Uso de VMware Horizon Client para Linux

Última modificación: 15 de septiembre de 2017
VMware Horizon Client for Linux 4.5

vmware®

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

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

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Uso de VMware Horizon Client para Linux

Esta guía, *Uso de VMware Horizon Client para Linux*, proporciona información acerca de la instalación y el uso del software VMware Horizon® Client™ en un sistema cliente Linux para conectarse a un escritorio de View del centro de datos.

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

Esta información está destinada a administradores que deban configurar una implementación de View que incluya sistemas cliente Linux. Asimismo, está destinada a los administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las 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 View. 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.

Instalación y requisitos del sistema

1

Los sistemas cliente deben cumplir ciertos requisitos de software y hardware. El proceso de instalación de Horizon Client es similar al de otras aplicaciones.

Este capítulo cubre los siguientes temas:

Requisitos del sistema para sistemas cliente Linux

El equipo o equipo portátil Linux en los que instala Horizon Client y los periféricos que utilicen deben cumplir ciertos requisitos del sistema.

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 View. Las funciones que están disponibles para cada dispositivo cliente ligero o cero y los sistemas operativos admitidos están determinados por el proveedor, 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.

NOTA:

- A partir de la versión 7.0, View Agent pasa a ser Horizon Agent.
- VMware Blast, el protocolo de visualización que está disponible a partir de Horizon Client 4.0 y Horizon Agent 7.0, también se denomina VMware Blast Extreme.

Arquitectura

i386, x86_64 y ARM

Memoria

Al menos 2 GB de RAM

Sistema operativo

Sistema operativo	Versión
Ubuntu	12.04, 14.04
Ubuntu de 64 bits	12.04, 14.04 y 16.04
Red Hat Enterprise Linux (RHEL)	6.8, 6.9
Red Hat Enterprise Linux (RHEL) de 64 bits	6.8/6.9, 7.2/7.3
SUSE Linux Enterprise Desktop (SLED)	11 SP4
SUSE Linux Enterprise Desktop (SLED) 64 bits	12 SP2
CentOS	6.8/6.9

Requisito de OpenSSL

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

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

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

Si los sistemas cliente se conectan desde fuera del firewall corporativo, VMware le recomienda que use un servidor de seguridad. Con un servidor de seguridad, los sistemas cliente no necesitarán una conexión VPN.

Las aplicaciones remotas (alojadas) solo están disponibles en servidores de View u Horizon 6.0 (o versiones posteriores).

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:
	`20MB + (24 * (# monitors) * (monitor width) * (monitor height))`
	Como guía general, puede utilizar los siguientes cálculos:
	`1 monitor: 1600 x 1200: 64MB`
	`2 monitors: 1600 x 1200: 128MB`
	`3 monitors: 1600 x 1200: 256MB`

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 View 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. ■ `libudev0.so.0` **NOTA:** A partir de Horizon Client 4.2, `libudev0` se necesita para iniciar Horizon Client. De forma predeterminada, `libudev0` no está instalado en Ubuntu 14.04.

- 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 la función Audio/vídeo en tiempo real

Audio/vídeo en tiempo real funciona con los dispositivos de cámaras web estándar y de audio analógicos y USB, así como con las aplicaciones de conferencias estándar tipo Skype, WebEx y Google Hangouts. Para que esta función sea compatible, la implementación de Horizon debe cumplir ciertos requisitos de software y hardware.

Escritorios remotos

Los escritorios deben tener instalado View Agent 5.2 o versiones posteriores, o Horizon Agent 7.0 o versiones posteriores. Los escritorios con View Agent 5.2 también deben tener instalado el agente de experiencia remota correspondiente. Por ejemplo, si View Agent 5.2 está instalado, también debe instalar el agente de experiencia remota de View 5.2 Feature Pack 2. Consulte el documento *Instalación y administración de View Feature Pack*. Si tiene View Agent 6.0 o versiones posteriores, o Horizon Agent 7.0 o versiones posteriores, no se necesitará ningún feature pack. Para utilizar la función Audio/vídeo en tiempo real con aplicaciones y escritorios publicados, debe tener Horizon Agent 7.0.2 o versiones posteriores.

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. Para que esta función sea compatible, no tendrá que instalar los controladores de dispositivos en el sistema operativo de escritorio en el que esté instalado el agente.

Protocolos de visualización

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

Requisitos del sistema para el redireccionamiento multimedia (MMR)

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

Escritorios remotos

- Los escritorios de usuario único deben tener instalados View Agent 6.0.2 o una versión posterior, o Horizon Agent 7.0 o una versión posterior.
- Los escritorios basados en sesiones deben tener instalados View Agent 6.1.1 o una versión posterior, o Horizon Agent 7.0 o una versión superior.

- Para obtener información sobre los requisitos de los sistemas operativos, otros requisitos de software y opciones de configuración para las aplicaciones o los escritorios remotos, consulte los temas sobre el redireccionamiento multimedia de Windows Media en *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 SLED 11 SP4, si se encuentra con problemas relacionados con la reproducción de vídeos como una pantalla en negro, elimine la biblioteca libvdpau.

En clientes ligeros HP, debe eliminar el archivo `/usr/lib/gstreamer-0.10/libgstfluvadec.so` para evitar problemas relacionados con la reproducción de vídeos como un error de Horizon Client o una pantalla en negro.

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

Son compatibles los formatos de medios compatibles con Windows Media Player. Por ejemplo: M4V; MOV; MP4; WMP; MPEG-4 Parte 2; WMV 7, 8 y 9; WMA; AVI; ACE; MP3; WAV.

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

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, se 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 JavaScript que el administrador de una página web incrustó en la misma. Cuando un usuario del escritorio virtual haga clic en el vínculo URL designado desde una página web, JavaScript intercepta y realiza un redireccionamiento de ShockWave File (SWF) desde la sesión del escritorio virtual 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.

Esta función está disponible cuando se use con la versión correcta del software agente. En View 5.3, está función está incluida en el agente de experiencia remota, que es parte de View Feature Pack. En View 6.0 y versiones posteriores, esta función se incluye en View Agent o Horizon Agent.

Para usar esta función, debe configurar la página web y los dispositivos cliente. Los sistemas cliente deben cumplir ciertos 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 el programa `wget` o compruebe que este programa ya esté instalado.
- `libffi.so.5` es necesario para que las distribuciones de Ubuntu 14.04 y 16.04 hagan que el redireccionamiento URL de Flash funcione, pero estas distribuciones solo cuentan con `libffi.so.6` de forma predeterminada. Puede solucionar esta limitación creando un vínculo simbólico entre `libffi.so.6` y `libffi.so.5`.

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 la documentación de Horizon.

Requisitos para la autenticación con tarjetas inteligentes

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

Cada sistema 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
- Controladores de aplicaciones específicos para el producto

También puede instalar controladores de aplicaciones específicos para el producto en el escritorio remoto o en el host de Microsoft RDS.

Los usuarios que se autentican con tarjetas inteligentes deben contar con una, y cada tarjeta inteligente debe tener un certificado de usuario.

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

- 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 View*.

  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 host del servidor de conexión o en el host del servidor de seguridad. Estos certificados incluyen certificados raíz y deben incluir certificados intermedios si el certificado de la tarjeta inteligente del usuario fue emitido por una entidad de certificación intermedia.
- Para obtener más información sobre las tareas que son necesarias en Active Directory para implementar la autenticación con tarjeta inteligente, consulte el documento *Administración de View*.

Habilitar el campo 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 introducen el nombre de usuario en el campo **Sugerencia de nombre de usuario** durante el inicio de sesión mediante tarjeta inteligente.

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 la instancia del servidor de conexión en Horizon Administrator. 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 View*.

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 sea compatible con 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*.

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

Configurar Horizon Client para la autenticación con tarjeta inteligente

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

Prerequisitos

- 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 View*.

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/lib/pkcs11/libgtop11dotnet.so
                  /usr/lib/vmware/view/pkcs11
   ```

Sistemas operativos del escritorio compatibles

Los administradores pueden crear máquinas virtuales con sistemas operativos invitados e instalar 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 View*.

Algunos sistemas operativos invitados Linux también son compatibles si cuentan con View Agent 6.1.1 o Horizon Agent 7.0, o bien con una versión posterior de ambos productos. Para obtener más información sobre los requisitos del sistema, sobre cómo configurar las máquinas virtuales Linux para usarlas en Horizon, así como una lista de funciones compatibles, consulte *Configurar escritorios de Horizon 6 for Linux* o *Configurar escritorios de Horizon 7 for Linux*.

Preparar el servidor de conexión para Horizon Client

Los administradores deben realizar tareas específicas para permitir que los usuarios finales puedan conectarse a aplicaciones y escritorios remotos.

Antes de que los usuarios finales se puedan conectar al servidor de conexión o a un servidor de seguridad y acceder a una aplicación o un escritorio remotos, debe configurar ciertas opciones de grupo y de seguridad:

- Si tiene pensado usar 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 llevan a cabo la misma función que antes solo realizaban los servidores de seguridad.
- Si utiliza un servidor de seguridad, compruebe que esté utilizando las últimas versiones de mantenimiento del servidor de conexión 5.3.x y del servidor de seguridad 5.3.x o versiones posteriores. Para obtener más información, consulte el documento *Instalación de View*.
- Si tiene pensado utilizar una conexión en túnel segura para dispositivos cliente y si la conexión segura está configurada con un nombre de host DNS para el servidor de conexión o un servidor de seguridad, compruebe que el dispositivo cliente pueda resolver este nombre DNS.

  Para habilitar o deshabilitar el túnel de seguridad, en Horizon Administrator, acceda al cuadro de diálogo **Editar la configuración del servidor de conexión de Horizon** y utilice el cuadro de diálogo **Usar conexión en túnel segura para el escritorio**.
- 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 el documento *Configurar escritorios virtuales en Horizon 7* o el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Para utilizar una autenticación en dos fases con Horizon Client, así como la autenticación RSA SecurID o RADIUS, debe habilitar esta característica en el servidor de conexión. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento *Administración de View*.
- Para ocultar la información de seguridad de Horizon Client, incluida la información sobre la URL del servidor y el menú desplegable **Dominio**, habilite las opciones **Ocultar la información del servidor en la interfaz de usuario del cliente** y **Ocultar la lista de dominios en la interfaz de usuario del cliente** en Horizon Administrator. Estas configuraciones globales están disponibles a partir de la versión 7.1 de Horizon 7. Para obtener más información sobre cómo establecer configuraciones globales, consulte el documento *Administración de View*.

Para autenticarse cuando el menú desplegable **Dominio** está oculto, los usuarios deben proporcionar la información del dominio introduciendo el nombre de usuario con el formato ***dominio**nombredeusuario*** o con el formato ***usuario*nombre@*dominio*** en el cuadro de texto **Nombre de usuario**.

IMPORTANTE: Si habilita las opciones **Ocultar la información del servidor en la interfaz de usuario del cliente** y **Ocultar la lista de dominios en la interfaz de usuario del cliente** y selecciona la autenticación de dos fases (RSA SecureID o RADIUS) para la instancia del servidor de conexión, no exija que coincidan los nombres de usuarios de Windows. Si exige que coincidan los nombres de usuarios de Windows, se impide a los usuarios que introduzcan información de dominio en el cuadro de texto del nombre de usuario y siempre se producirá un error al iniciar sesión. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento *Administración de View*.

- Para proporcionar a los usuarios acceso sin autenticar a las aplicaciones publicadas en Horizon Client, debe habilitar esta función en el servidor de conexión. Para obtener más información, consulte los temas relacionados con el acceso sin autenticar en el documento *Administración de View*.

Opciones de instalación

Durante el proceso de instalación de Horizon Client, se le solicita que confirme si desea instalar varios componentes. La acción predeterminada es instalar todos los componentes.

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

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

Opción	Descripción
Redireccionamiento USB	Proporciona a los usuarios acceso a dispositivos USB conectados de forma local en las aplicaciones y los escritorios. El redireccionamiento USB es compatible con las aplicaciones y los escritorios remotos que se implementan en equipos de un solo usuario. Los archivos de componentes se instalan en `/usr/lib/vmware/view/usb/`. Si permite que el instalador registre e inicie los servicios instalados tras finalizar este proceso, se ejecuta automáticamente el demonio del árbitro USB, `vmware-USBArbitrator`. Si no es así, puede iniciar el demonio de forma manual ejecutando el siguiente comando: `sudo /etc/init.d/vmware-USBArbitrator start` **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 *Configurar funciones de escritorios remotos en Horizon 7*.
Audio/vídeo en tiempo real	Redirecciona los dispositivos de audio y de cámara web que están conectados al sistema cliente para que se puedan usar en el escritorio remoto. El archivo de componente se instala en `/usr/lib/pcoip/vchan_plugins/`.

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

Opción	Descripción
Impresión virtual	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. Los archivos de componentes se instalan en `/usr/lib/vmware/view/virtualPrinting/`. Una vez instalado el cliente, no es necesario que configure manualmente esta función si permite al instalador registrar e iniciar los servicios instalados después del proceso de instalación. En caso contrario, puede configurar y habilitar esta función según las instrucciones disponibles en Habilitar la función de impresión virtual en un cliente Linux. En Horizon 6.0.2 y versiones posteriores, se admite la impresión virtual en las siguientes aplicaciones y escritorios remotos: ■ 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).
Redireccionamiento multimedia (MMR)	Redirecciona la transmisión multimedia desde el escritorio al equipo cliente, donde esta se procesa. El archivo de componente se instala en `/usr/lib/vmware/view/vdpService/`.
Tarjeta inteligente	Permite al usuario autenticarse con tarjetas inteligentes cuando usan los protocolos de visualización VMware Blast o PCoIP. Aunque esta opción se selecciona en el instalador cliente de forma predeterminada, no se selecciona de forma predeterminada cuando ejecuta el instalador de View Agent en el escritorio remoto. La tarjeta inteligente es compatible con escritorios remotos que se implementan en equipos de un solo usuario y en hosts RDS. Para la compatibilidad de tarjetas inteligentes en hosts RDS, debe contar con View Agent 6.1.1 o una versión posterior. Los archivos de componentes se instalan en `/usr/lib/pcoip/vchan_plugins/`.
Redireccionamiento de unidades de cliente	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. Los archivos de componentes se instalan en `/usr/lib/vmware/view/vdpService/`.

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. En las distribuciones SUSE Linux, el paquete de instalación inicia un asistente de la línea de comandos. También puede ejecutar el instalador con la opción `--console` para iniciar el asistente de la línea de comandos.

Prerequisitos

- 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 a raíz del sistema host.
- 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.
- En las distribuciones SUSE Linux, ejecute `sudo zypper install python-curses` para instalar la biblioteca de `curses`.
- En un entorno python2 de distribuciones de Ubuntu 16.04 x64, ejecute `sudo apt-get install python-gtk2` para instalar la biblioteca de `gtk2`.

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 Clienthttp://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	`sudo ./VMware-Horizon-Client-`*`x.x.x-yyyyyyy.arch`*`.bundle`
Para el asistente GUI, si no tiene configurados permisos ejecutables	`sudo sh ./VMware-Horizon-Client-`*`x.x.x-yyyyyyy.arch`*`.bundle`
Para el instalador de la línea de comandos	`sudo ./VMware-Horizon-Client-`*`x.x.x-yyyyyyy.arch`*`.bundle --console`

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

3 Siga los pasos que se le indican para finalizar la instalación.

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, no será necesario iniciar los servicios de redireccionamiento USB de forma manual cada vez que reinicie y no necesitará habilitar manualmente la función de impresión virtual.

4 Después de que se complete la instalación, 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.

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

Qué hacer a continuación

Inicie Horizon Client y compruebe que pueda iniciar sesión en el escritorio virtual correcto. Consulte Conectarse a una aplicación o escritorio remotos.

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-yyyyyyy.arch.bundle`*`.bundle`.

Tabla 1-2. Opciones de instalación de la línea de comandos en Linux

Opción	Descripción
`--help`	Muestra información de uso.
`--console`	Le permite usar el instalador de la línea de comandos en una ventana de terminal.
`--custom`	Muestra todas preguntas de instalación, incluso si las respuestas predeterminadas se generan por script, como, por ejemplo, al usar las opciones `--set-setting`. La opción predeterminada es `--regular`, que muestra únicamente las preguntas que no tienen una respuesta predeterminada.
`--eulas-agreed`	Acepta el contrato de licencia para el usuario final.

Tabla 1-2. Opciones de instalación de la línea de comandos en Linux (Continua)

Opción	Descripción
`--gtk`	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.
`--ignore-errors` o `-I`	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.
`--regular`	Muestra las preguntas de instalación que no se respondieron o que son necesarias. Esta es la opción predeterminada.
`--required`	Muestra la solicitud del contrato de licencia y, a continuación, comienza a instalar el cliente. La opción predeterminada es `--regular`, que muestra únicamente las preguntas que no tienen una respuesta predeterminada.
`--set-setting vmware-horizon-smartcard smartcardEnable yes`	Instala el componente de la tarjeta inteligente.
`--set-setting vmware-horizon-rtav rtavEnable yes`	Instala el componente Audio/vídeo en tiempo real.
`--set-setting vmware-horizon-usb usbEnable yes`	Instala la función de redireccionamiento USB.
`--set-setting vmware-horizon-virtual-printing tpEnable yes`	Instala la función de impresión virtual.
`--set-setting vmware-horizon-tsdr tsdrEnable yes`	Instala la función de redireccionamiento de la unidad cliente.
`--set-setting vmware-horizon-mmr mmrEnable yes`	Instala la función de redireccionamiento multimedia (MMR).
`--stop-services`	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 1-3. Opciones de instalación de variables del entorno de Linux

Variable	Descripción
`TERM=dumb`	Muestra una interfaz de usuario de texto básico.
`VMWARE_EULAS_AGREED=yes`	Le permite aceptar silenciosamente el Contrato de licencia para el usuario final del producto.
`VMIS_LOG_LEVEL=`*valor*	Use uno de los siguientes valores para *valor*: ■ `NOTSET` ■ `DEBUG` ■ `INFO` ■ `WARNING` ■ `ERROR` ■ `CRITICAL` La información de los registros se almacena en `/tmp/vmware-root/vmware-installer-`*pid*`.log`.

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
```

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.

Prerequisitos

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 `.thnuclnt` en el directorio `home`.

```
$ mkdir ~/.thnuclnt/
```

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 `thnuclnt.conf` en la carpeta `~/.thnuclnt` y agregue el siguiente texto al archivo:

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

connector svc {
   protocol = listen
   interface = /home/user/.thnuclnt/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 `thnuclnt`.

```
$ thnuclnt –fg
```

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

```
$ export TPCLIENTADDR=/home/user/.thnuclnt/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 `thnuclnt`.

```
$ killall thnuclnt
```

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

Las impresoras ya no estarán redirigidas.

Instalar Horizon Client para Linux desde el Centro de software de Ubuntu

Si tiene un sistema Ubuntu, puede instalar el cliente desde el Centro de software de Ubuntu como alternativa a instalar la versión proporcionada en el sitio web de descargas de VMware. Si usa el Centro de software de Ubuntu, instale el cliente mediante el gestor de paquetes Synaptic.

Este tema proporciona instrucciones para obtener el software cliente del Centro de software de Ubuntu. También puede obtener el software de Horizon Client desde el sitio web de descargas de productos de VMware, tal y como se describe en Instalar o actualizar Horizon Client para Linux desde la página de descargas de productos de VMware.

IMPORTANTE: Los clientes que usen clientes ligeros basados en Linux deben ponerse en contacto con el proveedor de clientes ligeros para las actualizaciones de Horizon Client. Los clientes que compilaron correctamente sus propios endpoints basados en Linux y necesitan un cliente actualizado deben ponerse en contacto con el representante de ventas de VMware.

Prerequisitos

- Compruebe que el sistema cliente utilice un sistema operativo compatible. Consulte Requisitos del sistema para sistemas cliente Linux.
- Compruebe que tenga instalada la versión correcta de OpenSSL. Consulte Requisitos del sistema para sistemas cliente Linux.
- Compruebe que pueda iniciar sesión como administrador 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 de View Client 1.x o 2.x. Consulte Desinstalar Horizon Client para Linux.

Procedimiento

1 En su equipo o portátil Linux, habilite Socios de Canonical.

a En la barra de menús, seleccione **Sistema > Administración > Gestor de actualizaciones**.

b Haga clic en el botón **Configuración** y proporcione la contraseña para realizar tareas administrativas.

c En el cuadro de diálogo Orígenes del software, haga clic en la pestaña **Otro software** y seleccione la casilla **Socios de Canonical** para seleccionar el archivo del software que proporciona Canonical para sus partners.

d Haga clic en **Cerrar** y siga las instrucciones para actualizar la lista de paquetes.

2 Si tiene Ubuntu 12.04 o 14.04, descargue e instale el paquete desde el Centro de software de Ubuntu, tal y como se especifica a continuación.

a Abra una ventana de terminal e introduzca el comando para obtener nuevos paquetes:

```
sudo apt-get update
```

Los nuevos paquetes se descargarán y podrá ver una lista de estos en la ventana de terminal.

b Abra el Gestor de actualizaciones y busque e instale las actualizaciones.

c Abra la aplicación Centro de software de Ubuntu y busque **`vmware-view-client`**.

d Instale la aplicación `vmware-view-client`.

Si el sistema operativo es Ubuntu 12.04 o 14.04, se instalará la última versión de Horizon Client.

Aparecerá un icono para la aplicación **VMware Horizon Client** en el programa de inicio de las aplicaciones.

Qué hacer a continuación

Inicie Horizon Client y compruebe que pueda iniciar sesión en el escritorio virtual correcto. Consulte Conectarse a una aplicación o escritorio remotos.

Configurar las opciones de VMware Blast

Puede configurar la descodificación H.264 y las opciones de condición de la red para las sesiones de aplicaciones y escritorios remotos que utilizan el protocolo de visualización VMware Blast.

La resolución máxima que se admite depende de la capacidad de la unidad de procesamiento gráfico (GPU) en el cliente. Puede que una GPU capaz de admitir una resolución 4K para los formatos JPEG y PNG no admita una resolución 4K de H.264. Si no se admite una resolución de H.264, Horizon Client utiliza JPEG o PNG en su lugar.

La descodificación H.264 es compatible en las GPU de AMD, NVIDIA e Intel. La descodificación 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 descodificación H.264 con una GPU de NVIDIA, instale VDPAU (API para descodificación 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 `vainfo`, se muestran los perfiles H.264. Si la versión del controlador VA-API es 1.2.x o anterior, debe agregar la entrada `mks.enableGLBasicRenderer = TRUE` en `/etc/vmware/config`, `/usr/lib/vmware/config` o `~/.vmware/config`. Se procesan los archivos de configuración en el siguiente orden:

1 `/etc/vmware/config`

2 `/usr/lib/vmware/config`

3 `~/.vmware/config`

Si Red Hat 7.2, la GPU de Intel, el controlador Intel con la versión 1.2 o anterior, OpenGL 3.2 y H.264 están habilitados, debe agregar las siguientes entradas a uno de los tres archivos de configuración para evitar problemas de visualización, por ejemplo, una pantalla en negro.

```
mks.enableGLRenderer=FALSE
mks.enableGLBasicRenderer=TRUE
```

H.264 no es compatible con SLED 11 SP4 con la GPU de Intel porque la versión xorg es demasiado antigua.

No puede cambiar la opción de condición de la red tras iniciar sesión en un servidor. Puede configurar la descodificación H.264 antes o después de iniciar sesión en un servidor.

Prerequisitos

Esta función requiere la versión 7.0 de Horizon Agent o una versión posterior.

Procedimiento

1 Seleccione **Archivo > Configurar VMware Blast** en la barra de menús.

2 Configure las opciones de descodificación y condición de la red.

Opción	Acción
H.264	Configure esta opción antes o después de conectarse al servidor de conexión, para permitir la descodificación H.264 en Horizon Client. Cuando está seleccionada esta opción (la opción predeterminada), Horizon Client utiliza la descodificación H.264 si el agente es compatible con la descodificación mediante hardware o software H.264. Si el agente no es compatible con la descodificación mediante hardware o software H.264, Horizon Client usa la descodificación JPG/PNG. Anule la selección de esta opción para usar la descodificación JPG o PNG.
Seleccione la condición de su red para disfrutar de la mejor experiencia	Solo puede configurar esta opción antes de conectarse al servidor de conexión. Seleccione una de las siguientes opciones de condición de la red: ■ **Excelente**: Horizon Client utiliza únicamente redes TCP. Esta opción es ideal para un entorno de LAN. ■ **Normal (predeterminado)**: Horizon Client trabaja en modo mixto. En el modo mixto, Horizon Client usa redes TCP al conectarse al servidor y utiliza Blast Extreme Adaptive Transport (BEAT) si el agente y la puerta de enlace de seguridad de Blast (si estuviese habilitada) admiten la conectividad con BEAT. Esta es la opción predeterminada. ■ **Deficiente**: Horizon Client utiliza únicamente las redes BEAT si el servidor del túnel de BEAT está habilitado en el servidor. De lo contrario, cambia a modo mixto. **NOTA:** En Horizon 7, versión 7.1 y versiones anteriores, las instancias del servidor de conexión y del servidor de seguridad no son compatibles con el servidor del túnel de BEAT. Unified Access Gateway 2.9 y versiones posteriores son compatibles con el servidor del túnel de BEAT. La puerta de enlace de seguridad de Blast para las instancias del servidor de conexión y del servidor de seguridad no son compatibles con las redes de BEAT.

3 Haga clic en **Aceptar** para guardar los cambios.

Los cambios de H.264 tendrán efecto la próxima vez que un usuario se conecte a una aplicación o un escritorio remotos y seleccione el protocolo de visualización VMware Blast. Los cambios no afectan a las sesiones VMware Blast existentes.

Datos de Horizon Client recopilados por VMware

Si su compañía participa en el programa de mejora de la experiencia de cliente, VMware recopila datos de ciertos campos de Horizon Client. Los campos que contienen información personal son anónimos.

VMware recopila datos de los clientes para priorizar la compatibilidad entre el hardware y el software. Si el administrador de la compañía decidió participar en el programa de mejora de la experiencia de cliente, VMware recopila datos anónimos acerca de la implementación para mejorar la respuesta de VMware a los requisitos del cliente. No se recopila ningún dato que identifique a su organización. La información de Horizon Client se envía primero al servidor de conexión y después a VMware, junto con los datos de las instancias de los servidores de conexión y los escritorios remotos.

Aunque la información esté cifrada mientras se envía al servidor de conexión, la información en el sistema cliente se registra sin cifrar en un directorio específico. Los registros no contienen información de identificación personal.

El administrador que instale el servidor de conexión puede seleccionar si desea participar en el programa de mejora de la experiencia de cliente de VMware mientras el asistente de instalación del servidor de conexión esté en ejecución. Del mismo modo, un administrador puede configurar una opción en Horizon Administrator después de la instalación.

Tabla 1-4. 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 *x.x.x-yyyyyy*, donde *x.x.x* es el número de la versión cliente e *yyyyyy* es el número de compilación).
Arquitectura binaria del cliente	No	Ejemplos que incluyen los siguientes valores: ■ i386 ■ x86_64 ■ arm
Nombre de compilación del cliente	No	Ejemplos que incluyen los siguientes valores: ■ 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: ■ 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: ■ 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)

Tabla 1-4. Datos recopilados de las instancias de Horizon Client para el programa de mejora de la experiencia de cliente (Continua)

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Arquitectura del sistema operativo del host	No	Ejemplos que incluyen los siguientes valores: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Modelo de sistema del host	No	Ejemplos que incluyen los siguientes valores: ■ 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: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ desconocido (para iPad)
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: ■ 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: ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID del producto del dispositivo USB	No	Ejemplos que incluyen los siguientes valores: ■ Data Traveler ■ Controlador para juegos ■ Unidad de almacenamiento ■ Mouse inalámbrico
Familia de dispositivos USB	No	Ejemplos que incluyen los siguientes valores: ■ Seguridad ■ Dispositivo de interfaz de usuario ■ Imágenes
Recuento del uso del dispositivo USB	No	(Número de veces que se compartió el dispositivo)

Configurar Horizon Client para usuarios finales 2

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 cubre los siguientes temas:

Opciones de configuración comunes

Horizon Client proporciona varios mecanismos de configuración para simplificar la experiencia de selección de escritorios 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 2-1. Opciones de configuración comunes

Ajuste	Mecanismos de configuración
Dirección del servidor de conexión	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 del escritorio para mostrar	URI, propiedad del archivo de configuración y línea de comandos

Tabla 2-1. Opciones de configuración comunes (Continua)

Ajuste	Mecanismos de configuración
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 SSL y algoritmos criptográficos	Propiedad del archivo de configuración, línea de comandos

Utilizar los archivos de configuración y la interfaz de línea de comandos de Horizon Client

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-default-config`

2 `~/.vmware/view-preferences`

3 Argumentos de la línea de comandos

4 `/etc/vmware/view-mandatory-config`

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` del 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 2-2. 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`	Oculta el sistema operativo del host y abre la interfaz de usuario de Horizon Client en modo de pantalla completa en todos los monitores que estén conectados cuando se inicie el cliente. Si establece la clave de configuración, especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es "FALSE".
`view.allowDefaultBroker`	`-l`, `--lockServer`	Al usar esta opción de la línea de comandos o al configurar la propiedad como "FALSE", se deshabilita el campo **Servidor** si el cliente no se conectó nunca a ningún servidor y además, no se proporciona ninguna dirección de servidor en la línea de comandos ni en el archivo de preferencias. Ejemplo de cómo usar la opción de la línea de comandos: `--lockServer -s view.company.com`
`view.autoConnectBroker`	Ninguna	Se conecta automáticamente al último servidor de View utilizado, a menos que la propiedad de configuración `view.defaultBroker` esté establecida o que se use la opción de la 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 2-2. Claves de archivo de configuración y opciones de la línea de comandos de Horizon Client (Continua)

Clave de configuración	Opción de línea de comandos	Descripción
`view.autoConnectDesktop`	Ninguna	Se conecta automáticamente al último escritorio de View utilizado, a menos que la propiedad de configuración `view.defaultDesktop` esté establecida o que se use la opción de la línea de comandos `--desktopName=`. Especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es "FALSE". Si se establece esta propiedad y la propiedad `view.autoConnectBroker` en "TRUE", esta acción es equivalente a establecer la propiedad `view.nonInteractive` en "TRUE".
`view.autoDisconnectEmptyAppSession`	Ninguna	Cuando se establece en **"TRUE"** (predeterminado), si la sesión de la aplicación se vacía porque el usuario cierra todas las aplicaciones, aparecerá 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 View Administrator, que de forma predeterminada se desconectará después de un minuto.
`view.defaultAppHeight`	Ninguna	Especifica en píxeles la altura predeterminada de la ventana de las aplicaciones remotas. Use esta propiedad junto con `view.defaultAppWidth` cuando especifique un tamaño de escritorio personalizado (la propiedad `view.defaultAppSize` está establecida en "5"). El valor predeterminado es "480".
`view.defaultAppSize`	`--appSize=`	Establece el tamaño predeterminado de la ventana de las aplicaciones remotas. ■ Para usar todos los monitores, especifique **"1"**. ■ Para usar el modo de pantalla completa en un monitor, especifique **"2"**. ■ Para usar una ventana grande, especifique **"3"**. ■ Para usar una ventana pequeña, especifique **"4"**. ■ Para configurar un tamaño personalizado, especifique **"5"** y, a continuación, establezca también las propiedades `view.defaultAppWidth` y `view.defaultAppHeight`. El valor predeterminado es "1".

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.defaultAppWidth`	Ninguna	Especifica en píxeles el ancho predeterminado de la ventana de las aplicaciones remotas. Use esta propiedad junto con `view.defaultAppHeight` cuando especifique un tamaño de escritorio personalizado (la propiedad `view.defaultAppSize` está establecida en "5"). El valor predeterminado es "640".

`view.defaultBroker`	`-s`, `--serverURL=`	Agrega el nombre que especificó en el campo **Servidor** de Horizon Client. Especifique un nombre de dominio completo. También puede especificar un número de puerto si no utiliza el puerto 443 predeterminado.
		El último valor usado es el predeterminado.
		Ejemplos de cómo usar la opción de la línea de comandos:
		`--serverURL=https://view.company.com`
		`-s view.company.com`
		`--serverURL=view.company.com:1443`

`view.defaultDesktop`	`-n`, `--desktopName=`	Especifica el escritorio que se usará cuando `autoConnectDesktop` se configura como "TRUE" y el usuario tiene acceso a varios escritorios. Este es el nombre que verá en el cuadro de diálogo Seleccionar escritorio. El nombre suele ser el nombre del grupo.
`view.defaultDesktopHeight`	Ninguna	Especifica en píxeles la altura predeterminada de la ventana del escritorio de View. Use esta propiedad junto con `view.defaultDesktopWidth` cuando especifique un tamaño de escritorio personalizado (la propiedad `view.defaultDesktopSize` está establecida en "5").

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

Clave de configuración	Opción de línea de comandos	Descripción

`view.defaultDesktopSize`	`--desktopSize=`	Establece el tamaño predeterminado de la ventana del escritorio de View:
		■ 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`*`"`**.
		Ejemplos de cómo usar la opción de la línea de comandos:
		`--desktopSize="1280x800"`
		`--desktopSize="all"`

`view.defaultDesktopWidth`	Ninguna	Especifica en píxeles el ancho predeterminado de la ventana del escritorio de View. Use esta propiedad junto con `view.defaultDesktopHeight` cuando especifique un tamaño de escritorio personalizado (la propiedad `view.defaultDesktopSize` está establecida en "5").
`view.defaultDomain`	`-d`, `--domainName=`	Establece el nombre de dominio que Horizon Client usa en todas las conexiones y agrega el nombre de dominio que especificó en el campo **Nombre de dominio** en el cuadro de diálogo de autenticación.

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.defaultLogLevel`	Ninguna	Establece el nivel de los registros de Horizon Client. Establezca la propiedad en uno de los siguientes valores: ■ 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. El valor predeterminado es "3".
`view.defaultPassword`	`-p "-", --password="-"`	Para las conexiones `rdesktop`, VMware Blast y PCoIP, especifique siempre **`"-"`** para que la contraseña se lea desde `stdin`. Establece la contraseña que Horizon Client usa para todas las conexiones y agrega la contraseña al campo **Contraseña** en el cuadro de diálogo de autenticación si el servidor de conexión de View acepta la autenticación de contraseña. **NOTA:** No puede usar una contraseña en blanco. Es decir, no puede especificar lo siguiente: --password=""
`view.defaultProtocol`	`--protocol=`	Especifica el protocolo de visualización que se usará. Especifique **`"PCOIP"`** o **`"RDP"`**. Estos valores distinguen entre mayúsculas y minúsculas. Por ejemplo, si introduce **`rdp`**, el protocolo que se use será el predeterminado. Este se especifica en View Administrator, en la configuración del grupo. Si usa RDP y desea usar FreeRDP en lugar de `rdesktop`, debe utilizar también la opción `rdpClient`.

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.defaultUser`	`-u`, `--userName=`	Establece el nombre de usuario que Horizon Client usa en todas las conexiones y agrega el nombre de usuario que especificó en el campo **Nombre de usuario** en el cuadro de diálogo de autenticación. En pantalla completa, 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-`**.
`view.disableMaximizedApp`	`--disableMaximizedApp`	Si se establece como **`"FALSE"`** (predeterminado), la aplicación se inicia en modo de pantalla completa.
`view.enableMMR`	Ninguna	Habilita el redireccionamiento multimedia (MMR). Especifique **`"TRUE"`** o **`"FALSE"`**. El valor predeterminado es "FALSE".
`view.fullScreen`	`--fullscreen`	Oculta el sistema operativo del host y abre la interfaz de usuario de Horizon Client en modo de pantalla completa en un monitor. Esta opción no afecta al modo de pantalla de la sesión del escritorio. Si establece la clave de configuración, especifique **`"TRUE"`** o **`"FALSE"`**. El valor predeterminado es "FALSE".

`view.kbdLayout`	`-k`, `--kbdLayout=`	Especifica qué configuración local usar en la distribución del teclado.
		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:
		`xfreerdp --kbd-list`
		Ejemplo de cómo usar la opción de la línea de comandos de rdesktop:
		`--kbdLayout="en-us"`
		`-k "fr"`
		Ejemplo de cómo usar la opción de la línea de comandos de freerdp:
		`-k "0x00010407"`

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.kioskLogin`	`--kioskLogin`	Especifica que Horizon Client usará una cuenta en pantalla completa para las autenticaciones. Si establece la clave de configuración, especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es "FALSE". Consulte el ejemplo de pantalla completa que aparece tras esta tabla.
`view.mmrPath`	`-m`, `--mmrPath=`	(Disponible únicamente con distribuciones por parte de terceros). Especifica la ruta al directorio que contiene las bibliotecas Wyse MMR (redireccionamiento multimedia). Ejemplo de cómo usar la opción de la línea de comandos: `--mmrPath="/usr/lib/altmmr"`
`view.monitors`	`--monitors=` *lista numerada*	Le permite especificar los monitores adyacentes que utilizará para Horizon Client. Use `--allmonitors` (o `view.allMonitors`) para especificar que desea usar la pantalla completa en todos los monitores y `--monitors=`*lista numerada* para especificar el subconjunto de monitores que se usará. Ejemplo de cómo usar la opción de línea de comandos para especificar el primer y el segundo monitor en una configuración donde 3 monitores están situados uno junto a otro de forma horizontal: `--allmonitors --monitors="1,2" `` Para ayudar a distinguir qué monitor físico está asociado a un icono de monitor en la IU de cliente, se muestra un rectángulo en la esquina superior izquierda del monitor físico que usted haya especificado que se debe utilizar. El rectángulo tiene el color y el número correspondientes que se utilizan en el icono para el monitor seleccionado.
`view.noMenuBar`	`--nomenubar`	Suprime la barra de menús de Horizon Client cuando el cliente está en modo pantalla completa, por lo que el usuario no puede acceder a las opciones del menú para cerrar sesión, desconectarse de un escritorio de View ni tampoco restablecerlo. Utilice esta opción cuando configure la pantalla completa. Si establece la clave de configuración, especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es "FALSE".

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.nonInteractive`	`-q`, `--nonInteractive`	Oculta 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. Si establece la clave de configuración, especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es "FALSE". Si se establece esta propiedad en "TRUE", esta acción es equivalente a establecer las propiedades `view.autoConnectBroker` y `view.autoConnectDesktop` en "TRUE". Ejemplo de cómo usar la opción de la línea de comandos: `--nonInteractive --serverURL="https://view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"`
`view.once`	`--once`	Especifica que no desea que Horizon Client vuelva a intentar conectarse si se produce un error. Debe especificar esta opción si utiliza la pantalla completa y utilizar el código de salida para solucionar el error. De lo contrario, será difícil terminar el proceso `vmware-view` de forma remota. Si establece la clave de configuración, especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es "FALSE".
`view.rdesktopOptions`	`--rdesktopOptions=`	(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. Ejemplo de cómo usar la opción de la línea de comandos: `--rdesktopOptions="-f -m"`

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

Clave de configuración	Opción de línea de comandos	Descripción
Ninguna	`-r`, `--redirect=`	(Disponible si usa el protocolo de visualización Microsoft RDP). Especifica un dispositivo local para que rdesktop lo redireccione al escritorio de View. Especifique la información del dispositivo que desea que se transfiera a la opción `-r` de rdesktop. Puede establecer varias opciones de dispositivos en un único comando. Ejemplo de cómo usar la opción de la línea de comandos: `--redirect="sound:off"`
`view.rdpClient`	`--rdpclient=`	(Disponible si usa el protocolo de visualización Microsoft RDP). Especifica el tipo de cliente RDP que se usará. El predeterminado es `rdesktop`. Para usar FreeRDP en su lugar, especifique `xfreerdp`. **NOTA:** Para usar FreeRDP, debe tener instalada la versión adecuada de FreeRDP, junto con las revisiones correspondientes. Si desea obtener más información, consulte Instalar y configurar FreeRDP.
Ninguna	`--save`	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 introduzca estos nombres la próxima vez que se le soliciten las credenciales de inicio de sesión.
`view.sendCtrlAltDelToLocal`	Ninguna	(Disponible si usa los protocolos de visualización VMware Blast o PCoIP). Si se configura como **"TRUE"**, envía la combinación de teclas Ctrl+Alt +Supr al sistema cliente en lugar de abrir un cuadro de diálogo para solicitarle al usuario que se desconecte del escritorio de View. El valor predeterminado es "FALSE". **NOTA:** Si usa el protocolo de visualización Microsoft RDP, puede realizar esta función con la opción `-K`, por ejemplo, `vmware-view -K`. Esta opción tiene la misma prioridad que la configuración del archivo `/etc/vmware/view-keycombos-config`.

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.sendCtrlAltDelToVM`	Ninguna	(Disponible si usa los protocolos de visualización VMware Blast o PCoIP). Si se configura como **"TRUE"**, envía la combinación de teclas Ctrl+Alt +Supr al escritorio virtual en lugar de abrir un cuadro de diálogo para solicitarle al usuario que se desconecte del escritorio de View. El valor predeterminado es "FALSE". Esta opción tiene más prioridad que la configuración del archivo `/etc/vmware/view-keycombos-config`.
`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 directiva GPO del agente, llamada "Usar una clave alternativa para enviar la secuencia de aviso de seguridad", disponible en la plantilla `pcoip.adm`. Consulte el tema "Configuración del teclado para PCoIP" del capítulo "Configurar directivas para grupos de escritorios y aplicaciones" del documento *Configurar funciones de escritorios remotos en Horizon 7*. Esta opción tiene menos prioridad que la configuración del archivo `/etc/vmware/view-keycombos-config`.
`view.shareRemovableStorage`	Ninguna	Cuando se establece en **"TRUE"**, habilita la opción **Permitir acceso a almacenamiento extraíble**. El valor predeterminado es "TRUE".
`view.sslCipherString`	`--sslCipherString=`	Configura la lista de cifrado para restringir el uso de ciertos algoritmos criptográficos antes de establecer una conexión SSL cifrada. Para obtener una lista de cadenas de cifrado, consulte http://www.openssl.org/docs/apps/ciphers.html . El valor predeterminado de Horizon Client es "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES".

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.sslProtocolString`	`--sslProtocolString=`	Configura la lista de cifrado para restringir el uso de ciertos protocolos criptográficos antes de establecer una conexión SSL cifrada. Los protocolos admitidos son SSLv3/SSLv3.0, TLSv1.0/TLSv1, 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. El valor predeterminado es "TLSv1.0:TLSv1.1:TLSv1.2".
`view.sslVerificationMode`	Ninguna	Establece el modo de verificación del certificado del servidor. 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".
`view.UnauthenticatedAccessEnabled`	`--unauthenticatedAccessEnabled`	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. 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. 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. Si establece la clave de configuración, especifique **`"TRUE"`** o **`"FALSE"`**. Ejemplos de cómo usar la opción de la línea de comandos: `--unauthenticatedAccessEnabled="TRUE"`

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

Clave de configuración	Opción de línea de comandos	Descripción
`view.UnauthenticatedAccessAccount`	`--unauthenticatedAccessAccount`	Especifica la cuenta que se utilizará cuando `unauthenticatedAccessEnabled` esté establecido en "TRUE". Si la `unauthenticatedAccessEnabled` está establecida en **"FALSE"**, esta configuración se ignorará. Ejemplos de cómo usar la opción de la línea de comandos con la cuenta de usuario **`anonymous1`**: `--unauthenticatedAccessAccount='anonymous1'`
`view.usbAutoConnectAtStartup`	`--usbAutoConnectAtStartUp=`	Redirecciona de forma automática los dispositivos USB a un escritorio Horizon si estos dispositivos se introducen en el sistema del host antes de que se conecte el escritorio. Esta opción no se aplica a las aplicaciones remotas. Especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es **"TRUE"**.
`view.usbAutoConnectOnInsert`	`--usbAutoConnectOnInsert=`	Redirecciona de forma automática los dispositivos USB a un escritorio Horizon cuando estos dispositivos se introducen en el sistema del host después de que se conecte el escritorio. Esta opción no se aplica a las aplicaciones remotas. Especifique **"TRUE"** o **"FALSE"**. El valor predeterminado es **"TRUE"**.
`view.xfreerdpOptions`	`--xfreerdpOptions=`	(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`. **NOTA:** Para usar FreeRDP, debe tener instalada la versión adecuada de FreeRDP, junto con las revisiones correspondientes. Si desea obtener más información, consulte Instalar y configurar FreeRDP.

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

Clave de configuración	Opción de línea de comandos	Descripción
Ninguna	`--enableNla`	(Se aplica si utiliza FreeRDP para las conexiones RDP). Habilita la autenticación a nivel de red (NLA). Debe usar esta opción junto con la opción `--ignore-certificate`. Si desea obtener más información, consulte Utilizar FreeRDP para las conexiones RDP. NLA se desactiva de forma predeterminada si usa FreeRDP. Debe tener instalada la versión adecuada de FreeRDP, junto con las revisiones correspondientes. Si desea obtener más información, consulte Instalar y configurar FreeRDP. **NOTA:** El programa `rdesktop` no es compatible con NLA.
Ninguna	`--printEnvironmentInfo`	Muestra información sobre el entorno de un dispositivo cliente, incluidos el nombre de dominio, de equipo, la dirección MAC y la dirección IP. En la pantalla completa, puede crear una cuenta para el cliente en función de la dirección MAC. Para mostrar la dirección MAC, debe usar esta opción con la opción `-s`. Ejemplo de cómo usar la opción de la línea de comandos: `--printEnvironmentInfo -s view.company.com`
Ninguna	`--usb=`	Especifica las opciones que se usarán para el redireccionamiento USB. Consulte Requisitos del sistema para la función de redireccionamiento USB.
Ninguna	`--version`	Muestra la información de la versión de Horizon Client.

Ejemplo: Ejemplo de pantalla completa

Entre los usuarios de pantalla completa, 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 de View. Aun así, se les solicitará a los usuarios que proporcionen credenciales de autenticación en algunas aplicaciones.

Para configurar la pantalla completa, debe usar la interfaz de la línea de comando `vdmadmin` en la instancia del servidor de conexión de View y realizar varios procedimientos que aparecen en el capítulo sobre la pantalla completa en el documento *Administración de View*. Tras configurar la pantalla completa, puede usar el comando `vmware-view` en un cliente Linux para conectarse a un escritorio de View en pantalla completa.

Para conectarse a escritorios de View desde clientes Linux en pantalla completa, 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=`

La pantalla completa no admite la omisión de estas opciones de configuración. Si el servidor de conexión de View se configura de forma que sea necesario un nombre de usuario de pantalla completa no predeterminado, debe también configurar la propiedad `view.defaultUser` o bien 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 pantalla completa predeterminado.

NOTA: Si configura la clave de configuración de `view.sslVerificationMode`, asegúrese de establecerla en el archivo `/etc/vmware/view-mandatory-config`. Cuando se ejecuta el cliente en pantalla completa, 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 del servidor de conexión y escritorio de View y no se le solicitan las 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 pantalla completa. 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 al servidor de conexión de View de nuevo.

```
./vmware-view --kioskLogin --nonInteractive --once --fullscreen --nomenubar
--serverURL="server.mycomany.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 de View, el usuario debe confirmar el mensaje antes de que se le permita acceder al escritorio. Para evitar este problema, utilice View Administrator para deshabilitar los mensajes previos al inicio de sesión.

Utilizar URI para configurar Horizon Client

Con los identificadores uniformes de recursos (URI), puede crear un correo electrónico o una página web con vínculos en los que los usuarios finales hacen clic para iniciar Horizon Client, conectarse a un servidor y abrir una aplicación o un escritorio específicos con opciones de configuración concretas.

Para simplificar el proceso de conexión a una aplicación o un escritorio remotos, cree vínculos web o de correo electrónico para los usuarios finales. 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 del servidor de conexión
- Número de puerto del servidor de conexión
- Nombre de usuario de Active Directory
- Nombre de dominio
- Nombre del escritorio o de la aplicación para mostrar
- Tamaño de la ventana
- Acciones (como restablecer e iniciar o cerrar sesión)
- Protocolo de visualización

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

NOTA: Puede utilizar URI para iniciar Horizon Client solo si el software cliente ya está instalado en equipos cliente.

Sintaxis para crear URI de vmware-view

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

Especificación de URI

Al crear un URI, básicamente está llamando a `vmware-view` con la cadena completa de URI de View 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`. En algunas versiones de determinados sistemas operativos cliente, el nombre del esquema distingue entre mayúsculas y minúsculas. Por lo tanto, utilice `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

Especifica 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

Especifica el escritorio o la aplicación. Utilice el nombre del escritorio o de la aplicación para mostrar. Este nombre es el que se especifica en Horizon Administrator al crear el grupo de aplicaciones o de escritorios. Si el nombre para mostrar contiene un espacio, utilice el mecanismo de codificación **%20** para representar el espacio.

query-part

Especifica las opciones de configuración que se van a utilizar o las acciones de la aplicación o el escritorio que se van a realizar. Las consultas no distinguen entre mayúsculas y minúsculas. Para utilizar varias consultas, utilice el signo et (&) entre ellas. Si se produce un conflicto entre ellas, se utilizará la última consulta de la lista. Utilice la siguiente sintaxis:

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

Consultas admitidas

En este tema, se incluyen las consultas admitidas para este tipo de Horizon Client. Si crea URI para varios tipos de clientes (por ejemplo, clientes móviles y de escritorio), consulte la guía *Uso de VMware Horizon Client* correspondiente a cada tipo de sistema cliente.

action

Tabla 2-3. Valores que se pueden utilizar con la consulta action

Valor	Descripción
`browse`	Muestra una lista de las aplicaciones y los escritorios disponibles y alojados en el servidor especificado. No tendrá que especificar un escritorio ni una aplicación al utilizar esta acción.
`start-session`	Abre la aplicación o el escritorio especificados. Si no se proporciona ninguna consulta action y se facilita el nombre de la aplicación o el escritorio, `start-session` es la acción predeterminada.
`reset`	Cierra y reinicia la aplicación remota o el escritorio 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.

Tabla 2-3. Valores que se pueden utilizar con la consulta action (Continua)

Valor	Descripción
`restart`	Cierra y reinicia el escritorio 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 guardaran antes de reiniciar.
`logoff`	Cierra la sesión del usuario en el sistema operativo invitado del escritorio remoto. Si especifica una aplicación, 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 agregarán al iniciar una aplicación remota. 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 remotas, los valores válidos son **`PCOIP`** y **`BLAST`**. Por ejemplo, para especificar PCoIP, utilice la sintaxis **`appProtocol=PCOIP`**.

desktopLayout

Establece el tamaño de la ventana que muestra un escritorio remoto. Para utilizar esta consulta, debe establecer la consulta `action` en **`start-session`** o bien no tener una consulta `action`.

Tabla 2-4. 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.
*W*x*H*	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	El nombre de dominio NETBIOS asociado al usuario que se conecta a la aplicación o al escritorio remotos. Por ejemplo, puede usar `mycompany` en lugar de `mycompany.com`.
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 primer servidor, lo que provocará que las sesiones de aplicaciones y escritorios 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`**.
unauthenticatedAccess Enabled	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`**.
unauthenticatedAccess Account	Establece la cuenta que se debe utilizar si la función Acceso sin autenticar está habilitada. 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

Es posible crear botones o vínculos de hipertexto con el esquema URI `vmware-view` e incluir estos vínculos en un correo electrónico o en una página web. Los usuarios finales pueden hacer clic en estos vínculos para, por ejemplo, abrir 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 inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio cuyo nombre para mostrar es **Escritorio primario** y el usuario inicia sesión en el sistema operativo cliente.

NOTA: Se utilizan el tamaño de ventana y el protocolo de visualización predeterminados. El protocolo de visualización predeterminado es PCoIP. El tamaño de ventana predeterminado es pantalla completa.

Es posible cambiar estos valores predeterminados. Consulte Utilizar los archivos de configuración y la interfaz de línea de comandos de Horizon Client.

2
```
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 el servidor de conexión. (El puerto predeterminado es 443). Dado que se proporciona el identificador del escritorio, este se abre aunque la acción `start-session` no se incluya en el URI.

3
```
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 inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **fred**. El usuario debe proporcionar el nombre de dominio y la contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio 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.

4
```
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 inicio de sesión, el usuario debe proporcionar el nombre de usuario, de dominio y la contraseña. Tras iniciar sesión correctamente, el cliente se conecta a la aplicación cuyo nombre para mostrar es **Calculadora**. La conexión utiliza el protocolo de visualización VMware Blast.

5
```
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 inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **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 cuyo nombre para mostrar es **Escritorio de finanzas** y el usuario inicia sesión en el sistema operativo cliente.

6
```
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`.

7
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. El cuadro 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 de escritorio para dicho escritorio.

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

Horizon Client se inicia y se conecta al servidor `view.mycompany.com`. El cuadro 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 reiniciar el Escritorio primario.

NOTA: Esta acción solo está disponible si Horizon Administrator habilitó la función de reinicio de escritorio para dicho escritorio.

9
```
vmware-view://
```

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

10
```
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 `Nuevo archivo.txt` al comando del inicio de la aplicación. El nombre del archivo aparece entre comillas dobles porque contiene espacios.

11
```
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.text b.txt` al comando del inicio de la aplicación. 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 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`.

12
```
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 que aparece como **Test Link** y un botón que aparece 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 la comprobación del certificado para usuarios finales

Los administradores pueden configurar el modo de verificación del certificado para que, por ejemplo, siempre se realice una verificación completa.

La comprobación del certificado se aplica a las conexiones SSL entre el servidor de conexión y Horizon Client. Los administradores pueden configurar el modo de verificación para usar una de las siguientes estrategias:

- Se permite a los usuarios finales elegir el modo de verificación. El resto de esta lista describe los tres modos de verificación.
- (Sin verificación) No se comprueban los certificados.
- (Advertir) Se advierte a los usuarios finales si el servidor presenta un certificado autofirmado. Los usuarios pueden elegir si desean permitir este tipo de conexión.
- (Seguridad completa) Se realiza una verificación completa y se rechazan las conexiones que dicha verificación no apruebe.

Para obtener más detalles acerca de los tipos de comprobación de verificación que se realizan, consulte Configurar el modo de comprobación del certificado en Horizon Client.

Use la propiedad `view.sslVerificationMode` para configurar el modo de verificación predeterminado:

- **1** implements `Full Verification`.
- **2** implements `Warn If the Connection May Be Insecure`.

- **3** implements `No Verification Performed`.

Para configurar el modo de forma que los usuarios finales no puedan cambiarlo, configure la propiedad `view.allowSslVerificationMode` como **`"False"`** en el archivo `/etc/vmware/view-mandatory-config` del sistema cliente. Consulte Opciones de la línea de comandos y configuración de Horizon Client.

Configurar las opciones avanzadas de TLS/SSL

Puede seleccionar los protocolos de seguridad y los algoritmos criptográficos que se utilizan para cifrar la comunicación entre Horizon Client y los servidores de Horizon o entre Horizon Client y el agente en el 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, se habilitan TLS v1.0, TLS v1.1 y TLS v1.2. No se admiten SSL v2.0 y v3.0.

NOTA: Si TLS v1.0 y RC4 están deshabilitados, el redireccionamiento USB no funciona cuando los usuarios están conectados a escritorios remotos de Windows XP. Tenga en cuenta el riesgo de seguridad si elige que esta función esté activa al habilitar TLS v1.0 y RC4.

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/SSL y de conexión.

IMPORTANTE: Al menos uno de los protocolos que habilitó en Horizon Client debe estar habilitado también en el escritorio remoto. De lo contrario, los dispositivos USB no se pueden redireccionar al escritorio remoto.

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 Horizon Client 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>scanCode
scanCode
```

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 2-5. 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

Tabla 2-5. Teclas multimedia (Continua)

Nombre de la tecla	Código de tecla
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 2-6. Teclas Hangul y Hanja

Nombre de la tecla	Código de tecla
HANGUL_ES	0x72
HANJA_ES	0x71
HANGUL_KO	0x172
HANJA_KO	0x171
HANGUL	0xF2
HANJA	0xF1

Tabla 2-7. 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 Horizon Client.

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\administrator'"`

  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.

Prerequisitos

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`. 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, está 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 y los escritorios remotos

3

Use Horizon Client para conectarse al servidor de conexión o a un servidor de seguridad, iniciar sesión o cerrarla en un escritorio remoto y usar las aplicaciones remotas. Para solucionar problemas, también puede restablecer las aplicaciones y los escritorios remotos.

Según el modo en que el administrador configure las directivas para los escritorios remotos, los usuarios finales podrán realizar varias operaciones en estos escritorios.

Este capítulo cubre los siguientes temas:

Conectarse a una aplicación o escritorio remotos

Después de iniciar sesión en un servidor, puede conectarse a las aplicaciones 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 utilizar aplicaciones remotas, debe conectarse al servidor de conexión de View 6.0 o a una versión posterior.

Prerequisitos

- 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, el nombre de usuario y el código de acceso de la autenticación 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 no utiliza un servidor de seguridad para acceder a la aplicación o escritorio remoto, compruebe que el dispositivo cliente está configurado para usar una conexión VPN y actívela.

  IMPORTANTE: En la mayoría de los casos, utilice un servidor de seguridad en lugar de una VPN.

- Compruebe que tiene un nombre de dominio completo (FQDN) del servidor que proporciona acceso a la aplicación o al escritorio remotos. 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 la opción de la directiva de grupo agente AllowDirectRDP está habilitada.

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. Haga doble clic en el botón **+ Agregar servidor** si aún no se ha agregado ningún servidor o haga clic en el botón **+ Servidor nuevo** en la barra de menús e introduzca el nombre del servidor de conexión o de un servidor de seguridad y haga clic en **Conectar**.

   Las conexiones entre Horizon Client y el servidor de conexión siempre utilizan SSL. El puerto predeterminado para las conexiones SSL es 443. Si el servidor de conexión no está configurado para utilizar el puerto predeterminado, utilice el formato que se muestra en este ejemplo: `view.company.com:1443`.

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

   NOTA: Una vez que se ha efectuado la conexión correctamente, se guarda un icono de este servidor en la ventana de inicio de Horizon Client. La próxima vez que utilice Horizon Client para conectarse al servidor, puede hacer doble clic en el icono o, si utiliza solo este servidor, puede hacer clic con el botón secundario en el icono del servidor y seleccionar **Conectarse automáticamente a este servidor** en el menú contextual.

3. Si se le solicita las credenciales RSA SecurID o las credenciales de la autenticación RADIUS, introduzca el nombre de usuario, el código de acceso y haga clic en **Aceptar**.

4 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, debe introducir el nombre de usuario con el formato **`dominio\nombre de usuario`** o **`nombre de usuario@dominio`**.

   b (Opcional) Seleccione un valor de dominio en el menú desplegable **Dominio**.

   c Haga clic en **Aceptar**.

5 Si el indicador de seguridad del escritorio se vuelve de color rojo y aparece un mensaje de advertencia, responda a la solicitud.

   Normalmente, esta advertencia significa que el servidor de conexión no envía una huella digital de certificado al cliente. La huella digital es un hash de la clave pública del certificado y se utiliza como su abreviatura.

6 (Opcional) Para configurar los ajustes de la pantalla para escritorios remotos, haga clic con el botón secundario en el icono del escritorio, o selecciónelo y haga clic en el icono **Configuración** (en forma de engranaje) junto al nombre del servidor situado en la parte superior de la ventana.

Opción	Descripción
Protocolo de visualización	Si lo permitió el administrador, puede usar la lista **Conectarse a través de** para seleccionar el protocolo de visualización. VMware Blast requiere Horizon Agent 7.0 o una versión posterior.
Diseño de pantalla	Use la lista **Pantalla** para seleccionar un tamaño de ventana o para usar varios monitores.

7 (Opcional) Para marcar una aplicación o un escritorio remotos como favorito, haga clic con el botón secundario y seleccione **Marcar como favorito** en el menú contextual que aparece.

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

8 Haga doble clic en una aplicación o un escritorio remotos 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.

La ventana del cliente se mostrará cuando se haya conectado.

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

- Determine si se ha configurado el servidor de conexión de View para que no use SSL. El software cliente necesita conexiones SSL. Compruebe si la configuración global de View Administrator correspondiente a la casilla de verificación **Usar SSL para conexiones de cliente** no se encuentra seleccionada. Si es así, debe seleccionar la casilla de verificación, de modo que se use SSL, o bien configurar su entorno de modo que los clientes puedan conectarse a un equilibrador de carga compatible con HTTPS u otro dispositivo intermedio que esté configurado para establecer una conexión HTTP al servidor de conexión de View.
- Verifique que el certificado de seguridad del servidor de conexión de View funcione correctamente. En caso contrario, en View Administrator, puede que también detecte que no es posible obtener acceso a View Agent en los escritorios. Estos son síntomas de problemas de conexión adicionales provocados por problemas con el certificado.
- Verifique que las etiquetas definidas en la instancia del servidor de conexión de View permiten el establecimiento de conexiones desde este usuario. Consulte el documento sobre *administración de View*.
- 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*.
- 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.

Prerequisitos

- Compruebe que el servidor de conexión de la versión 7.1 de Horizon 7 está configurado para acceso sin autenticar.
- Compruebe que se crearon sus usuarios de acceso sin autenticar en Horizon Administrator. 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 el servidor que necesita aún no está agregado, haga doble clic en el botón **+ Agregar servidor** si aún no se agregó ningún servidor o haga clic en el botón **+ Nuevo servidor** en la barra de menús para agregar un nuevo servidor, 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 la lista 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 Haga doble clic en una de las aplicaciones publicadas para iniciarla.

Se mostrará la ventana de la aplicación.

6 Salga de la aplicación publicada 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.

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

Puede configurar Horizon Client para compartir carpetas y unidades de sus sistema local con aplicaciones y escritorios remotos. Las unidades pueden incluir unidades asignadas y dispositivos de almacenamiento USB. Esta función se denomina redireccionamiento de unidades cliente.

En un escritorio remoto de Windows, las unidades y carpetas compartidas aparecen en la sección **Dispositivos y unidades** de la carpeta **Este equipo**, o bien en la sección **Otro** de la carpeta **Equipo**, según la versión del sistema operativo. En una aplicación remota, como el Bloc de notas, puede explorar y abrir un archivo que se encuentre en una unidad o carpeta compartida. Las carpetas y unidades que seleccione para compartir se muestran en el sistema de archivos como unidades de red que usan la nomenclatura ***nombre* en *NOMBRE DEL EQUIPO***.

No es necesario estar conectado a una aplicación o escritorio remoto para configurar el redireccionamiento de unidades cliente. La configuración se aplica a todas las aplicaciones y escritorios remotos. Es decir, no puede definir la configuración de modo que las carpetas locales del cliente se compartan con una aplicación o un escritorio remotos, pero no con otras aplicaciones o escritorios remotos.

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`

Configurar el navegador en el sistema cliente para que use un servidor proxy podría provocar un rendimiento deficiente del redireccionamiento de unidades cliente si el túnel seguro está habilitado en la instancia del servidor de conexión. Para que el rendimiento del redireccionamiento de unidades cliente sea óptimo, configure el navegador para que use un servidor proxy no detecte automáticamente la configuración de la red LAN.

Prerequisitos

Para compartir carpetas y unidades con una aplicación o un escritorio remotos, es necesario que habilite la función de redireccionamiento de unidades cliente. Esta tarea incluye la instalación de View Agent 6.1.1 o posterior, o Horizon Agent 7.0 o posterior, así como habilitar la opción de **redireccionamiento de unidades cliente** del agente. También puede implicar la configuración de directivas o del 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*.

En las distribuciones de Ubuntu 16.04 x64, la biblioteca `libglibmm-2.4.so.1.3.0` incluida en la distribución es incompatible con la implementación actual del redireccionamiento de unidades de cliente (CDR). Para saltarse esta limitación, copie el archivo de la biblioteca `libglibmm-2.4.so.1.3.0` desde una distribución de Ubuntu14.04 x64 hasta su distribución de Ubuntu 16.04 x64.

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 o escritorio, 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 que se muestra al conectarse a un escritorio o aplicación	Haga clic en **Permitir** para compartir su directorio de inicio, o en **Denegar** para no hacerlo.
Desde un SO de escritorio	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 y escritorios remotos	Haga clic en el botón **Agregar**, desplácese hasta la carpeta o unidad que desee compartir, selecciónela, y haga clic en **Aceptar**. **NOTA:** No puede compartir una carpeta que se encuentre en un dispositivo USB si el dispositivo ya está conectado a una aplicación o a un escritorio remotos mediante la función de redireccionamiento 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 y 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*.
Compartir dispositivo de almacenamiento USB con aplicaciones y escritorios remotos	Seleccione la casilla de verificación **Permitir acceso a almacenamiento extraíble**. La función de redireccionamiento de unidades cliente comparte automáticamente todos los dispositivos de almacenamiento USB insertados en el sistema cliente y todas las unidades externas FireWire y Thunderbolt conectadas. No tiene que seleccionar un dispositivo específico para compartir. **NOTA:** No se compartirán los dispositivos de almacenamiento que ya se encuentren conectados a una aplicación o a un escritorio remotos con la función de redireccionamiento USB. Si esta casilla de verificación no está seleccionada, puede usar la función de redireccionamiento USB para conectar dispositivos de almacenamiento USB a aplicaciones y escritorios remotos.
No mostrar el cuadro de diálogo Compartir al conectarse a una aplicación o a un escritorio remotos	Seleccione la casilla de verificación **No mostrar el cuadro de diálogo al conectarse a un escritorio o una aplicación**. Si no se selecciona esta casilla de verificación, el cuadro de diálogo Compartir se mostrará la primera vez que se conecte a un escritorio o aplicación después de haberse conectado a un servidor. Por ejemplo, si inicia sesión en un servidor y se conecta a un escritorio, se mostrará el cuadro de diálogo Compartir. Si a continuación se conecta a otro escritorio o aplicación, no se volverá a mostrar el cuadro de diálogo. Para que se muestre el cuadro de diálogo de nuevo, deberá desconectarse del servidor e iniciar sesión otra vez.

Qué hacer a continuación

Verifique que puede ver las carpetas compartidas desde la aplicación o el escritorio remotos:

- En un escritorio remoto Windows, abra el explorador de archivos y busque en la sección **Dispositivos y unidades** de la carpeta **Este equipo**; o bien, abra el Explorador de Windows y busque en la sección **Otro** de la carpeta **Equipo**.
- En una aplicación remota, si corresponde, seleccione **Archivo > Abrir** o **Archivo > Guardar como** y desplácese hasta la carpeta o unidad, que aparece en el sistema de archivos como una unidad de red con la nomenclatura ***nombre de carpeta* en *NOMBRE DEL EQUIPO***.

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
   ```

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

Los administradores y, en ocasiones, los usuarios finales pueden configurar si las conexiones de cliente se rechazan en caso de que se produzca un error en una o varias comprobaciones de los certificados del servidor.

La comprobación del certificado se aplica a las conexiones SSL entre el servidor de conexión y Horizon Client. La verificación de los certificados 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.

NOTA: 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.

Además de presentar un certificado del servidor, el servidor de conexión también envía una huella digital del certificado a Horizon Client. La huella digital es un hash de la clave pública del certificado y se utiliza como su abreviatura. Si el servidor de conexión no envía una huella digital, aparecerá una advertencia que informa de que la conexión no es de confianza.

Puede establecer el modo de comprobación del certificado si su administrador lo ha permitido. Seleccione **Archivo > Preferencias** desde la barra de menú. Tiene tres opciones:

- **No conectarse nunca a servidores que no sean de confianza**. Si se produce un error en las comprobaciones de los certificados, el cliente no puede conectarse al servidor. Aparece un mensaje de error con las comprobaciones que han fallado.

- **Advertirme antes de conectarme a servidores que no sean de confianza**. Si se produce un error en una comprobación del certificado porque el servidor utiliza un certificado autofirmado, puede hacer clic en **Continuar** para ignorar la advertencia. En lo que respecta a los certificados autofirmados, el nombre del certificado no tiene que coincidir con el nombre del servidor introducido en Horizon Client.
- **No comprobar los certificados de identidad de los servidores**. Esta opción significa que no se ha llevado a cabo ninguna comprobación del certificado.

Cambiar escritorios o aplicaciones

Si está conectado a un escritorio remoto, puede cambiar a otro. También se puede conectar a aplicaciones remotas 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	Realice una de las siguientes acciones: ■ 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	Realice cada una de las siguientes acciones: ■ 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

Con algunas configuraciones, si se desconecta desde un escritorio remoto sin cerrar sesión, las aplicaciones de dicho escritorio permanecerán abiertas. También se puede desconectar desde un servidor y dejar las aplicaciones remotas en ejecución.

Aunque no tenga ningún escritorio remoto abierto, puede cerrar sesión en el sistema operativo del escritorio remoto. Utilizar esta función tiene el mismo resultado que si envía la secuencia Ctrl+Alt+Supr al escritorio 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.
Elegir un escritorio remoto diferente del mismo servidor	Seleccione **Escritorio > Desconectar** en la barra de menú.
Elegir un escritorio remoto diferente en un servidor diferente	Seleccione **Archivo > Desconectarse del servidor** en la barra de menú.

  NOTA: El administrador puede configurar el escritorio para cerrar sesión de forma automática cuando se desconecte. En ese caso, se detendrán todos los programas abiertos en el escritorio.

- Cerrar sesión y desconectarse desde un escritorio remoto.

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

- Cerrar sesión cuando no tenga ningún escritorio remoto abierto.
  a 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.
  b 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 cerrarán sin guardar.

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

4

Horizon Client para Linux es compatible con muchas funciones.

Este capítulo cubre los siguientes temas:

- Matriz de compatibilidad de funciones para Linux
- Internacionalización
- Teclados y monitores
- Conectar dispositivos USB
- Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos
- Guardar documentos en una aplicación remota
- Configurar las preferencias de impresión para la función de impresora virtual en un escritorio remoto
- Copiar y pegar texto

Matriz de compatibilidad de funciones para Linux

Algunas funciones son compatibles en un tipo de Horizon Client pero no en otro.

Cuando planifique el protocolo de visualización y las funciones que estarán disponibles para el usuario final, utilice la siguiente información para determinar qué sistema operativo cliente admite la función.

Tabla 4-1. Funciones de escritorio remoto admitidas por los clientes Linux

Función	Escritorio de Windows XP (View Agent 6.0.2 y versiones anteriores)	Escritorio de Windows Vista (View Agent 6.0.2 y versiones anteriores)	Escritorio de Windows 7	Escritorio de Windows 8.x	Escritorio de Windows 10	Escritorios de Windows Server 2016 o Windows Server 2008/2012 R2
Redireccionamiento USB	Limitado	Limitado	X	X	X	X
Audio/vídeo en tiempo real (RTAV)	Limitado	Limitado	X	X	X	X
Redireccionamiento del escáner						

Tabla 4-1. Funciones de escritorio remoto admitidas por los clientes Linux (Continua)

Función	Escritorio de Windows XP (View Agent 6.0.2 y versiones anteriores)	Escritorio de Windows Vista (View Agent 6.0.2 y versiones anteriores)	Escritorio de Windows 7	Escritorio de Windows 8.x	Escritorio de Windows 10	Escritorios de Windows Server 2016 o Windows Server 2008/2012 R2
Redireccionamiento del puerto serie						
Protocolo de visualización RDP	Limitado	Limitado	X	X	X	X
Protocolo de visualización PCoIP	Limitado	Limitado	X	X	X	X
Protocolo de visualización VMware Blast			X	X	X	X
Persona Management						
Wyse MMR	Solo sistemas cliente de partners y únicamente con RDP	Solo sistemas cliente de partners y únicamente con RDP				
Redireccionamiento multimedia (MMR) de Windows Media			X	X	X	
Impresión según ubicación	Limitado	Limitado	X	X	X	X
Impresión virtual	Limitado	Limitado	X	X	X	X
Tarjetas inteligentes	Limitado	Limitado	X	X	X	X
RSA SecurID o RADIUS	Limitado	Limitado	X	X	X	X
Single Sign-On	Limitado	Limitado	X	X	X	X
Varios monitores	Limitado	Limitado	X	X	X	X
Redireccionamiento de unidades cliente			X	X	X	X

Los escritorios de Windows 10 necesitan la versión de View Agent 6.2 o una versión posterior. Los escritorios de Windows Server 2012 R2 necesitan View Agent 6.1 o una versión posterior. 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.

IMPORTANTE: View Agent 6.1 y las versiones posteriores no son compatibles con los escritorios de Windows XP y Windows Vista. View Agent 6.0.2 es la versión más reciente de View compatible con estos sistemas operativos invitados. Los clientes que tengan un acuerdo de compatibilidad ampliado con Microsoft para Windows XP y Vista y un acuerdo de compatibilidad ampliado con VMware para estos sistemas operativos de invitado pueden implementar la versión 6.0.2 de View Agent de sus escritorios de Windows XP y Vista con el servidor de conexión de View 6.1.

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 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 4-2. Funciones compatibles con hosts RDS con View Agent 6.0.x o posterior, o Horizon Agent 7.0.x o posterior, instalados

Función	Host RDS con Windows Server 2008 R2	Host RDS con Windows Server 2012	Host RDS con Windows Server 2016
RSA SecurID o RADIUS	X	X	Horizon Agent 7.0.2 y posterior
Tarjeta inteligente	View Agent 6.1 y posterior	View Agent 6.1 y posterior	Horizon Agent 7.0.2 y posterior
Single Sign-On	X	X	Horizon Agent 7.0.2 y posterior
Protocolo de visualización de RDP (para clientes de escritorio)	X	X	Horizon Agent 7.0.2 y posterior
Protocolo de visualización PCoIP	X	X	Horizon Agent 7.0.2 y posterior
Protocolo de visualización VMware Blast	Horizon Agent 7.0 y posterior	Horizon Agent 7.0 y posterior	Horizon Agent 7.0.2 y posterior
HTML Access	View Agent 6.0.2 y posterior (solo máquinas virtuales)	View Agent 6.0.2 y posterior (solo máquinas virtuales)	Horizon Agent 7.0.2 y posterior
Redireccionamiento multimedia (MMR) de Windows Media	View Agent 6.1.1 y posterior	View Agent 6.1.1 y posterior	Horizon Agent 7.0.2 y posterior
Redireccionamiento de unidades cliente	View Agent 6.1.1 y posterior	View Agent 6.1.1 y posterior	Horizon Agent 7.0.2 y posterior
Impresión virtual (para clientes de escritorio)	View Agent 6.0.1 y posterior (solo máquinas virtuales)	View Agent 6.0.1 y posterior (solo máquinas virtuales)	Horizon Agent 7.0.2 y posterior (solo máquinas virtuales)

Tabla 4-2. Funciones compatibles con hosts RDS con View Agent 6.0.x o posterior, o Horizon Agent 7.0.x o posterior, instalados (Continua)

Función	Host RDS con Windows Server 2008 R2	Host RDS con Windows Server 2012	Host RDS con Windows Server 2016
Impresión según ubicación	View Agent 6.0.1 y posterior (solo máquinas virtuales)	View Agent 6.0.1 y posterior (solo máquinas virtuales)	Horizon Agent 7.0.2 y posterior (solo máquinas virtuales)
Varios monitores (para clientes de escritorio)	X	X	Horizon Agent 7.0.2 y posterior
Unity Touch (para clientes móviles y Chrome OS)	X	X	Horizon Agent 7.0.2 y posterior
Audio/vídeo en tiempo real (RTAV)	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.3 y posterior

Para obtener información sobre qué service pack o qué ediciones de cada sistema operativo invitado son compatibles, consulte el documento *Instalación de View*.

Limitaciones en funciones específicas

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

Tabla 4-3. Requisitos para funciones específicas

Función	Requisitos
Audio/vídeo en tiempo real	■ Para un software cliente de terceros, esta función requiere View 5.2 con Feature Pack 2 o una versión posterior. ■ Para Horizon Client de VMware, esta función necesita View Agent 6.0.2 o una versión posterior. Son necesarios los protocolos de visualización VMware Blast o PCoIP.
Impresión virtual e impresión según ubicación para escritorios de Windows Server 2008 R2, escritorios de RDS (en hosts RDS de máquinas virtuales) y aplicaciones remotas	■ Para software cliente de terceros, esta función requiere Horizon 6.0.1 con View o una versión posterior. ■ Para Horizon Client de VMware, esta función necesita View Agent 6.0.2 o una versión posterior. Son necesarios los protocolos de visualización VMware Blast o PCoIP.
Redireccionamiento USB	■ Para software cliente de terceros, esta función requiere View 5.1 o una versión posterior. ■ Para Horizon Client de VMware, esta función necesita View Agent 6.0.2 o una versión posterior. Son necesarios los protocolos de visualización VMware Blast o PCoIP.

Tabla 4-3. Requisitos para funciones específicas (Continua)

Función	Requisitos
Tarjetas inteligentes	Para escritorios de máquinas virtuales de usuario único, esta función requiere View Agent 6.0.2 o una versión posterior. Para los escritorios basados en sesiones proporcionados por hosts RDS, esta función requiere View Agent 6.1 o una versión posterior.
Redireccionamiento de unidades cliente	View Agent 6.1.1 o posterior.

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.

Puede utilizar aplicaciones remotas únicamente si está conectado al servidor de conexión 6.0 o posterior. Para obtener más información sobre los sistemas operativos que admite el host RDS, el cual proporciona aplicaciones y escritorios publicados, consulte el documento *Instalación de View*.

NOTA: Las funciones que están disponibles para cada dispositivo cliente ligero están determinadas por el proveedor, así como el modelo y la configuración que una empresa elije utilizar. 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 View*.

Compatibilidad de funciones para los escritorios de Linux

Algunos sistemas operativos invitados de Linux son compatibles si cuentan con View Agent 6.1.1 o bien con una versión posterior. 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*.

Internacionalización

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

Si utiliza un sistema cliente Linux Ubuntu 10.4 y desea que la interfaz del usuario cliente aparezca en otro idioma que no sea inglés, debe configurar el sistema cliente para que use una configuración regional con la codificación UTF-8.

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 aparecerá 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 aparecerá en el monitor de la derecha porque ese es el monitor que está situado más arriba/izquierda.
- Puede usar hasta 4 monitores si cuenta con RAM de vídeo suficiente.

  Para usar más de 2 monitores para mostrar el escritorio remoto en un sistema cliente Ubuntu, debe configurar la opción `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 2 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 4.0 y utiliza más de 2 monitores, dichos monitores deben estar en el mismo modo y deben tener la misma resolución de pantalla. Esto significa que si usa 3 monitores, todos los monitores deben estar en modo horizontal o vertical y deben 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 2 monitores.

- Si especifica que desea usar todos los monitores y utiliza los protocolos de visualización VMware Blast o PCoIP, puede especificar también un subgrupo de monitores adyacentes para utilizarlo. Para ello, haga clic con el botón secundario en la ventana de selección del escritorio, seleccione **Pantalla completa - Todos los monitores** en la lista desplegable **Pantalla** y, a continuación, haga clic para seleccionar los monitores que desea usar.

  NOTA: Si cuenta con un sistema cliente Ubuntu, debe seleccionar el monitor situado en la parte superior izquierda como uno de los monitores. Por ejemplo, si tiene 4 monitores apilados 2 X 2, debe seleccionar los 2 monitores en la parte superior o los 2 monitores 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 2 monitores, puede ajustar la resolución de cada monitor de forma separada, con una resolución de hasta 2560x1600 por pantalla. Si utiliza más de 2 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

  El escritorio remoto debe tener instalado View Agent 6.2 o posterior, o Horizon Agent 7.0 o posterior. Para obtener un rendimiento óptimo, 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

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 View Agent. Utilice la directiva para **activar la sincronización del PCoIP del idioma de entrada predeterminado del usuario**, disponible como parte del archivo de plantilla ADM de variables de la sesión PCoIP 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 del administrador de ventanas que utilice, VMware le recomienda desactivar el protector de pantalla en el escritorio remoto y no especificar el tiempo de suspensión.

Conectar dispositivos USB

Puede acceder a dispositivos USB conectados de forma local como por ejemplo, unidades de memoria flash o cámaras e impresoras, desde un escritorio remoto. Esta función se denomina redireccionamiento USB.

Con esta función, la mayoría de dispositivos USB conectados al sistema de cliente local están disponibles en un menú de Horizon Client. Este menú permite conectar y desconectar los dispositivos.

El uso de dispositivos USB con escritorios remotos tiene las limitaciones siguientes:

- Al obtener acceso a un dispositivo USB desde un menú de Horizon Client y usar el dispositivo en un escritorio remoto, no podrá obtener acceso al dispositivo en el equipo local.
- Los dispositivos USB que no aparezcan en el menú, pero que están disponibles en un escritorio remoto, incluyen dispositivos de interfaz humana como teclados y dispositivos señaladores. El escritorio remoto y el equipo local usan estos dispositivos de forma simultánea. La interacción con estos dispositivos 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.
- Algunos dispositivos USB requieren controladores específicos. Si un controlador requerido aún no está instalado en un escritorio remoto, puede que se le pida que lo instale al conectar el dispositivo USB al escritorio remoto.

- Si tiene previsto conectar dispositivos USB que usen controladores MTP como tablets y smartphones Samsung con Android, debe configurar Horizon Client para que conecte automáticamente los dispositivos USB a su escritorio remoto. 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.
- Las cámaras web no son compatibles con el redireccionamiento USB a través del menú **Conectar dispositivo USB**. Para usar un dispositivo de entrada de audio o cámara web, deberá usar la función Audio/vídeo en tiempo real. Esta función se encuentra disponible cuando se utiliza junto con View 5.2 Feature Pack 2 o posterior. Consulte Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos.
- 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. Si tiene la función Audio/vídeo en tiempo real incluida en View 5.2 Feature Pack 2 o posterior, los dispositivos de entrada y salida de audio funcionarán de forma óptima con esa función y no necesitará utilizar el redireccionamiento USB con ellos.

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

NOTA: No redirija dispositivos USB como dispositivos USB Ethernet y de pantalla táctil al escritorio remoto. Si redirige un dispositivo USB Ethernet, su sistema cliente perderá la conectividad de red. Si redirige un dispositivo de pantalla táctil, el escritorio remoto recibirá la entrada táctil, pero no la del teclado. Si ha configurado el escritorio virtual para que conecte dispositivos USB automáticamente, puede configurar una directiva para excluir dispositivos específicos. Consulte el tema "Configurar los ajustes de directiva de filtro para dispositivos USB" del documento *Configurar funciones de escritorios remotos en Horizon 7*.

IMPORTANTE: Este procedimiento describe cómo usar el menú de Horizon Client para conectar dispositivos USB y configurar que se conecten de forma automática. 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 Requisitos del sistema para la función de redireccionamiento USB. Para obtener más información sobre la creación de directivas de grupo, consulte el documento sobre *configuración de grupos de aplicaciones y escritorios en View*.

Prerequisitos

- Para usar dispositivos USB con un escritorio remoto, View Administrator debe tener la función USB habilitada para el escritorio remoto.

  Esta tarea incluye la instalación del componente de **redireccionamiento USB** del agente, y puede incluir la configuración de directivas relacionadas con el redireccionamiento USB. Para obtener más información, consulte el documento *Administración de View* si usa el servidor de conexión y la versión 5.3.x de Agent. Consulte *Configurar funciones de escritorios remotos en Horizon 7* si usa la versión 6.0 o posterior del agente y el servidor de conexión.

- Al instalar Horizon Client, se debió instalar también el componente de **redireccionamiento USB**. 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**.

Procedimiento

- Conecte manualmente el 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 redirige manualmente desde el sistema local al escritorio remoto.
- Conecte el dispositivo USB a una aplicación alojada de forma remota.
  a En la ventana de selección de aplicaciones y escritorios, abra la aplicación remota.

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

    Ahora puede usar el dispositivo USB con la aplicación remota. El dispositivo USB no queda liberado inmediatamente después de cerrar la aplicación.
  f Cuando haya terminado de usar la aplicación, para liberar el dispositivo USB con el fin de obtener acceso a él desde el sistema local, de nuevo en la ventana de selección de aplicaciones y escritorios, abra la ventana Configuración, seleccione **Dispositivos USB** y, a continuación, **Desconectarse**.
- Configure Horizon Client para conectar los dispositivos USB automáticamente al escritorio remoto cuando se inicie Horizon Client.

  Esta opción está seleccionada de manera predeterminada.
  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. 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 al escritorio remoto al insertarlos en el sistema local.

  Habilite esta opción si tiene previsto conectar dispositivos que utilicen controladores MTP como tablets y smartphones Samsung con Android. Esta opción está seleccionada de manera predeterminada.

  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.

También puede configurar si desea conectar automáticamente dispositivos USB mediante las opciones del archivo de configuración `view.usbAutoConnectAtStartup` y `view.usbAutoConnectOnInsert`. Para obtener más información, consulte Opciones de la línea de comandos y configuración de Horizon Client.

Si pasados unos minutos el dispositivo USB no aparece en el escritorio, desconéctelo del equipo cliente y vuelva a conectarlo.

Qué hacer a continuación

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*.

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 equipo local en su escritorio remoto. Esta función es compatible con las aplicaciones de conferencias estándares y las aplicaciones de vídeo basadas en el explorador. Además, admite entrada de audio analógica, dispositivos de audio USB y cámaras web estándar.

Para obtener más información sobre cómo configurar la función Audio/vídeo en tiempo real, la velocidad de fotogramas y la resolución de la imagen en un escritorio remoto, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*. Para obtener información sobre cómo configurar estos ajustes en los sistemas cliente, consulte el artículo de la base de conocimiento de VMware *Configurar la velocidad de fotogramas y la resolución para la función Audio/vídeo en tiempo real en Horizon View Clients*, disponible en la página http://kb.vmware.com/kb/2053644.

Para descargar una aplicación de prueba que verifique la correcta instalación y funcionamiento de la función Audio/vídeo en tiempo real, acceda a la página http://labs.vmware.com/flings/real-time-audio-video-test-application. Esta aplicación de prueba está disponible como VMware Fling y, por tanto, no podrá disponer de soporte técnico.

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 puede utilizar su cámara web

Si un Horizon Administrator configuró la función Audio/vídeo en tiempo real (y si utiliza el protocolo de visualización de VMware Blast o de PCoIP), puede utilizar una cámara web en su escritorio que esté integrada o conectada a su equipo local. 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 el escritorio remoto, puede elegir dispositivos de entrada y salida desde los menús en la aplicación. Para los escritorios de las máquinas virtuales, puede elegir el micrófono virtual de VMware y la cámara web virtual de VMware. Para los escritorios publicados, puede elegir el dispositivo de audio remoto y la cámara web virtual de VMware.

Sin embargo, esta función se puede utilizar con un gran número de aplicaciones sin necesidad de seleccionar un dispositivo de entrada.

Si su equipo local está utilizando actualmente la cámara web, esta no podrá ser utilizada simultáneamente por el escritorio remoto. Además, si el escritorio remoto está utilizando la cámara web, esta no podrá ser utilizada simultáneamente por su equipo local.

IMPORTANTE: Si está utilizando una cámara web USB, su administrador no debe configurar el cliente para reenviar automáticamente dispositivos a través de redireccionamiento USB. Si la cámara web se conecta a través de un redireccionamiento USB, el rendimiento no será adecuado para realizar una videollamada.

Si tiene más de una cámara web conectada a su equipo local, puede configurar una cámara web preferida para utilizarla en su escritorio remoto.

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 Horizon 7. 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 analógica.

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.

Prerequisitos

- 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 Horizon 7. 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.

Prerequisitos

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.

Guardar documentos en una aplicación remota

Con determinadas aplicaciones remotas como, por ejemplo, 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.

Los administradores pueden utilizar un archivo de plantilla ADMX para establecer una directiva de grupo que especifique la ubicación en la que se guardarán los documentos. Esta directiva se denomina **Establecer directorio principal de usuario de Servicios de Escritorio remoto**. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Configurar las preferencias de impresión para la función de impresora virtual en un escritorio remoto

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. 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, etc.

IMPORTANTE: La función de impresión virtual solo está disponible en Horizon Client 3.2 o en una versión posterior disponible en la página web de descargas de los productos de VMware o con la versión de Horizon Client para Linux proporcionada por otros proveedores.

Esta función también cuenta con los siguientes requisitos:

- El escritorio remoto debe tener instalado View Agent 6.0.2 o una versión posterior, o Horizon Agent 7.0 o una versión superior.
- Debe utilizar el protocolo de visualización de 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. Los usuarios que tienen privilegios de administrador pueden instalar controladores de impresión en el escritorio remoto sin crear un conflicto con el componente de la 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 de impresión 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.

Este procedimiento se aplica a un escritorio remoto que tenga los sistemas operativos Windows 7 o Windows 8.x (Escritorio). Se emplea un procedimiento similar (pero no exactamente el mismo) para Windows Server 2008 y Windows Server 2012.

Prerequisitos

Compruebe que el componente de la impresión virtual del agente está instalado en el escritorio remoto. En el sistema de archivos del escritorio remoto, compruebe que exista la siguiente carpeta: `C:\Program Files\Common Files\ThinPrint`.

Para usar la impresión virtual, el administrador de Horizon debe habilitar dicha función para 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 relativas al comportamiento de la impresión virtual. Para obtener más información, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

1. En el escritorio remoto de Windows 7 o Windows 8.x, haga clic en **Inicio > Dispositivos e impresoras**.
2. En la ventana Dispositivos e impresoras, haga clic con el botón secundario en la impresora predeterminada, seleccione **Propiedades de impresora** en el menú contextual y seleccione la impresora.

   Las impresoras virtuales aparecen como *<nombre_impresora>* en los escritorios de máquinas virtuales de usuario único y como *<nombre_impresora>(s<ID_sesión>)* en los escritorios publicados en los hosts de RDS si está instalado View Agent 6.2 o una versión posterior, o bien Horizon Agent 7.0 o una versión posterior. Si está instalado View Agent 6.1 o una versión anterior en el escritorio remoto, las impresoras virtuales aparecen como *<printer_name>#:<number>*.
3. En la ventana Propiedades de impresora, haga clic en la pestaña **Instalación del dispositivo** y especifique qué configuración utilizar.
4. En la pestaña **General**, haga clic en **Preferencias** y especifique qué configuración utilizar.
5. En el cuadro de diálogo Preferencias de impresión, seleccione las diferentes pestañas y especifique qué configuración utilizar.

   En la configuración avanzada **Ajuste de página**, VMware le recomienda que mantenga la configuración predeterminada.
6. Haga clic en **Aceptar**.

Copiar y pegar texto

Es posible realizar operaciones de copiado y pegado en las aplicaciones y los escritorios remotos. View Administrator puede establecer esta función para que sea posible realizar estas operaciones desde su sistema cliente a una aplicación o un escritorio remotos, así como desde una aplicación o un escritorio remotos a su sistema cliente, o ninguna o ambas posibilidades.

Esta función está disponible si utiliza los protocolos de visualización VMware Blast o PCoIP. Las aplicaciones remotas son compatibles con Horizon 6.0 o versiones posteriores.

Los administradores configuran la posibilidad de copiar y pegar utilizando los objetos de directiva de grupo (GPO) que pertenecen a View Agent o a Horizon Agent en los escritorios remotos. Para obtener más información, consulte el capítulo sobre cómo configurar directivas en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Puede copiar texto de Horizon Client a una aplicación o escritorio remotos o viceversa, pero el texto pegado será 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=value
```

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 un valor, el tamaño de 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 `~/.vmware/config`

2 `/usr/lib/vmware/config`

3 `/etc/vmware/config`

En función de la red, si el tamaño de la memoria del portapapeles cliente 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.

Solucionar problemas relacionados con Horizon Client 5

Puede resolver la mayoría de problemas con Horizon Client reiniciando o restableciendo el escritorio o reinstalando la aplicación VMware Horizon Client.

Este capítulo cubre los siguientes temas:

Problemas con la entrada de teclado

Si al escribir en una aplicación o un escritorio remotos ninguna de las pulsaciones de teclas funcionan, el problema puede estar relacionado con el software de seguridad del sistema cliente local.

Problema

Mientras se encuentra conectado a una aplicación o un escritorio remotos, no aparece ningún carácter cuando escribe. Otro síntoma puede ser que se mantenga una única tecla repitiéndose.

Origen

Algunos programas de seguridad, como Norton 360 Total Security, incluyen una función que detecta programas registradores de pulsaciones de teclas y bloquea el registro de estas pulsaciones. Esta función de seguridad se emplea para proteger el sistema contra spyware no deseados que, por ejemplo, roban las contraseñas y los números de las tarjetas de crédito. Desgraciadamente, este software de seguridad no permite que Horizon Client envíe pulsaciones de teclas a la aplicación o al escritorio remotos.

Solución

- En el sistema cliente, desactive la función de detección del registrador de pulsaciones de teclas del antivirus o del software de seguridad.

Conexión a un servidor en el modo Workspace ONE

Si no puede conectarse a un servidor directamente a través de Horizon Cliento si las autorizaciones de aplicaciones y escritorios no están visibles en Horizon Client, es posible que el modo Workspace ONE esté habilitado en el servidor.

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 o aplicación mediante un URI o un acceso directo o al abrir un archivo local a través de la asociación de archivos, la solicitud le redireccionará al portal de Workspace ONE para autenticarse.
- Después de que abra un escritorio o una aplicación a través de Workspace ONE y se inicie Horizon Client, no podrá ver ni abrir otros escritorios o aplicaciones remotos autorizados en Horizon Client.

Origen

A partir de la versión 7.2 de Horizon 7, un administrador podrá 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 y escritorios remotos.

Reiniciar un escritorio remoto

Es posible que tenga que reiniciar un escritorio remoto si el sistema operativo del escritorio deja de responder. Reiniciar un escritorio remoto es el equivalente del comando de reinicio del sistema operativo Windows. El sistema operativo del escritorio normalmente le pide que guarde los datos que no haya guardado antes de reiniciar.

Puede reiniciar un escritorio remoto solo si un administrador de Horizon ha habilitado la función de reinicio de escritorio 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
Desde dentro del escritorio	Seleccione **Conexión > Reiniciar escritorio** de la barra de menús.
Desde la ventana de selección de escritorios	Seleccione el escritorio remoto y seleccione **Conexión > Reiniciar escritorio** en la barra de menús.

  Horizon Client le pide que confirme la acción de reinicio.

Se reinicia el sistema operativo del escritorio remoto y Horizon Client se desconecta y cierra la sesión del escritorio.

Qué hacer a continuación

Espere un periodo de tiempo apropiado para que se inicie 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 un escritorio remoto o aplicaciones remotas.

Restablecer un escritorio remoto o aplicaciones remotas

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. Al restablecer las aplicaciones remotas, se sale de todas las aplicaciones abiertas.

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.

Restablecer las aplicaciones remotas es equivalente a salir de todas las aplicaciones sin guardar. Se cierran todas las aplicaciones abiertas, incluso las que proceden de diferentes granjas de servidores RDS.

Solo puede restablecer un escritorio remoto si un administrador de Horizon ha habilitado la función de restablecimiento de escritorio 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	Seleccione el escritorio remoto y, a continuación, seleccione **Conexión > Restablecer** en la barra de menú.
Restablecer una aplicación remota desde la ventana para seleccionar la aplicación y el escritorio	Haga clic en el botón **Configuración** (icono de rueda dentada) situado en la esquina superior derecha de la ventana, seleccione **Aplicaciones** en el panel izquierdo, haga clic en **Restablecer** y, a continuación, haga clic en **Continuar**.

Cuando restablezca un escritorio remoto, el sistema operativo del escritorio remoto se reinicia y Horizon Client desconecta y cierra la sesión del escritorio. Cuando restablece aplicaciones remotas, se sale de las aplicaciones.

Qué hacer a continuación

Espere un periodo de tiempo apropiado para iniciar el sistema antes de intentar volver a conectarse a la aplicación o el escritorio remoto.

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.

Prerequisitos

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-yyyyyyy.arch.bundle -u vmware-horizon-client
```

En el nombre del archivo, *x.x.x* es el número de la versión, *yyyyyyy* es el número de compilación y *arq* 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.

Qué hacer a continuación

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.

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 View Agent 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 cubre los siguientes temas:

Requisitos del sistema para la función de redireccionamiento USB

La función de redireccionamiento USB solo está disponible en algunas versiones del software cliente.

Para el software Horizon Client que proporcionan los proveedores de terceros, la función de redireccionamiento USB tiene los siguientes requisitos:

- La versión del servidor de conexión de View y View Agent debe ser View 5.1 o una posterior.
- Las funciones de filtrado USB y de división de dispositivos que se describen en este documento están disponibles en la versión 5.1 del servidor de conexión de View y en versiones posteriores.

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 Horizon Client, la función de redireccionamiento USB tiene los siguientes requisitos:

- El escritorio remoto debe tener instalado View Agent 6.0.2 o versiones posteriores.

- Debe utilizar el protocolo de visualización de VMware Blast o PCoIP.

Si utiliza Horizon 6.0.1 y versiones posteriores, puede conectar dispositivos USB 3.0 en puertos USB 3.0. Los dispositivos USB 3.0 solo son compatibles con una única transmisión. Como las transmisiones múltiples aún no son compatibles, el rendimiento de los dispositivos USB no se ha mejorado. Tenga en cuenta que en el sistema cliente Linux, los procesadores i386 son compatibles, mientras que las arquitecturas armel y armhf no. La versión de kernel de Linux debe ser 2.6.35 o una posterior.

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 `/etc/vmware/config`

2 `/usr/lib/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. Ubuntu 12.04 incluye la versión del kernel 3.2.0-27.43. 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: `viewusb.AllowAutoDeviceSplitting`	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: `viewusb.SplitExcludeVidPid`	Excluye un dispositivo USB compuesto especificado mediante los ID de producto y proveedor procedentes de la división. El formato de la configuración es `vid-`*xxx1*`_pid-`*yyy1*[`;vid-`*xxx2*`_pid-`*yyy2*]... Debe especificar los números ID en hexadecimales. 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 (Continua)

Propiedad y nombre de directiva	Descripción
Dividir un dispositivo Vid/Pid Propiedad: `viewusb.SplitVidPid`	Trata los componentes de un dispositivo USB compuesto especificado por los ID del producto y del proveedor como dispositivos separados. El formato de la configuración es `vid-`*xxxx*`_pid-`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` 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. Por ejemplo: **`vid-0781_pid-554c(exintf:01;exintf:02)`** **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. El valor predeterminado no está definido.
Permitir dispositivos de entrada de audio Propiedad: `viewusb.AllowAudioIn`	Permite que se redireccionen los dispositivos de entrada de audio. 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.
Permitir dispositivos de salida de audio Propiedad: `viewusb.AllowAudioOut`	Permite que se redireccionen los dispositivos de salida de audio. El valor predeterminado no está definido, lo que equivale a **`false`**.
Permitir HID Propiedad: `viewusb.AllowHID`	Permite que se redireccionen otros dispositivos de entrada que no sean dispositivos de teclado o mouse. El valor predeterminado no está definido, lo que equivale a **`true`**.
Permitir HIDBootable Propiedad: `viewusb.AllowHIDBootable`	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). El valor predeterminado no está definido, lo que equivale a **`true`**.
Permitir el descriptor del dispositivo Failsafe Propiedad: `viewusb.AllowDevDescFailsafe`	Permite el redireccionamiento de los dispositivos aunque se produzca un error en Horizon Client para obtener los descriptores del dispositivo y la configuración. 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`. El valor predeterminado no está definido, lo que equivale a **`false`**.
Permitir los dispositivos de teclado y mouse Propiedad: `viewusb.AllowKeyboardMouse`	Permite que se redireccionen teclados con dispositivos señaladores integrados (como un mouse, bola de seguimiento o panel táctil). El valor predeterminado no está definido, lo que equivale a **`false`**.
Permitir tarjetas inteligentes Propiedad: `viewusb.AllowSmartcard`	Permite que se redireccionen los dispositivos de tarjeta inteligente. El valor predeterminado no está definido, lo que equivale a **`false`**.

Tabla 6-1. Propiedades de configuración para el redireccionamiento USB (Continua)

Propiedad y nombre de directiva	Descripción
Permitir dispositivos de vídeo Propiedad: `viewusb.AllowVideo`	Permite que se redireccionen los dispositivos de vídeo. 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.
Deshabilitar la descarga de la configuración remota Propiedad: `viewusb.DisableRemoteConfig`	Deshabilita el uso de la configuración de View Agent cuando se realiza el filtrado de dispositivos USB. El valor predeterminado no está definido, lo que equivale a **`false`**.
Excluir todos los dispositivos Propiedad: `viewusb.ExcludeAllDevices`	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. Si establece el valor de `Exclude All Devices` en **`true`** en View Agent y esta configuración se traslada a Horizon Client, la configuración de View Agent reemplazará la de Horizon Client. El valor predeterminado no está definido, lo que equivale a **`false`**.
Excluir familia de dispositivos Propiedad: `viewusb.ExcludeFamily`	Excluye el redireccionamiento de familias de dispositivos. El formato de la configuración es *family_name_1*[`;`*family_name_2*]... Por ejemplo: **`bluetooth;smart-card`** 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. El valor predeterminado no está definido.
Excluir un dispositivo Vid/Pid Propiedad: `viewusb.ExcludeVidPid`	Excluye el redireccionamiento de dispositivos con los ID de producto y de proveedor específicos. El formato de la configuración es `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Debe especificar los números ID en hexadecimales. Puede utilizar el carácter comodín (`*`) en lugar de dígitos individuales en un ID. Por ejemplo: **`vid-0781_pid-****;vid-0561_pid-554c`** El valor predeterminado no está definido.
Excluir ruta Propiedad: `viewusb.ExcludePath`	Excluye el redireccionamiento de dispositivos en rutas de puerto o concentrador especificado. El formato de la configuración es `bus-`*x1*[*/y1*]..._`port-`*z1*[`;bus-`*x2*[*/y2*]..._`port-`*z2*]... Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta. Por ejemplo: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** El valor predeterminado no está definido.
Incluir familia de dispositivos Propiedad: `viewusb.IncludeFamily`	Incluye familias de dispositivos que se pueden redireccionar. El formato de la configuración es *family_name_1*[`;`*family_name_2*]... Por ejemplo: **`storage`** El valor predeterminado no está definido.

Tabla 6-1. Propiedades de configuración para el redireccionamiento USB (Continua)

Propiedad y nombre de directiva	Descripción
Incluir ruta Propiedad: `viewusb.IncludePath`	Incluye dispositivos en rutas de puerto o concentrador que pueden redireccionarse. El formato de la configuración es `bus-`*x1*[*/y1*]..._`port-`*z1*[`;bus-`*x2*[*/y2*]..._`port-`*z2*]... 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 `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Debe especificar los números ID en hexadecimales. 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 del dispositivo de 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 View Agent en el escritorio remoto (o reemplazarlas). Para obtener más información sobre cómo funciona las propiedades de división y filtrado USB en el cliente junto con las directivas USB de View Agent, consulte los temas relacionados con el uso de las directivas para controlar el redireccionamiento USB en el documento *Administración de View*.

Familias de dispositivos USB

Cuando cree reglas de filtrado USB para Horizon Client, View Agent o Horizon Agent, puede especificar una familia.

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.
`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.

Tabla 6-2. Familias de dispositivos USB (Continua)

Nombre de la familia de dispositivos	Descripción
`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.