Uso de VMware Horizon Client para Windows

VMware Horizon Client for Windows 4.4

vmware®

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

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

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

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

Usar VMware Horizon Client para Windows

Esta guía, *Usar VMware Horizon Client para Windows*, proporciona información acerca de la instalación y el uso del software VMware Horizon® Client™ en un sistema cliente Microsoft Windows para conectarse a una aplicación o un escritorio remotos del centro de datos.

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

Esta información está destinada a administradores que necesiten configurar una implementación de Horizon que incluya sistemas cliente Microsoft Windows, como equipos de escritorio o portátiles. 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.

Configuración y requisitos del sistema para clientes basados en Windows

1

El sistema que ejecuta los componentes de Horizon Client debe cumplir ciertos requisitos de hardware y software.

Horizon Client en sistemas Windows utiliza la configuración de Microsoft Internet Explorer, incluida la configuración del proxy, cuando se conecta al servidor de conexión. Asegúrese de que la configuración de Internet Explorer sea correcta y que puede acceder a la URL del servidor de conexión a través de dicho navegador.

Este capítulo cubre los siguientes temas:

Requisitos del sistema para clientes Windows

Puede instalar Horizon Client para Windows en equipos o equipos portátiles que utilicen un sistema operativo de Microsoft Windows compatible.

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

Modelo

Todos los dispositivos Windows x86 o x86-64

Memoria

Al menos 1 GB de RAM

Sistemas operativos

Los siguientes sistemas operativos son compatibles:

SO	Versión	Service Pack u opción de mantenimiento	Ediciones compatibles
Windows 10	32 o 64 bits	Rama actual (Current Branch, CB) versión 1607 Rama actual para empresas (CBB) versión 1607 Rama de mantenimiento a largo plazo (LTSB) versión 1607	Home, Pro, Enterprise e IoT Core
Windows 8 o 8.1	32 o 64 bits	Ninguno o actualización 2	Pro, Enterprise e Industry Embedded
Windows 7	32 o 64 bits	SP1	Home, Enterprise, Professional y Ultimate
Windows Server 2008 R2	64 bits	Última actualización	Standard
Windows Server 2012 R2	64 bits	Última actualización	Standard

Windows Server 2008 R2 y Windows Server 2012 R2 pueden ejecutar Horizon Client en el modo anidado. Si desea obtener más información, consulte "Funciones compatibles con el modo anidado," página 89.

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

Versión de mantenimiento más reciente de View 5.3.x y versiones posteriores

Si los sistemas cliente se conectan desde fuera del firewall corporativo, VMware le recomienda que utilice un servidor de seguridad o un dispositivo Access Point para que los sistemas cliente no necesiten una conexión VPN.

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

NOTA: Los clientes también se pueden conectar al dispositivo Access Point, que está disponible en la versión 6.2 de Horizon 6 o en versiones posteriores.

Protocolos de visualización

VMware Blast, PCoIP y RDP

Requisitos de hardware para PCoIP y VMware Blast

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

Requisitos de software para RDP

- Para Windows 7, utilice RDP 7.1 o 8.0. Windows 7 incluye RDP 7. Windows 7 SP1 incluye RDP 7.1.
- Para Windows 8, utilice RDP 8.0. Para Windows 8.1, utilice RDP 8.1.
- Para Windows 10, utilice RDP 10.0.
- (Solo compatible con View Agent 6.0.2 y versiones anteriores). Para máquinas virtuales de escritorio de Windows XP, debe instalar las revisiones de RDP incluidas en los artículos 323497 y 884020 de Microsoft Knowledge Base (KB). Si no instala las revisiones de RDP, es posible que aparezca un mensaje de `error de Windows Sockets` en el cliente.
- El instalador del agente configura la regla del firewall local para que las conexiones RDP entrantes coincidan con el puerto RDP actual del sistema operativo del host, que suele ser 3389. Si cambia el número de puerto RDP, deberá modificar las reglas del firewall asociadas.

Puede descargar versiones del cliente de Escritorio remoto del centro de descargas de Microsoft.

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 todos los sistemas operativos con Horizon Client para Windows. Para obtener más información, consulte "Requisitos del sistema para clientes Windows," página 10. ■ 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 para el redireccionamieno del escáner

Puede escanear información en las aplicaciones y los escritorios remotos con escáneres que estén conectados al sistema cliente local.

Para usar esta función, las aplicaciones, los escritorios remotos y los equipos cliente deben cumplir ciertos requisitos de sistema.

Escritorios remotos	Los escritorios remotos deben tener instalados View Agent 6.0.2 o Horizon Agent 7.0, o bien una versión posterior de ambos productos, con la opción de configuración Redireccionamiento del escáner, en las máquinas virtuales de plantilla o principal o los hosts RDS. En escritorios Windows y sistemas operativos invitados Windows Server, la opción de configuración Redireccionamiento del escáner de Horizon Agent no está seleccionada de forma predeterminada. Para obtener más información sobre los sistemas operativos invitados compatibles con máquinas virtuales de usuario único y con hosts RDS, así como para obtener información sobre la configuración del redireccionamiento del escáner en aplicaciones o escritorios remotos, consulte "Configurar Redireccionamiento de escáner" en *Configurar funciones de escritorios remotos en Horizon 7*.
Equipo con Horizon Client o dispositivo de acceso del cliente	■ El redireccionamiento del escáner es compatible con Windows 7, Windows 8/8.1 y Windows 10. ■ Los controladores del escáner deben estar instalados y este dispositivo debe estar operativo en el equipo cliente. No es necesario que instale los controladores del escáner en el sistema operativo del escritorio remoto donde está instalado el agente.
Estándar del escáner	TWAIN o WIA
Protocolos de visualización	■ PCoIP

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

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

Requisitos para el redireccionamiento del puerto serie

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

Escritorios remotos

Los escritorios remotos deben tener instalados View Agent 6.1.1 o Horizon Agent 7.0, o bien una versión posterior de ambos productos, con la opción de configuración Redireccionamiento del puerto serie, en las máquinas virtuales de plantilla o principal. De manera predeterminada, esta opción de configuración no está seleccionada.

Los siguientes sistemas operativos invitados se admiten en las máquinas virtuales de sesión única:

- Windows 7 de 64 o 32 bits
- Windows 8.x de 64 o 32 bits
- Windows 10 de 64 o 32 bits
- Windows Server 2008 R2 configurado como escritorio
- Windows Server 2012 R2 configurado como escritorio
- Windows Server 2016 configurado como escritorio

Actualmente, esta función no es compatible con hosts Windows Server RDS.

No es necesario que los controladores del dispositivo de puerto serie estén instalados en el sistema operativo del escritorio en el que el agente está instalado.

NOTA: Para obtener más información acerca de la configuración del redireccionamiento del puerto serie en los escritorios remotos, consulte "Configurar el redireccionamiento del puerto serie" en *Configurar funciones de escritorios remotos en Horizon 7*.

Equipo con Horizon Client o dispositivo de acceso del cliente

- El redireccionamiento del puerto serie es compatible con Windows 7, sistemas cliente Windows 8.x y Windows 10.
- Los controladores del puerto serie necesarios deben estar instalados y este puerto debe estar operativo en el equipo cliente. No es necesario que instale los controladores del dispositivo en el sistema operativo del escritorio remoto donde está instalado el agente.

Protocolos de visualización

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

El redireccionamiento del puerto serie VMware Horizon no se admite en las sesiones de escritorio RDP.

Requisitos 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

Windows 7, Windows 8.x o Windows 10 de 32 o 64 bits.

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.

Requisitos para la redirección de Flash

Con la redirección de Flash, si usa Internet Explorer 9, 10 u 11, el contenido Flash se envía al sistema cliente. El sistema cliente reproduce el contenido multimedia, que reduce la carga en el host ESXi.

Escritorio remoto

- La versión 7.0 o versiones posteriores de Horizon Agent 7.0 se deben instalar en un escritorio remoto (VDI) de usuario único con la opción de redirección de Flash. La opción de redirección de Flash no está seleccionada de forma predeterminada.

  Consulte los temas sobre cómo instalar Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7*.
- Se deben configurar las opciones de la directiva de grupo. Consulte los temas sobre cómo configurar la redirección de Flash en el documento *Configurar escritorios virtuales en Horizon 7*.
- La redirección de Flash es compatible con los escritorios de usuario único Windows 7, Windows 8, Windows 8.1 y Windows 10.
- Se debe instalar Internet Explorer 9, 10 u 11 con el complemento Flash ActiveX correspondiente.

	■ Después de la instalación, la extensión VMware View FlashMMR Server debe estar habilitada en Internet Explorer.
Equipo con Horizon Client o dispositivo de acceso del cliente	■ La redirección de Flash es compatible con Windows 7, Windows 8, Windows 8.1 y Windows 10. ■ El complemento Flash ActiveX debe estar instalado y habilitado
Protocolo de visualización para la sesión remota	VMware Blast, PCoIP

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:

- 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 Adobe Flash Player 10.1 o una versión superior para Internet Explorer (que usa ActiveX).

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 del redireccionamiento del contenido URL

Con el redireccionamiento del contenido URL, puede redireccionar el contenido URL desde un cliente hacia una aplicación o un escritorio remotos, o viceversa. Por ejemplo, puede hacer clic en un vínculo en la aplicación Microsoft Word nativa en el cliente y que este se abra en la aplicación Internet Explorer remota, o bien puede hacer clic en un vínculo en la aplicación Internet Explorer remota y que este se abra en un navegador nativo del cliente.

Puede configurar el número de protocolos que desee para el redireccionamiento, incluidos HTTP, mailto y callto. Esta función es compatible con el redireccionamiento en ambas direcciones:

- De un cliente a una aplicación o un escritorio remotos (de cliente a agente)

  Horizon Client inicia una aplicación o un escritorio remotos para controlar la URL. Si se inicia un escritorio, la aplicación predeterminada del protocolo de URL la procesa.

- De una aplicación o un escritorio remotos a un cliente (de agente a cliente)

  Horizon Agent envía la URL a Horizon Client, que inicia la aplicación predeterminada para el protocolo que se especifica en la URL.

Esta función tiene los siguientes requisitos:

El escritorio remoto o el host RDS que proporciona aplicaciones remotas	■ Horizon Agent 7.0 o posterior. Esta función debe estar instalada si desea configurar el redireccionamiento de agente a cliente. ■ Horizon Administrator debe configurar las opciones que especifican cómo Horizon Agent redirecciona el contenido URL desde una aplicación o un escritorio remotos al sistema cliente. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*. ■ Los navegadores compatibles en los que puede introducir una URL o hacer clic en ella y que redireccionen esa URL son Internet Explorer 9, 10 y 11.
Equipo con Horizon Client o dispositivo de acceso del cliente	■ Esta función debe estar instalada si desea configurar el redireccionamiento de cliente a agente. ■ Horizon Administrator debe configurar las opciones que especifican cómo Horizon Client redirecciona el contenido de la URL desde el sistema cliente a una aplicación o un escritorio remotos. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*. ■ Los navegadores compatibles en los que puede introducir una URL o hacer clic en ella y que redireccionen esa URL son Internet Explorer 9, 10 y 11.
Protocolo de visualización para la sesión remota	■ VMware Blast ■ PCoIP

Requisitos para usar Microsoft Lync con Horizon Client

Es posible usar un cliente Microsoft Lync 2013 en escritorios remotos para participar en llamadas de comunicaciones unificadas (UC), de VoIP (voz sobre IP) y videollamadas con dispositivos de audio y vídeo USB certificados por Lync. Ya no es necesario un teléfono IP dedicado.

Esta arquitectura requiere la instalación de un cliente Microsoft Lync 2013 en el escritorio remoto y un complemento VDI de Microsoft Lync en el endpoint cliente. Los usuarios pueden usar el cliente Microsoft Lync 2013 para las funciones de presencia, de mensajería instantánea, de conferencias web y de Microsoft Office.

Cuando se produce una videollamada o una llamada VoIP de Lync, el complemento Lync VDI descarga todos los elementos multimedia procesados en el servidor del centro de datos al endpoint cliente y codifica todo este contenido en códecs de vídeo y de audio optimizados para Lync. Esta arquitectura optimizada es altamente escalable, con ella se reduce el uso de ancho de banda de red y proporciona una entrega multimedia punto a punto con compatibilidad para vídeo y VoIP de alta calidad y a tiempo real. Para obtener más información, consulte las notas del producto sobre Horizon 6 y Microsoft Lync 2013 disponibles en http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf.

NOTA: Aún no se admite la grabación de audio. Esta integración solo es compatible con el protocolo de visualización PCoIP.

Esta función también cuenta con los siguientes requisitos.

Sistema operativo

- Sistema operativo cliente: Windows 7 SP1, Windows 8.x o Windows 10.
- El sistema operativo (agente) de la máquina virtual depende de la versión del agente.

Versión	Sistema operativo de invitado
View Agent 6.2 o Horizon Agent 7.0 o versiones posteriores de ambos productos	Windows 7 SP1 de 32 o 64 bits, Windows 8.x, Windows 10 o Windows Server 2008 R2 SP1 de 64 bits Para los hosts de Microsoft RDS: Windows Server 2008 R2, Windows Server 2012, o Windows Server 2012 R2
View Agent 6.0 o 6.1	Windows 7 SP1 de 32 o 64 bits, Windows 8.x o Windows Server 2008 R2 SP1 de 64 bits
View Agent 5.3	Windows 7 SP1 de 64 o 32 bits

Software del sistema cliente

- Versión de 32 bits del complemento VDI de Microsoft Lync

  IMPORTANTE: La versión de 64 bits de Microsoft Office no se debe instalar en la máquina cliente. El complemento VDI de Microsoft Lync de 32 bits necesario no es compatible con Microsoft Office 2013 de 64 bits.

- El certificado de seguridad generado durante la implementación de Microsoft Lync Server 2013 debe importarse al directorio Entidades de certificación raíz de confianza.

Software del escritorio remoto (agente)

- View Agent 5.3 o Horizon Agent 7.0 o versiones posteriores de ambos productos
- Cliente Microsoft Lync 2013

  Con View 5.3 o un agente posterior, no es necesario que el nivel de bits del cliente Lync 2013 coincida con el nivel de bits del sistema operativo de la máquina virtual.

- El certificado de seguridad generado durante la implementación de Microsoft Lync Server 2013 debe importarse al directorio Entidades de certificación raíz de confianza.

Servidores necesarios

- Un servidor que ejecute Connection Server 5.3 o una versión posterior
- Un servidor que ejecute Microsoft Lync Server 2013
- Una infraestructura vSphere para alojar las máquinas virtuales

  vCenter Server y los hosts ESXi deben ejecutar vSphere 5.0 o una versión posterior.

Hardware

- Hardware compatible con cada uno de los componentes de software necesarios enumerados anteriormente

- Endpoint cliente: 1,5 GHz o una CPU más veloz y un mínimo de 2 GB de RAM para el complemento Microsoft Lync 2013

NOTA: Para obtener información sobre cómo solucionar problemas, consulte los artículos de la base de conocimientos de VMware 2063769 y 2053732.

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.

Horizon es compatible con las tarjetas inteligentes y los lectores que utilizan PKCS#11 o el proveedor Microsoft CryptoAPI. Puede instalar de forma opcional el conjunto de software ActivIdentity ActivClient, que proporciona herramientas para interactuar con tarjetas inteligentes.

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

Para instalar certificados en una tarjeta inteligente, debe configurar un equipo para que actúe como una estación de inscripción. Este equipo debe tener autorización para emitir certificados de tarjetas inteligentes para los usuarios y debe ser miembro del dominio para el que está emitiendo los certificados.

IMPORTANTE: Cuando registre una tarjeta inteligente, puede seleccionar el tamaño de la clave del certificado resultante. Para utilizar tarjetas inteligentes con escritorios locales, debe seleccionar un tamaño de clave de 1024 o 2048 bits durante el registro de las tarjetas inteligentes. Los certificados con claves de 512 bits no son compatibles.

El sitio web de Microsoft TechNet incluye información detallada sobre cómo planificar e implementar la autenticación con tarjetas inteligentes en sistemas Windows.

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 Access Point en lugar de un servidor de seguridad para el acceso externo seguro, debe configurar el dispositivo Access Point para que sea compatible con la función de sugerencias de nombre de usuario de la tarjeta inteligente. Dicha función es compatible únicamente con Access Point 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 Access Point, consulte el documento *Implementación y configuración de Access Point*.

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.

Requisitos de autenticación del dispositivo

Si lo desea, puede configurar la autenticación del certificado para los dispositivos cliente.

Esta función también cuenta con los siguientes requisitos:

- Access Point 2.6 o posterior.
- Horizon 7 versión 7.0 o posterior.
- Se instaló un certificado en el dispositivo cliente que aceptará Access Point.

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 Access Point, configure el servidor de conexión para que funcione con Access Point. Consulte el documento *Implementación y configuración de Access Point*. Los dispositivos de Access Point 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*.

  IMPORTANTE: Si los usuarios finales cuentan con pantallas de alta resolución y van a utilizar la configuración del cliente en modo de alta resolución mientras ven los escritorio remotos en modo de pantalla completa, debe asignar una cantidad de VRAM suficiente para cada escritorio Windows 7 o con una versión posterior. La cantidad de VRAM depende del número de monitores configurados para los usuarios finales y en la resolución de pantalla. Para calcular la cantidad de vRAM que necesita, consulte el documento *Planificación de arquitectura de View*.
- 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*.

Borrar el último nombre de usuario con el que se inició sesión en un servidor

Si el usuario inicia sesión en una instancia del servidor de conexión que tenga habilitada la configuración global **Ocultar la lista de dominios en la interfaz de usuario del cliente**, el menú desplegable **Dominio** permanece oculto en Horizon Client y el usuario proporciona la información de dominio en el cuadro de texto Horizon Client **Nombre de usuario**. Por ejemplo, el usuario debe introducir su nombre de usuario con el formato ***dominio**nombre de usuario*** o ***nombre de usuario@dominio***.

En un sistema cliente Windows, una clave del Registro determina si el último nombre de usuario se guarda y se muestra en el cuadro de texto **Nombre de usuario** la próxima vez que un usuario inicie sesión en el servidor. Para evitar que el último nombre de usuario se muestre en el cuadro de texto **Nombre de usuario** y la información de dominio quede expuesta, debe establecer el valor de la clave del Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` en 1 en el sistema cliente Windows.

Para obtener información sobre cómo ocultar información de seguridad en Horizon Client, incluidos el menú desplegable **Dominio** y la información sobre la URL del servidor, consulte los temas relacionados con la configuración global en el documento *Administración de View*.

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 de 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.

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 Haga clic en el botón **Opciones** en la barra de menús y seleccione **Configurar VMware Blast**.

Si ha iniciado sesión en un servidor, puede hacer clic en el icono **Configuración** (engranaje) y seleccionar **VMware Blast**. No puede cambiar la opción de condición de la red tras iniciar sesión en un servidor.

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. VMware Access Point 2.9 y las 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 de VMware Blast. Los cambios no afectan a las sesiones VMware Blast existentes.

Utilizar la configuración del proxy de Internet Explorer

Horizon Client Utiliza automáticamente la configuración del proxy de Internet Explorer.

Omitir la configuración del proxy

Horizon Client Utiliza la configuración de omisión del proxy de Internet Explorer para omitir las conexiones HTTPS a un dispositivo Access Point, servidor de seguridad o host del servidor de conexión.

Si el túnel seguro está habilitado en el dispositivo Access Point, servidor de seguridad o host del servidor de conexión, debe utilizar la opción de la directiva de grupo `Lista de direcciones para omitir proxy de túnel` del archivo de plantilla ADM y ADMX Configuración de Horizon Client para especificar una lista de direcciones para omitir la conexión del túnel. El servidor proxy no se usa en estas direcciones. Use un punto y coma (;) para separar varias entradas. Esta opción de la directiva de grupo crea la clave del Registro siguiente:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

No puede utilizar esta opción de la directiva de grupo para conexiones directas. Si la aplicación de la opción de la directiva de grupo no funciona como se espera, intente omitir el proxy para las direcciones locales. Si desea obtener más información, consulte https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Error de proxy

Horizon Client Admite un error de proxy con la opción **Usar script de configuración automática** en **Configuración automática** dentro de **Opciones de Internet > Conexiones> Configuración LAN** en Internet Explorer. Para utilizar esta opción debe crear un script de configuración automática que devuelva varios servidores proxy.

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 1-1. 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

Tabla 1-1. 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
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)
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

Tabla 1-1. 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
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)

Instalar Horizon Client para Windows 2

Puede obtener el instalador de Horizon Client para Windows desde el sitio web de VMware o desde una página de acceso web proporcionada por el servidor de conexión. Después de instalar Horizon Client, puede establecer varias opciones de inicio para los usuarios finales.

Este capítulo cubre los siguientes temas:

Habilitar el modo FIPS en el sistema operativo cliente Windows

Si tiene pensado instalar Horizon Client con un cifrado que cumpla el estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS), debe habilitar el modo FIPS en el sistema operativo cliente antes de ejecutar el instalador de Horizon Client.

Cuando el modo FIPS está habilitado en el sistema operativo cliente, las aplicaciones solo utilizan algoritmos criptográficos conformes a FIPS-140 y que cumplan los modos de operación aprobados por FIPS. Puede habilitar el modo FIPS si habilita una configuración de seguridad específica, ya sea en la Directiva de seguridad local o como parte de una directiva de grupo, o bien si edita una clave del Registro de Windows.

IMPORTANTE: La instalación de Horizon Client con un cifrado conforme a FIPS solo se admite en sistemas cliente con sistemas operativos Windows 7 SP1.

Para obtener más información sobre la compatibilidad con FIPS, disponible con Horizon 6 versión 6.2 o posterior, consulte el documento *Instalación de View*.

Establecer la propiedad de configuración FIPS

Para habilitar el modo FIPS en el sistema operativo cliente, puede utilizar una opción de directiva de grupo de Windows o una opción del Registro de Windows para el equipo cliente.

- Para utilizar la configuración de directiva de grupo, abra el Editor de directivas de grupo, desplácese hasta `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options` y habilite la opción **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash**.
- Para utilizar el Registro de Windows, acceda a `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` y defina el valor 1 a la opción **Habilitado**.

Para obtener más información sobre el modo FIPS, diríjase a https://support.microsoft.com/en-us/kb/811833.

IMPORTANTE: Si no habilita el modo FIPS antes de ejecutar el instalador de Horizon Client, la opción para utilizar el cifrado conforme a FIPS no aparecerá durante el proceso de instalación personalizada. Este cifrado no se habilita durante el proceso de instalación clásica. Si instala Horizon Client sin esta opción y decide utilizarla más adelante, deberá desinstalar el cliente, habilitar el modo FIPS en el sistema operativo cliente y volver a ejecutar el instalador de Horizon Client.

Instalar Horizon Client para Windows

Los usuarios finales abren Horizon Client para conectarse a sus aplicaciones y escritorios remotos desde un sistema cliente. Puede ejecutar el archivo de un instalador basado en Windows para instalar todos los componentes de Horizon Client.

El instalador determina si el sistema cliente es de 64 o 32-bits e instala la versión correcta de Horizon Client para el sistema cliente. El instalador no se ejecuta en Windows XP ni Windows Vista.

Este procedimiento describe la instalación de Horizon Client con un asistente de instalación interactivo. Para instalar la función de redireccionamiento de contenido URL, debe ejecutar el instalador desde la línea de comandos y especificar el parámetro `URL_FILTERING_ENABLED`, por ejemplo, `VMware-Horizon-Client-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1`. Para utilizar la función de instalación silenciosa de la línea de comandos de Microsoft Windows Installer (MSI), consulte "Instalar Horizon Client silenciosamente," página 30.

NOTA: Puede instalar Horizon Client en una máquina virtual del escritorio remoto si dicho escritorio utiliza View Agent 6.0 o versiones posteriores, o Horizon Agent 7.0 o versiones posteriores. Es posible que las compañías utilicen esta estrategia de instalación si los usuarios finales acceden a las aplicaciones remotas desde dispositivos de cliente ligero de Windows.

Prerequisitos

- Compruebe que el sistema cliente utilice un sistema operativo compatible. Consulte "Requisitos del sistema para clientes Windows," página 10.
- Compruebe que cuenta con la URL de una página de descargas que contenga el instalador de Horizon Client. Esta URL puede ser de la página Descargas de VMware disponible en http://www.vmware.com/go/viewclients o puede ser la URL de una instancia de un servidor de conexión.
- Compruebe que pueda iniciar sesión como administrador en el sistema cliente.
- Compruebe que los controladores de dominio cuentan con las últimas revisiones y suficiente espacio libre en el disco y se pueden comunicar entre sí. En caso contrario, si ejecuta el instalador en un sistema Windows 8.1, este puede tardar demasiado en finalizar. Este problema se produce si no se puede acceder al controlador de dominio del equipo (u otro controlador de dominio en esta jerarquía) o este no responde.
- Si tiene pensado instalar Horizon Client con criptografía conforme a FIPS, habilite el modo FIPS en el sistema operativo cliente antes de ejecutar el instalador de Horizon Client. Consulte "Habilitar el modo FIPS en el sistema operativo cliente Windows," página 27.
- Si tiene pensado instalar el componente **Redireccionamiento USB**, haga lo siguiente:
  - Determine si la persona que utiliza el dispositivo cliente está autorizada a acceder a los dispositivos USB conectados de forma local desde un escritorio remoto. Si el acceso no está permitido, no instale el componente **Redireccionamiento USB** o instálelo y deshabilítelo mediante una opción de directiva de grupo. Si utiliza una directiva de grupo para deshabilitar el redireccionamiento USB, no tendrá que volver a instalar Horizon Client si decide habilitar el redireccionamiento USB para un cliente más adelante. Si desea obtener más información, consulte "Configuración de la definición de scripting para los GPO cliente," página 48.

- Compruebe que la función Actualizaciones automáticas de Windows no esté desactivada en el equipo cliente.

- Decida si va a utilizar la función que permite a los usuarios finales iniciar sesión en Horizon Client y sus escritorios remotos como el usuario que inició la sesión actual. La información de credenciales que el usuario introduce cuando inicia sesión en el sistema cliente se envía a la instancia del servidor de conexión y, por último, al escritorio remoto. Algunos sistemas operativos cliente no son compatibles con esta función.
- Si no desea solicitar a los usuarios finales que proporcionen el nombre del dominio plenamente cualificado (FQDN) de la instancia del servidor de conexión, determine el FQDN de forma que lo pueda proporcionar durante la instalación.

Procedimiento

1 Inicie sesión en el sistema cliente como administrador.

2 Acceda a la página de productos de VMware: http://www.vmware.com/go/viewclients.

3 Descargue el archivo del instalador, por ejemplo, `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

xxxxxx es el número de compilación e *y.y.y* es el número de la versión.

4 Haga doble clic en el archivo del instalador para empezar la instalación.

5 Seleccione el tipo de instalación y siga los mensajes.

Opción	Descripción
Típico	Instala el protocolo de Internet IPv4 y el redireccionamiento USB, así como el inicio de sesión como funciones del usuario actual. Si se habilita el modo FIPS en el sistema operativo cliente, la criptografía conforme a FIPS se deshabilita.
Personalizado	Le permite seleccionar los componentes que se van a instalar. Siga estas directrices a la hora de seleccionar componentes: ■ No seleccione el protocolo de Internet IPv6, a menos que todos los componentes del entorno de Horizon utilicen este protocolo. Si selecciona IPv6, algunas funciones no estarán disponibles. Para obtener más información, consulte el documento *Instalación de View*. ■ Solo podrá habilitar la criptografía conforme a FIPS si habilitó el modo FIPS en el sistema operativo cliente.

El instalador instala ciertos servicios de Windows, entre ellos, VMware Horizon Client (`horizon_client_service`) y VMware USB Arbitration Service (`VMUSBArbService`).

Qué hacer a continuación

Inicie Horizon Client y compruebe que puede iniciar sesión en la aplicación o el escritorio remotos correctos. Consulte "Conectarse a una aplicación o escritorio remotos," página 73.

Instalar Horizon Client silenciosamente

Puede instalar Horizon Client silenciosamente al escribir el nombre de archivo del instalador y las opciones de instalación en la línea de comandos. La instalación silenciosa le permite implementar los componentes de Horizon correctamente en una empresa de gran tamaño.

Instalar Horizon Client silenciosamente

Puede usar la función de instalación silenciosa de Microsoft Windows Installer (MSI) para instalar Horizon Client en varios equipos Windows. En una instalación silenciosa, puede usar la línea de comando y no es necesario que responda a los mensajes del asistente.

El instalador determina si el sistema cliente es de 64 o 32-bits e instala la versión correcta de Horizon Client para el sistema cliente.

Prerequisitos

- Compruebe que el sistema cliente utilice un sistema operativo compatible. Consulte "Requisitos del sistema para clientes Windows," página 10.
- Compruebe que pueda iniciar sesión como administrador en el sistema cliente.
- Compruebe que los controladores de dominio cuentan con las últimas revisiones y suficiente espacio libre en el disco y se pueden comunicar entre sí. En caso contrario, si ejecuta el instalador en un sistema Windows 8.1, este puede tardar demasiado en finalizar. Este problema se produce si no se puede acceder al controlador de dominio del equipo (u otro controlador de dominio en esta jerarquía) o este no responde.
- Si tiene pensado instalar Horizon Client con criptografía conforme a FIPS, habilite el modo FIPS en el sistema operativo cliente antes de ejecutar el instalador de Horizon Client. Consulte "Habilitar el modo FIPS en el sistema operativo cliente Windows," página 27.
- Decida si va a utilizar la función que permite a los usuarios finales iniciar sesión en Horizon Client y sus escritorios remotos como el usuario que inició la sesión actual. La información de credenciales que el usuario introduce cuando inicia sesión en el sistema cliente se envía a la instancia del servidor de conexión y, por último, al escritorio remoto. Algunos sistemas operativos cliente no son compatibles con esta función.
- Familiarícese con las opciones de la línea de comandos del instalador MSI. Consulte "Opciones de la línea de comandos de Microsoft Windows Installer," página 32.
- Familiarícese con las propiedades de la instalación silenciosa (MSI) disponibles con Horizon Client. Consulte "Propiedades de la instalación silenciosa de Horizon Client," página 31.
- Determine si desea permitir a los usuarios finales acceder a los dispositivos USB conectados desde los escritorios virtuales. Si no, establezca la propiedad MSI, `ADDLOCAL`, para la lista de funciones de interés y omita la función USB. Para obtener más información, consulte "Propiedades de la instalación silenciosa de Horizon Client," página 31.
- Si no desea solicitar a los usuarios finales que proporcionen el nombre del dominio plenamente cualificado (FQDN) de la instancia del servidor de conexión, determine el FQDN de forma que lo pueda proporcionar durante la instalación.

Procedimiento

1 Inicie sesión en el sistema cliente como administrador.

2 Acceda a la página de productos de VMware: http://www.vmware.com/go/viewclients.

3 Descargue el archivo del instalador de Horizon Client, por ejemplo, `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

   xxxxxx es el número de compilación e *y.y.y* es el número de la versión.

4 Abra una ventana del símbolo del sistema en el equipo cliente Windows.

5 Escriba el comando de instalación en una línea.

   Este ejemplo instala Horizon Client de forma silenciosa:

   ```
   VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,USB,TSSO"
   ```

   También puede utilizar `ADDLOCAL=ALL` en lugar de `ADDLOCAL=Core,USB,TSSO`.

   NOTA: La función `Núcleo` es obligatoria.

El instalador instala ciertos servicios de Windows, entre ellos, VMware Horizon Client (`horizon_client_service`) y VMware USB Arbitration Service (`VMUSBArbService`).

Qué hacer a continuación

(Opcional) Si instaló Horizon Client con la función de redireccionamiento de contenido URL, asegúrese de que la función esté instalada. Para ello, compruebe que los archivos `vmware-url-protocol-launch-helper.exe` y `vmware-url-filtering-plugin.dll` estén instalados en el directorio `%PROGRAMFILES %\VMware\VMware Horizon View Client\`. Asimismo, compruebe que el complemento de filtro de URL de VMware Horizon View para Internet Explorer esté instalado y habilitado.

Inicie Horizon Client y compruebe que puede iniciar sesión en la aplicación o el escritorio remotos correctos. Consulte "Conectarse a una aplicación o escritorio remotos," página 73.

Propiedades de la instalación silenciosa de Horizon Client

Puede incluir propiedades específicas cuando instale Horizon Client de forma silenciosa desde la línea de comandos. Debe usar un formato *`PROPERTY=value`* para que Microsoft Windows Installer (MSI) pueda interpretar las propiedades y los valores.

Tabla 2-1 muestra las propiedades de instalación silenciosa de Horizon Client que puede usar en la línea de comandos.

Tabla 2-1. Propiedades MSI para instalar Horizon Client de forma silenciosa

Propiedad MSI	Descripción	Valor predeterminado
INSTALLDIR	La ruta y la carpeta en las que el software Horizon Client está instalado. Por ejemplo: `INSTALLDIR=""D:\abc\my folder""` Si se incluyen comillas dobles que abran y cierren la ruta, el instalador MSI puede interpretar el espacio como parte válida de la ruta.	`%ProgramFiles %\VMware\VMware Horizon View Client`
VDM_IP_PROTOCOL_USAGE	Especifica la versión IP (protocolo de red) que los componentes de Horizon usan para comunicarse. Los valores posibles son **`IPv4`** e **`IPv6`**.	IPv4
VDM_SERVER	El nombre de dominio completo (FQDN) de la instancia del servidor de conexión de Horizon a la que los usuarios de Horizon Client se conectarán de forma predeterminada. Cuando configura esta propiedad, los usuarios de Horizon Client no tienen que proporcionar este FQDN. Por ejemplo: `VDM_SERVER=cs1.companydomain.com` La propiedad MSI es opcional.	Ninguna

Tabla 2-1. Propiedades MSI para instalar Horizon Client de forma silenciosa (Continua)

Propiedad MSI	Descripción	Valor predeterminado
DESKTOP_SHORTCUT	Configura un icono de acceso directo para Horizon Client. El valor 1 instala el acceso directo. El valor 0 no instala el acceso directo.	1
STARTMENU_SHORTCUT	Configura un acceso directo de Horizon Client en el menú Inicio. El valor 1 instala el acceso directo. El valor 0 no instala el acceso directo.	1
URL_FILTERING_ENABLED	Especifica si instalar la función de redireccionamiento de contenido URL. El valor 1 instala la función. **NOTA:** La opción `ADDLOCAL=ALL` no incluye esta función.	0
VDM_FIPS_ENABLED	Especifica si instalar Horizon Client con criptografía conforme a FIPS. El valor 1 instala el cliente con criptografía conforme a FIPS. El valor 0 no lo hace. **NOTA:** Antes de configurar esta opción en 1, debe habilitar el modo FIPS en el sistema operativo cliente Windows. Consulte "Habilitar el modo FIPS en el sistema operativo cliente Windows," página 27.	0

En un comando de instalación silenciosa, puede usar la propiedad MSI, `ADDLOCAL=`, para especificar las funciones que configura el instalador de Horizon Client. Cada función de la instalación silenciosa corresponde a una opción de configuración que puede seleccionar durante una instalación interactiva.

Tabla 2-2 muestra las funciones de Horizon Client que puede escribir en la línea de comandos y las opciones de instalación interactiva correspondientes.

Tabla 2-2. Funciones de instalación silenciosa de Horizon Client y opciones de configuración personalizada interactiva

Función de instalación silenciosa	Opción de configuración personalizada en una instalación interactiva
Núcleo Si especifica funciones individuales con la propiedad MSI, `ADDLOCAL=`, debe incluir **`Core`**.	Ninguna. Durante una instalación interactiva, las funciones del núcleo Horizon Client están instaladas de forma predeterminada.
TSSO	Inicia sesión como el usuario del dominio de Windows que ya tiene la sesión iniciada
USB	Redireccionamiento USB

Opciones de la línea de comandos de Microsoft Windows Installer

Para instalar silenciosamente Horizon Client, debe usar las propiedades y las opciones de la línea de comandos de Microsoft Windows Installer (MSI). Los instaladores de Horizon Client son programas MSI y usan funciones estándares de dicho instalador. También puede usar las opciones de la línea de comandos MSI para desinstalar Horizon Client silenciosamente.

Si desea obtener más información sobre MSI, consulte el sitio web de Microsoft. En cuanto a las opciones de la línea de comandos MSI, consulte el sitio web Microsoft Developer Network (MSDN) Library y busque las opciones de la línea de comandos MSI. Para consultar el uso de la línea de comandos MSI, puede abrir una ventana del símbolo del sistema en el equipo cliente y escribir `msiexec /?`.

Para ejecutar el instalador Horizon Client silenciosamente, debe silenciar el programa de arranque que extrae el instalador en un directorio temporal y comenzar una instalación interactiva.

La siguiente tabla muestra las opciones de la línea de comandos que controlan el programa de arranque del instalador.

Tabla 2-3. Opciones de la línea de comandos para el programa de arranque

Opción	Descripción
`/s`	Deshabilita la pantalla de presentación de arranque y el cuadro de diálogo de extracción, lo que evita que aparezcan cuadros de diálogo interactivos. Por ejemplo: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /s` Es necesaria la opción `/s` para ejecutar una instalación silenciosa. En los ejemplos, *xxxxxx* es el número de compilación e *y.y.y* es el número de la versión.
`/v"`*`opciones_de_línea_de_comandos_para_MSI`*`"`	Ordena al instalador que envíe la cadena entre comillas dobles que introdujo en la línea de comandos como un conjunto de opciones para que MSI las interprete. Debe escribir las entradas de la línea de comandos entre comillas dobles. Escriba comillas dobles después de `/v` y al final de la línea de comandos. Por ejemplo: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"`*`opciones_de_línea_de_comandos`*`"` Si desea que el instalador MSI interprete una cadena que contiene espacios, escriba dos grupos de comillas dobles en la cadena. Por ejemplo, es posible que quiera instalar el cliente en una ruta de instalación cuyo nombre contenga espacios. Por ejemplo: `VMware-Horizon-View-Client-y.y.y-xxxxxx.exe /s /v"`*`opciones_de_línea_de_comandos`*` INSTALLDIR=""d:\abc\mi carpeta"""` En este ejemplo, el instalador MSI transmitirá la ruta del directorio de instalación y no intentará interpretar la cadena como dos opciones de la línea de comandos. Tenga en cuenta que las últimas comillas dobles cierran toda la línea de comandos. Es necesaria la opción `/v"`*`opciones_de_línea_de_comandos`*`"` para ejecutar una instalación silenciosa.

Puede controlar el aviso de una instalación silenciosa al enviar las opciones de la línea de comandos y los valores de la propiedad MSI para el instalador MSI, `msiexec.exe`. El instalador MSI incluye el código de instalación de Horizon Client. El instalador usa los valores y las opciones que introdujo en la línea de comandos para interpretar las elecciones de instalación y las opciones de configuración que son específicas para Horizon Client.

La siguiente tabla muestra las opciones de la línea de comandos y los valores de la propiedad MSI que se envían al instalador MSI.

Tabla 2-4. Opciones de la línea de comandos y de las propiedades MSI

Propiedad u opción MSI	Descripción
`/qn`	Envía instrucciones al instalador MSI para que no muestre las páginas del asistente de instalación. Por ejemplo, es posible que quiera instalar el agente de forma silenciosa y usar únicamente las funciones y las opciones de configuración predeterminadas: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn"` En los ejemplos, *xxxxxx* es el número de compilación e *y.y.y* es el número de la versión. También puede utilizar las opciones `/qr` o `/qb` para realizar una instalación automatizada y no interactiva. Con la opción `/qr`, aparecerán las páginas del asistente durante el proceso de instalación, pero no podrá responder a los mensajes. Con la opción `/qb`, aparecerá una barra indicadora de progreso sencilla. Las opciones `/qn`, `/qb` o `/qr` son necesarias para realizar una instalación no interactiva.
`INSTALLDIR`	(Opcional) Especifica una ruta de instalación alternativa para el directorio de instalación. Use el formato *`INSTALLDIR=path`* para especificar una ruta de instalación. Puede ignorar la propiedad MSI si desea instalar el cliente en la ruta predeterminada.

Tabla 2-4. Opciones de la línea de comandos y de las propiedades MSI (Continua)

Propiedad u opción MSI	Descripción
ADDLOCAL	(Opcional) Determina las funciones específicas del componente que se instalarán. En una instalación interactiva, el instalador muestra las opciones de configuración personalizadas para que las seleccione. La propiedad MSI ADDLOCAL le permite especificar estas opciones de configuración en la línea de comandos. Para instalar todas las opciones de configuración personalizadas disponibles, introduzca ADDLOCAL=ALL. Por ejemplo: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" Si no usa la propiedad MSI (ADDLOCAL), se instalan las opciones de configuración predeterminadas. Para especificar opciones individuales de configuración, introduzca una lista separada por comas de los nombres de las opciones de configuración. No use espacios entre los nombres. Utilice el formato *ADDLOCAL=valor,valor,valor....* Por ejemplo, es posible que quiera instalar el cliente con la función Redireccionamiento USB pero sin la función Iniciar sesión como usuario actual: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,USB"
LOGINASCURRENTUSER_DISPLAY	(Opcional) Determina si la casilla de verificación **Iniciar sesión como usuario actual** se muestra en el cuadro de diálogo de conexiones de Horizon Client. Los valores válidos son 1 (habilitado) y 0 (deshabilitado). El predeterminado es 1, lo que supone que la casilla de verificación está visible y los usuarios pueden marcarla, desmarcarla y sobrescribir el valor predeterminado. Cuando está oculta, los usuarios no pueden sustituir su valor predeterminado en el cuadro de diálogo de conexiones de Horizon Client.
LOGINASCURRENTUSER_DEFAULT	(Opcional) Especifica el valor predeterminado de la casilla de verificación **Iniciar sesión como usuario actual** en el cuadro de diálogo de conexiones de Horizon Client. Los valores válidos son 1 (habilitado) y 0 (deshabilitado). No existe ningún valor predeterminado, lo que supone que la casilla de verificación está desmarcada y los usuarios deben proporcionar información de credenciales y de identidad varias veces antes de poder acceder a un escritorio remoto. Cuando se selecciona la casilla de verificación **Iniciar sesión como usuario actual**, la información de credencial e identidad proporcionada por el usuario al iniciar sesión en el sistema cliente se transmite a la instancia del servidor de conexión y, por último, al escritorio remoto. Utilice esta opción junto con la opción LOGINASCURRENTUSER_DISPLAY . Por ejemplo: LOGINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 Si un usuario ejecuta Horizon Client desde la línea de comandos y especifica la opción logInAsCurrentUser, dicho valor sustituye esta configuración.
REBOOT	(Opcional) Puede usar la opción REBOOT=ReallySuppress para suprimir todos los reinicios, así como los mensajes de reinicio.
/l*v *archivo_de_registro*	(Opcional) Escribe información de registro en el archivo de registro especificado. Por ejemplo: /l*v ""%TEMP%\vmmsi.log"" Este ejemplo genera un archivo de registro detallado que es similar al que se genera durante una instalación interactiva. Puede usar esta opción para registrar funciones personalizadas que únicamente se puedan aplicar a su instalación. Es posible utilizar la información guardada para especificar funciones de instalación en futuras instalaciones silenciosas.

Ejemplo: Ejemplos de instalación

En los siguientes ejemplos, *xxxxxx* es el número de compilación, *y.y.y* es el número de versión, *carpeta_instalación* es la ruta de la carpeta de instalación y view.miempresa.com es el nombre de una instancia ficticia del servidor de conexión.

Ejemplo de instalación predeterminada:

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress
INSTALLDIR=carpeta_instalación ADDLOCAL=ALL DESKTOP_SHORTCUT=1 STARTMENU_SHORTCUT=1
VDM_SERVER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

Ejemplo de configuración e instalación para la función Iniciar sesión como usuario actual:

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn INSTALLDIR=carpeta_instalación
ADDLOCAL=Core,TSSO LOGINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 DESKTOP_SHORTCUT=1
STARTMENU_SHORTCUT=1 VDM_SERVER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

En este ejemplo, se omite `REBOOT=ReallySuppress` porque la opción `TSSO` (iniciar sesión como el usuario actual del dominio de Windows) requiere que se reinicie el sistema.

Actualizar Horizon Client en línea

Puede actualizar Horizon Client en línea si la función de actualización en línea está habilitada. Esta función está deshabilitada de forma predeterminada.

Para habilitar esta función, modifique la configuración de directivas de grupo `Enable Horizon Client online update` y `URL for Horizon Client online update`. Si desea obtener más información, consulte "Configuración general para los GPO cliente," página 57.

Prerequisitos

- Guarde su trabajo antes de actualizar Horizon Client. Es posible que la actualización haga que el sistema se reinicie.
- Compruebe que pueda iniciar sesión como administrador en el sistema cliente.

Procedimiento

1 Inicie sesión como administrador.

2 En Horizon Client, haga clic en **Actualizaciones de software** en una de las dos pantallas.

Pantalla de Horizon Client	Acción
Antes de conectarse a un servidor de conexión	Haga clic en **Opciones > Actualizaciones de software**.
Tras conectarse a un servidor de conexión	Haga clic en **Ayuda > Actualizaciones de software**.

3 Haga clic en **Buscar actualizaciones**.

4 Haga clic en **Descargar e instalar**.

Configurar Horizon Client para usuarios finales 3

La configuración de Horizon Client para usuarios finales puede incluir la configuración de los URI para iniciar Horizon Client, del modo de verificación del certificado y de las opciones avanzadas de TLS/SSL, así como el uso de los archivos de plantillas ADM y ADMX de la directiva de grupo para configurar las opciones personalizadas.

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 3-1. Opciones de configuración comunes

Ajuste	Mecanismos de configuración
Dirección del servidor de conexión	URI, directiva de grupo, línea de comandos y registro de Windows
Nombre de usuario de Active Directory	URI, directiva de grupo, línea de comandos y registro de Windows
Nombre de dominio	URI, directiva de grupo, línea de comandos y registro de Windows
Nombre del escritorio para mostrar	URI, directiva de grupo y línea de comandos
Tamaño de la ventana	URI, directiva de grupo y línea de comandos
Protocolo de visualización	URI y línea de comandos

Tabla 3-1. Opciones de configuración comunes (Continua)

Ajuste	Mecanismos de configuración
Configurar la comprobación del certificado	Directiva de grupo, registro de Windows
Configurar protocolos SSL y algoritmos criptográficos	Directiva de grupo, registro de Windows

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 usuario de RSA SecurID o RADIUS (si es distinto al 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
- Opciones para redirigir dispositivos USB

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

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 3-2. 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.

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

Valor	Descripción
`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.
`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`**.

connectUSBOnInsert

Conecta un dispositivo USB al escritorio en primer plano al conectar el dispositivo. Esta consulta se establece de forma implícita si especifica la consulta `unattended`. Para utilizar esta consulta, debe establecer la consulta `action` en **`start-session`** o bien no tener una consulta `action`. Los valores válidos son **`yes`** y **`no`**. Un ejemplo de sintaxis es **`connectUSBOnInsert=yes`**.

connectUSBOnStartup

Redirecciona al escritorio todos los dispositivos USB conectados actualmente al sistema cliente. Esta consulta se establece de forma implícita si especifica la consulta `unattended`. Para utilizar esta consulta, debe establecer la consulta `action` en **`start-session`** o bien no tener una consulta `action`. Los valores válidos son **`yes`** y **`no`**. Un ejemplo de sintaxis es **`connectUSBOnStartup=yes`**.

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 3-3. 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.

Tabla 3-3. Valores válidos para la consulta desktopLayout (Continua)

Valor	Descripción
`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`.

filePath

Especifica la ruta del archivo del sistema local que desea abrir con la aplicación remota. Debe utilizar la ruta completa, incluida la letra de unidad. 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`**.

Por ejemplo, para representar la ruta de archivo `C:\test file.txt`, utilice **`C%3A%5Ctest%20file.txt`**.

tokenUserName

Especifica el nombre de usuario de RSA o RADIUS. Utilice esta consulta solo si el nombre de usuario de RSA o RADIUS es diferente al de Active Directory. Si no especifica esta consulta y se necesita la autenticación RSA o RADIUS, se utilizará el nombre de usuario de Windows. La sintaxis es **`tokenUserName=`*`name`***.

unattended

Crea una conexión de servidor a un escritorio remoto en el modo de pantalla completa. Si utiliza esta consulta, no especifique información de usuario si generó el nombre de usuario a partir de la dirección MAC del dispositivo cliente. Sin embargo, si creó nombres de cuenta personalizados en ADAM (por ejemplo, nombres que empiecen con "custom-"), deberá especificar la información de la cuenta.

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`**.

unauthenticatedAccessEnabled

Si esta opción está establecida como **`true`**, la función Acceso sin autenticar está habilitada de forma predeterminada. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** aparece seleccionada y visible en la interfaz de usuario. Si esta opción está establecida como **`false`**, la función Acceso sin autenticar está deshabilitada. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está desmarcada y oculta. Cuando esta

	opción está establecida como **""**, la función Acceso sin autenticar está deshabilitada y la opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está deshabilitada y no aparece en la interfaz de usuario. 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.

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://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true`

Este URI tiene el mismo efecto que el primer ejemplo y todos los dispositivos USB conectados al sistema cliente se redireccionan al escritorio remoto.

10 `vmware-view://`

Este URI inicia Horizon Client si aún no está en ejecución o bien cambia Horizon Client a primer plano si ya se está ejecutando.

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

Inicia Notepad++ en el servidor 10.10.10.10 y envía el argumento `Nuevo archivo.txt` al comando del inicio de la aplicación. Para salir de los espacios y las comillas dobles, se utiliza el porcentaje. El nombre del archivo aparece entre comillas dobles porque contiene espacios.

También puede escribir este comando en la solicitud de la línea de comandos de Windows mediante la siguiente sintaxis:

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

En este ejemplo, las comillas dobles se incluyen en esta secuencia de escape utilizando los caracteres \".

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

Inicia Notepad++ 12 en el servidor 10.10.10.10 y envía el argumento `a.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`.

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

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

Ejemplos de códigos HTML

Si lo desea, puede utilizar los URI para hacer que los botones y los vínculos de hipertexto se incluyan en correos electrónicos o en páginas web. Los siguientes ejemplos muestran cómo usar el URI en el primer ejemplo de URI para codificar un vínculo de hipertexto 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," página 45.

Use los archivos de plantilla ADM o ADMX Configuración cliente (`vdm_client.adm` o `vdm_client.admx`) para establecer el modo de verificación. Todos los archivos ADM y ADMX proporcionados por la configuración de las directivas de grupo están disponibles en un archivo `.zip` con el nombre `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, donde *x.x.x* es la versión y *yyyyyyy* es el número de compilación. Puede descargar el paquete GPO desde el sitio de descargas de VMware Horizon en http://www.vmware.com/go/downloadview. Para obtener más información acerca de cómo usar esta plantilla para controlar la configuración GPO, consulte "Usar la plantilla de directiva de grupo para configurar VMware Horizon Client para Windows," página 47.

NOTA: También puede usar el archivo de plantilla ADM o ADMX Configuración de cliente para restringir el uso de ciertos algoritmos criptográficos y protocolos antes de establecer una conexión SSL cifrada. Para obtener más información acerca de esta opción, consulte "Configuración de seguridad para los GPO cliente," página 50.

Si no desea configurar la opción de la verificación del certificado como una directiva de grupo, puede habilitar esta verificación al agregar el nombre de valor `CertCheckMode` a una de las siguientes claves de registro en el equipo cliente:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Para Windows de 64 bits: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Use los siguientes valores en las claves de registro:

- **`0`** implements `Do not verify server identity certificates`.
- **`1`** implements `Warn before connecting to untrusted servers`.
- **`2`** implements `Never connect to untrusted servers`.

Si configura tanto la opción de la directiva de grupo como la de `CertCheckMode` en la clave de registro, la opción de la directiva de grupo tiene prioridad sobre el valor de la clave de registro.

NOTA: En una versión futura, es posible que no sea compatible configurar esta opción mediante el registro de Windows. Se debe usar una configuración GPO.

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:

- ¿Se revocó el certificado?
- ¿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 en todos los sistemas cliente de Windows en un dominio, consulte "Agregar el certificado raíz a entidades de certificación raíz de confianza" en el documento Instalación de *View*.

Cuando utilice Horizon Client para iniciar sesión en un escritorio, si su administrador lo ha permitido, puede hacer clic en **Configurar SSL** para establecer el modo de comprobación del certificado. 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.

  También puede recibir una advertencia si el certificado expiró.

- **No comprobar los certificados de identidad de los servidores**. Esta opción significa que no se ha llevado a cabo ninguna comprobación del certificado.

Si el modo de comprobación del certificado está establecido en el estado de **advertencia**, puede seguir conectándose a una instancia del servidor de conexión que utilice un certificado autofirmado.

Si un administrador instala más tarde un certificado de seguridad desde una entidad de certificación de confianza (de forma que se superen todas las comprobaciones de certificados al realizar la conexión), esta conexión de confianza se recordará para este servidor específico. En el futuro, si este servidor volviera a presentar un certificado autofirmado, se producirá un error de conexión. Después de que un servidor concreto presente un certificado que pueda comprobarse en su totalidad, siempre debe hacerse.

IMPORTANTE: Si configuró previamente los sistemas cliente de su empresa para utilizar un cifrado específico a través de GPO como, por ejemplo, al configurar los ajustes de la directiva de grupo Orden de conjuntos de claves de cifrado SSL, ahora debe utilizar una configuración de directiva de grupo de Horizon Client incluida en los archivos de plantillas ADM y ADMX. Consulte "Configuración de seguridad para los GPO cliente," página 50. También puede utilizar la configuración del registro `SSLCipherList` en el cliente. Consulte "Utilizar el Registro de Windows para configurar Horizon Client," página 70.

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 de seguridad también se utilizan para cifrar el canal USB.

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 una opción de directiva de grupo o una opción del Registro de Windows para cambiar los protocolos y los cifrados predeterminados. Para obtener más información sobre el uso de un GPO, consulte la opción denominada "Configurar protocolos SSL y algoritmos criptográficos" en "Configuración de seguridad para los GPO cliente," página 50. Para obtener más información sobre el uso de la opción SSLCipherList en el Registro de Windows, consulte "Utilizar el Registro de Windows para configurar Horizon Client," página 70.

Configurar el comportamiento de reconexión de las aplicaciones

Al desconectarse de un servidor, es posible que las aplicaciones en ejecución permanezcan abiertas. Puede configurar el comportamiento de las aplicaciones en ejecución al volver a conectarse al servidor.

Un administrador de Horizon puede deshabilitar la configuración correspondiente al comportamiento de reconexión de las aplicaciones en Horizon Client, ya sea desde la línea de comandos o configurando una opción de directiva de grupo. La opción de directiva de grupo tiene prioridad sobre la opción de la línea de comandos. Para obtener más información, consulte la opción `–appSessionReconnectionBehavior` en "Uso de los comandos de Horizon Client," página 65 o la opción de directiva de grupo **Comportamiento de reanudación de las sesiones de aplicaciones desconectadas** en "Configuración de la definición de scripting para los GPO cliente," página 48.

Procedimiento

1 En la ventana para seleccionar una aplicación y un escritorio de Horizon Client, haga clic con el botón secundario en una aplicación remota y seleccione **Configuración**.

2 En el panel Aplicaciones remotas que aparece, seleccione una opción correspondiente al comportamiento de reconexión de las aplicaciones.

Opción	Descripción
Solicitar volver a conectarse a las aplicaciones abiertas	Horizon Client le indica que tiene una o varias aplicaciones remotas ejecutándose al volver a conectarse al servidor. Puede hacer clic en **Volver a conectarse a las aplicaciones** para volver a abrir las ventanas de las aplicaciones o en **Ahora no** para no volver a abrir estas ventanas.
Volver a conectarse automáticamente a las aplicaciones abiertas	Las ventanas de las aplicaciones en ejecución se vuelven a abrir automáticamente al conectarse al servidor de nuevo.
No solicitar volver a conectarse y no conectarse automáticamente	Horizon Client no le solicita que vuelva a abrir las aplicaciones en ejecución y sus ventanas no se vuelven a abrir al conectarse al servidor de nuevo.

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

Esta opción se aplicará la próxima vez que se conecte al servidor.

Usar la plantilla de directiva de grupo para configurar VMware Horizon Client para Windows

VMware Horizon Client incluye archivos de plantillas ADM y ADMX de la directiva de grupo que puede utilizar para configurar VMware Horizon Client. Puede optimizar y establecer conexiones seguras al escritorio remoto al agregar la configuración de la directiva del archivo de plantilla ADM o ADMX en un GPO nuevo o ya existente en Active Directory.

Los archivos de plantillas contienen tanto las directivas de grupo Configuración de usuario como las de Configuración del equipo.

- Las directivas Configuración del equipo se aplican a Horizon Client, independientemente de quién ejecute el cliente en el host.
- Sin embargo, la Configuración de usuario establece directivas de Horizon Client que se aplican a todos los usuarios que ejecutan Horizon Client, así como la configuración de la conexión RDP. Las directivas Configuración de usuario sobrescriben las equivalentes de Configuración del equipo.

Horizon aplica las directivas al iniciar el escritorio y cuando el usuario inicia sesión.

Los archivos de plantillas ADM y ADMX Configuración de Horizon Client (`vdm_client.adm` y `vdm_client.admx`) y todos los archivos ADM y ADMX proporcionados por la configuración de las directivas de grupo están disponibles en un archivo `.zip` con el nombre `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, donde *x.x.x* es la versión y *yyyyyyy* es el número de compilación. Puede descargar los archivos desde el sitio web de descargas de VMware Horizon en http://www.vmware.com/go/downloadview. Debe copiar estos archivos en el servidor de Active Directory y usar el Editor de administración de directivas de grupo para agregar las plantillas administrativas. Para obtener instrucciones, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Configuración de la definición de scripting para los GPO cliente

Es posible establecer directivas para muchas de las opciones usadas cuando ejecuta VMware Horizon Client desde la línea de comandos, incluidos el nombre del dominio, el nombre y el tamaño del escritorio, entre otros.

La siguiente tabla describe la configuración de la definición de scripting en los archivos de plantillas ADM y ADMX Configuración de VMware Horizon Client. Los archivos de plantillas proporcionan una versión de la configuración de usuario y de equipo para cada opción de definición de scripting. Las opciones de configuración de usuario reemplazan las del equipo equivalente.

Tabla 3-4. Plantilla de configuración de VMware Horizon Client : definiciones de scripting

Ajuste	Descripción
`Automatically connect if only one launch item is entitled`	Se conecta automáticamente al escritorio si es el único autorizado para el usuario. Esta opción evita que el usuario tenga que seleccionar el escritorio en una lista que solo contiene un elemento.
`Connect all USB devices to the desktop on launch`	Determina si todos los dispositivos USB disponibles en el sistema cliente se conectan al escritorio al iniciarlo.
`Connect all USB devices to the desktop when they are plugged in`	Determina si los dispositivos USB se conectan al escritorio cuando se insertan en el sistema cliente.
`DesktopLayout`	Especifica el diseño de la ventana VMware Horizon Client que ve un usuario al iniciar sesión en un escritorio remoto. Las opciones de diseño son las siguientes: ■ `Full Screen` ■ `Multimonitor` ■ `Window – Large` ■ `Window – Small` Esta configuración está disponible solo cuando `DesktopName to select setting` también está configurado.
`DesktopName to select`	Especifica el escritorio predeterminado que VMware Horizon Client usa en el inicio de sesión.
`Disable 3rd-party Terminal Services plugins`	Determina si VMware Horizon Client verifica los complementos de Terminal Services de terceros que están instalados como complementos RDP normales. Si no configura esta opción, VMware Horizon Client verifica los complementos de terceros predeterminados. Estas opciones no afectan a los complementos específicos de Horizon, como el redireccionamiento USB.

Tabla 3-4. Plantilla de configuración de VMware Horizon Client : definiciones de scripting (Continua)

Ajuste	Descripción
`Locked Guest Size`	Especifica la resolución de pantalla del escritorio remoto si la visualización se realiza en un solo monitor. Esto significa que estas opciones no funcionan si establece que se visualice el escritorio remoto en todos los monitores. Después de habilitar esta opción, la función de autoajuste del escritorio remoto está deshabilitada. El tamaño mínimo de la pantalla es 640 x 480. El tamaño máximo de la pantalla es 4096 x 4096. Esta opción solo se aplica a las conexiones PCoIP y no a las conexiones RDP. **IMPORTANTE:** Como práctica recomendada, no establezca la resolución en un valor superior a la resolución máxima admitida por el escritorio remoto, configurada en Horizon Administrator: ■ Si se habilita la visualización 3D, se admiten hasta 2 monitores con una resolución máxima de 1920 x 1200. ■ Si el procesamiento 3D no está habilitado, se admiten hasta 4 monitores con una resolución máxima de 2560 x 1600. En la práctica, esta opción del lado del cliente se ignorará si está configurada con una resolución superior a la permitida, dada la versión del sistema operativo, la cantidad de vRAM y la profundidad de color del escritorio remoto. Por ejemplo, si la resolución en este escritorio está establecida en 1920 x 1200 en Horizon Administrator, la resolución que se muestra en el cliente no podrá ser superior a este valor, dependiendo de las capacidades del escritorio remoto.
`Logon DomainName`	Especifica el dominio NetBIOS que Horizon Client usa en el inicio de sesión.
`Logon Password`	Especifica la contraseña que Horizon Client usa en el inicio de sesión. Active Directory almacena la contraseña en texto sin formato. Para mejorar la seguridad, se recomienda que no especifique esta opción. Los usuarios pueden introducir la contraseña de forma interactiva.
`Logon UserName`	Especifica la contraseña que Horizon Client usa en el inicio de sesión. Active Directory almacena la contraseña en texto sin formato.
`Server URL`	Especifica la URL que Horizon Client usa durante el inicio de sesión, por ejemplo, `https://view1.example.com`.
`Suppress error messages (when fully scripted only)`	Determina si los mensajes de error de Horizon Client se ocultan durante el inicio de sesión. Esta opción solo se aplica cuando el proceso de inicio de sesión se genera totalmente por script, por ejemplo, cuando toda la información necesaria para iniciar sesión aparece rellena según la directiva. Si se produce un error en el inicio de sesión debido a que la información proporcionada no es correcta, el usuario no recibirá ninguna notificación y se finalizará el proceso de Horizon Client.
`Disconnected application session resumption behavior`	Determina el comportamiento de las aplicaciones en ejecución cuando un usuario se vuelve a conectar a un servidor. Las opciones son las siguientes: ■ Solicitar volver a conectarse a las aplicaciones abiertas ■ Volver a conectarse automáticamente a las aplicaciones abiertas ■ No solicitar volver a conectarse y no conectarse automáticamente Cuando esta opción está habilitada, los usuarios finales no pueden configurar el comportamiento de reconexión de las aplicaciones en la página Configuración de Horizon Client. Cuando esta opción está deshabilitada, los usuarios finales pueden configurar el comportamiento de reconexión de las aplicaciones en Horizon Client. Esta opción está deshabilitada de forma predeterminada.

Tabla 3-4. Plantilla de configuración de VMware Horizon Client : definiciones de scripting (Continua)

Ajuste	Descripción
`Enable Unauthenticated Access to the server`	Determina si se requiere a los usuarios que introduzcan sus credenciales para acceder a sus aplicaciones mediante Horizon Client. Si esta opción está habilitada, la opción **Iniciar sesión de forma anónima con Acceso sin autenticar** de Horizon Client está visible, deshabilitada y seleccionada. El posible que el cliente tenga que recurrir de nuevo a otro método de autenticación si la función Acceso sin autenticar no está disponible. Si esta opción está deshabilitada, siempre se requiere al usuario que introduzca sus credenciales para iniciar sesión y acceder a sus aplicaciones. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** de Horizon Client está oculta y desmarcada. Si esta opción no está configurada (la predeterminada), el usuario puede habilitar la función Acceso sin autenticar en Horizon Client. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está visible, habilitada y desmarcada.
`Account to use for Unauthenticated Access`	Especifica la cuenta de usuario de acceso sin autenticar que Horizon Client utiliza para iniciar sesión de forma anónima en el servidor si la opción de la directiva de grupo `Enable Unauthenticated Access to the server` está habilitada o si el usuario habilita Acceso sin autenticar mediante la selección de **Iniciar sesión de forma anónima con Acceso sin autenticar** en Horizon Client. Si la opción Acceso sin autenticar no se utiliza para una conexión específica a un servidor, se ignorará. Si esta opción no está configurada, el usuario puede elegir una cuenta. Esta opción no está configurada de forma predeterminada.

Configuración de seguridad para los GPO cliente

La configuración de seguridad incluye las opciones del certificado de seguridad, credenciales de inicio de sesión y la función Single Sign-On.

La siguiente tabla describe la configuración de seguridad en los archivos de plantillas ADM y ADMX Configuración de Horizon Client. Esta tabla muestra si las opciones incluyen la configuración de usuario y de equipo o únicamente esta última. En la configuración de seguridad que incluye ambos tipos, la de usuario reemplaza las opciones de configuración de equipo.

Tabla 3-5. Plantilla de configuración de Horizon Client : configuración de seguridad

Ajuste	Descripción
`Allow command line credentials` (Parámetro de configuración de equipos)	Determina si se pueden proporcionar credenciales de usuario con opciones de línea de comandos de Horizon Client. Si esta configuración está deshabilitada, las opciones `smartCardPIN` y `password` no estarán disponibles cuando los usuarios ejecuten Horizon Client desde la línea de comandos. Esta configuración está habilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `AllowCmdLineCredentials`.
`Servers Trusted For Delegation` (Parámetro de configuración de equipos)	Especifica las instancias del servidor de conexión que aceptan la información de credencial e identidad de usuario que se transmite cuando un usuario selecciona la casilla de verificación **Iniciar sesión como usuario actual**. Si no especifica ninguna instancia del servidor de conexión, todas ellas aceptan esta información. Para agregar una instancia del servidor de conexión, use uno de los siguientes formatos: ■ **`dominio\sistema$`** ■ **`sistema$@dominio.com`** ■ El nombre de entidad de seguridad de servicio (SPN) del servicio del servidor de conexión. El valor equivalente en el Registro de Windows es `BrokersTrustedForDelegation`.

Tabla 3-5. Plantilla de configuración de Horizon Client : configuración de seguridad (Continua)

Ajuste	Descripción
`Certificate verification mode` (Parámetro de configuración de equipos)	Configura el nivel de comprobación de certificados que realiza Horizon Client. Puede seleccionar uno de estos modos: ■ `No Security`. Horizon no realiza la comprobación de certificados. ■ `Warn But Allow`. Horizon proporciona un certificado autofirmado. En este caso, se acepta si el nombre del certificado no coincide con el nombre del servidor de conexión proporcionado por el usuario en Horizon Client. Si se produce cualquier otra situación de error relacionada con certificados, Horizon muestra un cuadro de diálogo de error e impide que el usuario se conecte al servidor de conexión. `Warn But Allow` es el valor predeterminado. ■ `Full Security`. Si se produce cualquier tipo de error relacionado con los certificados, el usuario no podrá conectarse al servidor de conexión. Horizon muestra al usuario los errores relacionados con los certificados. Cuando se define esta configuración de directiva de grupo, los usuarios pueden consultar el modo de verificación de certificados seleccionado en Horizon Client, pero no pueden modificar esta configuración. El cuadro de diálogo de configuración de SSL informa a los usuarios de que el administrador ha bloqueado la configuración. Cuando esta configuración no está definida o está deshabilitada, los usuarios de Horizon Client pueden seleccionar un modo de verificación de certificados. Para permitir a un servidor que realice la comprobación de los certificados proporcionados por Horizon Client, el cliente debe realizar conexiones HTTPS con el host del servidor de seguridad o el servidor de conexión. La comprobación de certificados no se admite si transfiere la SSL a un dispositivo intermedio que establezca conexiones HTTP con el servidor de conexión o con el host del servidor de seguridad. Si no desea configurar esta opción como una directiva de grupo, puede habilitar esta verificación al agregar el nombre de valor `CertCheckMode` a una de las siguientes claves del Registro en el equipo cliente: ■ Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ Para Windows de 64 bits: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security` Use los siguientes valores en la clave del Registro: ■ **`0`** implements `No Security`. ■ **`1`** implements `Warn But Allow`. ■ **`2`** implements `Full Security`. Si configura tanto la opción de la directiva de grupo como la de `CertCheckMode` en la clave del Registro de Windows, la opción de la directiva de grupo tiene prioridad sobre el valor de la clave del Registro. **NOTA:** En una versión futura, es posible que no sea compatible configurar esta opción mediante el registro de Windows. Se debe usar una configuración GPO.

Tabla 3-5. Plantilla de configuración de Horizon Client : configuración de seguridad (Continua)

Ajuste	Descripción
`Default value of the 'Log in as current user' checkbox` (Parámetro de configuración de usuarios y equipos)	Especifica el valor predeterminado de la casilla de verificación **Iniciar sesión como usuario actual** en el cuadro de diálogo de conexiones de Horizon Client. Esta configuración sustituye el valor predeterminado especificado durante la instalación de Horizon Client. Si un usuario ejecuta Horizon Client desde la línea de comandos y especifica la opción `logInAsCurrentUser`, dicho valor sustituye esta configuración. Cuando se selecciona la casilla de verificación **Iniciar sesión como usuario actual**, la información de credencial e identidad proporcionada por el usuario al iniciar sesión en el sistema cliente se transmite a la instancia del servidor de conexión y, por último, al escritorio remoto. Cuando esta casilla de verificación no está seleccionada, los usuarios deberán proporcionar la información de credencial e identidad varias veces para poder obtener acceso a un escritorio remoto. Esta opción está deshabilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `LogInAsCurrentUser`.
`Display option to Log in as current user` (Parámetro de configuración de usuarios y equipos)	Determina si la casilla de verificación **Iniciar sesión como usuario actual** se muestra en el cuadro de diálogo de conexiones de Horizon Client. Cuando se muestra esta casilla de verificación, los usuarios pueden seleccionarla o anular su selección y sustituir su valor predeterminado. Cuando está oculta, los usuarios no pueden sustituir su valor predeterminado en el cuadro de diálogo de conexiones de Horizon Client. La configuración de directivas `Default value of the 'Log in as current user' checkbox` permite especificar el valor predeterminado de la casilla de verificación **Iniciar sesión como usuario actual**. Esta configuración está habilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `LogInAsCurrentUser_Display`.
`Enable jump list integration` (Parámetro de configuración de equipos)	Determina si se muestra una lista de accesos directos en el icono de Horizon Client de la barra de tareas de Windows 7 y sistemas posteriores. La lista de accesos directos permite a los usuarios conectarse a escritorios remotos y a instancias recientes del servidor de conexión. Si se comparte Horizon Client, es posible que no desee que los usuarios puedan ver los nombres de los escritorios recientes. Deshabilite esta configuración para deshabilitar la lista de accesos directos. Esta configuración está habilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `EnableJumplist`.
`Enable SSL encrypted framework channel` (Parámetro de configuración de usuarios y equipos)	Determina si SSL está habilitada para escritorios View 5.0 y anteriores. Antes de View 5.0, no se cifraban los datos enviados al escritorio a través del puerto TCP 32111. ■ **Habilitar**: habilita SSL, pero permite recurrir a la conexión no cifrada anterior si el escritorio remoto no admite SSL. Por ejemplo, los escritorios View 5.0 y anteriores no admiten SSL. **Habilitar** es la configuración predeterminada. ■ **Deshabilitar**: deshabilita SSL. No se recomienda esta configuración, pero puede resultar útil para tareas de depuración o si no hay un túnel de canal y se podría optimizar mediante un producto acelerador de WAN. ■ **Exigir**: habilita SSL e impide la conexión a escritorios que no admitan SSL. El valor equivalente en el Registro de Windows es `EnableTicketSSLAuth`.

Tabla 3-5. Plantilla de configuración de Horizon Client : configuración de seguridad (Continua)

Ajuste	Descripción
`Configures SSL protocols and cryptographic algorithms` (Parámetro de configuración de usuarios y equipos)	Configura la lista de cifrado para restringir el uso de ciertos protocolos y algoritmos criptográficos antes de establecer una conexión SSL cifrada. La lista de cifrado consta de una o más cadenas de cifrado separadas por dos puntos. **NOTA:** La cadena de cifrado distingue entre mayúsculas y minúsculas. El valor predeterminado es **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Esto significa que se habilitan TLS v1, TLS v1.1 y TLS v1.2. (Se han eliminado SSL v2.0 y v3.0). 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. Vínculo de referencia para la configuración: http://www.openssl.org/docs/apps/ciphers.html El valor equivalente en el Registro de Windows es `SSLCipherList`.
`Enable Single Sign-On for smart card authentication` (Parámetro de configuración de equipos)	Determina si Single Sign-On está habilitado para la autenticación de tarjeta inteligente. Cuando Single Sign-On está habilitado, Horizon Client almacena el PIN de la tarjeta inteligente cifrada en una memoria temporal antes de enviarlo al servidor de conexión. Cuando está deshabilitado, Horizon Client no muestra un cuadro de diálogo de PIN deshabilitado. El valor equivalente en el Registro de Windows es `EnableSmartCardSSO`.
`Ignore bad SSL certificate date received from the server` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con fechas de certificado de servidor no válidas. Estos errores se producen cuando un servidor envía un certificado con una fecha ya pasada. El valor equivalente en el Registro de Windows es `IgnoreCertDateInvalid`.
`Ignore certificate revocation problems` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con un certificado de servidor revocado. Estos errores se producen cuando el servidor envía un certificado que se ha revocado y cuando el cliente no puede verificar un estado de revocación de un certificado. Esta opción está deshabilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `IgnoreRevocation`.
`Ignore incorrect SSL certificate common name (host name field)` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con nombres comunes de certificado de servidor incorrectos. Estos errores se producen cuando el nombre común del certificado no coincide con el nombre de host del servidor que lo envía. El valor equivalente en el Registro de Windows es `IgnoreCertCnInvalid`.
`Ignore incorrect usage problems` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con el uso incorrecto de un certificado de servidor. Estos errores se producen cuando el servidor envía un certificado con un objetivo diferente al de verificar la identidad del remitente y cifrar las comunicaciones del servidor. El valor equivalente en el Registro de Windows es `IgnoreWrongUsage`.
`Ignore unknown certificate authority problems` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con una entidad de certificación desconocida (CA) en el certificado de servidor. Estos errores se producen cuando el servidor envía un certificado firmado por una entidad de certificación que no es de confianza. El valor equivalente en el Registro de Windows es `IgnoreUnknownCa`.

Configuración RDP para los GPO cliente

Cuando utiliza el protocolo de visualización Microsoft RDP, es posible configurar directivas de grupo para ciertas opciones como, por ejemplo, el redireccionamiento de audio, las impresoras, los puertos y otros dispositivos.

La siguiente tabla describe la configuración del Protocolo de escritorio remoto (RDP) en los archivos de plantillas ADM y ADMX Configuración de Horizon Client. Todas las opciones RDP son opciones de Configuración de usuario.

Tabla 3-6. Plantilla administrativa de configuración de Horizon Client : configuración de RDP

Ajuste	Descripción
`Audio redirection`	Determina si se redirecciona la información de audio que se reproduce en el escritorio remoto. Seleccione una de las siguientes opciones: ■ **Deshabilitar audio**: el audio está deshabilitado. ■ **Reproducir en la máquina virtual (necesaria para la compatibilidad USB VoIP)**: el audio se reproduce en el escritorio remoto. Esta opción necesita un dispositivo de audio USB compartido para proporcionar sonido al cliente. ■ **Redireccionamiento al cliente**: el audio se redirecciona al cliente. Este modo es el predeterminado. Esta opción se aplica únicamente al audio RDP. El audio que se redirecciona a través de MMR se reproduce en el cliente.
`Enable audio capture redirection`	Determina si el dispositivo de entrada de audio se redirecciona desde el cliente a la sesión remota. Cuando esta opción está habilitada, el dispositivo de grabación de audio del cliente aparece en el escritorio remoto y puede grabar la entrada de audio. Esta opción aparece como deshabilitada de forma predeterminada.
`Bitmap cache file size in` *Unidad* `for` *número* `bpp bitmaps`	Especifica el tamaño de la caché del mapa de bits, en kilobytes o megabytes, que se usará en cada configuración específica de bits por píxel (bpp) para los colores de los mapas de bits. Hay disponibles distintas versiones de este ajuste para las siguientes combinaciones de unidades y bpp: ■ KB/8bpp ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`Bitmap caching/cache persistence active`	Determina si se usa un almacenamiento en caché persistente de mapas de bits (activa). El almacenamiento en caché persistente de mapa de bits puede mejorar el rendimiento, pero requiere un espacio de disco adicional.
`Color depth`	Especifica la profundidad del color del escritorio remoto. Seleccione una de las opciones disponibles: ■ 8 bits ■ 15 bits ■ 16 bits ■ 24 bits ■ 32 bits En sistemas Windows XP de 24 bits, debe habilitar la directiva Limitar máxima profundidad de color en **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Terminal Services** y configurarla en 24 bits.
`Cursor shadow`	Determina si debe aparecer una sombra bajo el cursor en el escritorio remoto.
`Desktop background`	Determina si el fondo de escritorio aparece cuando el cliente se conecta a un escritorio remoto.

Tabla 3-6. Plantilla administrativa de configuración de Horizon Client : configuración de RDP (Continua)

Ajuste	Descripción
`Desktop composition`	(Windows Vista o versiones posteriores) Determina si se habilita la composición del escritorio en el escritorio remoto. Cuando esta opción está habilitada, las ventanas individuales ya no se dibujarán directamente en la pantalla o en el dispositivo de visualización primario, como sucedía en las versiones anteriores de Microsoft Windows. En su lugar, las tareas de dibujar ventanas se redireccionan a superficies fuera de la pantalla en la memoria de vídeo, que se procesan a continuación para representar una imagen de escritorio y mostrarla en la pantalla.
`Enable compression`	Determina si se comprimen los datos RDP. Esta configuración está habilitada de forma predeterminada.
`Enable RDP Auto-Reconnect`	Determina si el componente cliente RDP intenta volver a conectarse a un escritorio remoto después de un error de conexión del protocolo RDP. Esta opción no tiene efecto si está habilitada **Usar la conexión de túnel segura al escritorio** en Horizon Administrator. Esta opción está deshabilitada de forma predeterminada.
`Font smoothing`	(Windows Vista o versiones posteriores) Determina si se aplica el suavizado en las fuentes del escritorio remoto.
`Menu and window animation`	Determina si se habilita la animación para menús y ventanas cuando los clientes se conectan a un escritorio remoto.
`Redirect clipboard`	Determina si la información del portapapeles local se redirecciona cuando los clientes se conectan al escritorio remoto.
`Redirect drives`	Determina si las unidades del disco local se redireccionan cuando los clientes se conectan al escritorio remoto. De forma predeterminada, se redireccionan las unidades locales. Al habilitar esta opción, o al dejarla sin configurar, se pueden copiar los datos de la unidad redireccionada en la unidad del equipo cliente. Deshabilite esta opción si el envío de datos del escritorio remoto a los equipos cliente de los usuarios representa un riesgo potencial de seguridad en su implementación. Otra posibilidad es deshabilitar el redireccionamiento de carpetas en la máquina virtual del escritorio remoto. Para ello, es necesario habilitar la opción de directiva de grupo de Microsoft Windows, `Do not allow drive redirection`. La opción `Redirect drives` se aplica únicamente a RDP.
`Redirect printers`	Determina si las impresoras se redireccionan cuando los clientes se conectan al escritorio remoto.
`Redirect serial ports`	Determina si los puertos COM locales se redireccionan cuando los clientes se conectan al escritorio remoto.
`Redirect smart cards`	Determina si las tarjetas inteligentes locales se redireccionan cuando los clientes se conectan al escritorio remoto. **NOTA:** Esta opción se aplica a las conexiones PCoIP y RDP.
`Redirect supported plug-and-play devices`	Determina si los dispositivos de punto de venta y Plug and Play se redireccionan cuando los clientes se conectan al escritorio remoto. Este comportamiento es diferente al redireccionamiento y lo gestiona el componente Redireccionamiento USB del agente.
`Shadow bitmaps`	Determina si los mapas de bits aparecen sombreados. Esta opción no tiene efecto en modo de pantalla completa.
`Show contents of window while dragging`	Determina si el contenido de las carpetas aparece cuando los usuarios arrastran una carpeta a una ubicación nueva.

Tabla 3-6. Plantilla administrativa de configuración de Horizon Client : configuración de RDP (Continua)

Ajuste	Descripción
`Themes`	Determina si aparecen los temas cuando el cliente se conecta a un escritorio remoto.
`Windows key combination redirection`	Determina dónde se aplican las combinaciones de teclas de Windows. Esta opción le permite enviar combinaciones de teclas a las máquinas virtuales o aplicar las combinaciones de teclas de forma local. Si esta opción no está configurada, las combinaciones de teclas se aplican localmente.

Configuración general para los GPO cliente

La configuración incluye opciones de proxy, de zona horaria, de aceleración multimedia y otras opciones de visualización.

Configuración general

La siguiente tabla describe la configuración general en los archivos de plantillas ADM y ADMX Configuración de Horizon Client. La configuración general incluye las opciones de configuración de equipo y de usuario. Las opciones de configuración de usuario reemplazan las del equipo equivalente.

Tabla 3-7. Plantilla de configuración de Horizon Client : configuración general

Ajuste	Descripción
`Always on top` (Parámetro de configuración de usuario)	Determina si la ventana que está más arriba es la de Horizon Client. Al habilitar esta opción, se evita que la barra de tareas de Windows impida ver una ventana de Horizon Client en pantalla completa. Esta opción está deshabilitada de forma predeterminada.
`Default value of the "Hide the selector after launching an item" check box` (Parámetro de configuración de usuarios y equipos)	Establece si la casilla **Ocultar el selector después de iniciar un elemento** está habilitada de forma predeterminada. Esta opción está deshabilitada de forma predeterminada.
`Determines if the VMware View Client should use proxy.pac file` (Parámetro de configuración de equipos)	(Solo para View 4.6 y versiones anteriores) Determina si Horizon Client usa un archivo de configuración automática de proxy (PAC). Si se habilita esta opción, Horizon Client utilizará un archivo PAC. Los archivos PAC (comúnmente llamados `proxy.pac`) ayudan a los exploradores web y otros agentes de usuario a encontrar el servidor proxy apropiado para las solicitudes de sitio web o URL determinadas. Si habilita esta opción en un equipo de núcleo múltiple, se puede producir un fallo en la aplicación WinINet que Horizon Client usa para encontrar la información del servidor proxy. Deshabilite esta opción si se produce este problema en su equipo. Esta opción está deshabilitada de forma predeterminada. **NOTA:** Esta opción solo se aplica a conexiones directas. No afecta a las conexiones de túnel.
`Disable time zone forwarding` (Parámetro de configuración de equipos)	Determina si la sincronización de la zona horaria entre el escritorio remoto y el cliente conectado está deshabilitada.
`Disable toast notifications` (Parámetro de configuración de usuarios y equipos)	Determina si es necesario deshabilitar las notificaciones del sistema de Horizon Client. Habilite esta opción si no desea que el usuario vea notificaciones del sistema en la esquina de la pantalla. **NOTA:** Si habilita esta opción, el usuario no verá la advertencia de 5 minutos cuando está activada la función Tiempo de espera de sesión.

Tabla 3-7. Plantilla de configuración de Horizon Client : configuración general (Continua)

Ajuste	Descripción
`Disallow passing through client information in a nested session` (Parámetro de configuración de equipos)	Especifica si Horizon Client debe enviar información a través del cliente en una sesión anidada. Cuando está habilitada, si Horizon Client se ejecuta dentro de una sesión de Horizon, enviará la información del cliente físico actual en lugar de la información del dispositivo de la máquina virtual. Esta configuración se aplica a las siguientes partes de la información cliente: dominio y nombre del dispositivo, tipo de cliente, direcciones IP y MAC. Esta opción se encuentra deshabilitada por defecto, lo que significa que permite que se envíe información del cliente en una sesión anidada.
`Don't check monitor alignment on spanning` (Parámetro de configuración de usuario)	De forma predeterminada, el escritorio cliente no se expande en varios monitores si la pantalla no forma un rectángulo exacto cuando se combinan. Habilite esta opción para reemplazar la predeterminada. Esta opción está deshabilitada de forma predeterminada.
`Enable multi-media acceleration` (Parámetro de configuración de usuario)	Determina si el redireccionamiento multimedia (MMR) está habilitado en el cliente. MMR no funciona correctamente si el hardware de visualización de vídeo de Horizon Client no tiene compatibilidad overlay.
`Enable relative mouse` (Parámetro de configuración de usuarios y equipos)	(Solo para View 5.2 y versiones posteriores) Habilita el mouse relativo cuando se usa el protocolo de visualización PCoIP. El modo de mouse relativo mejora el comportamiento del mouse en juegos y aplicaciones gráficas. Si el escritorio remoto no admite el mouse relativo, no se usará esta opción. Esta opción está deshabilitada de forma predeterminada.
`Enable the shade` (Parámetro de configuración de usuario)	Determina si la barra de menús sombreada situada en la parte superior de la ventana de Horizon Client está visible. Esta configuración está habilitada de forma predeterminada. **NOTA:** La barra de menús sombreada está deshabilitada de forma predeterminada para el modo de pantalla completa.
`Enable Horizon Client online update` (Parámetro de configuración de equipos)	Habilita la función de actualización en línea. Esta opción está deshabilitada de forma predeterminada.
`Tunnel proxy bypass address list` (Parámetro de configuración de equipos)	Especifica una lista de direcciones de túnel. El servidor proxy no se usa en estas direcciones. Use un punto y coma (;) para separar varias entradas.
`URL for View Client online help` (Parámetro de configuración de equipos)	Especifique una URL alternativa desde la que Horizon Client pueda recuperar páginas de ayuda. Esta opción está destinada a entornos que no pueden recuperar el sistema de ayuda alojado de forma remota porque no tienen acceso a Internet.
`URL for Horizon Client online update` (Parámetro de configuración de equipos)	Especifique una URL alternativa desde la que Horizon Client pueda recuperar actualizaciones. Esta opción está destinada a entornos que definen su propio centro de actualización personal o privado. Si no está habilitada, se usará el servidor de actualización oficial de VMware.
`Pin the shade` (Parámetro de configuración de usuario)	Determina si se habilita que la sombra aparezca siempre en la parte superior de la ventana de Horizon Client y que la barra de menús no se oculte automáticamente. Esta opción no suerte efecto si la sombra está deshabilitada. Esta configuración está habilitada de forma predeterminada.
`Disable desktop disconnect messages` (Parámetro de configuración de usuarios y equipos)	Especifica si los mensajes que se suelen mostrar en la desconexión de los escritorios se deberían deshabilitar. Estos mensajes se muestran de forma predeterminada.

Tabla 3-7. Plantilla de configuración de Horizon Client : configuración general (Continua)

Ajuste	Descripción
`Disable sharing files and folders` (Parámetro de configuración de usuario)	Especifica si la función de redireccionamiento de unidades cliente está disponible en Horizon Client. Cuando esta opción está habilitada, la función de redireccionamiento de unidades cliente se deshabilita por completo en Horizon Client, incluida la opción para abrir archivos locales con aplicaciones remotas. Además, los siguientes elementos se ocultan en la interfaz de usuario de Horizon Client: ■ Panel Compartir del cuadro de diálogo Configuración ■ Elemento **Compartir carpetas** en el menú **Opción** de un escritorio remoto ■ Elemento **Compartir** de Horizon Client en la bandeja del sistema ■ El cuadro de diálogo Compartir que aparece la primera vez que se conecta a una aplicación o un escritorio remotos después de conectarse a un servidor Cuando esta opción está deshabilitada, la función de redireccionamiento de unidades cliente es completamente funcional. Si esta opción no se configura, el valor predeterminado es Deshabilitado. Esta opción no está configurada de forma predeterminada.
`Always hide the remote floating language (IME) bar for Hosted Apps` (Parámetro de configuración de usuarios y equipos)	Desactiva la barra de idiomas flotante en las sesiones de aplicaciones. Cuando esta opción está habilitada, la barra de idiomas flotante nunca se muestra en una sesión de una aplicación remota, independientemente de que la función IME local esté habilitada. Si esta opción está deshabilitada, la barra de idiomas flotante se muestra solo si la función IME local está habilitada. Esta opción está deshabilitada de forma predeterminada.
`Put icon cache in user's Local profile folder` (Parámetro de configuración de equipos)	Especifica si Horizon Client coloca los archivos de la caché de su icono en la carpeta `Local` del usuario en vez de colocarlos en la carpeta `Itinerancia` utilizada anteriormente. Cuando esta opción está habilitada, Horizon Client coloca los archivos de la caché de su icono en la carpeta `Local` del usuario. La primera vez que inicie Horizon Client, los archivos que haya en la caché se moverán de la carpeta `Itinerancia` a la carpeta `Local` y los nuevos archivos de la caché se colocarán en la carpeta `Local`. Al habilitar esta directiva, se puede ayudar a mejorar el tiempo de respuesta de las aplicaciones remotas cuando se utilizan perfiles de itinerancia si se evita sincronizar los archivos de la caché. Si esta opción no se configura, el valor predeterminado es Deshabilitado. Esta opción no está configurada de forma predeterminada.
`Allow opening local files in hosted applications` (Parámetro de configuración de usuario)	Especifica si Horizon Client registra controladores locales para las extensiones de archivo compatibles con las aplicaciones alojadas. Si esta opción está deshabilitada, Horizon Client no registra ningún controlador para las extensiones de archivo y no permite al usuario invalidar la opción. Si esta opción está habilitada, Horizon Client registra siempre controladores para las extensiones de archivo. De forma predeterminada, los controladores para las extensiones de archivo están registrados, pero los usuarios pueden deshabilitar esta función en la interfaz de usuario de Horizon Client si utilizan **Activar la capacidad para abrir un archivo local con una aplicación remota desde la configuración del sistema de archivos locales** en el panel Compartir del cuadro de diálogo Configuración. Si desea obtener más información, consulte "Compartir el acceso a unidades y carpetas locales," página 78. Si esta opción no se configura, el valor predeterminado es Habilitado. Esta opción no está configurada de forma predeterminada.

Configuración USB para los GPO cliente

Puede definir la configuración de la directiva USB para el agente y para Horizon Client en Windows. Mientras está conectado, Horizon Client descarga la configuración de directivas USB desde el agente y la usa junto con la propia configuración de directivas USB de Horizon Client para determinar qué dispositivos permitirá que estén disponibles para su redireccionamiento desde el equipo host.

La siguiente tabla describe cada opción de configuración de directivas para dividir USB compuestos en los archivos de plantillas ADM y ADMX Configuración de Horizon Client. La configuración se aplica a nivel de equipo. De forma preferencial, Horizon Client lee la configuración desde el GPO a nivel de equipo y si no es así, desde el registro que se encuentra en `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Para obtener una descripción de cómo Horizon aplica las directivas para la división de dispositivos USB compuestos, consulte los temas relacionados con el uso de directivas para controlar el redireccionamiento USB en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Tabla 3-8. Plantilla de configuración de Horizon Client : configuración de división USB

Ajuste	Propiedades
`Allow Auto Device Splitting`	Permite la división automática de dispositivos USB compuestos. El valor predeterminado no está definido, lo que equivale a **`false`**.
`Exclude Vid/Pid Device From Split`	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-`*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-55**`** El valor predeterminado no está definido.
`Split Vid/Pid Device`	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:** Horizon no incluye automáticamente los componentes que no ha excluido explícitamente. Debe especificar una directiva de filtrado como `Include Vid/Pid Device` para incluir estos componentes. El valor predeterminado no está definido.

La siguiente tabla describe cada opción de directiva para filtrar los dispositivos USB en los archivos de plantillas ADM y ADMX Configuración de Horizon Client. La configuración se aplica a nivel de equipo. De forma preferencial, Horizon Client lee la configuración desde el GPO a nivel de equipo y si no es así, desde el registro que se encuentra en `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Para obtener una descripción de cómo Horizon aplica las directivas para filtrar dispositivos USB, consulte los temas sobre configuración de directivas de filtrado para redireccionamiento USB en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Tabla 3-9. Plantilla de configuración de Horizon Client : configuración del filtrado de dispositivos USB

Ajuste	Propiedades
`Allow Audio Input Devices`	Permite que se redireccionen los dispositivos de entrada de audio. El valor predeterminado no está definido, lo que equivale a **`true`**.
`Allow Audio Output Devices`	Permite que se redireccionen los dispositivos de salida de audio. El valor predeterminado no está definido, lo que equivale a **`false`**.

Tabla 3-9. Plantilla de configuración de Horizon Client : configuración del filtrado de dispositivos USB (Continua)

Ajuste	Propiedades
`Allow HIDBootable`	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`**.
`Allow Device Descriptor Failsafe Behavior`	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`**.
`Allow Other Input Devices`	Permite el redireccionamiento de dispositivos de entrada que no sean dispositivos con arranque HID o teclados con dispositivos señaladores integrados. El valor predeterminado no está definido, lo que equivale a **`true`**.
`Allow Keyboard and Mouse Devices`	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`**.
`Allow Smart Cards`	Permite que se redireccionen los dispositivos de tarjeta inteligente. El valor predeterminado no está definido, lo que equivale a **`false`**.
`Allow Video Devices`	Permite que se redireccionen los dispositivos de vídeo. El valor predeterminado no está definido, lo que equivale a **`true`**.
`Disable Remote Configuration`	Deshabilita el uso de la configuración del agente al realizar el filtrado de dispositivos USB. El valor predeterminado no está definido, lo que equivale a **`false`**.
`Exclude All Devices`	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 el agente y esta configuración se envía a Horizon Client, la configuración del agente sustituirá la de Horizon Client. El valor predeterminado no está definido, lo que equivale a **`false`**.
`Exclude Device Family`	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, Horizon 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, Horizon examinará la familia del dispositivo de todo el dispositivo USB compuesto. El valor predeterminado no está definido.
`Exclude Vid/Pid Device`	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.
`Exclude Path`	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.

Tabla 3-9. Plantilla de configuración de Horizon Client : configuración del filtrado de dispositivos USB (Continua)

Ajuste	Propiedades
`Include Device Family`	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.
`Include Path`	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.
`Include Vid/Pid Device`	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.

Opciones de las plantillas ADM de las variables de las sesiones del cliente PCoIP

Los archivos de plantillas ADM y ADMX de las variables de las sesiones del cliente PCoIP (`pcoip.client.adm` y `pcoip.cient.admx`) incluyen opciones de directivas relacionadas con el protocolo de visualización de PCoIP. Puede establecer las opciones en los valores predeterminados que puede anular un administrador o en los valores que no se pueden anular.

Los archivos ADM y ADMX están disponibles en un archivo de paquete `.zip` con el nombre `VMware-Horizon-Extras-Bundle-`*x.x.x-yyyyyyy*`.zip`, que puede descargar desde el sitio de descargas de VMware en https://my.vmware.com/web/vmware/downloads. En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el archivo de paquete `.zip`.

Tabla 3-10. Variables de las sesiones del cliente PCoIP

Ajuste	Descripción
`Configure PCoIP client image cache size policy`	Controla el tamaño de la caché de imágenes del cliente PCoIP. El cliente utiliza la caché de imágenes para almacenar partes de la pantalla transmitidas anteriormente. La caché de imágenes reduce la cantidad de datos que se retransmiten. Cuando esta opción no está configurada o está deshabilitada, PCoIP utiliza un tamaño predeterminado de 250 MB para la caché de imágenes del cliente. Al habilitar esta opción, podrá configurar un tamaño para la caché de imágenes del cliente de entre 50 y 300 MB. El valor predeterminado es 250 MB.
`Configure PCoIP event log verbosity`	Establece el nivel de detalle del registro de eventos PCoIP. Los valores oscilan entre 0 (el menor nivel de detalle) y 3 (el mayor nivel de detalle). Cuando esta opción está habilitada, puede establecer el nivel de detalle de 0 a 3. Cuando la opción no está configurada o está deshabilitada, el nivel de detalle predeterminado del registro de eventos es 2. Cuando esta opción se modifica durante una sesión PCoIP activa, la nueva opción se aplica de forma inmediata.

Tabla 3-10. Variables de las sesiones del cliente PCoIP (Continua)

Ajuste	Descripción
`Configure PCoIP session encryption algorithms`	Controla los algoritmos de cifrado que muestra el endpoint PCoIP durante la negociación de la sesión. Al marcar una de las casillas, se deshabilita el algoritmo de cifrado asociado. Debe habilitar al menos un algoritmo. Esta opción se aplica tanto al agente como al cliente. Los endpoints negocian el algoritmo de cifrado de la sesión actual que se utiliza. Si se habilita el modo aprobado FIPS140-2, el valor **Deshabilitar cifrado AES-128-GCM** se anulará si el cifrado AES-128-GCM y AES-256-GCM se deshabilitan. Si la opción `Configure SSL Connections` está deshabilitada o no está configurada, los algoritmos Salsa20-256round12 y AES-128-GCM estarán disponibles para la negociación en este endpoint. Los algoritmos de cifrado compatibles (por orden de preferencia) son SALSA20/12-256, AES-GCM-128 y AES-GCM-256. De forma predeterminada, todos los algoritmos de cifrado compatibles están disponibles para la negociación en este endpoint.
`Configure PCoIP virtual channels`	Especifica los canales virtuales que pueden o no pueden utilizarse en sesiones PCoIP. Esta opción también determina si se debe deshabilitar el procesamiento del portapapeles en el host PCoIP. Los canales virtuales que se utilizan en sesiones PCoIP deben aparecer en la lista de autorización de canales virtuales. Los canales virtuales que aparezcan en la lista de canales virtuales no autorizados no se podrán utilizar en sesiones PCoIP. Puede especificar un máximo de 15 canales virtuales para utilizarlos en sesiones PCoIP. Separe los nombres de varios canales con el carácter de barra vertical (|). Por ejemplo, la cadena de autorización de canales virtuales para permitir los canales virtuales mksvchan y vdp_rdpvcbridge es **`mksvchan|vdp_rdpvcbridge`**. Si el nombre de un canal contiene el carácter de barra vertical o de barra diagonal invertida (\\), introduzca este último carácter antes del nombre. Por ejemplo, escriba el nombre del canal awk|ward\channel como **`awk\\|ward\\channel`**. Cuando la lista de canales virtuales autorizados está vacía, ningún canal virtual está permitido. Cuando la lista de canales virtuales no autorizados está vacía, todos los canales virtuales están permitidos. La opción de canales virtuales se aplica tanto al agente como al cliente. Los canales virtuales se deben habilitar tanto en el agente como en el cliente para poder utilizarlos. Esta opción proporciona una casilla independiente que le permite deshabilitar el procesamiento del portapapeles remoto en el host PCoIP. Este valor solo se aplica al agente. De forma predeterminada, todos los canales virtuales están habilitados (incluido el procesamiento del portapapeles).
`Configure the Client PCoIP UDP port`	Especifica el puerto del cliente UDP que utilizan los clientes PCoIP del software. El valor del puerto UDP especifica el puerto UDP base que se va a utilizar. El valor del rango de puertos UDP determina la cantidad de puertos adicionales que se van a probar si el puerto base no está disponible. El intervalo abarca desde el puerto base hasta la suma del puerto base y del rango de puertos. Por ejemplo, si el puerto base es 50002 y el rango de puertos es 64, el intervalo abarcará desde 50002 a 50066. Esta opción solo se aplica al cliente. De forma predeterminada, el puerto base es 50002 y el rango de puertos es 64.

Tabla 3-10. Variables de las sesiones del cliente PCoIP (Continua)

Ajuste	Descripción
`Configure the maximum PCoIP session bandwidth`	Especifica el ancho de banda máximo (en kilobits por segundo) en una sesión PCoIP. El ancho de banda incluye todo el tráfico PCoIP de control, imágenes, audio, canales virtuales y dispositivos USB. Establezca este valor en la capacidad general del vínculo al que esté conectado su endpoint teniendo en cuenta el número de sesiones PCoIP simultáneas esperado. Por ejemplo, en el caso de una configuración de VDI de usuario único (una sesión PCoIP única) que se conecta a través de una conexión a Internet de 4 Mbits/s, establezca este valor en 4 Mbits o en un 10% menos de este valor para permitir otro tráfico de red. Cuando espera que varias sesiones PCoIP simultáneas compartan un vínculo (que contiene varios usuarios de VDI o una configuración de RDS), le recomendamos que ajuste la opción según sea necesario. Sin embargo, si disminuye este valor, se restringirá el ancho de banda máximo de cada sesión activa. Al configurar este valor, se evita que el agente intente realizar transmisiones a una velocidad mayor que la capacidad del vínculo, lo que provocaría una pérdida de paquetes excesiva y una experiencia de usuario deficiente. Este valor es simétrico. Fuerza al cliente y al agente a utilizar el valor más bajo de los dos que están establecidos en el lado del agente y del cliente. Por ejemplo, al establecer un ancho de banda máximo de 4 Mbit/s, se fuerza al agente a realizar transmisiones a una velocidad menor, incluso si la opción está configurada en el cliente. Cuando esta opción está deshabilitada o no está configurada en un endpoint, este no establece ningún límite de ancho de banda. Cuando esta opción está configurada, se utiliza como el límite del ancho de banda máximo del endpoint (en kilobits por segundo). Cuando esta opción no está configurada, el valor predeterminado es 900.000 kilobits por segundo. Esta opción se aplica al agente y al cliente. Si los dos endpoints tienen opciones diferentes, se utiliza el valor menor.
`Configure the PCoIP transport header`	Configura el encabezado de transporte PCoIP y establece la prioridad de la sesión de transporte. El encabezado de transporte PCoIP es un encabezado de 32 bits que se agrega a todos los paquetes UDP PCoIP (solo si el encabezado de transporte está habilitado y es compatible con los dos lados). El encabezado de transporte PCoIP permite a los dispositivos de red mejorar la definición de prioridades o tomar mejores decisiones de calidad de servicio cuando se produce una congestión de redes. El encabezado de transporte está habilitado de forma predeterminada. La prioridad de la sesión de transporte determina la prioridad de la sesión PCoIP que se incluye en el encabezado de transporte PCoIP. Los dispositivos de red realizan una mejor definición de prioridades o toman mejores decisiones de calidad de servicio en función de la prioridad de la sesión de transporte especificada. Cuando la opción `Configure the PCoIP transport header` está habilitada, las siguientes prioridades de sesión de transporte están disponibles: ■ **Alta** ■ **Media** (valor predeterminado) ■ **Baja** ■ **No definida** El cliente y el agente PCoIP negocian el valor de la prioridad de la sesión de transporte. Si el agente PCoIP especifica un valor de prioridad de la sesión de transporte, la sesión utilizará la prioridad de la sesión especificada por el agente. Si solo el cliente especificó una prioridad de la sesión de transporte, la sesión utilizará la prioridad de la sesión especificada por el cliente. Si ninguno de los dos especificó una prioridad de la sesión de transporte o se especificó **Prioridad no definida**, la sesión utilizará el valor predeterminado (prioridad **Media**).
`Enable/disable audio in the PCoIP session`	Determina si el audio está habilitado en las sesiones PCoIP. Ambos endpoints deben tener el audio habilitado. Cuando esta opción está habilitada, el audio PCoIP está permitido. Cuando está deshabilitada, el audio PCoIP se deshabilita. Cuando esta opción no está configurada, el audio está habilitado de forma predeterminada.

Tabla 3-10. Variables de las sesiones del cliente PCoIP (Continua)

Ajuste	Descripción
`Configure the PCoIP session bandwidth floor`	Especifica un límite inferior (en kilobits por segundo) para el ancho de banda que reserva la sesión PCoIP. Esta opción configura el intervalo mínimo esperado de transmisión del ancho de banda del endpoint. Cuando utiliza esta opción para reservar el ancho de banda para un endpoint, el usuario no tiene que esperar a que el ancho de banda esté disponible, lo que mejora la capacidad de respuesta de la sesión. Asegúrese de que no satura el ancho de banda total reservado para todos los endpoints. Compruebe que la suma de los valores mínimos del ancho de banda de todas las conexiones de su configuración no supere la capacidad de la red. El valor predeterminado es 0, lo que significa que no se reserva ningún ancho de banda mínimo. Cuando esta opción está deshabilitada o no está configurada, no se reserva ningún ancho de banda mínimo. Esta opción se aplica al agente y al cliente, pero esta solo afecta al endpoint en el que está configurada. Cuando esta opción se modifica durante una sesión PCoIP activa, el cambio se aplica de forma inmediata.
`Configure the PCoIP session MTU`	Especifica el tamaño de la unidad de transmisión máxima (MTU) de los paquetes UDP para una sesión PCoIP. El tamaño de MTU incluye los encabezados de los paquetes UDP e IP. TCP utiliza el mecanismo de detección de MTU estándar para establecer MTU. Además, esta opción no afecta a TCP. El tamaño de MTU máximo es 1.500 bytes. El tamaño de MTU mínimo es 500 bytes. El valor predeterminado es 1.300 bytes. Normalmente, no tendrá que cambiar el tamaño de MTU. Cambie este valor si tiene una configuración de red inusual que provoca la fragmentación de paquetes PCoIP. Esta opción se aplica al agente y al cliente. Si los dos endpoints tienen opciones de tamaño de MTU diferentes, se utilizará el menor tamaño. Si esta opción está deshabilitada o no está configurada, el cliente utilizará el valor predeterminado en la negociación con el agente.

Ejecutar Horizon Client desde la línea de comandos

Es posible ejecutar Horizon Client para Windows desde la línea de comandos o desde los scripts. Puede que quiera hacerlo si está implementando una aplicación basada en pantalla completa que proporciona a los usuarios finales accesos a aplicaciones de escritorio.

Puede usar el comando `vmware-view.exe` para ejecutar Horizon Client para Windows desde la línea de comandos. El comando incluye opciones que puede especificar para modificar el comportamiento de Horizon Client.

Uso de los comandos de Horizon Client

La sintaxis de los comandos de `vmware-view` controla la operación de Horizon Client.

Use el siguiente formato del comando de `vmware-view` en una ventana de símbolo de sistema de Windows.

`vmware-view [`*`opción_línea_comandos`* `[`*`argumento`*`]] ...`

La ruta predeterminada del archivo ejecutable del comando `vmware-view` depende del sistema.

- En sistemas de 32 bits, la ruta es `C:\Program Files\VMware\VMware Horizon View Client\`.
- En sistemas de 64 bits, la ruta es `C:\Program Files (x86)\VMware\VMware Horizon View Client\`.

Para su comodidad, agregue esta ruta en la variable del entorno *RUTA*.

La siguiente tabla muestra las opciones de la línea de comandos que puede usar con el comando `vmware-view`.

Tabla 3-11. Opciones de la línea de comandos de Horizon Client

Opción	Descripción
`/?`	Muestra la lista de las opciones de la línea de comandos.
`–appName` *nombre_aplicación*	Especifica el nombre de la aplicación que aparece en la ventana de selección de aplicaciones y escritorios. Este es el nombre para mostrar que se especificó para el grupo de aplicaciones en el asistente de creación del grupo.
`–appSessionReconnectionBehavior` *argumento*	Especifica la opción del comportamiento de reconexión de las aplicaciones. ■ `always` implementa **Volver a conectarse automáticamente a las aplicaciones abiertas**. ■ `never` implementa **No solicitar volver a conectarse y no conectarse automáticamente**. ■ `ask` implementa **Solicitar volver a conectarse a las aplicaciones abiertas**. Cuando utiliza esta opción, las opciones de reconexión de las aplicaciones se deshabilitan en la página Configuración de Horizon Client.
`–args` *argumento*	Especifica los argumentos de la línea de comandos que se agregarán al iniciar una aplicación remota. Por ejemplo: `vmware–view.exe ––serverURL 10.10.10.10 ––appName "My Notepad++" ––args "\"my new.txt\""`
`–connectUSBOnStartup`	Cuando aparezca configurado como `true`, se redireccionarán todos los dispositivos USB al escritorio que están conectados actualmente al host. Esta opción está configurada implícitamente si especifica la opción `–unattended`. El valor predeterminado es `false`.
`–connectUSBOnInsert`	Cuando aparezca configurado como `true`, se conectará un dispositivo USB al escritorio en primer plano cuando conecte el dispositivo. Esta opción está configurada implícitamente si especifica la opción `–unattended`. El valor predeterminado es `false`.
`–desktopLayout` *tamaño_ventana*	Especifica cómo se muestra la ventana del escritorio: **`fullscreen`** Se muestra en pantalla completa. **`multimonitor`** Se muestra en varios monitores. **`windowLarge`** Ventana grande. **`windowSmall`** Ventana pequeña. **`length X width`** Tamaño personalizado. Por ejemplo: 800x600
`–desktopName` *nombre_escritorio*	Especifica el nombre del escritorio que aparece en la ventana de selección de aplicaciones y escritorios. Este es el nombre para mostrar que se especificó para el grupo de escritorios en el asistente de creación del grupo. **IMPORTANTE:** No especifique esta opción para clientes en modo de pantalla completa. Esta opción no surte efecto cuando el escritorio se ejecuta en pantalla completa. Para el modo de pantalla completa, la conexión se establece con el primer escritorio que aparece en la lista de escritorios autorizados.
`–desktopProtocol` *protocolo*	Especifica el protocolo de visualización que aparece en la ventana de selección de aplicaciones y escritorios. El protocolo de visualización puede ser Blast, PCoIP o RDP.
`–domainName` *nombre_dominio*	Especifica el dominio NETBIOS que usa el usuario final para iniciar sesión en Horizon Client. Por ejemplo, utilizaría `mycompany` en lugar de `mycompany.com`.
`–file` *ruta_archivo*	Especifica la ruta de un archivo de configuración que contiene argumentos y opciones de comandos adicionales. Consulte "Archivo de configuración de Horizon Client," página 69.
`–h`	Muestra opciones de ayuda.

Tabla 3-11. Opciones de la línea de comandos de Horizon Client (Continua)

Opción	Descripción
`–hideClientAfterLaunchSession`	Cuando se establece como `true`, se ocultan la ventana de selección de aplicaciones y escritorios remotos y el menú **Mostrar VMware Horizon Client** después de iniciar una sesión remota. Cuando se establece como `false`, se muestran la ventana de selección de aplicaciones y escritorios remotos y el menú **Mostrar VMware Horizon Client** después de iniciar una sesión remota. El valor predeterminado es `true`.
`–languageId` *ID_local*	Proporciona soporte de localización en Horizon Client para diferentes idiomas. Si una biblioteca de recursos está disponible, especifique el ID local (LCID) que se usará. Para inglés de los EE.UU., introduzca el valor 0x409.

`–listMonitors`	Incluye información del diseño de pantalla y los valores de índice de los monitores conectados. Por ejemplo:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (–900, –410, 0, 1190)`
	Puede utilizar los valores de índice en la opción `–monitors`.

`–logInAsCurrentUser`	Cuando está establecido como `true`, se usa la información de credenciales que el usuario final proporciona cuando inicia sesión en el sistema cliente para, a su vez, iniciar sesión en la instancia del servidor de conexión y, por último, en el escritorio remoto. El valor predeterminado es `false`.
`–monitors "`*n*`[,`*n*`,`*n*`,`*n*`]"`	Especifica los monitores que se van a utilizar en una configuración de varios monitores, en la que *n* es el valor de índice de un monitor. Puede utilizar la opción `–listMonitors` para determinar los valores de índice de los monitores conectados. Puede especificar hasta cuatro valores de índice separados por comas. Por ejemplo: **`–monitors "1,2"`** Esta opción no tiene ningún efecto, excepto si `–desktopLayout` se establece en `multimonitor`.
`–nonInteractive`	Suprime los cuadros de mensajes de error cuando se inicia Horizon Client desde un script. Esta opción está configurada implícitamente si especifica la opción `–unattended`.
`–noVMwareAddins`	Evita la carga de canales virtuales específicos de VMware como las impresiones virtuales.
`–password`*contraseña*	Especifica la contraseña que el usuario final utiliza para iniciar sesión en Horizon Client. La consola de comando o cualquier herramienta de scripting procesan la contraseña en texto sin formato. No es necesario que especifique esta opción para clientes en modo de pantalla completa si generó la contraseña automáticamente. Para mejorar la seguridad, se recomienda que no especifique esta opción. Los usuarios pueden introducir la contraseña de forma interactiva.
`–printEnvironmentInfo`	Muestra las direcciones IP, MAC y el nombre del equipo del dispositivo cliente.
`–serverURL` *servidor_conexión*	Especifica la URL, la dirección IP o el FQDN de la instancia del servidor de conexión.
`–shutdown`	Cierra todos los escritorios y las aplicaciones, así como los componentes relevantes de la interfaz de usuario.
`–singleAutoConnect`	Especifica que si el usuario tiene autorización solo para una aplicación o un escritorio remotos, una vez que se autentique en el servidor, el escritorio o la aplicación se conecten automáticamente y el usuario inicie sesión. Esta opción evita que el usuario tenga que seleccionar la aplicación o el escritorio en una lista que solo contiene un elemento.
`–smartCardPIN` *PIN*	Especifica el PIN cuando un usuario final introduce una tarjeta inteligente para iniciar sesión.
`–usernameHint` *nombre_usuario*	Especifica el nombre de la cuenta que se usará como sugerencia de nombre de usuario.

Tabla 3-11. Opciones de la línea de comandos de Horizon Client (Continua)

Opción	Descripción
`–standalone`	Se admite para proporcionar compatibilidad con versiones anteriores. Este es el comportamiento predeterminado para este cliente. No es necesario especificar `–standalone`. Inicia una segunda instancia de Horizon Client que se puede conectar a la misma instancia del servidor de conexión o a una diferente. Se admite el uso del túnel de seguridad para varias conexiones de escritorios al mismo servidor o a un servidor distinto. **NOTA:** La conexión de escritorio secundaria puede no tener acceso al hardware local como dispositivos USB, tarjetas inteligentes, impresoras y varios monitores.
`–supportText` *nombre_archivo*	Especifica la ruta completa de un archivo de texto. El contenido del archivo se muestra en el cuadro de diálogo Información de soporte técnico.
`–unattended`	Ejecuta Horizon Client en modo no interactivo, adecuado para clientes en modo de pantalla completa. También debe especificar: ■ El nombre de la cuenta del cliente, si no generó el nombre de la cuenta desde la dirección MAC del dispositivo cliente. El nombre debe comenzar por la cadena "custom-" o un prefijo alternativo que configurara en ADAM. ■ La contraseña del cliente, si no generó ninguna contraseña automáticamente cuando configuró la cuenta de dicho cliente. La opción `–unattended` establece implícitamente las opciones `–nonInteractive`, `–connectUSBOnStartup`, `–connectUSBOnInsert` y `–desktopLayout multimonitor`.
`–unauthenticatedAccessAccount`	Especifica una cuenta de usuario de acceso sin autenticar que se utilizará para iniciar sesión de forma anónima en el servidor cuando se habilite la función Acceso sin autenticar. Si la función Acceso sin autenticar no está habilitada, esta opción se ignora. Por ejemplo: `vmware–view.exe –serverURL ag–broker.agwork.com –unauthenticatedAccessEnabled true –unauthenticatedAccessAccount anonymous1`
`–unauthenticatedAccessEnabled`	Especifica un comportamiento de acceso sin autenticar: ■ `true` Habilita la función Acceso sin autenticar. El posible que el cliente tenga que recurrir de nuevo a otro método de autenticación si la función Acceso sin autenticar no está disponible. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está visible, deshabilitada y seleccionada en Horizon Client. ■ `false` requiere que introduzca sus credenciales para iniciar sesión y acceder a sus aplicaciones. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está oculta y desmarcada en Horizon Client. Si no especifica esta opción, puede habilitar Acceso sin autenticar en Horizon Client. La opción **Iniciar sesión de forma anónima con Acceso sin autenticar** está visible, habilitada y desmarcada.

Tabla 3-11. Opciones de la línea de comandos de Horizon Client (Continua)

Opción	Descripción

`–useExisting`	Le permite iniciar varias aplicaciones y escritorios remotos desde una sesión de Horizon Client única.
	Cuando especifica esta opción, Horizon Client determina si ya existe una sesión con el mismo nombre de usuario, dominio y URL del servidor y, si es así, vuelve a utilizar dicha sesión en lugar de crear una nueva.
	Por ejemplo, en el siguiente comando, el usuario 1 inicia la aplicación Calculadora y se crea una nueva sesión.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Calculator –serverURL view.mycompany.com –useExisting`
	En el siguiente comando, el usuario 1 inicia la aplicación Paint con el mismo nombre de usuario, dominio y URL del servidor, por lo que se utiliza la misma sesión.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Paint –serverURL view.mycompany.com –useExisting`

`–userName` *nombre_usuario*	Especifica el nombre de la cuenta que usa el usuario final para iniciar sesión en Horizon Client. No es necesario que especifique esta opción para clientes que estén en modo de pantalla completa si genera el nombre de la cuenta desde la dirección MAC del dispositivo cliente.

Puede especificar todas las opciones con las directivas de grupo de Active Directory excepto para `–file`, `–languageId`, `–printEnvironmentInfo`, `–smartCardPIN` y `–unattended`.

NOTA: La configuración de la directiva de grupo tiene prioridad ante la configuración que especificó en la línea de comandos.

Archivo de configuración de Horizon Client

Es posible leer las opciones de la línea de comandos de Horizon Client desde un archivo de configuración.

Puede especificar la ruta del archivo de configuración como un argumento de la opción `–file` *file_path* del comando `vmware–view`. El archivo debe ser de texto ASCII o Unicode (UTF-16).

Ejemplo: Ejemplo de un archivo de configuración para una aplicación no interactiva

El siguiente ejemplo muestra los contenidos de un archivo de configuración para una aplicación no interactiva.

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

Ejemplo: Ejemplo de un archivo de configuración para un cliente en modo de pantalla completa

El siguiente ejemplo muestra un cliente en modo de pantalla completa cuyo nombre de cuenta se basa en su dirección MAC. El cliente cuenta con una contraseña generada automáticamente.

```
–serverURL 145.124.24.100
–unattended
```

Utilizar el Registro de Windows para configurar Horizon Client

Puede definir la configuración predeterminada de Horizon Client en el Registro de Windows en lugar de especificarla en la línea de comandos. La configuración de las directivas de grupo tiene preferencia sobre la configuración del Registro de Windows y esta última tiene preferencia sobre la línea de comandos.

NOTA: Es posible que la configuración del Registro de Windows que se indica en esta sección no sea compatible en una próxima versión. Se deberá utilizar la configuración del GPO.

En Tabla 3-12, se muestra la configuración del Registro para iniciar sesión en Horizon Client. Esta configuración se encuentra en la ubicación `HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\` del registro. Esta ubicación es específica para un usuario particular, mientras que la configuración `HKEY_LOCAL_MACHINE` (que se describe en la siguiente tabla) es para todo el equipo y se aplica a todos los usuarios locales y de dominio de un entorno de dominio de Windows que tienen permiso para iniciar sesión en el equipo.

Tabla 3-12. Configuración del Registro de credenciales de Horizon Client

Configuración del Registro	Descripción
`Password`	Especifica la contraseña predeterminada.
`UserName`	Especifica el nombre de usuario predeterminado.

En Tabla 3-13, se muestra la configuración del Registro de Horizon Client que no incluye credenciales de inicio de sesión. La ubicación de esta configuración depende del tipo de sistema:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- Para Windows de 64 bits: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Tabla 3-13. Configuración del Registro de Horizon Client

Configuración del Registro	Descripción
`DomainName`	Especifica el nombre de dominio NETBIOS predeterminado. Por ejemplo, utilizaría `mycompany` en lugar de `mycompany.com`.
`EnableShade`	Especifica si la barra de menús (sombra) de la parte superior de la ventana de Horizon Client está habilitada. La barra de menús está habilitada de forma predeterminada excepto para los clientes en el modo de pantalla completa. Un valor de **`false`** deshabilita la barra de menú. **NOTA:** Esta configuración solo se puede aplicar cuando establece la opción **Todos los monitores** o **Pantalla completa** para el diseño de presentación.
`ServerURL`	Especifica la instancia del servidor de conexión predeterminada por su URL, dirección IP o FQDN.
`EnableSoftKeypad`	Si se establece en **`true`** y una ventana de Horizon Client tiene el foco, los eventos del panel de escritura a mano, del mouse, del teclado en pantalla y del teclado físico se enviarán a la aplicación o el escritorio remotos, aunque el mouse o el teclado en pantalla estén fuera de la ventana de Horizon Client. El valor predeterminado es **`false`**.

En la siguiente tabla se muestra la configuración de seguridad que puede agregar. La ubicación de esta configuración depende del tipo de sistema:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Para Windows de 64 bits: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Tabla 3-14. Configuración de seguridad

Configuración del Registro	Descripción y valores válidos
`CertCheckMode`	Especifica el modo de comprobación del certificado. ■ **`0`** implements `Do not verify server identity certificates`. ■ **`1`** implements `Warn before connecting to untrusted servers`. ■ **`2`** implements `Never connect to untrusted servers`.
`SSLCipherList`	Configura la lista de cifrado para restringir el uso de ciertos protocolos y algoritmos criptográficos antes de establecer una conexión SSL cifrada. La lista de cifrado consta de una o más cadenas de cifrado separadas por dos puntos. **NOTA:** Todas las cadenas de cifrado distinguen mayúsculas y minúsculas. El valor predeterminado es **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH +AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Esto significa que TLSv.1, TLSv1.1 y TLSv1.2 están habilitados (Se han eliminado SSL v2.0 y v3.0). 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. Vínculo de referencia para la configuración: http://www.openssl.org/docs/apps/ciphers.html

Administrar las conexiones de las aplicaciones y los escritorios remotos

4

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. Es posible que tenga que especificar un servidor y proporcionar las credenciales de su cuenta de usuario.

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

La función **Iniciar sesión como usuario actual** está disponible aunque Horizon Client no esté instalado en un escritorio remoto.

Prerequisitos

- Obtenga las credenciales para iniciar 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," página 20.
- Si se encuentra fuera de la red corporativa y no utiliza un servidor de seguridad para acceder al escritorio remoto, compruebe que el dispositivo cliente está configurado para usar una conexión VPN y actívela.

  IMPORTANTE: VMware le recomienda usar 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 (_). También es necesario incluir el número de puerto si el puerto no es el 443.
- 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.
- Si lo ha permitido su administrador, configure el modo de comprobación del certificado SSL que presente el servidor de conexión. Para decidir el modo que debe usar, consulte "Configurar el modo de comprobación del certificado en Horizon Client," página 45.

Procedimiento

1. Haga doble clic en el acceso directo de escritorio de **VMware Horizon Client** o haga clic en **Inicio > Programas > VMware Horizon Client**.
2. (Opcional) Para configurar el modo de comprobación del certificado, haga clic en el botón **Opciones** situado en la barra de menú y seleccione **Configurar SSL**.

   Solo podrá configurar esta opción si lo permite el administrador.
3. (Opcional) Para iniciar sesión como el usuario de dominio de Windows que inició la sesión actual, haga clic en el botón **Opciones**, situado en la barra de menú y seleccione, **Iniciar sesión como usuario actual**.

   Esta opción está disponible si el módulo **Iniciar sesión como usuario actual** está instalado en el sistema cliente y si el administrador habilitó la configuración global para esta función. Algunas compañías prefieren no habilitar esta función.
4. 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 pantalla de inicio de Horizon Client. La próxima vez que abra 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.
5. 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 **Continuar**.

6 Introduzca las credenciales de un usuario que tenga autorización para usar al menos un grupo de aplicaciones o escritorios, seleccione el dominio y haga clic en **Inicio de sesión**.

Si escribe un nombre de usuario con el formato **`nombre de usuario@dominio`**, se tratará como un nombre principal de usuario (UPN) debido al signo @, y el menú desplegable **Dominio** se deshabilitará.

Si está oculto el menú desplegable **Dominio**, debe escribir el nombre de usuario de una de las siguientes maneras: ***`nombre_de_usuario@dominio`*** o ***`dominio\nombre_de_usuario`***.

7 (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 rueda dentada) junto al nombre del servidor situado en la parte superior de la pantalla.

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.

8 (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.

9 Para conectarse a una aplicación o un escritorio remotos, puede hacer doble clic en el icono o hacer clic con el botón secundario en el icono y seleccionar **Iniciar** en el menú contextual.

Si va a conectarse a un escritorio remoto publicado, alojado en un host de Microsoft RDS, y dicho 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.

Después de conectarse, aparecerá la ventana de la aplicación o del escritorio remotos. Si tiene autorización para más de un escritorio o aplicación, la ventana de selección de la aplicación y del escritorio también se quedará abierta, así que podrá conectarse a varios elementos al mismo tiempo.

Use este cuadro de diálogo para permitir o denegar el acceso a los archivos de su sistema local. Si desea obtener más información, consulte "Compartir el acceso a unidades y carpetas locales," página 78.

Si se produce un error en el proceso de autenticación del servidor o 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 para que no use SSL. El software cliente necesita conexiones SSL. Compruebe que el ajuste global en Horizon Administrator para la casilla **Usar SSL para conexiones de cliente** no esté 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 conexiones.
- Verifique que el certificado de seguridad del servidor de conexión funcione correctamente. En caso contrario, en Horizon Administrator, puede que también detecte que no es posible obtener acceso al agente 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 permiten el establecimiento de conexiones desde este usuario. Consulte el documento *Administración de View*.

- Verifique que el usuario esté autorizado a obtener acceso a esta aplicación o a este escritorio. Consulte el documento *Configurar escritorios virtuales en Horizon 7* o *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.

Qué hacer a continuación

Configure las opciones de inicio. Si no desea solicitar a los usuarios finales que proporcionen el nombre del host de la instancia del servidor de conexión o desea configurar otras opciones de inicio, utilice una opción de línea de comandos para crear un acceso directo de escritorio. Consulte "Ejecutar Horizon Client desde la línea de comandos," página 65.

Utilizar la función Acceso sin autenticar para conectarse a aplicaciones remotas

Un administrador de Horizon puede utilizar la función Acceso sin autenticar para crear usuarios de acceso sin autenticar y autorizar a dichos usuarios a utilizar las aplicaciones remotas en una instancia del servidor de conexión. Los usuarios de acceso sin autenticar pueden iniciar sesión en el servidor de forma anónima para conectarse a sus aplicaciones remotas.

De forma predeterminada, el usuario selecciona la opción **Iniciar sesión de forma anónima con Acceso sin autenticar** en el menú **Opciones** y selecciona una cuenta de usuario para iniciar sesión de forma anónima. El administrador de Horizon puede configurar las opciones de la directiva de grupo para cambiar el comportamiento de la función Acceso sin autenticar para que la opción **Iniciar sesión de forma anónima con Acceso sin autenticar** ya aparezca seleccionada y los usuarios inicien sesión automáticamente con una cuenta de usuario específica de acceso sin autenticar.

Prerequisitos

- Realice las tareas administrativas descritas en "Preparar el servidor de conexión para Horizon Client," página 20.
- Configurar usuarios de acceso sin autenticar en la instancia del servidor de conexión. Si desea obtener más información, consulte el tema sobre cómo proporcionar acceso sin autenticar para aplicaciones publicadas en el documento *Administración de View*.
- (Opcional) Configure las opciones de las directivas de grupo **Cuenta para Acceso sin autenticar** e **Iniciar sesión de forma anónima con Acceso sin autenticar** para cambiar el comportamiento predeterminado de la función Acceso sin autenticar. Para obtener información, consulte "Configuración de la definición de scripting para los GPO cliente," página 48.

Procedimiento

1. Haga doble clic en el acceso directo de escritorio de **VMware Horizon Client** o haga clic en **Inicio > Programas > VMware Horizon Client**.
2. Si el administrador de Horizon se lo indica, haga clic en el botón **Opciones** en la barra de menús y seleccione **Iniciar sesión de forma anónima con Acceso sin autenticar**.

   En función de cómo esté configurado el sistema cliente, es posible que esta opción ya esté seleccionada.
3. (Opcional) Para configurar el modo de comprobación del certificado, haga clic en el botón **Opciones** situado en la barra de menú y seleccione **Configurar SSL**.

   Solo podrá configurar esta opción si lo permite el administrador.

4 Conéctese al servidor al que tiene acceso sin autenticar para las aplicaciones remotas.

Opción	Acción
Conectarse a un servidor nuevo	Haga doble clic en el botón **+ Agregar servidor** o bien haga clic en el botón **+ Nuevo servidor** en la barra de menús, introduzca el nombre del servidor y haga clic en **Conectarse**.
Conectarse a un servidor existente	Haga doble clic en el icono del servidor en la pantalla de inicio de Horizon Client.

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.

5 Cuando el cuadro de diálogo de inicio de sesión aparezca, seleccione una cuenta de usuario en el menú desplegable **Cuenta de usuario** si fuera necesario.

Si solo hay disponible una cuenta de usuario, el menú desplegable se deshabilita y la cuenta de usuario se selecciona automáticamente.

6 (Opcional) Si la casilla de verificación **Usar siempre esta cuenta** está disponible, selecciónela para omitir el cuadro de diálogo de inicio de sesión la próxima vez que se conecte al servidor.

Puede desmarcar esta opción antes de conectarse al servidor la próxima vez si hace clic con el botón secundario en el icono del servidor en la pantalla de inicio de Horizon Client y selecciona **Olvidar la cuenta de Acceso sin autenticar guardada**.

7 Haga clic en **Inicio de sesión** para conectarse al servidor.

Se mostrará la ventana de selección de aplicaciones.

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

Consejos para usar el selector de aplicaciones y escritorios

Para su comodidad, puede reorganizar o reducir el número de iconos en la pantalla de selección de aplicaciones y escritorios de Horizon Client.

Después de autenticarse y conectarse a un servidor determinado, aparecerá una pantalla que incluye los iconos de todas las aplicaciones y escritorios remotos para los que está autorizado. Pruebe las siguientes sugerencias para iniciar rápidamente las aplicaciones y los escritorios remotos que usa con más frecuencia:

- Escriba rápidamente las primeras letras del nombre. Por ejemplo, si tiene iconos para Paint, PowerPoint y Publisher, puede escribir rápidamente ***pa*** para seleccionar la aplicación Paint.

  Si hay coincidencia entre más de un elemento y las letras que escribió, puede pulsar F4 para ir al siguiente elemento que coincida. Cuando llegue al último elemento, puede pulsar F4 para volver al primero.

- Para marcar un icono como favorito, haga clic con el botón secundario en el icono y seleccione **Marcar como favorito** en el menú contextual. Después de seleccionar los favoritos, haga clic en el botón **Mostrar vista de favoritos** (botón de estrella) para eliminar todos los iconos que no son favoritos.

- En la vista Favoritos, seleccione un icono y arrástrelo para cambiar el orden de los iconos. Cuando no se encuentre en la vista Favoritos, de forma predeterminada, los iconos de los escritorios se muestran en primer lugar, en orden alfabético, seguidos por los iconos de aplicaciones, que también aparecen en orden alfabético. Sin embargo, puede arrastrar y soltar iconos para cambiar su posición mientras se encuentra en la vista Favoritos.

El orden de los iconos se guarda en el servidor que está usando, tanto cuando se desconecta del servidor como cuando inicia un escritorio o una aplicación. Si no se desconecta de forma manual del servidor ni inicia un elemento, los cambios no se guardarán.

- Cree un acceso directo para poder acceder a la aplicación o escritorio remotos desde su escritorio local y evitar la ventana de selección por completo. Haga clic con el botón secundario en el icono y seleccione **Crear acceso directo** en el menú contextual.
- Haga clic con el botón secundario en el icono de la aplicación o escritorio remotos y seleccione **Agregar al menú de inicio** en el menú contextual, para poder acceder a la aplicación o al escritorio remotos desde su propio menú Inicio local y evitar la ventana de selección por completo.

NOTA: Si utiliza un sistema cliente Windows 7 o una versión posterior, después de conectarse a un servidor, un escritorio o una aplicación, puede abrir Horizon Client y hacer clic con el botón secundario en el icono de Horizon Client en la barra de tareas de Windows para seleccionar el servidor, el escritorio o la aplicación que se utilizaron recientemente. Aparecen hasta 10 elementos en la lista. Para eliminar un elemento, haga clic con el botón secundario en él y seleccione **Quitar de esta lista**.

Si hace clic con el botón secundario en el icono de Horizon Client en la barra de tareas y no aparece un lista de accesos directos, haga clic con el botón secundario en la barra de tareas, seleccione **Propiedades** y, a continuación, haga clic en la pestaña **Menú de inicio**. En la sección Privacidad, seleccione la casilla **Almacenar y mostrar elementos abiertos recientemente en el menú Inicio y en la barra de tareas** y haga clic en **Aceptar**.

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.

También puede activar la posibilidad de abrir archivos locales directamente desde el sistema de archivos local mediante aplicaciones remotas. Al hacer clic con el botón secundario en un archivo local, el menú **Abrir con** muestra también las aplicaciones remotas disponibles. Asimismo, puede establecer que los archivos se abran automáticamente mediante aplicaciones remotas al hacer doble clic en el archivo. Al habilitar esta función, todos los archivos que se encuentren en su sistema de archivos local con determinadas extensiones de archivo se registran en el servidor en el que ha iniciado sesión. Por ejemplo, si Microsoft Word es una de las aplicaciones remotas disponibles en el servidor, puede hacer clic con el botón secundario en un archivo `.docx` de su sistema local y abrirlo con la aplicación MS Word remota. Esta función requiere agentes y servidores Horizon 6.2.

Un administrador puede ocultar la función de redireccionamiento de la unidad cliente en Horizon Client al habilitar una configuración de directiva de grupo. Para obtener más información, consulte cómo **deshabilitar el uso compartido de carpetas y archivos** en Tabla 3-7.

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 para controlar el comportamiento del redireccionamiento de unidades cliente. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Procedimiento

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

Opción	Descripción
En la ventana para seleccionar la aplicación y el escritorio	Haga clic con el botón secundario en el icono de una aplicación o escritorio, seleccione **Configuración** y, a continuación, **Compartir** en el panel izquierdo de la ventana que se abre.
En el cuadro de diálogo Compartir que se muestra al conectarse a un escritorio o aplicación	En el cuadro de diálogo, haga clic en el vínculo **Configuración > Compartir**.
Desde un SO de escritorio	En la barra de menús, seleccione **Opciones > Compartir carpetas**.

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. Por otro lado, no active la función de redireccionamiento que conecta dispositivos USB automáticamente al inicio o al insertar el dispositivo. Si lo hace, la próxima vez que inicie Horizon Client o inserte el dispositivo USB, el dispositivo se conectará mediante la función de redireccionamiento USB en lugar de hacerlo con la de redireccionamiento de unidades cliente.
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 usuario local	Seleccione la casilla de verificación **Compartir los archivos locales*nombre de usuario***.
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.

Opción	Acción
Activar la posibilidad de abrir un archivo local con una aplicación remota desde el sistema de archivos local	Seleccione la casilla de verificación **Abrir archivos locales en aplicaciones alojadas en el host**. Con esta opción, puede hacer clic con el botón secundario en el sistema de archivos local y seleccionar que se abra el archivo con una aplicación remota. También puede cambiar las propiedades del archivo de modo que todos los archivos con dicha extensión se abran mediante la aplicación remota de forma predeterminada, de la misma forma que ocurre al hacer doble clic en él. Por ejemplo, puede hacer clic con el botón secundario en un archivo, seleccionar **Propiedades** y hacer clic en **Cambiar** para seleccionar que la aplicación remota abra los archivos de ese tipo. Su administrador puede deshabilitar esta función.
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***.

Ocultar la ventana de VMware Horizon Client

Puede ocultar la ventana de VMware Horizon Client después de abrir una aplicación o un escritorio remotos.

Puede establecer una preferencia de modo que siempre se oculte la ventana de VMware Horizon Client después de abrirse una aplicación o un escritorio remotos.

NOTA: Los administradores pueden usar una configuración de directiva de grupo para establecer si la ventana siempre se oculta después de abrir una aplicación o un escritorio remotos.

Si desea obtener más información, consulte "Configuración general para los GPO cliente," página 57.

Procedimiento

- Para ocultar la ventana de VMware Horizon Client después de abrir una aplicación o un escritorio remotos, haga clic en el botón **Cerrar** situado en la esquina de la ventana de VMware Horizon Client.
- Para establecer una preferencia que siempre oculte la ventana de VMware Horizon Client después de que se abra una aplicación o un escritorio remotos, antes de conectarse a un servidor, haga clic en el botón **Opciones** de la barra de menús y seleccione **Ocultar el selector después de iniciar un elemento**.
- Para que se muestre la ventana de VMware Horizon Client después de que se haya ocultado, haga clic con el botón secundario en el icono de VMware Horizon Client en la bandeja del sistema y seleccione **Mostrar VMware Horizon Client**, o bien, si ha iniciado sesión en un escritorio remoto, haga clic en el botón **Opciones** de la barra de menús y seleccione **Cambiar a otro escritorio**.

Volver a conectarse a una aplicación o escritorio

Por razones de seguridad, los administradores establecen un tiempo de espera que cerrará la sesión de un servidor después de un número determinado de horas y que bloqueará una aplicación remota después de un número determinado de minutos de inactividad.

Con la función de aplicaciones remotas de View 6.0, si no usa una aplicación remota durante un tiempo determinado, recibirá una advertencia 30 segundos antes de que la aplicación se bloquee automáticamente. Si no responde, la aplicación se bloquea. De forma predeterminada, ese tiempo expira después de 15 minutos de inactividad, pero el administrador puede cambiarlo.

Por ejemplo, si tiene una o más aplicaciones abiertas y se aleja del equipo, cuando vuelva una hora más tarde, las ventanas de las aplicaciones ya no estarán abiertas. En su lugar, es posible que aparezca un cuadro de diálogo que le solicite que haga clic en el botón **Aceptar** para que las ventanas de aplicaciones vuelvan a aparecer.

El límite de tiempo del servidor se suele establecer en varias horas de inactividad. De forma predeterminada, si tiene abierto Horizon Client y conectado a un servidor concreto durante más de 10 horas, se le solicitará que vuelva a iniciar sesión. Este tiempo de espera se aplica sin tener en cuenta si se encuentra conectado a una aplicación remota o escritorio remotos.

En Horizon Administrator, para configurar esta opción de tiempo de espera, acceda a **Configuración global** y edite las opciones generales.

Crear un acceso directo al escritorio o a la aplicación en el escritorio cliente o el menú Inicio

Es posible crear un acceso directo para una aplicación o un escritorio remotos. El acceso directo aparece en el escritorio cliente, al igual que los accesos directos de las aplicaciones instaladas de forma local. También puede crear un elemento en el menú Inicio que aparezca en la lista Programas.

Procedimiento

1 Inicie Horizon Client y, a continuación, inicie sesión en el servidor.

2 En la ventana de selección de aplicaciones y escritorios, haga clic con el botón secundario en una aplicación o un escritorio y seleccione **Crear acceso directo** o **Agregar al menú Inicio** en el menú contextual que aparece.

Según el comando que seleccionó, se crea un acceso directo en el escritorio cliente o en el menú Inicio de su sistema cliente.

Qué hacer a continuación

Puede cambiarle el nombre, eliminarlo y realizar las mismas acciones en este acceso directo que las que puede realizar en los accesos directos de las aplicaciones instaladas de forma local. Cuando use el acceso directo, si aún no inició sesión en el servidor, se le solicitará que lo haga antes de que se abra la ventana de la aplicación o del escritorio remotos.

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 ya inició sesión en un escritorio remoto, seleccione **Opciones > Cambiar a otro escritorio** en la barra de menú de Horizon Client y seleccione la aplicación o el escritorio que desee iniciar. ■ Si ya inició sesión en una aplicación remota, haga clic con el botón secundario en el icono **VMware Horizon Client** situado en la bandeja del sistema, seleccione **Mostrar VMware Horizon Client** para que aparezca la ventana para seleccionar la aplicación y el escritorio y haga doble clic en el icono de la otra aplicación o escritorio. ■ 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 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**.

NOTA: La combinación de teclas Ctrl+Alt+Supr de Windows no es compatible con los escritorios remotos. Haga clic en el botón **Enviar Ctrl+Alt+Supr** en la barra de menú como equivalente a pulsar Ctrl+Alt+Supr. También puede pulsar Ctrl+Alt+Insert en la mayoría de los casos.

Procedimiento

- Desconectarse desde un escritorio remoto sin cerrar sesión.

Opción	Acción
En la ventana del escritorio remoto	Realice una de las siguientes acciones: ■ Haga clic en el botón **Cerrar** situado en la esquina de la ventana del escritorio. ■ Seleccione **Opciones > Desconectar** en la barra de menú de la ventana del escritorio.
En la ventana para seleccionar la aplicación y el escritorio	La ventana para seleccionar la aplicación y el escritorio está abierta si tiene autorización para utilizar varios escritorios o aplicaciones en el servidor. En la parte superior izquierda de la ventana para seleccionar el escritorio, haga clic en el icono **Desconectarse del servidor** y después en **Sí** en el cuadro de advertencia.

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 **Opciones > Desconectar y cerrar sesión**. Si utiliza este procedimiento, los archivos que estén abiertos en el escritorio remoto se cerrarán sin guardar.

- Desconectarse desde una aplicación remota.

Opción	Acción
Desconectarse de la aplicación, pero no del servidor	Salga de la aplicación con el procedimiento habitual, por ejemplo, haciendo clic en el botón **Cerrar** en la esquina de la ventana de la aplicación.
Desconectarse de la aplicación y del servidor	Realice una de las siguientes acciones: ■ En la parte superior izquierda de la ventana para seleccionar la aplicación, haga clic en el icono **Desconectarse del servidor** y después en **Sí** en el cuadro de advertencia. ■ Haga clic con el botón secundario en el icono de Horizon Client en la bandeja del sistema y seleccione **Salir**.
Cerrar la ventana para seleccionar la aplicación pero mantener la aplicación en ejecución	Al hacer clic en el botón **Cerrar** solo se cierra la ventana para seleccionar la aplicación.

- Cerrar sesión cuando no tenga ningún escritorio remoto abierto.

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

  a Inicie Horizon Client, conéctese al servidor que proporciona acceso al escritorio remoto y proporcione sus credenciales de autenticación.

  b Haga clic con el botón secundario y seleccione **Cerrar sesión**.

Trabajar en una aplicación o un escritorio remotos 5

Horizon proporciona el entorno de aplicaciones y de escritorios familiares y personalizados que el usuario final espera encontrar. Los usuarios finales pueden acceder a dispositivos USB y de otro tipo conectados al equipo local, enviar documentos a las impresoras que este equipo pueda detectar, autenticarse con tarjetas inteligentes y usar varios monitores.

Este capítulo cubre los siguientes temas:

Matriz de compatibilidad de funciones para clientes Windows

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 5-1. Funciones de escritorios remotos compatibles con sistemas Horizon Client basados en Windows

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
Redireccionamiento de unidades de cliente			X	X	X	X
Audio/vídeo en tiempo real (RTAV)	Limitado	Limitado	X	X	X	X
Redireccionamiento del escáner		Limitado	X	X	X	X
Redireccionamiento del puerto serie			X	X	X	X
Protocolo de visualización de VMware Blast			X	X	X	X
Protocolo de visualización RDP	Limitado	Limitado	X	X	X	X
Protocolo de visualización PCoIP	Limitado	Limitado	X	X	X	X
Persona Management	Limitado	Limitado	X	X		
Wyse MMR	Limitado	Limitado				
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

Los escritorios de Windows 10 necesitan la versión de View Agent 6.2 o Horizon Agent 7.0, o bien una versión posterior de dichos productos. Los escritorios de Windows Server 2012 R2 necesitan View Agent 6.1 o Horizon Agent 7.0, o bien una versión posterior de dichos productos.

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 de invitado. 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.

Para obtener información sobre qué service pack o qué ediciones de los sistemas operativos cliente son compatibles, consulte "Requisitos del sistema para clientes Windows," página 10.

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 5-2. 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 de 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 USB (solo dispositivos de almacenamiento USB)		View Agent 6.1 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 5-2. 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
Redireccionamiento del escáner	View Agent 6.0.2 y posterior	View Agent 6.0.2 y posterior	Horizon Agent 7.0.2 y posterior
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 clientes basados en Windows tienen las siguientes restricciones.

Tabla 5-3. Requisitos para funciones específicas

Función	Requisitos
Redireccionamiento multimedia (MMR) de Windows Media	Requiere View 6.0.2 o posterior. Para usar la función MMR de Windows Media con los escritorios RD, debe tener View Agent 6.1.1 o Horizon Agent 7.0, o bien una versión posterior de ambos productos. Si usa el protocolo de visualización VMware Blast, debe contar con Horizon Agent 7.0 o una versión posterior.
Redireccionamiento del puerto serie	Requiere View 6.1.1 o posterior. Para Windows 10, son necesarias las versiones de View Agent 6.2 o Horizon Agent 7.0, o bien una versión posterior de dichos productos. Si usa el protocolo de visualización VMware Blast, debe contar con Horizon Agent 7.0 o una versión posterior.
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	Requiere Horizon 6.0.1 con View o una versión posterior. Si usa el protocolo de visualización VMware Blast para esta función, debe contar con Horizon Agent 7.0 o una versión posterior.

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

Función	Requisitos
Redireccionamiento del escáner	Requiere View 6.0.2 o posterior. Requiere el protocolo de visualización PCoIP. Para Windows 10, son necesarias las versiones de View Agent 6.2 o Horizon Agent 7.0, o bien una versión posterior de dichos productos. Si usa el protocolo de visualización VMware Blast, debe contar con Horizon Agent 7.0 o una versión posterior.
Redireccionamiento de unidades de cliente	En los escritorios de las máquinas virtuales de usuario único y los escritorios publicados en hosts RDS, son necesarios View Agent 6.1.1 o Horizon Agent 7.0, o bien una versión posterior de ambos productos. Si usa el protocolo de visualización VMware Blast, debe contar con Horizon Agent 7.0 o una versión 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*.

Para las descripciones de estas funciones y sus limitaciones, consulte el documento acerca de *cómo planificar la arquitectura de View*.

Compatibilidad de funciones para los escritorios de Linux

Algunos sistemas operativos invitados Linux 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 una lista de los sistemas operativos Linux admitidos e información sobre funciones compatibles, consulte *Configurar escritorios de Horizon 6 for Linux* o *Configurar escritorios virtuales en Horizon 7*.

Funciones compatibles con el modo anidado

El modo anidado se suele utilizar para los clientes ligeros o cero. En este modo, cuando el usuario final inicia sesión en el cliente cero, Horizon Client se abre y el usuario inicia sesión en un escritorio remoto de forma automática. En este escritorio remoto, el usuario inicia aplicaciones alojadas.

En esta configuración, el escritorio remoto puede ser un escritorio de máquina virtual de usuario único o un escritorio proporcionado por un host RDS. En cualquier caso, el software Horizon Client debe instalarse en el escritorio remoto para proporcionar aplicaciones alojadas. Esta configuración se denomina modo anidado porque el cliente se conecta a un escritorio que también tiene el cliente instalado.

Los siguientes sistemas operativos son compatibles cuando se ejecuta Horizon Client en el modo anidado.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7 Enterprise SP1
- Windows 10 Enterprise (versión 1607)

Las siguientes funciones son compatibles cuando un usuario utiliza Horizon Client en el modo anidado.

- Protocolos de visualización VMware Blast, PCoIP y RDP
- Impresión según ubicación
- Impresión virtual

- Single Sign-On (sin tarjetas inteligentes)
- Redireccionamiento del portapapeles
- Redireccionamiento de contenido URL

Internacionalización

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

Utilizar un IME local con aplicaciones remotas

Cuando utilice configuraciones locales y una distribución de teclado que incluya caracteres especiales, puede utilizar un IME (editor de métodos de entrada) instalado en su sistema local para enviar caracteres especiales a una aplicación remota alojada en host.

También puede utilizar las teclas de acceso rápido y los iconos del área de notificación (bandeja del sistema) de su sistema local para cambiar a otro IME. No es necesario instalar ningún IME en el host RDS remoto.

Cuando esta función está activada, se utiliza el IME local. Si se instala y se configura un IME en un host RDS donde está instalada una aplicación remota, se ignora dicho IME remoto.

De forma predeterminada, esta función está desactivada. Si cambia la configuración para activar o desactivar dicha función, se debe desconectar del servidor y volver a iniciar sesión antes de que se aplique el cambio.

Prerequisitos

- Compruebe que uno o más IME estén instalados en el sistema cliente.
- Asegúrese de que el idioma de entrada de su sistema cliente local coincida con el idioma utilizado en el IME.

  No se puede aplicar el idioma de entrada en el host de RDS.
- Compruebe que el escritorio remoto tenga instalado View Agent 6.0.2 o Horizon Agent 7.0 o una versión posterior.

Procedimiento

1. En la ventana para seleccionar una aplicación y un escritorio de Horizon Client, haga clic con el botón secundario en una aplicación remota y seleccione **Configuración**.
2. En el panel Aplicaciones remotas que aparece, seleccione la casilla **Extender el IME local a las aplicaciones alojadas en el host** y haga clic en **Aceptar**.
3. Reinicie la sesión utilizando una de las siguientes opciones:

Opción	Descripción
Cerrar sesión del servidor	Desconéctese del servidor y, a continuación, vuelva a iniciar sesión y a conectarse con la aplicación. Puede reanudar las aplicaciones que estaban desconectadas pero que no se cerraron, así como los escritorios remotos.
Restablecer las aplicaciones	Haga clic con el botón secundario en el icono de la aplicación remota, seleccione **Configuración** y haga clic en **Restablecer**. Al utilizar esta opción, los escritorios remotos que tenga abiertos no se desconectan. Sin embargo, se cierran todas las aplicaciones remotas y debe volver a iniciarlas.

Se aplica la configuración después de reiniciar la sesión. Se aplica la configuración a todas las aplicaciones remotas alojadas en los hosts del servidor.

4 Utilice el IME local como lo haría con cualquier aplicación instalada de forma local.

La designación del idioma y un icono del IME aparecen en el área de notificaciones (bandeja del sistema) de su sistema cliente local. Puede utilizar las teclas de acceso rápido para cambiar de idioma o de IME. Seguirán funcionando las combinaciones de teclas que realizan ciertas acciones como Ctrl+X para cortar un texto y Alt+Flecha derecha para pasar a otra pestaña.

NOTA: En los sistemas Windows 7 y 8.x, puede especificar teclas de acceso rápido para los IME a través del cuadro de diálogo Servicios de texto e idiomas de entrada (puede acceder a él a través de **Panel de control > Región e idioma > pestaña Teclados e idiomas > botón Cambiar teclados > Servicios de texto e idiomas de entrada > pestaña Configuración avanzada de teclas**).

Habilitar compatibilidad con los teclados en pantalla

Puede configurar su sistema cliente, de forma que si una ventana de Horizon Client tiene el foco, los eventos del panel de escritura a mano, del mouse, del teclado en pantalla y del teclado físico se enviarán a la aplicación o escritorio remotos, aunque el mouse o el teclado en pantalla estén fuera de la ventana de Horizon Client.

Esta función es especialmente práctica si utiliza un tablet Windows basado en x86, como Windows Surface Pro. Para utilizar esta función, debe configurar la clave de registro de Windows `EnableSoftKeypad` como `true`. La ubicación de esta clave depende del tipo de sistema:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- Para Windows de 64 bits: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Cambiar el tamaño de la ventana del escritorio remoto

Para cambiar el tamaño de la ventana del escritorio remoto, debe arrastrar una esquina de la misma. La información sobre herramientas mostrará la resolución de la pantalla en la esquina inferior derecha de la ventana.

Si está utilizando los protocolos de visualización VMware Blast o PCoIP, la información sobre herramientas pasa a mostrar las distintas resoluciones de la pantalla al cambiar el tamaño de la ventana del escritorio. Esta información resulta útil si necesita cambiar el tamaño del escritorio remoto a una resolución específica.

No puede cambiar la resolución de la ventana del escritorio remoto si algún administrador habilitó la opción Locked Guest Size o si usted está utilizando el protocolo de visualización RDP. En tales casos, la información sobre herramientas de resolución muestra la resolución inicial.

Resolución de pantalla y monitores

Puede ampliar un escritorio remoto a varios monitores. Si cuenta con un monitor de alta resolución, puede ver la aplicación o el escritorio remotos en alta resolución.

El modo de visualización Todos los monitores muestra la ventana de un escritorio remoto en varios monitores. La ventana del escritorio remoto aparece en todos los monitores de forma predeterminada. Puede utilizar la función selectiva de varios monitores para mostrar la ventana de un escritorio remoto en un subconjunto de los monitores.

Si utiliza el modo Todos los monitores y hace clic en el botón Minimizar, al maximizar la ventana, esta volverá a dicho modo. De forma similar, si utiliza el modo Pantalla completa y minimiza la ventana, cuando la maximice, esta volverá a dicho modo en uno de los monitores.

Si configuró Horizon Client para que use todos los monitores, al maximizar la ventana de una aplicación se ampliará a pantalla completa solo en el monitor en el que se encuentra.

Configuraciones de varios monitores compatibles

Horizon Client es compatible con las siguientes configuraciones de varios monitores:

- Si utiliza dos monitores, no es necesario que se encuentren en el mismo modo. Por ejemplo, si usa un portátil conectado a un monitor externo, este puede presentar una orientación vertical u horizontal.
- Los monitores pueden estar colocados uno al lado del otro, o bien apilados de dos en dos o en vertical solo si utiliza dos monitores y la altura total es inferior a 4096 píxeles.
- Para utilizar la función selectiva de varios monitores, debe utilizar los protocolos de visualización VMware Blast o PCoIP. Si desea obtener más información, consulte "Seleccionar monitores específicos en una configuración de varios monitores," página 93.
- Para usar la función de procesamiento 3D, debe utilizar los protocolos de visualización VMware Blast o PCoIP. Puede utilizar hasta dos monitores con una resolución máxima de 1920x1200. Con una resolución de 4K (3840x2160), solo se admite un monitor.
- Si utiliza grupos de escritorios clonados instantáneos, el número máximo de monitores que puede usar para mostrar un escritorio remoto es dos, con una resolución máxima de 2560x1600.
- Gracias a los protocolos de visualización de 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 este escenario, puede configurar los PPP del equipo cliente con las opciones correctas y puede habilitar la función Sincronización de PPP para redireccionar la configuración del PPP del equipo cliente al escritorio remoto.

- Si utiliza Microsoft RDP 7, el número máximo de monitores que puede usar para mostrar un escritorio remoto es 16.
- Si utiliza el protocolo de visualización Microsoft RDP, debe tener instalada en el escritorio remoto la versión 6.0 de la Conexión a Escritorio remoto (RDC) de Microsoft o una posterior.

Seleccionar monitores específicos en una configuración de varios monitores

Puede usar la función selectiva de varios monitores para seleccionar los monitores en los que se mostrará una ventana de escritorio remoto. Por ejemplo, si dispone de tres monitores, puede especificar que la ventana del escritorio remoto solo aparezca en dos de esos monitores. De forma predeterminada, la ventana de un escritorio remoto aparecerá en todos los monitores de una configuración de varios monitores.

Puede seleccionar hasta cuatro monitores contiguos. Los monitores pueden estar colocados uno al lado del otro, o bien apilados de dos en dos o en vertical. Se puede apilar un máximo de dos monitores en vertical.

Esta función no es compatible con las aplicaciones remotas.

Procedimiento

1 Inicie Horizon Client e inicie sesión en un servidor.

2 En la ventana de selección de aplicaciones y escritorios, haga clic con el botón secundario en el escritorio remoto y seleccione **Configuración**.

3 Seleccione **PCoIP** o **VMware Blast** en el menú desplegable **Conectarse a través de**.

4 Seleccione **Todos los monitores** en el menú desplegable **Pantalla**.

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

5 Haga clic en una miniatura para seleccionar un monitor en el que se mostrará la ventana del escritorio remoto o para anular la selección.

Al seleccionar un monitor, su miniatura se vuelve verde. Aparecerá un mensaje de advertencia si infringe alguna regla de selección de pantalla.

6 Haga clic en **Aplicar** para guardar los cambios.

7 Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

8 Conéctese al escritorio remoto.

Los cambios se aplicarán inmediatamente cuando se conecte al escritorio remoto. Los cambios se guardarán en el archivo de preferencias de Horizon Client del escritorio remoto después de salir de Horizon Client.

Utilizar un monitor en una configuración de varios monitores

Si tiene varios monitores pero desea que la ventana de un escritorio remoto aparezca solo en un monitor, puede configurar esta ventana para que se abra en solo un monitor.

Esta preferencia no es compatible con las aplicaciones remotas.

Procedimiento

1 Inicie Horizon Client e inicie sesión en un servidor.

2 En la ventana de selección de aplicaciones y escritorios, haga clic con el botón secundario en el escritorio remoto y seleccione **Configuración**.

3 Seleccione **PCoIP** o **VMware Blast** en el menú desplegable **Conectarse a través de**.

4 En el menú **Pantalla**, seleccione **Ventana - Grande**, **Ventana - Pequeña** o **Personalizado**.

Si elige la opción **Personalizado**, puede seleccionar un tamaño de ventana específico.

5 Haga clic en **Aplicar** para guardar los cambios.

Los cambios se aplicarán inmediatamente después de hacer clic en **Aplicar**.

6 Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

De forma predeterminada, la ventana del escritorio remoto se abre en el monitor principal. Puede arrastrar la ventana del escritorio remoto a un monitor que no sea el principal y, la próxima vez que abra el escritorio remoto, dicha ventana aparecerá en ese mismo monitor. La ventana se abre, se sitúa en la parte central del monitor y utiliza el tamaño de ventana que seleccionó como modo de visualización, no en el tamaño que pudo crear al arrastrar la pantalla para cambiarle el tamaño.

Utilizar la función Ajuste de escala de la pantalla

Un usuario que tenga una pantalla de alta resolución como un monitor 4K o que tenga problemas de visión suele tener habilitada la función de escala de pantalla. Para ello, configura los puntos por pulgada (PPP) para que sean superiores al 100% en el equipo cliente. Con la función Ajuste de escala de la pantalla, la aplicación o el escritorio remotos admiten la configuración de la escala del equipo cliente y se mostrarán en tamaño normal en lugar de muy pequeños.

Horizon Client guarda la configuración de la opción Ajuste de escala de la pantalla para cada escritorio remoto de forma independiente. En las aplicaciones remotas, la configuración de la opción Ajuste de escala de la pantalla se aplica a todas las aplicaciones remotas que están disponibles para el usuario que tiene la sesión iniciada. La opción de ajuste de escala de la pantalla aparece incluso si la configuración PPP está establecida en el 100% en el equipo cliente.

Un administrador puede habilitar la opción de directiva de grupo Horizon Client **Locked Guest Size** para ocultar la opción de ajuste de escala de la pantalla. Al habilitar la directiva de grupo **Locked Guest Size** no se deshabilita la función de sincronización PPP. Para deshabilitar la función de sincronización PPP, un administrador debe deshabilitar la opción de la directiva de grupo **Sincronización PPP**. Si desea obtener más información, consulte "Usar la sincronización PPP," página 94.

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

Este procedimiento explica cómo habilitar la función Ajuste de escala de la pantalla antes de conectarse a una aplicación o un escritorio remotos. Puede habilitar esta función después de conectarse a un escritorio remoto. Para ello, seleccione **Opciones > Permitir ajuste de escala de la pantalla**.

Procedimiento

1 Inicie Horizon Client y conéctese a un servidor.

2 En la ventana de selección de aplicaciones y escritorios, haga clic con el botón secundario en la aplicación o el escritorio remotos y seleccione **Configuración**.

3 Marque la casilla de verificación **Permitir ajuste de escala de la pantalla**.

4 Haga clic en **Aplicar** para guardar los cambios.

5 Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Usar la sincronización PPP

La función de sincronización PPP asegura que la configuración PPP del escritorio remoto coincide con la configuración PPP del equipo cliente en las nuevas sesiones remotas. Cuando inicia una nueva sesión, Horizon Agent establece los valores PPP en el escritorio remoto para que coincida con el valor PPP del equipo cliente.

La función Sincronización PPP no puede cambiar la configuración PPP para las sesiones remotas activas. Si vuelve a conectarse a una sesión remota existente, la función de escala de pantalla (si está habilitada) ajusta la aplicación o escritorio remotos de forma apropiada.

La función Sincronización PPP está habilitada de forma predeterminada. Un administrador puede deshabilitar la función Sincronización PPP al deshabilitar la configuración de la directiva de grupo **Sincronización PPP** de Horizon Agent. Debe cerrar sesión e iniciarla de nuevo para que se realicen los cambios en la configuración. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

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

Para escritorios de máquinas virtuales de sesión única, la función Sincronización PPP es compatible con los siguientes sistemas operativos invitados:

- Windows 7 de 64 o 32 bits
- Windows 8.x de 64 o 32 bits
- Windows 10 de 64 o 32 bits
- Windows Server 2008 R2 configurado como escritorio
- Windows Server 2012 R2 configurado como escritorio
- Windows Server 2016 configurado como escritorio

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

- Windows Server 2012 R2
- Windows Server 2016

La función Sincronización PPP requiere Horizon Agent 7.0.2 o versiones posteriores y Horizon Client 4.2 o versiones posteriores.

NOTA: La función Sincronización PPP no está disponible si utiliza Horizon Client 4.2 con Horizon Agent 7.0 o 7.0.1 u Horizon Client 4.0 o 4.1 con Horizon Agent 7.0.2 o versiones posteriores. Únicamente la función Ajuste de escala de la pantalla está disponible en esos casos.

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

- Si cambia la configuración PPP en el equipo cliente, deberá cerrar sesión y volverla a iniciar para que Horizon Client reconozca la nueva configuración PPP. Este requisito se aplica aunque el equipo cliente ejecute Windows 10.
- Si inicia una sesión remota en un equipo cliente que tenga una configuración PPP de más del 100% y utiliza la misma sesión en otro equipo cliente que tenga una configuración PPP diferente de más del 100%, debe cerrar sesión y volver a iniciarla en el segundo equipo cliente para hacer que la sincronización PPP funcione en dicho equipo.
- Aunque los equipos Windows 10 y Windows 8.x sean compatibles con diferentes configuraciones PPP en diferentes monitores, la función Sincronización PPP usa solo el valor PPP que se estableció en el monitor principal del equipo cliente. Todos los monitores en el escritorio remoto también utilizan la misma configuración PPP que el monitor principal del equipo cliente. Horizon Client no admite diferentes configuraciones PPP en monitores diferentes.
- Si un administrador cambia el valor configurado para la directiva de grupo **Sincronización PPP** para Horizon Agent, debe cerrar sesión y volver a iniciarla para que se aplique la nueva configuración.

- Cuando conecte un equipo portátil que admita diferentes configuraciones PPP en monitores distintos a un monitor externo y configure este monitor como el principal, Windows cambiará automáticamente el monitor principal y su configuración PPP cada vez que desconecta o conecta el monitor externo. En esta situación, debe cerrar sesión y volver a iniciarla en el sistema cliente para que Horizon Client reconozca el cambio del monitor principal y debe cerrar sesión y volver a iniciarla en la aplicación o el escritorio remotos para hacer que ambas opciones de PPP sean las mismas en el sistema cliente y en la aplicación o el escritorio remotos.
- Para equipos con Windows 10, haga clic con el botón secundario en su escritorio, seleccione **Configuración de pantalla > Configuración de pantalla avanzada > Tamaño avanzado de texto y otros elementos**, haga clic en el vínculo para **establecer un nivel de escala personalizado** y, a continuación, cierre la sesión y vuelva a iniciarla para que la nueva configuración PPP surta efecto.

Cambiar el modo de visualización mientras la ventana del escritorio está abierta

Puede cambiar los modos de visualización, por ejemplo, del modo Todos los monitores al modo Pantalla completa, sin tener que desconectarse de un escritorio remoto.

Esta función no es compatible con las aplicaciones remotas.

Prerequisitos

Compruebe que utiliza los protocolos de visualización VMware Blast o PCoIP.

Procedimiento

1 En el sistema cliente, en el área de notificaciones (bandeja del sistema), haga clic con el botón secundario en el icono **Horizon Client** y seleccione la opción para abrir la ventana Configuración.

NOTA: También puede abrir la ventana Configuración desde la ventana de selección del escritorio y la aplicación.

2 Seleccione el escritorio remoto y escoja una opción de visualización.

Conectar dispositivos USB

Puede usar dispositivos USB conectados localmente, como unidades de memoria flash, cámaras e impresoras, desde un escritorio remoto. Esta función se denomina redireccionamiento USB.

Cuando se usa esta función, la mayoría de dispositivos USB conectados al sistema de cliente local pasan a estar disponibles en un menú de Horizon Client. Este menú permite conectar y desconectar los dispositivos.

NOTA: Con View Agent 6.1 o posterior, o Horizon Agent 7.0 o posterior, puede también redirigir unidades USB de memoria flash y unidades de disco duro para su uso en aplicaciones y escritorios publicados. Otros tipos de dispositivos USB, entre los que se incluyen otros dispositivos de almacenamiento, como unidades de almacenamiento de seguridad y de CD-ROM USB, no son compatibles con aplicaciones y escritorios publicados. Con Horizon Agent 7.0.2 o versiones posteriores, las aplicaciones y los escritorios publicados pueden admitir dispositivos USB que sean más genéricos, entre los que se incluyen los dispositivos de firma digital Wacom y TOPAZ Signature Pad, así como el pedal Olympus Dictation Foot. Otros tipos de dispositivos USB, incluidas las unidades de almacenamiento de seguridad y las unidades CD-ROM USB, no son compatibles con aplicaciones y escritorios publicados.

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 tabletas y smartphones Samsung con Android, configure 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.
- No use el menú **Conectar dispositivo USB** para la conexión de escáneres. Para usar un dispositivo de escáner, emplee la función de redireccionamiento de escáneres. Esta función se encuentra disponible para Horizon Client cuando se usa con View Agent 6.0.2 o posterior o Horizon Agent 7.0 o posterior. Consulte "Usar escáneres," página 107.
- 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 en View 5.2 Feature Pack 2 o posterior. Consulte "Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos," página 100.
- 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 usar el redireccionamiento USB para 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.

IMPORTANTE: Este procedimiento indica cómo usar un elemento de menú de VMware Horizon Client para configurar la conexión automática d dispositivos USB a un escritorio remoto. También puede configurar la conexión automática mediante la interfaz de línea de comandos de Horizon Client o mediante la creación de una directiva de grupo.

Para obtener más información sobre la interfaz de línea de comandos, consulte "Ejecutar Horizon Client desde la línea de comandos," página 65. Para obtener más información sobre la creación de directivas de grupo, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Prerequisitos

- Para usar dispositivos USB con un escritorio remoto, un administrador de Horizon debe tener la función de 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 *Configurar funciones de escritorios remotos en Horizon 7*.

- 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 VMware 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, seleccione **Dispositivos USB** y, a continuación, **Desconectarse**.
- Configure Horizon Client para conectar automáticamente dispositivos USB al escritorio remoto al insertarlos en el sistema local.

  Use la función de conexión automática si tiene previsto conectar dispositivos que usen controladores MTP, como tabletas y smartphones Samsung con Android.
  a Antes de insertar el dispositivo USB, inicie Horizon Client y conéctese a un escritorio remoto.
  b En la barra de menús de VMware Horizon Client, seleccione **Conectar dispositivo USB > Conectar automáticamente dispositivos USB al insertarlos**.
  c Inserte el dispositivo USB.

  Los dispositivos USB que conecte al sistema local después de iniciar Horizon Client se redirigen al escritorio remoto.
- Configure Horizon Client para conectar los dispositivos USB automáticamente al escritorio remoto cuando se inicie Horizon Client.
  a En la barra de menús de VMware Horizon Client, seleccione **Conectar dispositivo USB > Conectar automáticamente dispositivos USB al inicio**.
  b Inserte el dispositivo USB y reinicie Horizon Client.

Los dispositivos USB que estén conectados al sistema local al iniciar Horizon Client se redirigen al escritorio remoto.

El dispositivo USB se mostrará en el escritorio. Un dispositivo USB puede tardar hasta 20 segundos en mostrarse en el escritorio. Es posible que se le pida que instale algunos controladores la primera vez que conecte el dispositivo al escritorio.

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*.

Configurar los clientes para que vuelvan a conectarse cuando los dispositivos USB se reinician

Si no configura Horizon Client para que conecte automáticamente los dispositivos USB al escritorio remoto, puede configurar Horizon Client para que se vuelva a conectar a dispositivos específicos que se reinician en algunas ocasiones. De lo contrario, cuando se reinicie un dispositivo durante una actualización, este se conectará al sistema local en lugar de conectarse al escritorio remoto.

Si tiene pensado conectar un dispositivo USB como un smartphone o tablet, que se reinician automáticamente durante las actualizaciones del sistema operativo, puede configurar Horizon Client para que vuelva a conectar ese dispositivo específico al escritorio remoto. Para realizar esta tarea, debe editar un archivo de configuración en el cliente.

Si usa la opción **Conectarse automáticamente al insertar el dispositivo** en Horizon Client, todos los dispositivos que conecte al sistema cliente se redireccionan al escritorio remoto. Si no desea que se conecten todos los dispositivos, configure Horizon Client siguiendo el procedimiento que se indica a continuación para que solo se vuelvan a conectar automáticamente ciertos dispositivos USB.

Prerequisitos

Determine el formato hexadecimal del ID del proveedor (VID) y el ID del producto (PID) del dispositivo. Para obtener más instrucciones, consulte el artículo de la base de conocimientos de VMware disponible en http://kb.vmware.com/kb/1011600.

Procedimiento

1 Use un editor de texto para abrir el archivo `config.ini` en el cliente.

Versión del SO	Ruta de archivo
Windows 7, 8.x o Windows 10	`C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini`
Windows XP	`C:\Documents and Settings\All Users\Application Data\VMware\VMware USB Arbitration Service\config.ini`

2 Configure la propiedad `slow-reconnect` para los dispositivos específicos.

```
usb.quirks.device0 = "vid:pid slow-reconnect"
```

En este caso, *vid*:*pid* representan los ID del proveedor y del producto, en formato hexadecimal, para el dispositivo. Por ejemplo, las siguientes líneas establecen esta propiedad para dos dispositivos USB:

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

Especifique las propiedades del dispositivo `usb.quirks.device`*N* en orden, empezando desde 0. Por ejemplo, si a continuación de la línea `usb.quirks.device0` aparece una línea con `usb.quirks.device2` en lugar de `usb.quirks.device1`, solo se lee la primera línea.

Cuando dispositivos como smartphones y tablets actualizan el sistema operativo o el firmware, la actualización se realizará correctamente porque el dispositivo se reiniciará y se conectará al escritorio remoto que lo administra.

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.

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, no la conecte desde el menú **Conectar dispositivo USB** en Horizon Client. Si lo hace, el dispositivo se enrutará a través de un redireccionamiento USB y 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 una cámara web o un micrófono preferidos en un sistema cliente Windows

Con la función Audio/vídeo en tiempo real, si cuenta con varias cámaras web o micrófonos en su sistema cliente, solo uno de ellos se utiliza en su aplicación o escritorio remotos. Para especificar la cámara web o el micrófono preferido, puede configurar las opciones de Audio/vídeo en tiempo real en Horizon Client.

Se usa la cámara web o el micrófono preferidos en el escritorio remoto si están disponibles. Si no es así, se usa otra cámara web u otro micrófono.

Con la función Audio/vídeo en tiempo real, los dispositivos de vídeo, así como los dispositivos de entrada y de 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.

NOTA: Si está utilizando una cámara web o un micrófono USB, no los conecte desde el menú **Conectar dispositivo USB** en Horizon Client. Al hacer esto, se enruta el dispositivo en el redireccionamiento USB para que el dispositivo no pueda usar la función Audio/vídeo en tiempo real.

Prerequisitos

- Asegúrese de que disponga de una cámara web USB, un micrófono USB u otro tipo de micrófono instalado y operativo en el sistema cliente.
- Compruebe que utiliza el protocolo de visualización VMware Blast o el protocolo de visualización PCoIP en la aplicación o el escritorio remotos.
- Conéctese a un servidor.

Procedimiento

1. Abra el cuadro de diálogo Configuración y seleccione **Audio/vídeo en tiempo real** que se encuentra en el panel izquierdo.

   Para abrir el cuadro de diálogo Configuración, haga clic en el icono (rueda dentada) **Configuración** situado en la esquina superior derecha de la pantalla de la aplicación y del escritorio, o haga clic con el botón secundario en el icono de la aplicación o del escritorio y seleccione **Configuración**.

2. Seleccione la cámara web preferida en el menú desplegable **Cámara web preferida** y el micrófono preferido en el menú desplegable **Micrófono preferido**.

   Los menús desplegables muestran las cámaras web y los micrófonos disponibles en el sistema cliente.

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

La próxima vez que inicie una aplicación o escritorio remotos, la cámara web o el micrófono preferidos que seleccionó se redireccionan a la aplicación o al escritorio remotos.

Copiar y pegar texto e imágenes

De forma predeterminada, puede copiar y pegar texto desde su sistema cliente a una aplicación o escritorio remotos. Si un administrador de Horizon habilita la función, también puede copiar y pegar texto desde una aplicación o escritorio remotos a su sistema cliente o entre dos aplicaciones o escritorios remotos. Entre los formatos de archivo admitidos se incluyen texto, imágenes y RTF (formato de texto enriquecido). Se aplican algunas restricciones.

Si utiliza el protocolo de visualización de VMware Blast o el protocolo de visualización de PCoIP, un administrador de Horizon puede establecer esta función de forma que las operaciones de copiar y pegar solo se permitan desde su sistema cliente a una aplicación o a un escritorio remotos, o desde una aplicación o un escritorio remotos a un sistema cliente o ambas posibilidades o ninguna.

Los administradores de Horizon pueden configurar la capacidad de copiar y pegar; para ello configuran una directiva de grupo que pertenezca a Horizon Agent. En función de la versión del agente y del servidor Horizon, los administradores también pueden usar directivas de grupo para restringir los formatos del portapapeles durante las operaciones de copiar y pegar, o bien usar directivas inteligentes para controlar el comportamiento de estas operaciones en escritorios remotos. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

En la versión 7.0 de Horizon 7 o en versiones anteriores, así como en Horizon Client 4.0 y versiones anteriores, el portapapeles puede admitir 1 MB de datos para las operaciones de copiar y pegar. 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.

Si copia texto con formato, algunos de los datos son texto y otros son información de formato. Si copia una gran cantidad de texto con formato o texto e imagen, al intentar pegar el texto y la imagen, es posible que aparezca el texto sin formato (en su totalidad o parte del mismo), pero no se mostrará la imagen ni el formato. El motivo es que los tres tipos de datos se almacenan en ocasiones por separado. Por ejemplo, en función del tipo de documento desde el que va a copiar, las imágenes se pueden almacenar como imágenes o como datos RTF.

Si el texto y los datos RTF juntos utilizan un tamaño menor al máximo permitido para el portapapeles, se pegará el texto con formato. En ocasiones, los datos RTF no se pueden truncar, de tal forma que si el texto y el formato utilizan un tamaño mayor que el máximo permitido para el portapapeles, se rechazarán los datos RTF y el texto sin formato se pegará.

Si no puede pegar todas las imágenes y el texto con formato seleccionados en una operación, es posible que tenga que copiar y pegar cantidades menores en cada operación.

No 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, modifique el valor del Registro de Windows `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. El tipo de valor es REG_DWORD. Se especifica el valor en KB. Si especifica 0 o no especifica un valor, el tamaño de memoria del portapapeles cliente es 8192 KB (8 MB).

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.

Usar aplicaciones remotas

Las aplicaciones remotas se muestran y actúan igual que las aplicaciones que están instaladas en el equipo o portátil cliente.

- Puede minimizar y maximizar una aplicación remota a través de la aplicación. Cuando se minimiza una aplicación remota, esta aparece en la barra de tareas de su sistema cliente. También puede minimizar y maximizar la aplicación remota al hacer clic en su icono en la barra de tareas.

- Puede salir de una aplicación remota a través de la aplicación o al hacer clic con el botón secundario en el icono que aparece en la barra de tareas.
- Puede pulsar Alt+Tabulador para cambiar entre aplicaciones remotas abiertas.
- Si una aplicación remota crea un elemento en la bandeja del sistema de Windows, ese elemento también aparecerá en la bandeja del sistema en el equipo cliente Windows. De forma predeterminada, los iconos de la bandeja del sistema aparecen únicamente para mostrar notificaciones, pero puede personalizar este comportamiento siguiendo el mismo procedimiento que con las aplicaciones instaladas nativas.

NOTA: Si abre el Panel de control para personalizar los iconos del área de notificaciones, los nombres de los iconos de las aplicaciones remotas aparecen en una lista como VMware Horizon Client - *nombre de la aplicación*.

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*.

Imprimir desde una aplicación o escritorio remotos

Desde un escritorio remoto, puede imprimir a una impresora virtual o a una impresora USB que esté conectada a su equipo cliente. La impresión virtual y la impresión USB funcionan juntas sin que se produzca ningún conflicto.

Puede utilizar la función de impresión virtual con los siguientes tipos de aplicaciones y escritorios remotos:

- Escritorios remotos que ejecutan sistemas operativos de Windows Server
- Escritorios basados en sesión (en hosts de RDS de máquina virtual)
- Aplicaciones alojadas remotas

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.

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**.

7 Para personalizar los formularios en papel, defina los formularios en el cliente.

a Diríjase a **Panel de control > Hardware y sonido > Dispositivos e impresoras**.

b Seleccione la impresora y haga clic en la opción **Propiedades del servidor de impresión** situada en la parte superior de la pantalla.

c En la pestaña **Formularios**, especifique la configuración y haga clic en **Guardar formulario**.

Este formulario estará disponible a partir de ahora en el escritorio remoto.

Utilizar impresoras USB

En un entorno de Horizon, las impresoras virtuales y las impresoras USB redirigidas pueden funcionar juntas sin generar ningún conflicto.

Una impresora USB es una impresora que está conectada a un puerto USB en el sistema cliente local. Para enviar tareas de impresión a una impresora USB, puede utilizar la función de redireccionamiento USB o utilizar la función de impresión virtual. A veces, las impresiones USB pueden ser más rápidas que las impresiones virtuales, dependiendo de las condiciones de red.

- Puede utilizar la función de redireccionamiento USB para conectar una impresora USB a un puerto USB virtual en el escritorio remoto si los controladores necesarios también están instalados en el escritorio remoto.

  Si utiliza esta función de redireccionamiento, la impresora ya no estará conectada de forma local al puerto USB físico en el cliente. Esta es la razón por la que la impresora no aparece en la lista de impresoras locales en el equipo cliente local. Esto también implica que pueda imprimir con la impresora USB desde el escritorio remoto, pero no desde el equipo cliente local.

  En el escritorio remoto, las impresoras USB redirigidas aparecen como <*printer_name*>.

  Para obtener más información sobre cómo conectar una impresora USB, consulte "Conectar dispositivos USB," página 96.

- En algunos clientes, puede utilizar como alternativa la función de impresión virtual para enviar tareas de impresión a una impresora USB. Si utiliza la función de impresión virtual, puede imprimir en la impresora USB desde el escritorio remoto y el cliente local, y no necesita instalar los controladores de la impresora en el escritorio remoto.

Controlar la visualización de Adobe Flash

El administrador de Horizon puede configurar el contenido de Adobe Flash que se mostrará en el escritorio remoto a un nivel diseñado para ahorrar recursos informáticos. En algunos casos, esta configuración puede provocar una baja calidad de la reproducción. Al desplazar el cursor del mouse dentro del contenido de Adobe Flash, puede reemplazar las opciones de Adobe Flash que especifique el administrador de Horizon.

El control de visualización de Adobe Flash está disponible únicamente para sesiones de Internet Explorer en Windows y las versiones 9 y 10 de Adobe Flash. Para controlar la calidad de la visualización de Adobe Flash, este no se debe ejecutar en modo de pantalla completa.

Procedimiento

1 Desde Internet Explorer, busque el contenido de Adobe Flash relevante e inícielo si es necesario en el escritorio remoto.

Según la configuración de las opciones de Adobe Flash establecida por parte del administrador de Horizon, es posible que perciba fotogramas descartados o baja calidad de reproducción.

2 Desplace el cursor del mouse dentro del contenido de Adobe Flash mientras se está reproduciendo.

La calidad de la visualización mejora mientras el cursor se encuentra en el contenido de Adobe Flash.

3 Para mantener esta mejora en la calidad, haga doble clic dentro del contenido de Adobe Flash.

Clic en vínculos de URL que se abren fuera de Horizon Client

Un administrador puede configurar vínculos URL en los que hará clic dentro de una aplicación o un escritorio remotos para que se abran en el explorador predeterminado de su sistema cliente. Un vínculo puede ser a una página web, un número de teléfono, una dirección de correo, o cualquier otro tipo de vínculo. Esta función se denomina redireccionamiento de contenido URL.

Un administrador también puede configurar vínculos URL en los que puede hacer clic dentro de un navegador o una aplicación en su sistema cliente para abrirlo en una aplicación o escritorio remotos. En este escenario, si Horizon Client aún no está abierto, se inicia y le solicita que inicie sesión.

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

La primera vez que inicie Horizon Client y se conecte a un servidor en el que esté configurada la función de redireccionamiento de contenido URL, Horizon Client le pide que abra la aplicación VMware Horizon URL Filter al hacer clic en un vínculo para redireccionamiento. Haga clic en **Abrir** para permitir el redireccionamiento de contenido URL.

Dependiendo de cómo se haya configurado la función de redireccionamiento de contenido URL, puede que Horizon Client muestre un mensaje de alerta que le pida que cambie el navegador web predeterminado a VMware Horizon URL Filter. Si ve este aviso, haga clic en el botón **Utilizar "VMware Horizon URL Filter"** para permitir a VMware Horizon URL Filter convertirse en el navegador predeterminado. Este aviso solo se muestra una vez, a menos que cambie el navegador predeterminado tras hacer clic en **Utilizar "VMware Horizon URL Filter"**.

Horizon Client también podría mostrar un mensaje de alerta que le pida que seleccione una aplicación al hacer clic en una URL. Si ve este mensaje, puede hacer clic en **Seleccionar aplicación** para buscar una aplicación en su sistema cliente o haga clic en **Buscar en App Store** para buscar e instalar una nueva aplicación. Si hace clic en **Cancelar**, no se abre la URL.

Cada empresa configura sus propias directivas de redireccionamiento de URL. Si tiene alguna pregunta sobre cómo se comporta esta función en su empresa, póngase en contacto con el administrador del sistema.

Usar la función del mouse relativo para las aplicaciones 3D y CAD

Si usa los protocolos de visualización Blast Extreme o PCoIP cuando use aplicaciones 3D o CAD en un escritorio de View 5.2 o un escritorio posterior, el rendimiento del mouse mejora si habilita la función del mouse relativo.

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

Para las tareas que necesiten usar aplicaciones con un alto consumo gráfico, como AutoCAD, o para jugar a videojuegos 3D, puede mejorar el rendimiento del mouse habilitando la función de mouse relativo, que usa coordenadas relativas en lugar de absolutas. Para usar esta función, seleccione **Opciones > Habilitar mouse relativo** desde la barra de menú de Horizon Client.

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

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

IMPORTANTE: Para usar esta función, es necesario un escritorio de View 5.2 o posterior y debe activar el procesamiento 3D en el grupo de escritorios. Para obtener más información sobre la configuración de grupo y las opciones disponibles para el procesamiento 3D, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Usar escáneres

Puede escanear información en las aplicaciones y los escritorios remotos con escáneres que estén conectados al sistema cliente local. Esta función redirecciona los datos escaneados con un ancho de banda significativamente inferior al que se puede alcanzar utilizando un redireccionamiento USB.

Se puede realizar el redireccionamiento del escáner en escáneres estándares que son compatibles con formatos TWAIN y WIA (Windows Image Acquisition). Aunque debe tener instalados todos los controladores del escáner en el sistema cliente, no es necesario que instale estos controladores en el sistema operativo del escritorio remoto donde el agente esté instalado.

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

IMPORTANTE: Si está utilizando un escáner, no lo conecte desde el menú **Conectar dispositivo USB** en Horizon Client. Si lo hace, el dispositivo se enrutará a través de un redireccionamiento USB y el rendimiento no será adecuado.

Cuando se redirecciona la información escaneada a una aplicación o escritorio remotos, no puede acceder al escáner en el equipo local. En cambio, cuando un escáner está en uso en el equipo local, no podrá acceder a él en la aplicación o el escritorio remotos.

Consejos para usar la función de redireccionamiento del escáner

- Haga clic en el icono del escáner ( ) en la bandeja del sistema o en el área de notificaciones del escritorio remoto para seleccionar un escáner no predeterminado o para cambiar las opciones de configuración. En aplicaciones RDS, el icono de la bandeja del sistema se redireccionará al equipo cliente local.

  No es necesario que use el menú que aparece cuando hace clic en este icono. El redireccionamiento del escáner funciona sin necesidad de configurar nada. El menú de iconos le permite configurar opciones, como cambiar el dispositivo que desea usar si existe más de un dispositivo conectado al equipo cliente.

  NOTA: Si el menú que aparece no muestra ningún escáner, esto significa que un escáner que no es compatible está conectado en el equipo cliente. Si no aparece el icono del escáner, esto significa que la función del redireccionamiento del escáner está deshabilitada o no se instaló en el escritorio remoto. Este icono no aparece en sistemas cliente Mac o Linux porque esta función no es compatible con estos sistemas.

- Haga clic en la opción **Preferencias** del menú para seleccionar opciones para controlar la compresión de imagen, ocultar las cámaras web del menú del redireccionamiento del escáner y determinar cómo seleccionar el escáner predeterminado.

  Puede seleccionar la opción para ocultar las cámaras web si tiene pensado usar la función Audio/vídeo en tiempo real para redireccionar las cámaras web (opción recomendada por VMware). Use el redireccionamiento del escáner con cámaras web para hacerse una foto y escanearla.

  NOTA: Si configura el redireccionamiento del escáner para usar un escáner específico y dicho escáner no está disponible, el redireccionamiento no funcionará.

- Aunque la mayoría de los escáneres TWAIN muestran un cuadro de diálogo de configuración del dispositivo de forma predeterminada, algunos no lo hacen. Para aquellos que no muestren las opciones de configuración, puede usar la opción **Preferencias** en el menú de iconos del escáner y seleccionar la opción **Mostrar siempre el diálogo de las opciones del escáner**.
- Es posible que no se pueda escanear una imagen de gran tamaño o escanear con una resolución elevada. En este caso, puede observar que el indicador del proceso se bloquea o que se salga de la aplicación del escáner de forma inesperada. Si minimiza el escritorio remoto, puede aparecer un mensaje de error en su sistema cliente que le notifica que la resolución es demasiado elevada. Para solucionar este problema, reduzca la resolución o recorte la imagen y vuelva a escanearla.

Usar el redireccionamiento del puerto serie

Con esta función, los usuarios pueden redireccionar los puertos serie conectados (COM) de forma local, como los puertos RS232 integrados, a adaptadores USB a puerto serie. Los dispositivos, como impresoras, lectores de códigos de barra y otros dispositivos serie, se pueden conectar a estos puertos y se pueden usar en los escritorios remotos.

Si un administrador de Horizon configuró la función de redireccionamiento del puerto serie y usa los protocolos de visualización VMware Blast Extreme o PCoIP, el redireccionamiento del puerto serie funciona en su escritorio remoto sin necesidad de configurar nada más. Por ejemplo, COM1 en el sistema cliente local se redirecciona como COM1 en el escritorio remoto. En el caso de COM2, se redirecciona como COM2, a menos que el puerto COM ya se esté utilizando. Si es así, los puertos COM se asignan para evitar conflictos. Por ejemplo, si COM1 y COM2 ya existen en el escritorio remoto, se asigna el COM1 del cliente a COM3 de forma predeterminada.

Aunque debe tener instalados todos los controladores de los dispositivos requeridos en el sistema cliente, no es necesario que instale estos controladores en el sistema operativo del escritorio remoto donde el agente esté instalado. Por ejemplo, si utiliza un adaptador USB a puerto serie que requiera controladores específicos que funcionen en el sistema cliente local, debe instalar estos controladores únicamente en el sistema cliente.

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

Consejos para usar la función de redireccionamiento del puerto serie

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

Cuando haga clic en el icono del puerto serie, aparece el menú contextual **Redireccionamiento COM serie para VMware Horizon**.

NOTA: Si los elementos del menú contextual aparecen atenuados, significa que el administrador bloqueó la configuración. También tenga en cuenta que el icono aparece únicamente si usa las versiones necesarias del agente y de Horizon Client para Windows y debe conectarse a través de Blast Extreme o PCoIP. El icono no aparece si está conectado a un escritorio remoto desde un cliente móvil, Linux o Mac.

- En el menú contextual, los elementos del puerto aparecen en una lista con el siguiente formato, por ejemplo: **COM1 mapped to COM3**. El primer puerto, que se corresponde a COM1 en este ejemplo, es el puerto físico o el adaptador USB a puerto serie que se usa en el sistema cliente local. El segundo puerto, que se corresponde a COM3 en este ejemplo, es el puerto utilizado en el escritorio virtual.
- Haga clic con el botón secundario en el puerto COM para seleccionar el comando **Propiedades de puerto**.

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

  También puede cambiar el número de puerto usado en el escritorio remoto. Por ejemplo, si el puerto COM1 del cliente está asignado a COM3 en el escritorio remoto, pero la aplicación que utiliza necesita el COM1, puede cambiar el número de puerto a COM1. Si COM1 ya existe en el escritorio remoto, verá **COM1 (superpuesto)**. Puede seguir utilizando este puerto superpuesto. El escritorio remoto puede recibir datos en serie a través del puerto desde el host ESXi y también desde el sistema cliente.
- Asegúrese de conectarse a un puerto COM asignado antes de intentar iniciar una aplicación que necesite acceder a este puerto. Por ejemplo, haga clic con el botón secundario en el puerto COM y seleccione **Conectar** para usar el puerto en el escritorio remoto. Cuando inicie la aplicación, esta abrirá el puerto serie.

  Cuando se abra un puerto COM redireccionado y en uso en un escritorio remoto, no podrá acceder al puerto en el equipo local. Recíprocamente, cuando un puerto COM está en uso en el equipo local, no podrá acceder al puerto en el escritorio remoto.
- En el escritorio remoto, puede usar la pestaña **Configuración de puerto** en el Administrador de dispositivos de Windows para establecer la velocidad en baudios de un puerto COM específico. Asegúrese de usar la misma configuración en el Administrador de dispositivos de Windows en el sistema cliente. Tenga en cuenta que la configuración de esta pestaña se utiliza solo si la aplicación no especifica la configuración del puerto.
- Antes de poder desconectar el puerto COM, debe cerrar dicho puerto en la aplicación o cerrar la propia aplicación. Puede seleccionar el comando **Desconectar** para desconectarse y hacer que el puerto COM físico esté disponible para su uso en el equipo cliente.
- La función de conexión automática no funcionará si configura un puerto serie para conectarse automáticamente, inicia una aplicación que abra el puerto serie y, a continuación, desconecta y vuelve a conectar la sesión del escritorio. Tampoco se podrá conectar usando la opción del menú del icono de la bandeja del sistema del puerto serie. En la mayoría de los casos, la aplicación no podrá seguir utilizando el puerto serie. Este es un comportamiento previsto. Debe terminar la aplicación, desconectar la sesión del escritorio y volverse a conectar para resolver el problema.

Métodos abreviados de teclado

Es posible usar métodos abreviados de teclado para los comandos del menú y acciones comunes.

Métodos abreviados que funcionan igual tanto en Horizon Client como en todas las aplicaciones

Tabla 5-4. Métodos abreviados de teclado comunes

Acción	Tecla o combinación de teclas
Hacer clic en el botón destacado en el cuadro de diálogo.	Pulse Intro.
Invocar el menú contextual.	Pulse Mayús+F10.
Hacer clic en el botón **Cancelar** en el cuadro de diálogo.	Pulse ESC.
Desplazarse entre los elementos de la ventana de la sección del servidor o la ventana de selección de aplicaciones y escritorios.	Utilice una tecla de dirección para moverse en la dirección de la flecha. Pulse Tabulador para moverse a la derecha. Pulse Mayús+Tabulador para moverse a la izquierda.
Elimine un elemento de la ventana de la sección del servidor o de la ventana de selección de aplicaciones o escritorios.	Pulse Eliminar.
En Windows 8.x, desplazarse entre la pantalla Inicio y la pantalla del escritorio	Pulse la tecla Windows.

Métodos abreviados en la ventana de Horizon Client (lista de selección de servidores)

Tabla 5-5. Combinaciones de teclas para la ventana en la que especifica a qué servidor conectarse

Acción o comando de menú	Combinación de teclas
Abrir el sistema de ayuda en una ventana del navegador	Alt+O+H, Ctrl+H
Comando **Servidor nuevo**	Alt+N
Mostrar la ventana Información de soporte técnico	Alt+O+S
Mostrar la ventana Acerca de Horizon Client	Alt+O+V
Comando **Configurar SSL**	Alt+O+O
Comando **Ocultar el selector después de iniciar un elemento**	Alt+O+I

Métodos abreviados del selector de aplicaciones y escritorios remotos

Tabla 5-6. Teclas y combinaciones de teclas para usarlas en la ventana de selección de aplicaciones y escritorios

Acción o comando de menú	Combinación de teclas
Abrir el sistema de ayuda en una ventana del navegador	Alt+O+H, Ctrl+H
Mostrar el menú **Opciones**	Alt+O
Mostrar la ventana Información de soporte técnico	Alt+O+S
Mostrar la ventana Acerca de Horizon Client	Alt+O+V
Cerrar sesión del escritorio remoto	Mayús+F10+O
Desconectarse y cerrar sesión del servidor	Alt+D
Activar o desactivar **Mostrar favoritos** y **Mostrar todo**	Alt+F

Tabla 5-6. Teclas y combinaciones de teclas para usarlas en la ventana de selección de aplicaciones y escritorios (Continua)

Acción o comando de menú	Combinación de teclas
Mientras se muestran los favoritos, después de escribir los primeros caracteres del nombre del escritorio o de la aplicación, diríjase al elemento que coincida con la búsqueda	F4
Mientas se muestran los favoritos, diríjase al elemento previo que coincida con la búsqueda	Mayús+F4
Marcar o desmarcar como favorito	Mayús+F10+F
Mostrar el menú **Configuración**	Alt+S o Mayús+F10+S
Iniciar el elemento seleccionado	Entrar o Mayús+F10+L
Anclar un acceso directo de la aplicación o el escritorio remotos en el menú Inicio del sistema cliente (en Windows 7 o versiones anteriores) o la pantalla Inicio (en Windows 8.x)	Mayús+F10+A
Mostrar el menú contextual Configuración de pantalla del escritorio remoto seleccionado	Mayús+F10+D
Utilizar el protocolo de visualización PCoIP para conectarse al escritorio remoto seleccionado	Mayús+F10+P
Utilizar el protocolo de visualización RDP para conectarse al escritorio remoto seleccionado	Mayús+F10+M
Crear un acceso directo al escritorio del elemento seleccionado	Mayús+F10+C
Agregar el elemento seleccionado a su menú o pantalla de Inicio	Mayús+F10+A
Restablecer el escritorio seleccionado (si su administrador le permite restablecerlo)	Mayús+F10+R
Actualizar la lista de aplicaciones y escritorios	F5

Métodos abreviados en la ventana del escritorio (con sesiones VMware Blast Extreme o PCoIP)

Estos métodos abreviados funcionan si pulsa primero Ctrl+Alt o hace clic en la barra de menú de Horizon Client en lugar de hacerlo dentro del sistema operativo del escritorio remoto, antes de pulsar las teclas.

Tabla 5-7. Combinaciones de teclas para las sesiones PCoIP y VMware Blast

Acción o comando de menú	Combinación de teclas
Liberar el cursor del mouse para que ya no esté dentro del sistema operativo del escritorio remoto	Ctrl+Alt
Mostrar el menú Opciones	Alt+O
Mostrar la ventana Información de soporte técnico	Alt+O+M
Mostrar la ventana Acerca de Horizon Client	Alt+O+V
Invocar el cuadro de diálogo de la configuración de las carpetas compartidas	Alt+O+F
Activar o desactivar **Habilitar escala de la pantalla**	Alt+O+N
Comando **Cambiar a otro escritorio**	Alt+O+S
Comando **Conectarse automáticamente a este escritorio**	Alt+O+A

Tabla 5-7. Combinaciones de teclas para las sesiones PCoIP y VMware Blast (Continua)

Acción o comando de menú	Combinación de teclas
Comando **Habilitar mouse relativo**	Alt+O+E
Comando **Enviar Ctrl+Alt+Supr**	Alt+O+C
Comando **Desconectar**	Alt+O+D
Comando **Desconectar y cerrar sesión**	Alt+O+L
Comando **Conectar dispositivo USB**	Alt+U

Solucionar problemas relacionados con Horizon Client 6

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.

Qué hacer si Horizon Client termina de forma inesperada

Es posible que Horizon Client termine aunque no lo cierre.

Problema

Es posible que Horizon Client termine de forma inesperada. Según la configuración del servidor de conexión, es posible que vea el mensaje `No hay conexión segura al servidor de conexión de View`. En algunos casos, no se muestra ningún mensaje.

Origen

Este problema se produce cuando se pierde la conexión al servidor de conexión.

Solución

- Reiniciar Horizon Client. Puede conectarse correctamente cuando el servidor de conexión vuelve a ejecutarse. Si continúa teniendo problemas de conexión, póngase en contacto con el administrador de Horizon.

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 escritorio**.

Opción	Acción
Desde el SO de escritorio	Seleccione **Opciones > Reiniciar escritorio** en la barra de menús.
Desde la ventana de selección de escritorios	Haga clic con el botón secundario en el icono del escritorio y seleccione **Reiniciar escritorio**.

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," página 114.

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

1 Para restablecer un escritorio remoto, utilice el comando **Restablecer escritorio**.

Opción	Acción
Desde el SO de escritorio	Seleccione **Opciones > Restablecer escritorio** en la barra de menú.
En la ventana para seleccionar la aplicación y el escritorio	Haga clic con el botón secundario y seleccione **Restablecer escritorio**.

2 Para restablecer aplicaciones remotas, utilice el botón **Restablecer** en el escritorio y la ventana de selección de aplicaciones.

   a Haga clic en el botón **Configuración** (icono de rueda dentada) en la barra de menú.

   b Seleccione **Aplicaciones** en el panel izquierdo, haga clic en el botón **Restablecer** y, finalmente, haga clic en **Aceptar**.

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

En ocasiones, para solucionar los problemas relacionados con Horizon Client, debe desinstalar y volver a instalar la aplicación Horizon Client.

Para desinstalar Horizon Client, utilice el mismo método que suele usar para desinstalar cualquier otra aplicación.

Por ejemplo, utilice el applet **Agregar o quitar programas** disponible en su sistema operativo de Windows para eliminar la aplicación VMware Horizon Client.

Una vez que el proceso de desinstalación haya finalizado, puede volver a instalar la aplicación.

Consulte Capítulo 2, “Instalar Horizon Client para Windows,” página 27.

Índice

U

V

W