel izquierdo del cuadro de diálogo Configuración.

Las miniaturas de los monitores conectados actualmente al sistema cliente aparecen en **Configuración de pantalla**. La topología de visualización se corresponde con la configuración de pantalla del sistema cliente.

- 4 Para seleccionar o anular la selección de un monitor en el que visualizar aplicaciones publicadas, haga clic en una miniatura.

Al seleccionar un monitor, su miniatura cambia de color. Sin infringe alguna regla de selección de visualización, aparece un mensaje de advertencia.

Configurar la sincronización de las teclas de bloqueo

Puede configurar Horizon Client para que se utilice el estado de las teclas Bloq Num, Bloq Despl y Bloq mayús del sistema cliente en un escritorio remoto, y desde un escritorio remoto al sistema cliente. La configuración se aplica globalmente a todos los escritorios remotos en una conexión de servidor determinada.

Procedimiento

- 1 Inicie Horizon Client y conéctese a un servidor.
- 2 Abra el cuadro de diálogo Configuración de un escritorio remoto.
 - En la esquina superior derecha de la ventana de selección de aplicaciones y escritorios, haga clic en el botón **Configuración** (rueda dentada) y seleccione cualquier escritorio remoto en el panel izquierdo.
 - En la ventana de selección de aplicaciones y escritorios, haga clic con el botón secundario en cualquier escritorio remoto y seleccione **Configuración**.
- 3 Para habilitar la función de sincronización de las teclas de bloqueo, seleccione la casilla de verificación **Sincronizar automáticamente las teclas Bloq Num, Bloq mayús y Bloq Despl** y haga clic en **Cerrar**.

Nota Si el escritorio remoto no admite la capacidad para sincronizar el estado de la tecla de bloqueo, la casilla de verificación **Sincronizar automáticamente las teclas Bloq Num, Bloq mayús y Bloq Despl** aparecerá atenuada y no se podrá seleccionar.

Resultados

La función de sincronización de las teclas de bloqueo está habilitada para todos los escritorios remotos en la conexión del servidor.

Si anula la selección de la casilla de verificación **Sincronizar automáticamente las teclas Bloq Num, Bloq mayús y Bloq Despl**, la función de sincronización de la tecla de bloqueo estará deshabilitada para todos los escritorios remotos en la conexión del servidor.

Mejorar el rendimiento del mouse en escritorios remotos

Si usa los protocolos de visualización VMware Blast o PCoIP cuando use aplicaciones 3D en un escritorio remoto, el rendimiento del mouse mejora si habilita la función del mouse relativo.

En la mayoría de los casos, si utiliza aplicaciones que no necesiten un procesamiento 3D, Horizon Client transmite información sobre los movimientos del puntero del mouse usando coordenadas absolutas. Con las coordenadas absolutas, el cliente procesa los movimientos del mouse de forma local, lo que mejora el rendimiento, especialmente si se encuentra fuera de la red corporativa.

Para las tareas que necesiten usar aplicaciones con un alto consumo gráfico, como AutoCAD, o para jugar a videojuegos 3D, puede mejorar el rendimiento del mouse habilitando la función de mouse relativo, que usa coordenadas relativas en lugar de absolutas.

La función de mouse relativo de Horizon Client no está habilitada de forma predeterminada. Puede usar la clave de configuración `view.enableRelativeMouse` del archivo `~/.vmware/view-preferences` para habilitar o deshabilitar el mouse relativo de Horizon Client y no permitir que los usuarios cambien la opción en la interfaz de usuario Horizon Client. Debe configurar la opción de mouse relativo antes de que los usuarios finales se conecten a un servidor. La opción se aplica a la sesión actual de conexión al escritorio. Si la opción de mouse relativo de Horizon Client se configura usando el archivo `~/.vmware/view-preferences`, los usuarios finales no pueden cambiar la opción después de conectarse a un servidor.

Cuando la función del mouse relativo esté habilitada, es posible que el rendimiento sea más lento si se encuentra fuera de la red corporativa (en una WAN).

Requisitos previos

Un administrador de Horizon debe activar el procesamiento 3D para el grupo de escritorios. Para obtener información sobre la configuración de grupo y las opciones disponibles para el procesamiento 3D, consulte los documentos *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- 1 Inicie Horizon Client y, a continuación, inicie sesión en el servidor.
- 2 Haga clic con el botón secundario en el escritorio remoto y seleccione **VMware Blast** o **PCoIP**.
- 3 Conéctese al escritorio remoto.

4 Seleccione **Conexión > Habilitar mouse relativo** en la barra de menú de Horizon Client.

La opción es un botón para habilitar o deshabilitar. Para deshabilitar la función de mouse relativo, vuelva a seleccionar **Conexión > Habilitar mouse relativo**.

Nota Si usa Horizon Client en modo de ventana en lugar de en modo de pantalla completa y el mouse relativo está habilitado, es posible que no pueda mover el puntero del mouse hacia las opciones del menú de Horizon Client ni mover el puntero fuera de la ventana de Horizon Client. Para solucionar esta situación, pulse Ctrl+Alt.

Uso del redireccionamiento USB para conectar dispositivos USB

Con la función de redireccionamiento USB, puede usar los dispositivos USB conectados de forma local, como unidades de memoria flash, en un escritorio remoto o una aplicación publicada.

Cuando se usa la función de redireccionamiento USB, la mayoría de los dispositivos USB conectados al sistema de cliente local pasan a estar disponibles en los menús de Horizon Client. Estos menús permiten conectar y desconectar los dispositivos.

Puede redireccionar unidades de memoria flash USB conectadas de forma local y unidades de disco duro para usarlas en las aplicaciones y los escritorios publicados. A partir de Horizon Agent 7.0.2, las aplicaciones y los escritorios publicados también pueden admitir dispositivos USB que sean más genéricos, entre los que se incluyen los dispositivos de firma digital Wacom y TOPAZ Signature Pad, así como el pedal Olympus Dictation Foot. Otros tipos de dispositivos USB, como unidades de almacenamiento de seguridad y unidades CD-ROM USB, no se admiten en aplicaciones y escritorios publicados.

Puede conectar dispositivos USB a un escritorio remoto o una aplicación publicada de forma manual o automática.

Importante En los siguientes procedimientos se describe cómo usar Horizon Client para conectar dispositivos USB a un escritorio remoto o una aplicación publicada. También puede configurar el redireccionamiento USB con un archivo de configuración o si crea una directiva de grupo. Para obtener más información sobre cómo usar un archivo de configuración, consulte [Capítulo 6 Configurar el redireccionamiento USB en el cliente](#). Para obtener más información sobre la creación de directivas de grupo, consulte el documento sobre *configuración de grupos de aplicaciones y escritorios en Horizon 7*.

Requisitos previos

- Para utilizar dispositivos USB con un escritorio remoto o una aplicación publicada, un administrador de Horizon debe habilitar la función USB.

Esta tarea incluye la instalación del componente Redireccionamiento USB de Horizon Agent, y puede incluir la configuración de directivas relacionadas con el redireccionamiento USB. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7* y [Establecer las propiedades de configuración USB](#).

- El componente de redireccionamiento USB debe instalarse en Horizon Client. Si no incluyó este componente en la instalación, desinstale el cliente y ejecute el programa de instalación de nuevo para incluir el componente de redireccionamiento USB.
- Familiarícese con [Limitaciones del redireccionamiento USB](#).

Procedimiento

- ◆ Conecte un dispositivo USB a un escritorio remoto.
 - a Conecte el dispositivo USB al sistema de cliente local.
 - b En la barra de menús de Horizon Client, haga clic en **Conectar dispositivo USB**.
 - c Seleccione el dispositivo USB.

El dispositivo se redirigirá del sistema local al escritorio remoto.

- ◆ Conecte un dispositivo USB a una aplicación publicada.
 - a Conecte el dispositivo USB al sistema de cliente local.
 - b En la ventana de selección de aplicaciones y escritorios, abra la aplicación publicada.

El nombre de la aplicación es el nombre que su administrador ha configurado para la aplicación.
 - c En la ventana de selección de aplicaciones y escritorios, haga clic con el botón secundario en el icono de la aplicación y seleccione **Configuración**.
 - d En el panel izquierdo, seleccione **Dispositivos USB**.
 - e En el panel derecho, seleccione el dispositivo USB y haga clic en **Conectarse**.
 - f Seleccione la aplicación y haga clic en **Aceptar**.

Nota El nombre de la aplicación que se muestra en la lista procede de la propia aplicación y puede que no coincida con el nombre de aplicación que configuró el administrador para que se mostrara en la ventana de selección de aplicaciones y escritorios.

Horizon Client conectará el dispositivo USB a la aplicación publicada seleccionada. El dispositivo USB también estará disponible para otras aplicaciones de la misma granja que la aplicación seleccionada. El dispositivo USB no queda liberado inmediatamente después de cerrar la aplicación.

- g **(Opcional)** Si desea configurar Horizon Client para que conecte automáticamente el dispositivo USB a la aplicación publicada cuando esta se inicie, seleccione la casilla de verificación **Conectar automáticamente al inicio** y haga clic en **Aplicar**. Esta opción no está seleccionada de forma predeterminada y se guarda en `~/.vmware/view-brokers-prefs`.

Esta opción también se aplica a las demás aplicaciones de la misma granja que la aplicación que seleccionó.

Nota La clave de configuración `view.usbAutoConnectAtStartup` y la opción de la línea de comandos `--usbAutoConnectAtStartup` reemplazan la configuración guardada en `~/.vmware/view-brokers-prefs`. Para obtener más información, consulte [Opciones de la línea de comandos y configuración de Horizon Client](#).

- h **(Opcional)** Si desea que Horizon Client conecte automáticamente el dispositivo USB a la aplicación publicada al insertar el dispositivo en el sistema local, seleccione la casilla de verificación **Conectar automáticamente al insertar** y haga clic en **Aplicar**. Esta opción no está seleccionada de forma predeterminada y se guarda en `~/.vmware/view-brokers-prefs`.

Para que esto sea posible, la aplicación publicada debe estar activada y en primer plano. Esta opción también se aplica a las demás aplicaciones de la misma granja que la aplicación que seleccionó.

Nota La clave de configuración `view.usbAutoConnectOnInsert` y la opción de la línea de comandos `--usbAutoConnectOnInsert` reemplazan la configuración guardada en `~/.vmware/view-brokers-prefs`. Para obtener más información, consulte [Opciones de la línea de comandos y configuración de Horizon Client](#).

- i Para cerrar la ventana Configuración, haga clic en **Cerrar**.
 - j Cuando termine de utilizar la aplicación, libere el dispositivo USB para que pueda acceder a él desde el sistema local. En la ventana de selección de aplicaciones y escritorios, vuelva a abrir la ventana Configuración, seleccione **Dispositivos USB** y, a continuación, seleccione **Desconectar**.
- ◆ Configure Horizon Client para conectar los dispositivos USB automáticamente a un escritorio remoto cuando se inicie Horizon Client.

De forma predeterminada, esta opción no está seleccionada.

- a Antes de insertar el dispositivo USB, inicie Horizon Client y conéctese a un escritorio remoto.
- b En la barra de menús de Horizon Client, haga clic en **Conectar dispositivo USB**.
- c Seleccione **Conectarse automáticamente al inicio**.
- d Inserte el dispositivo USB y reinicie Horizon Client.

Los dispositivos USB que conecte al sistema local después de iniciar Horizon Client se redirigen al escritorio remoto.

- ◆ Configure Horizon Client para conectar automáticamente dispositivos USB a un escritorio remoto al insertarlos en el sistema local.

Para que esto sea posible, el escritorio remoto debe estar activado y en primer plano.

Habilite esta opción si tiene previsto conectar dispositivos que utilicen controladores MTP como tablets y smartphones Samsung con Android. De forma predeterminada, esta opción no está seleccionada.

- a Antes de insertar el dispositivo USB, inicie Horizon Client y conéctese a un escritorio remoto.
- b En la barra de menús de Horizon Client, haga clic en **Conectar dispositivo USB**.
- c Seleccione **Conectarse automáticamente al insertar el dispositivo**.
- d Inserte el dispositivo USB.

Los dispositivos USB que conecte al sistema local después de iniciar Horizon Client se redirigen al escritorio remoto.

Nota También puede configurar la conexión automática de dispositivos USB a escritorios remotos con las opciones del archivo de configuración `view.usbAutoConnectAtStartup` y `view.usbAutoConnectOnInsert`. Si desea obtener más información, consulte [Opciones de la línea de comandos y configuración de Horizon Client](#).

Resultados

Si el dispositivo USB no aparece en el escritorio remoto o la aplicación publicada pasados unos minutos, desconéctelo del sistema cliente y vuelva a conectarlo.

Pasos siguientes

Si tiene problemas con el redireccionamiento USB, consulte el tema sobre la resolución de problemas de redireccionamiento en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Limitaciones del redireccionamiento USB

La función de redireccionamiento USB tiene algunas limitaciones.

- Al obtener acceso a un dispositivo USB desde un menú de Horizon Client y usar el dispositivo en un escritorio remoto o aplicación publicada, no podrá obtener acceso al dispositivo USB en el dispositivo local.
- Los dispositivos USB que no aparezcan en el menú, pero que están disponibles en un escritorio remoto o aplicación publicada, incluyen dispositivos de interfaz humana como teclados y dispositivos señaladores. Tanto el escritorio remoto o la aplicación publicada como el dispositivo local usan estos dispositivos de forma simultánea. La interacción con estos dispositivos USB puede ser lenta en algunas ocasiones debido a la latencia de la red.

- Las unidades de disco USB de gran tamaño pueden tardar varios minutos en aparecer en el escritorio remoto o la aplicación publicada.
- Algunos dispositivos USB requieren controladores específicos. Si un controlador requerido aún no está instalado, puede que se le pida que lo instale al conectar el dispositivo USB al escritorio remoto o la aplicación publicada.
- Si tiene previsto conectar dispositivos USB que usen controladores MTP, como tabletas y smartphones Samsung con Android, configure Horizon Client para que conecte los dispositivos USB al escritorio remoto o la aplicación publicada automáticamente. En caso contrario, si intenta redirigir manualmente el dispositivo USB mediante un elemento de menú, no lo hará a menos que desconecte el dispositivo y lo vuelva a conectar.
- No use el menú **Conectar dispositivo USB** para la conexión de escáneres. Para usar un dispositivo de escáner, emplee la función de redireccionamiento de escáneres. Esta función está disponible para Horizon Client cuando se utiliza con Horizon Agent 7.8 o versiones posteriores. Consulte [Usar escáneres](#).
- El redireccionamiento de dispositivos de audio USB depende del estado de la red y no es fiable. Algunos dispositivos requieren un elevado rendimiento de datos incluso cuando están inactivos. Los dispositivos de entrada y salida de audio funcionan correctamente con la función Audio/vídeo en tiempo real. No es necesario utilizar el redireccionamiento USB para esos dispositivos.
- No puede formatear una unidad USB redireccionada de un escritorio publicado, a menos que se conecte como usuario administrador.

Nota No redirija dispositivos USB, como USB Ethernet y de pantalla táctil, a un escritorio remoto o una aplicación publicada. Si redirige un dispositivo USB Ethernet, su sistema cliente perderá la conectividad de red. Si redirige un dispositivo de pantalla táctil, el escritorio remoto o la aplicación publicada recibirán la entrada táctil, pero no la del teclado. Si configuró el escritorio remoto o la aplicación publicada para que conecte automáticamente dispositivos USB, puede configurar una directiva para excluir dispositivos específicos. Consulte "Configurar los ajustes de directiva de filtro para dispositivos USB" del documento *Configurar funciones de escritorios remotos en Horizon 7*.

Usar el redireccionamiento del puerto serie


Con el redireccionamiento de puerto serie, puede redireccionar los puertos serie conectados localmente (/dev/ttyS), como es el caso de los puertos RS232 integrados y los adaptadores de puerto USB a puerto serie. Los dispositivos, como impresoras, lectores de códigos de barra y otros dispositivos serie, se pueden conectar a estos puertos y se pueden usar en escritorios virtuales y escritorios alojados en RDS.

Si un administrador de Horizon configuró la función de redireccionamiento del puerto serie y se usa el protocolo de visualización VMware Blast o PCoIP, el redireccionamiento del puerto serie funcionará en el escritorio virtual o el escritorio alojado en RDS sin necesidad de configurar nada más. Por ejemplo, `/dev/ttyS0` en el sistema cliente local se redirecciona como COM1 en el escritorio remoto. El puerto serie `/dev/ttyS1` se redirecciona como COM2. Si el puerto `/dev/ttyS` ya está en uso, se asigna para evitar conflictos. Por ejemplo, si COM1 y COM2 existen en el escritorio remoto, `/dev/ttyS0` del sistema cliente se asigna a COM3 de forma predeterminada.

Debe tener instalado todos los controladores del dispositivo en el sistema cliente local, pero no tiene que instalar los controladores del dispositivo en el escritorio remoto. Por ejemplo, si utiliza un adaptador USB a puerto serie que requiera controladores específicos que funcionen en el sistema cliente local, debe instalar estos controladores únicamente en el sistema cliente.

Importante Si utiliza un dispositivo que se enchufe en un adaptador USB a puerto serie, no conecte el dispositivo desde el menú **Conectar dispositivo USB** en Horizon Client. Al hacer esto, se enruta el dispositivo a través del redireccionamiento USB y se deriva la función del redireccionamiento del puerto serie.

Consejos para usar la función de redireccionamiento del puerto serie

- Haga clic en el icono de puerto serie () en la bandeja del sistema (o el área de notificaciones) del escritorio remoto para conectarse, desconectarse o personalizar los puertos `/dev/ttyS` asignados.

Cuando haga clic en el icono del puerto serie, aparece el menú contextual

Redireccionamiento COM serie para VMware Horizon. Si un administrador bloqueó la configuración, se atenúan los elementos del menú contextual. El icono aparece solo si un administrador de Horizon configuró la función de redireccionamiento del puerto serie y se cumplen todos los requisitos. Si desea obtener más información, consulte [Requisitos del sistema para el redireccionamiento del puerto serie](#).

- En el menú contextual, los elementos del puerto aparecen como **puerto se asignó a puerto**, por ejemplo **`/dev/ttyS0` se asignó a COM1**. El primer puerto, que se corresponde a `/dev/ttyS0` en este ejemplo, es el puerto físico o el adaptador USB a puerto serie del sistema cliente local. El segundo puerto, que se corresponde a COM1 en este ejemplo, es el puerto utilizado en el escritorio remoto.
- Para seleccionar el comando **Propiedades del puerto**, haga clic con el botón secundario en el puerto `/dev/ttyS`.

En el cuadro de diálogo de las propiedades de COM, puede configurar un puerto para que se conecte automáticamente cuando una sesión del escritorio remoto se inicie, o puede ignorar el DSR (señal del conjunto de datos preparado), que es necesario para algunos módems y otros dispositivos.

También puede cambiar el número de puerto que el escritorio remoto usa. Por ejemplo, si el puerto `/dev/ttyS0` del sistema cliente está asignado a COM3 del escritorio remoto, puede cambiar el número de puerto a COM1. Si COM1 existe en el escritorio remoto, verá **COM1 (superpuesto)**. Puede seguir utilizando este puerto superpuesto. El escritorio remoto puede recibir datos en serie a través del puerto desde el servidor y también desde el sistema cliente.

- Conéctese a un puerto COM asignado seleccionando **Conectar** para usar el puerto en el escritorio remoto.

Cuando se abra un puerto COM redireccionado y en uso en un escritorio remoto, no podrá acceder al puerto en el equipo local. Del mismo modo, cuando un puerto `/dev/ttyS` está en uso en el equipo local, no podrá acceder al puerto del escritorio remoto.

- Puede seleccionar el comando **Desconectar** para desconectarse y hacer que el puerto COM físico esté disponible para su uso en el equipo cliente.

Usar escáneres

La función de redireccionamiento del escáner permite escanear información en escritorios remotos con escáneres que estén conectados al sistema cliente local. Puede controlar la configuración del escáner mediante las opciones de la interfaz del escritorio remoto. Esta función redirecciona los datos escaneados con un ancho de banda significativamente inferior al que se puede alcanzar utilizando un redireccionamiento USB.

El redireccionamiento del escáner está disponible en los dispositivos de escáner compatibles con el estándar de interfaz SANE. Debe instalar los controladores del escáner SANE en el sistema cliente local. No es necesario instalar los controladores de del escáner en un escritorio remoto.

La función de redireccionamiento del escáner no es compatible con las cámaras web. VMware recomienda utilizar la función Audio/vídeo en tiempo real para redireccionar las cámaras web.

Nota El redireccionamiento de escáneres al escritorio remoto no funciona cuando se escanea desde una aplicación que admite el estándar WIA (Adquisición de imágenes de Windows). Para usar el redireccionamiento de escáneres, escanee desde una aplicación con soporte para el estándar TWAIN.

Si un administrador de Horizon configuró la función de redireccionamiento del escáner y si usa los protocolos de visualización VMware Blast o PCoIP, es posible utilizar un escáner conectado a su sistema cliente local en un escritorio remoto.

Importante No use el menú **Conectar dispositivo USB** para la conexión de escáneres en Horizon Client. El rendimiento no será adecuado.


Si se redirecciona la información escaneada a un escritorio remoto, no podrá acceder al escáner en el equipo cliente local. Por el contrario, cuando un escáner está en uso en el equipo cliente local, no podrá acceder a él en el escritorio remoto.

Nota Si conecta un escáner a un puerto USB en el equipo cliente local, Horizon Client envía la información escaneada al escritorio remoto a través del redireccionamiento USB de forma predeterminada. Si prefiere enviar los datos a través de redireccionamiento de escáner, configure una directiva de redireccionamiento USB para excluir su dispositivo de escaneado. Si desea obtener más información, consulte [Establecer las propiedades de configuración USB](#).

Un administrador de Horizon puede configurar la directiva de grupo para controlar las opciones que están disponibles en el cuadro de diálogo Preferencias de redirección de VMware Horizon Scanner. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Nota Si un administrador de Horizon configura el redireccionamiento del escáner para usar un escáner específico y dicho escáner no está disponible, el redireccionamiento no funcionará.

Consejos para usar la función de redireccionamiento del escáner

- Para cambiar la configuración de redireccionamiento del escáner, haga clic en el icono del escáner () en la bandeja del sistema o el área de notificaciones del escritorio remoto.

Si el escáner o el servicio de puerto serie no se inician, reinicie el sistema cliente local.

Nota No es necesario que use el menú que aparece cuando hace clic en el icono del escáner. El redireccionamiento del escáner funciona sin necesidad de configurar nada. Si el menú que aparece no muestra ningún escáner, un escáner que no es compatible está conectado en el equipo cliente. Si no aparece el icono del escáner, la función del redireccionamiento del escáner está deshabilitada o no se instaló en el escritorio remoto. El icono de escáner tampoco aparece en sistemas cliente locales que no admitan esta función.

- Si desea que aparezca el cuadro de diálogo de propiedades de escaneo TWAIN aunque una aplicación de escaneo no lo muestre, haga clic en la opción **Preferencias** del menú del icono del escáner y seleccione la casilla de verificación **Forzar el cuadro de diálogo de propiedades de escaneo TWAIN**.
- Para mostrar los nombres de escáner reales en lugar de VMware Virtual *nnn* scanner, haga clic en la opción **Preferencias** del menú del icono del escáner y seleccione la casilla de verificación **Usar nombres definidos por el proveedor para escáneres TWAIN**.
- Para seleccionar opciones para controlar la compresión de imágenes o determinar cómo seleccionar el escáner predeterminado, haga clic en la opción **Preferencias** del menú del icono del escáner y seleccione la pestaña **Compresión** o **Valores predeterminados**.

- La mayoría de los escáneres muestran un cuadro de diálogo de configuración del dispositivo de forma predeterminada, aunque algunos no lo hacen. Para los escáneres que no muestren las opciones de configuración, puede usar la opción **Preferencias** del menú del icono del escáner y seleccionar la opción **Mostrar siempre el cuadro de diálogo de configuración del escáner**.
- Para mostrar el cuadro de diálogo de propiedades del escáner TWAIN en el escritorio remoto, haga clic en la opción **Preferencias** del menú del icono del escáner y seleccione la casilla de verificación **Agente (cuadro de diálogo de propiedades de escaneado de VMware)**. Horizon Client para Linux no admite la opción **Cliente (cuadro de diálogo de propiedades de escaneado nativo, si se admite)**.
- Es posible que no se pueda escanear una imagen de gran tamaño o escanear con una resolución elevada. En este caso, puede observar que el indicador del proceso se bloquea o que se salga de la aplicación del escáner de forma inesperada. Si minimiza el escritorio remoto, puede aparecer un mensaje de error en el sistema cliente local que le notifica que la resolución es demasiado elevada. Para solucionar este problema, reduzca la resolución o recorte la imagen y vuelva a escanearla.

Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos

Con la función Audio/vídeo en tiempo real, puede utilizar el micrófono o la cámara web del sistema cliente local en un escritorio remoto o aplicación publicada. Audio/vídeo en tiempo real es compatible con las aplicaciones de vídeo basadas en el navegador y las aplicaciones de conferencia estándar. Admite la entrada de audio analógico, dispositivos USB de audio y cámaras web estándar.

Para obtener información sobre cómo configurar la función Audio/vídeo en tiempo real en la máquina agente, incluídas la velocidad de fotogramas y la resolución de la imagen, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Nota Esta función está disponible solo con la versión de Horizon Client para Linux proporcionada por proveedores externos o con el software de Horizon Client disponible desde el sitio web de descarga de productos de VMware.

Cuándo se puede utilizar una cámara web con la función Audio/vídeo en tiempo real

Si un administrador de Horizon ha configurado la función Audio/vídeo en tiempo real, podrá utilizar una cámara web integrada o conectada al equipo cliente en escritorios remotos o aplicaciones publicadas. Puede utilizar la cámara web en aplicaciones de conferencias como, por ejemplo, Skype, Webex o Google Hangouts.

Durante la configuración de una aplicación como Skype, Webex o Google Hangouts en un escritorio remoto, puede seleccionar dispositivos de entrada y salida desde los menús de la aplicación.

En los escritorios remotos y las aplicaciones publicadas, a las cámaras web redireccionadas se les asigna el nombre "cámara web virtual de VMware" en las aplicaciones.

Para la mayoría de las aplicaciones, no tiene que seleccionar ningún dispositivo de entrada.

Cuando el equipo cliente usa la cámara web, la sesión remota no podrá usarla al mismo tiempo. Cuando la sesión remota usa la cámara web, el equipo cliente tampoco podrá usarla al mismo tiempo.

Importante Si los usuarios finales usan cámaras web USB, no configure el cliente para reenviar dispositivos a través del redireccionamiento USB. Si la cámara web se conecta a través de un redireccionamiento USB, el rendimiento no es adecuado para realizar una videollamada.

Si hay más de una cámara web conectada al equipo cliente local, puede configurar una cámara web preferida para usarla en sesiones remotas.

Seleccionar un micrófono predeterminado en un sistema cliente Linux

Si dispone de varios micrófonos en su sistema cliente, solo se utilizará uno de ellos en el escritorio remoto. Para especificar el micrófono predeterminado, puede usar el control de sonidos en el sistema cliente.

Con la función Audio/vídeo en tiempo real, los dispositivos de entrada y salida de audio funcionan sin que sea necesario utilizar el redireccionamiento USB, lo que reduce considerablemente la cantidad de ancho de banda necesaria. También se admiten los dispositivos de entrada de audio analógico.

Este procedimiento describe cómo elegir un micrófono predeterminado desde la interfaz de usuario del sistema cliente. Los administradores también pueden configurar un micrófono preferido al editar el archivo de configuración. Consulte [Seleccionar una cámara web o un micrófono preferidos en un sistema cliente Linux](#).

Requisitos previos

- Compruebe que tiene instalado y operativo un micrófono USB o cualquier otro tipo de micrófono en el sistema cliente.
- Compruebe que usa los protocolos de visualización VMware Blast o PCoIP en el escritorio remoto.

Procedimiento

- 1 En la interfaz gráfica de usuario de Ubuntu, seleccione **Sistema > Preferencias > Sonido**.
También puede hacer clic en el icono **Sonido** situado en la parte derecha de la barra de herramientas en la parte superior de la pantalla.
- 2 Haga clic en la pestaña **Entrada** del cuadro de diálogo Preferencias de sonido.
- 3 Seleccione el dispositivo preferido y haga clic en **Cerrar**.

Seleccionar una cámara web o un micrófono preferidos en un sistema cliente Linux

Con la función Audio/vídeo en tiempo real, si cuenta con varias cámaras web o micrófonos en el sistema cliente, solo se puede usar una cámara web y un micrófono en el escritorio remoto. Para especificar la cámara web y el micrófono preferidos, puede editar un archivo de configuración.

La cámara web o el micrófono preferidos se utilizan en el escritorio remoto si está disponible. Si no es así, se usa otra cámara web u otro micrófono.

Con la función Audio/vídeo en tiempo real, las cámara web y los dispositivos de entrada y salida de audio funcionan sin que sea necesario utilizar el redireccionamiento USB, lo que reduce considerablemente la cantidad de ancho de banda de red necesario. También se admiten los dispositivos de entrada de audio analógica.

Para establecer las propiedades en el archivo `/etc/vmware/config` y especificar un dispositivo preferido, debe determinar los valores de algunos campos. Puede buscar el archivo de registro de los valores de estos campos.

- Para las cámaras web, establezca la propiedad `rtav.srcWCamId` en el valor del campo `UserId` de la cámara web y la propiedad `rtav.srcWCamName` en el valor del campo `Name` de la cámara web.

La propiedad `rtav.srcWCamName` tiene mayor prioridad que la propiedad `rtav.srcWCamId`. Ambas propiedades deben especificar la misma cámara web. Si las propiedades especifican cámaras web diferentes, se usa la especificada por `rtav.srcWCamName`, si existe. Si no existe, se usa la cámara web especificada por `rtav.srcWCamId`. Si no se encuentra ninguna cámara, se usa la predeterminada.

- Para los dispositivos de audio, establezca la propiedad `rtav.srcAudioInId` en el valor del campo `device.description` de `PulseAudio`.

Requisitos previos

En función de que configure una cámara web preferida, un micrófono preferido o ambos, realice las tareas necesarias apropiadas:

- Compruebe que tiene instalada y operativa una cámara web USB en el sistema cliente.
- Compruebe que tiene instalado y operativo un micrófono USB o cualquier otro tipo de micrófono en el sistema cliente.
- Compruebe que usa los protocolos de visualización VMware Blast o PCoIP en el escritorio remoto.

Procedimiento

- 1 Inicie el cliente y, a continuación, la aplicación del micrófono o de la cámara web para realizar una enumeración de dispositivos de audio o de cámaras en el registro del cliente.
 - a Conecte el dispositivo de audio o la cámara web que desea usar.
 - b Use el comando `vmware-view` para iniciar Horizon Client.
 - c Inicie una llamada y luego deténgala.

Este proceso crea un archivo de registro.

2 Busque las entradas de registro del micrófono o la cámara web.

- a Abra el archivo de registro de depuración con un editor de texto.

El archivo de registro con mensajes de registro de audio y vídeo en tiempo real se encuentra en `/tmp/vmware-<username>/vmware-RTAV-<pid>.log`. El registro del cliente se encuentra en `/tmp/vmware-<username>/vmware-view-<pid>.log`.

- b Busque en el archivo de registro las entradas que se refieran a las cámaras web y los micrófonos conectados.

El siguiente ejemplo muestra un extracto de la selección de la cámara web:

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:0819)
UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.5
SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

El siguiente ejemplo muestra un extracto de la selección del dispositivo de audio y el nivel de audio actual para cada uno:

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of Microsoft
LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
```

Las advertencias se muestran si los niveles de audio de origen del dispositivo seleccionado no cumplen los criterios de PulseAudio, si el origen no está establecido al 100% (0 dB) o si el dispositivo de origen está silenciado, como aparece a continuación:

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0: 67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

- 3 Copie la descripción del dispositivo y úsela para configurar la propiedad apropiada en el archivo `/etc/vmware/config`.

En el caso de una cámara web, copie Microsoft® LifeCam HD-6000 for Notebooks y Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 para establecer que la cámara web de Microsoft sea la preferida y configure las propiedades como aparece a continuación:

```
rtav.srcWCamName = "Microsoft® LifeCam HD-6000 for Notebooks"
rtav.srcWCamId = "Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6"
```

Para este ejemplo, también puede configurar la propiedad `rtav.srcWCamId` como "Microsoft". La propiedad `rtav.srcWCamId` admite coincidencias exactas y parciales. La propiedad `rtav.srcWCamName` admite solo una coincidencia exacta.

En el caso de un dispositivo de audio, copie Logitech USB Headset Analog Mono para especificar los auriculares Logitech como el dispositivo de audio preferido y establecer las propiedades tal y como aparece a continuación:

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

- 4 Guarde los cambios y cierre el archivo de configuración `/etc/vmware/config`.
- 5 Cierre sesión del escritorio e inicie una nueva sesión.

Usar la función de redireccionamiento de contenido URL

Un administrador de Horizon puede configurar vínculos URL en los que hará clic dentro de una aplicación publicada o un escritorio remoto, de forma que se abran en el navegador predeterminado del sistema cliente local. El vínculo URL puede ser a una página web, un número de teléfono, una dirección de correo o cualquier otro tipo de vínculo. Esta función se denomina redireccionamiento de contenido URL.

Un administrador de Horizon también puede configurar vínculos URL en los que puede hacer clic dentro de un navegador o una aplicación del sistema cliente local para abrirlos en una aplicación publicada o un escritorio remoto. Si Horizon Client aún no está abierto, haga clic en el vínculo URL. Este se inicia y le solicita que inicie sesión.

Un administrador de Horizon puede configurar la función Redireccionamiento de contenido URL por motivos de seguridad. Por ejemplo, si se encuentra en su puesto de trabajo y hace clic en un vínculo que lleve a una URL fuera de la red empresarial, el vínculo se puede abrir de forma más segura en una aplicación publicada. Un administrador puede configurar las aplicaciones publicadas que abren el vínculo.

Usar Redireccionamiento de contenido URL con Firefox

La primera vez que se redireccione una URL desde el navegador Firefox del sistema cliente, se le solicitará que abra la URL en Horizon Client. Si selecciona la casilla de verificación **Recordar mi selección para los enlaces vmware-view** y, a continuación, hace clic en **Abrir enlace**, esta solicitud no volverá a aparecer.

Compartir sesiones de escritorios remotos

La función Session Collaboration permite invitar a otros usuarios a que se unan a una sesión de escritorio remoto existente. Las sesiones de escritorio remoto que se comparten de esta forma se denominan sesiones colaborativas. El usuario que comparte una sesión con otro usuario se conoce como propietario de la sesión, mientras que el usuario que se une a una sesión compartida se denomina colaborador de la sesión.

Un administrador de Horizon debe habilitar la función Session Collaboration.

En escritorios Windows, esta tarea incluye habilitar la función Session Collaboration en el nivel de granja o de grupo de escritorios. También puede incluir el uso de directivas de grupo para configurar las funciones que se incluyen en Session Collaboration, como los métodos de invitación disponibles. Para conocer todos los requisitos, consulte [Requisitos de la función Session Collaboration](#).

Para obtener más información sobre cómo habilitar la función Session Collaboration en escritorios Windows, consulte el documento *Configurar escritorios virtuales en Horizon 7*. Para obtener más información sobre cómo habilitar la función Session Collaboration en una granja, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*. Si desea obtener más información sobre cómo usar las opciones de la directiva de grupo para configurar la función Session Collaboration, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Para obtener más información sobre cómo habilitar la función Session Collaboration en escritorios Linux, consulte el documento *Configurar escritorios de Horizon 7 for Linux*.

Invitar a un usuario a que se una a una sesión de escritorio remoto

La función Session Collaboration le permite invitar a otros usuarios a que se unan a una sesión de escritorio remoto enviándoles invitaciones de colaboración por correo electrónico, en un mensaje instantáneo (solo escritorios remotos Windows) o copiando el vínculo en el portapapeles y reenviándoselo a los usuarios.

Solo puede invitar a usuarios que pertenezcan a un dominio que el servidor admita para la autenticación. De forma predeterminada, puede invitar hasta cinco usuarios. Un administrador de Horizon puede cambiar el número máximo de usuarios a los que puede invitar.


La función Session Collaboration tiene las siguientes limitaciones.

- Si tiene varios monitores, los colaboradores de sesión solo ven el monitor principal.
- Debe seleccionar el protocolo de visualización VMware Blast cuando cree una sesión de escritorio remoto para compartirla. La función Session Collaboration no admite sesiones RDP ni PCoIP.
- No se admite la codificación H.264 de hardware. Si el propietario de la sesión usa la codificación de hardware y un colaborador se une a la sesión, ambos recurrirán a la codificación de software.
- No se admite la colaboración anónima. Los colaboradores de la sesión se deben identificar mediante mecanismos de autenticación que Horizon admita.
- Los colaboradores de sesión deben tener instalado Horizon Client 4.7 para Windows, Mac o Linux, o bien usar la versión 4.7 de HTML Access o una posterior.
- Si un colaborador de sesión tiene una versión no admitida de Horizon Client, aparece un mensaje de error cuando el usuario hace clic en un vínculo de colaboración.
- No puede usar la función Session Collaboration para compartir sesiones de aplicaciones publicadas.

Requisitos previos

- La función Session Collaboration debe estar habilitada y configurada.
- Para usar el método de invitación por correo electrónico, debe estar instalada una aplicación de correo electrónico.
- Para usar el método de invitación por IM en un escritorio remoto Windows, Skype Empresarial debe estar instalado y configurado.

Procedimiento

- 1 Debe conectarse a un escritorio remoto que tenga habilitada la función Session Collaboration. Debe utilizar el protocolo de visualización VMware Blast.
- 2 En la bandeja del sistema del escritorio remoto, haga clic en el icono **Colaboración de VMware Horizon**, por ejemplo, .

El icono de colaboración es diferente según la versión del sistema operativo.

- 3 Cuando se abra el cuadro de diálogo Colaboración de VMware Horizon, escriba el nombre de usuario (por ejemplo, **testuser** o **domain\testuser**), o bien la dirección de correo electrónico del usuario que quiere que se una a la sesión de escritorio remoto.

La primera vez que escriba el nombre de usuario o la dirección de correo electrónico de un usuario en concreto, debe hacer clic en **Buscar "usuario"**, escribir una coma (,) o pulsar la tecla **Entrar** para validar al usuario. En escritorios remotos Windows, la función Session Collaboration recuerda al usuario la próxima vez que escriba el nombre o la dirección de correo electrónico del usuario.

- 4 Seleccione un método de invitación.

Es posible que no todos los métodos de invitación estén disponibles.

Opción	Acción
Correo electrónico	Copia la invitación de colaboración al portapapeles y abre un nuevo mensaje de correo electrónico en la aplicación de correo electrónico predeterminada. Para usar este método de invitación, debe estar instalada una aplicación de correo electrónico.
IM	(Solo para escritorios remotos Windows) Copia la invitación de colaboración al portapapeles y abre una nueva ventana en Skype Empresarial. Pulse Ctrl +V para pegar el vínculo en la ventana de Skype Empresarial. Skype Empresarial debe estar instalado y configurado para usar este método de invitación.
Copiar vínculo	Copia la invitación de colaboración en el portapapeles. De forma manual, debe abrir otra aplicación, como Bloc de notas, y pulsar Ctrl+V para pegar la invitación.

Resultados

Después de enviar una invitación, el icono Colaboración de VMware Horizon también aparece en el escritorio y la interfaz de usuario de Session Collaboration pasa a ser un panel de control que muestra el estado actual de la sesión de colaboración, y le permite realizar ciertas acciones.

Cuando un colaborador de sesión acepta la invitación para unirse a la sesión del escritorio remoto Windows, recibirá una notificación de la función Session Collaboration y aparecerá un punto rojo en el icono Colaboración de VMware Horizon de la bandeja del sistema. Cuando un colaborador acepte la invitación para unirse a una sesión de escritorio remoto de Linux, aparecerá una notificación en el escritorio de la sesión principal.

Pasos siguientes

Administre la sesión de escritorio remoto en el cuadro de diálogo Colaboración de VMware Horizon. Consulte [Administrar una sesión de escritorio remoto compartida](#).

Administrar una sesión de escritorio remoto compartida

Después de enviar una invitación para colaborar en una sesión, la interfaz de usuario de Session Collaboration pasa a ser un panel de control que muestra el estado actual de la sesión de escritorio remoto compartida (sesión colaborativa), y le permite realizar ciertas acciones.

Un administrador de Horizon puede evitar que se transfiera el control a un colaborador de la sesión. En los escritorios remotos Windows, consulte la configuración de directiva de grupo **Permitir que el control se transfiera a los colaboradores** en el documento *Configurar funciones de escritorios remotos en Horizon 7*. En escritorios remotos Linux, consulte el parámetro `collaboration.enableControlPassing` en el documento *Configurar escritorios de Horizon 7 for Linux*.

Requisitos previos

Inicie una sesión de colaboración. Consulte [Invitar a un usuario a que se una a una sesión de escritorio remoto](#).

Procedimiento

- 1 En el escritorio remoto, haga clic en el icono **Colaboración de VMware Horizon** de la bandeja del sistema.

Los nombres de todos los colaboradores de la sesión aparecen en la columna Nombre y sus estados aparecen en la columna Estado.

- 2 Utilice el panel de control VMware Horizon Session Collaboration para administrar la sesión colaborativa.

Opción	Acción
Revocar una invitación o eliminar un colaborador	Haga clic en Eliminar en la columna Estado.
Transferir el control a un colaborador de la sesión	Después de que el colaborador de la sesión se una, cambie el conmutador de la columna Control a Activado . Para reanudar el control de la sesión, haga doble clic o pulse cualquier tecla. El colaborador de la sesión también puede devolver el control. Para ello deberá cambiar el conmutador de la columna Control a Desactivado o hará clic en el botón Devolver el control .
Agregar colaborador	Haga clic en Agregar colaboradores .
Cerrar la sesión colaborativa	Haga clic en Finalizar la colaboración . Se desconectan todas las colaboraciones activas. En escritorios remotos Windows, también puede finalizar la sesión colaborativa si hace clic en el botón Detener que aparece junto al icono VMware Horizon Session Collaboration . El botón Detener no está disponible en escritorios remotos Linux.

Unirse a una sesión de escritorio remoto

Para unirse a una sesión de escritorio remoto mediante la función Session Collaboration, puede hacer clic en el vínculo de la invitación de colaboración. El vínculo puede estar en un correo electrónico o un mensaje instantáneo, o bien en un documento que el propietario de la sesión le envíe. Además, puede iniciar sesión en el servidor y hacer doble clic en el icono de la sesión situado en la ventana para seleccionar la aplicación y el escritorio remoto.

Este procedimiento describe cómo unirse a una sesión de escritorio remoto desde una invitación de colaboración.

Nota En un entorno arquitectura Cloud Pod, no puede unirse a una sesión colaborativa iniciando sesión en el servidor, a menos que inicie sesión en el pod del propietario de la sesión.

Si se une a una sesión de escritorio remoto con la función Session Collaboration, no podrá utilizar las siguientes funciones en la sesión de escritorio remoto.

- Redireccionamiento USB
- Audio/vídeo en tiempo real (RTAV)
- Redireccionamiento multimedia
- Redireccionamiento de unidades cliente
- Redireccionamiento de tarjetas inteligentes
- Impresión virtual
- Redireccionamiento del portapapeles

Tampoco podrá cambiar la resolución del escritorio remoto en la sesión de escritorio remoto.

Requisitos previos

Para unirse a una sesión de escritorio remoto con la función Session Collaboration, debe tener Horizon Client 4.7 para Windows, Mac o Linux instalado en el sistema cliente, o bien debe usar HTML Access 4.7 o una versión posterior.

Procedimiento

- 1 Haga clic en el vínculo de la invitación de colaboración.
Horizon Client se abre en el sistema cliente.
- 2 Introduzca sus credenciales para iniciar sesión en Horizon Client.
Después de autenticarse correctamente, comienza la sesión colaborativa y puede ver el escritorio remoto del propietario de la sesión. Si el propietario de la sesión le transfiere el control del teclado y del mouse, puede usar el escritorio remoto.
- 3 Para devolver el control del teclado y del mouse al propietario de la sesión, haga clic en el icono **Colaboración de VMware Horizon** de la bandeja del sistema y cambie el conmutador de la columna Control a **Desactivado**, o haga clic en el botón **Devolver el control**.
- 4 Para salir de la sesión de colaboración, haga clic en **Opciones > Desconectar**.

Usar varias sesiones de una aplicación publicada desde dispositivos cliente diferentes

Cuando se habilita el modo de sesión múltiple para una aplicación publicada, puede utilizar varias sesiones de la misma aplicación al iniciar sesión en el servidor desde diferentes dispositivos cliente.

Por ejemplo, si abre una aplicación publicada en modo de sesión múltiple en el cliente A y abre la misma aplicación publicada en el cliente B, la aplicación publicada sigue abierta en el cliente A y se abre una nueva sesión de la aplicación publicada en el cliente B. Por el contrario, cuando el modo de sesión múltiple está deshabilitado (modo de sesión única), la sesión de la aplicación publicada en el cliente A se desconecta y se vuelve a conectar en el cliente B.

La función del modo de sesión múltiple tiene las siguientes limitaciones.

- El modo de sesión múltiple no funciona para aplicaciones que no admiten varias instancias, como Skype Empresarial.
- Si la sesión de aplicación se desconecta mientras utiliza una aplicación publicada en modo de sesión múltiple, se cierra la sesión automáticamente y se pierden los datos que no se guardaron.

Requisitos previos

Un administrador de Horizon debe habilitar el modo de sesión múltiple en el grupo de aplicaciones. Los usuarios no pueden modificar el modo de sesión múltiple para una aplicación publicada, a menos que el administrador de Horizon lo permita. Consulte *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para usar esta función se necesita Horizon 7 7.7 o versiones posteriores.

Procedimiento

- 1 Conéctese a un servidor.
- 2 Haga clic en el botón **Configuración** (rueda dentada) situado en la esquina superior derecha de la ventana para seleccionar la aplicación y el escritorio, y seleccione **Inicio múltiple**.

Si ninguna aplicación publicada se puede usar en modo de sesión múltiple, la opción **Inicio múltiple** no aparece.
- 3 Seleccione las aplicaciones publicadas que quiere usar en modo de sesión múltiple y haga clic en **Aceptar**.

Si un administrador de Horizon aplicó el modo de sesión múltiple para una aplicación publicada, no puede cambiar esta opción.

Usar la función de aplicación remota

Con la función de aplicación remota, puede interactuar con una aplicación que se ejecuta en un escritorio remoto como si fuera una aplicación que se ejecuta localmente.

A partir de Horizon Client 4.9 para Linux, la función de aplicación remota se habilita de forma predeterminada y está disponible para todos los sistemas Linux.

Guardar documentos en una aplicación publicada

Con determinadas aplicaciones publicadas, como Microsoft Word o WordPad, puede crear y guardar documentos. La ubicación en la que se guardan estos documentos depende del entorno de red de su empresa. Por ejemplo, los documentos se pueden guardar en un recurso compartido principal en su equipo local.

Un administrador de Horizon puede usar la opción de directiva de grupo de perfiles RDS llamada **Establecer directorio principal de usuario de Servicios de Escritorio remoto** para especificar la ubicación en la que se guardan los documentos. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Imprimir desde un escritorio remoto

Puede imprimir desde un escritorio remoto a través de una impresora virtual o una impresora USB que estén conectadas al equipo cliente local.

Puede utilizar la función Impresión virtual o VMware Integrated Printing, dependiendo de la función que esté habilitada en Horizon Agent.

Para obtener más información sobre los tipos de escritorios remotos que admiten las funciones Impresión virtual y VMware Integrated Printing, consulte [Matriz de compatibilidad de funciones para clientes Linux](#).

Establecer las preferencias de impresión para la función de impresión virtual

Puede establecer las preferencias de impresión en un escritorio remoto para la función Impresión virtual. Con la función Impresión virtual, puede usar impresoras de red o conectadas de forma local desde un escritorio remoto sin tener que instalar controladores de impresora adicionales en el escritorio remoto. En cada impresora disponible en esta función, puede configurar las

preferencias relativas a la compresión de datos, la calidad de la impresión, la impresión a doble cara, el color y otras opciones.

Importante La función Impresión virtual solo está disponible en Horizon Client 3.2 o versiones posteriores disponibles, que está disponible en la página web de descargas de productos de VMware, o bien con la versión de Horizon Client para Linux proporcionada por otros proveedores.

Esta función requiere los protocolos de visualización VMware Blast o PCoIP.

Para obtener más información sobre los partners del cliente delgado o un cliente Zero, consulte la *Guía de compatibilidad de VMware* en <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm>. Para el software cliente proporcionado por otros proveedores, debe utilizar el protocolo de visualización de VMware Blast, PCoIP o FreeRDP. Esta función no es compatible con rdesktop.

Después de agregar una impresora al equipo local, Horizon Client agrega dicha impresora a la lista de impresoras disponibles en el escritorio remoto. No necesita realizar ningún tipo de configuración. Si tiene privilegios de administrador, puede instalar controladores de impresión en el escritorio remoto sin crear un conflicto con el componente Impresora virtual.

Importante Esta función no está disponible para los siguientes tipos de impresoras.

- Impresoras USB que utilizan la función de redireccionamiento USB para conectarse a un puerto USB virtual en el escritorio remoto.

Debe desconectar la impresora USB del escritorio remoto para utilizar la función Impresión virtual en él.

- La función de Windows para imprimir a un archivo.

La función para seleccionar la casilla **Imprimir a un archivo** en el cuadro de diálogo Imprimir no funciona, pero sí se puede utilizar un controlador de impresión que cree un archivo. Por ejemplo, puede utilizar un escritor de PDF para imprimir un archivo PDF.

Requisitos previos

Para usar Impresión virtual, un administrador de Horizon debe habilitar dicha función en el escritorio remoto. Esta tarea incluye habilitar la opción de configuración **Impresión virtual** en el instalador del agente y puede incluir el establecimiento de directivas que controlan el comportamiento de la función Impresión virtual. Para obtener información sobre cómo instalar Horizon Agent, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para obtener más información sobre cómo configurar directivas, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Para determinar si la función Impresión virtual está instalada en un escritorio remoto, verifique que exista la carpeta C:\Program Files\Common Files\ThinPrint en el sistema de archivos del escritorio remoto.

Procedimiento

- 1 En el escritorio remoto Windows, acceda a **Panel de control > Hardware y sonido > Dispositivos e impresoras**.
- 2 En la ventana **Dispositivos e impresoras** haga clic con el botón secundario en la impresora virtual y seleccione **Propiedades de impresora** en el menú contextual.

En un escritorio de máquina virtual de un solo usuario, cada impresora virtual aparece como `<nombre_impresora>`. En un escritorio publicado, cada impresora virtual aparece como `<nombre_impresora>(s<ID_sesión>)`.

- 3 En la pestaña **General**, haga clic en **Preferencias**.
- 4 En el cuadro de diálogo Preferencias de impresión, seleccione las diferentes pestañas y especifique qué configuración utilizar.
- 5 Para guardar los cambios, haga clic en **Aceptar**.

Establecer las preferencias de impresión para la función VMware Integrated Printing

Puede establecer las preferencias de impresión en un escritorio remoto para la función VMware Integrated Printing. La función VMware Integrated Printing permite usar impresoras locales o de red desde un escritorio remoto sin tener que instalar controladores de impresora adicionales en el escritorio remoto Windows. En cada impresora disponible en esta función, puede configurar las preferencias relativas a la compresión de datos, la calidad de la impresión, la impresión a doble cara, el color y otras opciones.

A partir de Horizon Agent 7.12, puede usar la configuración de directiva de grupo **Nombre de la impresora para los agentes RDSH** para configurar la convención de nomenclatura de las impresoras cliente que se redireccionan a una aplicación publicada o a un escritorio remoto. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Requisitos previos

Para usar la función VMware Integrated Printing, un administrador de Horizon debe habilitarla en el escritorio remoto. Esta tarea implica habilitar la opción **VMware Integrated Printing** en el instalador de Horizon Agent y configurar las directivas que controlen el comportamiento de la impresión virtual. Para obtener información sobre cómo instalar Horizon Agent, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para obtener más información sobre cómo configurar directivas, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Para determinar si la función VMware Integrated Printing está instalada en un escritorio remoto, compruebe que los archivos `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` y `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` se encuentren ubicados en el sistema de archivos del escritorio remoto.

Esta función requiere la versión 7.9 de Horizon Agent o una versión posterior.

Procedimiento

- 1 En el escritorio remoto Windows, acceda a **Panel de control > Hardware y sonido > Dispositivos e impresoras**.
- 2 En la ventana **Dispositivos e impresoras** haga clic con el botón secundario en la impresora virtual y seleccione **Propiedades de impresora** en el menú contextual.

En un escritorio de máquina virtual de un solo usuario, cada impresora virtual aparece como *<nombre_impresora>(vdi)*. De forma predeterminada, en un escritorio publicado o aplicación publicada, cada impresora virtual aparece como *<nombre_impresora> (v<ID_sesión>)*.

- 3 En la pestaña **General**, haga clic en **Preferencias**.
- 4 En el cuadro de diálogo Preferencias de impresión, seleccione las diferentes pestañas y especifique qué configuración utilizar.
- 5 Para guardar los cambios, haga clic en **Aceptar**.

Imprimir desde un escritorio remoto a una impresora USB local

Una impresora USB es una impresora que está conectada a un puerto USB en el sistema cliente local. Puede enviar trabajos de impresión a una impresora USB conectada al sistema cliente local desde un escritorio remoto.

Para imprimir en una impresora USB desde un escritorio remoto, puede usar las funciones Redireccionamiento USB, Impresión virtual o VMware Integrated Printing. Las impresoras USB redireccionadas y las impresoras virtuales pueden funcionar juntas sin que se produzca ningún conflicto.

Usar la función Redireccionamiento USB

Para poder usar la función Redireccionamiento USB para conectar una impresora USB a un puerto USB virtual en un escritorio remoto, los controladores de impresora necesarios deben estar instalados en el escritorio remoto y en el sistema cliente.

Si utiliza esta función Redireccionamiento USB para redirigir una impresora USB, esta ya no estará conectada de forma lógica al puerto USB físico del sistema cliente local y no aparecerá en la lista de impresoras locales del sistema cliente local. Podrá imprimir con la impresora USB desde el escritorio remoto, pero ya no podrá imprimir en la impresora USB desde el sistema cliente local.

En un escritorio remoto, las impresoras USB redirigidas aparecen como *<printer_name>*.

Si desea obtener más información, consulte [Uso del redireccionamiento USB para conectar dispositivos USB](#).

Usar la función Impresión virtual o la función VMware Integrated Printing

Si utiliza la función Impresión virtual o la función VMware Integrated Printing para enviar tareas de impresión a una impresora USB, podrá imprimir en la impresora USB desde el escritorio remoto y el sistema cliente local, y no será necesario instalar controladores de impresora en el escritorio remoto.

Para usar la función Impresión virtual o la función VMware Integrated Printing, la función deberá estar habilitada al instalar Horizon Agent. Para obtener información sobre la instalación, consulte los documentos *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Para obtener más información, consulte [Establecer las preferencias de impresión para la función de impresión virtual](#) o [Establecer las preferencias de impresión para la función VMware Integrated Printing](#).

Copiar y pegar texto

Puede copiar texto del escritorio remoto y las aplicaciones publicadas y pegarlo en ellos. Un administrador de Horizon puede configurar esta función para que sea posible realizar estas operaciones del sistema cliente a una aplicación publicada o un escritorio remoto, de una aplicación publicada o un escritorio remoto al sistema cliente, ambas posibilidades o ninguna.

Copiar y pegar entre el sistema cliente (donde está instalado Horizon Client) y un escritorio remoto o aplicación publicada (y viceversa) es igual que copiar y pegar entre aplicaciones del mismo sistema. Por ejemplo, puede pulsar Ctrl+C para copiar texto y Ctrl+V para pegarlo.

Esta función está disponible si utiliza los protocolos de visualización VMware Blast o PCoIP.

Un administrador de Horizon puede configurar la capacidad de copiar y pegar mediante la configuración de directiva de grupo que pertenece a Horizon Agent para las aplicaciones publicadas y los escritorios remotos. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Puede copiar texto de Horizon Client y pegarlo en una aplicación publicada o un escritorio remoto (o viceversa), pero el texto se pegará como texto sin formato.

No puede copiar y pegar gráficos. Tampoco puede copiar y pegar archivos entre un escritorio remoto y el sistema de archivos de su equipo cliente.

Configurar el tamaño de la memoria del portapapeles cliente

En la versión 7.0.1 y versiones posteriores de Horizon 7, así como en Horizon Client 4.1 y versiones posteriores, el tamaño de la memoria del portapapeles se puede configurar tanto para el servidor como para el cliente.

Cuando se establece una sesión de PCoIP o VMware Blast, el servidor envía el tamaño de memoria de su portapapeles al cliente. El tamaño de memoria efectivo del portapapeles es el menor de los valores de tamaño de memoria del portapapeles del servidor y del cliente.

Para establecer el tamaño de la memoria del portapapeles cliente, agregue los siguientes parámetros en cualquiera de los tres archivos de configuración: `~/.vmware/config`, `/usr/lib/vmware/config` o `/etc/vmware/config`.

```
mksvchan.clipboardSize=valor
```

value es el tamaño de la memoria del portapapeles cliente en kilobytes (KB). Puede especificar un valor máximo de 16384 KB. Si especifica 0 o no especifica ningún valor, el tamaño de la memoria del portapapeles cliente es 8192 KB (8 MB).

Horizon Client busca el tamaño de la memoria del portapapeles en los archivos de configuración siguiendo este orden y se detiene cuando encuentra un valor que no sea cero.

- 1 `/usr/lib/vmware/config`
- 2 `/etc/vmware/config`
- 3 `~/.vmware/config`

En función de la red, si el tamaño de la memoria del portapapeles es muy grande, el rendimiento puede verse afectado de forma negativa. VMware le recomienda que no asigne al tamaño de memoria del portapapeles un valor superior a 16 MB.

Registrar la actividad de copiar y pegar

Cuando habilite la función de auditoría del portapapeles, Horizon Agent registra información sobre la actividad de copiado y pegado en un registro de eventos de la máquina agente. Esta función de auditoría del portapapeles está deshabilitada de forma predeterminada.

Para habilitar la función de auditoría del portapapeles, debe habilitar la opción de directiva de grupo **Configurar auditoría del portapapeles** para VMware Blast o PCoIP.

De forma opcional, puede configurar la directiva de grupo **Si se bloquea el redireccionamiento del portapapeles al cliente cuando el cliente no admite auditoría** para VMware Blast y PCoIP, y especificar si desea bloquear el redireccionamiento del portapapeles a los clientes que no admitan la función de auditoría del portapapeles.

Para obtener más información sobre cómo configurar estas opciones de directiva de grupo, consulte los temas "Configuración de la directiva VMware Blast" y "Configuración del portapapeles de PCoIP" del documento *Configurar funciones de escritorios remotos en Horizon 7*.

Esta función requiere que Horizon Agent 7.7 o una versión posterior esté instalado en la máquina agente.

El registro de eventos donde se registra la información sobre la actividad de copiado y pegado se denomina VMware Horizon RX Audit. Para ver el registro de eventos en la máquina agente, use el visor de eventos de Windows. Para consultar el registro de eventos en una ubicación centralizada, configure VMware Log Insight o Recopilador de eventos de Windows. Para obtener más información acerca de Log Insight, acceda a <https://docs.vmware.com/es/vRealize-Log-Insight/index.html>. Para obtener información sobre el Recopilador de eventos de Windows, consulte la documentación de Microsoft.

Configurar el redireccionamiento USB en el cliente

6

Con la función del redireccionamiento USB, puede usar un archivo de configuración en el sistema cliente para especificar los dispositivos USB que se pueden redireccionar al escritorio remoto.

Por ejemplo, puede restringir los tipos de dispositivos USB en los que Horizon Client permite el redireccionamiento, hacer que evite que ciertos dispositivos USB se envíen desde un equipo cliente y especificar si Horizon Client debe dividir los dispositivos USB compuestos en componentes independientes para su redireccionamiento.

Este capítulo incluye los siguientes temas:

- [Requisitos del sistema para la función de redireccionamiento USB](#)
- [Archivos de registro específicos de dispositivos USB](#)
- [Establecer las propiedades de configuración USB](#)
- [Familias de dispositivos USB](#)

Requisitos del sistema para la función de redireccionamiento USB

Para poder usar el redireccionamiento USB, el sistema debe cumplir ciertos requisitos.

Para obtener más información sobre los partners del cliente ligero o del cliente cero, consulte la [Guía de compatibilidad de VMware](#). Para utilizar los componentes USB disponibles para los proveedores de terceros, se deben instalar algunos archivos en ciertas ubicaciones, así como se deben configurar algunos procesos para que se inicien antes de que lo haga Horizon Client. La información de este documento no recoge estos detalles.

Para usar la función de redireccionamiento USB en Horizon Client se requiere el protocolo de visualización VMware Blast o PCoIP.

Archivos de registro específicos de dispositivos USB

Horizon Client envía información de dispositivos USB a archivos de registro.

Para especificar el nivel de registro USB, agregue el siguiente parámetro en uno de los archivos de configuración.

```
view-usbd.logLevel = "value"
```

Use uno de los siguientes valores para *valor*.

- **trace**
- **info**
- **debug**
- **error**

Los archivos de configuración se encuentran en las siguientes ubicaciones y se procesan siguiendo el orden que aparece a continuación:

- 1 /usr/lib/vmware/config
- 2 /etc/vmware/config
- 3 ~/.vmware/config

Para solucionar problemas, puede aumentar la cantidad de información que se envía a registros específicos de dispositivos USB con los siguientes comandos:

- 1 Detenga el demonio del árbitro USB.

```
# sudo /etc/init.d/vmware-USBArbitrator stop
```

- 2 Reinicie el demonio del árbitro USB usando la opción verbose.

```
# sudo /usr/lib/vmware/view/usb/vmware-usbarbitrator -verbose
```

El archivo de registro predeterminado del árbitro USB se encuentra en /var/log/vmware/vmware-usbarb-*<pid>*.log, donde *<pid>* es el ID de proceso del demonio del árbitro USB.

Para obtener una lista de información de uso, utilice el comando siguiente:

```
# sudo /usr/lib/vmware/view/usb/vmware-usbarbitrator -h
```

Establecer las propiedades de configuración USB

Si lo desea, puede establecer las propiedades de configuración USB en los archivos de configuración/etc/vmware/config, /usr/lib/vmware/config y ~/.vmware/config.

Use la siguiente sintaxis para establecer las propiedades de configuración USB en los archivos de configuración.

```
viewusb.property1 = "value1"
```

Con las propiedades de configuración USB, puede controlar si se redireccionan ciertos tipos de dispositivos. El filtro de propiedades está disponible para permitirle incluir o excluir ciertos tipos de dispositivos. En el caso de clientes Linux 1.7 y versiones posteriores y para los clientes Windows, también se proporcionan las propiedades para dividir los dispositivos compuestos.

Algunos valores de propiedades requieren el VID (ID del proveedor) y el PID (ID del producto) de un dispositivo USB. Para encontrar el VID y el PID, puede realizar una búsqueda en Internet con el nombre del producto combinado con vid y pid. Además, puede consultar el archivo `/tmp/vmware-<usuario_actual>/vmware-view-usbd-*.log` después de conectar dicho dispositivo USB al sistema local mientras Horizon Client se está ejecutando. Para establecer la ubicación de este archivo, use la propiedad `view-usbd.log.fileName` del archivo `/etc/vmware/config`, por ejemplo:

```
view-usbd.log.fileName = "/tmp/usbd.log"
```

Importante Al redireccionar dispositivos de audio, asegúrese de que la versión de kernel del sistema Ubuntu es 3.2.0-27.43 o una versión posterior. Si no puede actualizar a esta versión del kernel, de forma alternativa, puede deshabilitar el acceso del host al dispositivo de audio. Por ejemplo, puede agregar la línea `"blacklist snd-usb-audio"` al final del archivo `/etc/modprobe.d/blacklist.conf`. Si el sistema no cumple estos requisitos, el sistema cliente puede bloquearse cuando Horizon Client intenta redireccionar el dispositivo de audio. De forma predeterminada, los dispositivos de audio se redireccionan.

La siguiente tabla describe las propiedades de configuración USB disponibles.

Tabla 6-1. Propiedades de configuración para el redireccionamiento USB

Propiedad y nombre de directiva	Descripción
Permitir la división automática del dispositivo Propiedad: <code>viewusb.AllowAutoDeviceSplitting</code>	Permite la división automática de dispositivos USB compuestos. El valor predeterminado no está definido, lo que equivale a false .
Excluir el dispositivo Vid/Pid de la división Propiedad: <code>viewusb.SplitExcludeVidPid</code>	Excluye de una posible división un dispositivo USB compuesto especificado mediante los ID de producto y proveedor. El formato de la configuración es <code>vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2]...</code> Debe especificar los números de ID en hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID. Por ejemplo: vid-0781_pid-55** El valor predeterminado no está definido.

Tabla 6-1. Propiedades de configuración para el redireccionamiento USB (continuación)

Propiedad y nombre de directiva	Descripción
Dividir un dispositivo Vid/Pid Propiedad: viewusb.SplitVidPid	<p>Trata los componentes de un dispositivo USB compuesto especificado por los ID del producto y del proveedor como dispositivos distintos. El formato de la configuración es</p> <pre>vid-xxxx_pid-yyyy([exintf:zz[;exintf:ww]])[:...]</pre> <p>Puede usar la palabra clave exintf para excluir componentes del redireccionamiento al especificar el número de interfaz. Debe especificar números ID de forma hexadecimal. Además, los números de interfaz en decimales deben incluir un cero a la izquierda. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Por ejemplo: vid-0781_pid-554c(exintf:01;exintf:02)</p> <hr/> <p>Nota Si el dispositivo compuesto incluye componentes que se excluyen automáticamente, como los dispositivos de mouse y teclado, View no incluirá automáticamente los componentes que no haya excluido explícitamente. Debe especificar una directiva de filtrado como Include Vid/Pid Device para incluir estos componentes.</p> <hr/> <p>El valor predeterminado no está definido.</p>
Permitir dispositivos de entrada de audio Propiedad: viewusb.AllowAudioIn	<p>Permite que se redireccionen los dispositivos de entrada de audio.</p> <p>El valor predeterminado no está definido, lo que es igual a false ya que la función Audio/vídeo en tiempo real se usa en los dispositivos de entrada y salida de audio y, de forma predeterminada, no se usa el redireccionamiento USB para dichos dispositivos.</p>
Permitir dispositivos de salida de audio Propiedad: viewusb.AllowAudioOut	<p>Permite que se redireccionen los dispositivos de salida de audio.</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>
Permitir HID Propiedad: viewusb.AllowHID	<p>Permite que se redireccionen otros dispositivos de entrada que no sean dispositivos de teclado o mouse.</p> <p>El valor predeterminado no está definido, lo que equivale a true.</p>
Permitir HIDBootable Propiedad: viewusb.AllowHIDBootable	<p>Permite que se redireccionen otros dispositivos de entrada que no sean dispositivos de teclado o mouse y que estén disponibles en el momento del arranque (también denominados dispositivos con arranque HID).</p> <p>El valor predeterminado no está definido, lo que equivale a true.</p>
Permitir el descriptor del dispositivo Failsafe Propiedad: viewusb.AllowDevDescFailsafe	<p>Permite el redireccionamiento de los dispositivos aunque se produzca un error en Horizon Client para obtener los descriptores del dispositivo y la configuración.</p> <p>Para permitir un dispositivo aunque se produzca un error en la configuración o la descripción, es necesario que aparezca en los filtros de incluidos como IncludeVidPid o IncludePath.</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>
Permitir los dispositivos de teclado y mouse Propiedad: viewusb.AllowKeyboardMouse	<p>Permite que se redireccionen teclados con dispositivos señaladores integrados (como un mouse, bola de seguimiento o panel táctil).</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>

Tabla 6-1. Propiedades de configuración para el redireccionamiento USB (continuación)

Propiedad y nombre de directiva	Descripción
<p>Permitir tarjetas inteligentes</p> <p>Propiedad: viewusb.AllowSmartcard</p>	<p>Permite que se redireccionen los dispositivos de tarjeta inteligente.</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>
<p>Permitir dispositivos de vídeo</p> <p>Propiedad: viewusb.AllowVideo</p>	<p>Permite que se redireccionen los dispositivos de vídeo.</p> <p>El valor predeterminado no está definido, lo que es igual a false ya que la función Audio/vídeo en tiempo real se usa en los dispositivos de entrada y salida de audio y, de forma predeterminada, no se usa el redireccionamiento USB para dichos dispositivos.</p>
<p>Deshabilitar la descarga de la configuración remota</p> <p>Propiedad: viewusb.DisableRemoteConfig</p>	<p>Deshabilita el uso de la configuración Horizon Agent al realizar el filtrado de dispositivos USB.</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>
<p>Excluir todos los dispositivos</p> <p>Propiedad: viewusb.ExcludeAllDevices</p>	<p>Excluye el redireccionamiento de todos los dispositivos USB. Si está configurado como true, puede usar otras opciones de directivas para permitir el redireccionamiento de dispositivos o familias de dispositivos específicas. Si está configurado como false, puede usar otras opciones de directivas para evitar el redireccionamiento de dispositivos o familias de dispositivos específicas.</p> <p>Si establece el valor Exclude All Devices en true en Horizon Agent y esta configuración se envía a Horizon Client, la configuración de Horizon Agent reemplazará la de Horizon Client.</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>
<p>Excluir familia de dispositivos</p> <p>Propiedad: viewusb.ExcludeFamily</p>	<p>Excluye el redireccionamiento de familias de dispositivos. El formato de la configuración es <i>family_name_1[;family_name_2]</i>...</p> <p>Por ejemplo: bluetooth;smart-card</p> <p>Si habilitó la división automática de dispositivo, View examinará la familia de dispositivos de cada interfaz de un dispositivo USB compuesto para decidir cuál debe excluir. Si deshabilitó la división automática del dispositivo, View examinará la familia del dispositivo de todo el dispositivo USB compuesto.</p> <p>El valor predeterminado no está definido.</p>
<p>Excluir un dispositivo Vid/Pid</p> <p>Propiedad: viewusb.ExcludeVidPid</p>	<p>Excluye el redireccionamiento de dispositivos con los ID de producto y de proveedor específicos. El formato de la configuración es <i>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]</i>...</p> <p>Debe especificar los números de ID en hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Por ejemplo: vid-0781_pid-****;vid-0561_pid-554c</p> <p>El valor predeterminado no está definido.</p>
<p>Excluir ruta</p> <p>Propiedad: viewusb.ExcludePath</p>	<p>Excluye el redireccionamiento de dispositivos en rutas de puerto o concentrador especificado. El formato de la configuración es <i>bus-x1[/y1]..._port-z1[;bus-x2[/y2]..._port-z2]</i>...</p> <p>Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta.</p> <p>Por ejemplo: bus-1/2/3_port-02;bus-1/1/4_port-ff</p> <p>El valor predeterminado no está definido.</p>

Tabla 6-1. Propiedades de configuración para el redireccionamiento USB (continuación)

Propiedad y nombre de directiva	Descripción
Incluir familia de dispositivos Propiedad: viewusb.IncludeFamily	Incluye familias de dispositivos que se pueden redireccionar. El formato de la configuración es <i>family_name_1[;family_name_2]...</i> Por ejemplo: storage El valor predeterminado no está definido.
Incluir ruta Propiedad: viewusb.IncludePath	Incluye dispositivos en rutas de puerto o concentrador que pueden redireccionarse. El formato de la configuración es <i>bus-x1[/y1]..._port-z1[;bus-x2[/y2]..._port-z2]...</i> Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta. Por ejemplo: bus-1/2_port-02;bus-1/7/1/4_port-0f El valor predeterminado no está definido.
Incluir un dispositivo Vid/Pid Propiedad: viewusb.IncludeVidPid	Incluye el redireccionamiento de dispositivos con los ID de producto y de proveedor específicos. El formato de la configuración es <i>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</i> Debe especificar los números de ID en hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID. Por ejemplo: vid-0561_pid-554c El valor predeterminado no está definido.

Ejemplos del redireccionamiento USB

A cada ejemplo le sigue una descripción del efecto en el redireccionamiento USB.

- Incluya la mayoría de dispositivos dentro de la familia de dispositivos del mouse.

```
viewusb.IncludeFamily = "mouse"
viewusb.ExcludeVidPid = "Vid-0461_Pid-0010;Vid-0461_Pid-4d20"
```

La primera propiedad en este ejemplo comunica a Horizon Client que permita que se realice un redireccionamiento de los dispositivos de mouse a un escritorio de View. La segunda propiedad reemplaza a la primera y comunica a Horizon Client que mantenga dos dispositivos de mouse específicos locales y que no los redireccione.

- Active la división de dispositivos automática, pero excluya un dispositivo determinado. En otro dispositivo determinado, mantenga uno de sus componentes locales y redireccione los otros componentes al escritorio remoto:

```
viewusb.AllowAutoDeviceSplitting = "True"
viewusb.SplitExcludeVidPid = "Vid-03f0_Pid-2a12"
viewusb.SplitVidPid = "Vid-0911_Pid-149a(exintf:03)"
viewusb.IncludeVidPid = "Vid-0911_Pid-149a"
```

Los dispositivos USB compuestos están formados por una combinación de dos o más dispositivos, como un dispositivo de entrada de vídeo y un dispositivo de almacenamiento. La primera propiedad de este ejemplo activa la división automática de los dispositivos compuestos. La segunda propiedad excluye la división del dispositivo USB compuesto especificado (Vid-03f0_Pid-2a12).

La tercera línea le comunica a Horizon Client que trate los componentes de otro dispositivo compuesto (Vid-0911_Pid-149a) como dispositivos independientes, pero excluye el redireccionamiento del componente cuyo número de interfaz es 03. Este componente se mantiene de forma local.

Debido a que este dispositivo compuesto incluye un componente que se suele excluir de forma predeterminada, como un mouse o un teclado, la cuarta línea es necesaria para que los otros componentes del dispositivo compuesto Vid-0911_Pid-149a se puedan redireccionar al escritorio de View.

Las tres primeras propiedades son propiedades de división. La última propiedad es una propiedad de filtrado. Las propiedades de filtrado se procesan antes que las propiedades de división.

Importante Las propiedades de la configuración del cliente deben combinarse con las directivas correspondientes establecidas para Horizon Agent en el escritorio remoto (o reemplazarlas). Para obtener más información sobre cómo funcionan las propiedades de división y filtrado USB en el cliente junto con las directivas USB de Horizon Agent, consulte los temas relacionados con el uso de las directivas para controlar el redireccionamiento USB en el documento *Administración de VMware Horizon Console*.

Familias de dispositivos USB

Puede especificar una familia de dispositivos USB cuando crea reglas de filtrado de dispositivos USB para Horizon Client, para View Agent o para Horizon Agent.

Nota Algunos dispositivos no pertenecen a ninguna familia de dispositivos.

Tabla 6-2. Familias de dispositivos USB

Nombre de la familia de dispositivos	Descripción
audio	Cualquier dispositivo de entrada o salida de audio.
audio-in	Dispositivos de entrada de audio como micrófonos.
audio-out	Dispositivos de salida de audio como auriculares y altavoces.
bluetooth	Dispositivos conectados por Bluetooth.
comm	Dispositivos de comunicaciones como, por ejemplo, módems y adaptadores de red por cable.
hid	Dispositivos de interfaz de usuario, sin contar con teclados y dispositivos de señalización.

Tabla 6-2. Familias de dispositivos USB (continuación)

Nombre de la familia de dispositivos	Descripción
hid-bootable	Dispositivos de interfaz de usuario, que están disponibles durante el inicio, sin contar con teclados y dispositivos de señalización.
imaging	Dispositivos de imagen, como escáneres.
keyboard	Dispositivo de teclado.
mouse	Dispositivo de señalización, como un mouse.
other	Familia no especificada.
pda	Asistentes digitales personales.
physical	Dispositivos Force Feedback, como joysticks Force Feedback.
printer	Dispositivos de impresión.
security	Dispositivos de seguridad, como lectores de huella digital.
smart-card	Dispositivos de tarjeta inteligente.
storage	Dispositivos de almacenamiento masivo, como unidades flash y unidades de disco duro externas.
unknown	Familia no conocida.
vendor	Dispositivos con funciones específicas del proveedor.
video	Dispositivos de entrada de vídeo.
wireless	Adaptadores de red inalámbricos.
wusb	Dispositivos USB inalámbricos.

Solucionar problemas relacionados con Horizon Client

7

Puede solucionar la mayoría de los problemas de Horizon Client reiniciando o restableciendo los escritorios remotos o las aplicaciones publicadas, o bien reinstalando Horizon Client.

Este capítulo incluye los siguientes temas:

- [Reiniciar un escritorio remoto](#)
- [Restablecer aplicaciones publicadas o escritorios remotos](#)
- [Desinstalar Horizon Client para Linux](#)
- [Recopilar información de registro de Horizon Client](#)
- [Problemas con la entrada de teclado](#)
- [Conexión a un servidor en el modo Workspace ONE](#)

Reiniciar un escritorio remoto

Si el sistema operativo del escritorio remoto deja de responder, es posible que tenga que reiniciar un escritorio remoto. Reiniciar un escritorio remoto es similar a usar el comando de reinicio del sistema operativo Windows. El sistema operativo del escritorio remoto le suele pedir que guarde los datos que no guardó antes de reiniciar.

Solo puede reiniciar un escritorio remoto si un administrador de Horizon habilitó la función de reinicio para dicho escritorio.

Para obtener información sobre cómo habilitar la función de reinicio de escritorio, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- ◆ Utilice el comando **Reiniciar**.

Opción	Acción
Restablecer un escritorio remoto desde el mismo escritorio	Seleccione Conexión > Reiniciar escritorio de la barra de menús.
Restablecer un escritorio remoto desde la ventana para seleccionar la aplicación y el escritorio	<p>Siga uno de los estos procedimientos:</p> <ul style="list-style-type: none"> ■ Haga clic con el botón secundario en el icono del escritorio remoto y seleccione Reiniciar escritorio. ■ Seleccione el icono del escritorio remoto y haga clic en Conexión > Reiniciar escritorio en la barra de menús.

Horizon Client le pide que confirme la acción de reinicio.

Resultados

Se reinicia el sistema operativo del escritorio remoto, Horizon Client se desconecta y cierra la sesión del escritorio remoto.

Pasos siguientes

Espere un periodo de tiempo apropiado para que se reinicie el sistema antes de intentar volver a conectarse al escritorio remoto.

Si no se soluciona el problema reiniciando el escritorio remoto, puede que tenga que restablecer el escritorio remoto. Consulte [Restablecer aplicaciones publicadas o escritorios remotos](#).

Restablecer aplicaciones publicadas o escritorios remotos

Puede que tenga que restablecer un escritorio remoto si el sistema operativo del escritorio deja de responder y no se soluciona el problema reiniciando el escritorio remoto.

La acción de restablecer un escritorio remoto es equivalente a pulsar el botón Restablecer en un equipo físico para forzar su restablecimiento. Los archivos que estén abiertos en el escritorio remoto se cerrarán sin guardarse.

Al restablecer las aplicaciones publicadas, saldrá de todas las aplicaciones abiertas.

Solo puede restablecer un escritorio remoto si un administrador de Horizon habilitó la función de restablecimiento para dicho escritorio.

Para obtener información sobre cómo habilitar la función de restablecimiento de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- ◆ Utilizar el comando **Restablecer**.

Opción	Acción
Restablecer un escritorio remoto desde el mismo escritorio	Seleccione Conexión > Restablecer en la barra de menú.
Restablecer un escritorio remoto desde la ventana para seleccionar la aplicación y el escritorio	<p>Siga uno de los estos procedimientos:</p> <ul style="list-style-type: none"> ■ Haga clic con el botón secundario en icono del escritorio remoto y seleccione Restablecer escritorio. ■ Seleccione el icono de escritorio remoto y, a continuación, seleccione Conexión > Restablecer en la barra de menús.
Restablecer aplicaciones publicadas desde la ventana para seleccionar la aplicación y el escritorio	<p>Siga uno de los estos procedimientos:</p> <ul style="list-style-type: none"> ■ Haga clic con el botón derecho en el icono de la aplicación publicada y seleccione Configuración. Haga clic en Restablecer y, a continuación, de nuevo en Restablecer para confirmar la operación. ■ Seleccione el icono de cualquier aplicación publicada y haga clic en el botón Configuración (icono de la rueda dentada) situado en la esquina superior derecha de la ventana. Haga clic en Restablecer y, a continuación, de nuevo en Restablecer para confirmar la operación.

También puede utilizar identificadores de recursos uniformes (URI) para restablecer una aplicación o un escritorio remotos. Consulte más información sobre la sintaxis y algunos ejemplos en [Utilizar URI para configurar Horizon Client](#).

Resultados

Cuando restablezca un escritorio remoto, el sistema operativo del escritorio remoto se reinicia y Horizon Client desconecta y cierra la sesión del escritorio remoto. Al restablecer aplicaciones publicadas, se cerrarán dichas aplicaciones.

Pasos siguientes

Espere un periodo de tiempo apropiado para reiniciar el sistema antes de intentar volver a conectarse al escritorio remoto o la aplicación publicada.

Desinstalar Horizon Client para Linux

En ocasiones, para solucionar los problemas relacionados con Horizon Client, debe desinstalar y volver a instalar la aplicación Horizon Client.

El método que use para desinstalar Horizon Client para Linux depende de la versión y el método que usó para instalar el software cliente.

Requisitos previos

Compruebe que cuenta con acceso raíz en el sistema cliente Linux.

Procedimiento

- ◆ Si cuenta con Horizon Client 3.1 o una versión anterior, o si instaló el cliente desde Ubuntu Software Center, seleccione **Aplicaciones > Ubuntu Software Center** y, en la sección **Software instalado**, seleccione **vmware-view-client** y haga clic en **Eliminar**.
- ◆ Si cuenta con Horizon Client 3.2 o una versión posterior instalada desde el sitio web de descargas de productos de VMware, abra una ventana de terminal, cambie los directorios al que contiene el archivo instalador y ejecute el comando instalador con la opción `-u`.

```
sudo env VMWARE_KEEP_CONFIG=yes \
./VMware-Horizon-Client-x.x.x-yyyyyy.arch.bundle -u vmware-horizon-client
```

En el nombre del archivo, `x.x.x` es el número de la versión, `yyyyyy` es el número de compilación y `arch` es `x86`, o bien `x64`. Si usa la opción `VMWARE_KEEP_CONFIG=yes`, se mantendrán las opciones de configuración cuando el cliente se desinstale. Si esta variable del entorno no está configurada, se le solicitará que especifique si desea guardar las opciones de configuración.

Pasos siguientes

Puede volver a instalar el cliente o instalar una versión nueva. Consulte [Instalar o actualizar Horizon Client para Linux desde la página de descargas de productos de VMware](#).

Recopilar información de registro de Horizon Client

Puede utilizar el script de recopilación de registros de Horizon Client para recopilar registros de clientes de varias ubicaciones y empaquetarlos en un único archivo de registro para solucionar problemas. Para ejecutar el script de recopilación de registros desde el terminal de la línea de comandos, debe tener permiso de "ejecución" en el sistema cliente Linux.

La mayoría de los clientes ligeros basados en Linux suelen almacenar los registros de Horizon Client en una o varias de las siguientes ubicaciones:

- `/tmp/vmware-`
- `/tmp/teradici-`
- `/tmp/vmware-root`

El script de recopilación de registros compila los registros del cliente en un archivo de paquete denominado `horizon-log.tar.gz` de forma predeterminada.

Procedimiento

- 1 Asegúrese de que tiene permiso de "ejecución" en el script de recopilación de registros del sistema cliente Linux. En el terminal de la línea de comandos, ejecute el siguiente comando:

```
# sudo chmod +x /usr/bin/vmware-view-log-collector
```

- 2 Para iniciar el script de recopilación de registros, ejecute el siguiente comando:

```
# sudo /usr/bin/vmware-view-log-collector
```

De forma predeterminada, el script busca los últimos archivos de registro generados por Horizon Client y los compila en un archivo de paquete llamado `horizon-log.tar.gz`, que se encuentra en la carpeta desde la que se ejecutó el script.

Para personalizar el nombre y la ubicación del archivo del paquete, puede ejecutar un comando similar a uno de los siguientes ejemplos:

```
# sudo /usr/bin/vmware-view-log-collector abc.tar.gz
```

```
# sudo /usr/bin/vmware-view-log-collector /home/user/Downloads/abc.tar.gz
```

- En el primer ejemplo, se compilan los registros de clientes en un archivo de paquete llamado `abc.tar.gz` en la carpeta desde la que se ejecutó el script.
- En el segundo ejemplo, se compilan los registros de clientes en un archivo de paquete llamado `abc.tar.gz` en la carpeta `/home/user/Downloads/`.

Problemas con la entrada de teclado

Cuando escribe en un escritorio remoto o una aplicación publicada, parece que las pulsaciones de teclas no funcionan.

Problema

Cuando está conectado a una aplicación publicada o un escritorio remoto, no aparece ningún carácter cuando escribe. Otro síntoma puede ser que se mantenga una única tecla repitiéndose.

Causa

Algunos programas de seguridad, como Norton 360 Total Security, incluyen una función que detecta software para registrar pulsaciones de teclas y bloquea el registro de estas pulsaciones. Esta función de seguridad se emplea para proteger el sistema contra spyware que roban las contraseñas y los números de las tarjetas de crédito. Este software de seguridad no permite que Horizon Client envíe pulsaciones de teclas a la aplicación publicada o al escritorio remoto.

Solución

- ◆ En el sistema cliente, desactive la función de detección del registro de pulsaciones de teclas del antivirus o del software de seguridad.

Conexión a un servidor en el modo Workspace ONE

No se puede conectar directamente a un servidor mediante Horizon Client, o bien las autorizaciones de aplicaciones publicadas y escritorios remotos no están visibles en Horizon Client.

Problema

- Cuando intente conectarse al servidor directamente a través de Horizon Client, Horizon Client le redireccionará al portal de Workspace ONE.
- Al abrir un escritorio remoto o una aplicación publicada mediante un URI o un comando, la solicitud le redireccionará al portal de Workspace ONE para autenticarse.
- Después de que abra un escritorio remoto o una aplicación publicada a través de Workspace ONE y se inicie Horizon Client, no podrá ver ni abrir otros escritorios remotos o aplicaciones publicadas autorizados en Horizon Client.

Causa

A partir de la versión 7.2 de Horizon 7, un administrador de Horizon puede habilitar el modo Workspace ONE en una instancia del servidor de conexión. Este comportamiento es normal cuando se habilita el modo Workspace ONE en una instancia del servidor de conexión.

Solución

Utilice Workspace ONE para conectarse a un servidor habilitado de Workspace ONE y acceder a sus aplicaciones publicadas y escritorios remotos.