

Configurar funciones de escritorios remotos en Horizon 7

Modificado para Horizon 7 7.3.2
VMware Horizon 7 7.3



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2019 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

1	Configurar funciones de escritorios remotos en Horizon 7	7
2	Configurar funciones de escritorios remotos	8
	Configurar Unity Touch	9
	Requisitos del sistema para Unity Touch	9
	Configurar las aplicaciones favoritas mostradas por Unity Touch	9
	Configurar el redireccionamiento URL de Flash para la transmisión multidifusión o unidifusión	12
	Requisitos del sistema para la función Redireccionamiento URL flash	13
	Verificar que la función Redireccionamiento URL de Flash esté instalada	15
	Configurar páginas web que proporcionan transmisiones multidifusión o unidifusión	15
	Configurar dispositivos cliente para Redireccionamiento URL de Flash	16
	Deshabilitar o habilitar Redireccionamiento URL de Flash	16
	Configurar el redireccionamiento de Flash	17
	Requisitos del sistema para la función Redireccionamiento Flash	18
	Instalar y configurar el redireccionamiento de Flash	19
	Usar las opciones del Registro de Windows para configurar el redireccionamiento de Flash	22
	Configurar el Redireccionamiento multimedia HTML5	23
	Requisitos del sistema para el redireccionamiento multimedia HTML5	23
	Instalar y configurar el Redireccionamiento multimedia HTML5	24
	Forzar la instalación de la extensión Redireccionamiento HTML5 de VMware Horizon	26
	Configurar audio/vídeo en tiempo real	27
	Opciones de configuración de audio/vídeo en tiempo real	27
	Requisitos del sistema para la función Audio/vídeo en tiempo real	28
	Garantizar que se usa Audio/vídeo en tiempo real en lugar de redireccionamiento USB	29
	Seleccionar cámaras web y micrófonos preferidos	30
	Configurar los ajustes de directivas de grupo de audio/vídeo en tiempo real	39
	Ancho de banda de Audio/vídeo en tiempo real	43
	Configurar el redireccionamiento del escáner	44
	Requisitos del sistema para la función de redireccionamiento del escáner	44
	Operación del usuario de Redireccionamiento de escáner	45
	Configurar los ajustes de directivas de grupo de redireccionamiento del escáner	47
	Configurar el redireccionamiento del puerto serie	51
	Requisitos del sistema para el redireccionamiento del puerto serie	51
	Operación del usuario de redireccionamiento de puerto serie	52
	Directrices para configurar el redireccionamiento del puerto serie	54
	Configurar los ajustes de directivas de grupo de redireccionamiento de puertos serie	54
	Configurar adaptadores de USB a serie	59
	Administrar el acceso al Redireccionamiento multimedia (MMR) de Windows Media	60

Habilitar redireccionamiento multimedia en Horizon 7	60
Requisitos del sistema para MMR de Windows Media	61
Determinar si usar Redireccionamiento multimedia (MMR) de Windows Media según la latencia de red	62
Administrar el acceso al redireccionamiento de unidades cliente	63
Usar la directiva de grupo para deshabilitar el redireccionamiento de la unidad cliente	64
Usar las opciones del registro para configurar el redireccionamiento de la unidad cliente	64
Usar el redireccionamiento de unidades cliente en una implementación de Unified Access Gateway	66
Configurar Skype Empresarial	66
Recopilar registros para solucionar los problemas de Skype Empresarial	69
Activar el canal lateral de BEAT para el redireccionamiento de unidades cliente o USB	70
3 Configurar el redireccionamiento de contenido URL	72
Información sobre el redireccionamiento de contenido URL	72
Requisitos del redireccionamiento de contenido URL	73
Utilizar el redireccionamiento de contenido URL en un entorno de Arquitectura de Cloud Pod	73
Instalar Horizon Agent con la función Redireccionamiento de contenido URL	74
Configurar el redireccionamiento de agente a cliente	74
Agregar la plantilla ADMX de redireccionamiento de contenido URL a un GPO	75
Configuración de directiva de grupo del Redireccionamiento de contenido URL	76
Sintaxis para crear reglas de redireccionamiento de contenido URL	78
Ejemplo de directiva de grupo de redireccionamiento de agente a cliente	78
Configurar el redireccionamiento de cliente a agente	79
Instalar Horizon Client para Windows con la función de redireccionamiento de contenido URL	80
Usar la utilidad vdmutil de la línea de comandos	80
Crear una opción de redireccionamiento de contenido URL	82
Crear una opción de redireccionamiento de contenido URL global	84
Asignar una opción de redireccionamiento de contenido URL a un usuario o grupo	86
Configurar una opción de redireccionamiento de contenido URL	87
Administrar la opción de redireccionamiento de contenido URL	89
Usar la configuración de directiva de grupo para configurar el redireccionamiento de cliente a agente	90
Limitaciones de Redireccionamiento de contenido URL	90
Funciones no compatibles del redireccionamiento del contenido URL	91
4 Usar dispositivos USB con aplicaciones y escritorios remotos	93
Limitaciones sobre los tipos de dispositivos USB	94
Descripción general de la configuración del redireccionamiento USB	95
Tráfico de red y redireccionamiento USB	97
Habilitar la función de SDK de mejora de sesiones a través de USB	97
Conexiones automáticas a dispositivos USB	98

Implementar dispositivos USB en un entorno de Horizon 7 seguro	99
Deshabilitar el redireccionamiento USB en todos los tipos de dispositivos	99
Deshabilitar el redireccionamiento USB de dispositivos específicos	100
Usar archivos de registro para solucionar problemas y para determinar los ID de los dispositivos USB	102
Usar directivas para controlar el redireccionamiento USB	103
Configurar los ajustes de directiva de división de dispositivo para dispositivos USB compuestos	104
Configurar los ajustes de directiva de filtro para dispositivos USB	107
Familias de dispositivos USB	111
Opciones para los USB en la plantilla ADMX de configuración de Horizon Agent	112
Solucionar los problemas del redireccionamiento USB	115

5 Configurar directivas para grupos de escritorios y aplicaciones 118

Establecer directivas en Horizon Administrator	118
Configurar las opciones de la directiva global	119
Configurar directivas para los grupos de escritorios	119
Configurar directivas para los usuarios	120
Directivas de Horizon 7	120
Usar Directivas de Smart	121
Requisitos de Directivas de Smart	121
Instalar User Environment Manager	122
Configurar User Environment Manager	122
Opciones de directivas inteligentes de Horizon	123
Referencia del perfil de ancho de banda	124
Agregar condiciones a las definiciones de directivas de Horizon Smart	124
Crear una directiva de Horizon Smart en User Environment Manager	127
Usar las directivas de grupo de Active Directory	128
Crear una OU para los escritorios remotos	129
Habilitar procesamiento de bucle invertido para escritorios remotos	129
Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7	130
Archivos de plantilla ADMX de Horizon 7	130
Agregar los archivos de plantilla ADMX a Active Directory	132
Opciones de la plantilla ADMX de configuración de VMware View Agent	133
Información de sistema cliente enviada a escritorios remotos	141
Ejecutar comandos en escritorios de Horizon	145
Configuración de directiva de VMware Virtualization Pack para Skype Empresarial	145
Configuración de directivas de PCoIP	146
Configuración general de PCoIP	147
Configuración del portapapeles de PCoIP	156
Configuración de ancho de banda de PCoIP	159
Configuración del teclado para PCoIP	162

Función Compilación sin pérdida de PCoIP	163
Configuración de la directiva VMware Blast	164
Habilitar Compresión sin pérdida de información para VMware Blast	168
Usar Servicios de Escritorio remoto de directivas de grupo	169
Agregar el archivo ADMX de Servicios de Escritorio remoto a Active Directory	169
Configuración de compatibilidad de aplicación con RDS	170
Configuración de conexiones RDS	172
Configuración de redirección de dispositivo o recurso de RDS	177
Configuración de licencias de RDS	182
Configuración del redireccionamiento de la impresora RDS	184
Configuración de perfiles RDS	188
Configuración del servidor de conexión RDS	191
Configuración del entorno de sesión remota de RDS	195
Configuración de seguridad de RDS	204
Límites de tiempo de sesión RDS	209
Configuración de carpetas temporales de RDS	213
Filtrar las impresoras por impresión virtual	214
Configurar impresión según ubicación	214
Registrar el archivo DLL de la directiva de grupo de impresión según ubicación	216
Configurar la directiva de grupo de impresión según ubicación	216
Sintaxis de la opción de la directiva de grupo de impresión según ubicación	218
Ejemplo de directiva de grupo de Active Directory	220
Crear una unidad organizativa (OU) para máquinas de Horizon 7	221
Crear GPO para directivas de grupo de Horizon 7	221
Agregar un archivo de plantilla ADMX Horizon 7 a un GPO	222
Habilitar procesamiento de bucle invertido para escritorios remotos	223

Configurar funciones de escritorios remotos en Horizon 7

1

Configurar funciones de escritorios remotos en Horizon 7 describe cómo configurar las funciones de escritorios remotos que se instalan con Horizon Agent en los escritorios de máquinas virtuales o en un host RDS. También puede configurar directivas para controlar el comportamiento de grupos de escritorios y aplicaciones, máquinas y usuarios.

Público al que se dirige

Esta información está destinada a quienes desean configurar funciones de escritorios remotos o directivas en los escritorios de máquinas virtuales o en hosts RDS. La información está destinada a administradores de sistemas Windows que estén familiarizados con la tecnología de máquinas virtuales y operaciones de centros de datos.

Configurar funciones de escritorios remotos

2

Algunas funciones de escritorios remotos instaladas con Horizon Agent se pueden actualizar tanto en las versiones de actualizaciones de paquetes de características como en las versiones principales de Horizon 7. Puede configurar estas funciones para mejorar la experiencia de escritorio remoto de sus usuarios finales.

Entre estas funciones se incluyen HTML Access, Unity Touch, Redireccionamiento URL flash, Redireccionamiento multimedia HTML5, Audio/vídeo en tiempo real, Redireccionamiento multimedia (Multimedia Redirection, MMR) de Windows Media, Redireccionamiento USB, Redireccionamiento de escáner, Redireccionamiento de puerto serie y Redireccionamiento de contenido URL.

Para obtener información sobre HTML Access, consulte el documento *Guía de instalación y configuración de VMware Horizon HTML Access*. Para obtener información acerca del Redireccionamiento USB, consulte [Capítulo 4 Usar dispositivos USB con aplicaciones y escritorios remotos](#). Para obtener información acerca del Redireccionamiento de contenido URL, consulte [Capítulo 3 Configurar el redireccionamiento de contenido URL](#).

Este capítulo incluye los siguientes temas:

- [Configurar Unity Touch](#)
- [Configurar el redireccionamiento URL de Flash para la transmisión multidifusión o unidifusión](#)
- [Configurar el redireccionamiento de Flash](#)
- [Configurar el Redireccionamiento multimedia HTML5](#)
- [Configurar audio/vídeo en tiempo real](#)
- [Configurar el redireccionamiento del escáner](#)
- [Configurar el redireccionamiento del puerto serie](#)
- [Administrar el acceso al Redireccionamiento multimedia \(MMR\) de Windows Media](#)
- [Administrar el acceso al redireccionamiento de unidades cliente](#)
- [Configurar Skype Empresarial](#)
- [Activar el canal lateral de BEAT para el redireccionamiento de unidades cliente o USB](#)

Configurar Unity Touch

Con Unity Touch, los usuarios de tablets y smartphones pueden examinar, buscar y abrir fácilmente archivos y aplicaciones de Windows, elegir sus archivos y aplicaciones favoritos y cambiar de una aplicación en ejecución a otra, todo ello sin tener que usar el menú Inicio ni la barra de tareas. Puede configurar una lista predeterminada de aplicaciones favoritas que aparecen en la barra lateral de Unity Touch.

Puede deshabilitar o habilitar la función Unity Touch después de instalar Horizon Agent, si establece la opción de directiva de grupo **Habilitar Unity Touch** en el archivo de plantilla ADMX de configuración de Horizon Agent (`vdm_agent.admx`).

Los documentos de VMware Horizon Client para dispositivos iOS, Android y Chrome OS proporcionan más información sobre funciones de usuario final que ofrece Unity Touch.

Requisitos del sistema para Unity Touch

El software Horizon Client y los dispositivos móviles en los que instala Horizon Client deben cumplir algunos requisitos de la versión para admitir Unity Touch.

Escritorio de Horizon 7	<p>Para admitir Unity Touch, el siguiente software debe estar instalado en la máquina virtual a la que accederá el usuario final:</p> <ul style="list-style-type: none">■ Puede instalar la función Unity Touch al instalar View Agent 6.0 o una versión posterior. Consulte la sección sobre cómo instalar View Agent en una máquina virtual en el documento <i>Configurar escritorios virtuales en Horizon 7</i>.■ Sistemas operativos: Windows 7 (32 o 64 bits), Windows 8 (32 o 64 bits), Windows 8.1 (32 o 64 bits), Windows Server 2008 R2 o Windows Server 2012 R2, Windows 10 (32 o 64 bits)
Software de Horizon Client	<p>Unity Touch es compatible con las siguientes versiones de Horizon Client:</p> <ul style="list-style-type: none">■ Horizon Client para iOS■ Horizon Client para Android■ Horizon Client para Chrome OS

Configurar las aplicaciones favoritas mostradas por Unity Touch

Con la función Unity Touch, los usuarios de tablets y smartphones pueden acceder rápidamente a un archivo o una aplicación de escritorio de Horizon 7 desde una barra lateral de Unity Touch. Aunque los usuarios finales pueden especificar qué aplicaciones favoritas se muestran en la barra lateral, para una mayor comodidad, los administradores pueden configurar una lista predeterminada de aplicaciones favoritas.

Si usa grupos de escritorios de asignaciones flotantes, las aplicaciones y los archivos favoritos que especifiquen los usuarios finales se perderán cuando se desconecten de un escritorio, a menos que habilite los perfiles de itinerancia de usuarios en Active Directory.

La lista predeterminada de aplicaciones favoritas permanece en efecto cuando un usuario final se conecta por primera vez a un escritorio que tenga habilitada la función Unity Touch. Sin embargo, si el usuario configura su propia lista de aplicaciones favoritas, se ignora la lista predeterminada. La lista de aplicaciones favoritas del usuario permanece en el perfil móvil del usuario y está disponible cuando el usuario se conecta a distintas máquinas en un grupo flotante o dedicado.

Si crea una lista predeterminada de aplicaciones favoritas y una o varias aplicaciones no están instaladas en el sistema operativo del escritorio Horizon 7 o las rutas de acceso a estas aplicaciones no se encuentran en el menú Inicio, las aplicaciones no aparecerán en la lista de favoritos. Puede usar este comportamiento para configurar una lista predeterminada maestra de aplicaciones favoritas que se pueda aplicar a varias imágenes de máquinas virtuales con distintos conjuntos de aplicaciones instaladas.

Por ejemplo, si Microsoft Office y Microsoft Visio están instaladas en una máquina virtual y Windows Powershell y VMware vSphere Client están instaladas en una segunda máquina virtual, puede crear una lista que incluya las cuatro aplicaciones. Solo las aplicaciones instaladas aparecerán como aplicaciones favoritas predeterminadas en los escritorios correspondientes.

Puede utilizar distintos métodos para especificar una lista predeterminada de aplicaciones favoritas:

- Agregar un valor al registro de Windows en las máquinas virtuales del grupo de escritorios
- Crear un paquete de instalación administrativa desde el instalador de Horizon Agent y distribuir el paquete a las máquinas virtuales
- Ejecutar el instalador de Horizon Agent desde la línea de comandos en las máquinas virtuales

Nota Unity Touch asume que los accesos directos a las aplicaciones se encuentran en la carpeta Programas del menú **Inicio**. Si algún acceso directo se encuentra fuera de la carpeta Programas, anexe el prefijo **Programas** a la ruta de acceso del acceso directo. Por ejemplo, Windows Update.lnk se encuentra en la carpeta ProgramData\Microsoft\Windows\Menú Inicio. Para publicar este acceso directo como una aplicación favorita predeterminada, añada el prefijo **Programas** a la ruta de acceso del acceso directo. Por ejemplo: "Programas/Windows Update.lnk".

Requisitos previos

- Compruebe que Horizon Agent esté instalado en la máquina virtual.
- Compruebe que tenga derechos administrativos en la máquina virtual. Para este procedimiento, puede que tenga que editar una configuración del registro.
- Si tiene grupos de escritorios de asignación flotante, use Active Directory para configurar perfiles de usuarios móviles. Siga las instrucciones proporcionadas por Microsoft.

Los usuarios de grupos de escritorios de asignación flotante podrán ver su lista de aplicaciones favoritas y archivos favoritos cada vez que inicien sesión.

Procedimiento

- ◆ (opcional) Cree una lista predeterminada de aplicaciones favoritas añadiendo un valor al registro de Windows.

- a Abra regedit y vaya a la configuración de registro HKLM\Software\VMware, Inc.\VMware Unity.

En una máquina virtual de 64 bits, vaya al directorio HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity.

- b Cree un valor de cadena con el nombre FavAppList.
- c Especifique las aplicaciones favoritas predeterminadas.

Utilice el siguiente formato para especificar las rutas de los accesos directos a las aplicaciones que se utilizan en el menú **Inicio**.

```
path-to-app-1|path-to-app-2|path-to-app-3|...
```

Por ejemplo:

```
Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk
```

- ◆ (opcional) Cree una lista predeterminada de aplicaciones favoritas creando un paquete de instalación administrativa desde el instalador de Horizon Agent.

- a Desde la línea de comandos, use el siguiente formato para crear el paquete de instalación administrativa.

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""un recurso compartido de red para almacenar el paquete de instalación administrativa"" UNITY_DEFAULT_APPS=""la lista de aplicaciones favoritas predeterminadas que deben establecerse en el registro""
```

Por ejemplo:

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\ViewFeaturePack\""" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|""
```

- b Distribuya el paquete de instalación administrativa desde el recurso compartido de red hasta las máquinas virtuales de escritorios mediante un método de implementación estándar de Microsoft Windows Installer (MSI) que se utilice en su organización.

- ◆ (opcional) Cree una lista predeterminada de aplicaciones favoritas ejecutando el instalador de Horizon Agent en una línea de comandos directamente en una máquina virtual.

Utilice el siguiente formato.

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""la lista de aplicaciones favoritas predeterminadas que se deben establecer en el registro""
```

Nota El comando precedente combina la instalación de Horizon Agent con la especificación de la lista predeterminada de aplicaciones favoritas. No tiene que instalar Horizon Agent antes de ejecutar este comando.

Pasos siguientes

Si realizó esta tarea directamente en una máquina virtual (editando el registro de Windows o instalando Horizon Agent desde la línea de comandos), debe implementar la máquina virtual recién configurada. Puede crear una snapshot o hacer una plantilla y crear un grupo de escritorios, o recomponer un grupo existente. O puede crear una directiva de grupo de Active Directory para implementar la nueva configuración.

Configurar el redireccionamiento URL de Flash para la transmisión multidifusión o unidifusión

Ahora los clientes pueden usar Adobe Media Server y multidifusión o unidifusión para suministrar eventos de vídeo en directo en un entorno de infraestructura de escritorio virtual (virtual desktop infrastructure, VDI). Para suministrar transmisiones de vídeo en directo multidifusión o unidifusión en un entorno VDI, la secuencia de medios debe enviarse directamente desde el origen de medios hasta los endpoints, omitiendo los escritorios remotos. La función Redireccionamiento URL de Flash admite esta capacidad interceptando y redirigiendo el archivo ShockWave Flash (SWF) desde el escritorio remoto hasta el endpoint de cliente.

El contenido Flash se muestra a continuación mediante los reproductores multimedia Flash locales de los clientes.

Al enviar el contenido Flash directamente desde Adobe Media Server a endpoints de 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 de cliente.

La función Redireccionamiento URL de Flash usa un JavaScript incrustado en una página web HTML por el administrador de la página web. Cuando un usuario del escritorio remoto hace clic en el vínculo URL designado desde una página web, JavaScript intercepta y redirige el archivo SWF desde la sesión del escritorio remoto al endpoint de cliente. A continuación, el endpoint abre un Flash Projector local fuera de la sesión del escritorio virtual y reproduce la secuencia de medios de forma local.

Para configurar el Redireccionamiento URL de Flash, debe configurar su página web HTML y sus dispositivos cliente.

Procedimiento

1 Requisitos del sistema para la función Redireccionamiento URL flash

Para admitir el Redireccionamiento URL flash, la implementación de Horizon 7 debe cumplir ciertos requisitos de software y hardware.

2 Verificar que la función Redireccionamiento URL de Flash esté instalada

Antes de usar esta función, verifique que la función Redireccionamiento URL de Flash está instalada y se ejecute en los escritorios virtuales.

3 Configurar páginas web que proporcionan transmisiones multidifusión o unidifusión

Para permitir que se realice el redireccionamiento, debe insertar un comando de JavaScript en las páginas web MIME HTML (MHTML) que proporcionen vínculos a las transmisiones multidifusión o unidifusión. Los usuarios muestran estas páginas web en los navegadores de sus escritorios remotos para acceder a las transmisiones de vídeo.

4 Configurar dispositivos cliente para Redireccionamiento URL de Flash

La función Redireccionamiento URL de Flash redirecciona el archivo SWF desde escritorios remotos a dispositivos cliente. Para permitir que estos dispositivos cliente reproduzcan vídeos de Flash desde una transmisión multidifusión o unidifusión, debe verificar que la versión adecuada de Adobe Flash Player esté instalada en los dispositivos cliente. Los clientes también deben tener conectividad IP con el origen de medios.

5 Deshabilitar o habilitar Redireccionamiento URL de Flash

El Redireccionamiento URL de Flash está habilitado cuando realiza una instalación silenciosa de Horizon Agent con la propiedad `VDM_FLASH_URL_REDIRECTION=1`. Puede deshabilitar o rehabilitar la función de Redireccionamiento URL de Flash en escritorios remotos seleccionados estableciendo un valor en la clave de registro de Windows de esas máquinas virtuales.

Requisitos del sistema para la función Redireccionamiento URL flash

Para admitir el Redireccionamiento URL flash, la implementación de Horizon 7 debe cumplir ciertos requisitos de software y hardware.

Escritorio de Horizon 7

- Instale el Redireccionamiento URL Flash introduciendo la propiedad `VDM_FLASH_URL_REDIRECTION` en la línea de comandos durante una instalación silenciosa de View Agent 6.0 o una versión posterior. Consulte la sección sobre las propiedades de instalación silenciosa para Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7*.
- Los escritorios deben ejecutar sistemas operativos Windows 7 de 64 o 32 bits.

Reproductor multimedia Flash y ShockWave Flash (SWF)

- Entre los navegadores de escritorios compatibles se incluyen Internet Explorer 8, 9 y 10 y Chrome 29.x y Firefox 20.x.

Debe integrar un reproductor multimedia Flash, como Strobe Media Playback, en el sitio web. Para transmitir contenido multidifusión, puede usar `multicastplayer.swf` o `StrobeMediaPlayback.swf` en las páginas web. Para transmitir contenido unidifusión, debe usar `StrobeMediaPlayback.swf`. También puede usar `StrobeMediaPlayback.swf` para otras funciones compatibles, como la transmisión RTMP y la transmisión dinámica HTTP.

Software de Horizon Client

Las siguientes versiones de Horizon Client admiten la unidifusión y la multidifusión:

- Horizon Client 2.2 para Linux o una versión posterior
- Horizon Client 2.2 para Windows o una versión posterior

Las siguientes versiones de Horizon Client solo admiten la multidifusión (no admiten la unidifusión):

- Horizon Client 2.0 o 2.1 para Linux
- Horizon Client 5.4 para Windows

Equipo con Horizon Client o dispositivo de acceso del cliente

- El Redireccionamiento URL flash es compatible con todos los sistemas operativos que ejecutan Horizon Client for Linux en dispositivos de cliente ligero x86. Esta función no es compatible con procesadores ARM.
- La función Redireccionamiento URL flash es compatible con todos los sistemas operativos que ejecutan Horizon Client para Windows. Para obtener más información consulte el documento *Uso de VMware Horizon Client para Windows*.
- En los dispositivos cliente de Windows, debe instalar Adobe Flash Player 10.1 o una versión posterior para Internet Explorer.
- En los dispositivos de cliente ligero de Linux, debe instalar los archivos `libexpat.so.0` y `libflashplayer.so`. Consulte [Configurar dispositivos cliente para Redireccionamiento URL de Flash](#).

Nota Con Redireccionamiento URL de Flash, la transmisión multidifusión o unidifusión se redirecciona a los dispositivos cliente que puedan estar fuera del firewall de su organización. Los clientes deben tener acceso al servidor Adobe Web que aloja el archivo ShockWave Flash (SWF) que inicia las transmisiones multidifusión o unidifusión. Si es necesario, configure el firewall para abrir los puertos apropiados para permitir que los dispositivos cliente accedan a este servidor.

Verificar que la función Redireccionamiento URL de Flash esté instalada

Antes de usar esta función, verifique que la función Redireccionamiento URL de Flash está instalada y se ejecute en los escritorios virtuales.

La función Redireccionamiento URL de Flash debe estar presente en cada escritorio que desee que admita el redireccionamiento unidifusión o multidifusión. Si desea obtener instrucciones sobre cómo instalar Horizon Agent, consulte la sección sobre las propiedades de instalación silenciosa para Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7*.

Procedimiento

- 1 Inicie una sesión de escritorio remoto que use PCoIP.
- 2 Abra el Administrador de tareas.
- 3 Verifique que el proceso ViewMPServer.exe se esté ejecutando en el escritorio.

Configurar páginas web que proporcionan transmisiones multidifusión o unidifusión

Para permitir que se realice el redireccionamiento, debe insertar un comando de JavaScript en las páginas web MIME HTML (MHTML) que proporcionen vínculos a las transmisiones multidifusión o unidifusión. Los usuarios muestran estas páginas web en los navegadores de sus escritorios remotos para acceder a las transmisiones de vídeo.

Además, puede personalizar el mensaje de error en inglés que se muestra a los usuarios finales cuando se produce un problema con el redireccionamiento URL de Flash. Siga este paso opcional si quiere mostrar un mensaje de error localizado a sus usuarios finales. Debe insertar la configuración var vmwareScriptErrorMessage junto con la cadena de texto localizada en la página web MHTML.

Requisitos previos

Verifique que la biblioteca swfobject.js se importara a la página web MHTML.

Procedimiento

- 1 Inserte el comando de JavaScript viewmp.js en la página web MHTML.
 Por ejemplo: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`
- 2 (opcional) Personalice el mensaje de error de redireccionamiento URL de Flash que se va a mandar a sus usuarios.
 Por ejemplo: `"var vmwareScriptErrorMessage=mensaje de error localizado"`
- 3 Asegúrese de insertar el comando de JavaScript viewmp.js y, de manera opcional, puede personalizar el mensaje de error de redireccionamiento URL de Flash antes de que archivo de ShockWave Flash (SWF) se importe a la página web MHTML.

Cuando un usuario muestra la página web en un escritorio remoto, el comando de JavaScript `viewmp.js` invoca el mecanismo de redireccionamiento URL de Flash en el escritorio remoto, que redirecciona el archivo SWF del escritorio al dispositivo cliente.

Configurar dispositivos cliente para Redireccionamiento URL de Flash

La función Redireccionamiento URL de Flash redirecciona el archivo SWF desde escritorios remotos a dispositivos cliente. Para permitir que estos dispositivos cliente reproduzcan vídeos de Flash desde una transmisión multidifusión o unidifusión, debe verificar que la versión adecuada de Adobe Flash Player esté instalada en los dispositivos cliente. Los clientes también deben tener conectividad IP con el origen de medios.

Nota Con Redireccionamiento URL de Flash, la transmisión multidifusión o unidifusión se redirecciona a los dispositivos cliente que puedan estar fuera del firewall de su organización. Sus clientes deben tener acceso al servidor Adobe Web que aloja el archivo 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.

Procedimiento

- ◆ Instale Adobe Flash Player en sus dispositivos cliente.

Sistema operativo	Acción
Windows	Instale Adobe Flash Player 10.1 o una versión posterior para Internet Explorer.
Linux	<p>a Instale el archivo <code>libexpat.so.0</code> o verifique que este archivo ya esté instalado.</p> <p>Asegúrese de que este archivo esté instalado en el directorio <code>/usr/lib</code> o <code>/usr/local/lib</code>.</p> <p>b Instale el archivo <code>libflashplayer.so</code> o compruebe que este archivo ya esté instalado.</p> <p>Asegúrese de que el archivo esté instalado en el directorio del complemento Flash apropiado para el sistema operativo Linux.</p> <p>c Instale el programa <code>wget</code> o compruebe que este programa ya esté instalado.</p>

Deshabilitar o habilitar Redireccionamiento URL de Flash

El Redireccionamiento URL de Flash está habilitado cuando realiza una instalación silenciosa de Horizon Agent con la propiedad `VDM_FLASH_URL_REDIRECTION=1`. Puede deshabilitar o rehabilitar la función de Redireccionamiento URL de Flash en escritorios remotos seleccionados estableciendo un valor en la clave de registro de Windows de esas máquinas virtuales.

Procedimiento

- 1 Inicie el Editor del Registro de Windows en la máquina virtual.

- 2 Vaya a la clave de registro de Windows que controla el Redireccionamiento URL de Flash.

Opción	Descripción
Windows 7 de 64 bits	HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>
Windows 7 de 32 bits	HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>

- 3 Establezca el valor para deshabilitar o habilitar el Redireccionamiento de la dirección URL de flash.

Opción	Valor
Deshabilitado	0
Habilitado	1

El valor está establecido en 1 de forma predeterminada.

Configurar el redireccionamiento de Flash

Con el Redireccionamiento Flash, si un usuario final utiliza Internet Explorer 9, 10 u 11, el contenido Flash se envía al sistema cliente, lo que reduce la carga del host ESXi. El sistema cliente reproduce el contenido multimedia en una ventana de contenedor Flash usando la versión ActiveX de Flash Player.

Aunque el nombre de esta función es similar a la función denominada Redireccionamiento URL de Flash, hay diferencias importantes, descritas en la siguiente tabla.

Tabla 2-1. Comparación de las funciones Redireccionamiento de Flash y Redireccionamiento URL Flash

Elemento de diferenciación	Redireccionamiento de Flash	Redireccionamiento URL de Flash
Tipos de Horizon Client que admiten esta función	Solo cliente de Windows	Cliente de Windows y cliente de Linux
Protocolo de visualización	VMware Blast y PCoIP.	PCoIP
Exploradores	Internet Explorer 9, 10 u 11 para el escritorio remoto	Todos los navegadores que se admiten actualmente en Horizon Client y Horizon Agent
Mecanismo de configuración	Use una opción de directiva de grupo de Horizon Agent para especificar una lista blanca o una lista negra de los sitios web que usen o no usen el Redireccionamiento Flash	Para insertar el JavaScript necesario, modifique el código fuente de la página web.

Limitaciones de funciones

La función Redireccionamiento de Flash tiene las siguientes limitaciones:

- Al hacer clic en un vínculo URL dentro de la ventana de Flash Player, se abre un explorador en el cliente en lugar de en el escritorio remoto (lado de agente).

- Algunos sitios web no funcionan con el Redireccionamiento Flash en algunas versiones de los navegadores. Por ejemplo, vimeo.com no funciona con Internet Explorer 11.
- El scripting de Flash y Java puede que no funcione de la forma prevista.
- La ventana de Horizon Client puede quedarse congelada mientras se reproduce contenido Flash, aunque se puede establecer una clave del Registro de Windows para solucionar el problema de forma alternativa.

En un cliente de 32 bits, establezca el valor de la clave HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer en "FALSE" y en un cliente de 64 bits establezca la clave HKLM\SOFTWARE Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer en "FALSE".

- YouTube ya no admite el uso de medios con tecnología Flash.
- El Redireccionamiento de Flash no funciona en redbox.com.
- El menú contextual de Flash (que se activa haciendo clic con el botón secundario) está deshabilitado.
- Si Horizon Client 4.1 se conecta a un escritorio remoto con PCoIP, se produce un error en el Redireccionamiento Flash. Horizon Client reproduce el contenido Flash en el reproductor nativo del escritorio remoto o el usuario ve una pantalla en blanco.

Requisitos del sistema para la función Redireccionamiento Flash

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

Escritorio remoto

- Debe estar instalado Horizon Agent 7.0 o una versión posterior en un escritorio virtual con la opción de configuración personalizada Redireccionamiento Flash seleccionada. De forma predeterminada, la opción de configuración personalizada Redireccionamiento Flash no está seleccionada. 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 [Instalar y configurar el redireccionamiento de Flash](#).
- Los escritorios virtuales Windows 7, Windows 8, Windows 8.1 y Windows 10 admiten el Redireccionamiento Flash.
- 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**
- Debe estar instalado Horizon Client 4.0 o una versión posterior. La opción Redireccionamiento Flash está habilitada de forma predeterminada. Consulte el tema sobre cómo instalar Horizon Client en el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*.
 - 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
- Protocolos de visualización para la sesión remota**
- PCoIP
 - VMware Blast (requiere Horizon Agent 7.0 o una versión posterior)

Instalar y configurar el redireccionamiento de Flash

Para redireccionar contenido Flash desde un escritorio remoto hasta una ventana de Flash Player en el sistema cliente local, es necesario instalar la función Redireccionamiento Flash e Internet Explorer en el escritorio remoto y en el sistema cliente, y especificar qué sitios web usan esta función.

Para habilitar esta función y especificar los sitios web que usen esta función, establezca la configuración de directiva de grupo. De forma alternativa, puede usar la configuración del Registro de Windows del escritorio remoto para establecer una lista blanca de sitios web que pueda usar para el Redireccionamiento Flash. Consulte [Usar las opciones del Registro de Windows para configurar el redireccionamiento de Flash](#).

Requisitos previos

- Instale Horizon Client en el sistema cliente y Horizon Agent en el escritorio remoto con la función Redireccionamiento Flash habilitada. Para obtener más información sobre las versiones necesarias, las opciones de configuración y todos los requisitos del sistema, consulte [Requisitos del sistema para la función Redireccionamiento Flash](#).
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC en su servidor de Active Directory.
- Agregue la plantilla ADMX de configuración de Horizon Agent (archivo `vdm_agent.admx`) a la unidad organizativa del escritorio remoto. Para obtener instrucciones de instalación, consulte [Agregar los archivos de plantilla ADMX a Active Directory](#).
- Compile una lista de sitios web que puedan (lista blanca) o no puedan (lista negra) redireccionar contenido Flash.

- Verifique que Flash ActiveX esté instalado y funcione adecuadamente. Para verificar la instalación, ejecute Internet Explorer y acceda a <https://helpx.adobe.com/flash-player.html>.

Procedimiento

- 1 Si es necesario, instale en el sistema cliente la versión ActiveX de Flash Player (en lugar de la versión NPAPI).

Flash Player está instalado de forma predeterminada en Internet Explorer 10 y 11. En cuanto a Internet Explorer 9, es posible que necesite acceder a <https://get.adobe.com/flashplayer/> para descargar e instalar Flash Player.

- 2 En el escritorio remoto, realice los siguientes pasos de instalación.

- a Instale Internet Explorer 9, 10 u 11.

- b Si es necesario, instale la versión ActiveX de Flash Player (en lugar de la versión NPAPI).

Flash Player está instalado de forma predeterminada en Internet Explorer 10 y 11. En cuanto a Internet Explorer 9, es posible que necesite acceder a <https://get.adobe.com/flashplayer/> para descargar e instalar Flash Player.

- 3 En el escritorio remoto, abra Internet Explorer y seleccione **Herramientas > Administrar complementos** en la barra de menús y verifique que **VMware View FlashMMR Server** aparezca en la lista y esté habilitado.
- 4 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y establezca la configuración de directiva del Redireccionamiento Flash en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración de VMware View Agent > VMware FlashMMR**.

Ajuste	Descripción
Habilitar el redireccionamiento multimedia flash	Especifica si el redireccionamiento de Flash (FlashMMR) está activado en el escritorio remoto (agente). Cuando está activada, esta función redirige los datos multimedia de Flash desde las URL designadas hasta el cliente a través de un canal TCP e invoca al Flash Player local del sistema cliente. Esta función reduce en gran medida la demanda de ancho de banda de CPU y de red por parte del agente.
Tamaño mínimo de rectángulo para habilitar FlashMMR	Especifica la anchura y la altura mínimas en píxeles del rectángulo en el que se reproduce el contenido de Flash. Por ejemplo, 400,300 especifica una anchura de 400 píxeles y una altura de 300 píxeles. La función Redireccionamiento Flash solo se usa si el contenido Flash es mayor o igual que los valores especificados en esta directiva. Si este GPO no está configurado, el valor que se usa de forma predeterminada es 320,200 .

- 5 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y establezca la configuración de directiva del Redireccionamiento Flash en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Configuración de VMware View Agent > VMware FlashMMR**.
 - a Para definir una lista de las URL del host que se usarán con el redireccionamiento Flash, abra la opción **Definición para uso de lista de URL de FlashMMR** y seleccione **Habilitado**.
 - b En el menú desplegable **Definición para uso de lista de URL de FlashMMR**, seleccione **Habilitar lista blanca** o **Habilitar lista negra** y haga clic en **Aceptar**.

La lista blanca está habilitada de forma predeterminada.
 - c Para agregar la lista de las URL del host que usan o no la función Redireccionamiento Flash, abra la opción **Lista de URL de hosts para habilitar FlashMMR** y seleccione **Habilitado**.
 - d Haga clic en **Mostrar** e introduzca las URL completas que compiló para la lista blanca o negra en la columna Nombre de valor.

Incluya el prefijo `http://` o `https://` en la URL. Puede usar expresiones comunes. Por ejemplo, puede especificar `https://*.google.com` y `http://www.cnn.com/*`.

De forma opcional, puede especificar `requireIECompatibility=true`, `appMode=0` o ambos en la columna Valor. Utilice una coma para separar las dos cadenas.

De forma predeterminada, la compatibilidad con la interfaz externa se habilita cuando se ejecuta el Redireccionamiento Flash lo cual puede reducir el rendimiento. En algunas situaciones, establecer `appMode=0` puede mejorar el rendimiento y proporcionar una mejor experiencia de usuario.
 - e Haga clic en **Aceptar** para guardar la lista de URL y haga clic en **Aceptar** para guardar la configuración de directiva.
- 6 En el escritorio remoto, abra un símbolo de sistema y desplácese hasta el directorio `%Program Files%\Common Files\VMware\Remote Experience`.
- 7 Para agregar la lista blanca o la lista negra a Internet Explorer, ejecute el comando `cscript mergeflashmmrwhitelist.vbs`.
- 8 Reinicie Internet Explorer.

Los sitios en los que estableció el parámetro `requireIECompatibility=true` se agregan a la vista de compatibilidad de Internet Explorer. Para comprobar que estos sitios se encuentran en la vista de compatibilidad, seleccione **Herramientas > Configuración de vista de compatibilidad**.

Los sitios se agregan también a la lista de sitios de confianza de Internet Explorer. Para comprobar los sitios de confianza, seleccione **Herramientas > Opciones de Internet** en la barra de menú de Internet Explorer y haga clic en **Sitios** y en la pestaña **Seguridad**.

Usar las opciones del Registro de Windows para configurar el redireccionamiento de Flash

Si es un usuario de dominio que no tiene privilegios de administrador en el servidor de Active Directory, puede configurar de forma alternativa el redireccionamiento de Flash estableciendo los valores apropiados de las claves del Registro de Windows en el escritorio remoto.

Puede usar este procedimiento como alternativa a usar la configuración de directiva de grupo para establecer el redireccionamiento Flash.

Requisitos previos

- Para garantizar que solo las URL especificadas en la lista puedan redireccionar contenido Flash, compile una lista blanca de sitios web. No puede usar la configuración del Registro de Windows para habilitar una lista negra. Para habilitar una lista negra, use la configuración de directiva de grupo de la función Redireccionamiento Flash.
- Compruebe que la versión 7.0 de Horizon Agent o una versión posterior, Flash Player e Internet Explorer 9, 10 u 11 estén instalados en el escritorio remoto. Consulte [Requisitos del sistema para la función Redireccionamiento Flash](#).
- Verifique que Horizon Client 4.0 o una versión posterior y la versión ActiveX de Flash Player estén instalados en el sistema cliente.

Procedimiento

- 1 Utilice Horizon Client para acceder al escritorio remoto.
- 2 Abra el editor del Registro de Windows (regedit.exe) en el escritorio remoto, acceda a la carpeta HKLM\Software\VMware, Inc.\VMware FlashMMR y establezca **FlashRedirection** a **1**.

Nota Esta opción habilita la función Redireccionamiento Flash. Esta opción está deshabilitada (establecida a 0) en HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR, la función Redireccionamiento Flash está deshabilitada en todo el dominio y requiere un administrador de dominio para habilitarla.

- 3 Acceda a la carpeta HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR.
Si esta carpeta no existe, créela.
- 4 En la carpeta VMware FlashMMR, cree una subclave denominada **UrlWhiteList**.
- 5 Haga clic con el botón secundario en la clave **UrlWhiteList**, seleccione **Nuevo > Valor de cadena** e introduzca la URL de un sitio web que use el Redireccionamiento Flash en el nombre.

Puede usar expresiones comunes. Por ejemplo, puede especificar **https://*.google.com**. Deje en blanco el valor **Datos**.

- 6 (opcional) En el campo de datos del nuevo valor de registro, agregue los datos **requireIECompatibility=true, appMode=0** o ambos.

Utilice una coma para separar las dos cadenas. De forma predeterminada, la compatibilidad con la interfaz externa se habilita cuando se ejecuta el Redireccionamiento Flash lo cual puede reducir el rendimiento. En algunas situaciones, la opción **appMode=0** puede mejorar el rendimiento y **appMode=1** puede proporcionar una experiencia de usuario mejorada.

- 7 Para agregar más URL, repita el paso anterior y cierre el editor del Registro.
- 8 En el escritorio remoto, abra un símbolo de sistema y desplácese hasta el directorio %Program Files%\Common Files\VMware\Remote Experience.
- 9 Para agregar la lista blanca a Internet Explorer, ejecute el comando `cscript mergeflashmmrwhitelist.vbs`.
- 10 Reinicie Internet Explorer.

Los sitios que tienen el parámetro **requireIECompatibility=true** se agregan a la vista de compatibilidad de Internet Explorer. Para comprobar que estos sitios se encuentran en la vista de compatibilidad, seleccione **Herramientas > Configuración de vista de compatibilidad**.

Los sitios se agregan también a la lista de sitios de confianza de Internet Explorer. Para comprobar los sitios de confianza, seleccione **Herramientas > Opciones de Internet** en la barra de menú de Internet Explorer y haga clic en **Sitios** de la pestaña **Seguridad**.

Configurar el Redireccionamiento multimedia HTML5

Con el Redireccionamiento multimedia HTML5, si un usuario final utiliza el navegador Chrome, el contenido multimedia HTML5 se envía al sistema cliente, reduciendo la carga del host ESXi. El sistema cliente reproduce el contenido multimedia y el usuario obtiene una experiencia mejorada de audio y vídeo.

Requisitos del sistema para el redireccionamiento multimedia HTML5

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

Escritorio remoto

- Los escritorios virtuales deben tener instalado Horizon Agent 7.3 o una versión posterior con la opción de configuración personalizada Redireccionamiento multimedia HTML5 seleccionada. De forma predeterminada, esta opción no está seleccionada. Consulte los temas sobre cómo instalar Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7*.
- Los hosts RDS para los escritorios virtuales deben tener instalado Horizon Agent 7.3 o una versión posterior con la opción de

configuración personalizada Redireccionamiento multimedia HTML5 seleccionada. De forma predeterminada, esta opción no está seleccionada. Consulte los temas sobre cómo instalar Horizon Agent en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

- Los ajustes de directiva de grupo Redireccionamiento multimedia HTML5 deben estar configurados en el servidor de Active Directory. Consulte [Instalar y configurar el Redireccionamiento multimedia HTML5](#).
- El navegador Chrome debe estar instalado.
- La extensión Redireccionamiento multimedia HTML5 de VMware Horizon debe estar instalada en el navegador Chrome. Consulte [Forzar la instalación de la extensión Redireccionamiento HTML5 de VMware Horizon](#).

Sistema cliente

- Debe instalarse Horizon Client 4.6 o una versión posterior con la opción de configuración personalizada Redireccionamiento multimedia HTML5 seleccionada. Esta opción está seleccionada de manera predeterminada. Consulte los temas sobre cómo instalar Horizon Client en el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*. No se admiten los sistemas cliente no sean Windows.

Protocolo de visualización para la sesión remota

- PCoIP
- VMware Blast

Instalar y configurar el Redireccionamiento multimedia HTML5

El redireccionamiento del contenido multimedia HTML5 de un escritorio remoto al sistema cliente local requiere que se lleve a cabo la instalación de la función Redireccionamiento multimedia HTML5 y el navegador Chrome en el escritorio remoto, que se habilite dicha función y que se especifiquen los sitios web que la usen.

Para habilitar el Redireccionamiento multimedia HTML5 y especificar los sitios web que usen esta función, establezca la configuración de directiva de grupo en el servidor de Active Directory. Debe compilar una lista de las URL de los sitios web que puedan redireccionar el contenido multimedia HTML5. Incluya el prefijo `http://` o `https://` en las direcciones URL. Puede utilizar patrones de coincidencia en las URL. Por ejemplo, para redireccionar todos los vídeos de YouTube, especifique `https://www.youtube.com/*`. Para redireccionar todos los vídeos de Vimeo, especifique `https://www.vimeo.com/*`. Para obtener más información, consulte https://developer.chrome.com/extensions/match_patterns.

Requisitos previos

- Instale Horizon Client en el sistema cliente y Horizon Agent en el escritorio remoto con la función Redireccionamiento multimedia HTML5 habilitada. Para obtener más información sobre las versiones necesarias, las opciones de configuración y todos los requisitos del sistema, consulte [Requisitos del sistema para el redireccionamiento multimedia HTML5](#).
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC en su servidor de Active Directory.
- Agregue el archivo de plantilla ADMX de configuración de Horizon Agent, `vdm_agent.admx`, a un GPO que esté vinculado a la OU del escritorio virtual o al host RDS del escritorio publicado. Para obtener instrucciones de instalación, consulte [Agregar los archivos de plantilla ADMX a Active Directory](#).
- Compile una lista de las URL de los sitios web que puedan redireccionar el contenido multimedia HTML5.

Procedimiento

- 1 Instale el navegador Chrome en el escritorio remoto.
- 2 En el servidor de Active Directory, abra Editor de administración de directivas de grupo y acceda a la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración de VMware View Agent > Redireccionamiento multimedia HTML5 de VMware**.
- 3 Abra la opción **Habilitar la función Redireccionamiento multimedia HTML5 de VMware**, seleccione **Habilitado** y haga clic en **Aceptar**.
- 4 Abra la opción **Habilite la lista de URL para la función Redireccionamiento multimedia HTML5 de VMware** y seleccione **Habilitado**.
- 5 Haga clic en **Mostrar** e introduzca las URL que compiló en la columna Nombre de valor.
Solo las URL que especifique pueden redireccionar contenido multimedia HTML5. De forma predeterminada, no se agrega ninguna URL. Deje la columna Valor vacía.
- 6 Haga clic en **Aceptar** para guardar la lista de URL y, a continuación, haga clic en **Aceptar** para guardar la configuración de directiva.

Pasos siguientes

Instale la extensión de redireccionamiento HTML5 de VMware Horizon en el navegador Chrome del escritorio remoto. Consulte [Forzar la instalación de la extensión Redireccionamiento HTML5 de VMware Horizon](#).

Forzar la instalación de la extensión Redireccionamiento HTML5 de VMware Horizon

Para utilizar la función Redireccionamiento multimedia HTML5, debe forzar la instalación de la extensión Redireccionamiento HTML5 de VMware Horizon en el escritorio remoto. Puede instalar la extensión estableciendo una opción de directiva de grupo de Google Chrome en el servidor de Active Directory.

Para aplicar la opción de directiva de grupo de Chrome al escritorio remoto, debe agregar el archivo de plantilla ADMX a un GPO del servidor de Active Directory. En un escritorio virtual, el GPO debe estar vinculado a la OU que contiene el escritorio virtual. En un escritorio publicado, el GPO debe estar vinculado a la OU que contiene el host RDS.

Requisitos previos

- Configurar la función Redireccionamiento multimedia HTML5. Consulte [Instalar y configurar el Redireccionamiento multimedia HTML5](#).
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC en su servidor de Active Directory.

Procedimiento

- 1 Descargue el archivo `policy_templates.zip` de https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.
- 2 Descomprima el archivo `policy_templates.zip` y copie los archivos `chrome.admx` y `chrome.adml` al servidor de Active Directory.

El archivo `chrome.admx` se encuentra en la carpeta `\windows\admx` y el archivo `chrome.adml` se encuentra en la carpeta `\windows\admx\language` en el archivo `policy_templates.zip`.

- a Copie el archivo `chrome.admx` a la carpeta `%systemroot%\PolicyDefinitions` del servidor de Active Directory.
- b Copie el archivo de recursos de idioma `chrome.adml` en la subcarpeta del idioma adecuado de `%systemroot%\PolicyDefinitions` del servidor de Active Directory.

Por ejemplo, copie la versión de `en_us` del archivo `chrome.adml` a la subcarpeta `%systemroot%\PolicyDefinitions\en_us` del servidor de Active Directory.

- 3 En el servidor de Active Directory, abra Editor de administración de directivas de grupo y acceda a la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Google Chrome > Extensiones**.
- 4 Abra la opción de directiva **Configurar la lista de las extensiones y las aplicaciones instaladas** y haga clic en **Habilitado**.
- 5 Haga clic en **Mostrar** y escriba `ljmaegmnepbgjekghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx` en la columna Valor.

- 6 Haga clic en **Aceptar** para guardar el ID de la extensión o la URL de la actualización, y haga clic en **Aceptar** para guardar la opción de directiva.
- 7 Verifique que la extensión Redireccionamiento multimedia HTML5 esté instalada en el escritorio remoto.
 - a Conéctese al escritorio remoto e inicie Chrome.
 - b Escriba **chrome://extensions** en la barra de direcciones de Chrome.

Extensión Redireccionamiento HTML5 de VMware Horizon aparece en la lista Extensiones.

Configurar audio/vídeo en tiempo real

La función de Audio/vídeo en tiempo real permite a los usuarios de Horizon 7 ejecutar en sus escritorios remotos Skype, Webex, Google Hangouts y otras aplicaciones de conferencia conectadas. Con Audio/vídeo en tiempo real, la webcam y los dispositivos de audio conectados localmente al sistema cliente se redireccionan al escritorio remoto. Esta función redirecciona los datos de audio y vídeo al escritorio con un ancho de banda significativamente inferior al que se puede alcanzar utilizando un redireccionamiento USB.

La función de Audio/vídeo en tiempo real es compatible con las aplicaciones de conferencias estándares y las aplicaciones de vídeo basadas en explorador. Además, admite entrada de audio analógica, dispositivos de audio USB y cámaras web estándar.

Esta función instala la webcam virtual de VMware y el micrófono virtual de VMware en el sistema operativo del escritorio. La webcam virtual de VMware usa un controlador de webcam de modo kernel que proporciona una mejor compatibilidad con aplicaciones de vídeo basadas en explorador y otro software de conferencia de terceros.

Cuando se inicia una aplicación de conferencia o vídeo, muestra y usa estos dispositivos virtuales de VMware, que gestionan el redireccionamiento de audio/vídeo desde los dispositivos conectados localmente en el cliente. La webcam y el micrófono virtuales de VMware aparecen en el Administrador de dispositivos del sistema operativo del escritorio.

Los controladores para los dispositivos de audio y webcam deben estar instalados en sus sistemas de Horizon Client para habilitar el redireccionamiento.

Opciones de configuración de audio/vídeo en tiempo real

Después de instalar Horizon Agent con audio/vídeo en tiempo real, la función puede utilizarse en sus escritorios de Horizon 7 sin necesidad de realizar ninguna configuración adicional. Los valores predeterminados para la velocidad de fotogramas de webcam están recomendados para la mayoría de dispositivos y aplicaciones convencionales.

Puede configurar los ajustes de directiva de grupo para cambiar estos valores predeterminados a fin de que se adapten a aplicaciones, webcams o entornos específicos. También puede establecer una directiva para deshabilitar o habilitar la función al completo. Un archivo de plantilla ADMX le permite instalar la configuración de directiva de grupo Audio/vídeo en tiempo real en Active Directory o en escritorios individuales. Consulte [Configurar los ajustes de directivas de grupo de audio/vídeo en tiempo real](#).

Si los usuarios tienen varios dispositivos de entrada de audio y webcams conectados a sus equipos cliente, puede configurar sus dispositivos de entrada de audio y webcams preferidos que se redirigirán a sus escritorios. Consulte [Seleccionar cámaras web y micrófonos preferidos](#).

Nota Puede seleccionar un dispositivo de audio preferido, pero no hay disponibles otras opciones de configuración de audio.

Cuando la entrada de audio y las imágenes de la webcam se redirigen a un escritorio remoto, no se puede acceder a los dispositivos de audio ni a la webcam del equipo local. Por otra parte, cuando estos dispositivos están en uso en el equipo local, no se puede acceder a ellos en el escritorio remoto.

Para obtener información sobre las aplicaciones compatibles, consulte el artículo de la base de conocimientos de VMware, *Directrices para usar audio/vídeo en tiempo real con aplicaciones de terceros en escritorios de Horizon View*, en <http://kb.vmware.com/kb/2053754>.

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

Para instalar la función Audio/vídeo en tiempo real, instale View Agent 6.0 o una versión posterior, o bien Horizon Agent 7.0 o una versión posterior. Para utilizar esta función con aplicaciones y escritorios publicados, debe instalar Horizon Agent 7.0.2 o una versión posterior. Consulte el documento de configuración para obtener más información sobre cómo instalar Horizon Agent.

Software de Horizon Client

Horizon Client 2.2 para Windows o una versión posterior

Horizon Client 2.2 para Linux o una versión posterior. En el caso de Horizon Client para Linux 3.1 o versiones anteriores, esta función solo está disponible en la versión de Horizon Client para Linux proporcionada por proveedores de terceros. En el caso de Horizon Client para Linux 3.2 y versiones posteriores, esta función también está disponible en la versión de cliente disponible de VMware.

Horizon Client 2.3 para Mac o una versión posterior

Horizon Client 4.0 para iOS o una versión posterior.

Horizon Client 4.0 para Android o una versión posterior.

Equipo con Horizon Client o dispositivo de acceso del cliente

- Todos los sistemas operativos con Horizon Client para Windows.
- Todos los sistemas operativos con Horizon Client para Linux en dispositivos x86. Esta función no es compatible con procesadores ARM.
- Mac OS X Mountain Lion (10.8) y versiones posteriores. Está deshabilitada en todos los sistemas operativos anteriores de Mac OS X.
- Todos los sistemas operativos con Horizon Client para iOS.
- Todos los sistemas operativos con Horizon Client para Android.
- Para obtener información sobre los sistemas operativos cliente compatibles, consulte el documento de instalación y de configuración de Horizon Client del sistema o dispositivo apropiado.
- 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 remoto en el que esté instalado el agente.

Protocolos de visualización

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

Garantizar que se usa Audio/vídeo en tiempo real en lugar de redireccionamiento USB

Audio/vídeo en tiempo real admite el redireccionamiento de entrada de audio y de vídeo para su uso en aplicaciones de conferencia. La función de redireccionamiento USB que puede instalarse con Horizon Agent no admite el redireccionamiento de cámara web. Si redirecciona dispositivos de entrada de audio a través de redireccionamiento USB, la secuencia de audio no se sincroniza correctamente con el vídeo durante las sesiones de Audio/vídeo en tiempo real y perderá la ventaja de reducir la demanda de ancho de banda de red. Puede realizar acciones para asegurarse de que los dispositivos de entrada de audio y las cámaras web se redireccionen a sus escritorios a través de Audio/vídeo en tiempo real, no a través de redireccionamiento USB.

Si sus escritorios están configurados con redireccionamiento USB, los usuarios finales pueden conectarse y visualizar sus dispositivos USB conectados de forma local si seleccionan la opción **Conectar dispositivo USB** de la barra de menús del cliente Windows o en el menú **Escritorio > USB** del cliente Mac. Los clientes de Linux bloquean el redireccionamiento USB de los dispositivos de audio y de vídeo de forma predeterminada y no proporcionan las opciones de dispositivos USB a los usuarios finales.

Si un usuario final selecciona un dispositivo USB de la lista **Conectar dispositivo USB** o **Escritorio > USB**, ese dispositivo no podrá usarse para videoconferencias ni para conferencias de audio. Por ejemplo, si un usuario hace una llamada de Skype, es posible que la imagen de vídeo no aparezca o que la secuencia de audio se deteriore. Si un usuario final selecciona un dispositivo durante una conferencia, el redireccionamiento de audio o de la webcam se interrumpe.

Para ocultar estos dispositivos de los usuarios finales y evitar interrupciones potenciales, puede configurar la directiva de grupo de redireccionamiento USB para deshabilitar la visualización de entradas de dispositivos de audio y cámaras web en VMware Horizon Client.

En concreto, puede crear reglas de filtrado de redireccionamiento USB en Horizon Agent y especificar los nombres de la familia de dispositivos audio-in y video para deshabilitarlos. Para obtener información sobre la configuración de directivas y de las reglas de filtrado para el redireccionamiento USB, consulte [Usar directivas para controlar el redireccionamiento USB](#).

Precaución Si no establece ninguna regla de filtrado de redireccionamiento USB para deshabilitar las familias de dispositivos, informe a sus usuarios finales de que no podrán seleccionar dispositivos de audio o cámaras web de la lista **Conectar dispositivo USB** o **Escritorio > USB** en la barra de menús de VMware Horizon Client.

Seleccionar cámaras web y micrófonos preferidos

Si un equipo cliente tiene más de una cámara web y un micrófono, puede establecer una cámara web preferida y un micrófono predeterminado para que la función Audio/vídeo en tiempo real los redirija al escritorio. Estos dispositivos pueden estar integrados en el equipo cliente local o estar conectados a él.

En un equipo cliente Windows que tenga instalado Horizon Client para Windows 4.2 o una versión posterior, puede seleccionar una cámara web o un micrófono preferido si configura las opciones de Audio/vídeo en tiempo real en el cuadro de diálogo Configuración de Horizon Client. Para versiones de Horizon Client anteriores, modifique la configuración del registro para seleccionar una cámara web preferida, y utilice el control de sonido del sistema operativo Windows para seleccionar un micrófono predeterminado.

En un equipo cliente Mac, puede especificar una cámara web o un micrófono preferido si usa el sistema predeterminado de Mac.

En un equipo cliente Linux, puede especificar una cámara web preferida si edita un archivo de configuración. Para seleccionar un micrófono predeterminado, puede configurar el control de sonido del sistema operativo Linux en el equipo cliente.

Audio/vídeo en tiempo real redirige la cámara web preferida si está disponible. Si no lo está, Audio/vídeo en tiempo real usa la primera cámara web proporcionada por la enumeración del sistema.

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

Con la función Audio/vídeo en tiempo real, si existen múltiples cámaras web o micrófonos conectados al sistema cliente local, solo uno de los dispositivos se usa en la aplicación o el 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.

Requisitos previos

- Compruebe que se haya instalado una cámara web USB, un micrófono USB u otro tipo de micrófono en el sistema cliente local, y que estos estén operativos.
- Compruebe que usa los protocolos de visualización VMware Blast o 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 (engranaje) **Configuración** situado en la esquina superior derecha de la pantalla de la aplicación y del escritorio, o bien 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.

Seleccionar un micrófono predeterminado en un sistema cliente Mac

Si dispone de varios micrófonos en el sistema cliente, solo se utilizará uno en el escritorio remoto. Puede utilizar Preferencias del sistema del sistema cliente para especificar el micrófono predeterminado en el escritorio remoto.

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

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

Importante Si está utilizando un micrófono USB, no lo conecte desde el menú **Conexión > USB** en Horizon Client. Si lo hace, se enrutará el dispositivo a través de un redireccionamiento USB y el dispositivo no podrá usar la función Audio/vídeo en tiempo real.

Requisitos previos

- Compruebe que se haya instalado un micrófono USB o cualquier otro tipo de micrófono en el sistema cliente y que este esté en funcionamiento.
- Compruebe que usa los protocolos de visualización VMware Blast o PCoIP del escritorio remoto.

Procedimiento

- 1 En el sistema cliente, seleccione **Menú Apple > Preferencias del sistema** y haga clic en **Sonido**.
- 2 Abra el panel Entrada en las preferencias Sonido.
- 3 Seleccione el micrófono que prefiera utilizar.

La próxima vez que se conecte a un escritorio remoto e inicie una llamada, el escritorio usará el micrófono predeterminado que seleccionó en el sistema cliente.

Configurar Audio/vídeo en tiempo real en un cliente Mac

Puede configurar la opción Audio/vídeo en tiempo real en la línea de comandos utilizando el sistema Mac predeterminado. Con el sistema predeterminado puede leer, escribir y eliminar los valores predeterminados del usuario Mac a través de Terminal (/Applications/Utilities/Terminal.app).

Los valores predeterminados de Mac pertenecen a dominios. Los dominios suelen corresponder a aplicaciones individuales. El dominio de la función Audio/vídeo en tiempo real es com.vmware.rtav.

Sintaxis para configurar Audio/vídeo en tiempo real

Puede usar el siguiente comando para configurar la función Audio/vídeo en tiempo real.

Tabla 2-2. Sintaxis de comando para la configuración Audio/vídeo en tiempo real

Comando	Descripción
<code>defaults write com.vmware.rtav srcWCamId " <i>webcam-userid</i> "</code>	Establece la cámara web preferida que se usa en los escritorios remotos. Cuando este valor no está configurado, la cámara web se selecciona automáticamente por enumeración del sistema. Puede especificar cualquier cámara web conectada al sistema cliente o compilada en él.
<code>defaults write com.vmware.rtav srcAudioInId " <i>audio-device-userid</i> "</code>	Establece el micrófono preferido (dispositivo de entrada de audio) que se usa en los escritorios remotos. Cuando este valor no está configurado, los escritorios remotos usan el dispositivo de grabado predeterminado configurado en el sistema cliente. Puede especificar cualquier micrófono conectado al sistema cliente o compilado en él.
<code>defaults write com.vmware.rtav srcWCamFrameWidth <i>pixels</i></code>	Establece el ancho de la imagen. El valor predeterminado es un valor codificado de forma rígida de 320 píxeles. Puede cambiar el ancho de la imagen a cualquier valor de píxel.
<code>defaults write com.vmware.rtav srcWCamFrameHeight <i>pixels</i></code>	Establece la altura de la imagen. El valor predeterminado es un valor codificado de forma rígida de 240 píxeles. Puede cambiar la altura de la imagen a cualquier valor de píxel.
<code>defaults write com.vmware.rtav srcWCamFrameRate <i>fps</i></code>	Establece la velocidad de fotogramas. El valor predeterminado es 15 fps. Puede cambiar la velocidad de fotogramas a cualquier valor.
<code>defaults write com.vmware.rtav LogLevel " <i>level</i> "</code>	Establece el nivel de registro para el archivo de registro Audio/vídeo en tiempo real (~/.Library/Logs/VMware/vmware-RTAV- <i>pid</i> .log). Puede configurar el nivel de registro para que rastree o depure.
<code>defaults write com.vmware.rtav IsDisabled <i>value</i></code>	Determina si Audio/vídeo en tiempo real está habilitado o deshabilitado. La función Audio/vídeo en tiempo real está habilitada de forma predeterminada. (Este valor no tiene efecto). Para deshabilitar Audio/vídeo en tiempo real en el cliente, configure el valor como True.
<code>defaults read com.vmware.rtav</code>	Muestra las opciones de configuración de la función Audio/vídeo en tiempo real.
<code>defaults delete com.vmware.rtav <i>setting</i></code>	Elimina una opción de la configuración de Audio/vídeo en tiempo real, por ejemplo: <code>defaults delete com.vmware.rtav srcWCamFrameWidth</code>

Nota Puede ajustar la velocidad de fotogramas desde 1fps hasta un máximo de 25 fps y la resolución hasta 1920 x 1080. Es posible que una alta resolución en una velocidad de fotogramas rápida no sea compatible en todos los dispositivos ni en todos los entornos.

Configurar un micrófono o una cámara web preferidos en un sistema cliente Mac

Con la función Audio/vídeo en tiempo real, si cuenta con múltiples cámaras web o micrófonos en el sistema cliente, solo se puede usar una cámara web y un micrófono en el escritorio remoto. Puede

especificar la cámara web y el micrófono que prefiera en la línea de comandos al utilizar el sistema predeterminado Mac.

Con la función Audio/vídeo en tiempo real, las cámaras web, los dispositivos de entrada de audio (y los de salida) funcionan sin ser necesario el redireccionamiento USB y la cantidad de ancho de banda de red requerida se reduce considerablemente. También se admiten los dispositivos de entrada de audio analógica.

En la mayoría de los entornos, no es necesario configurar una cámara web o un micrófono preferidos. Si no establece un micrófono preferido, los escritorios remotos usan el dispositivo de audio predeterminado configurado en la opción Preferencias del sistema en el sistema cliente. Consulte [Seleccionar un micrófono predeterminado en un sistema cliente Mac](#). Si no configura una cámara web preferida, el escritorio remoto selecciona la cámara web por enumeración.

Requisitos previos

- Si configura una cámara web USB preferida, compruebe que dicho dispositivo esté instalado y funcione en el sistema cliente.
- Si configura un micrófono USB preferido u otro tipo de micrófono, compruebe que dicho dispositivo esté instalado y funcione en el sistema cliente.
- Compruebe que usa los protocolos de visualización VMware Blast o PCoIP del escritorio remoto.

Procedimiento

- 1 En el sistema cliente Mac, inicie la aplicación de la cámara web o el micrófono para activar una enumeración de dispositivos de cámara o de audio en el archivo de registro Audio/vídeo en tiempo real.
 - a Conecte el dispositivo de audio o de cámara web.
 - b En la carpeta **Aplicaciones**, haga doble clic en **VMware Horizon Client** para iniciar Horizon Client.
 - c Inicie una llamada y luego deténgala.
- 2 Busque las entradas de registro correspondientes a la cámara web o al micrófono en el archivo de registro Audio/vídeo en tiempo real.
 - a En un editor de texto, abra el archivo de registro Audio/vídeo en tiempo real.
El archivo de registro Audio/vídeo en tiempo real recibe el nombre `~/Library/Logs/VMware/vmware-RTAV-pid.log`, donde *pid* es el ID del proceso de la sesión actual.
 - b Busque en el archivo de registro Audio/vídeo en tiempo real entradas que identifiquen las cámaras web y los micrófonos conectados.

El siguiente ejemplo muestra cómo pueden aparecer las entradas de cámara web en el archivo de registro Audio/vídeo en tiempo real:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - 1
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-in)#0xfa20000005ac8509
SystemId=0xfa20000005ac8509
```

El siguiente ejemplo muestra cómo pueden aparecer las entradas de micrófono en el archivo de registro Audio/vídeo en tiempo real:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - 2
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Microphone   UserId=Built-in
Microphone#AppleHDAEngineInput:1B,0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

- 3 Busque la cámara web o el micrófono que prefiera en el archivo de registro Audio/vídeo en tiempo real y anote su ID de usuario.

El ID de usuario aparece después de la cadena `UserId=` en el archivo de registro. Por ejemplo, el ID de usuario de la cámara interna es `FaceTime HD Camera (Built-In)` y el ID de usuario del micrófono interno es `Built-in Microphone`.

- 4 En Terminal (`/Applications/Utilities/Terminal.app`), use el comando `defaults write` para configurar la cámara web o el micrófono preferidos.

Opción	Acción
Configurar la cámara web preferida	<p>Escriba <code>defaults write com.vmware.rtav srcWCamId "webcam-userid"</code>, donde <code>webcam-userid</code> es el ID de usuario de la cámara web preferida, que se obtiene en el archivo de registro Audio/vídeo en tiempo real. Por ejemplo:</p> <pre>defaults write com.vmware.rtav srcWCamId "HD Webcam C525"</pre>
Configurar el micrófono preferido	<p>Escriba <code>defaults write com.vmware.rtav srcAudioInId "audio-device-userid"</code>, donde <code>audio-device-userid</code> es el ID de usuario del micrófono preferido, que se obtiene en el archivo de registro Audio/vídeo en tiempo real. Por ejemplo:</p> <pre>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</pre>

- 5 (opcional) Use el comando `defaults read com.vmware.rtav` para comprobar los cambios en la función Audio/vídeo en tiempo real.

Por ejemplo: `defaults read com.vmware.rtav`

El comando enumera todas las opciones de Audio/vídeo en tiempo real.

La próxima vez que se conecte a un escritorio remoto e inicie una nueva llamada, el escritorio usa la cámara web o el micrófono preferidos que configuró, si están disponibles. Si no están disponibles la cámara web o el micrófono preferidos, el escritorio remoto puede usar otra cámara web o micrófono disponibles.

Seleccionar un micrófono predeterminado en un sistema cliente Linux

Si dispone de varios micrófonos en su sistema cliente, solo se utilizará uno de ellos en el escritorio Horizon 7. Para especificar el micrófono predeterminado, puede usar el control de sonidos en el sistema cliente.

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

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

Requisitos previos

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

Procedimiento

- 1 En la interfaz gráfica de usuario de Ubuntu, seleccione **Sistema > Preferencias > Sonido**.

También puede hacer clic en el icono **Sonido** situado en la parte derecha de la barra de herramientas en la parte superior de la pantalla.

- 2 Haga clic en la pestaña **Entrada** del cuadro de diálogo Preferencias de sonido.
- 3 Seleccione el dispositivo preferido y haga clic en **Cerrar**.

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

Con la función Audio/vídeo en tiempo real, si cuenta con varias cámaras web o micrófonos en el sistema cliente, solo se puede usar una cámara web y un micrófono en el escritorio Horizon 7. Para especificar la cámara web y el micrófono preferidos, puede editar un archivo de configuración.

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

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

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

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

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

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

Requisitos previos

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

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

Procedimiento

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

Este proceso crea un archivo de registro.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configurar los ajustes de directivas de grupo de audio/vídeo en tiempo real

Puede configurar los ajustes de directiva de grupo que controlan el comportamiento del audio/vídeo en tiempo real (Real-Time Audio-Video, RTAV) en escritorios de Horizon 7. Estas opciones determinan la velocidad de fotogramas y la resolución de imagen máxima de la webcam. Las opciones le permiten administrar el ancho de banda máximo que puede consumir cualquier usuario. Una opción adicional deshabilita o habilita la función RTAV.

No tiene que configurar estos ajustes de directivas. La función RTAV funciona con la velocidad de fotogramas y la resolución de imagen establecidas para la webcam en los sistemas cliente. Las opciones predeterminadas se recomiendan para la mayoría de aplicaciones de audio y webcam.

Si desea ver ejemplos de uso del ancho de banda durante el audio/vídeo en tiempo real, consulte [Ancho de banda de Audio/vídeo en tiempo real](#).

Estos ajustes de directiva afectan a sus escritorios de Horizon 7, no a los sistemas cliente a los que se conectan los dispositivos físicos. Para configurar estas opciones en los escritorios, agregue a Active Directory el archivo de plantilla administrativa (ADMX) de directivas de grupo de RTAV.

Para obtener información sobre cómo configurar los ajustes en sistemas cliente, consulte el artículo de la base de conocimientos de VMware *Configurar la velocidad de fotogramas y la resolución para la función Audio/vídeo en tiempo real en Horizon View Clients*, disponible en <http://kb.vmware.com/kb/2053644>.

Agregar la plantilla ADMX de RTAV en Active Directory y configurar los ajustes

Puede agregar la configuración de directiva del archivo ADMX de RTAV (`vdm_agent_rtav.admx`) a objetos de directiva de grupo (Group Policy Objects, GPO) en Active Directory y configurar los ajustes en el Editor de objetos de directiva de grupo.

Requisitos previos

- Compruebe que esté instalada la opción de configuración RTAV en los escritorios de las máquinas virtuales y en los hosts RDS. Esta opción de configuración está instalada de forma predeterminada, pero se puede anular su selección durante la instalación. La configuración no tendrá efecto si no se ha instalado RTAV. Consulte el documento de configuración para obtener más información sobre cómo instalar Horizon Agent.
- Compruebe que los GPO de Active Directory se creen para los ajustes de directiva de grupo de RTAV. Los GPO deben estar vinculados a la OU que contiene los hosts RDS o los escritorios de las máquinas virtuales. Consulte [Ejemplo de directiva de grupo de Active Directory](#).
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC de Microsoft en su servidor de Active Directory.
- Familiarícese con los ajustes de directiva de grupo de RTAV. Consulte [Configuración de la directiva de grupo Audio/vídeo en tiempo real](#).

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, donde `x.x.x` es la versión y `yyyyyy` es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware–Horizon–Extras–Bundle–x.x.x-yyyyyy.zip y copie los archivos ADMX al servidor de Active Directory.
 - a Copie el archivo vdm_agent_rtav.admx y la carpeta en-US a la carpeta C:\Windows\PolicyDefinitions del servidor de Active Directory.
 - b (opcional) Copie el archivo de recursos de idioma (vdm_agent_rtav.adml) a la subcarpeta adecuada en C:\Windows\PolicyDefinitions\ del servidor de Active Directory.
- 3 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y escriba la ruta de acceso al archivo de plantilla en el editor.

La configuración se encuentra en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración de VMware View Agent > Configuración de RTAV de View.**

Pasos siguientes

Configure los ajustes de directiva de grupo.

Configuración de la directiva de grupo Audio/vídeo en tiempo real

La configuración de la directiva de grupo Audio/vídeo en tiempo real (RTAV) controla la resolución máxima de la imagen y la velocidad de fotogramas máxima de la cámara web virtual. Una opción adicional le permite habilitar o deshabilitar la función RTAV. Esta configuración afecta a los escritorios remotos, no a los sistemas cliente donde están conectados los dispositivos físicos.

Si no configura las opciones de la directiva de grupo RTAV, esta usará los valores que estén establecidos en los sistemas cliente. En los sistemas cliente, la velocidad de fotogramas predeterminada de la cámara web es de 15 fotogramas por segundo. La resolución predeterminada de la imagen de la cámara web es de 320 x 240 píxeles.

La configuración de directiva de grupo sobre resolución determina los valores máximos que se pueden utilizar. Los valores de velocidad de fotogramas y de resolución establecidos en los sistemas cliente son valores absolutos. Por ejemplo, si configura las opciones de RTAV para que la resolución máxima de la imagen sea de 640 x 480 píxeles, la cámara web mostrará cualquier resolución que se establezca en el cliente hasta 640 x 480 píxeles. Si establece la resolución de la imagen en el cliente en un valor superior a 640 x 480 píxeles, la resolución del cliente se limitará a 640 x 480 píxeles.

No todas las configuraciones pueden alcanzar las opciones máximas de directiva de grupo de 1920 x 1080 píxeles a 25 fotogramas por segundo. La velocidad máxima de fotogramas que puede alcanzar su configuración a una resolución concreta depende de la cámara web que se use, el hardware del sistema cliente, el hardware virtual de Horizon Agent y el ancho de banda disponible.

La configuración de directiva de grupo sobre resolución determina los valores predeterminados que se usan cuando el usuario no establece los valores de resolución.

Configuración de directiva de grupo	Descripción
Disable RTAV	<p>Cuando habilita esta opción, se deshabilita Audio/vídeo en tiempo real.</p> <p>Cuando esta opción no está configurada o está deshabilitada, se habilita Audio/vídeo en tiempo real.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de audio/vídeo en tiempo real de View del Editor de administración de directivas de grupo.</p>
Max frames per second	<p>Determina la velocidad máxima por segundo a la que la cámara web captura fotogramas. Puede usar esta opción para limitar la velocidad de fotogramas de la cámara web en entornos de red con poco ancho de banda.</p> <p>El valor mínimo es de un fotograma por segundo. El valor máximo es de 25 fotogramas por segundo.</p> <p>Cuando esta opción no está configurada o está deshabilitada, la velocidad máxima de fotogramas no está establecida. La función Audio/vídeo en tiempo real usa la velocidad de fotogramas que se seleccionó para la cámara web en el sistema cliente.</p> <p>De forma predeterminada, las cámaras web cliente tienen una velocidad de 15 fotogramas por segundo. Si no hay ninguna opción configurada en el sistema cliente y la opción Fotogramas máximos por segundo no está configurada o está deshabilitada, la cámara web capturará 15 fotogramas por segundo.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de audio/vídeo en tiempo real de View > Opciones de cámara web de RTAV de View en el Editor de administración de directivas de grupo.</p>
Resolution – Max image width in pixels	<p>Determina la anchura máxima en píxeles de los fotogramas de las imágenes que captura la cámara web. Al establecer un valor bajo para la anchura máxima de imagen, puede disminuir la resolución de los fotogramas capturados, lo que puede mejorar la experiencia de imagen en entornos de red con poco ancho de banda.</p> <p>Cuando esta opción no está configurada o está deshabilitada, la anchura máxima de la imagen no está establecida. RTAV usa la anchura de imagen que está establecida en el sistema cliente. La anchura predeterminada de una imagen de cámara web en un sistema cliente es de 320 píxeles.</p> <p>El límite máximo para cualquier imagen de cámara web es 1920 x 1080. Si configura esta opción con un valor superior a 1920 píxeles, la anchura real de la imagen será de 1920 píxeles.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de audio/vídeo en tiempo real de View > Opciones de cámara web de RTAV de View en el Editor de administración de directivas de grupo.</p>
Resolution – Max image height in pixels	<p>Determina la altura máxima en píxeles de los fotogramas de las imágenes que captura la cámara web. Al establecer un valor bajo para la altura máxima de imagen, puede disminuir la resolución de los fotogramas capturados, lo que puede mejorar la experiencia de imagen en entornos de red con poco ancho de banda.</p> <p>Cuando esta opción no está configurada o está deshabilitada, la altura máxima de la imagen no está establecida. RTAV usa la altura de imagen que está establecida en el sistema cliente. La altura predeterminada de una imagen de cámara web en un sistema cliente es de 240 píxeles.</p> <p>El límite máximo para cualquier imagen de cámara web es 1920 x 1080. Si configura esta opción con un valor superior a 1080 píxeles, la altura real de la imagen será de 1080 píxeles.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de audio/vídeo en tiempo real de View > Opciones de cámara web de RTAV de View en el Editor de administración de directivas de grupo.</p>

Configuración de directiva de grupo	Descripción
Resolution – Default image resolution width in pixels	<p>Determina la anchura predeterminada en píxeles de la resolución de los fotogramas de las imágenes que captura la cámara web. Esta opción se usa cuando el usuario no definió ningún valor para la resolución.</p> <p>Cuando esta opción no está configurada o está deshabilitada, la anchura predeterminada de la imagen es de 320 píxeles.</p> <p>El valor que se configure en esta opción de directiva se aplica solo si se usa View Agent 6.0 o versiones posteriores y Horizon Client 3.0 o versiones posteriores. Esta opción de directiva no tiene efecto en versiones anteriores de View Agent y de Horizon Client, donde la anchura predeterminada de la imagen es de 320 píxeles.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de audio/vídeo en tiempo real de View > Opciones de cámara web de RTAV de View en el Editor de administración de directivas de grupo.</p>
Resolution – Default image resolution height in pixels	<p>Determina la altura predeterminada en píxeles de la resolución de los fotogramas de las imágenes que captura la cámara web. Esta opción se usa cuando el usuario no definió ningún valor para la resolución.</p> <p>Cuando esta opción no está configurada o está deshabilitada, la altura predeterminada de la imagen es de 240 píxeles.</p> <p>El valor que se configure en esta opción de directiva se aplica solo si se usa View Agent 6.0 o versiones posteriores y Horizon Client 3.0 o versiones posteriores. Esta opción de directiva no tiene efecto en versiones anteriores de View Agent y de Horizon Client, donde la altura predeterminada de la imagen es de 240 píxeles.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de audio/vídeo en tiempo real de View > Opciones de cámara web de RTAV de View en el Editor de administración de directivas de grupo.</p>

Ancho de banda de Audio/vídeo en tiempo real

El ancho de banda de Audio/vídeo en tiempo real varía en función de la velocidad de fotogramas y la resolución de la imagen de la cámara web y de los datos de audio y de imagen que se estén capturando.

Los ejemplos de pruebas que se muestran en [Tabla 2-3. Resultados de las pruebas de ancho de banda al mandar datos de audio/vídeo en tiempo real desde Horizon Client hasta Horizon Agent](#) miden el ancho de banda que usa Audio/vídeo en tiempo real en un entorno de View con unos dispositivos de entrada de audio y cámara web estándares. Las pruebas miden el ancho de banda necesario para enviar datos tanto de vídeo como de audio desde Horizon Client hasta Horizon Agent. El ancho de banda total necesario para ejecutar una sesión de escritorio desde Horizon Client puede ser mayor que los valores mostrados. En estas pruebas, la cámara web captura imágenes a 15 fotogramas por segundo para cada resolución de imagen.

Tabla 2-3. Resultados de las pruebas de ancho de banda al mandar datos de audio/vídeo en tiempo real desde Horizon Client hasta Horizon Agent

Resolución de imagen (ancho x alto)	Ancho de banda usado (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

Configurar el redireccionamiento del escáner

Mediante el uso del redireccionamiento del escáner, los usuarios de Horizon 7 pueden digitalizar la información de sus aplicaciones y escritorios remotos con dispositivos de digitalización e imagen conectados localmente a sus equipos locales. El redireccionamiento del escáner está disponible en Horizon 6.0.2 y versiones posteriores.

El redireccionamiento del escáner es compatible con los dispositivos de digitalización e imagen convencionales compatibles con los formatos TWAIN y WIA.

Después de instalar Horizon Agent con la opción de configuración Redireccionamiento del escáner, la función estará operativa en sus aplicaciones y escritorios remotos sin necesidad de realizar ninguna configuración adicional. No tiene que configurar controladores específicos del escáner en aplicaciones o escritorios remotos.

Puede configurar los ajustes de directiva de grupo para cambiar los valores predeterminados a fin de que se adapten a entornos o aplicaciones de digitalización e imagen específicos. También puede establecer una directiva para deshabilitar o habilitar la función por completo. Con un archivo de plantilla ADMX, puede instalar la configuración de directiva de grupo de redireccionamiento del escáner en Active Directory o escritorios individuales. Consulte [Configurar los ajustes de directivas de grupo de redireccionamiento del escáner](#).

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

Requisitos del sistema para la función de redireccionamiento del escáner

Para admitir el redireccionamiento del escáner, la implementación de Horizon 7 debe cumplir ciertos requisitos de software y hardware.

Aplicación o escritorio remotos de Horizon 7

Esta función se admite en escritorios RDS, aplicaciones RDS y escritorios RDS que se implementan en máquinas virtuales de usuario único.

Debe instalar View Agent 6.0.2 o una versión posterior y seleccionar la opción Redireccionamiento de escáner en la máquina virtual principal o de plantilla, o bien en 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.

Se admiten los siguientes sistemas operativos invitados en máquinas virtuales de usuario único y, si se especifica, en hosts RDS:

- Windows 7 de 64 o 32 bits
- Windows 8 de 64 o 32 bits.x

- Windows 10 de 64 o 32 bits
- Windows Server 2008 R2 configurado como un escritorio o un host RDS
- Windows Server 2012 R2 configurado como un escritorio o un host RDS

Importante La función Experiencia de escritorio se debe instalar en los sistemas operativos invitados Windows Server, ya estén configurados como escritorios o como hosts RDS.

No es necesario que los controladores del escáner estén instalados en el sistema operativo del escritorio en el que Horizon Agent está instalado.

Software de Horizon Client

Horizon Client 3.2 para Windows o una versión posterior

Equipo con Horizon Client o dispositivo de acceso del cliente

Sistemas operativos compatibles:

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

Los controladores del escáner deben estar instalados y este dispositivo debe estar operativo en el equipo cliente.

Estándar del escáner

TWAIN o WIA

Protocolo de visualización para Horizon 7


PCoIP

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

Operación del usuario de Redireccionamiento de escáner

Con Redireccionamiento de escáner, los usuarios pueden trabajar con dispositivos de imagen y con escáneres físicos que estén conectados a los equipos cliente como dispositivos virtuales que realicen operaciones de escaneado en las aplicaciones y los escritorios remotos.

Los usuarios pueden trabajar con los escáneres virtuales de forma similar a la que usan los escáneres en los equipos cliente conectados de forma local.

- Después de que se instale la opción Redireccionamiento de escáner con Horizon Agent, se agrega al escritorio un icono de bandeja de la herramienta de escáner (). En aplicaciones RDS, el icono de la bandeja de la herramienta se redireccionará al equipo cliente local.

No es necesario que utilice el icono de bandeja de la herramienta de escáner. El Redireccionamiento de escáner funciona sin que tenga que establecer ninguna configuración. Puede usar el icono para configurar opciones, como cambiar el dispositivo que desea usar si existe más de un dispositivo conectado al equipo cliente.

- Cuando hace clic en el icono del escáner, aparece el menú Redireccionamiento de escáner de VMware Horizon. No aparece ningún escáner en la lista del menú si los que están conectados al equipo cliente no son compatibles.
- De forma predeterminada, los escáneres están seleccionados de forma automática. Los escáneres TWAIN y WIA se seleccionan por separado. Puede tener un escáner TWAIN y otro WIA seleccionados al mismo tiempo.
- Si están configurados varios escáneres conectados de forma local, puede seleccionar un escáner diferente al que está seleccionado de forma predeterminada.
- Los escáneres WIA aparecen en el menú Administrador de dispositivos del escritorio remoto, en **Dispositivos de imagen**. El escáner WIA se denomina **VMware Virtual WIA Scanner**.
- En el menú Redireccionamiento de escáner de VMware Horizon, puede hacer clic en **Preferencias** y seleccionar opciones, por ejemplo para ocultar cámaras web del menú de redireccionamiento de escáner y para determinar cómo seleccionar el escáner predeterminado.

También puede controlar esas funciones si establece la configuración de la directiva de grupo del redireccionamiento de escáner en Active Directory. Consulte [Configuración de la directiva de grupo de redireccionamiento del escáner](#).

- Cuando trabaja con un escáner TWAIN, el menú Redireccionamiento de escáner TWAIN para VMware Horizon proporciona opciones adicionales para seleccionar regiones de una imagen, escanear en color, en blanco y negro o en la escala de grises, así como seleccionar otras funciones comunes.
- Para mostrar la ventana de la interfaz de usuario de TWAIN para el software del escáner TWAIN que no aparece de forma predeterminada, puede seleccionar la opción **Mostrar siempre el diálogo de las opciones del escáner** del cuadro de diálogo Preferencias del Redireccionamiento de escáner de VMware Horizon.

Tenga en cuenta que la mayor parte del software para escáneres TWAIN muestra la ventana de la interfaz de usuario TWAIN de forma predeterminada. Para este software, la ventana siempre aparece, aunque seleccione o desmarque la opción **Mostrar siempre el diálogo de las opciones del escáner**.

Nota Si ejecuta dos aplicaciones RDS que están alojadas en diferentes granjas, en el equipo cliente aparecen dos iconos de bandeja de la herramienta de redireccionamiento del escáner. Solo suele estar conectado un escáner a un equipo cliente. En este caso, ambos iconos hacen referencia al mismo dispositivo y no es relevante cuál de los dos seleccione. En algunas situaciones, es posible que tenga dos escáneres conectados de forma local y dos aplicaciones RDS que se ejecuten en granjas diferentes. En ese caso, debe abrir cada icono para ver el menú de redireccionamiento de escáner que controla cada aplicación RDS.

Para obtener instrucciones de usuario final para los escáneres redireccionados en funcionamiento, consulte el documento *Usar VMware Horizon Client para Windows*.

Configurar los ajustes de directivas de grupo de redireccionamiento del escáner

Puede configurar los ajustes de directivas de grupo que controlan el comportamiento del redireccionamiento del escáner en sus escritorios y aplicaciones de Horizon 7. Con estos ajustes de directivas, puede controlar desde Active Directory, de manera centralizada, las opciones disponibles en el cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon en las aplicaciones y los escritorios de usuarios.

No tiene que configurar estos ajustes de directivas. El redireccionamiento del escáner funciona con los ajustes predeterminados configurados para dispositivos de digitalización en sistemas cliente y escritorios remotos.

Estos ajustes de directivas afectan a sus escritorios y aplicaciones remotos, no a los sistemas cliente a los que se conectan los escáneres físicos. Para configurar estas opciones en los escritorios y las aplicaciones, agregue a Active Directory el archivo de plantilla administrativa (ADMX) de directivas de grupo de redireccionamiento del escáner.

Agregar las plantillas ADMX de redireccionamiento de escáner en Active Directory

Puede agregar la configuración de directiva del archivo de plantilla ADMX de redireccionamiento del escáner (`vdm_agent_scanner.admx`) a objetos de directiva de grupo (Group Policy Objects, GPO) en Active Directory y configurar los ajustes en el Editor de objetos de directiva de grupo.

Requisitos previos

- Compruebe que esté instalada la opción de configuración Redireccionamiento de escáner en los escritorios de las máquinas virtuales o en los hosts RDS. Los ajustes de directiva de grupo no tienen efecto si no se ha instalado el redireccionamiento del escáner. Consulte el documento de configuración para obtener más información sobre cómo instalar Horizon Agent.
- Compruebe que los GPO de Active Directory se creen para los ajustes de directiva de grupo de redireccionamiento del escáner. Los GPO deben estar vinculados a la OU que contiene los hosts RDS o los escritorios virtuales. Consulte [Ejemplo de directiva de grupo de Active Directory](#).
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC en su servidor de Active Directory.
- Familiarícese con los ajustes de directiva de grupo de redireccionamiento del escáner. Consulte [Configuración de la directiva de grupo de redireccionamiento del escáner](#).

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip, donde x.x.x es la versión y yyyyyyy es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip y copie los archivos ADMX al servidor de Active Directory.
 - a Copie el archivo vdm_agent_scanner.admx y la carpeta en-US a la carpeta C:\Windows\PolicyDefinitions del servidor de Active Directory.
 - b (opcional) Copie el archivo de recursos de idioma (vdm_agent_scanner.adml) a la subcarpeta adecuada en C:\Windows\PolicyDefinitions\ del servidor de Active Directory.
- 3 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y escriba la ruta de acceso al archivo de plantilla en el editor.

La configuración se encuentra en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración de VMware View Agent > Redireccionamiento de escáner**.

La mayoría de las configuraciones también se agregan a la carpeta **Configuración de usuario**, ubicada en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Configuración de VMware View Agent > Redireccionamiento de escáner**.

Pasos siguientes

Configure los ajustes de directiva de grupo.

Configuración de la directiva de grupo de redireccionamiento del escáner

La configuración de directiva de grupo de redireccionamiento del escáner controla las opciones disponibles en el cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon en las aplicaciones y los escritorios de usuarios.

Los archivos de plantilla ADMX de redireccionamiento del escáner contienen tanto las directivas de Configuración del equipo como las de Configuración de usuario. Las directivas de Configuración de usuario le permiten establecer diferentes configuraciones para usuarios de escritorios VDI, de escritorios RDS y de aplicaciones RDS. Se pueden aplicar distintas directivas de Configuración de usuario aunque las sesiones de escritorio y las aplicaciones de los usuarios se ejecuten en los mismos hosts RDS. Todas las opciones se encuentran en la carpeta **Configuración de VMware Horizon Agent > Redireccionamiento de escáner** del Editor de administración de directivas de grupo.

Configuración de directiva de grupo			
Directiva de grupo	Equipo	Usuario	Descripción
Disable functionality	X		<p>Deshabilita la función de redireccionamiento del escáner.</p> <p>Cuando habilite esta opción, los escáneres no podrán redireccionarse y no aparecerán en el menú de escáner de las aplicaciones y de los escritorios de los usuarios.</p> <p>Cuando deshabilite o no configure esta opción, el redireccionamiento de escáner funcionará y los escáneres aparecerán en el menú de escáner.</p>
Lock config	X		<p>Bloquea la interfaz de usuario de redireccionamiento del escáner y evita que los usuarios cambien las opciones de configuración de sus escritorios y aplicaciones.</p> <p>Cuando habilite esta opción, los usuarios no podrán configurar las opciones que están disponibles desde el menú de la bandeja de sus escritorios y sus aplicaciones. Los usuarios pueden mostrar el cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon, pero las opciones estarán inactivas y no se podrán cambiar.</p> <p>Cuando deshabilita esta función o no la configura, los usuarios pueden configurar las opciones del cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p>
Compression		X	<p>Establece el índice de compresión de imágenes durante la transferencia de imágenes a la aplicación o al escritorio remoto.</p> <p>Puede elegir los siguientes modos de compresión:</p> <ul style="list-style-type: none"> ■ Deshabilitar. La compresión de imágenes está deshabilitada. ■ Sin pérdida. Se usa la compresión sin pérdida de calidad de la imagen (zlib). ■ JPEG. Se usa la compresión con pérdida de calidad de la imagen JPEG. Especifique el nivel de calidad de la imagen en el campo Calidad de compresión JPEG. La calidad de compresión JPEG debe ser un valor entre 0 y 100. <p>Cuando habilite esta opción, se establecerá el modo de compresión seleccionado para todos los usuarios afectados por esta directiva. Sin embargo, los usuarios pueden cambiar la opción Compresión en el cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon y anular la opción de la directiva.</p> <p>Si deshabilita o no configura esta opción de directiva, se usa el modo de compresión JPEG.</p>

Configuración de directiva de grupo	Equipo	Usuario	Descripción
Hide Webcam	X	X	<p>Evita que las cámaras web aparezcan en el menú de selección de escáneres del cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p> <p>De forma predeterminada, las cámaras web pueden redirigirse a escritorios y a aplicaciones. Los usuarios pueden seleccionar cámaras web y usarlas como escáneres virtuales para capturar imágenes.</p> <p>Cuando habilite esta opción como directiva de Configuración del equipo, se ocultarán las cámaras web de todos los usuarios de los equipos afectados. Los usuarios no podrán cambiar la opción Ocultar cámaras web del cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p> <p>Cuando habilite esta opción como directiva de Configuración de usuario, se ocultarán las cámaras web de todos los usuarios afectados. Sin embargo, los usuarios sí podrán cambiar la opción Ocultar cámaras web del cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p> <p>Cuando habilite esta opción como directiva de Configuración del equipo y como directiva de Configuración de usuario, la opción Ocultar cámaras web de la Configuración del equipo anulará la opción correspondiente de la directiva Configuración de usuario para todos los usuarios de los equipos afectados.</p> <p>Cuando deshabilite esta opción o no la configure en ninguna de las directivas, la opción Ocultar cámaras web la definirá la opción de directiva correspondiente (Configuración de usuario o Configuración del equipo) o la seleccionará el usuario en el cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p>
Default Scanner	X	X	<p>Proporciona una gestión centralizada de la selección automática de escáneres.</p> <p>Seleccione las opciones de selección automática de escáneres de forma independiente para los escáneres TWAIN y los escáneres WIA. Puede elegir las siguientes opciones de selección automáticas:</p> <ul style="list-style-type: none"> ■ Ninguna. No selecciona escáneres de forma automática. ■ Selección automática Selecciona el escáner conectado localmente de forma automática. ■ Último usado Selecciona el último escáner usado de forma automática. ■ Especificado Selecciona el escáner cuyo nombre introduzca en el cuadro de texto Escáner especificado. <p>Cuando habilite esta opción como directiva de Configuración del equipo, se determinará el modo de selección automática de escáneres para todos los usuarios de los equipos afectados. Los usuarios no podrán cambiar la opción Escáner predeterminado del cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p> <p>Cuando habilite esta opción como directiva de Configuración de usuario, se determinará el modo de selección automática de escáneres para todos los usuarios afectados. Sin embargo, los usuarios sí podrán cambiar la opción Escáner predeterminado del cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p> <p>Cuando habilite esta opción como directiva de Configuración del equipo y como directiva de Configuración de usuario, el modo de selección automática de escáneres de la Configuración del equipo anulará la opción correspondiente de la directiva Configuración de usuario para todos los usuarios de los equipos afectados.</p> <p>Cuando deshabilite esta opción o no la configure en ninguna de las directivas, el modo de selección automática de escáneres lo definirá la opción de directiva correspondiente (Configuración de usuario o Configuración del equipo) o lo seleccionará el usuario en el cuadro de diálogo Preferencias de redireccionamiento del escáner de VMware Horizon.</p>

Configurar el redireccionamiento del puerto serie

Con el redireccionamiento del puerto serie, los usuarios pueden redirigir los puertos serie conectados localmente (COM), como es el caso de los puertos RS232 integrados o los adaptadores de puerto USB a puerto serie. Los dispositivos, como impresoras, lectores de códigos de barra y otros dispositivos serie, se pueden conectar a estos puertos y se pueden usar en los escritorios remotos.

El redireccionamiento de puerto serie está disponible en Horizon 6 versión 6.1.1 y versiones posteriores con Horizon Client para Windows 3.4 y versiones posteriores.

Después de instalar Horizon Agent y configurar la función de redireccionamiento del puerto serie, la función estará operativa en sus escritorios remotos sin necesidad de realizar ninguna configuración adicional. Por ejemplo, COM1 en el sistema de cliente local se redirige como COM1 en el escritorio remoto y COM2 se redirige como COM2, salvo que ya exista un puerto COM en el escritorio remoto. De ser así, se asigna el puerto COM 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. No tiene que configurar los puertos COM ni instalar controladores de dispositivos en los escritorios remotos.

Para dejar activo un puerto COM redirigido, un usuario debe seleccionar la opción **Conectar** del menú en el icono de la bandeja de herramientas del puerto serie durante una sesión de escritorio. El usuario también puede establecer un dispositivo de puerto COM para que se conecte automáticamente cuando el usuario inicie sesión en el escritorio remoto. Consulte [Operación del usuario de redireccionamiento de puerto serie](#).

Puede configurar los ajustes de directivas de grupo para cambiar la configuración predeterminada. Por ejemplo, puede bloquear los ajustes para que los usuarios no puedan cambiar las propiedades o asignaciones de puertos COM. También puede establecer una directiva para deshabilitar o habilitar la función por completo. Con un archivo de plantilla ADMX, puede instalar la configuración de directivas de grupo de redireccionamiento de puertos serie en Active Directory o en escritorios individuales. Consulte [Configurar los ajustes de directivas de grupo de redireccionamiento de puertos serie](#).

Cuando un puerto COM redirigido esté abierto y en uso en un escritorio remoto, no se puede acceder al puerto en el equipo local. Recíprocamente, cuando un puerto COM está en uso en el equipo local, no se puede acceder al puerto en el escritorio remoto.

Requisitos del sistema para el redireccionamiento del puerto serie

Con esta función, los usuarios finales 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.

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.

Operación del usuario de redireccionamiento de puerto serie

Los usuarios pueden trabajar con dispositivos de puerto COM físicos que están conectados a los equipos cliente y pueden usar una virtualización del puerto serie para conectar los dispositivos a los escritorios remotos, donde las aplicaciones de terceros pueden acceder a los dispositivos.

- Después de que se instale la opción Redireccionamiento de puerto serie con Horizon Agent, se agrega al escritorio un icono de bandeja de la herramienta de puerto serie (). En las aplicaciones publicadas, el icono se redirecciona al equipo cliente local.

Este icono solo aparece si usa las versiones requeridas de Horizon Agent y Horizon Client para Windows y se conecta a través de PCoIP. El icono no aparece si está conectado a un escritorio remoto desde un cliente móvil, Linux o Mac.

Puede usar el icono para configurar las opciones de conexión a los puertos COM asignados, así como para desconectarse de ellos o personalizarlos.

- Cuando haga clic en el icono del puerto serie, aparece el menú **Redireccionamiento COM serie para VMware Horizon**.
- De forma predeterminada, los puertos COM conectados de forma local están asignados a los puertos COM correspondientes en el escritorio remoto. Por ejemplo: **COM1 asignado a COM3**. De forma predeterminada, los puertos asignados no están conectados.
- Para usar un puerto COM asignado, debe seleccionar de forma manual la opción **Conectar** en el menú **Redireccionamiento COM serie para VMware Horizon** o con la opción **Conectarse automáticamente**, que se estableció durante una sesión de escritorio previa, o bien configurando una opción de la directiva de grupo. **Conectarse automáticamente** configura un puerto asignado al que conectarse automáticamente cuando se inicia una sesión de escritorio remoto.
- Cuando selecciona la opción **Conectarse**, el puerto redireccionado está activo. En el Administrador de dispositivos del sistema operativo invitado del escritorio remoto, el puerto redireccionado aparece como **Redireccionamiento de puerto serie para VMware Horizon (COMn)**.

Cuando el puerto COM está conectado, puede abrir el puerto en una aplicación de terceros, que puede intercambiar datos con el dispositivo del puerto COM que está conectado en la máquina cliente. Mientras un puerto está abierto en una aplicación, no puede desconectar el puerto del menú **Redireccionamiento COM serie para VMware Horizon**.

Antes de poder desconectar el puerto COM, debe cerrar dicho puerto en la aplicación o cerrar la propia aplicación. Puede seleccionar la opción **Desconectar** para desconectar el puerto y hacer que el puerto COM físico esté disponible para su uso en la máquina cliente.

- En el menú **Redireccionamiento COM serie para VMware Horizon**, puede hacer clic con el botón secundario en un puerto redireccionado para seleccionar el comando **Propiedades de puerto**.

En el cuadro de diálogo de propiedades de COM, puede configurar un puerto al que conectarse automáticamente cuando se inicie una sesión de escritorio remoto, ignorar la señal Conjunto de datos preparado (DSR), habilitar el puerto para que sea permanente y asignar el puerto local del cliente a otro puerto COM en el escritorio remoto si selecciona un puerto de la lista desplegable **Nombre de puerto personalizado**.

Es posible que aparezca un puerto de escritorio remoto superpuesto. Por ejemplo, es posible que aparezca **COM1 (superpuesto)**. En este caso, la máquina virtual está configurada con un puerto COM en el hardware virtual del host ESXi. Puede usar un puerto redireccionado aunque esté asignado a un puerto superpuesto en la máquina virtual. La máquina virtual recibe datos de serie a través del puerto desde el host ESXi o desde el sistema cliente.

- En el Administrador de dispositivos del sistema operativo invitado, puede usar la pestaña **Propiedades > Configuración de puerto** para configurar las opciones de un puerto COM redireccionado. Por ejemplo, puede establecer la velocidad en baudios y los bits de datos. Sin embargo, las opciones que configura en el Administrador de dispositivos se ignoran si la aplicación especifica las opciones del puerto.

Para obtener instrucciones de usuario final para los puertos COM serie redirigidos en funcionamiento, consulte el documento *Usar VMware Horizon Client para Windows*.

Directrices para configurar el redireccionamiento del puerto serie

A través de la configuración de las directivas de grupo, puede configurar el redireccionamiento del puerto serie y controlar la medida en la que los usuarios pueden personalizar los puertos COM redireccionados. Su elección dependerá de las funciones que tengan los usuarios y de las aplicaciones de terceros de las que dispongan en su organización.

Para obtener más información sobre la configuración de la directiva de grupo, consulte [Configuración de la directiva de grupo de redireccionamiento de puertos serie](#).

- Si sus usuarios ejecutan las mismas aplicaciones de terceros y dispositivos de puerto COM, asegúrese de que los puertos redireccionados se configuren del mismo modo. Por ejemplo, en un banco o en una tienda que usen dispositivos de punto de venta, asegúrese de que todos los dispositivos de puerto COM estén conectados a los mismos puertos en el endpoint cliente y que todos los puertos estén asignados a los mismos puertos COM redireccionados en los escritorios remotos.

Ajuste la configuración de la directiva **ConfiguraciónDePuerto** para asignar puertos cliente a los puertos redireccionados. Seleccione el elemento **ConexiónAutomática** en **ConfiguraciónDePuerto** para asegurarse de que los puertos redireccionados estén conectados al inicio de cada sesión de escritorio. Habilite la configuración de la directiva **Bloqueo de configuración** para evitar que los usuarios cambien la asignación de los puertos o personalicen la configuración de los puertos. En este escenario, los usuarios nunca tendrán que conectarse o desconectarse manualmente y se evitará que, accidentalmente, hagan que un puerto COM redireccionado sea inaccesible a una aplicación de terceros.

- Si sus usuarios son trabajadores del conocimiento que usan gran variedad de aplicaciones de terceros y posiblemente, también usen los puertos COM de forma local en sus máquinas cliente, asegúrese de que puedan conectarse a los puertos COM redireccionados y desconectarse de los mismos.

Es posible que tenga que ajustar la configuración de la directiva **ConfiguraciónDePuerto** si las asignaciones predeterminadas de los puertos son incorrectas. Puede configurar o no el elemento **ConexiónAutomática**, en función de los requisitos de sus usuarios. No habilite la configuración de la directiva **Bloqueo de configuración**.

- Asegúrese de que las aplicaciones de terceros abran el puerto COM que está asignado al escritorio remoto.
- Asegúrese de que la velocidad en baudios que esté usando el dispositivo coincida con la velocidad en baudios que esté intentando usar la aplicación de terceros.
- Puede redireccionar hasta cinco puertos COM desde un sistema cliente hasta un escritorio remoto.

Configurar los ajustes de directivas de grupo de redireccionamiento de puertos serie

Puede configurar los ajustes de directivas de grupo que controlan el comportamiento del redireccionamiento de puertos serie en los escritorios remotos. Con estos ajustes de directivas, puede

controlar de manera centralizada y desde Active Directory las opciones disponibles en el menú **Redireccionamiento COM serie para VMware Horizon** en los escritorios de usuarios.

No tiene que configurar estos ajustes de directivas. El redireccionamiento de puerto serie funciona con los ajustes predeterminados configurados para puertos COM redireccionados en sistemas cliente y escritorios remotos.

Estos ajustes de directivas afectan a sus escritorios remotos, no a los sistemas cliente a los que se conectan los dispositivos de puerto COM físicos. Para configurar estas opciones en los escritorios, agregue a Active Directory el archivo de plantilla administrativa (ADMX) de directivas de grupo de redireccionamiento de puertos serie.

Agregar la plantilla ADMX de redireccionamiento de puerto serie en Active Directory

Puede agregar la configuración de directiva del archivo ADMX de COM serie (redireccionamiento de puerto serie) (`vdm_agent_serialport.admx`) a los objetos de directiva de grupo (Group Policy Object, GPO) en Active Directory y configurar los ajustes en el Editor de objetos de directiva de grupo.

Requisitos previos

- Compruebe que esté instalada en sus escritorios la opción de configuración de redireccionamiento de puerto serie. Los ajustes de directiva de grupo no tienen efecto si no se ha instalado el redireccionamiento de puerto serie. Consulte el documento de configuración para obtener más información sobre cómo instalar Horizon Agent.
- Compruebe que los GPO de Active Directory se creen para los ajustes de directiva de grupo de redireccionamiento de puerto serie. Los GPO deben estar vinculados a la OU que contiene sus escritorios. Consulte [Ejemplo de directiva de grupo de Active Directory](#).
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC en su servidor de Active Directory.
- Familiarícese con los ajustes de directiva de grupo de redireccionamiento de puerto serie. Consulte [Configuración de la directiva de grupo de redireccionamiento de puertos serie](#).

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, donde `x.x.x` es la versión y `yyyyyy` es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip y copie los archivos ADMX al servidor de Active Directory.
 - a Copie el archivo vdm_agent_serialport.admx y la carpeta en-US a la carpeta C:\Windows\PolicyDefinitions del servidor de Active Directory.
 - b (opcional) Copie el archivo de recursos de idioma (vdm_agent_serialport.adml) a la subcarpeta adecuada en C:\Windows\PolicyDefinitions\ del servidor de Active Directory.
- 3 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y escriba la ruta de acceso al archivo de plantilla en el editor.

La configuración se encuentra en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración de VMware View Agent > COM serie**.

La mayoría de las configuraciones también se agregan a la carpeta **Configuración de usuario**, ubicada en **Configuración de usuario > Directivas > Plantillas administrativas > Configuración de VMware View Agent > COM serie**.

Pasos siguientes

Configure los ajustes de directiva de grupo.

Configuración de la directiva de grupo de redireccionamiento de puertos serie

La configuración de la directiva de grupo de redireccionamiento de puertos serie controla la configuración del puerto COM redireccionado, incluidas las opciones que están disponibles en el menú

Redireccionamiento COM serie para VMware Horizon de los escritorios remotos.

El archivo ADMX de redireccionamiento de puerto serie contiene tanto las directivas de Configuración del equipo, como las de Configuración de usuario. Las directivas de Configuración de usuario le permiten establecer diferentes configuraciones para usuarios de escritorios VDI especificados. Las opciones de directiva que se establecen en la Configuración del equipo tienen preferencia sobre las opciones que se establecen en la Configuración de usuario.

**Configuración de
directiva de
grupo**
Equipo**Usuario****Descripción**

PortSettings1

X

X

PortSettings2

PortSettings3

PortSettings4

PortSettings5

La configuración del puerto determina la asignación entre el puerto COM del sistema cliente y el puerto COM redireccionado del escritorio remoto, así como otras opciones que afectan al puerto COM redireccionado. Configure de forma individual cada puerto COM redireccionado.

Están disponibles cinco configuraciones de directivas para la configuración del puerto, lo que permite que asigne hasta cinco puertos COM del cliente al escritorio remoto. Seleccione una configuración de directiva para cada puerto COM que quiera configurar. Cuando habilite la configuración de directiva para la configuración del puerto, podrá configurar los siguientes elementos que afectan al puerto COM redireccionado:

- La opción **Número de puerto origen** especifica el número de puertos COM físicos que se conectan al sistema cliente.
- La opción **Número de puerto de destino virtual** especifica el número de puertos COM virtuales redireccionados al escritorio remoto.
- La opción **Conexión automática** conecta automáticamente el puerto COM al puerto COM redireccionado al inicio de cada sesión de escritorio.
- Con la opción **IgnoreDSR**, el puerto COM redireccionado ignora la señal del Conjunto de datos preparado (DSR).
- La opción **Pausa antes de cerrar puerto (en milisegundos)** especifica el tiempo (en milisegundos) que tarda un puerto redireccionado en cerrarse después de que un usuario lo cierre. Algunos adaptadores de USB a puerto serie necesitan este tiempo para asegurar que los datos transmitidos se conservaran. Esta opción sirve para solucionar problemas.
- La opción **Serial2USBModeChangeEnabled** resuelve problemas de los adaptadores de USB a puerto serie que usan el conjunto de chips de Prolific, incluido el adaptador GPS GlobalSat BU353. Si no habilita esta opción para los adaptadores de conjunto de chips Prolific, los dispositivos conectados pueden transmitir datos pero no recibirlos.
- La opción **Deshabilitar errores en máscara de espera** deshabilita el valor de error en la máscara del puerto COM. Esta opción de solución de problemas es necesaria para algunas aplicaciones. Si desea obtener más información, consulte la documentación de Microsoft sobre la función WaitCommEvent en [http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx).
- La opción **HandleBtDisappears** admite el comportamiento de los puertos COM Bluetooth. Esta opción sirve para solucionar problemas.
- La opción **UsbToComTroubleShooting** resuelve algunos problemas de los adaptadores de USB a puerto serie. Esta opción sirve para solucionar problemas.
- La opción **Permanente** mantiene el estado del puerto COM redireccionado en la sesión remota, aunque el cliente se desconecte.

Cuando habilite la configuración de directiva para la configuración de un puerto COM concreto, los usuarios podrán conectar y desconectar el puerto redireccionado, pero no podrán configurar propiedades del puerto en el escritorio remoto. Por ejemplo, los usuarios no pueden establecer que el puerto se redireccione automáticamente cuando inician sesión en el escritorio y no pueden ignorar la señal DSR. La opción de directiva de grupo controla estas propiedades.

Nota Los puertos COM redireccionados solo estarán conectados y activos si el puerto COM físico se conecta de forma local al sistema cliente. Si asigna un puerto COM que no existe en el cliente, el puerto redireccionado aparecerá como inactivo y no estará disponible en el menú de la bandeja de la herramienta en el escritorio remoto.

**Configuración de
directiva de
grupo**
Equipo**Usuario****Descripción**

			<p>Cuando la configuración de directiva para la configuración del puerto está deshabilitada o no se estableció, el puerto COM redireccionado usa las opciones que los usuarios configuran en el escritorio remoto. Las opciones del menú Redireccionamiento COM serie para VMware Horizon están activas y disponibles para los usuarios.</p> <p>Estas configuraciones se encuentran en la carpeta Configuración de VMware View Agent > COM serie > PortSettings del Editor de administración de directivas de grupo.</p>
Local settings priority	X	X	<p>Da prioridad a las opciones configuradas en el escritorio remoto.</p> <p>Cuando habilite esta directiva, las opciones de redireccionamiento de puerto serie que configure un usuario en el escritorio remoto tendrán preferencia sobre las opciones de la directiva de grupo. Las opciones de directiva de grupo solo se aplican si alguna opción no está configurada en el escritorio remoto.</p> <p>Cuando la opción está deshabilitada o no está configurada, las opciones de directiva de grupo tienen preferencia sobre las opciones configuradas en el escritorio remoto.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > COM serie del Editor de administración de directivas de grupo.</p>
Disable functionality	X		<p>Deshabilita la función de redireccionamiento de puerto serie.</p> <p>Cuando habilite esta opción, los puertos no se redireccionarán al escritorio remoto. El icono de bandeja de la herramienta de puerto serie del escritorio remoto no se muestra.</p> <p>Cuando esta opción está deshabilitada, el redireccionamiento de puerto serie funciona, el icono de bandeja de la herramienta de puerto serie se muestra y los puertos COM aparecen en el menú Redireccionamiento COM serie para VMware Horizon.</p> <p>Cuando esta opción no está configurada, las opciones que sean locales del escritorio remoto determinan si el redireccionamiento de puerto serie está deshabilitado o habilitado.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > COM serie del Editor de administración de directivas de grupo.</p>
Lock configuration	X	X	<p>Bloquea la interfaz de usuario de redireccionamiento del puerto serie y evita que los usuarios cambien las opciones de configuración del escritorio remoto.</p> <p>Cuando habilite esta opción, los usuarios no podrán configurar las opciones disponibles en el menú de la bandeja de la herramienta en sus escritorios. Los usuarios pueden mostrar el menú Redireccionamiento COM serie para VMware Horizon, pero las opciones están inactivas y no se pueden cambiar.</p> <p>Cuando esta opción está deshabilitada, los usuarios pueden configurar las opciones en el menú Redireccionamiento COM serie para VMware Horizon.</p> <p>Cuando esta opción no está configurada, las opciones de programa locales del escritorio remoto determinan si los usuarios pueden configurar las opciones de redireccionamiento del puerto COM.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > COM serie del Editor de administración de directivas de grupo.</p>

Configuración de directiva de grupo

Equipo	Usuario	Descripción
Bandwidth limit	X	<p>Establece un límite para la velocidad de transferencia de datos, en kilobytes por segundo, entre el puerto serie redireccionado y los sistemas cliente.</p> <p>Cuando habilite esta opción, podrá establecer un valor en el cuadro Límite de ancho de banda (en kilobytes por segundo) que determine la velocidad máxima de transferencia de datos entre el puerto serie redireccionado y el cliente. El valor 0 deshabilita el límite de ancho de banda.</p> <p>Cuando esta opción está deshabilitada, no hay ningún límite de ancho de banda establecido.</p> <p>Cuando esta opción no está configurada, las opciones de programa locales del escritorio remoto determinan si establecer un límite de ancho de banda.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > COM serie del Editor de administración de directivas de grupo.</p>

Configurar adaptadores de USB a serie

Puede configurar adaptadores de USB a serie que utilicen un conjunto de chips Prolific para que sean redirigidos a escritorios remotos mediante la función de redireccionamiento de puertos serie.

Para asegurarse de que los datos se transmitan adecuadamente en adaptadores del conjunto de chips Prolific, puede habilitar un ajuste de directivas de grupo de redireccionamiento de puertos serie en Active Directory o una máquina virtual de escritorio individual.

Si no configura el ajuste de directiva de grupo para resolver problemas de adaptadores de conjunto de chips Prolific, los dispositivos conectados pueden transmitir datos pero no recibirlos.

No tiene que configurar un ajuste de directiva ni clave de registro en los sistemas cliente.

Requisitos previos

- Compruebe que esté instalada en sus escritorios la opción de configuración de redireccionamiento de puerto serie. Los ajustes de directiva de grupo no tienen efecto si no se ha instalado el redireccionamiento de puerto serie. Consulte el documento de configuración para obtener más información sobre cómo instalar Horizon Agent.
- Verifique que se agregó el archivo de plantilla ADMX de redireccionamiento de puertos serie en Active Directory o en la máquina virtual de escritorio.
- Familiarícese con el elemento **Serial2USBModeChangeEnabled** en el ajuste de directiva de grupo **PortSettings**. Consulte [Configuración de la directiva de grupo de redireccionamiento de puertos serie](#).

Procedimiento

- 1 En Active Directory o en la máquina virtual, abra el Editor de objetos de directiva de grupo.
- 2 Vaya a la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Plantillas administrativas clásicas > Configuración de VMware View Agent > COM serie**.
- 3 Seleccione la carpeta **PortSettings**.

- 4 Seleccione y habilite un ajuste de la directiva de grupo **PortSettings**.
- 5 Especifique los números de los puertos COM de origen y destino para asignar el puerto COM.
- 6 Seleccione la casilla **Serial2USBModeChangeEnabled**.
- 7 Configure otros elementos del ajuste de directiva **PortSettings** en la medida que sea necesario.
- 8 Haga clic en **Aceptar** y cierre el Editor de objetos de directiva de grupo.

Los adaptadores de USB a serie se pueden redirigir a escritorios remotos y pueden recibir datos correctamente cuando los usuarios inicien sus próximas sesiones de escritorio.

Administrar el acceso al Redireccionamiento multimedia (MMR) de Windows Media

Horizon 7 incluye la función MMR de Windows Media para escritorios VDI que se ejecutan en máquinas de usuario único y en escritorios RDS.

MMR distribuye la transmisión multimedia directamente a los equipos cliente. Con MMR, la transmisión multimedia se procesa, es decir, se descodifica, en el sistema cliente. El sistema cliente reproduce el contenido multimedia, por lo que se descarga la demanda en el host ESXi.

Los datos MMR se envían a través de la red sin ningún cifrado basado en aplicación y pueden contener información confidencial, dependiendo del contenido que se redirecciona. Para asegurarse de que esta información no se supervise en la red, use MMR únicamente en una red segura.

Si el túnel seguro está habilitado, las conexiones MMR entre los clientes y la puerta de enlace de seguridad de View son seguras, pero las conexiones de la puerta de enlace de seguridad de View a los equipos de escritorios no están cifradas. Si el túnel seguro está deshabilitado, las conexiones MMR de los clientes a los equipos de escritorios no están cifradas.

Habilitar redireccionamiento multimedia en Horizon 7

Puede realizar acciones para asegurarse de que solo pueden acceder al redireccionamiento multimedia los sistemas Horizon Client que tienen suficientes recursos para gestionar descodificaciones multimedia locales y que están conectadas a Horizon 7 en una red segura.

De forma predeterminada, la directiva global de View Administrator, **Redireccionamiento multimedia (MMR)** está configurada como **Denegar**.

Para usar el redireccionamiento multimedia, debe configurar explícitamente este valor como **Permitir**.

Para controlar el acceso al redireccionamiento multimedia, puede habilitar o deshabilitar la directiva **Redireccionamiento multimedia (MMR)** de forma global, para grupos de escritorios individuales o para usuarios específicos.

Si necesita obtener instrucciones para establecer directivas globales en Horizon Administrator, consulte [Directivas de Horizon 7](#).

Requisitos del sistema para MMR de Windows Media

Para admitir el redireccionamiento de contenido multimedia (MMR) de Windows Media, la implementación de Horizon 7 debe cumplir ciertos requisitos de software y hardware. MMR de Windows Media se incluye en Horizon 6.0.2 y versiones posteriores.

Escritorio remoto de Horizon 7

- Esta función es compatible con escritorios de máquinas virtuales que se implementan en máquinas virtuales de un solo usuario y en escritorios RDS.

Para admitir esta función en escritorios de RDS, es necesario tener View Agent 6.1.1 o posterior.

Para admitir esta función en máquinas de un solo usuario, es necesario tener View Agent 6.0.2 o posterior.

- Son compatibles los siguientes sistemas operativos invitados:
 - Windows 10 de 32 o 64 bits. Windows Media Player es compatible. El reproductor de películas y TV predeterminado no es compatible.
 - Windows Server 2016 es una función de Tech Preview. Windows Media Player es compatible. El reproductor de películas y TV predeterminado no es compatible.
 - Windows 7 SP1 Enterprise o Ultimate de 64 o 32 bits (máquina de un solo usuario). Windows 7 Professional no es compatible.
 - Windows 8/8.1 Professional o Enterprise de 64 o 32 bits (máquina de un solo usuario)
 - Windows Server 2008 R2 configurado como host RDS
 - Windows Server 2012 y 2012 R2 configurado como host RDS
- El **procesamiento 3D** se puede habilitar o deshabilitar en el grupo de escritorios.
- El usuario debe reproducir los vídeos en Windows Media Player 12 o posterior o en Internet Explorer 8 o posterior.

Para utilizar Internet Explorer, deberá deshabilitar el modo protegido. En el cuadro de diálogo Opciones de Internet, haga clic en la pestaña **Seguridad** y anule la selección de la opción para **habilitar el modo protegido**.

Software de Horizon Client

Se necesita Horizon Client 3.2 para Windows o una versión posterior para compatibilidad con MMR de Windows Media en máquinas de un solo usuario.

Equipo con Horizon Client o dispositivo de acceso del cliente

- El cliente debe ejecutar sistemas operativos con Windows 7, Windows 8/8.1 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.

Directivas de Horizon

En Horizon Administrator, establezca la directiva **Redireccionamiento multimedia (MMR)** como **Permitir**. El valor predeterminado es **Denegar**.

Firewall back-end

Si la implementación de Horizon 7 incluye un firewall back-end entre los servidores de seguridad basados en DMZ y la red interna, verifique que el firewall back-end permita el tráfico al puerto 9427 en los escritorios.

Determinar si usar Redireccionamiento multimedia (MMR) de Windows Media según la latencia de red

MMR de Windows Media se adapta de forma predeterminada a las condiciones de red en escritorios de usuario único que se ejecuten en Windows 8 o posterior y en escritorios RDS que se ejecuten en Windows Server 2012 o 2012 R2 o posteriores. Si la latencia de red entre Horizon Client y el escritorio remoto es de 29 milisegundos o menor, el vídeo se redirecciona con MMR de Windows Media. Si la latencia de red es de 30 milisegundos o mayor, el vídeo no se redirecciona. En lugar de hacerlo, se generará en el host ESXi y se enviará al cliente a través de PCoIP.

Esta función se aplica a escritorios de usuario único de Windows 8 o posteriores, o a escritorios RDS de Windows Server 2012, 2012 R2 o posteriores. Los usuarios pueden ejecutar cualquier sistema cliente compatible, Windows 7 o Windows 8/8.1.

Esta función no se aplica a los escritorios de usuario único de Windows 7 o a los escritorios RDS de Windows Server 2008 R2. En estos sistemas operativos invitados, MMR de Windows Media siempre realiza redirecciones multimedia, independientemente de la latencia de red.

Puede anular esta función, forzando a que MMR de Windows Media siempre realice redirecciones multimedia independientemente de la latencia de red estableciendo la configuración del registro `RedirectionPolicy` en el escritorio.

Procedimiento

- 1 Inicie el Editor del Registro de Windows en el escritorio remoto.

2 Vaya a la clave de registro de Windows que controla las directivas de redireccionamiento.

La clave de registro que configure para un escritorio remoto dependerá de los bits de la versión del Reproductor de Windows Media.

Opción	Descripción
Reproductor de Windows Media de 64 bits	■ Para un escritorio de 64 bits, use la clave de registro: HKEY_LOCAL_MACHINE \Software\VMware, Inc.\VMware tsmmr
Reproductor de Windows Media de 32 bits	■ Para un escritorio de 32 bits, use la clave de registro: HKEY_LOCAL_MACHINE \Software\VMware, Inc.\VMware tsmmr ■ Para un escritorio de 64 bits, use la clave de registro: HKEY_LOCAL_MACHINE \Software\Wow6432Node\VMware, Inc.\VMware tsmmr

3 Establezca el valor RedirectionPolicy en always.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

4 Reinicie el Reproductor de Windows Media en el escritorio para permitir que el valor actualizado se aplique.

Administrar el acceso al redireccionamiento de unidades cliente

Cuando implementa Horizon Client y Horizon Agent con el redireccionamiento de unidades cliente, se cifran los archivos y las carpetas para enviarlos por la red.

Las conexiones de redireccionamiento de unidades cliente entre clientes y la puerta de enlace segura de View y las conexiones desde la puerta de enlace segura de View a las máquinas de escritorios son seguras. Si VMware Blast está habilitado, los archivos y las carpetas se cifran para enviarlos por un canal virtual.

Las conexiones TCP en el puerto 9427 son necesarias para admitir el redireccionamiento de la unidad cliente. Si la implementación de Horizon 7 incluye un firewall back-end entre los servidores de seguridad basados en DMZ y la red interna, el firewall back-end debe permitir el tráfico al puerto 9427 en los escritorios remotos. Si se habilita VMware Blast, no es necesario que el puerto TCP 9427 esté abierto porque el redireccionamiento de unidades cliente envía los datos a través del canal virtual.

La opción de configuración **Redireccionamiento de unidades cliente** personalizada en el instalador de Horizon Agent está seleccionada de forma predeterminada. Como práctica recomendada, habilite la opción de configuración **Redireccionamiento de unidades cliente** personalizada solo en escritorios remotos donde los usuarios necesiten esta función.

Con versiones de Horizon Client anteriores a la versión 3.5 o versiones de Horizon Agent anteriores a la versión 6.2, las carpetas y los archivos del redireccionamiento de unidades cliente se envían sin cifrar a través de la red y pueden tener datos confidenciales, según el contenido que se redirecciona. Si el túnel de seguridad está habilitado, las conexiones de redireccionamiento de unidades cliente entre Horizon

Client y la puerta de enlace de seguridad de View son seguras, pero las conexiones de la puerta de enlace de seguridad de View a los equipos de escritorios no están cifradas. Si el túnel de seguridad está deshabilitado, las conexiones de redireccionamiento de unidades cliente desde Horizon Client a las máquinas de escritorio no están cifradas. Para asegurarse de que estos datos no se supervisen en la red, use el redireccionamiento de unidades cliente solo en una red segura con versiones anteriores del agente y del cliente.

Usar la directiva de grupo para deshabilitar el redireccionamiento de la unidad cliente

Puede deshabilitar el redireccionamiento de unidades cliente configurando una opción de directiva de grupo para los escritorios remotos en el servidor de Active Directory.

La opción de directiva de grupo sobrescribe el registro local y la configuración de Directivas de Smart que habilita la función del redireccionamiento de unidades cliente.

Requisitos previos

- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC en su servidor de Active Directory.
- Agregue el archivo de plantilla ADMX de Servicios de Escritorio remoto `vmware_rds_server.admx` a un GPO que esté vinculado a la OU de los escritorios virtuales o al host RDS de los escritorios publicados. Para obtener instrucciones de instalación, consulte [Agregar los archivos de plantilla ADMX a Active Directory](#).

Procedimiento

- 1 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y acceda a **Configuración del equipo\Directivas\Plantillas administrativas\Componentes de Windows\Servicios de Escritorio remoto\Host de sesión de Escritorio remoto\Redirección de dispositivo o recurso**.
- 2 Abra la opción de directiva de grupo **No permitir redirección de unidad**, seleccione **Habilitado** y haga clic en **Aceptar**.

Usar las opciones del registro para configurar el redireccionamiento de la unidad cliente

Puede usar las opciones de la clave del Registro de Windows para controlar el comportamiento del redireccionamiento de la unidad cliente en un escritorio remoto. Esta función requiere Horizon Agent 7.0 y Horizon Client 4.0 o versiones posteriores.

Las opciones del Registro de Windows que controla el redireccionamiento de la unidad cliente en un escritorio remoto se encuentra en la siguiente ruta:

```
HKLM\Software\VMware, Inc.\VMware TSDR
```


Puede usar el Editor del Registro de Windows en el escritorio remoto para editar la configuración del registro local.

Nota Las directivas del redireccionamiento de la unidad cliente que se establecen con Directivas de Smart tienen prioridad sobre la configuración del registro local.

Deshabilitar el redireccionamiento de unidades cliente

Para deshabilitar el redireccionamiento de unidades cliente, cree un nuevo valor de cadena denominado `disabled` y establezca su valor en `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

El valor predeterminado es `false` (habilitado).

No permitir el acceso de escritura a las carpetas compartidas

Si no desea permitir el acceso de lectura a todas las carpetas que se comparten con el escritorio remoto, cree un nuevo valor de cadena denominado `permissions` y establezca su valor a cualquier cadena que empiece por `r`, excepto las que empiecen por `rw`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

El valor predeterminado es `rw` (todas las carpetas compartidas se pueden leer y escribir).

Compartir carpetas específicas

Para compartir carpetas específicas con el escritorio remoto, cree una nueva clave denominada `default shares` y cree una nueva subclave para cada carpeta que desee compartir con el escritorio remoto. En cada subclave, cree un nuevo valor de cadena denominado `name` y establezca su valor a la ruta de la carpeta que desee compartir. El siguiente ejemplo comparte las carpetas `C:\ebooks` y `C:\spreadsheets`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Si establece `name` en `*all`, todas las unidades cliente se comparten con el escritorio remoto. La opción `*all` solo es compatible con los sistemas cliente Windows.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

Para que el cliente no comparta carpetas adicionales (es decir, carpetas que no especifica la clave `default shares`), cree un valor de cadena denominado `ForcedByAdmin` y establezca su valor en `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

Si el valor es `true`, el cuadro de diálogo Compartir no aparece cuando los usuarios se conectan al escritorio remoto en Horizon Client. El valor predeterminado es `false` (los clientes pueden compartir carpetas adicionales).

El siguiente ejemplo comparte las carpetas C:\ebooks y C:\spreadsheets, hace que ambas sean de solo lectura y no permite que el cliente comparta carpetas adicionales.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Nota No use la función ForcedByAdmin como una función de seguridad o para controlar los elementos que se comparten. Un usuario puede anular la opción ForcedByAdmin=true si crea un vínculo a un recurso compartido existente que se dirija a carpetas que no están especificadas en la clave default shares.

Usar el redireccionamiento de unidades cliente en una implementación de Unified Access Gateway

Si la implementación de Horizon 7 usa un dispositivo Unified Access Gateway en lugar de un servidor de seguridad, los usuarios utilizan el redireccionamiento de unidades cliente con el protocolo de visualización PCoIP, y los equipos de Horizon Client y Horizon Agent están en diferentes redes, el Servidor del túnel UDP debe estar habilitado para el dispositivo Unified Access Gateway.

Para habilitar el Servidor del túnel UDP, en la IU de administración de Unified Access Gateway, establezca la opción **Servidor del túnel UDP habilitado** en **Sí**.

Si no habilita el Servidor del túnel UDP, los usuarios no podrán usar la función de redireccionamiento de unidades cliente con el protocolo de visualización PCoIP. El redireccionamiento de unidades cliente funciona con el protocolo de visualización VMware Blast, independientemente de si el Servidor del túnel UDP está habilitado.

Para obtener más información, consulte la documentación de Unified Access Gateway.

Configurar Skype Empresarial

Puede realizar llamadas de voz o videollamadas con una buena calidad si cuenta con Skype Empresarial en un escritorio virtual. Esto no afectará de forma negativa la infraestructura virtual ni sobrecargará la red.

Todos los procesos multimedia tienen lugar en el equipo cliente, en lugar de en el escritorio virtual, cuando se realizan las llamadas de voz o videollamadas de Skype.

VMware Horizon Virtualization Pack para Skype Empresarial

Para usar Skype Empresarial, debe contar con VMware Horizon Virtualization Pack para Skype Empresarial en la máquina cliente.

Puede configurar los ajustes de directivas de grupo para cambiar la configuración predeterminada. Consulte [Configuración de directiva de VMware Virtualization Pack para Skype Empresarial](#).

El administrador de Horizon debe instalar VMware Horizon Virtualization Pack para Skype Empresarial en el escritorio virtual durante la instalación de Horizon Agent. Para instalar Horizon Client para Windows, consulte el documento *Usar VMware Horizon Client para Windows*.

VMware Horizon Virtualization Pack para Skype Empresarial tiene estos módulos de software:

- Proxy de medios de Horizon instalado en el escritorio virtual.
- Proveedor de medios de Horizon instalado en el endpoint cliente

Funciones de Skype Empresarial

Skype Empresarial ofrece las siguientes funciones:

- Llamadas E911
- Responder y estacionar una llamada
- Conectarse a reuniones externas de forma anónima
- Redireccionar llamadas a dispositivos móviles
- Estadísticas de llamada
- Autenticación con tarjeta inteligente
- Llamadas de audio de punto a punto
- Videollamadas de punto a punto
- Llamadas PTSN mediante el teclado de marcado
- Transferir, reenviar, silenciar, poner en espera y reanudar una llamada
- Comandos HID
- Llamadas a PTSN con un servidor de mediación
- Conectividad remota y llamadas mediante servidores perimetrales
- Música en espera
- Tonos personalizados
- Integración de correo de voz
- Teléfonos USB
- Soporte de aplicaciones publicadas
- Corrección de errores de reenvío (Forward Error Correction, FEC) con audio y vídeo
- Conferencias con audio o vídeo entre varias entidades
- Opción Reunirse ahora
- Creación de pizarras y uso compartido de pantallas

Requisitos del sistema

Esta función es compatible con estas configuraciones.

Tabla 2-4. Requisitos del sistema para Skype Empresarial

Sistema	Requisitos
Servidor de Microsoft	Lync Server 2013, Skype Empresarial 2015, Office365
Cliente Microsoft	VMware recomienda enfáticamente el uso de la actualización más reciente del cliente Skype Empresarial 2015 (15.0.4933.100 o una versión posterior). Skype Empresarial 2016 como parte de Office 365 Plus: 16.0.7571.2072 o posteriores Skype Empresarial 2016 como parte de Office 2016: 16.0.4561.1000 o posteriores
Sistemas operativos de escritorios virtuales	<ul style="list-style-type: none"> ■ Windows 7 SP1 ■ Windows 8.1 ■ Escritorios con Windows 10 persistentes y no persistentes ■ Escritorios con Windows 2008 R2 SP1 ■ Escritorios con Windows 2012 R2 ■ Escritorios con Windows 2008 R2 SP1 RDSH ■ Escritorios con Windows 2012 R2 RDSH ■ Soporte de aplicaciones publicadas
Sistemas operativos de máquinas cliente	<ul style="list-style-type: none"> ■ Windows 7 SP1 ■ Windows 8.1 ■ Windows 10 ■ WES7 ■ Windows 10 IoT ■ Ubuntu 14.04 32 bits ■ Ubuntu 14.04 64 bits ■ Ubuntu 16.04 64 bits ■ RHEL 6.9 32 bits ■ RHEL 6.9 64 bits ■ RHEL 7.3 64 bits ■ CentOS 6.x 32 bits ■ CentOS 6.x 64 bits ■ SLED 12 SP2 64 bits
Implementaciones	Solo VDI (en las instalaciones y la nube), escritorios persistentes y no persistentes
Protocolos de visualización	VMware Blast y PCoIP
Puertos de red	Los mismos puertos que los que utiliza el cliente nativo Skype Empresarial. Consulte los puertos cliente en https://technet.microsoft.com/en-us/library/gg398833.aspx
Cámaras web y micrófonos	Los mismos dispositivos que funcionan con Skype Empresarial. Puede consultar las cámaras web en https://technet.microsoft.com/en-us/office/dn947482.aspx

Sistema	Requisitos
Códecs de audio y vídeo	Los mismos que los códecs de audio y de vídeo que utiliza el cliente nativo Skype Empresarial. Consulte https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&MSPPErr=-2147217396
Media Feature Pack	Debe estar instalado en el escritorio remoto para las versiones N y KN de Windows 10. Puede instalar Media Feature desde https://www.microsoft.com/en-us/download/details.aspx?id=48231

Limitaciones

Skype Empresarial tiene las siguientes limitaciones:

- IPv6 no es compatible. Solo se admiten implementaciones IPv4.
- No admiten las funciones de respuesta a llamadas grupales ni de llamadas a través de X (casa, trabajo, etc.)
- En estos momentos no se admite la vista de galería.
- No se puede grabar las llamadas.
- No se admiten los escenarios de dos saltos, como Horizon Agent anidado con Horizon Client.
- No es posible usar Lync o Skype Empresarial en la máquina cliente al mismo tiempo que el cliente Skype Empresarial optimizado en el escritorio remoto.
- No hay soporte para la interfaz de usuario del cliente de Lync 2013 cuando se conecta un cliente Skype 2015 a un servidor Lync 2013. Un administrador puede configurar la interfaz de usuario cliente de Skype en el servidor: <https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx>
- En la ventana de vista previa del vídeo, si desea obtener una vista previa de una cámara diferente a la que aparece, seleccione el dispositivo, cierre el diálogo y vuelva a abrirlo.
- Si está conectado a una red privada en el momento en el que instala Skype Empresarial en el escritorio remoto, el instalador agrega reglas entrantes y salientes en el firewall que se aplican a dicho perfil de red. Si inicia sesión en un escritorio remoto desde una red de dominios y utiliza Skype Empresarial, aparecerá una excepción de firewall. Si desea solucionar el problema, agregue excepciones de firewall para el cliente Skype Empresarial de forma manual en las reglas del firewall para todos los perfiles de red.
- La opción de control de volumen del sistema operativo del escritorio remoto no afecta al nivel del volumen de una llamada de Skype en curso. Para modificar el volumen, puede utilizar el control de volumen de la llamada de Skype o el control de volumen de la máquina cliente.

Recopilar registros para solucionar los problemas de Skype Empresarial

Para solucionar los problemas de Skype Empresarial, recopile los registros de Horizon Agent y de Horizon Client para Windows.

Procedimiento

- 1 Para recopilar registros de Horizon, incluidos los registros de proxy de medios, de Horizon Agent, inicie sesión en una máquina virtual en la que Horizon Agent esté instalado.
- 2 Abra una ventana de símbolo de sistema y ejecute `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat`.
- 3 Para recopilar los registros de Horizon, incluidos los registros del proveedor de medios, de Horizon Client, inicie sesión en una máquina virtual o un equipo físico donde Horizon Client esté instalado.
- 4 Abra una ventana de símbolo de sistema y ejecute:
 - 32 bits: `C:\Program Files\VMware\VMware Horizon View Client\DCT\support.bat`
 - 64 bits: `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`

En el escritorio aparece una carpeta `vdm-sdct` con archivos de registro comprimidos e incluye los directorios que contienen registros de VMware Horizon Virtualization Pack para Skype Empresarial:

- Dispositivo cliente: `%TEMP%\vmware-<username>\VMWMediaProvider`
- Escritorio virtual:
 - `%TEMP%\vmware-<username>\VMWMediaProviderProxy`
 - `%TEMP%\vmware-<username>\VMWMediaProviderProxyLocal`
 - `%TEMP%\vmware-<username>\MMAPlugin`

Si el tamaño del nivel de registro y los volcados de memoria son pequeños, el nivel de registro predeterminado es 7. Puede aumentar el nivel de registro a 8 para los registros máximos y los volcados de memoria completos. Todas las opciones son DWORD:

- Cliente: `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMWMediaProvider\DebugLogging/LoggingPriority = 8`
- Agente: `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8`
- Agente: `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8`

Activar el canal lateral de BEAT para el redireccionamiento de unidades cliente o USB

Con el protocolo de visualización VMware Blast, se pueden configurar las funciones de redireccionamiento de unidades cliente y de redireccionamiento USB para enviar tráfico de canal lateral a través de una conexión Blast Extreme Adaptive Transport (BEAT) en lugar de hacerlo a través del canal virtual de VMware (VVC) o el canal lateral de TCP.

El canal lateral de BEAT le permite consolidar los requisitos de puertos de red para el redireccionamiento de unidades cliente y USB. Si la red admite el tráfico de sesiones de VMware Blast, no es necesario abrir puertos UDP adicionales, puesto que el canal lateral de BEAT comparte el mismo puerto UDP con el tráfico de base (mouse, teclado y pantalla) de las sesiones de VMware Blast. Por el contrario, el canal lateral de TCP, que no comparte el puerto TCP que se utiliza para el tráfico de sesiones, necesita que se abra otro puerto TCP.

Esta función solo puede utilizarse con Horizon Client para Windows. No se admiten clientes que no sean Windows en esta versión.

Procedimiento

- 1 Para activar el canal lateral de BEAT con la función de redireccionamiento de unidades cliente, siga estos pasos.
 - a Abra el Editor del Registro de Windows (`regedit.exe`) en el equipo agente.
 - b Acceda a `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware TSDR` y establezca el valor `beat` a la clave `sideChannelType`.
- 2 Para activar el canal lateral de BEAT con la función Redireccionamiento USB siga estos pasos.
 - a Abra el editor del Registro de Windows (`regedit.exe`) en el equipo agente.
 - b Acceda a `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration` y establezca el valor `true` a la clave `UsbVirtualChannelEnabled`.
 - c Acceda a `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection` y asigne el valor `true` a la clave `vchanSideChannelEnabled` y el valor `beat` a la clave `sideChannelType`.
 - d Abra el Editor del Registro de Windows (`regedit.exe`) en el equipo cliente.
 - e Acceda a `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client` y establezca el valor `true` a la clave `EnableUsbVirtualChannelOnClient`.

Configurar el redireccionamiento de contenido URL

3

Con la función de redireccionamiento de contenido URL, puede configurar URL específicas para que se abran en el equipo cliente o en una aplicación o escritorio remotos. Puede redireccionar las URL que los usuarios introduzcan en la barra de direcciones de Internet Explorer o en una aplicación.

Este capítulo incluye los siguientes temas:

- [Información sobre el redireccionamiento de contenido URL](#)
- [Requisitos del redireccionamiento de contenido URL](#)
- [Utilizar el redireccionamiento de contenido URL en un entorno de Arquitectura de Cloud Pod](#)
- [Instalar Horizon Agent con la función Redireccionamiento de contenido URL](#)
- [Configurar el redireccionamiento de agente a cliente](#)
- [Configurar el redireccionamiento de cliente a agente](#)
- [Limitaciones de Redireccionamiento de contenido URL](#)
- [Funciones no compatibles del redireccionamiento del contenido URL](#)

Información sobre el redireccionamiento de contenido URL

La función Redireccionamiento de contenido URL admite el redireccionamiento de una aplicación o un escritorio remotos a un cliente y viceversa.

El redireccionamiento de una aplicación o un escritorio remotos a un cliente se denomina redireccionamiento de agente a cliente. El redireccionamiento de un cliente a una aplicación o un escritorio remotos se denomina redireccionamiento de cliente a agente.

Redireccionamiento de agente a cliente

Con el redireccionamiento de agente a cliente, Horizon Agent envía la URL a Horizon Client, que abre la aplicación predeterminada del protocolo en la dirección URL del equipo cliente.

Redireccionamiento de cliente a agente

Con el redireccionamiento de cliente a agente, Horizon Client abre la aplicación o el escritorio remotos que especificó para gestionar la dirección URL. Si la URL se redirecciona a un escritorio remoto, el vínculo se abre

en el navegador predeterminado del protocolo del escritorio. Si la URL se redirecciona a una aplicación remota, el vínculo se abre con la aplicación especificada. El usuario final debe tener autorización para el grupo de aplicaciones o de escritorios.

Puede redireccionar algunas URL de una aplicación o un escritorio remotos a un cliente y otras URL de un cliente a una aplicación o escritorio remotos. Puede redireccionar cualquier número de protocolos, incluidos HTTP, HTTPS, mailto y callto.

Requisitos del redireccionamiento de contenido URL

Para usar la función Redireccionamiento de contenido URL, los equipos cliente, los equipos de escritorio remoto y los hosts RDS deben cumplir algunos requisitos.

Clientes de Windows	<p>Horizon Client 4.0 para Windows o una versión posterior.</p> <p>Para usar el redireccionamiento de cliente a agente, debe habilitar la función Redireccionamiento de contenido URL durante la instalación de Horizon Client para Windows. No es necesario que habilite la función Redireccionamiento de contenido URL de Horizon Client para Windows para usar el redireccionamiento de agente a cliente.</p>
clientes Mac	<p>Horizon Client 4.2 para Mac o una versión posterior.</p> <p>En Horizon Client 4.2 o 4.3 para Mac, la función Redireccionamiento de contenido URL es una función de vista previa y solo admite el redireccionamiento de agente a cliente. A partir de Horizon Client 4.4 para Mac, se admite oficialmente la función Redireccionamiento de contenido URL y esta, a su vez, admite tanto el redireccionamiento de agente a cliente, como el de cliente a agente.</p>
Hosts RDS y máquinas virtuales de escritorio	<p>Horizon Agent 7.0 o posterior en máquinas de escritorio remotos y hosts RDS que proporcionan aplicaciones y escritorios.</p> <p>Debe habilitar la función Redireccionamiento de contenido URL durante la instalación de Horizon Agent.</p>
Navegadores web	Internet Explorer 9,10 y 11
Protocolos de visualización	VMware Blast y PCoIP

Utilizar el redireccionamiento de contenido URL en un entorno de Arquitectura de Cloud Pod

Si tiene un entorno de Arquitectura de Cloud Pod, puede establecer la configuración global del redireccionamiento de contenido URL, además de la configuración local de dicho redireccionamiento.

A diferencia de la configuración local del redireccionamiento de contenido URL, que solo es visible en el pod local, la configuración global del mismo es visible en toda la federación de pods. Con estas opciones, puede redirigir vínculos URL del cliente a recursos globales, como autorizaciones de escritorio o aplicaciones globales.

Cuando un usuario utiliza Horizon Client para iniciar sesión en una instancia del servidor de conexión en la federación de pods, dicha instancia busca todas las opciones locales y globales del redireccionamiento de contenido URL asignadas al usuario. Las configuraciones global y local se unen y se usan cuando el usuario hace clic en una URL en el equipo cliente.

Para obtener más información sobre cómo configurar y administrar un entorno Arquitectura de Cloud Pod, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

Instalar Horizon Agent con la función Redireccionamiento de contenido URL

Para utilizar el redireccionamiento de contenido URL desde una aplicación o escritorio remotos en un cliente (redireccionamiento de agente a cliente), o desde un cliente a una aplicación o escritorio remotos (redireccionamiento de cliente a agente), debe habilitar la función de redireccionamiento de contenido URL al instalar Horizon Agent.

En lugar de hacer doble clic en el archivo del instalador, inicie la instalación de Horizon Agent ejecutando el siguiente comando en una ventana de símbolo del sistema:

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Siga los pasos que se le indican y complete la instalación.

Para comprobar que la función de redireccionamiento de contenido URL esté instalada, asegúrese de que los archivos `vmware-url-protocolo-inicio-helper.exe` y `vmware-url-filtrado-plugin.dll` estén en el directorio `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection`.

Asimismo, compruebe que el complemento VMware Horizon View URL Filtering Plugin de Internet Explorer esté habilitado.

Configurar el redireccionamiento de agente a cliente

Con el redireccionamiento de agente a cliente, Horizon Agent la URL se envía a Horizon Client, que abre la aplicación predeterminada del protocolo en la dirección URL.

Para habilitar el redireccionamiento de agente a cliente, realice las siguientes tareas de configuración.

- Active la función de redireccionamiento de contenido URL en Horizon Agent. Consulte [Instalar Horizon Agent con la función Redireccionamiento de contenido URL](#).
- Aplique la configuración de directivas de grupo de redireccionamiento de contenido URL a sus aplicaciones y escritorios remotos. Consulte [Agregar la plantilla ADMX de redireccionamiento de contenido URL a un GPO](#).

- Configure la configuración de directivas de grupo para indicar, para cada protocolo, cómo Horizon Agent debe redireccionar la URL. Consulte [Configuración de directiva de grupo del Redireccionamiento de contenido URL](#).

Agregar la plantilla ADMX de redireccionamiento de contenido URL a un GPO

El archivo de plantilla ADMX de redireccionamiento de contenido URL, denominado `urlRedirection.admx`, contiene opciones que le permiten controlar si un vínculo URL se abre en el cliente (redireccionamiento de agente a cliente), o bien en una aplicación o un escritorio remotos (redireccionamiento de cliente a agente).

Para aplicar la configuración de directiva de grupo de redireccionamiento de contenido URL a las aplicaciones y escritorios remotos, agregue el archivo de plantilla ADMX a los GPO en el servidor de Active Directory. Para las reglas relativas a vínculos URL en los que se hace clic en un escritorio o aplicación remotos, los GPO deben estar vinculados a la OU que contenga sus escritorios virtuales y hosts RDS.

También puede aplicar la configuración de la directiva de grupo a un GPO que esté vinculado a la OU que contenga los equipos cliente Windows, pero el método preferido para configurar el redireccionamiento de agente a cliente es utilizar la utilidad de la línea de comandos `vdmutil`. Como macOS no admite los GPO, debe utilizar `vdmutil` si dispone de los clientes Mac.

Requisitos previos

- Compruebe que la función de redireccionamiento de contenido URL se incluya al instalar Horizon Agent. Consulte [Instalar Horizon Agent con la función Redireccionamiento de contenido URL](#).
- Compruebe que los GPO de Active Directory se creen para la configuración de directiva de grupo de redireccionamiento de contenido URL.
- Compruebe que estén disponibles los complementos Editor de administración de directivas de grupo y MMC en su servidor de Active Directory.

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, donde `x.x.x` es la versión y `yyyyyyy` es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip y copie el archivo ADMX de redireccionamiento de contenido URL a su servidor de Active Directory.

- a Copie el archivo urlRedirection.admx a la carpeta C:\Windows\PolicyDefinitions\.
- b Copie el archivo de recursos de idioma urlRedirection.adml a la subcarpeta adecuada en C:\Windows\PolicyDefinitions.

Por ejemplo, para la configuración regional EN, copie el archivo de urlRedirection.adml a la carpeta C:\Windows\PolicyDefinitions\en-US.

- 3 En su servidor de Active Directory, abra el Editor de administración de directivas de grupo.

La configuración de directiva de grupo de redireccionamiento de contenido URL se instala en

Configuración del equipo > Directivas > Plantillas administrativas > Redireccionamiento URL de VMware Horizon.

Pasos siguientes

Configure los ajustes de directiva de grupo.

Configuración de directiva de grupo del Redireccionamiento de contenido URL

El archivo de plantilla del Redireccionamiento de contenido URL contiene la configuración de directiva de grupo que permite crear reglas para los redireccionamientos de agente a cliente y de cliente a agente. El archivo de plantilla contiene únicamente la opción Configuración del equipo. Todas las configuraciones se encuentran en la carpeta **Redireccionamiento URL de VMware Horizon** del Editor de administración de directivas de grupo.

La siguiente tabla describe la configuración de directiva de grupo del archivo de plantilla Redireccionamiento de contenido URL.

Tabla 3-1. Configuración de directiva de grupo del Redireccionamiento de contenido URL

Configuración	Propiedades
IE Policy: Prevent users from changing URL Redirection plugin loading behavior	<p>Determina si los usuarios pueden deshabilitar la función Redireccionamiento de contenido URL.</p> <p>Esta opción no está configurada de forma predeterminada.</p>
IE Policy: Automatically enable URL Redirection plugin	<p>Determina si los complementos de Internet Explorer recientemente instalados se activan automáticamente.</p> <p>Esta opción no está configurada de forma predeterminada.</p>
Url Redirection Enabled	<p>Determina si la función Redireccionamiento de contenido URL está habilitada. Puede usar esta opción para deshabilitar la función Redireccionamiento de contenido URL, independientemente de que se instalara en el cliente o en el agente.</p> <p>Esta opción no está configurada de forma predeterminada.</p>

Configuración	Propiedades
Url Redirection Protocol 'http'	<p>En todas las URL que usen el protocolo HTTP, especifica las URL que se deben redireccionar. Esta configuración tiene las siguientes opciones:</p> <ul style="list-style-type: none"> ■ brokerHostname: dirección IP o nombre completo del host del servidor de conexión que se usa cuando se redireccionan las URL a una aplicación o un escritorio remotos. ■ remoteltem: muestra el nombre del grupo de aplicaciones o de escritorios remotos que pueden gestionar las URL especificadas en agentRules. ■ clientRules: las URL que se deben redireccionar al cliente. Por ejemplo, si configura clientRules como .*.mycompany.com, todas las URL que incluyen mycompany.com se redireccionan al cliente basado en Windows y se abren en el navegador predeterminado del cliente. ■ agentRules: las URL que se deben redireccionar a la aplicación o al escritorio remotos especificados en remoteltem. Por ejemplo, si configura agentRules como .*.mycompany.com, todas las URL que incluyan "mycompany.com" se redireccionan a la aplicación o al escritorio remotos. <p>Cuando cree reglas del agente, también debe usar la opción brokerHostname para especificar la dirección IP o el nombre de dominio completo del host del servidor de conexión y la opción remoteltem para especificar el nombre para mostrar del grupo de aplicaciones o de escritorios.</p> <p>Nota El método preferido para configurar las reglas del cliente es usar la utilidad <code>vdmutil</code> de la línea de comandos.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
Url Redirection Protocol '[...]'	<p>Utilice esta opción para los protocolos que no sean HTTP, como HTTPS, email o callto.</p> <p>Las opciones son las mismas que para Url Redirection Protocol 'http'.</p> <p>Si no necesita configurar otros protocolos, puede eliminar o anular el comentario de esta entrada antes de agregar el archivo de plantilla Redireccionamiento de contenido URL a Active Directory.</p> <p>Como práctica recomendada, establezca la misma opción de redireccionamiento para los protocolos HTTP y HTTPS. De esta manera, si un usuario escribe una URL parcial en Internet Explorer, como mycompany.com, y ese sitio redirecciona automáticamente de HTTP a HTTPS, la función Redireccionamiento de contenido URL funcionará correctamente. En este ejemplo, si establece una regla para HTTPS, pero no establece la misma opción de redireccionamiento para HTTP, no se redirecciona la URL abreviada que el usuario introduce.</p> <p>Esta opción no está configurada de forma predeterminada.</p>

Para el redireccionamiento de cliente a agente, si configura un protocolo que no tenga un controlador predeterminado, después de configurar una configuración de directiva de grupo para este protocolo, debe iniciar Horizon Client tras el redireccionamiento de las URL que especifica este protocolo.

Sintaxis para crear reglas de redireccionamiento de contenido URL

Puede usar expresiones regulares cuando especifique las URL que se abrirán en el cliente o en una aplicación o escritorio remotos. Utilice punto y coma para separar varias entradas. No se permite el uso de espacio entre entradas.

En la siguiente tabla se describen algunas entradas de ejemplo.

Entrada	Descripción
<code>.*</code>	Especifica que se redireccionarán todas las URL. Si utiliza esta configuración para las reglas del agente (opción agentRules), se abrirán todas las URL en la aplicación o el escritorio remotos especificados. Si usa esta configuración para las reglas del cliente (clientRules), todas las URL especificadas se redireccionarán al cliente.
<code>.*.acme.com;.*.example.com</code>	Especifica que se redireccionarán todas las URL que incluyan el texto <code>.acme.com</code> o <code>example.com</code> .
[espacio o dejar vacío]	Especifica que no se redireccionará ninguna URL. Por ejemplo, si deja la opción clientRules vacía, esto especifica que ninguna URL se redireccionará al cliente.

Ejemplo de directiva de grupo de redireccionamiento de agente a cliente

Es posible que desee usar el redireccionamiento de agente a cliente para ahorrar recursos o como una capa de seguridad adicional. Si los empleados están trabajando en una aplicación o un escritorio remotos y desean ver vídeos, por ejemplo, puede redireccionar esas URL a la máquina cliente para que no se produzca una carga adicional en el centro de datos. Por razones de seguridad, para los empleados que trabajen fuera de la red corporativa, es posible que desee que todas las URL que se dirigen a ubicaciones externas a la red corporativa se abran en una máquina cliente del empleado.

Puede, por ejemplo, configurar reglas para que cualquier contenido que no sea relativo a la compañía, es decir, las URL que no se dirijan a la red corporativa, se redirija para que se abra en la máquina cliente. En este caso, podría usar las siguientes opciones, que incluyen expresiones comunes:

- Para **agentRules**: `.*.mycompany.com`

Esta regla redirige cualquier dirección URL que contenga el texto `mycompany.com` para que se abra en la aplicación o escritorio remoto especificados (agente).

- Para **clientRules**: `.*`

Esta regla redirecciona todas las direcciones URL al cliente, para que se abran con el navegador predeterminado del mismo.

La función de redireccionamiento de contenido URL utiliza el siguiente proceso para aplicar reglas del agente y del cliente:

- 1 Cuando un usuario hace clic en un vínculo de una aplicación o un escritorio remotos, se comprueban las reglas del cliente en primer lugar.
- 2 Si una URL coincide con una regla del cliente, las reglas del agente se comprueban a continuación.

- 3 Si hay un conflicto entre las reglas del agente y las del cliente, el vínculo se abre de forma local. En este caso, la dirección URL se abre en el equipo del agente.
- 4 Si no existe ningún conflicto, la URL se redirecciona al cliente.

En el ejemplo, hay un conflicto entre las reglas del cliente y del agente porque las URL con **mycompany.com** son un subconjunto de todas las URL. Debido a este conflicto, las direcciones URL que incluyen **mycompany.com** se abren localmente. Si hace clic en un vínculo que incluye **mycompany.com** en la URL mientras se encuentra en un escritorio remoto, la URL se abrirá en ese escritorio remoto. Si hace clic en un vínculo con **mycompany.com** en la URL mientras se encuentra en un sistema cliente, la URL se abrirá en el cliente.

Configurar el redireccionamiento de cliente a agente

Con el redireccionamiento de cliente a agente, Horizon Client abre un escritorio o aplicación remotos para controlar un vínculo URL en el que un usuario hace clic en el cliente. Si se abre un escritorio remoto, la aplicación predeterminada del protocolo en la dirección URL procesa la URL. Si se abre una aplicación remota, la aplicación procesa la URL.

Para utilizar el redireccionamiento de cliente a agente, realice las siguientes tareas de configuración.

- Active la función de redireccionamiento de contenido URL en Horizon Agent. Consulte [Instalar Horizon Agent con la función Redireccionamiento de contenido URL](#).
- (Solo para clientes Windows) Habilite la función de redireccionamiento de contenido URL en Horizon Client para Windows. Consulte [Instalar Horizon Client para Windows con la función de redireccionamiento de contenido URL](#).
- Use la utilidad de la línea de comandos `vdmutil` para crear una opción de redireccionamiento de contenido URL que indique, para cada protocolo, cómo Horizon Client debe redireccionar las URL. Consulte [Crear una opción de redireccionamiento de contenido URL](#) o [Crear una opción de redireccionamiento de contenido URL global](#).
- Use la utilidad de la línea de comandos `vdmutil` para asignar la opción de redireccionamiento de contenido URL a grupos o usuarios de Active Directory. Consulte [Asignar una opción de redireccionamiento de contenido URL a un usuario o grupo](#).
- Compruebe la opción de redireccionamiento de contenido URL. Consulte [Configurar una opción de redireccionamiento de contenido URL](#).

Nota Puede utilizar la configuración de directiva de grupo para configurar las reglas de redireccionamiento de cliente a agente, pero se recomienda utilizar la utilidad de la línea de comandos `vdmutil`. Para obtener más información sobre cómo usar la configuración de la directiva de grupo, consulte [Usar la configuración de directiva de grupo para configurar el redireccionamiento de cliente a agente](#). En los clientes Mac, debe utilizar `vdmutil` para configurar el redireccionamiento de cliente a agente. Como los GPO no son compatibles con macOS, no es posible la configuración de directiva de grupo para establecer la configuración de cliente a agente si tiene clientes Mac.

Instalar Horizon Client para Windows con la función de redireccionamiento de contenido URL

Para utilizar el redireccionamiento de contenido URL desde un cliente Windows a una aplicación o escritorio remotos (redireccionamiento de cliente a agente), debe instalar Horizon Client para Windows con la función de redireccionamiento de contenido URL.

Para habilitar la función de redireccionamiento de contenido URL, debe utilizar Horizon Client para Windows Installer con una opción de línea de comandos. En lugar de hacer doble clic en el archivo del instalador, inicie la instalación ejecutando el siguiente comando en una ventana de símbolo del sistema:

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Para comprobar que la función está instalada, asegúrese de que los archivos `vmware-url-protocolo-inicio-helper.exe` y `vmware-url-filtrado-plugin.dll` están en el directorio `%PROGRAMFILES%\VMware\VMware Horizon View Client`. Asimismo, compruebe que esté habilitado el complemento VMware Horizon View URL Filtering Plugin de Internet Explorer.

Nota Horizon Client 4.4 para Mac admite el redireccionamiento de cliente a agente de forma predeterminada. No es necesario realizar pasos de instalación adicionales. Horizon Client 4.2 y 4.3 para Mac no admiten el redireccionamiento de cliente a agente.

Usar la utilidad vdmutil de la línea de comandos

Puede utilizar la interfaz de la línea de comandos `vdmutil` para crear, asignar y administrar la configuración del redireccionamiento de contenido URL de cliente a agente.

Nota Debe utilizar el comando `vdmutil` para configurar el redireccionamiento de cliente a agente para clientes Mac. Como los GPO no son compatibles con macOS, no es posible utilizarlos para establecer la configuración de cliente a agente si tiene clientes Mac.

Uso de los comandos

La sintaxis del comando `vdmutil` controla la operación desde un símbolo del sistema de Windows.

```
vdmutil opción_comando [opción_adicional argumento] ...
```

Las opciones adicionales que puede usar dependen de la opción del comando.

De forma predeterminada, la ruta del archivo ejecutable de comandos `vdmutil` es `C:\Program Files\VMware\VMware View\Server\tools\bin`. Si desea evitar introducir la ruta en la línea de comando, agréguela a la variable de entorno `PATH`.

Autenticación del comando

Debe ejecutar el comando `vdmutil` como un usuario con la función Administradores.

Horizon Administrator permite asignar la función de administradores a un usuario. Para obtener más información, consulte el documento *Administración de View*.

El comando `vdmutil` incluye opciones para especificar el nombre de usuario, el dominio y la contraseña que se deben usar en la autenticación. Debe usar estas opciones de autenticación con todas las opciones del comando `vdmutil`, excepto con `--help` y con `--verbose`.

Tabla 3-2. Opciones de autenticación del comando `vdmutil`

Opción	Descripción
<code>--authAs</code>	Nombre de un usuario Horizon Administrator para autenticarse en la instancia del servidor de conexión. No use dominio\nombredeusuario ni el formato de nombre principal de usuario (UPN).
<code>--authDomain</code>	Nombre de dominio completo del usuario Horizon Administrator especificado en la opción <code>--authAs</code> .
<code>--authPassword</code>	Contraseña del Horizon Administrator especificado en la opción <code>--authAs</code> . Al escribir "*" en lugar de una contraseña, el comando <code>vdmutil</code> solicitará la contraseña y no admitirá contraseñas que distingan entre mayúsculas y minúsculas en el historial de la línea de comandos.

Por ejemplo, el siguiente comando `vdmutil` inicia sesión en `midominio\juan` del usuario.

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

Salida de comando

El comando `vdmutil` devuelve 0 cuando una operación se realiza correctamente y un código que no es cero específico de errores cuando una operación no se realiza correctamente. El comando `vdmutil` escribe mensajes de error de los errores estándar. Cuando una operación genera una salida o cuando el registro detallado está habilitado con la opción `--verbose`, el comando `vdmutil` escribe la salida estándar en inglés de Estados Unidos.

Opciones del redireccionamiento de contenido URL

Puede usar las siguientes opciones del comando `vdmutil` para crear, asignar y administrar la configuración del redireccionamiento de contenido URL. Todas las opciones aparecen precedidas de dos guiones (--).

Tabla 3-3. Opciones del comando `vdmutil` para el redireccionamiento de contenido URL

Opción	Descripción
<code>--addGroupURLSetting</code>	Asigna un grupo a una opción del redireccionamiento de contenido URL en concreto.
<code>--addUserURLSetting</code>	Asigna un usuario a una opción del redireccionamiento de contenido URL en concreto.
<code>--createURLSetting</code>	Crea una opción del redireccionamiento de contenido URL.
<code>--deleteURLSetting</code>	Elimina una opción del redireccionamiento de contenido URL.
<code>--disableURLSetting</code>	Deshabilita una opción del redireccionamiento de contenido URL.
<code>--enableURLSetting</code>	Habilita una opción del redireccionamiento de contenido URL que estaba deshabilitada con la opción <code>--disableURLSetting</code> .

Opción	Descripción
<code>--listURLSetting</code>	Enumera todas las opciones del redireccionamiento de contenido URL de la instancia del servidor de conexión.
<code>--readURLSetting</code>	Muestra información sobre una opción del redireccionamiento de contenido URL.
<code>--removeGroupURLSetting</code>	Elimina una asignación de grupo de una opción del redireccionamiento de contenido URL.
<code>--removeUserURLSetting</code>	Elimina una asignación de usuario de una opción del redireccionamiento de contenido URL.
<code>--updateURLSetting</code>	Actualiza una opción del redireccionamiento de contenido URL ya existente.

Puede mostrar la información de sintaxis de todas las opciones de `vdmutil` si escribe **`vdmutil --help`**. Para mostrar información detallada de la sintaxis de una opción en particular, escriba **`vdmutil --option --help`**.

Crear una opción de redireccionamiento de contenido URL

Puede crear una opción de redireccionamiento de contenido URL que redirija URL específicas para que se abran en una aplicación o escritorio remotos. Una opción de redireccionamiento de contenido URL local está visible solo en el pod local.

Puede configurar el número de protocolos que desee para el redireccionamiento, incluidos HTTP, HTTPS, mailto y callto.

Como práctica recomendada, establezca la misma opción de redireccionamiento para los protocolos HTTP y HTTPS. De esta manera, si un usuario escribe una URL parcial en Internet Explorer, como `mycompany.com`, y ese sitio redirige automáticamente de HTTP a HTTPS, la función Redireccionamiento de contenido URL funcionará correctamente. En este ejemplo, si establece una regla para HTTPS, pero no establece la misma opción de redireccionamiento para HTTP, no se redirige la URL abreviada que el usuario introduce.

Para crear una opción de redireccionamiento de contenido URL global que sea visible en toda la federación de pods, consulte [Crear una opción de redireccionamiento de contenido URL global](#).

Requisitos previos

Familiarícese con los requisitos y las opciones de la interfaz de la línea de comandos `vdmutil` y verifique que tenga privilegios suficientes para ejecutar el comando `vdmutil`. Consulte [Usar la utilidad `vdmutil` de la línea de comandos](#).

Procedimiento

- 1 Inicie sesión en la instancia del servidor de conexión.

- 2 Ejecute el comando `vdmutil` con la opción `--createUrlSetting` para crear la opción de redireccionamiento de contenido URL.

```
vdmutil --createUrlSetting --urlSettingName valor --urlRedirectionScope LOCAL
[--description valor] [--urlScheme valor] [--entitledApplication valor | --entitledDesktop valor]
[--agentURLPattern valor]
```

Opción	Descripción
<code>--urlSettingName</code>	Nombre único para la opción de redireccionamiento de contenido URL. El nombre puede tener entre 1 y 64 caracteres.
<code>--urlRedirectionScope</code>	Ámbito de la opción de redireccionamiento de contenido URL. Especifique LOCAL para que la opción sea visible solo en el pod local.
<code>--description</code>	Descripción de la opción de redireccionamiento de contenido URL. La descripción puede tener entre 1 y 1024 caracteres.
<code>--urlScheme</code>	Protocolo al que se aplica la opción de redireccionamiento de contenido URL, por ejemplo: http, https, mailto o callto.
<code>--entitledApplication</code>	Nombre para mostrar de un grupo de aplicaciones locales que se usan para abrir las URL especificadas, por ejemplo, <code>iexplore-2012</code> . También puede utilizar esta opción para especificar el nombre para mostrar de un grupo de escritorios RDS local.
<code>--entitledDesktop</code>	Nombre para mostrar de un grupo de escritorios locales que se usa para abrir las URL especificadas, por ejemplo, <code>xx</code> . Para grupos de escritorios RDS, utilice la opción <code>--entitledApplication</code> .
<code>--agentURLPattern</code>	Una cadena entre comillas que especifica la URL que debe abrirse en la aplicación o escritorio remotos. Debe incluir el prefijo de protocolo. Puede utilizar caracteres comodines para especificar un patrón de URL que coincida con varias URL. Por ejemplo, si escribe <code>"http://google.*"</code> , todas las URL que incluyen el texto google se redireccionan al escritorio remoto o grupo de aplicaciones que especificó. Si escribe <code>.*</code> (punto, asterisco), todas las URL se redireccionan a la aplicación o escritorio remotos.

- 3 (opcional) Ejecute el comando `vdmutil` con la opción `--updateURLSetting` para agregar más protocolos, URL y recursos locales a la opción de redireccionamiento de contenido URL que creó.

```
vdmutil --updateURLSetting --urlSettingName valor --urlRedirectionScope LOCAL
[--description valor][--urlScheme valor][--entitledApplication valor | --entitledDesktop valor]
[--agentURLPattern valor]
```

Las opciones son las mismas que para el comando `vdmutil` con la opción `--createUrlSetting`.

Ejemplo: Crear una opción de redireccionamiento de contenido URL local

En el siguiente ejemplo, se crea una opción de redireccionamiento del contenido URL local denominada `url-filtering`, que redirecciona todas las URL cliente que incluyan `http://google.*` al grupo de aplicaciones llamado `iexplore2012`.

```
VdmUtil --createUrlSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

El siguiente ejemplo actualiza la opción `url-filtering` para redireccionar al mismo tiempo todas las URL cliente que contengan el texto `https://google.*` al grupo de aplicaciones llamado `iexplore2012`.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

El siguiente ejemplo actualiza la opción `url-filtering` para redireccionar todas las URL clientes que contengan el texto `mailto://.*.mycompany.com` al grupo de aplicaciones llamado `Outlook2008`.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://.*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

Pasos siguientes

Asigne la opción de redireccionamiento de contenido URL a un usuario o grupo. Consulte [Asignar una opción de redireccionamiento de contenido URL a un usuario o grupo](#).

Crear una opción de redireccionamiento de contenido URL global

Si tiene un entorno Arquitectura de Cloud Pod, puede crear una opción de redireccionamiento de contenido URL global que redirija las URL específicas para que se abran en una aplicación o escritorio remotos en cualquier pod de la federación.

Una opción de redireccionamiento de contenido URL global está visible en toda la federación de pods. Cuando cree una opción de redireccionamiento de contenido URL global, puede redireccionar las URL a recursos globales, como las autorizaciones de escritorios globales y las autorizaciones de aplicaciones globales.

Puede configurar el número de protocolos que desee para el redireccionamiento, incluidos HTTP, HTTPS, mailto y callto.

Como práctica recomendada, establezca la misma opción de redireccionamiento para los protocolos HTTP y HTTPS. De esta manera, si un usuario escribe una URL parcial en Internet Explorer, como `mycompany.com`, y ese sitio redirecciona automáticamente de HTTP a HTTPS, la función Redireccionamiento de contenido URL funcionará correctamente. En este ejemplo, si establece una regla para HTTPS, pero no establece la misma opción de redireccionamiento para HTTP, no se redirecciona la URL abreviada que el usuario introduce.

Para obtener más información sobre cómo configurar y administrar un entorno Arquitectura de Cloud Pod, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

Para crear una opción de redireccionamiento de contenido URL local, consulte [Crear una opción de redireccionamiento de contenido URL](#).

Requisitos previos

Familiarícese con los requisitos y las opciones de la interfaz de la línea de comandos `vdmutil` y verifique que tenga privilegios suficientes para ejecutar el comando `vdmutil`. Consulte [Usar la utilidad `vdmutil` de la línea de comandos](#).

Procedimiento

- 1 Inicie sesión en cualquier instancia del servidor de conexión en la federación de pods.
- 2 Ejecute el comando `vdmutil` con la opción `--createUrlSetting` para crear la opción de redireccionamiento de contenido URL.

```
vdmutil --createUrlSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description valor] [--urlScheme valor] [--entitledApplication valor | --entitledDesktop
valor] [--agentURLPattern valor]
```

Opción	Descripción
<code>--urlSettingName</code>	Nombre único para la opción de redireccionamiento de contenido URL. El nombre puede tener entre 1 y 64 caracteres.
<code>--urlRedirectionScope</code>	Ámbito de la opción de redireccionamiento de contenido URL. Especifique GLOBAL para que la opción esté visible en toda la federación de pods.
<code>--description</code>	Descripción de la opción de redireccionamiento de contenido URL. La descripción puede tener entre 1 y 1024 caracteres.
<code>--urlScheme</code>	Protocolo al que se aplica la opción de redireccionamiento de contenido URL, por ejemplo: http, https, mailto o callto.
<code>--entitledApplication</code>	Nombre para mostrar de una autorización de aplicación global que se usa para abrir las URL especificadas.
<code>--entitledDesktop</code>	Nombre para mostrar de una autorización de escritorio global que se usa para abrir las URL especificadas, por ejemplo, GE-1.
<code>--agentURLPattern</code>	Una cadena entre comillas que especifica la URL que debe abrirse en la aplicación o escritorio remotos. Debe incluir el prefijo de protocolo. Puede utilizar caracteres comodines para especificar un patrón de URL que coincida con varias URL. Por ejemplo, si escribe "http://google.*", todas las URL que incluyan el texto google se redireccionan a la aplicación o escritorio remotos. Si escribe .* (punto, asterisco), todas las URL se redireccionan a la aplicación o escritorio remotos.

- 3 (opcional) Ejecute el comando `vdmutil` con la opción `--updateURLSetting` para agregar más protocolos, URL y recursos globales a la opción de redireccionamiento de contenido URL que creó.

```
vdmutil --updateURLSetting --urlSettingName valor --urlRedirectionScope GLOBAL
[--description valor][--urlScheme valor][--entitledApplication valor | --entitledDesktop
valor] [--agentURLPattern valor]
```

Las opciones son las mismas que para el comando `vdmutil` con la opción `--createUrlSetting`.

Ejemplo: Configurar una opción de redireccionamiento de contenido URL global

En el siguiente ejemplo, se crea una opción de redireccionamiento de contenido URL global denominada `Operations-Setting` que redirecciona todas las URL cliente que incluyan `http://google.*` a la autorización de aplicación global denominada `GAE1`.

```
vdmutil --createUrlSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

El siguiente ejemplo actualiza la opción `Operations-Setting` para redireccionar también todas las URL que contengan el texto `https://google.*` a la autorización de aplicación global denominada `GAE1`.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

El siguiente ejemplo actualiza la opción `Operations-Setting` para redireccionar todas las URL que contengan el texto `"mailto://.*.Mycompany.com"` a la autorización de aplicación global denominada `GA2`.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://.*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

Pasos siguientes

Asigne la opción de redireccionamiento de contenido URL a un usuario o grupo. Consulte [Asignar una opción de redireccionamiento de contenido URL a un usuario o grupo](#).

Asignar una opción de redireccionamiento de contenido URL a un usuario o grupo

Después de crear una opción de redireccionamiento de contenido URL, puede asignarla a un grupo o a un usuario de Active Directory.

Requisitos previos

Familiarícese con los requisitos y las opciones de interfaz de la línea de comandos `vdmutil` y verifique que tiene privilegios suficientes para ejecutar el comando `vdmutil`. Consulte [Usar la utilidad vdmutil de la línea de comandos](#).

Procedimiento

- ◆ Para asignar una opción de redireccionamiento de contenido URL a un usuario, ejecute el comando `vdmutil` con la opción `--addUserURLSetting`.

```
vdmutil --addUserURLSetting --urlSettingName valor --userName valor
```

Opción	Descripción
<code>--urlSettingName</code>	Nombre de la opción de redireccionamiento de contenido URL para asignar.
<code>--userName</code>	Nombre del usuario de Active Directory en formato dominio\nombre de usuario.

- ◆ Para asignar una opción de redireccionamiento de contenido URL a un grupo, ejecute el comando `vdmutil` con la opción `--addGroupURLSetting`.

```
vdmutil --addGroupURLSetting --urlSettingName valor --groupName valor
```

Opción	Descripción
<code>--urlSettingName</code>	Nombre de la opción de redireccionamiento de contenido URL para asignar.
<code>--groupName</code>	Nombre del grupo de Active Directory en formato dominio\grupo.

Ejemplo: Asignar una opción de redireccionamiento de contenido URL

El ejemplo siguiente asigna la opción de redireccionamiento de contenido URL denominada `url-filtering` al usuario `midominio\fulanitadetal`.

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

El ejemplo siguiente asigna la opción de redireccionamiento de contenido URL denominada `url-filtering` al grupo `midominio\grupodeusuario`.

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

Pasos siguientes

Compruebe las opciones de redireccionamiento de contenido URL. Consulte [Configurar una opción de redireccionamiento de contenido URL](#).

Configurar una opción de redireccionamiento de contenido URL

Después de crear y asignar una opción de redireccionamiento de contenido URL, realice diferentes pasos para verificar que funcione correctamente.

Requisitos previos

Familiarícese con los requisitos y las opciones de la interfaz de la línea de comandos `vdmutil` y verifique que tenga privilegios suficientes para ejecutar el comando `vdmutil`. Consulte [Usar la utilidad `vdmutil` de la línea de comandos](#).

Procedimiento

- 1 Inicie sesión en la instancia del servidor de conexión.
- 2 Ejecute el comando `vdmutil` con la opción `--readURLSetting`.

Por ejemplo:

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

El comando muestra información detallada sobre la configuración del redireccionamiento de contenido URL. Por ejemplo, la siguiente salida de comando de la opción `url-filtering` muestra que las URL HTTP y HTTPS que contengan el texto `google.*` se redireccionan del cliente a un grupo local de aplicaciones denominado `iexplore2012`.

```
URL Redirection setting url-filtering
  Description                : null
  Enabled                    : true
  Scope of URL Redirection Setting : LOCAL
  URL Scheme And Local Resource handler pairs
    URL Scheme               : http
    Handler type              : APPLICATION
    Handler Resource name     : iexplore2012
    URL Scheme               : https
    Handler type              : APPLICATION
    Handler Resource name     : iexplore2012
  AgentPatterns
    https://google.*
    http://google.*
  ClientPatterns
    No client patterns configured
```

- 3 En un equipo Windows cliente, abra Horizon Client, conéctese a la instancia del servidor de conexión, haga clic en las URL que coincidan con los patrones configurados en la opción y verifique que las URL se redireccionen correctamente.
- 4 En el mismo equipo Windows cliente (`regedit`) y compruebe las claves de registro de la ruta `\Computer\HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\URLRedirection\`.

Debería mostrarse una clave por cada protocolo especificado en la configuración. Puede hacer clic en un protocolo para consultar las reglas asociadas a ese protocolo. Por ejemplo, `agentRules` muestra las URL que se redireccionan, `brokerHostName` muestra la dirección IP o el nombre de host completo de la instancia del servidor de conexión que se usa cuando se redireccionan las URL y `remoteItem` muestra el nombre para mostrar del grupo de aplicaciones o de escritorios que gestiona las URL redireccionadas.

Administrar la opción de redireccionamiento de contenido URL

Puede utilizar comandos `vdmutil` para administrar la opción de redireccionamiento de contenido URL.

Debe especificar las opciones `--authAs`, `--authDomain` y `--authPassword` con todos los comandos. Si desea obtener más información, consulte [Usar la utilidad `vdmutil` de la línea de comandos](#).

Mostrar opciones

Ejecute el comando `vdmutil` con la opción `--listURLSetting` para mostrar los nombres de todas las opciones de redireccionamiento de contenido URL.

```
vdmutil --listURLSetting
```

Ejecute el comando `vdmutil` con `--readURLSetting` para ver información detallada sobre una opción de redireccionamiento de contenido URL determinada.

```
vdmutil --readURLSetting --urlSettingName valor
```

Eliminar una opción

Ejecute el comando `vdmutil` con la opción `--deleteURLSetting` para eliminar una opción de redireccionamiento de contenido URL.

```
vdmutil --deleteURLSetting --urlSettingName valor
```

Deshabilitar y habilitar una opción

Ejecute el comando `vdmutil` con la opción `--disableURLSetting` para deshabilitar una opción de redireccionamiento de contenido URL.

```
vdmutil --disableURLSetting --urlSettingName valor
```

Ejecute `vdmutil` con la opción `--enableURLSetting` para habilitar una opción de redireccionamiento de contenido URL que se deshabilitó.

```
vdmutil --enableURLSetting --urlSettingName valor
```

Eliminar un grupo o un usuario de una opción

Ejecute el comando `vdmutil` con la opción `--removeUserURLSetting` para quitar un usuario de una opción de redireccionamiento de contenido URL.

```
vdmutil --removeUserURLSetting --urlSettingName valor --userName valor
```

Ejecute el comando `vdmutil` con la opción `--removeGroupURLSetting` para quitar un grupo de una opción de redireccionamiento de contenido URL.

```
vdmutil --removeGroupURLSetting --urlSettingName valor --userGroup valor
```

Utilice el formato `dominio\nombredeusuario` o `dominio\nombredegrupo` al especificar un nombre de usuario o grupo.

Usar la configuración de directiva de grupo para configurar el redireccionamiento de cliente a agente

El archivo de plantilla ADMX de redireccionamiento de contenido URL (`urlRedirection.admx`) contiene una configuración de directiva de grupo que puede usar para crear reglas que redirijan las URL del cliente a la aplicación o al escritorio remoto (redireccionamiento de cliente a agente).

Nota El método preferido para configurar el redireccionamiento de cliente a agente es usar la interfaz `vdmutil` de la línea de comandos. Como los GPO no son compatibles con macOS, no es posible utilizarlos para establecer la configuración de cliente a agente si tiene clientes Mac.

Si desea crear una regla para establecer un redireccionamiento de cliente a agente, use la opción **remoteltem** para especificar el nombre para mostrar de un grupo de aplicaciones o escritorios remotos y la opción **agentRules** para especificar las URL que se deben redirigir a la aplicación o al escritorio remoto. Debe usar también la opción **brokerHostname** para especificar la dirección IP o el nombre de dominio completo del host del servidor de conexión que se usará al redirigir las URL a una aplicación o escritorio remoto.

Por ejemplo, por razones de seguridad, es posible que quiera que todas las URL de HTTP que se dirigen a la red corporativa se abran en una aplicación o en un escritorio remoto. En este caso, puede establecer la opción **agentRules** como `.*.mycompany.com`.

Para obtener más instrucciones sobre la instalación de archivo de plantilla de redireccionamiento de contenido URL, consulte [Agregar la plantilla ADMX de redireccionamiento de contenido URL a un GPO](#).

Limitaciones de Redireccionamiento de contenido URL

El comportamiento de la función Redireccionamiento del contenido URL puede tener algunos resultados no esperados.

- Si la dirección URL abre una página de un país específico según la configuración regional, el origen del vínculo determina la página de la configuración regional que se abre. Por ejemplo, si el escritorio remoto (origen del agente) se encuentra en un centro de datos en Japón y el equipo del usuario se encuentra en los EE. UU., al redirigir la URL del agente a la máquina cliente, la página que se abre en el cliente estadounidense es la japonesa.
- Si los usuarios crean favoritos a partir de páginas web, estos se crean después del redireccionamiento. Por ejemplo, si un usuario hace clic en un vínculo en el equipo cliente, la URL se redirige a un escritorio remoto (agente) y el usuario establece esa página como favorita, el favorito se crea en el agente. La próxima vez que el usuario abra el navegador en la máquina cliente, esperará encontrarse el favorito en la máquina cliente, pero este se almacenó en el escritorio remoto (origen del agente).

- Los archivos que los usuarios descargan aparecen en el equipo cuyo navegador se usó para abrir la URL; por ejemplo, si un usuario hace clic en un vínculo en la máquina cliente y la URL se redirecciona a un escritorio remoto. Si el vínculo descargó un archivo o si es para una página web desde donde el usuario descarga un archivo, este se descarga en el escritorio remoto en lugar de en la máquina cliente.
- Si instala Horizon Agent y Horizon Client en el mismo equipo, puede habilitar el Redireccionamiento de contenido URL en Horizon Agent o en Horizon Client, pero no en ambos. En esta máquina, puede configurar tanto el redireccionamiento de agente a cliente como el de agente a cliente, pero no ambos.

Funciones no compatibles del redireccionamiento del contenido URL

La función Redireccionamiento de contenido URL no funciona en ciertas circunstancias.

Direcciones URL abreviadas

Las URL abreviadas, como `https://goo.gl/abc`, se pueden redireccionar de acuerdo a las reglas de filtrado, pero el mecanismo de filtrado no busca en la URL original sin abreviar.

Por ejemplo, si tiene una regla que redirija las URL que contengan `acme.com`, una URL original, como `http://www.acme.com/some-really-long-path`, y una URL abreviada de la original, como `https://goo.gl/xyz`, se redirige la URL original, pero no la abreviada.

Puede solucionar esta limitación creando reglas para bloquear o redireccionar las URL desde los sitios web que use con más frecuencia para abreviar las URL.

Páginas HTML integradas

Las páginas HTML integradas omiten el redireccionamiento URL, por ejemplo, cuando un usuario accede a una URL que no coincide con la regla del redireccionamiento de URL. Si una página contiene una página HTML integrada (iFrame o marco flotante) que contenga una URL que no coincida con ninguna regla de redireccionamiento, la regla de redireccionamiento no funciona. La regla solo funciona en la URL de nivel superior.

Complementos de Internet Explorer deshabilitados

El redireccionamiento del contenido URL no funciona en situaciones en las que los complementos de Internet Explorer están deshabilitados; por ejemplo, cuando un usuario cambia al modo de exploración de InPrivate. Los usuarios usan la navegación privada para que las páginas web y los archivos descargados no se registren en los historiales de descargas y de navegación del equipo. Esta limitación ocurre porque la función Redireccionamiento URL requiere que se habilite un complemento de Internet Explorer y la navegación privada lo deshabilita.

Puede solucionar esta limitación usando la opción del GPO para evitar que los usuarios deshabiliten los complementos. Entre estas opciones se incluyen: "No permitir que usuarios habiliten ni deshabiliten complementos" y "Habilitar automáticamente los complementos instalados recientemente". En el Editor de administración de directivas de grupo, estas opciones se encuentran en **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer**.

Para solucionar esta limitación específicamente para Internet Explorer, use la opción del GPO para deshabilitar el modo InPrivate. Esta opción se denomina "Desactivar la exploración de InPrivate". En el Editor de administración de directivas de grupo, estas opciones se encuentran en **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer > Privacidad**.

Se recomienda la implementación de estas soluciones alternativas y, además, pueden evitar los problemas con el redireccionamiento que se puedan producir en otras situaciones diferentes.

La aplicación universal de Windows 10 es el controlador predeterminado de un protocolo

El redireccionamiento URL no funciona si una aplicación universal de Windows 10 es el controlador predeterminado de un protocolo especificado en un vínculo. Las aplicaciones universales se compilan en la plataforma universal de Windows para que se puedan descargar en equipos, tabletas y teléfonos, y entre ellas se incluyen el navegador Microsoft Edge, Correo, Maps, Fotos y Groove Música, entre otras.

Si hace clic en un vínculo cuyo controlador predeterminado es una de estas aplicaciones, la URL no se redirecciona. Por ejemplo, si un usuario hace clic en un vínculo de correo electrónico en una aplicación y la aplicación de correo electrónico predeterminada es la aplicación universal Correo, la URL especificada en el vínculo no se redirecciona.

Puede solucionar esta limitación si establece una aplicación diferente como el controlador predeterminado del protocolo de las URL que desee redireccionar. Por ejemplo, si el navegador predeterminado es Edge, cámbielo a Internet Explorer.

Equipos con el arranque seguro habilitado

Las máquinas que tengan el arranque seguro habilitado no activan la función del redireccionamiento del contenido URL. Las URL no se pueden redireccionar desde esas máquinas. Sin embargo, se pueden redireccionar a esas máquinas.

Usar dispositivos USB con aplicaciones y escritorios remotos

4

Los administradores pueden configurar la capacidad de usar los dispositivos USB, como unidades de memoria flash, cámaras, dispositivos VoIP (voz sobre IP) e impresoras, desde un escritorio remoto. Esta función se denomina redireccionamiento USB y admite los protocolos de visualización Microsoft RDP, PCoIP o Blast Extreme. Un escritorio remoto puede admitir hasta 128 dispositivos USB.

También puede redireccionar unidades de memoria flash USB conectadas de forma local y unidades de disco duro para usarlas en las aplicaciones y los escritorios RDS. Otros dispositivos USB, entre los que se incluyen otros tipos de dispositivos de almacenamiento, no son compatibles con aplicaciones y escritorios RDS.

Cuando use esta función en grupos de escritorios que se implementan en máquinas de usuario único, la mayoría de los dispositivos USB que están conectados al sistema cliente están disponibles en el escritorio remoto. Incluso puede conectar un iPad y administrarlo desde un escritorio remoto. Por ejemplo, puede sincronizar el iPad con el iTunes que está instalado en el escritorio remoto. En algunos dispositivos cliente, como los equipos Windows y Mac, los dispositivos USB aparecen en un menú de Horizon Client. Este menú permite conectar y desconectar los dispositivos.

En la mayoría de los casos, no puede usar un dispositivo USB en el sistema cliente y en la aplicación o el escritorio remotos al mismo tiempo. Solo se pueden compartir algunos tipos de dispositivos USB entre el escritorio remoto y el equipo local. Estos dispositivos incluyen lectores de tarjetas inteligentes y dispositivos de interfaz humana, como teclados y dispositivos señaladores.

Los administradores pueden especificar los tipos de dispositivos USB a los que los usuarios finales pueden conectarse. En los dispositivos compuestos que contengan varios tipos de dispositivos, como un dispositivo de entrada de vídeo y uno de almacenamiento, en algunos sistemas cliente, los administradores pueden dividir el dispositivo, de forma que se permita un dispositivo (por ejemplo, el de entrada de vídeo) pero el otro no (por ejemplo, el de almacenamiento).

La función de redireccionamiento USB solo está disponible en algunos tipos de clientes. Para saber si es compatible con un tipo de cliente concreto, consulte la matriz de compatibilidad de funciones en el documento "Utilizar VMware Horizon Client" para el tipo específico de dispositivo de cliente móvil o de escritorio. Visite https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Importante Cuando implemente la función de redireccionamiento USB, puede realizar acciones para proteger a su organización de las vulnerabilidades que pueden afectar a los dispositivos USB. Consulte [Implementar dispositivos USB en un entorno de Horizon 7 seguro](#).

Este capítulo incluye los siguientes temas:

- [Limitaciones sobre los tipos de dispositivos USB](#)
- [Descripción general de la configuración del redireccionamiento USB](#)
- [Tráfico de red y redireccionamiento USB](#)
- [Conexiones automáticas a dispositivos USB](#)
- [Implementar dispositivos USB en un entorno de Horizon 7 seguro](#)
- [Usar archivos de registro para solucionar problemas y para determinar los ID de los dispositivos USB](#)
- [Usar directivas para controlar el redireccionamiento USB](#)
- [Solucionar los problemas del redireccionamiento USB](#)

Limitaciones sobre los tipos de dispositivos USB

Aunque Horizon 7 no evita de forma explícita que ningún dispositivo funcione en un escritorio remoto, algunos dispositivos funcionan mejor que otros debido a factores como el ancho de banda o la latencia de red. De forma predeterminada, algunos dispositivos están bloqueados o filtrados automáticamente para que no se usen.

En Horizon 6.0.1 junto con Horizon Client 3.1 o una versión posterior, puede conectar dispositivos USB 3.0 a puertos USB 3.0 de la máquina cliente en clientes Windows, Linux y Mac. Los dispositivos USB 3.0 solo son compatibles con una única transmisión. Dado que las transmisiones múltiples no se han implementado en esta versión, el rendimiento de los dispositivos USB no se mejoró. Es posible que algunos dispositivos USB 3.0 que requieren un rendimiento elevado constante para funcionar correctamente no funcionen en una sesión VDI debido a la latencia de red.

En versiones anteriores de View, aunque los dispositivos USB 3.0 Superspeed no son compatibles, los dispositivos USB 3.0 conectados a un puerto USB 2.0 de la máquina cliente suelen funcionar. Sin embargo, es posible que haya excepciones en función del tipo de conjunto de chips USB de la placa base del sistema cliente.

Es posible que los siguientes tipos de dispositivos no sean apropiados para redireccionamiento USB a un escritorio remoto implementado en una máquina de usuario único:

- Debido a los requisitos de ancho de banda de las cámaras web, que normalmente consumen más de 60 Mbps, estas no son compatibles con el redireccionamiento USB. Para las cámaras web, puede usar la función Audio/vídeo en tiempo real.

- 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, los dispositivos de entrada y salida de audio funcionarán de forma óptima con esa función y no necesitará utilizar el redireccionamiento USB con ellos.
- Las grabadoras de CD o DVD USB no son compatibles.
- El rendimiento de algunos dispositivos USB varía enormemente según la latencia de red y la fiabilidad, sobre todo en una red WAN. Por ejemplo, una única solicitud de lectura de un dispositivo de almacenamiento USB necesita tres recorridos de ida y vuelta entre el cliente y el escritorio remoto. Es posible que la lectura de un archivo completo requiera varias operaciones de lectura USB y, cuanto mayor sea la latencia, se empleará un tiempo de ida y vuelta mayor.

La estructura de archivos puede ser muy grande en función del formato. Las unidades de disco USB de gran tamaño pueden tardar varios minutos en aparecer en el escritorio. Formatear un dispositivo USB como NTFS en lugar de FAT ayuda a reducir el tiempo de conexión inicial. Un vínculo de red poco fiable provoca reintentos y esto reduce mucho el rendimiento.

Del mismo modo, los lectores de CD y DVD USB, los escáneres y los dispositivos táctiles como las tabletas para firmas no funcionan correctamente en una red latente como una red WAN.

- El redireccionamiento de escáneres USB depende del estado de la red, y es posible que los escaneados tarden más tiempo de lo normal en completarse.

Puede redireccionar los siguientes tipos de dispositivos a una aplicación o escritorio publicados en un host RDS:

- Unidades flash portátiles USB
- Discos duros USB

A partir de la versión 7.0.2 de Horizon 7, puede redireccionar los dispositivos de firma digital, los pedales de transcripción y algunas tabletas Wacom a una aplicación o un escritorio publicados. Estos dispositivos están deshabilitados de forma predeterminada en la versión 7.0.2 de Horizon 7. Para habilitarlos, elimine las opciones de la clave del Registro de Windows `ExcludeAllDevices` y `IncludeFamily` desde la siguiente ruta: `HKLM\Software\Policies\VMware, Inc\VMware VDM\Agent\USB`. Estos dispositivos están habilitados de forma predeterminada en la versión 7.0.3 de Horizon 7 y versiones posteriores.

No puede redireccionar otros tipos de dispositivos USB ni otros tipos de dispositivos de almacenamiento USB como unidades de almacenamiento de seguridad y de CD-ROM USB a una aplicación o escritorio publicados.

Descripción general de la configuración del redireccionamiento USB

Si quiere configurar su implementación para que los usuarios finales puedan conectar dispositivos extraíbles como unidades flash, cámaras y auriculares USB, debe instalar algunos componentes tanto en el escritorio remoto o el host RDS como en el dispositivo cliente y comprobar que la opción global para los dispositivos USB esté habilitada en View Administrator.

La lista de verificación incluye las tareas obligatorias y opcionales para configurar el redireccionamiento USB en su empresa.

La función de redireccionamiento USB está disponible solo en algunos tipos de clientes como Windows, Mac y clientes Linux suministrados por un partner. Para saber si es compatible con un tipo de cliente concreto, consulte la matriz de compatibilidad de funciones en el documento "Utilizar VMware Horizon Client" para el tipo específico de dispositivo de cliente. Visite https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Importante Cuando implemente la función de redireccionamiento USB, puede realizar acciones para proteger a su organización de las vulnerabilidades que pueden afectar a los dispositivos USB. Por ejemplo, puede usar la configuración de directiva de grupo para deshabilitar el redireccionamiento USB para algunos usuarios y escritorios remotos, o bien para restringir qué tipos de dispositivos USB se pueden redireccionar. Consulte [Implementar dispositivos USB en un entorno de Horizon 7 seguro](#).

- 1 Cuando ejecute el asistente de instalación de Horizon Agent en el host RDS o en el escritorio remoto de origen, asegúrese de incluir el componente de redireccionamiento USB.

De forma predeterminada, este componente no está seleccionado. Para instalar este componente, debe seleccionarlo.
- 2 Cuando ejecute el asistente de instalación de VMware Horizon Client en el sistema cliente, asegúrese de incluir el componente de redireccionamiento USB.

Este complemento está incluido de forma predeterminada.
- 3 Verifique que el acceso a los dispositivos USB desde una aplicación o un escritorio remoto esté habilitado en View Administrator.

En View Administrator, acceda a **Directivas > Directivas globales** y verifique que **Acceso USB** esté establecido en **Permitir**.
- 4 (Opcional) Configure las directivas de grupo de Horizon Agent para especificar qué tipos de dispositivos pueden redireccionarse.

Consulte [Usar directivas para controlar el redireccionamiento USB](#).
- 5 (Opcional) Establezca una configuración similar en el dispositivo cliente.

También puede configurar si los dispositivos están conectados automáticamente cuando Horizon Client se conecta a la aplicación o al escritorio remotos o cuando el usuario conecta un dispositivo USB. El método para establecer la configuración de USB en el dispositivo cliente depende del tipo de dispositivo. Por ejemplo, para los endpoints cliente de Windows, puede configurar las directivas de grupo, mientras que para los endpoints de Mac se usa un comando de línea de comandos. Para obtener instrucciones, consulte el documento "Usar VMware Horizon Client" para el tipo específico de dispositivo cliente.
- 6 Conecte los usuarios finales a una aplicación o escritorio remotos o bien conecte sus dispositivos USB al sistema cliente local.

Si el controlador para el dispositivo USB no está instalado en el host RDS o en el escritorio remoto, el sistema operativo cliente detecta el dispositivo USB y busca un controlador adecuado, como haría en un equipo físico Windows.

Tráfico de red y redireccionamiento USB

El redireccionamiento USB es independiente del protocolo de visualización y el tráfico USB normalmente usa el puerto TCP 32111. El tráfico de red entre un sistema cliente y una aplicación o escritorio remotos puede fluir en varias rutas en función de que el sistema cliente esté o no dentro de la red corporativa y de cómo el administrador eligiera configurar la seguridad.

Si el sistema cliente está dentro de la red corporativa y, por lo tanto, se puede establecer una conexión directa entre el cliente y la aplicación o el escritorio remotos, el tráfico USB usa el puerto TCP 32111.

Si el sistema cliente está fuera de la red corporativa, el cliente puede conectarse a través de un dispositivo de Unified Access Gateway o de un servidor de seguridad de la DMZ. Los dispositivos de Unified Access Gateway y los servidores de seguridad de la DMZ se comunican con las instancias del servidor de conexión dentro del firewall empresarial y proporcionan una capa adicional de seguridad, protegiendo las instancias del servidor de conexión de la parte pública de Internet.

No es necesario abrir puertos adicionales en el firewall para el tráfico USB si se utiliza un dispositivo de Unified Access Gateway (método preferido). En el caso de un servidor de seguridad, es necesario abrir el puerto TCP 32111 en el firewall para el tráfico USB. Para conocer todos los requisitos de los puertos del servidor de seguridad, consulte "Reglas del firewall para servidores de seguridad basados en DMZ" en el documento *Planificación de la arquitectura de View*.

Puede configurar la función de SDK de mejora de sesiones a través de USB para que no se abra el puerto TCP 32111. Consulte [Habilitar la función de SDK de mejora de sesiones a través de USB](#).

Nota Si se usa un cliente cero, el tráfico USB se redirecciona mediante un canal virtual PCoIP en lugar del puerto TCP 32111. La puerta de seguridad PCoIP encapsula y cifra los datos mediante el puerto TCP/UDP 4172. Si se usan clientes cero, no es necesario abrir el puerto TCP 32111.

Habilitar la función de SDK de mejora de sesiones a través de USB

Con la función de SDK de mejora de sesiones a través de USB, no es necesario que abra el puerto TCP 32111 para el tráfico USB. Esta función es compatible con escritorios virtuales y escritorios publicados en hosts RDS.

Para habilitar la función de SDK de mejora de sesiones a través de USB, abra el editor del Registro de Windows (regedit.exe) en el escritorio remoto, acceda a HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration y establezca la clave UsbVirtualChannelEnabled a true.

Cuando esta función esté habilitada, el tráfico USB puede utilizar la conexión TCP o Blast Extreme Adaptive Transport (BEAT) que utiliza el protocolo de visualización, o bien puede utilizar una conexión TCP o BEAT dedicada. La conexión que utiliza el tráfico USB depende de la configuración.

Por ejemplo, con el protocolo de visualización VMware Blast, el tráfico USB puede usar canal de VVC, el canal lateral de BEAT o el canal lateral de TCP. Con el protocolo de visualización PCoIP, el tráfico USB solamente utiliza el canal lateral de TCP.

De forma predeterminada, el canal lateral de TCP utiliza el puerto TCP 9427. El canal de VVC y el canal lateral de BEAT utilizan el mismo puerto que el protocolo de visualización VMware Blast.

Los contadores de USB que aparecen cuando utiliza PerfMon en agentes de Windows son válidos si el tráfico USB está configurado para utilizar el canal de VVC.

Si desea obtener más información sobre cómo utilizar el canal lateral de BEAT para el tráfico USB con VMware Blast, consulte [Activar el canal lateral de BEAT para el redireccionamiento de unidades cliente o USB](#).

Conexiones automáticas a dispositivos USB

En algunos sistemas cliente, los administradores, los usuarios finales o bien ambos pueden configurar conexiones automáticas de dispositivos USB a un escritorio remoto. Las conexiones automáticas se pueden realizar cuando el usuario conecta un dispositivo USB al sistema cliente o cuando el cliente se conecta al escritorio remoto.

Algunos dispositivos, como es el caso de los smartphones y las tablets, requieren conexiones automáticas porque estos dispositivos se reinician y, por consiguiente, se desconectan durante una actualización. Si estos dispositivos no se configuran para que se reconecten automáticamente al escritorio remoto, después de que los dispositivos se hayan reiniciado durante una actualización, se conectan al sistema cliente local en su lugar.

Las propiedades de configuración para conexiones USB automáticas que establecen los administradores en el cliente o que establecen usuarios finales mediante el uso de un elemento de menú de Horizon Client se aplican a todos los dispositivos USB salvo que estos estén configurados para que sean excluidos del redireccionamiento USB. Por ejemplo, en algunas versiones de cliente, las webcams y los micrófonos se excluyen de forma predeterminada del redireccionamiento USB porque estos dispositivos funcionan mejor mediante la función de audio/vídeo en tiempo real. En algunos casos, puede que no se excluya un dispositivo USB del redireccionamiento de forma predeterminada, pero puede que sea necesario que los administradores excluyan el dispositivo del redireccionamiento de forma explícita. Por ejemplo, los siguientes tipos de dispositivos USB no son buenos candidatos para el redireccionamiento USB y no se deben conectar automáticamente a un escritorio remoto:

- Dispositivos Ethernet USB. Si redirige un dispositivo Ethernet USB, su sistema cliente podría perder la conectividad de red si dicho dispositivo es el único dispositivo Ethernet.
- Dispositivos de pantalla táctil. Si redirige un dispositivo de pantalla táctil, el escritorio remoto recibirá la entrada táctil, pero no la del teclado.

Si ha configurado el escritorio remoto para que conecte automáticamente los dispositivos USB, puede configurar una directiva para que excluya dispositivos específicos, como pantallas táctiles y dispositivos de red. Si desea obtener más información, consulte [Configurar los ajustes de directiva de filtro para dispositivos USB](#).

En clientes Windows, como alternativa al uso de parámetros que conectan automáticamente todos los dispositivos salvo los excluidos, puede editar un archivo de configuración en el cliente que configure Horizon Client para que solo reconecte al escritorio remoto uno o varios dispositivos específicos, como smartphones y tablets. Para ver las instrucciones, consulte *Usar VMware Horizon Client para Windows*.

Implementar dispositivos USB en un entorno de Horizon 7 seguro

Los dispositivos USB pueden ser vulnerables ante una amenaza de seguridad llamada BadUSB, en la que el firmware de algunos dispositivos USB se puede piratear y reemplazar por un malware. Por ejemplo, un dispositivo puede estar pensado para redireccionar el tráfico de red o emular un teclado y capturar las pulsaciones de teclas. Puede configurar la función de redireccionamiento de USB para proteger la implementación de Horizon 7 ante esta vulnerabilidad de seguridad.

Al deshabilitar el redireccionamiento USB, puede evitar que se redirija todos los dispositivos USB a las aplicaciones y los escritorios de Horizon 7 de los usuarios. De forma alternativa, puede deshabilitar el redireccionamiento de dispositivos USB específicos, lo que permite que los usuarios tengan acceso únicamente a dispositivos específicos de las aplicaciones y los escritorios.

La decisión de realizar estos pasos depende de los requisitos de seguridad de su organización. Además, estos pasos no son obligatorios. Puede instalar el redireccionamiento USB y dejar la función habilitada para todos los dispositivos USB de la implementación de Horizon 7. Como mínimo, examine detenidamente hasta qué punto su organización debería intentar limitar su exposición a esta vulnerabilidad de seguridad.

Deshabilitar el redireccionamiento USB en todos los tipos de dispositivos

Algunos entornos de alta seguridad le piden que evite que se redirijan a las aplicaciones y los escritorios remotos todos los dispositivos USB conectados a los dispositivos cliente. Puede deshabilitar el redireccionamiento USB de todos los grupos de escritorios, de grupos de escritorios específicos o de usuarios específicos dentro de un grupo de escritorios.

Use la estrategia más adecuada según su situación:

- Cuando instala Horizon Agent en una imagen de escritorio o un host RDS, desmarque la opción de configuración **Redireccionamiento USB**. (La opción aparece desmarcada de forma predeterminada). Este enfoque no permite el acceso a dispositivos USB de todas las aplicaciones y los escritorios remotos que se implementan desde la imagen de escritorio o host RDS.
- En Horizon Administrator, edite la directiva **Acceso USB** de un grupo específico para permitir o rechazar el acceso. Con este enfoque, no es necesario que cambie la imagen de escritorio y puede controlar el acceso a los dispositivos USB de grupos de aplicaciones y escritorios específicos.

La directiva **Acceso USB** global solo está disponible para los grupos de aplicaciones y escritorios RDS. No puede establecer esta directiva para grupos de aplicaciones o RDS individuales.

- En View Administrator, después de establecer la directiva a nivel del grupo de aplicaciones o de escritorios, puede sobrescribirla para un usuario específico del grupo si selecciona la opción **Reemplazos del usuario** y selecciona al usuario.
- Establezca la directiva `Exclude All Devices` en **true** en Horizon Agent o en el cliente, según corresponda.
- Use Directivas de Smart para crear una directiva que deshabilite la opción de la directiva de Horizon **Redireccionamiento USB**. Con este enfoque, puede deshabilitar el redireccionamiento USB en un escritorio remoto específico si se cumplen ciertas condiciones. Por ejemplo, puede configurar una directiva que deshabilite el redireccionamiento USB cuando los usuarios se conecten a un escritorio remoto desde fuera de la red corporativa.

Si establece la directiva `Exclude All Devices` en **true**, Horizon Client no permite el redireccionamiento de todos los dispositivos USB. Puede usar otras opciones de directivas para permitir el redireccionamiento de familias de dispositivos o dispositivos específicos. Si establece la directiva en **false**, Horizon Client permite que se redireccionen todos los dispositivos USB, excepto aquellos que otras directivas bloquean. Puede establecer la directiva tanto en Horizon Agent como en Horizon Client. La siguiente tabla muestra cómo la directiva `Exclude All Devices`, que puede establecer para Horizon Agent y Horizon Client, se combina para generar una directiva efectiva en el equipo cliente. De forma predeterminada, se permite el redireccionamiento de todos los dispositivos USB, a menos que estén bloqueados.

Tabla 4-1. Efecto de combinar las directivas de exclusión de todos los dispositivos

Directivas de exclusión de todos los dispositivos en Horizon Agent	Directiva de exclusión de todos los dispositivos en Horizon Client	Directiva combinada de exclusión efectiva de todos los dispositivos
false o no definida (incluye todos los dispositivos USB)	false o no definida (incluye todos los dispositivos USB)	Incluir todos los dispositivos USB
false (incluye todos los dispositivos USB)	true (excluye todos los dispositivos USB)	Excluir todos los dispositivos USB
true (excluye todos los dispositivos USB)	Cualquiera o sin definir	Excluir todos los dispositivos USB

Si estableció la directiva `Disable Remote Configuration Download` en **true**, el valor de `Exclude All Devices` en Horizon Agent no se envía a Horizon Client, pero Horizon Agent y Horizon Client aplican el valor local de `Exclude All Devices`.

Estas directivas se incluyen en el archivo de plantilla ADMX de la configuración de Horizon Agent (`vdm_agent.admx`).

Deshabilitar el redireccionamiento USB de dispositivos específicos

Es posible que algunos usuarios tengan que redireccionar dispositivos USB específicos conectados de forma local para poder realizar tareas en las aplicaciones o escritorios remotos. Por ejemplo, un médico puede usar un dictáfono USB para grabar la información médica de los pacientes. En estos casos, no puede deshabilitar el acceso a todos los dispositivos USB. Puede usar la configuración de la directiva de grupo si desea habilitar o deshabilitar el redireccionamiento USB de dispositivos específicos.

Antes de habilitar el redireccionamiento USB para dispositivos específicos, compruebe que confíe en los dispositivos físicos que están conectados a los equipos clientes de su empresa. Asegúrese también de que confíe en la cadena de suministros. Si es posible, realice un seguimiento de una cadena de custodia de los dispositivos USB.

Además, forme a sus empleados para asegurarse de que no se conecten a dispositivos de origen desconocido. Si es posible, restrinja los dispositivos de su entorno a aquellos que solo aceptan actualizaciones de firmware firmadas, que tienen una certificación de Nivel 3 de FIPS 140-2 y que no admiten ningún tipo de firmware de campos actualizables. Es complicado ubicar el origen de este tipo de dispositivos USB y, según los requisitos del dispositivo, puede que no los encuentre. Es posible que estas opciones no sean prácticas, pero merece la pena tenerlas en cuenta.

Cada dispositivo USB tiene sus propios ID de proveedor y de producto que lo identifica en el equipo. Al establecer las opciones de la directiva de grupo de la configuración de Horizon Agent, puede establecer una directiva de inclusión para los tipos de dispositivos conocidos. Con este enfoque, elimina el riesgo de permitir que se introduzcan dispositivos desconocidos en el entorno.

Por ejemplo, puede prohibir el redireccionamiento de todos los dispositivos a la aplicación o el escritorio remotos, excepto los ID de producto y de proveedor de un dispositivo conocido, vid/pid=0123/abcd:

```
ExcludeAllDevices    Enabled
IncludeVidPid        o:vid-0123_pid-abcd
```

Nota Aunque esta configuración de ejemplo proporciona protección, pero un dispositivo en peligro puede informar sobre cualquier vid/pid, por lo que es posible que aún se produzca un ataque.

De forma predeterminada, Horizon 7 bloquea el redireccionamiento de algunas familias de dispositivos a la aplicación o el escritorio remotos. Por ejemplo, se bloquean los dispositivos de interfaz de usuario (HID) y los teclados para que no aparezcan en el invitado. Algunos códigos BadUSB publicados pueden dirigirse a teclados USB.

Puede prohibir el redireccionamiento de algunas familias de dispositivos específicas a la aplicación o el escritorio remotos. Por ejemplo, puede bloquear todos los dispositivos de almacenamiento masivo, de audio y de vídeo:

```
ExcludeDeviceFamily  o:video;audio;storage
```

También puede crear una lista blanca si prohíbe que se redireccionen todos los dispositivos, pero permite que se utilice una familia de dispositivos específica. Por ejemplo, puede bloquear todos los dispositivos excepto los de almacenamiento:

```
ExcludeAllDevices    Enabled
IncludeDeviceFamily   o:storage
```

Puede producirse otro riesgo si un usuario remoto inicia sesión en una aplicación o un escritorio y lo infecta. Puede prohibir el acceso USB a las conexiones de Horizon 7 que se inicien fuera del firewall corporativo. El dispositivo USB se puede usar de forma interna, pero no de forma externa.

Tenga en cuenta que si bloquea el puerto TCP 32111 para deshabilitar el acceso externo de los dispositivos USB, la sincronización de la zona horaria no funcionará, ya que este puerto también se usa para dicha sincronización. Para clientes cero, el tráfico USB está incrustado en un canal virtual en el puerto UDP 4172. Dado que el puerto 4172 se utiliza para el protocolo de visualización y para el redireccionamiento USB, no puede bloquearlo. Si es necesario, puede deshabilitar el redireccionamiento USB de los clientes cero. Para obtener más información, consulte la documentación del producto del cliente cero o póngase en contacto con el proveedor de dicho cliente.

Si configura las directivas para que bloqueen ciertas familias de dispositivos o dispositivos específicos, puede ayudar a disminuir el riesgo de infección por parte un malware BadUSB. Estas directivas no disminuyen todos los riesgos, pero pueden ser eficaces dentro de la estrategia de seguridad general.

Usar archivos de registro para solucionar problemas y para determinar los ID de los dispositivos USB

Los archivos de registro de los USB que son de ayuda se encuentran en el sistema cliente y en el host RDS o el sistema operativo del escritorio remoto. Use los archivos de registro que se encuentran en ambas ubicaciones para solucionar los problemas. Para encontrar los ID de producto de los dispositivos específicos, use los registros que se encuentran en el cliente.

Si está configurando el filtrado o la división de los dispositivos USB o si está examinando por qué un dispositivo en particular no aparece en un menú de Horizon Client, consulte los registros que se encuentran en el cliente. El servicio USB de Horizon View y el árbitro USB proporcionan los registros del cliente. De forma predeterminada, el registro está habilitado en clientes Windows y Linux. En clientes Mac, el registro está deshabilitado de forma predeterminada. Para habilitar el registro en clientes Mac, consulte el documento *Uso de VMware Horizon Client para Mac*.

Cuando configure las directivas para dividir y filtrar los dispositivos USB, algunos valores que estableció requieren el VID (ID de proveedor) y el PID (ID de producto) del dispositivo USB. Para encontrar el VID y el PID, puede realizar una búsqueda en Internet con el nombre del producto combinado con vid y pid. De forma alternativa, puede consultar el archivo de registro del cliente después de conectar dicho dispositivo USB al sistema local cuando Horizon Client se está ejecutando. La siguiente tabla muestra la ubicación predeterminada de los archivos de registro.

Tabla 4-2. Ubicaciones de los archivos de registro

Cliente o agente	Ruta a los archivos de registro
Cliente de Windows	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt
Cliente Mac	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /Library/Logs/VMware/vmware-usbarbitrator-xxxx.log
Cliente Linux	(Ubicación predeterminada) /tmp/vmware-root/vmware-view-usbd-*.log

Si se produce un problema con el dispositivo después de que se redirija a la aplicación o al escritorio remotos, consulte los registros del agente y del cliente.

Usar directivas para controlar el redireccionamiento USB

Puede configurar directivas de USB para la aplicación o el escritorio remotos (Horizon Agent) y para Horizon Client. Estas directivas especifican si el dispositivo cliente debe dividir los dispositivos USB compuestos en componentes independientes para el redireccionamiento. Puede dividir dispositivos para restringir los tipos de dispositivos USB que el cliente hace que estén disponibles para su redireccionamiento, y para que Horizon Agent no reenvíe ciertos dispositivos USB a un equipo cliente.

Si tiene instaladas versiones anteriores de Horizon Agent o Horizon Client, no todas las funciones de las directivas del redireccionamiento USB están disponibles. [Tabla 4-3. Compatibilidad de la configuración de las directivas de USB](#) muestra cómo Horizon 7 aplica las directivas para diferentes combinaciones de Horizon Agent y de Horizon Client.

Tabla 4-3. Compatibilidad de la configuración de las directivas de USB

Versión de Horizon Agent	Versión de Horizon Client	Efecto de la configuración de las directivas USB en el redireccionamiento USB
5.1 o posterior	5.1 o posterior	<p>La configuración de las directivas de USB se puede aplicar tanto a Horizon Agent como a Horizon Client. Puede usar la configuración de las directivas de USB Horizon Agent para bloquear el reenvío de los dispositivos USB a un escritorio. Horizon Agent puede enviar la configuración de directivas de filtrado y de división de dispositivos a Horizon Client. Puede usar la configuración de las directivas de USB de Horizon Client para que no se reenvíen los dispositivos USB de un equipo cliente a un escritorio.</p> <p>Nota En View Agent 6.1 o versiones posteriores, así como en Horizon Client 3.3 o versiones posteriores, esta configuración de las directivas de redireccionamiento USB se aplica a las aplicaciones y los escritorios RDS, así como a los escritorios remotos que se ejecutan en máquinas de usuario único.</p>
5.1 o posterior	5.0.x o anterior	<p>La configuración de las directivas de USB se aplica a Horizon Agent únicamente. Puede usar la configuración de las directivas de USB Horizon Agent para bloquear el reenvío de los dispositivos USB a un escritorio. No puede usar la configuración de las directivas de USB Horizon Client para controlar los dispositivos que se puedan redireccionar de un equipo cliente a un escritorio. Horizon Client no puede recibir la configuración de directivas de filtrado y de división de dispositivos desde Horizon Agent. La configuración existente del registro para el redireccionamiento USB en Horizon Client sigue siendo válida.</p>
5.0.x o anterior	5.1 o posterior	<p>La configuración de las directivas de USB se aplica a Horizon Client únicamente. Puede usar la configuración de las directivas de USB de Horizon Client para que no se reenvíen los dispositivos USB de un equipo cliente a un escritorio. No puede usar la configuración de las directivas de USB de Horizon Agent para bloquear el reenvío de los dispositivos USB a un escritorio. Horizon Agent no puede enviar la configuración de directivas de filtrado y de división de dispositivos a Horizon Client.</p>
5.0.x o anterior	5.0.x o anterior	<p>No se aplica la configuración de las directivas de USB. La configuración existente del registro para el redireccionamiento USB en Horizon Client sigue siendo válida.</p>

Si actualiza Horizon Client, cualquier configuración existente del registro para el redireccionamiento USB, como `HardwareIdFilters`, sigue siendo válida para definir las directivas USB para Horizon Client.

En los dispositivos cliente que no admiten las directivas de USB del cliente, puede usar las directivas de USB para que Horizon Agent controle los dispositivos USB que se pueden redireccionar desde el cliente a una aplicación o a un escritorio.

Configurar los ajustes de directiva de división de dispositivo para dispositivos USB compuestos

Los dispositivos USB compuestos consisten en una combinación de dos o varios dispositivos diferentes, como un dispositivo de entrada de vídeo y un dispositivo de almacenamiento o un micrófono y un mouse. Si quiere permitir que uno o varios de los componentes estén disponibles para su redireccionamiento, puede dividir el dispositivo compuesto en sus interfaces de componentes, excluir interfaces específicas del redireccionamiento e incluir otras.

Puede establecer una directiva que divida automáticamente dispositivos compuestos. Si no funciona la división automática de dispositivos para un dispositivo determinado o si la división automática no produce los resultados que necesita su aplicación, puede dividir los dispositivos compuestos manualmente.

División automática de dispositivos

Si habilita la división automática de dispositivos, Horizon 7 intentará dividir las funciones o dispositivos en un dispositivo compuesto conforme a las reglas de filtro que haya en efecto. Por ejemplo, un micrófono de dictado podría dividirse automáticamente para que el mouse siga siendo local para el cliente, mientras que el resto de dispositivos se reenvía al escritorio remoto.

En la siguiente tabla, se muestra cómo el valor del ajuste `Allow Auto Device Splitting` determina si Horizon Client intenta dividir automáticamente los dispositivos USB compuestos. La división automática está deshabilitada de forma predeterminada.

Tabla 4-4. Efecto de combinar las directivas de división automática deshabilitadas

Directiva Permitir división automática de dispositivos en Horizon Agent	Directiva Permitir división automática de dispositivos en Horizon Client	Directiva Permitir división automática de dispositivos combinada efectiva
Allow – Default Client Setting	falso (división automática deshabilitada)	División automática deshabilitada
Allow – Default Client Setting	verdadero (división automática habilitada)	División automática habilitada
Allow – Default Client Setting	Sin definir	División automática habilitada
Allow – Override Client Setting	Cualquiera o sin definir	División automática habilitada
Sin definir	Sin definir	División automática deshabilitada

Nota Estas directivas se incluyen en el archivo de plantilla ADMX de configuración de Horizon Agent. El archivo de plantilla ADMX se denomina (`vdm_agent.admx`).

De forma predeterminada, Horizon 7 deshabilita la división automática y excluye del redireccionamiento todos los componentes de salida de audio, teclado, mouse o tarjeta inteligente de un dispositivo USB compuesto.

Horizon 7 aplica los ajustes de la directiva de división de dispositivos antes de aplicar ningún ajuste de directiva de filtro. Si tiene habilitada la división automática y no excluye de la división a un dispositivo USB compuesto especificando su ID de producto y proveedor, Horizon 7 examina cada una de las interfaces del dispositivo USB compuesto para decidir qué interfaces deben excluirse o incluirse de acuerdo con los ajustes de directiva de filtro. Si ha deshabilitado la división automática de dispositivos y no especifica de forma explícita los ID de proveedor y producto de un dispositivo USB compuesto que quiera dividir, Horizon 7 aplica los ajustes de directiva de filtro a todo el dispositivo.

Si habilita la división automática, puede usar la directiva `Exclude Vid/Pid Device From Split` para especificar los dispositivos USB compuestos que quiere excluir de la división.

División manual de dispositivos

Puede usar la directiva `Split Vid/Pid Device` para especificar los ID de proveedor y producto de un dispositivo USB compuesto que quiera dividir. También puede especificar las interfaces de los componentes de un dispositivo USB compuesto que quiera excluir del redireccionamiento. Horizon 7 no aplica ningún ajuste de directiva de filtro a componentes que excluya de esta manera.

Importante Si usa la directiva `Split Vid/Pid Device`, Horizon 7 no incluye automáticamente los componentes que no haya excluido de forma explícita. Debe especificar una directiva de filtrado como `Include Vid/Pid Device` para incluir estos componentes.

[Tabla 4-5. Modificadores de división para los ajustes de directiva de división de dispositivos en Horizon Agent](#) muestra los modificadores que especifican cómo Horizon Client gestiona un ajuste de directiva de división de dispositivos de Horizon Agent si hay un ajuste de directiva de división de dispositivos equivalente para Horizon Client. Estos modificadores se aplican a todos los ajustes de directiva de división de dispositivos.

Tabla 4-5. Modificadores de división para los ajustes de directiva de división de dispositivos en Horizon Agent

Editor	Descripción
m (combinar, del inglés "merge")	Horizon Client aplica el ajuste de directiva de división de dispositivos de Horizon Agent además del ajuste de directiva de división de dispositivos de Horizon Client.
o (invalidar, del inglés "override")	Horizon Client usa el ajuste de directiva de división de Horizon Agent en lugar del ajuste de directiva de división de dispositivos de Horizon Client.

En [Tabla 4-6. Ejemplos de aplicar modificadores de división a los ajustes de directiva de división de dispositivos](#), se muestran ejemplos de cómo Horizon Client procesa los ajustes de `Exclude Device From Split by Vendor/Product ID` cuando especifica diferentes modificadores de división.

Tabla 4-6. Ejemplos de aplicar modificadores de división a los ajustes de directiva de división de dispositivos

Excluir dispositivo de la división mediante el ID de proveedor/producto en Horizon Agent	Excluir dispositivo de la división mediante el ID de proveedor/producto en Horizon Client	Ajuste de directiva de exclusión efectiva de dispositivo de la división mediante el ID de proveedor/producto usado por Horizon Client
m:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX
m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY

Horizon Agent no aplica los ajustes de directiva de división de dispositivos en su lado de la conexión.

Horizon Client evalúa los ajustes de directiva de división de dispositivos en el siguiente orden de precedencia.

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

Un ajuste de directiva de división de dispositivos que excluye un dispositivo de la división tiene precedencia frente a cualquier ajuste de directiva para dividir el dispositivo. Si excluye cualquier interfaz o dispositivo de la división, Horizon Client excluye los dispositivos de componentes correspondientes del redireccionamiento.

Ejemplos de establecer directivas para dividir dispositivos USB compuestos

Establezca directivas de división para escritorios para excluir del redireccionamiento dispositivos con ID de proveedor y producto específicos tras la división automática y pase estas directivas a los equipos de cliente:

- Para Horizon Agent, establezca la directiva Allow Auto Device Splitting en Allow – Override Client Setting.
- Para Horizon Agent, establezca la directiva Exclude VidPid From Split en **o:vid-xxx_pid-yyyy**, donde xxx y yyyy son los ID apropiados.

Permita la división automática de dispositivos para escritorios y especifique directivas para dividir dispositivos específicos en equipos cliente:

- Para Horizon Agent, establezca la directiva Allow Auto Device Splitting en Allow – Override Client Setting.
- Para el dispositivo cliente, establezca la directiva de filtro Include Vid/Pid Device para que incluya que quiere dividir, por ejemplo, **vid-0781_pid-554c**.

- Para el dispositivo cliente, establezca la directiva Split Vid/Pid Device en **vid-0781_pid-554c(exintf:00;exintf:01)** por ejemplo, de modo que divida un dispositivo USB compuesto especificado para que se excluyan del redireccionamiento las interfaces 00 y 01.

Configurar los ajustes de directiva de filtro para dispositivos USB

Los ajustes de directiva de filtro que configure para Horizon Agent y Horizon Client establecen qué dispositivos USB se pueden redirigir desde un equipo cliente hasta una aplicación o escritorio remotos. A menudo, las empresas usan el filtrado de dispositivos USB para deshabilitar el uso de dispositivos de almacenamiento en escritorios remotos o para bloquear el reenvío de un tipo específico de dispositivo, como un adaptador USB a Ethernet que conecte el dispositivo de cliente al escritorio remoto.

Al conectarse a un escritorio o aplicación, Horizon Client descarga los ajustes de directiva USB de Horizon Agent y los usa junto con los ajustes de directiva USB de Horizon Client para decidir qué dispositivos USB le permitirá redireccionar desde el equipo cliente.

Horizon 7 aplica todos los ajustes de directiva de división de dispositivos antes de aplicar los ajustes de directiva de filtro. Si ha dividido un dispositivo USB compuesto, Horizon 7 examina cada una de las interfaces del dispositivo para decidir qué se debería excluir o incluir de acuerdo con los ajustes de directiva de filtro. Si no ha dividido un dispositivo USB compuesto, Horizon 7 aplica los ajustes de directiva de filtro en todo el dispositivo.

Las directivas de división de dispositivos se incluyen en el archivo de plantilla ADMX de configuración de Horizon Agent (`vdm_agent.admx`).

Interacción de ajustes USB aplicados por el agente

La siguiente tabla muestra los modificadores que especifican cómo Horizon Client gestiona un ajuste de directiva de filtro de Horizon Agent para un ajuste aplicable por el agente si existe un ajuste de directiva de filtro equivalente para Horizon Client.

Tabla 4-7. Modificadores de filtros para ajustes aplicables por el agente

Editor	Descripción
m (combinar, del inglés "merge")	Horizon Client aplica los ajustes de directivas de filtro de Horizon Agent además de los ajustes de directivas de filtro de Horizon Client. En el caso de ajustes booleanos, o verdadero/falso, si no se ha establecido la directiva de cliente, se utilizan los ajustes del agente. Si se ha establecido la directiva de cliente, se ignoran los ajustes del agente, salvo en el caso del ajuste <code>Exclude All Devices</code> . Si se ha establecido la directiva <code>Exclude All Devices</code> en el lado del agente, la directiva reemplaza el ajuste de cliente.
o (invalidar, del inglés "override")	Horizon Client usa el ajuste de directiva de filtro de Horizon Agent en lugar del ajuste de directiva de filtro de Horizon Client.

Por ejemplo, la siguiente directiva en el lado del agente invalida cualquier regla de inclusión en el lado de cliente y solo se aplicará al dispositivo VID-0911_PID-149a una regla de inclusión:

```
IncludeVidPid: o:VID-0911_PID-149a
```

También puede usar asteriscos como caracteres comodín; por ejemplo: **o:vid-0911_pid-******

Importante Si configura el lado de agente sin el modificador **o** o **m**, la regla de configuración se considera no válida y se ignorará.

Interacción de ajustes USB interpretados por el cliente

La siguiente tabla muestra los modificadores que especifican cómo Horizon Client gestiona un ajuste de directiva de filtro de Horizon Agent para un ajuste interpretado por el cliente.

Tabla 4-8. Modificadores de filtros para ajustes interpretados por el cliente

Editor	Descripción
Default (d en el ajuste del registro)	Si no existe un ajuste de directiva de filtro de Horizon Client, Horizon Client usa el ajuste de directiva de filtro de Horizon Agent. Si existe un ajuste de directiva de filtro de Horizon Client, Horizon Client aplica ese ajuste de directiva e ignora el ajuste de directiva de filtro de Horizon Agent.
Override (o en el ajuste del registro)	Horizon Client usa el ajuste de directiva de filtro de Horizon Agent en lugar de cualquier ajuste de directiva de filtro de Horizon Client equivalente.

Horizon Agent no aplica el ajuste de directiva de filtro para ajustes interpretados por el cliente en su lado de la conexión.

En la siguiente tabla, se muestran ejemplos de cómo procesa Horizon Client los ajustes de Allow Smart Cards cuando usted especifica diferentes modificadores de filtros.

Tabla 4-9. Ejemplos de aplicar modificadores de filtros a ajustes interpretados por el cliente

Ajuste Permitir tarjetas inteligentes en Horizon Agent	Ajuste Permitir tarjetas inteligentes en Horizon Client	Ajuste de directiva efectiva Permitir tarjetas inteligentes usada por Horizon Client
Disable – Default Client Setting (d:false en el ajuste del registro)	true (Permitir)	true (Permitir)
Disable – Override Client Setting (o:false en el ajuste del registro)	true (Permitir)	false (Deshabilitar)

Si establece la directiva Disable Remote Configuration Download en **true**, Horizon Client ignora todos los ajustes de directiva de filtros que reciba de Horizon Agent.

Horizon Agent siempre aplica los ajustes de directiva de filtros de los ajustes aplicables por el agente en su lado de la conexión, incluso aunque configure Horizon Client para que use otro ajuste de directiva de filtros o deshabilite la descarga por parte de Horizon Client de ajustes de directiva de filtros desde Horizon Agent. Horizon Client no informa de que Horizon Agent impide el reenvío de un dispositivo.

Precedencia de ajustes

Horizon Client evalúa los ajustes de directiva de filtro en un determinado orden de precedencia. Un ajuste de directiva de filtro que impide que se redireccione un dispositivo tiene preferencia sobre un ajuste de directiva de filtro equivalente que incluye al dispositivo. Si Horizon Client no encuentra un ajuste de directiva de filtro para excluir un dispositivo, Horizon Client permite el redireccionamiento del dispositivo salvo que haya establecido la directiva `Exclude All Devices` en **true**. No obstante, si ha configurado un ajuste de directiva de filtro en Horizon Agent para que excluya el dispositivo, el escritorio o la aplicación bloquea cualquier intento de redireccionar el dispositivo hacia él.

Horizon Client evalúa los ajustes de directiva de filtro en orden de precedencia, teniendo en cuenta los ajustes de Horizon Client y los ajustes de Horizon Agent junto con los valores de modificador que aplique a los ajustes de Horizon Agent. En la siguiente lista, se muestra el orden de precedencia, donde el elemento n.º 1 tiene la precedencia más alta.

- 1 `Exclude Path`
- 2 `Include Path`
- 3 `Exclude Vid/Pid Device`
- 4 `Include Vid/Pid Device`
- 5 `Exclude Device Family`
- 6 `Include Device Family`
- 7 `Allow Audio Input Devices`, `Allow Audio Output Devices`, `Allow HIDBootable`, `Allow HID (Non Bootable and Not Mouse Keyboard)`, `Allow Keyboard and Mouse Devices`, `Allow Smart Cards` y `Allow Video Devices`
- 8 Directiva de `Exclude All Devices` efectiva combinada evaluada para excluir o incluir todos los dispositivos USB

Puede establecer los ajustes de directiva de filtro `Exclude Path` y `Include Path` solo para Horizon Client. Los ajustes de directiva de filtro `Allow` que hacen referencia a distintas familias de dispositivos tienen la misma precedencia.

Si configura un ajuste de directiva para que excluya dispositivos basándose en los valores de ID de proveedor y producto, Horizon Client excluirá los dispositivos cuyos ID de proveedor y producto coincidan con este ajuste de directiva, aunque puede que haya configurado un ajuste de directiva `Allow` para la familia a la que pertenece el dispositivo.

El orden de precedencia de los ajustes de directivas resuelve los conflictos entre ellos. Si configura `Allow Smart Cards` para que permita el redireccionamiento de tarjetas inteligentes, cualquier ajuste de directiva de exclusión con mayor precedencia invalidará esta directiva. Por ejemplo, puede que haya configurado un ajuste de directiva `Exclude Vid/Pid Device` para que excluya los dispositivos de tarjeta inteligente que tengan una ruta de acceso o ID de proveedor y producto coincidentes o puede que haya configurado un ajuste de la directiva `Exclude Device Family` que también excluye por completo la familia de dispositivos `smart-card`.

Si ha configurado cualquier ajuste de directiva de filtro de Horizon Agent, Horizon Agent evalúa y aplica los ajustes de directiva de filtro en el siguiente orden de precedencia en el escritorio o aplicación remotos, donde el elemento n.º 1 tiene la precedencia más alta.

- 1 Exclude Vid/Pid Device
- 2 Include Vid/Pid Device
- 3 Exclude Device Family
- 4 Include Device Family
- 5 Directiva Exclude All Devices aplicada por el agente establecida para excluir o incluir todos los dispositivos USB

Horizon Agent aplica este conjunto limitado de ajustes de directiva de filtro en su lado de la conexión.

Mediante la definición de ajustes de directiva de filtro para Horizon Agent, puede crear una directiva de filtrado para equipos de cliente no administrados. La función también le permite impedir el reenvío de dispositivos desde equipos cliente, incluso aunque los ajustes de directiva de filtro para Horizon Client permitan el redireccionamiento.

Por ejemplo, si configura una directiva que permita a Horizon Client permitir el redireccionamiento de un dispositivo, Horizon Agent bloquea el dispositivo si configura una directiva para que Horizon Agent excluya el dispositivo.

Ejemplos de establecer directivas para filtrar dispositivos USB

Los ID de proveedor y producto utilizados en estos ejemplos son solo ejemplos. Para obtener información sobre cómo determinar el ID de proveedor y producto de un dispositivo determinado, consulte [Usar archivos de registro para solucionar problemas y para determinar los ID de los dispositivos USB](#).

- En el cliente, excluya del redireccionamiento un dispositivo determinado:

```
Exclude Vid/Pid Device:    Vid-0341_Pid-1a11
```

- Bloquee el redireccionamiento de todos los dispositivos de almacenamiento hacia este grupo de escritorios o aplicaciones. Use un ajuste de lado de agente:

```
Exclude Device Family:    o:storage
```

- Para todos los usuarios de un grupo de escritorios, bloquee los dispositivos de audio y vídeo para asegurarse de que estos dispositivos estén siempre disponibles para la función Audio/vídeo en tiempo real. Use un ajuste de lado de agente:

```
Exclude Device Family:    o:video;audio
```

Otra estrategia consistiría en excluir dispositivos específicos por ID de proveedor y producto.

- En el cliente, bloquee el redireccionamiento de todos los dispositivos menos uno:

```
Exclude All Devices:      true
Include Vid/Pid Device:   Vid-0123_Pid-abcd
```

- Excluya todos los dispositivos creados por una empresa determinada porque estos dispositivos causan problemas a sus usuarios finales. Use un ajuste de lado de agente:

```
Exclude Vid/Pid Device:   o:Vid-0341_Pid-*
```

- En el cliente, incluya dos dispositivos específicos, pero excluya todos los demás:

```
Exclude All Devices:      true
Include Vid/Pid Device:   Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

Familias de dispositivos USB

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

Nota Algunos dispositivos no pertenecen a ninguna familia de dispositivos.

Tabla 4-10. Familias de dispositivos USB

Nombre de la familia de dispositivos	Descripción
audio	Cualquier dispositivo de entrada o salida de audio.
audio-in	Dispositivos de entrada de audio como micrófonos.
audio-out	Dispositivos de salida de audio como auriculares y altavoces.
bluetooth	Dispositivos conectados por Bluetooth.
comm	Dispositivos de comunicaciones como, por ejemplo, módems y adaptadores de red por cable.
hid	Dispositivos de interfaz de usuario, sin contar con teclados y dispositivos de señalización.
hid-bootable	Dispositivos de interfaz de usuario, que están disponibles durante el inicio, sin contar con teclados y dispositivos de señalización.
imaging	Dispositivos de imagen, como escáneres.
keyboard	Dispositivo de teclado.
mouse	Dispositivo de señalización, como un mouse.
other	Familia no especificada.
pda	Asistentes digitales personales.
physical	Dispositivos Force Feedback, como joysticks Force Feedback.
printer	Dispositivos de impresión.
security	Dispositivos de seguridad, como lectores de huella digital.
smart-card	Dispositivos de tarjeta inteligente.

Nombre de la familia de dispositivos	Descripción
storage	Dispositivos de almacenamiento masivo, como unidades flash y unidades de disco duro externas.
unknown	Familia no conocida.
vendor	Dispositivos con funciones específicas del proveedor.
video	Dispositivos de entrada de vídeo.
wireless	Adaptadores de red inalámbricos.
wusb	Dispositivos USB inalámbricos.

Opciones para los USB en la plantilla ADMX de configuración de Horizon Agent

Puede definir la configuración de la directiva de los USB para Horizon Agent y Horizon Client. Mientras está conectado, Horizon Client descarga la configuración de directivas USB desde Horizon Agent 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 la máquina cliente.

El archivo de plantilla ADMX de configuración de Horizon Agent contiene las opciones de configuración de las directivas relacionadas con los componentes de entorno y de autenticación de Horizon Agent, como el redireccionamiento USB. El archivo de plantilla ADMX se denomina (`vdm_agent.admx`). La configuración se aplica a nivel de equipo. De forma preferencial, Horizon Agent 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\Agent\USB`.

Opciones para configurar la división del dispositivo USB

La siguiente tabla describe las opciones de configuración de las directivas para dividir dispositivos USB compuestos en el archivo de plantilla ADMX de configuración de Horizon Agent. Todas estas opciones de configuración están en la carpeta **Configuración de VMware Horizon Agent > Configuración USB de View > Ajustes de solo descarga del cliente** del Editor de administración de directivas de grupo. Horizon Agent no aplica estas opciones. Horizon Agent envía las opciones a Horizon Client para que las interprete y las aplique según especifique el modificador para combinar (m) o para sobrescribir (o). Horizon Client usa la configuración para decidir si es necesario dividir los dispositivos USB compuestos en dispositivos componentes y si es necesario excluir los dispositivos componentes del redireccionamiento. Para obtener una descripción sobre cómo Horizon aplica las directivas para dividir dispositivos USB compuestos, consulte [Configurar los ajustes de directiva de división de dispositivo para dispositivos USB compuestos](#).

Tabla 4-11. Plantilla de configuración de Horizon Agent: opciones para dividir el dispositivo

Configuración	Propiedades
Allow Auto Device Splitting Propiedad: AllowAutoDeviceSplitting	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 Propiedad: SplitExcludeVidPid	Excluye un dispositivo USB compuesto especificado mediante los ID de producto y proveedor procedentes de la división. El formato de la configuración es {m o}: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: o:vid-0781_pid-55** El valor predeterminado no está definido.
Split Vid/Pid Device Propiedad: SplitVidPid	Trata los componentes de un dispositivo USB compuesto especificado por los ID del producto y del proveedor como dispositivos distintos. El formato de la configuración es {m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) o {m o}: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: o:vid-0781_pid-554c(exintf:01;exintf:02) Nota Horizon 7 no incluye automáticamente los componentes que no excluyó explícitamente. Debe especificar una directiva de filtrado como Include Vid/Pid Device para incluir estos componentes. El valor predeterminado no está definido.

Opciones de USB que aplica Horizon Agent

La siguiente tabla describe las opciones de directivas que aplica el agente para los USB y que se encuentran en el archivo de plantilla ADMX de configuración de Horizon Agent. Todas estas configuraciones se encuentran en la carpeta **Configuración de VMware Horizon Agent > Configuración USB de View** del Editor de administración de directivas de grupo. Horizon Agent usa las opciones para decidir si un dispositivo USB se puede reenviar a la máquina del host. Horizon Agent también envía las opciones a Horizon Client para interpretarlas y aplicarlas según especifique el modificador para combinar (m) o para sobrescribir (o). Horizon Client usa la configuración para decidir si un dispositivo USB está disponible para su redireccionamiento. Como Horizon Agent siempre aplica la opción de la directiva aplicada por el agente que especifique, el efecto puede contrarrestar la directiva que estableció para Horizon Client. Para obtener una descripción sobre cómo Horizon 7 aplica las directivas para filtrar dispositivos USB, consulte [Configurar los ajustes de directiva de filtro para dispositivos USB](#).

Tabla 4-12. Plantilla de configuración de Horizon Agent: opciones aplicadas por el agente

Configuración	Propiedades
Exclude All Devices Propiedad: ExcludeAllDevices	<p>Excluye el reenvío de todos los dispositivos USB. Si está configurado como true, puede usar otras opciones de directivas para permitir el reenvío de dispositivos o familias de dispositivos específicas. Si está configurado como false, puede usar otras opciones de directivas para evitar el reenvío de dispositivos o familias de dispositivos específicas.</p> <p>Si está configurado como true y se envía a Horizon Client, esta opción siempre sobrescribe la opción de Horizon Client. No puede usar el modificador para combinar (m) o para sobrescribir (o) con esta opción.</p> <p>El valor predeterminado no está definido, lo que equivale a false.</p>
Exclude Device Family Propiedad: ExcludeFamily	<p>Excluye el reenvío de familias de dispositivos. El formato de la opción es {m o}:<i>nombre_familia_1</i>[:<i>nombre_familia_2</i>]...</p> <p>Por ejemplo: o:bluetooth;smart-card</p> <p>Si habilitó la división automática de dispositivos, Horizon 7 examinará la familia de dispositivos de cada interfaz de un USB compuesto para decidir cuál debe excluir. Si deshabilitó la división automática de dispositivos, Horizon 7 examinará la familia de dispositivos de todo el USB compuesto.</p> <p>El valor predeterminado no está definido.</p>
Exclude Vid/Pid Device Propiedad: ExcludeVidPid	<p>Excluye el reenvío de dispositivos con los ID de producto y de proveedor específicos. El formato de la configuración es {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...</p> <p>Debe especificar los números ID en hexadecimales. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Por ejemplo: m:vid-0781_pid-****;vid-0561_pid-554c</p> <p>El valor predeterminado no está definido.</p>
Include Device Family Propiedad: IncludeFamily	<p>Incluye familias de dispositivos que se pueden reenviar. El formato de la opción es {m o}:<i>nombre_familia_1</i>[:<i>nombre_familia_2</i>]...</p> <p>Por ejemplo: m:storage</p> <p>El valor predeterminado no está definido.</p>
Include Vid/Pid Device Propiedad: IncludeVidPid	<p>Incluye el reenvío de dispositivos con los ID de producto y de proveedor específicos. El formato de la configuración es {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...</p> <p>Debe especificar los números ID en hexadecimales. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID.</p> <p>Por ejemplo: o:vid-0561_pid-554c</p> <p>El valor predeterminado no está definido.</p>

Configuración USB interpretada por el cliente

La siguiente tabla describe las opciones de directivas que interpreta el cliente del archivo de plantilla ADMX de configuración de Horizon Agent. Todas estas opciones de configuración están en la carpeta **Configuración de VMware Horizon Agent > Configuración USB de View > Ajustes de solo descarga del cliente** del Editor de administración de directivas de grupo. Horizon Agent no aplica estas opciones. Horizon Agent envía las opciones a Horizon Client para que las interprete y las aplique. Horizon Client usa la configuración para decidir si un dispositivo USB está disponible para su redireccionamiento.

Tabla 4-13. Plantilla de configuración de Horizon Agent: opciones interpretadas por el cliente

Configuración	Propiedades
Allow Audio Input Devices Propiedad: AllowAudioIn	Permite que se reenvíen los dispositivos de entrada de audio. El valor predeterminado no está definido, lo que equivale a true .
Allow Audio Output Devices Propiedad: AllowAudioOut	Permite que se reenvíen los dispositivos de salida de audio. El valor predeterminado no está definido, lo que equivale a false .
Allow HID-Bootable Propiedad: AllowHIDBootable	Permite que se reenvíen otros dispositivos de entrada que no sean dispositivos de teclado o de 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 Other Input Devices	Permite el reenvío de dispositivos de entrada que no sean dispositivos con arranque HID o teclados con dispositivos señaladores integrados. El valor predeterminado no está definido.
Allow Keyboard and Mouse Devices Propiedad: AllowKeyboardMouse	Permite que se reenvíen 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 Propiedad: AllowSmartcard	Permite que se reenvíen los dispositivos de tarjeta inteligente. El valor predeterminado no está definido, lo que equivale a false .
Allow Video Devices Propiedad: AllowVideo	Permite que se reenvíen los dispositivos de vídeo. El valor predeterminado no está definido, lo que equivale a true .

Solucionar los problemas del redireccionamiento USB

Pueden aparecer varios problemas relacionados con el redireccionamiento USB en Horizon Client.

Problema

El redireccionamiento USB de Horizon Client no puede hacer que los dispositivos locales estén disponibles en el escritorio remoto, o bien algunos dispositivos no aparecen disponibles para redireccionarlos en Horizon Client.

Causa

Las siguientes pueden ser causas por las que el redireccionamiento USB no funcione correctamente o como se esperaba.

- El dispositivo es un dispositivo USB compuesto y uno de los dispositivos que incluye se bloquea de forma predeterminada. Por ejemplo, un dispositivo de dictado que incluye un mouse se bloquea de forma predeterminada porque los dispositivos de mouse se bloquean de forma predeterminada. Para solucionar este problema, consulte "Configurar los ajustes de directiva de división de dispositivo para dispositivos USB compuestos" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

- El redireccionamiento USB no es compatible en hosts Windows Server 2008 RDS que implementan aplicaciones y escritorios remotos. El redireccionamiento USB es compatible con los hosts Windows Server 2012 RDS con View Agent 6.1 y versiones posteriores, pero solo para los dispositivos de almacenamiento USB. El redireccionamiento USB es compatible en sistemas Windows Server 2008 R2 y Windows Server 2012 R2 que se usan como escritorios de usuario único.
- Únicamente los discos duros y las unidades flash USB son compatibles con aplicaciones y escritorios RDS. No puede redireccionar otros tipos de dispositivos USB ni otros tipos de dispositivos de almacenamiento USB como unidades de almacenamiento de seguridad y de CD-ROM USB a una aplicación o escritorio RDS.
- Las cámaras web no son compatibles con el redireccionamiento.
- 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 aunque estén inactivos.
- El redireccionamiento USB no es compatible con los dispositivos de arranque. Si ejecuta Horizon Client en un sistema Windows que se arranca desde un dispositivo USB y redirecciona este dispositivo al escritorio remoto, el sistema operativo local no se podrá usar o no responderá. Consulte <http://kb.vmware.com/kb/1021409>.
- De forma predeterminada, Horizon Client para Windows no le permite seleccionar los dispositivos de salida de audio, de tarjetas inteligente, de mouse y de teclado para su redireccionamiento. Consulte <http://kb.vmware.com/kb/1011600>.
- RDP no admite el redireccionamiento de HID USB para la sesión de la consola o para los lectores de tarjeta inteligente. Consulte <http://kb.vmware.com/kb/1011600>.
- El Centro de dispositivos de Windows Mobile puede evitar el redireccionamiento de dispositivos USB en las sesiones RDP. Consulte <http://kb.vmware.com/kb/1019205>.
- Para algunos HID USB, debe configurar la máquina virtual para que actualice la posición del puntero del mouse. Consulte <http://kb.vmware.com/kb/1022076>.
- Es posible que algunos dispositivos de audio necesiten cambios en la configuración de las directivas o de los registros. Consulte <http://kb.vmware.com/kb/1023868>.
- La latencia de red puede causar una lenta interacción del dispositivo o que las aplicaciones aparezcan bloqueadas porque se diseñaron para interactuar con dispositivos locales. Las unidades de disco USB de gran tamaño pueden tardar varios minutos en aparecer en el Explorador de Windows.
- Las tarjetas flash USB con el formato del sistema de archivos FAT32 son lentas para realizar operaciones de carga. Consulte <http://kb.vmware.com/kb/1022836>.
- Un proceso o un servicio del sistema local abre el dispositivo después de conectarlo a la aplicación o al escritorio remotos.
- Un dispositivo USB redireccionado deja de funcionar si vuelve a conectar una sesión de aplicación o de escritorio, aunque la aplicación o el escritorio muestren que el dispositivo está disponible.
- El redireccionamiento USB está deshabilitado en Horizon Administrator.

- Los controladores de redireccionamiento USB no se encuentran o están deshabilitados en el invitado.

Solución

- ◆ Si está disponible, use PCoIP como protocolo en lugar de RDP.
- ◆ Si un dispositivo redireccionado sigue sin estar disponible o deja de funcionar después de una desconexión temporal, elimine el dispositivo, vuelva a conectarlo y vuelva a intentar el redireccionamiento.
- ◆ En Horizon Administrator, acceda a **Directivas > Directivas globales** y verifique que Acceso USB esté establecido como **Permitir** en Directivas de View.
- ◆ Examine las entradas de clase `ws_vhub` en el registro del invitado y las entradas de clase `vmware-view-usbd` en el registro del cliente.

Las entradas con esas clases se escriben en los registros si un usuario no es un administrador, o bien si los controladores del redireccionamiento USB no están instalados o no funcionan. Para conocer la ubicación de estos archivos de registro, consulte el apartado sobre cómo usar los archivos de registro para solucionar problemas y para determinar los ID de los dispositivos USB en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

- ◆ Abra el Administrador de dispositivos en el invitado, expanda los controladores Bus serie universal y vuelva a instalar los controladores VMware View Virtual USB Host Controller y VMware View Virtual USB Hub si no se encuentran o vuelva a habilitarlos si están deshabilitados.

Configurar directivas para grupos de escritorios y aplicaciones

5

Puede configurar directivas para controlar el comportamiento de grupos de escritorios y aplicaciones, máquinas y usuarios. Horizon Administrator permite establecer directivas para las sesiones de cliente. Puede usar los ajustes de directiva de grupo de Active Directory para controlar el comportamiento de Horizon Agent, Horizon Client para Windows y funciones que afectan a las máquinas de un único usuario, hosts RDS, PCoIP, o VMware Blast.

Este capítulo incluye los siguientes temas:

- [Establecer directivas en Horizon Administrator](#)
- [Usar Directivas de Smart](#)
- [Usar las directivas de grupo de Active Directory](#)
- [Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7](#)
- [Archivos de plantilla ADMX de Horizon 7](#)
- [Agregar los archivos de plantilla ADMX a Active Directory](#)
- [Opciones de la plantilla ADMX de configuración de VMware View Agent](#)
- [Configuración de directiva de VMware Virtualization Pack para Skype Empresarial](#)
- [Configuración de directivas de PCoIP](#)
- [Configuración de la directiva VMware Blast](#)
- [Usar Servicios de Escritorio remoto de directivas de grupo](#)
- [Filtrar las impresoras por impresión virtual](#)
- [Configurar impresión según ubicación](#)
- [Ejemplo de directiva de grupo de Active Directory](#)

Establecer directivas en Horizon Administrator

Horizon Administrator permite configurar directivas para las sesiones de cliente.

Puede establecer estas directivas para que afecten a usuarios específicos, a grupos de escritorios específicos o a todos los usuarios de las sesiones de cliente. Las directivas que afectan a grupos de escritorios y usuarios específicos se denominan directivas de nivel de usuario y directivas de nivel de grupo. Las directivas que afectan a todas las sesiones y usuarios se denominan directivas globales.

Las directivas de nivel de usuario heredan la configuración de las directivas de nivel de grupo. De forma similar, las directivas de nivel de grupo de escritorio heredan la configuración de las directivas globales equivalentes. La configuración de la directiva de nivel de escritorio tiene preferencia sobre la configuración de la directiva global equivalente. La configuración de la directiva de nivel de usuario tiene preferencia sobre la configuración de la directiva global equivalente y la directiva de nivel de grupo de escritorios.

La configuración de la directiva de nivel inferior puede ser más o menos restrictiva que la configuración de nivel superior equivalente. Por ejemplo, puede establecer una directiva global en **Denegar** y la directiva equivalente de nivel del grupo de escritorios en **Permitir** o viceversa.

Nota Solo las directivas globales están disponibles para los grupos de aplicaciones y los escritorios RDS. No puede establecer directivas de nivel de usuario ni de nivel de grupo para los grupos de aplicaciones y los escritorios RDS.

Configurar las opciones de la directiva global

Puede configurar directivas globales a fin de controlar el comportamiento de todos los usuarios de sesiones cliente.

Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Directivas > Directivas globales**.
- 2 Haga clic en **Editar directivas** en el panel **Directivas de View**.
- 3 Haga clic en **Aceptar** para guardar los cambios.

Configurar directivas para los grupos de escritorios

Puede configurar directivas en el nivel de escritorios para que afecten a grupos de escritorios específicos. La configuración de las directivas en el nivel de escritorios tiene preferencia sobre la configuración de directivas global equivalente.

Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.

- 2 Haga doble clic en el ID del grupo de escritorios y haga clic en la pestaña **Directivas**.

La pestaña **Directivas** muestra la configuración de directivas actual. Cuando se hereda una opción de la directiva global equivalente, **Heredada** aparece en la columna **Directiva del grupo de escritorios**.

- 3 Haga clic en **Editar directivas** en el panel **Directivas de View**.
- 4 Haga clic en **Aceptar** para guardar los cambios.

Configurar directivas para los usuarios

Puede configurar directivas en el nivel de usuarios para que afecten a usuarios específicos. La configuración de la directiva a nivel de usuario siempre tiene preferencia ante la configuración de directivas global equivalente y las directivas en el nivel de grupo de escritorios.

Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo de escritorios y haga clic en la pestaña **Directivas**.
La pestaña **Directivas** muestra la configuración de directivas actual. Cuando se hereda una opción de la directiva global equivalente, **Heredada** aparece en la columna **Directiva del grupo de escritorios**.
- 3 Haga clic en **Reemplazos del usuario** y, a continuación, en **Agregar usuario**.
- 4 Para buscar un usuario, haga clic en **Agregar**, escriba el nombre o la descripción del usuario y, a continuación, haga clic en **Buscar**.
- 5 Seleccione uno o varios usuarios de la lista, haga clic en **Aceptar** y, a continuación, en **Siguiente**.
Aparece el cuadro de diálogo Agregar directiva individual.
- 6 Configure las directivas de Horizon y haga clic en **Finalizar** para guardar los cambios.

Directivas de Horizon 7

Puede configurar las directivas de Horizon 7 para que afecten a todas las sesiones de cliente, o bien puede aplicarlas para que afecten a usuarios o grupos de escritorios específicos.

[Tabla 5-1. Directivas de Horizon](#) describe cada opción de las directivas de Horizon 7.

Tabla 5-1. Directivas de Horizon

Directiva	Descripción
Redireccionamiento multimedia (MMR)	<p>Determina si MMR está habilitado para los sistemas cliente.</p> <p>MMR es un filtro de Windows Media Foundation que reenvía datos multimedia desde códecs específicos que se encuentran en escritorios remotos directamente a través de un socket TCP al sistema cliente. Los datos se descodifican directamente en el sistema cliente, donde se reproducen.</p> <p>El valor predeterminado es Denegar.</p> <p>Si los sistemas cliente no tienen recursos suficientes para administrar la descodificación multimedia local, mantenga la opción como Denegar.</p> <p>Los datos del redireccionamiento multimedia (MMR) se envían a través de la red sin cifrado basado en las aplicaciones y pueden contener datos confidenciales, dependiendo del contenido que se redirija. Para asegurarse de que esta información no se supervise en la red, use MMR únicamente en una red segura.</p>
Acceso USB	<p>Determina si los escritorios remotos pueden usar los dispositivos USB conectados al sistema cliente.</p> <p>El valor predeterminado es Permitir. Para evitar el uso de dispositivos externos por seguridad, cambie la opción a Denegar.</p>
Aceleración de hardware PColP	<p>Determina si desea habilitar la aceleración del hardware del protocolo de visualización PColP y especifica la prioridad de aceleración que está asignada a la sesión del usuario de PColP.</p> <p>Esta opción solo tiene efecto si el dispositivo de aceleración del hardware PColP se encuentra en el equipo físico que aloja el escritorio remoto.</p> <p>El valor predeterminado es Permitir con la prioridad Media.</p>

Usar Directivas de Smart

Puede usar Directivas de Smart para crear directivas que controlen el comportamiento del redireccionamiento USB, la impresión virtual, el redireccionamiento del portapapeles, el redireccionamiento de la unidad cliente y las funciones del protocolo de visualización PColP en escritorios remotos específicos. También puede utilizar Directivas de Smart para crear directivas que controlen el comportamiento de las aplicaciones publicadas.

Con Directivas de Smart, puede crear directivas que se apliquen únicamente si se cumplen ciertas condiciones. Por ejemplo, puede configurar una directiva que deshabilite la función del redireccionamiento de la unidad cliente si un usuario se conecta a un escritorio remoto desde un lugar que no se encuentre dentro de la red corporativa.

Requisitos de Directivas de Smart

Para usar Directivas de Smart, su entorno de Horizon 7 tiene que cumplir algunos requisitos.

- Debe instalar Horizon Agent 7.0 o versiones posteriores y VMware User Environment Manager 9.0 y versiones posteriores en los escritorios remotos que desee administrar con Directivas de Smart.
- Los usuarios deben usar Horizon Client 4.0 o versiones posteriores para conectarse a los escritorios remotos que administre con Directivas de Smart.

Instalar User Environment Manager

Si quiere usar Directivas de Smart para controlar el comportamiento de las funciones de escritorios remotos en un escritorio remoto, debe instalar la versión de User Environment Manager 9.0 o posterior en el escritorio remoto.

Puede descargar el programa instalador de User Environment Manager desde la página de descargas de VMware. Debe instalar el componente de cliente VMware UEM FlexEngine en cada escritorio remoto que quiera administrar con User Environment Manager. Puede instalar el componente Consola de administración de User Environment Manager en cualquier escritorio desde el que quiera administrar el entorno de User Environment Manager.

En un grupo de clones vinculados, instale User Environment Manager en la máquina virtual principal que use como imagen de base para los clones vinculados. En un grupo de escritorios RDS, instale User Environment Manager en el host RDS que proporcione las sesiones de escritorios RDS.

Para conocer los requisitos del sistema y las instrucciones de instalación completas de User Environment Manager, consulte el documento de *Guía del administrador de User Environment Manager*.

Configurar User Environment Manager

Debe configurar User Environment Manager antes de poder usarlo para crear directivas inteligentes para funciones de escritorios remotos.

Para configurar User Environment Manager, siga las instrucciones de configuración en el *Guía del administrador de User Environment Manager*. Los siguientes pasos de configuración complementan la información incluida en dicho documento.

- Al configurar el componente de cliente VMware UEM FlexEngine en escritorios remotos, cree scripts de inicio y cierre de sesión para FlexEngine. Use el parámetro **–HorizonViewMultiSession –r** para el script de inicio de sesión y el parámetro **–HorizonViewMultiSession –s** para el script de cierre de sesión.

Nota No utilice scripts de inicio de sesión para iniciar otras aplicaciones en un escritorio remoto. Los scripts de inicio de sesión adicionales pueden demorar hasta en 10 minutos el inicio de sesión en el escritorio remoto.

- Habilite el ajuste de directivas de grupo Ejecutar scripts de inicio de sesión de forma sincrónica en escritorios remotos. Este ajuste se encuentra en la carpeta Configuración de usuario\Directivas\Plantillas administrativas\Sistema\Scripts.
- Habilite el ajuste de directivas de grupo del equipo Esperar siempre la detección de red al inicio del equipo y de sesión en escritorios remotos. Este ajuste se encuentra en la carpeta Configuración del equipo\Plantilla administrativa\Sistema\Inicio de sesión.
- En el caso de escritorios remotos con Windows 8.1, deshabilite el ajuste de directiva de grupo del equipo Configurar retraso de script de inicio de sesión. Este ajuste se encuentra en la carpeta Configuración del equipo\Plantillas administrativas\Sistema\Directiva de grupo.

- Para garantizar que se actualicen los ajustes de la directiva de Horizon Smart cuando los usuarios se reconecten a sesiones de escritorio, use la Consola de administración de User Environment Manager para crear una tarea desencadenada. Establezca el desencadenador en **Reconectar la sesión**, establezca la acción en **Actualización del entorno de usuario** y seleccione **Directivas de Horizon Smart** para la actualización.

Nota Si crea la tarea desencadenada mientras un usuario tiene la sesión iniciada en el escritorio remoto, este debe cerrar la sesión en el escritorio para que tenga efecto la tarea desencadenada.

Opciones de directivas inteligentes de Horizon

Para controlar el comportamiento de las funciones de escritorio remoto en User Environment Manager, cree una directiva inteligente de Horizon.

[Tabla 5-2. Opciones de directivas inteligentes de Horizon](#) describe las opciones que puede seleccionar cuando define una directiva inteligente de Horizon en User Environment Manager.

Tabla 5-2. Opciones de directivas inteligentes de Horizon

Configuración	Descripción
Redireccionamiento USB	Determina si el redireccionamiento USB está habilitado en el escritorio remoto. La función de redireccionamiento USB permite a los usuarios utilizar los dispositivos USB conectados de forma local (cámaras, impresoras o unidades flash portátiles) en el escritorio remoto.
Imprimir	Determina si la impresión virtual está habilitada en el escritorio remoto. La función de impresión virtual permite a los usuarios imprimir desde el escritorio remoto mediante una impresora virtual o USB que esté conectada al equipo cliente.
Portapapeles	<p>Determina la dirección en la que se permite el redireccionamiento del portapapeles. Puede seleccionar uno de estos valores:</p> <ul style="list-style-type: none"> ■ Deshabilitar. Deshabilita el redireccionamiento del portapapeles en ambas direcciones. ■ Permitir todo. Habilita el redireccionamiento del portapapeles. Los usuarios pueden copiar y pegar desde el sistema cliente al escritorio remoto y viceversa. ■ Permitir copia desde cliente a agente. Los usuarios pueden copiar y pegar solo desde el sistema cliente al escritorio remoto. ■ Permitir copia desde agente a cliente. Los usuarios pueden copiar y pegar solo desde el escritorio remoto al sistema cliente.
Redireccionamiento de unidades cliente	<p>Determina si el redireccionamiento de unidades cliente está habilitado en el escritorio remoto y si las carpetas y las unidades compartidas pueden editarse. Puede seleccionar uno de estos valores:</p> <ul style="list-style-type: none"> ■ Deshabilitar. Deshabilita el redireccionamiento de unidades cliente en el escritorio remoto. ■ Permitir todo. Las carpetas y unidades cliente se comparten con el escritorio remoto y pueden leerse y editarse. ■ Solo lectura. Las carpetas y unidades cliente se comparten con el escritorio remoto y pueden leerse pero no editarse. <p>Si no configura esta opción, dependerá de las opciones de registro local si las carpetas y las unidades compartidas pueden o no editarse. Si desea obtener más información, consulte Usar las opciones del registro para configurar el redireccionamiento de la unidad cliente.</p>

Configuración	Descripción
Perfil de ancho de banda	Configura un perfil de ancho de banda para las sesiones de Blast y PCoIP en el escritorio remoto. Puede seleccionar un perfil de ancho de banda predefinido, por ejemplo, LAN . Al seleccionar un perfil de ancho de banda predefinido, se evita que el agente intente realizar transmisiones a una velocidad mayor que la capacidad del vínculo. Si selecciona el perfil predeterminado, el ancho de banda máximo es de 90.000 kilobits por segundo. Si desea obtener más información, consulte Referencia del perfil de ancho de banda .
Transferencia de archivos de HTML Access	Determina la transferencia de archivos HTML entre cliente y agente.

En general, las opciones de directivas inteligentes de Horizon que configure para funciones de escritorios remotos en User Environment Manager anulan cualquier opción de directivas de grupo y cualquier clave de registro equivalentes.

Referencia del perfil de ancho de banda

Con las directivas de Smart, puede usar la opción de directiva de perfil de ancho de banda para configurar un perfil de ancho de banda para las sesiones de PCoIP o de Blast en escritorios remotos.

Tabla 5-3. Perfiles de ancho de banda

Perfil de ancho de banda	Ancho de banda máximo de sesión (Kbps)	Ancho de banda mínimo de sesión (Kbps)	Habilitar BTL	Calidad inicial máxima de la imagen	Calidad mínima de la imagen	Fotografías por segundo	Ancho de banda máximo de audio (Kbps)	Rendimiento de la calidad de la imagen
LAN de alta velocidad	900000	100	Sí	100	50	60	1600	50
LAN	900000	100	Sí	90	50	30	1600	50
WAN dedicada	900000	100	No	80	40	30	500	50
WAN de banda ancha	5000	100	No	70	40	20	500	50
WAN de baja velocidad	2000	100	No	70	30	15	200	25
Conexión de velocidad extremadamente lenta	1000	100	No	70	30	5	90	0

Agregar condiciones a las definiciones de directivas de Horizon Smart

Al definir una directiva de Horizon Smart en User Environment Manager, puede agregar condiciones que se deben cumplir para que la directiva tenga efecto. Por ejemplo, puede agregar una condición que deshabilite la función de redireccionamiento de unidad cliente solo en el caso de que un usuario se conecte al escritorio remoto desde fuera de la red corporativa.

Puede agregar varias condiciones para la misma función de escritorio remoto. Por ejemplo, puede agregar una condición que habilite la impresión local si un usuario es miembro del grupo de RR.HH.y otra condición que habilite la impresión local si el escritorio remoto está en el grupo Win7.

Para obtener información detallada sobre cómo agregar y editar condiciones en la Consola de administración de User Environment Manager, consulte la *Guía del administrador de User Environment Manager*.

Usar la condición de propiedad de Horizon Client

Cuando un usuario se conecta o reconecta a un escritorio remoto, Horizon Client recopila información sobre el equipo cliente y el servidor de conexión envía dicha información al escritorio remoto. Puede agregar la condición Propiedad de Horizon Client a una definición de directiva de Horizon para controlar cuándo tiene efecto la directiva basándose en la información que recibe el escritorio remoto.

Nota La condición Propiedad de Horizon Client solo es efectiva si un usuario inicia el escritorio remoto con el protocolo de visualización PCoIP del protocolo de visualización de VMware Blast. Si un usuario inicia el escritorio remoto con el protocolo de visualización RDP, la condición Propiedad de Horizon Client no tiene efecto.

[Tabla 5-4. Propiedades predefinidas para la condición de propiedad de Horizon Client](#) describe las propiedades predefinidas que se pueden seleccionar del menú desplegable **Propiedades** al utilizar la condición Propiedad de Horizon Client. Cada propiedad predefinida se corresponde con una clave del registro ViewClient_.

Tabla 5-4. Propiedades predefinidas para la condición de propiedad de Horizon Client

Propiedad	Clave del registro correspondiente	Descripción
Ubicación de cliente	ViewClient_Broker_GatewayLocation	<p>Especifica la ubicación del sistema de cliente de usuario. Los valores válidos son los siguientes:</p> <ul style="list-style-type: none"> ■ Interno: la directiva solo tiene efecto si un usuario se conecta al escritorio remoto desde dentro de la red corporativa. ■ Externo: la directiva solo tiene efecto si un usuario se conecta al escritorio remoto desde fuera de la red corporativa. <p>Para obtener información sobre la configuración de la ubicación de puerta de enlace para un host de servidor de seguridad o servidor de conexión, consulte el documento <i>Administración de View</i>.</p> <p>Para obtener información sobre el ajuste de la ubicación de puerta de enlace para un dispositivo de Access Point, consulte el documento <i>Implementación y configuración de Unified Access Gateway</i>.</p>
Etiquetas de inicio	ViewClient_Launch_Matched_Tags	<p>Especifica una o varias etiquetas. Para separar varias etiquetas, utilice una coma o punto y coma. La directiva se aplica solo si la etiqueta que permitió que se produjese el inicio del escritorio o la aplicación coincide con una de las etiquetas especificadas.</p> <p>Para obtener información sobre cómo asignar etiquetas a instancias del servidor de conexión y grupos de escritorios, consulte el documento de configuración.</p>
Nombre de grupo	ViewClient_Launch_ID	<p>Especifica un ID de grupo de aplicaciones o de escritorios. La directiva solo se aplica si el ID del grupo de escritorios o de aplicaciones que seleccionó el usuario al iniciar la aplicación o el escritorio remotos coincide con el ID especificado del grupo de aplicaciones o de escritorios. Por ejemplo, si el usuario seleccionó el grupo Win7 y esta propiedad se establece en Win7, la directiva tiene efecto.</p> <p>Nota Si se inicia más de un grupo de aplicaciones en la misma sesión de host RDS, el valor es el ID de la primera aplicación que se inicia desde Horizon Client.</p>

El menú desplegable **Propiedades** también es un cuadro de texto y se puede introducir en él cualquier clave del registro ViewClient_. No incluya el prefijo ViewClient_ al introducir la clave del registro. Por ejemplo, para especificar ViewClient_Broker_URL, escriba Broker_URL.

Puede utilizar el Editor del registro de Windows (regedit.exe) en el escritorio remoto para ver las claves del registro ViewClient_. Horizon Client escribe información del equipo cliente en la ruta de registro del sistema HKEY_CURRENT_USER\Volatile Environment en los escritorios remotos que se implementen en equipos de un solo usuario. En el caso de los escritorios remotos que se implementen en sesiones de RDS, Horizon Client escribe la información del equipo cliente en la ruta de registro del sistema HKEY_CURRENT_USER\Volatile Environment\x, donde x es el ID de sesión en el host RDS.

Uso de otras condiciones

La Consola de administración de User Environment Manager proporciona muchas condiciones. Las siguientes condiciones pueden ser especialmente útiles al crear directivas para funciones de escritorios remotos.

Miembro de grupo	Puede utilizar esta condición para configurar la directiva para que solo tenga efecto si un usuario es miembro de un grupo específico.
Protocolo de visualización remota	Puede utilizar esta condición para configurar la directiva para que solo tenga efecto si el usuario selecciona un protocolo de visualización específico. Los ajustes de la condición incluyen RDP, PCoIP y Blast.
Dirección IP	Puede utilizar esta condición para configurar la directiva para que solo tenga efecto si un usuario se conecta desde dentro o fuera de la red corporativa. Utilice los ajustes de la condición para especificar un rango de direcciones IP internas o un rango de direcciones IP externas.

Nota También puede utilizar la propiedad **Ubicación de cliente** en la condición Propiedad de Horizon Client.

Para obtener descripciones de todas las condiciones disponibles, consulte el documento *Guía del administrador de User Environment Manager*.

Crear una directiva de Horizon Smart en User Environment Manager

La Consola de administración de User Environment Manager se utiliza para crear una directiva de Horizon Smart en User Environment Manager. Al definir una directiva de Horizon Smart, puede agregar condiciones que se deben cumplir para que la directiva de Smart tenga efecto.

Requisitos previos

- Instalar y configurar User Environment Manager. Consulte [Instalar User Environment Manager](#) y [Configurar User Environment Manager](#).
- Familiarícese con los ajustes de la directiva de Horizon Smart. Consulte [Opciones de directivas inteligentes de Horizon](#).
- Familiarícese con las condiciones que puede agregar a las definiciones de directivas de Horizon Smart. Consulte [Agregar condiciones a las definiciones de directivas de Horizon Smart](#).

Para obtener información completa sobre el uso de la Consola de administración de User Environment Manager, consulte el documento *Guía del administrador de User Environment Manager*.

Procedimiento

- 1 En la Consola de administración de User Environment Manager, seleccione la pestaña **Entorno de usuario** y haga clic en **Directivas de Horizon Smart** en la vista de árbol.

Si hubiese definiciones de directivas de Horizon Smart existentes, se mostrarían en el panel Directivas de Horizon Smart.

- 2 Haga clic con el botón secundario en **Directivas de Horizon Smart** y seleccione **Crear definición de directiva de Horizon Smart** para crear una nueva directiva de Smart.

Se muestra el cuadro de diálogo Directiva de Horizon Smart.

- 3 Seleccione la pestaña **Configuración** y defina los ajustes de directiva de Smart.

- a En la sección Configuración general, escriba un nombre para la directiva de Smart en el cuadro de texto **Nombre**.

Por ejemplo, si la directiva de Smart afecta a la función de redireccionamiento de unidades cliente, puede darle a la directiva de Smart el nombre de CDR.

- b En la sección Configuración de directivas de Horizon Smart, seleccione los ajustes y las funciones de escritorio remoto que se deben incluir en la directiva de Smart.

Puede seleccionar varias funciones de escritorio remoto.

- 4 (opcional) Para agregar una condición a la directiva de Smart, seleccione la pestaña **Condiciones**, haga clic en **Agregar** y seleccione una condición.

Puede agregar múltiples condiciones a una definición de directiva de Smart.

- 5 Haga clic en **Guardar** para guardar la directiva de Smart.

User Environment Manager procesa la directiva de Horizon Smart cada vez que un usuario se conecta o reconecta al escritorio remoto.

User Environment Manager procesa varias directivas de Smart en orden alfabético basándose en el nombre de la directiva de Smart. Las directivas de Horizon Smart aparecen en orden alfabético en el panel Directivas de Horizon Smart. Si las directivas de Smart entran en conflicto, tiene precedencia la última directiva de Smart que se procesó. Por ejemplo, si tiene una directiva de Smart denominada Sue que habilite el redireccionamiento USB para el usuario denominado Sue y otra directiva de Smart denominada Pool que deshabilite el redireccionamiento USB del grupo de escritorios denominado Win7, la función de redireccionamiento USB se habilita cuando Sue se conecta a un escritorio remoto en el grupo de escritorios Win7.

Usar las directivas de grupo de Active Directory

Puede usar la Directiva de grupo de Microsoft Windows para optimizar y asegurar los escritorios remotos, para controlar el comportamiento de los componentes de Horizon 7 y para configurar la impresión según ubicación.

La Directiva de grupo es una función de los sistemas operativos Microsoft Windows que proporciona una configuración y administración centralizadas de los equipos y los usuarios remotos de un entorno de Active Directory.

La configuración de las directivas de grupo se encuentra en entidades denominadas objetos de directiva de grupo (GPO). Los GPO están asociados a objetos de Active Directory. Puede aplicar los GPO a componentes de Horizon 7 a nivel de dominio para controlar varias áreas del entorno de Horizon 7. Después de que se apliquen, la configuración de los GPO se almacena en el Registro de Windows local del componente especificado.

Puede usar el Editor de objetos de directiva de grupo de Microsoft Windows para administrar la configuración de la directiva de grupo. El Editor de objetos de directiva de grupo es un complemento de Microsoft Management Console (MMC). La MMC es parte de la Consola de administración de directivas de grupo de Microsoft (GPMC). Consulte el sitio web de Microsoft TechNet para obtener más información sobre cómo instalar y usar la GPMC.

Crear una OU para los escritorios remotos

Cree una unidad organizativa en Active Directory específicamente para los escritorios remotos.

Para evitar que se apliquen los ajustes de directiva de grupo en otros servidores de Windows u otras estaciones de trabajo en el mismo dominio que los escritorios remotos, cree un GPO para las directivas de grupo de Horizon 7 y vincúlelo a la OU que contenga los escritorios remotos.

Consulte la documentación de Microsoft Active Directory en el sitio web de Microsoft TechNet para obtener información sobre la creación de OU y GPO.

Habilitar procesamiento de bucle invertido para escritorios remotos

De forma predeterminada, las opciones de configuración de directiva de usuario proceden del conjunto de GPO que se aplican al objeto de usuario de Active Directory. Sin embargo, en el entorno de Horizon 7, los GPO se aplican a los usuarios según el equipo en el que inicien sesión.

Cuando habilita el procesamiento de bucle invertido, un conjunto consistente de directivas se aplica a todos los usuarios que inician sesión en un equipo determinado, independientemente de su ubicación en Active Directory.

Consulte la documentación de Active Directory de Microsoft para obtener información sobre la habilitación del procesamiento de bucle invertido.

Nota El procesamiento de bucle invertido es solo un enfoque para gestionar los GPO en Horizon 7. Es posible que necesite implementar un enfoque diferente.

Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7

Horizon 7 proporciona varios archivos de plantillas administrativas ADMX de directivas de grupo, específicos para los componentes. Puede optimizar y asegurar las aplicaciones y los escritorios remotos al agregar la configuración de la directiva de los archivos de plantilla ADMX a un GPO nuevo o ya existente de Active Directory.

Todos los archivos ADMX proporcionados por la configuración de las directivas de grupo de Horizon 7 están disponibles en un archivo de paquete .zip con el nombre VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip, donde x.x.x es la versión y yyyyyy es el número de compilación. Puede descargar el archivo 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.

Los archivos de plantilla ADMX de Horizon 7 contienen tanto las directivas de grupo Configuración de usuario como las de Configuración del equipo.

- Las directivas Configuración del equipo establecen directivas que se aplican a todos los escritorios remotos, sin tener en cuenta quién se conecta al escritorio.
- Las directivas Configuración de usuario establecen directivas que se aplican a todos los usuarios, independientemente de la aplicación o el escritorio remotos al que se conectan. Las directivas Configuración de usuario sobrescriben las equivalentes de Configuración del equipo.

Microsoft Windows aplica las directivas cuando el escritorio se inicia y cuando los usuarios inician sesión.

Archivos de plantilla ADMX de Horizon 7

Los archivos de plantilla ADMX de Horizon 7 proporcionan una configuración de directiva de grupo que le permite controlar y optimizar los componentes de Horizon 7.

Tabla 5-5. Archivos de plantilla ADMX de Horizon

Nombre de plantilla	Archivo de plantilla	Descripción
Configuración de VMware View Agent	vdm_agent.admx	Contiene la configuración de las directivas relacionada con los componentes de entorno y de autenticación de Horizon Agent.
Configuración de VMware Horizon Client	vdm_client.admx	<p>Contiene la configuración de las directivas relacionada con Horizon Client para Windows.</p> <p>Los clientes que se conectan desde fuera del dominio del host del servidor de conexión no se ven afectados por las directivas que se aplican a Horizon Client.</p> <p>Consulte el documento <i>Guía de instalación y configuración de VMware Horizon Client para Windows</i>.</p>

Nombre de plantilla	Archivo de plantilla	Descripción
Redireccionamiento URL de VMware Horizon	urlRedirection.admx	<p>Contiene la configuración de las directivas relacionada con la función de redireccionamiento de contenido URL. Si agrega esta plantilla a un GPO para un grupo de aplicaciones o de escritorios remotos, algunos vínculos URL a los que se hacen clic dentro de las aplicaciones o los escritorios remotos se pueden redireccionar a un cliente basado en Windows y se pueden abrir en un navegador del cliente.</p> <p>Si agrega esta plantilla en una GPO del cliente, cuando un usuario hace clic en ciertos vínculos URL en un sistema cliente basado en Windows, la URL se puede abrir en una aplicación o un escritorio remotos.</p> <p>Consulte Capítulo 3 Configurar el redireccionamiento de contenido URL y el documento <i>Guía de instalación y configuración de VMware Horizon Client para Windows</i>.</p>
Configuración común de VMware View Server	vdm_server.admx	<p>Contiene la configuración de las directivas relacionadas con el servidor de conexión.</p> <p>Consulte el documento <i>Administración de View</i>.</p>
Configuración común de VMware View Agent	vdm_common.admx	<p>Contiene la configuración de las directivas que son comunes a todos los componentes de Horizon.</p> <p>Consulte el documento <i>Administración de View</i>.</p>
Variables de las sesiones de PCoIP	pcoip.admx	<p>Contiene la configuración de directivas relacionada con el protocolo de visualización PCoIP.</p>
Variables de las sesiones del cliente PCoIP	pcoip.client.admx	<p>Contiene la configuración de las directivas relacionada con el protocolo de visualización PCoIP que afecta a Horizon Client para Windows.</p> <p>Consulte el documento <i>Guía de instalación y configuración de VMware Horizon Client para Windows</i>.</p>
Persona Management	ViewPM.admx	<p>Contiene la configuración de directivas relacionadas con Horizon Persona Management.</p> <p>Consulte el documento <i>Configurar escritorios virtuales en Horizon 7</i>.</p>
Servicios de Escritorio remoto	vmware_rdsh_server.admx	<p>Contiene la configuración de las directivas relacionadas con los Servicios de Escritorio remoto.</p> <p>Consulte Usar Servicios de Escritorio remoto de directivas de grupo.</p>
Configuración de audio/vídeo en tiempo real de View	vdm_agent_rtav.admx	<p>Contiene la configuración de las directivas relacionada con las cámaras web que se usan con la función Audio/vídeo en tiempo real.</p> <p>Consulte Configuración de la directiva de grupo Audio/vídeo en tiempo real.</p>

Nombre de plantilla	Archivo de plantilla	Descripción
Redireccionamiento de escáner	vdm_agent_scanner.admx	<p>Contiene la configuración de las directivas relacionadas con dispositivos de escáner que se redireccionan para usarlos en aplicaciones y dispositivos publicados.</p> <p>Consulte Configuración de la directiva de grupo de redireccionamiento del escáner.</p>
COM serie	vdm_agent_serialport.admx	<p>Contiene la configuración de las directivas relacionadas con los puertos (COM) serie que se redireccionan para usarlos en escritorios virtuales.</p> <p>Consulte Configuración de la directiva de grupo de redireccionamiento de puertos serie.</p>
Redireccionamiento de impresora de VMware Horizon	vdm_agent_printing.admx	<p>Contiene la configuración de directiva relacionada con el filtrado de impresoras redireccionadas.</p> <p>Consulte Filtrar las impresoras por impresión virtual.</p>

Agregar los archivos de plantilla ADMX a Active Directory

Puede agregar la configuración de directiva para funciones específicas de escritorios remotos en los archivos ADMX de Horizon 7 a los objetos de directiva de grupo (Group Policy Objects, GPO) de Active Directory.

Requisitos previos

- Compruebe que la opción de configuración para la función de escritorio remoto a la que va a aplicar la directiva esté instalada en los escritorios de máquina virtual y los hosts RDS. La configuración de directiva de grupo no tiene ningún efecto si la función de escritorio remoto no está instalada. Consulte el documento de configuración para obtener más información sobre cómo instalar Horizon Agent.
- Cree los GPO para las funciones de escritorio remoto a las que desee aplicar la configuración de directiva de grupo y vincúlelas a la OU que contenga los escritorios de máquina virtual o los hosts RDS.
- Compruebe el nombre del archivo de plantilla ADMX que desea agregar a Active Directory. Consulte [Archivos de plantilla ADMX de Horizon 7](#).
- Compruebe que esté disponible la función Administración de directivas de grupo en el servidor de Active Directory.

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip, donde *x.x.x* es la versión y *yyyyyyy* es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip y copie los archivos ADMX al servidor de Active Directory.
 - a Copie los archivos .admx y la carpeta en-US a la carpeta %systemroot%\PolicyDefinitions del servidor de Active Directory.
 - b Copie los archivos de recursos de idioma (.adml) a la subcarpeta adecuada en %systemroot%\PolicyDefinitions\ del servidor de Active Directory.
- 3 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y escriba la ruta de acceso a los archivos de plantilla en la que estos vayan a aparecer en el editor después de la instalación.

Pasos siguientes

Configure los ajustes de directiva de grupo.

Opciones de la plantilla ADMX de configuración de VMware View Agent

El archivo de plantilla ADMX de configuración de VMware View Agent (*vdm_agent.admx*) contiene la configuración de las directivas relacionadas con los componentes de entorno y de autenticación de Horizon Agent.

Los archivos 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.

La siguiente tabla describe la configuración de directiva del archivo de plantilla ADMX de configuración de VMware View Agent, además de las que se usan con los dispositivos USB. La plantilla contiene tanto las opciones de configuración del equipo como las de usuario. Las opciones de configuración de usuario reemplazan las del equipo equivalente.

Tabla 5-6. Opciones de la plantilla de configuración de VMware View Agent

Configuración	Equipo	Usuario	Propiedades
AllowDirectRDP	X		<p>Determina si otros clientes que no sean dispositivos Horizon Client pueden conectarse directamente a escritorios remotos mediante RDP. Cuando esta configuración está deshabilitada, el agente solo permite conexiones administradas mediante Horizon a través de Horizon Client.</p> <p>Cuando se conecte a un escritorio remoto desde Horizon Client para Mac, no deshabilite el parámetro AllowDirectRDP. Si está deshabilitado, la conexión falla con un error de acceso denegado.</p> <p>De forma predeterminada, mientras un usuario tenga la sesión iniciada en la sesión del escritorio remoto, puede usar RDP para conectarse a la máquina virtual. La conexión RDP finaliza la sesión del escritorio remoto y se pueden perder la configuración y los datos sin guardar del usuario. El usuario no puede iniciar sesión en el escritorio hasta que la conexión RDP externa se cierre. Para evitar esta situación, deshabilite la opción AllowDirectRDP.</p> <hr/> <p>Importante Es necesario que los Servicios de Escritorio remoto de Windows estén en ejecución en el sistema operativo invitado de cada escritorio. Puede usar esta configuración para impedir que los usuarios realicen conexiones RDP directas a sus escritorios.</p> <hr/> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
AllowSingleSignon	X		<p>Determina si se usa Single Sign-On (SSO) para conectar usuarios a escritorios y aplicaciones. Cuando esta configuración está habilitada, se requiere a los usuarios que introduzcan sus credenciales solo una vez, cuando inician sesión en el servidor. Cuando esta configuración está deshabilitada, los usuarios deben volver a autenticarse cuando se realiza la conexión remota.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
CommandsToRunOnConnect	X		<p>Especifica una lista de comandos o scripts de comandos que se ejecutarán al conectar una sesión por primera vez.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Consulte Ejecutar comandos en escritorios de Horizon para obtener más información.</p>

Configuración	Equipo	Usuario	Propiedades
CommandsToRunOnDisconnect	X		<p>Especifica una lista de comandos o scripts de comandos que se ejecutarán al desconectar una sesión.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Consulte Ejecutar comandos en escritorios de Horizon para obtener más información.</p>
CommandsToRunOnReconnect	X		<p>Especifica una lista de comandos o scripts de comandos que se ejecutarán al volver a conectar una sesión después de una desconexión.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Consulte Ejecutar comandos en escritorios de Horizon para obtener más información.</p>
ConnectionTicketTimeout	X		<p>Especifica la cantidad de tiempo en segundos durante los que es válido el ticket de conexión de Horizon.</p> <p>Los dispositivos Horizon Client usan un ticket de conexión para la verificación y Single Sign-On al conectarse al agente. Por motivos de seguridad, un ticket de conexión es válido por un periodo de tiempo limitado. Cuando un usuario se conecta a un escritorio remoto, la autenticación se debe realizar dentro del tiempo de espera del ticket de conexión; en caso contrario, la sesión agota el tiempo de espera. Si no se configura este parámetro, el periodo de tiempo de espera predeterminado es de 900 segundos.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p>
CredentialFilterExceptions	X		<p>Especifica los archivos ejecutables a los que no se permite cargar el filtro de credenciales del agente. Los nombres de archivo no deben incluir una ruta ni un sufijo. Use un punto y coma para separar varios nombres de archivo.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p>
Disable Time Zone Synchronization	X	X	<p>Determina si la zona horaria del escritorio de Horizon está sincronizada con la zona horaria del cliente conectado.</p> <p>Aunque se habilite esta opción, solo se aplicará si la opción Deshabilitar la redireccionamiento de la zona horaria de la directiva de Configuración de Horizon Client no está activada para estar deshabilitada.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta opción está deshabilitada de forma predeterminada.</p>

Configuración	Equipo	Usuario	Propiedades
DPI Synchronization	X	X	<p>Ajusta la configuración PPP del sistema para la sesión remota. Cuando esta opción está habilitada o no está configurada, la opción PPP de todo el sistema para la sesión remota está configurada para coincidir con la opción PPP correspondiente en el sistema operativo cliente. Cuando esta opción está deshabilitada, la opción PPP de todo el sistema para la sesión remota no cambia nunca.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta opción no está configurada de forma predeterminada.</p> <p>Nota Esta opción solo se aplica a clientes Windows en los que esté instalado Horizon Client 4.2 o una versión posterior.</p>
Enable multi-media acceleration	X		<p>Determina si el redireccionamiento multimedia (MMR) está habilitado en el escritorio remoto.</p> <p>MMR es un filtro de Windows Media Foundation que reenvía datos multimedia desde códecs específicos que se encuentran en el sistema remoto directamente a través de un socket TCP al cliente. Los datos se descodifican directamente en el cliente, donde se reproducen. Puede deshabilitar el MMR si el cliente no tiene suficientes recursos para gestionar descodificaciones multimedia locales.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
Force MMR to use software overlay	X		<p>El redireccionamiento multimedia (MMR) trata de usar la superposición de hardware a la hora de reproducir vídeos para lograr un mayor rendimiento. A la hora de trabajar con varias pantallas, la superposición de hardware solo se da en una de ellas, o bien la pantalla principal o en la que se ha iniciado el Reproductor de Windows Media. Si se arrastra el Reproductor de Windows Media a otra pantalla, el vídeo aparece como un rectángulo negro. Utilice esta opción para forzar al MMR a usar la superposición de software, que funciona en todas las pantallas.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta opción no está configurada de forma predeterminada.</p>
Single sign-on retry timeout	X		<p>Especifica cuánto tiempo, en milisegundos, transcurre hasta un nuevo intento de Single Sign-On. Establezca el valor en 0 para deshabilitar el nuevo intento de Single Sign-On. El valor predeterminado es 5.000 milisegundos.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta opción no está configurada de forma predeterminada.</p>

Configuración	Equipo	Usuario	Propiedades
ShowDiskActivityIcon	X		<p>Esta opción no es compatible con esta versión.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p>
Toggle Display Settings Control	X		<p>Determina si deshabilitar la pestaña Configuración del panel de control Pantalla cuando una sesión de cliente usa el protocolo de visualización PCoIP.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
UnAuthenticatedAccessEnabled			<p>Habilita o deshabilita la función Acceso sin autenticar. Cuando esta opción está habilitada, los usuarios con acceso no autenticado pueden acceder a las aplicaciones publicadas desde Horizon Client sin necesidad de introducir las credenciales de AD. Cuando esta configuración está deshabilitada, los usuarios con acceso no autenticado no pueden acceder a las aplicaciones publicadas desde Horizon Client sin introducir las credenciales de AD.</p> <p>Debe reiniciar el host RDS para que se aplique esta configuración.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Configuración de Agent del Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
Send updates for empty or offscreen windows	X		<p>Especifica si el cliente recibe actualizaciones sobre ventanas fuera de la pantalla o vacías. Cuando se deshabilita esta opción, no se envía al cliente información relativa a ventanas de menos de 2 x 2 píxeles o que se encuentren totalmente fuera de pantalla.</p> <p>Esta opción está en la carpeta Configuración de VMware View Agent > Unity Touch y aplicaciones alojadas en el Editor de administración de directivas de grupo.</p> <p>Esta opción está deshabilitada de forma predeterminada.</p>
Enable Unity Touch	X		<p>Determina si la funcionalidad Unity Touch está habilitada en el escritorio remoto. Unity Touch admite la distribución de aplicaciones remotas en Horizon y permite que los usuarios de dispositivos móviles accedan a las aplicaciones en la barra lateral de Unity Touch.</p> <p>Esta opción está en la carpeta Configuración de VMware View Agent > Unity Touch y aplicaciones alojadas en el Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>

Configuración	Equipo	Usuario	Propiedades
Enable system tray redirection for Hosted Apps	X		<p>Determina si el redireccionamiento de la bandeja del sistema está habilitado mientras un usuario ejecuta aplicaciones remotas.</p> <p>Esta opción está en la carpeta Configuración de VMware View Agent > Unity Touch y aplicaciones alojadas en el Editor de administración de directivas de grupo.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
Enable user profile customization for Hosted Apps	X	X	<p>Especifica si se debe personalizar el perfil de usuario cuando se utilicen las aplicaciones remotas. Si esta opción está habilitada, se genera un perfil de usuario, se personaliza el tema de Windows y se registran las aplicaciones de inicio.</p> <p>Este parámetro de configuración de equipos se encuentra en la carpeta Configuración de VMware View Agent > Unity Touch y aplicaciones alojadas en el Editor de administración de directivas de grupo. Las opciones de configuración de usuario se encuentran en la carpeta Configuración de VMware View Agent > Seguridad de Agent > Unity Touch y aplicaciones alojadas en el Editor de administración de directivas de grupo.</p> <p>Esta opción está deshabilitada de forma predeterminada.</p>
Limit usage of Windows hooks	X		<p>La mayoría de enlaces se deshabilitan cuando se utilizan las aplicaciones remotas o Unity Touch. Esta opción está pensada para las aplicaciones que tienen problemas de compatibilidad al establecer los enlaces de nivel del sistema operativo. Por ejemplo, al habilitar esta directiva se deshabilitan la mayoría de los enlaces en proceso y de accesibilidad activos de Windows.</p> <p>Esta opción está en la carpeta Configuración de VMware View Agent > Unity Touch y aplicaciones alojadas en el Editor de administración de directivas de grupo.</p> <p>Esta configuración está deshabilitada de forma predeterminada, lo que significa que se usan todos los enlaces preferidos.</p>
Accept SSL encrypted framework channel		X	<p>Habilita el canal de marco con cifrado SSL. Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> ■ Deshabilitar: deshabilitar SSL. ■ Habilitar: habilitar SSL. Permitir a los clientes heredados conectarse sin SSL. ■ Aplicar: habilitar SSL. Rechazar las conexiones de clientes heredados. <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Seguridad de Agent del Editor de administración de directivas de grupo.</p> <p>Esta opción no está configurada de forma predeterminada. El valor predeterminado es Habilitar.</p>

Configuración	Equipo	Usuario	Propiedades
Default Proxy Server	X		<p>Configuración de conexión de Internet Explorer predeterminada para el servidor proxy. Especifica el servidor proxy que se utilizará en las opciones de Internet > Configuración de la red de área local (LAN).</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Transparencia de IP de cliente de VMware en el Editor de administración de directivas de grupo. Esta opción no está habilitada de forma predeterminada.</p>
Enable	X		<p>Habilita la Transparencia de IP de cliente de VMware. Las conexiones remotas a Internet Explorer utilizan la dirección IP cliente en lugar de la dirección IP del equipo de escritorio remoto. Esta opción se aplica en el siguiente inicio de sesión.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Transparencia de IP de cliente de VMware en el Editor de administración de directivas de grupo.</p> <p>Si la opción de configuración personalizada Transparencia de IP de cliente de VMware está seleccionada en el instalador de Horizon Agent, esta opción se habilitará de forma predeterminada.</p>
Default auto detect proxy	X		<p>Configuración de la conexión de Internet Explorer predeterminada. Activa la opción para detectar automáticamente la configuración en Opciones de Internet > Configuración de la red de área local (LAN).</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Transparencia de IP de cliente de VMware en el Editor de administración de directivas de grupo. Esta opción no está habilitada de forma predeterminada.</p>
Set proxy for Java applet	X		<p>Establece el servidor proxy para applets Java. Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> ■ Utilizar transparencia de IP del cliente para proxy de Java: dirige una conexión remota para usar la dirección IP del cliente en vez de la dirección IP del equipo de escritorio remoto para applets Java. ■ Utilizar conexión directa para proxy de Java: utiliza una conexión directa para omitir la configuración del navegador para applets Java. ■ Utilizar valor predeterminado para proxy de Java: restablece la configuración original del proxy de Java. <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > Transparencia de IP de cliente de VMware en el Editor de administración de directivas de grupo. Esta opción no está habilitada de forma predeterminada.</p>
Enable flash multi-media redirection	X		<p>Especifica si el Redireccionamiento Flash está habilitado en el agente.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > VMware FlashMMR del Editor de administración de directivas de grupo.</p>

Configuración	Equipo	Usuario	Propiedades
Minimum rect size to enable FlashMMR	X		<p>Especifica el tamaño mínimo de rectángulo para habilitar el Redireccionamiento Flash.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > VMware FlashMMR del Editor de administración de directivas de grupo.</p> <p>El ancho predeterminado es de 320 píxeles y la altura predeterminada es de 200 píxeles.</p>
Definition for FlashMMR url list usage		X	<p>Define la regla de lista blanca o negra que habilita o deshabilita que las URL usen Redireccionamiento Flash.</p> <p>Si selecciona Habilitar lista blanca en el menú desplegable de Definición para uso de lista de URL de FlashMMR, solo las URL de la lista de URL están habilitadas para usar el Redireccionamiento Flash.</p> <p>Si decide Habilitar lista negra en el menú desplegable de Definición para uso de lista de URL de FlashMMR, las URL en la lista de URL no pueden usar el Redireccionamiento Flash.</p> <p>Especifica la lista de URL en la configuración de directiva de grupo Hosts Url list to enable FlashMMR.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > VMware FlashMMR del Editor de administración de directivas de grupo.</p> <p>Esta configuración especifica una lista blanca de forma predeterminada.</p>
Hosts Url list to enable FlashMMR		X	<p>Especifica la lista de URL que están habilitadas o deshabilitadas para usar el Redireccionamiento Flash según la configuración de directiva de grupo Definition for FlashMMR url list usage.</p> <p>Debe incluir http:// o https://. Puede usar expresiones comunes. Por ejemplo, puede especificar https://*.google.com y http://www.cnn.com.</p> <p>Esta configuración se encuentra en la carpeta Configuración de VMware View Agent > VMware FlashMMR del Editor de administración de directivas de grupo.</p>

Nota La opción Connect using DNS Name se eliminó de la versión 6.1 de Horizon 6. Puede establecer el atributo LDAP de Horizon 7, **pae-PreferDNS**, para que el servidor de conexión de Horizon otorgue preferencia a los nombres DNS cuando envíe las direcciones de los equipos de escritorio y de los hosts RDS a los clientes y a las puertas de enlace. Consulte el apartado sobre cómo otorgar preferencia a nombres DNS cuando el servidor de conexión de Horizon devuelve información de direcciones en el documento *Instalación de View*.

Configuración de USB para Horizon Agent

Consulte [Opciones para los USB en la plantilla ADMX de configuración de Horizon Agent](#).

Información de sistema cliente enviada a escritorios remotos

Cuando un usuario se conecta o reconecta a un escritorio remoto, Horizon Client recopila información sobre el sistema cliente y el servidor de conexión envía dicha información al escritorio remoto.

Horizon Agent escribe la información del equipo cliente en la ruta de registro del sistema HKCU\Volatile Environment en los escritorios remotos que se implementen en equipos de un solo usuario. En el caso de los escritorios remotos que se implementen en sesiones de RDS, Horizon Agent escribe la información del equipo cliente en la ruta de registro del sistema HKCU\Volatile Environment\x, donde x es el ID de sesión en el host RDS.

Si Horizon Client se ejecuta en el seno de una sesión de escritorio remoto, envía al escritorio remoto la información del cliente físico en lugar de la información de la máquina virtual. Por ejemplo, si un usuario se conecta desde su sistema cliente a un escritorio remoto, inicia Horizon Client dentro del escritorio remoto y se conecta a otro escritorio remoto, la dirección IP del sistema de cliente físico se envía al segundo escritorio remoto. Esta función se conoce como un modo anidado o un escenario de doble salto. Horizon Client envía ViewClient_Nested_Passthrough, que está establecido en 1, junto con la información del sistema cliente para indicar que envía información del modo anidado.

Nota Con Horizon Client 4.1, la información del sistema cliente se pasa al escritorio del segundo salto sobre la conexión del protocolo inicial. Con Horizon Client 4.2 y versiones posteriores, la información del sistema cliente también se actualiza si la conexión del protocolo del primer salto se desconecta y reconecta.

Puede agregar comandos a las opciones de directiva de grupo CommandsToRunOnConnect, CommandsToRunOnReconnect y CommandsToRunOnDisconnect de Horizon Agent para ejecutar comandos o scripts de comandos que lean esta información desde el registro del sistema cuando los usuarios se conecten y reconecten a escritorios. Consulte [Ejecutar comandos en escritorios de Horizon](#) para obtener más información.

Tabla 5-7. Información del sistema cliente describe las claves del registro que contienen información del sistema cliente y enumera los tipos de escritorios y sistemas cliente compatibles con dichas claves. Si aparece Sí en la columna **Compatible con modo anidado**, indica que la información del cliente físico (en lugar de la información de la máquina virtual) se envía a un escritorio de segundo salto.

Tabla 5-7. Información del sistema cliente

Clave del registro	Descripción	Compatible con modo anidado	Escritorios compatibles	Sistemas de cliente compatibles
ViewClient_IP_Address	La dirección IP del sistema cliente.	Sí	VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_MAC_Address	La dirección MAC del sistema cliente.	Sí	VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac y Android

Clave del registro	Descripción	Compatible con modo anidado	Escritorios compatibles	Sistemas de cliente compatibles
ViewClient_Machine_Name	El nombre de la máquina del sistema cliente.	Sí	VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Machine_Domain	El dominio del sistema cliente.	Sí	VDI (máquina de un solo usuario) RDS	Windows y Tienda Windows
ViewClient_LoggedOn_Username	El nombre de usuario utilizado para iniciar sesión en el sistema cliente.		VDI (máquina de un solo usuario) RDS	Windows, Linux y Mac
ViewClient_LoggedOn_Domainname	El nombre de dominio utilizado para iniciar sesión en el sistema cliente.		VDI (máquina de un solo usuario) RDS	Windows y Tienda Windows Para clientes Linux y Mac, tenga en cuenta que ViewClient_Machine_Domain.ViewClient_LoggedOn_Domainname no es proporcionado por el cliente Linux o Mac, porque las cuentas de Linux y Mac no están vinculadas a los dominios de Windows.
ViewClient_Type	El nombre del cliente ligero o tipo de sistema operativo del sistema cliente.	Sí	VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Broker_DNS_Name	El nombre DNS de la instancia del servidor de conexión de View.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_Broker_URL	La URL de la instancia del servidor de conexión de View.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_Broker_Tunneled	El estado de la conexión de túnel del servidor de conexión de View, que puede ser true (habilitado) o false (deshabilitado).		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.

Clave del registro	Descripción	Compatible con modo anidado	Escritorios compatibles	Sistemas de cliente compatibles
ViewClient_Broker_Tunnel_URL	La URL de la conexión de túnel del servidor de conexión de VIEW, si la conexión de túnel está habilitada.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_Broker_Remote_IP_Address	La dirección IP del sistema cliente que ve la instancia del servidor de conexión de View.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_TZID	El ID de la zona horaria Olson. Para deshabilitar la sincronización de zona horaria, habilite la opción de directiva de grupo Disable Time Zone Synchronization de Horizon Agent.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android e iOS
ViewClient_Windows_Timezone	La hora estándar GMT. Para deshabilitar la sincronización de zona horaria, habilite la opción de directiva de grupo Disable Time Zone Synchronization de Horizon Agent.		VDI (máquina de un solo usuario) RDS	Windows y Tienda Windows
ViewClient_Broker_DomainName	Nombre de dominio utilizado para autenticar el servidor de conexión de View.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_Broker_UserName	Nombre de usuario utilizado para autenticar el servidor de conexión de View.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_Client_ID	Especifica el Unique Client HardwareId utilizado como vínculo a la clave de licencia.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Displays.Number	Especifica el número de monitores que se utilizan en el cliente.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows

Clave del registro	Descripción	Compatible con modo anidado	Escritorios compatibles	Sistemas de cliente compatibles
ViewClient_Displays.Topology	Especifica la disposición, resolución y dimensiones de las pantallas en el cliente.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Keyboard.Type	Especifica el tipo de teclado que se utiliza en el cliente. Por ejemplo: japonés, coreano.		VDI (máquina de un solo usuario) RDS	Windows
ViewClient_Launch_SessionType	Especifica el tipo de sesión. El tipo puede ser escritorio o aplicación.		VDI (máquina de un solo usuario) RDS	El valor se envía directamente desde el servidor de conexión de View, no lo recopila Horizon Client.
ViewClient_Mouse.Identifier	Especifica el tipo de mouse.		VDI (máquina de un solo usuario) RDS	Windows
ViewClient_Mouse.NumButtons	Especifica el número de botones que admite el mouse.		VDI (máquina de un solo usuario) RDS	Windows
ViewClient_Mouse.SampleRate	Especifica la velocidad, en informes por segundo, a la que se muestra una entrada desde un mouse por PS/2.		VDI (máquina de un solo usuario) RDS	Windows
ViewClient_Protocol	Especifica el protocolo utilizado.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Language	Especifica el idioma del sistema operativo.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Launch_Matched_Tags	Especifica una o varias etiquetas.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Launch_ID	Especifica el ID único del grupo de escritorios o de aplicaciones.		VDI (máquina de un solo usuario) RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows
ViewClient_Broker_Farm_ID	Especifica el ID de granja del grupo de aplicaciones o de escritorios de un host RDS.		RDS	Windows, Linux, Mac, Android, iOS y Tienda Windows

Nota Las definiciones de `ViewClient_LoggedOn_Username` y `ViewClient_LoggedOn_Domainname` en [Tabla 5-7. Información del sistema cliente](#) se aplican a Horizon Client 2.2 para Windows o versiones posteriores.

En el caso de Horizon Client 5.4 para Windows o versiones anteriores, `ViewClient_LoggedOn_Username` envía el nombre de usuario introducido en Horizon Client y `ViewClient_LoggedOn_Domainname` envía el nombre de dominio introducido en Horizon Client.

Horizon Client 2.2 para Windows es una versión posterior a Horizon Client 5.4 para Windows. A partir de Horizon Client 2.2, los números de versión para Windows son consistentes con las versiones de Horizon Client en otros sistemas operativos y dispositivos.

Ejecutar comandos en escritorios de Horizon

Puede usar las opciones de directiva de grupo `Horizon AgentCommandsToRunOnConnect`, `CommandsToRunOnReconnect` y `CommandsToRunOnDisconnect` para ejecutar comandos y scripts de comandos en escritorios de Horizon cuando los usuarios se conectan, se vuelven a conectar y se desconectan.

Para ejecutar un comando o un script de comandos, agregue el nombre del comando o la ruta de acceso al archivo del script a la lista de comandos de la opción de directiva de grupo. Por ejemplo:

`date`

`C:\Scripts\myscript.cmd`

Para ejecutar scripts que requieran acceso a la consola, agregue la opción `-C` o `-c` al principio del script seguida de un espacio. Por ejemplo:

`-c C:\Scripts\Cli_clip.cmd`

`-C e:\procexp.exe`

Los tipos de archivos compatibles son `.CMD`, `.BAT` y `.EXE`. Los archivos `.VBS` no se ejecutarán a menos que se analicen con `cscript.exe` o con `wscript.exe`. Por ejemplo:

`-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs`

La longitud total de la cadena, incluida la opción `-C` o `-c`, no debe sobrepasar 260 caracteres.

Configuración de directiva de VMware Virtualization Pack para Skype Empresarial

El archivo de plantilla ADMX de configuración de VMware View Agent (`vdm_agent.admx`) contiene la configuración de la directiva relacionada con VMware Virtualization Pack para Skype Empresarial.

Esta configuración se encuentra dentro del Editor de administración de directivas de grupo, en la carpeta **Configuración del equipo > Plantillas administrativas > Configuración de VMware View Agent > VMware Virtualization Pack para Skype Empresarial**.

Tabla 5-8. Configuración de directiva de Virtualization Pack para Skype Empresarial

Ajuste	Descripción
Show Icon	Muestra el icono de la función Virtualization Pack para Skype Empresarial. Esta directiva está habilitada de forma predeterminada. El icono no aparece si la directiva Mostrar icono para la función Virtualization Pack para Skype Empresarial está deshabilitada. Si está deshabilitada, no puede consultar los mensajes ni las estadísticas de las llamadas.
Show Messages	Muestra los mensajes de la función Virtualization Pack para Skype Empresarial. Esta directiva está habilitada de forma predeterminada. Los mensajes no aparecen si las directivas Mostrar icono y Mostrar mensajes para la función Virtualization Pack para Skype Empresarial están deshabilitadas.

Configuración de directivas de PCoIP

El archivo de plantilla ADMX de PCoIP incluye la configuración de directiva relacionada con el protocolo de visualización PCoIP. El archivo de plantilla ADMX se denomina (`pcoip.admx`). Puede establecer las opciones en valores predeterminados que un administrador pueda sobrescribir o bien en valores que no se puedan sobrescribir.

Los archivos ADMX están disponibles en un archivo de paquete .zip con el nombre VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.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.

El archivo de plantilla ADMX de variables de sesión PCoIP incluye dos subcategorías:

Configuración del administrador que se puede sobrescribir Especifica los valores predeterminados de la configuración de directivas PCoIP. Los administradores pueden sobrescribir esta configuración. Esta configuración introduce los valores de las claves de registro en HKLM \Software\Policies\Teradici\PCoIP\pcoip_admin_defaults. Todas estas configuraciones están en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que se puede sobrescribir** en el Editor de administración de directivas de grupo.

Configuración del administrador que no se puede sobrescribir Contiene las mismas opciones que la configuración del administrador que se puede sobrescribir, pero los administradores no pueden sobrescribir estas opciones. Esta configuración graba valores de claves de registro en HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin. Todas estas configuraciones están en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que no se puede sobrescribir** en el Editor de administración de directivas de grupo.

La plantilla contiene tanto las opciones de configuración del equipo como las de usuario.

Claves de registro que no sean directivas

Si necesita aplicar una opción a una máquina local, pero no puede colocarla en HKLM\Software\Policies\Teradici, puede colocar las opciones de la máquina local con las claves de registro en HKLM\Software\Teradici. Se pueden situar las mismas claves de registro tanto en HKLM\Software\Teradici como en HKLM\Software\Policies\Teradici. Si la misma clave del registro está presente en las dos ubicaciones, la opción que se encuentre en HKLM\Software\Policies\Teradici anula el valor de la máquina local.

Configuración general de PCoIP

El archivo de plantilla ADMX de PCoIP incluye la configuración de directiva de grupo que permite establecer valores generales, tales como dispositivos USB, puertos de red y calidad de la imagen en PCoIP.

Todas estas configuraciones están en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que se puede sobrescribir** en el Editor de administración de directivas de grupo.

Todas estas configuraciones también están en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que no se puede sobrescribir** en el Editor de administración de directivas de grupo.

Tabla 5-9. Configuración de la directiva general de PCoIP

Ajuste	Descripción
Configure PCoIP event log cleanup by size in MB	<p>Habilita la configuración de la limpieza de los registros de eventos PCoIP por MB.</p> <p>Cuando esta directiva está configurada, la opción controla cuánto puede crecer un archivo de registro antes de que se limpie. Con una configuración de <i>m</i> que no sea cero, los archivos de registro que sean superiores a <i>m</i> MB se eliminarán automáticamente y de forma silenciosa. Una configuración 0 indica que no se realizará ninguna limpieza de archivos por tamaño.</p> <p>Cuando esta directiva está deshabilitada o no está configurada, el valor predeterminado de la limpieza de los registros de eventos es 100 MB.</p> <p>La limpieza del archivo de registro se realiza una vez que se inicia la sesión. Cualquier cambio en esta opción no se aplicará hasta la siguiente sesión.</p>
Configure PCoIP event log cleanup by time in days	<p>Habilita la configuración de la limpieza de los registros de eventos PCoIP por días.</p> <p>Cuando esta directiva está configurada, la opción controla cuántos días pueden pasar antes de que el archivo de registro se limpie. Con una configuración de <i>n</i> que no sea cero, los archivos de registro que tengan más de <i>n</i> días se eliminarán automáticamente y de forma silenciosa. Una configuración 0 indica que no se realizará ninguna limpieza de archivos por tiempo.</p> <p>Cuando esta directiva está deshabilitada o no está configurada, el valor predeterminado de la limpieza de los registros de eventos es 7 días.</p> <p>La limpieza del archivo de registro se realiza una vez que se inicia la sesión. Cualquier cambio en esta opción no se aplicará hasta la siguiente sesión.</p>

Ajuste	Descripción
Configure PCoIP event log verbosity	<p>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).</p> <p>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.</p> <p>Cuando esta opción se modifica durante una sesión PCoIP activa, la nueva opción se aplica de forma inmediata.</p>
Configure PCoIP image quality levels	<p>Controla cómo PCoIP procesa imágenes durante periodos de congestión en la red. Los valores Calidad mínima de la imagen, Calidad inicial máxima de la imagen y Velocidad de fotogramas máxima interoperan para proporcionar un control adecuado en entornos con ancho de banda limitado.</p> <p>Use el valor Calidad mínima de la imagen para equilibrar la calidad de la imagen y la velocidad de los fotogramas en escenarios con ancho de banda limitado. Puede especificar un valor entre 30 y 100. El valor predeterminado es 40. Un valor inferior permite una velocidad más elevada de fotogramas, pero puede derivar en una visualización con una calidad inferior. Un valor superior proporciona una calidad de imagen superior, pero puede derivar en una velocidad de fotogramas inferior si existe alguna limitación en el ancho de banda de la red. Cuando el ancho de banda de la red no está limitado, PCoIP mantiene la calidad máxima, sin tener en cuenta este valor.</p> <p>Use el valor Calidad inicial máxima de la imagen para reducir los picos de ancho de banda de red que requiere PCoIP al limitar la calidad inicial de las regiones modificadas de la imagen que se visualiza. Puede especificar un valor entre 30 y 100. El valor predeterminado es 80. Un valor inferior reduce la calidad de la imagen de los cambios del contenido y disminuye los requisitos de los picos del ancho de banda. Un valor superior aumenta la calidad de la imagen de los cambios del contenido y aumenta los requisitos de los picos del ancho de banda. Las regiones sin cambios de la imagen compilan de forma progresiva una calidad sin pérdidas (perfecta), independientemente de este valor. Un valor inferior a 80 (inclusive) utiliza mejor el ancho de banda disponible.</p> <p>El valor Calidad mínima de la imagen no puede superar el valor Calidad inicial máxima de la imagen.</p> <p>Use el valor Velocidad de fotogramas máxima para administrar el ancho de banda medio que se consume por usuario al limitar el número de actualizaciones de pantalla por segundo. Puede especificar un valor entre 1 y 120 fotogramas por segundo. El valor predeterminado es 30. Un valor superior usa más ancho de banda, pero proporciona menos vibración, lo que permite transiciones más fluidas en las imágenes cambiantes como, por ejemplo, en vídeos. Un valor inferior usa menos ancho de banda, pero genera más vibraciones.</p> <p>Estos valores de la calidad de la imagen se aplican únicamente al host del software y no se aplican a ningún cliente del software.</p> <p>Cuando esta opción está deshabilitada o no está configurada, se usan los valores predeterminados.</p> <p>Cuando esta opción se modifica durante una sesión PCoIP activa, la nueva opción se aplica de forma inmediata.</p>

Ajuste	Descripción
Configure frame rate vs image quality preference	<p>Configure la preferencia de la calidad de imagen y la velocidad del fotograma de 0 (velocidad más elevada del fotograma) a 100 (calidad más alta de imagen). Si esta directiva está deshabilitada o no está configurada, el valor predeterminado es 50.</p> <p>El valor máximo (máx.: 100) significa que prefiere calidad de imagen más alta aunque genere retrasos en la velocidad de fotogramas. El valor mínimo (mín.: 0) significa que prefiere disfrutar de una experiencia fluida con una calidad de imagen limitada.</p> <p>Esta opción puede funcionar con el GPO Configure PCoIP image quality levels, lo que determina el nivel máximo de la calidad inicial de la imagen y el nivel mínimo de la calidad de la imagen. Frame rate and image quality preference puede ajustar el nivel de la calidad de imagen en cada fotograma; sin embargo, no podrá salirse del umbral que establece el nivel máximo y mínimo de calidad que se configura en el GPO Configure PCoIP image quality levels.</p> <p>Si se cambian estas opciones durante el tiempo de ejecución, se aplicarán inmediatamente.</p>
Configure PCoIP session encryption algorithms	<p>Controla los algoritmos de cifrado que muestra el endpoint PCoIP durante la negociación de la sesión.</p> <p>Al marcar una de las casillas, se deshabilita el algoritmo de cifrado asociado. Debe habilitar al menos un algoritmo.</p> <p>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 el modo aprobado FIPS140-2 está habilitado, el valor Deshabilitar el cifrado AES-128-GCM se sobrescribe siempre, de forma que el cifrado AES-128-GCM esté habilitado.</p> <p>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.</p> <p>Si ambos endpoints están configurados para admitir los tres algoritmos y la conexión no usa una puerta de enlace de seguridad (SG), se negociará y se usará el algoritmo SALSA20. Sin embargo, si la conexión usa una SG, SALSA20 se deshabilita automáticamente, y se negociará y se usará AES128. Si el endpoint o la SG deshabilitan SALSA20 y el endpoint también deshabilita AES128, se negociará y se usará AES256.</p>

Ajuste	Descripción								
Configure PCoIP USB allowed and unallowed device rules	<p>Especifica los dispositivos USB con y sin autorización para las sesiones PCoIP que usan un cliente cero que ejecuta un firmware Teradici. Los dispositivos USB que se usan en sesiones PCoIP deben aparecer en la tabla de USB con autorización. Los dispositivos USB que aparecen en la tabla de USB sin autorización no se pueden usar en sesiones PCoIP.</p> <p>Puede definir un máximo de 10 reglas para autorizar a los USB y un mínimo de 10 reglas para no autorizarlos. Separe varias reglas con el carácter de barra vertical ().</p> <p>Cada regla puede ser una combinación de un ID del proveedor (VID) y un ID del producto (PID), o bien puede describir una clase de dispositivos USB. Una regla de clase puede permitir o prohibir una clase completa de dispositivos, una única subclase o un protocolo dentro de una subclase.</p> <p>El formato de una regla de combinación VID/PID es 1xxxxyyyy, donde xxxx es el VID en formato hexadecimal e yyyy es el PID en formato hexadecimal. Por ejemplo, la regla para autorizar o bloquear un dispositivo con VID 0x1a2b y PID 0x3c4d es 11a2b3c4d.</p> <p>Para las reglas de clase, use uno de los siguientes formatos:</p> <table> <tr> <td>Permitir todos los dispositivos USB</td><td>Formato: 23XXXXXX Ejemplo: 23XXXXXX</td></tr> <tr> <td>Permitir dispositivos USB con un ID de clase específico</td><td>Formato: 22claseXXXX Ejemplo: 22aaXXXX</td></tr> <tr> <td>Permitir una subclase específica</td><td>Formato: 21clase-subclaseXX Ejemplo: 21aabbXX</td></tr> <tr> <td>Permitir un protocolo específico</td><td>Formato: 20clase-subclase-protocolo Ejemplo: 20aabbcc</td></tr> </table> <p>Por ejemplo, la cadena de autorización USB para permitir dispositivos USB HID (mouse y teclado) (ID de clase 0x03) y cámaras web (ID de clase 0x0e) es 2203XXXX 220eXXXX. La cadena de USB sin autorización que no permite los dispositivos de almacenamiento masivo USB (ID de clase 0x08) es 2208XXXX.</p> <p>Si una cadena de USB con autorización está vacía, significa que ningún dispositivo USB está autorizado. Si una cadena de USB sin autorización está vacía, significa que no se excluye ningún dispositivo USB.</p> <p>Esta opción se aplica únicamente a Horizon Agent y solo cuando el escritorio remoto tiene una sesión con un cliente cero que ejecuta un firmware Teradici. El uso del dispositivo se negocia entre los endpoints.</p> <p>De forma predeterminada, se permiten todos los dispositivos y ninguno se excluye.</p>	Permitir todos los dispositivos USB	Formato: 23XXXXXX Ejemplo: 23XXXXXX	Permitir dispositivos USB con un ID de clase específico	Formato: 22claseXXXX Ejemplo: 22aaXXXX	Permitir una subclase específica	Formato: 21clase-subclaseXX Ejemplo: 21aabbXX	Permitir un protocolo específico	Formato: 20clase-subclase-protocolo Ejemplo: 20aabbcc
Permitir todos los dispositivos USB	Formato: 23XXXXXX Ejemplo: 23XXXXXX								
Permitir dispositivos USB con un ID de clase específico	Formato: 22claseXXXX Ejemplo: 22aaXXXX								
Permitir una subclase específica	Formato: 21clase-subclaseXX Ejemplo: 21aabbXX								
Permitir un protocolo específico	Formato: 20clase-subclase-protocolo Ejemplo: 20aabbcc								

Ajuste	Descripción
Configure PCoIP virtual channels	<p data-bbox="676 226 1378 315">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.</p> <p data-bbox="676 327 1422 447">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.</p> <p data-bbox="676 459 1358 514">Puede especificar un máximo de 15 canales virtuales para utilizarlos en sesiones PCoIP.</p> <p data-bbox="676 527 1422 646">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.</p> <p data-bbox="676 659 1394 779">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.</p> <p data-bbox="676 791 1422 882">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.</p> <p data-bbox="676 894 1422 984">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.</p> <p data-bbox="676 997 1422 1087">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.</p> <p data-bbox="676 1100 1353 1155">De forma predeterminada, todos los canales virtuales están habilitados (incluido el procesamiento del portapapeles).</p>

Ajuste	Descripción
Configure the PCoIP transport header	<p data-bbox="676 226 1396 281">Configura el encabezado de transporte PCoIP y establece la prioridad de la sesión de transporte.</p> <p data-bbox="676 296 1422 510">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.</p> <p data-bbox="676 525 1422 674">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.</p> <p data-bbox="676 688 1326 774">Cuando la opción Configure the PCoIP transport header está habilitada, las siguientes prioridades de sesión de transporte están disponibles:</p> <ul data-bbox="676 789 999 924" style="list-style-type: none"> ■ Alta ■ Media (valor predeterminado) ■ Baja ■ No definida <p data-bbox="676 938 1422 1182">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).</p>

Ajuste	Descripción
Configure the TCP port to which the PCoIP host binds and listens	<p>Especifica el puerto TCP agente al que se enlaza mediante los hosts PCoIP del software.</p> <p>El valor del puerto TCP especifica el puerto base TCP al que el agente intenta enlazarse. El valor del rango de puertos TCP determina a cuántos puertos adicionales debe intentar enlazarse si el puerto base no está disponible. El rango de puertos debe estar entre 1 y 10.</p> <p>El intervalo abarca desde el puerto base hasta la suma del puerto base y del intervalo del puerto. Por ejemplo, si el puerto base es 4172 y el rango de puertos es 10, el rango se extiende desde 4172 hasta 4182.</p> <p>No establezca el tamaño del rango del puerto de reintentos a 0. Establecer este valor en 0 produce un error de conexión cuando los usuarios inician sesión en el escritorio con el protocolo de visualización PCoIP. Horizon Client devuelve el mensaje de error En este momento, el protocolo de visualización de este escritorio no se encuentra disponible. Póngase en contacto con el administrador del sistema.</p> <p>Esta opción se aplica únicamente a Horizon Agent.</p> <p>En máquinas de un solo usuario, el puerto base TCP predeterminado es 4172 para View 4.5 y versiones posteriores. El puerto base predeterminado es 50002 para View 4.0.x y versiones anteriores. De forma predeterminada, el rango de puertos es 1.</p> <p>En los hosts RDS, el puerto TCP base predeterminado es 4173. Cuando se utiliza PCoIP con hosts RDS, se utiliza un puerto PCoIP aparte para cada conexión de usuario. El rango de puertos predeterminado establecido por el Servicio de escritorio remoto es lo suficientemente grande como para acomodar el número máximo previsto de conexiones de usuario simultáneas.</p> <hr/> <p>Importante Como procedimiento recomendado, no utilice esta opción de directiva para cambiar el rango de puertos predeterminado en hosts RDS ni cambie el valor predeterminado 4173 del puerto TCP. Y lo que es más importante, no establezca el valor del puerto TCP en 4172. Restablecer este valor a 4172 afectará de forma negativa al rendimiento de PCoIP en sesiones de RDS.</p>

Ajuste	Descripción
Configure the UDP port to which the PCoIP host binds and listens	<p>Especifica el puerto agente UDP al que se enlaza mediante los hosts PCoIP del software.</p> <p>El valor del puerto UDP especifica el puerto base UDP al que el agente intenta enlazarse. El valor del intervalo del puerto UDP determina la cantidad de puertos adicionales que se van a probar si el puerto base no está disponible. El rango de puertos debe estar entre 1 y 10.</p> <p>No establezca el tamaño del rango del puerto de reintentos a 0. Establecer este valor en 0 produce un error de conexión cuando los usuarios inician sesión en el escritorio con el protocolo de visualización PCoIP. Horizon Client devuelve el mensaje de error En este momento, el protocolo de visualización de este escritorio no se encuentra disponible. Póngase en contacto con el administrador del sistema.</p> <p>El intervalo abarca desde el puerto base hasta la suma del puerto base y del intervalo del puerto. Por ejemplo, si el puerto base es 4172 y el rango de puertos es 10, el rango se extiende desde 4172 hasta 4182.</p> <p>Esta opción se aplica únicamente a Horizon Agent.</p> <p>En máquinas de un solo usuario, el puerto UDP base predeterminado es 4172 para View 4.5 y versiones posteriores, y 50002 para View 4.0.x y versiones anteriores. De forma predeterminada, el rango de puertos es 10.</p> <p>En los hosts RDS, el puerto UDP base predeterminado es 4173. Cuando se utiliza PCoIP con hosts RDS, se utiliza un puerto PCoIP aparte para cada conexión de usuario. El rango de puertos predeterminado establecido por el Servicio de escritorio remoto es lo suficientemente grande como para acomodar el número máximo previsto de conexiones de usuario simultáneas.</p> <p>Importante Como procedimiento recomendado, no utilice esta opción de directiva para cambiar el rango de puertos predeterminado en hosts RDS o cambie el valor predeterminado 4173 de puerto UDP. Y lo que es más importante, no establezca el valor del puerto UDP en 4172. Restablecer este valor a 4172 afectará de forma negativa al rendimiento de PCoIP en sesiones de RDS.</p>
Enable access to a PCoIP session from a vSphere console	<p>Determina si se permite que una consola de vSphere Client muestre una sesión PCoIP activa y envíe la entrada al escritorio.</p> <p>De forma predeterminada, cuando un cliente se conecta mediante PCoIP, la pantalla de la consola de vSphere Client aparece en blanco y la consola no puede enviar la entrada. La opción predeterminada garantiza que un usuario malintencionado no pueda ver el escritorio del usuario ni proporcionar la entrada al host de forma local cuando una sesión PCoIP está activa.</p> <p>Esta opción se aplica únicamente a Horizon Agent.</p> <p>Cuando esta opción está deshabilitada o no está configurada, no se permite el acceso a la consola. Cuando esta opción está habilitada, la consola muestra la sesión PCoIP y se permite la entrada de la consola.</p> <p>Cuando esta opción está habilitada, la consola muestra una sesión PCoIP que se ejecuta en un sistema Windows 7 únicamente cuando la máquina virtual Windows 7 tiene la versión 8. La versión 8 del hardware solo está disponible en las versiones 5.0 y posteriores de ESXi. Por el contrario, se permite la entrada de la consola a un sistema Windows 7 con cualquier versión de hardware de la máquina virtual.</p>

Ajuste	Descripción
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.
Enable/disable microphone noise and DC offset filter in PCoIP session	Determina si se habilita el ruido de micrófono y el filtro del desnivel de corriente continua para la entrada del micrófono durante las sesiones PCoIP. Esta opción se aplica únicamente a Horizon Agent y al controlador de audio Teradici. Si esta opción no está configurada, el controlador de audio Teradici usa el ruido del micrófono y el filtro del desnivel de corriente continua de forma predeterminada.
Turn on PCoIP user default input language synchronization	Determina si el idioma de entrada predeterminado para el usuario de la sesión PCoIP se sincroniza con el idioma de entrada predeterminado del endpoint del cliente PCoIP. Cuando esta opción está habilitada, se permite la sincronización. Si esta opción está deshabilitada o no está configurada, no se permite la sincronización. Esta opción se aplica únicamente a Horizon Agent.
Configure SSL Connections to satisfy Security Tools	Especifica cómo se establecen las conexiones de negociación de la sesión SSL. Con el fin de satisfacer detectores de puertos, habilite la opción "Configurar conexiones SSL" y, en Horizon Agent, complete las siguientes tareas: <ol style="list-style-type: none"> 1 En Microsoft Management Console, almacene un certificado firmado y con nombre correcto en el almacén Personal de la cuenta del Equipo local y márcalo como exportable. 2 Almacene el certificado firmado por la entidad de certificación en el almacén de certificados raíz de confianza. 3 Deshabilite las conexiones a VMware View 5.1 y a versiones anteriores. 4 Configure Horizon Agent de forma que cargue certificados únicamente desde el almacén de certificados. Si el almacén Personal del Equipo local está en uso, no cambie los nombres de los almacenes de certificado "MY" y "ROOT" (sin las comillas), a menos que se empleara una ubicación diferente durante los pasos 1 y 2. <p>El PCoIP Server resultante utilizará las herramientas de seguridad, como los escáneres de puertos.</p>

Ajuste	Descripción
Configure SSL Protocols	<p>Configura los protocolos OpenSSL para limitar el uso de ciertos protocolos antes de establecer una conexión SSL cifrada. La lista de protocolos cuenta con una o varias cadenas de protocolos openssl separadas por dos puntos. Tenga en cuenta que todas las cadenas de cifrado distinguen entre mayúsculas y minúsculas.</p> <p>El valor predeterminado es: "TLS1.1:TLS1.2"</p> <p>Esto significa que están habilitados tanto TLS v1.1 y TLS v1.2 (SSL v2.0, SSLv3.0 y TLS v1.0 están deshabilitados).</p> <p>Esta opción se aplica tanto a Horizon Agent como a Horizon Client.</p> <p>Si está configurada en ambos lados, se seguirá la regla de negociación del protocolo OpenSSL.</p>
Configure SSL cipher list	<p>Configura una lista de cifrado SSL para restringir el uso de conjuntos de claves de cifrado antes de establecer una conexión SSL cifrada. La lista consta de una o varias cadenas del conjunto de claves de cifrado separadas por dos puntos. Todas las cadenas del conjunto de claves de cifrado distinguen entre mayúsculas y minúsculas.</p> <p>El valor predeterminado es ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDSA-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH.</p> <p>Si esta opción está configurada, se ignora la casilla de verificación Aplicar AES-256 o cifrados más seguros para la negociación de la conexión SSL de la opción Configurar conexiones SSL para utilizar las herramientas de seguridad.</p> <p>Esta opción debe aplicarse tanto al servidor PCoIP como al cliente PCoIP.</p>

Configuración del portapapeles de PCoIP

El archivo de plantilla ADMX de PCoIP de Horizon incluye la configuración de directiva de grupo que permite establecer los valores del portapapeles para las operaciones de copiado y pegado.

Todas estas configuraciones están en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que se puede sobrescribir** en el Editor de administración de directivas de grupo.

Todas estas configuraciones también están en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que no se puede sobrescribir** en el Editor de administración de directivas de grupo.

Tabla 5-10. Configuración de la directiva del portapapeles de PCoIP

Ajuste	Descripción
Configure clipboard memory size on server (in kilobytes)	<p>Especifica el valor del tamaño de la memoria del portapapeles del servidor, en kilobytes. El cliente también tiene un valor del tamaño de la memoria del portapapeles. Una vez que se configura la sesión, el servidor envía el valor del tamaño de la memoria del portapapeles al cliente. El valor efectivo del tamaño de la memoria del portapapeles es el menor de los valores del tamaño de la memoria del portapapeles del cliente y del servidor.</p> <p>Puede especificar un valor mínimo de 512 kilobytes y un valor máximo de 16384 kilobytes. Si especifica 0 o no especifica ningún valor, el tamaño de la memoria del portapapeles del servidor es 1.024 kilobytes.</p> <p>Esta opción solo es compatible con la versión 7.0.1 o posteriores y con los clientes Windows, Linux o Mac en los que esté instalado Horizon Client 4.1 o versiones posteriores. En versiones anteriores, el tamaño de la memoria del portapapeles es 1 MB.</p> <p>Nota En función de la red, si el tamaño de la memoria del portapapeles es muy grande, el rendimiento puede verse afectado de forma negativa. VMware le recomienda que no asigne al tamaño de memoria del portapapeles un valor superior a 16 MB.</p>
Configure clipboard redirection	<p>Determina la dirección en la que se permite el redireccionamiento del portapapeles. Puede seleccionar uno de estos valores:</p> <ul style="list-style-type: none"> ■ Habilitado solo del cliente al agente (es decir, permite operaciones de copiado y pegado únicamente desde el sistema cliente al escritorio remoto). ■ Deshabilitado en ambas direcciones ■ Habilitado en ambas direcciones ■ Habilitado solo del agente al cliente (es decir, permite operaciones de copiado y pegado únicamente desde el escritorio remoto al sistema cliente). <p>El redireccionamiento del portapapeles se implementa como un canal virtual. Si se deshabilitan los canales virtuales, el redireccionamiento del portapapeles no funciona.</p> <p>Esta opción se aplica únicamente a Horizon Agent.</p> <p>Si esta opción está deshabilitada o no está configurada, el valor predeterminado es Habilitado solo del cliente al agente.</p>
Filter text out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos textuales a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto enriquecido a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>

Ajuste	Descripción
Filter images out of the incoming clipboard data	<p>Especifica si se deben filtrar las imágenes a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto de Microsoft Office (formato BIFF12) a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos de gráficos y SmartArt de Microsoft Office (Art::GVML ClipFormat) a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Text Effects data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos de efectos de texto de Microsoft Office (formato HTML) a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter text out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos textuales de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Rich Text Format data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto enriquecido de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter images out of the outgoing clipboard data	<p>Especifica si se deben filtrar las imágenes de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>

Ajuste	Descripción
Filter Microsoft Office text data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto Microsoft Office (formato BIFF12) de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos de gráficos y SmartArt de Microsoft Office (Art::GVML ClipFormat) de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Text Effects data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos de efectos de texto de Microsoft Office (formato HTML) de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>

Configuración de ancho de banda de PCoIP

El archivo de plantilla ADMX de PCoIP de Horizon incluye la configuración de directiva de grupo que permite establecer las características de ancho de banda de PCoIP.

Todas estas configuraciones están en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que se puede sobrescribir** en el Editor de administración de directivas de grupo.

Todas estas configuraciones también están en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que no se puede sobrescribir** en el Editor de administración de directivas de grupo.

Tabla 5-11. Variables de ancho de banda de las sesiones PCoIP de Horizon

Ajuste	Descripción
Configure the maximum PCoIP session bandwidth	<p>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.</p> <p>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.</p> <p>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.</p> <p>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).</p> <p>Cuando esta opción no está configurada, el valor predeterminado es 900.000 kilobits por segundo.</p> <p>Esta opción se aplica a Horizon Agent y al cliente. Si los dos endpoints tienen opciones diferentes, se utiliza el valor menor.</p>
Configure the PCoIP session bandwidth floor	<p>Especifica un límite inferior (en kilobits por segundo) para el ancho de banda que reserva la sesión PCoIP.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Esta opción se aplica a Horizon Agent y al cliente, pero solo afecta al endpoint en el que está configurada.</p> <p>Cuando esta opción se modifica durante una sesión PCoIP activa, el cambio se aplica de forma inmediata.</p>

Ajuste	Descripción
Configure the PCoIP session MTU	<p>Especifica el tamaño de la unidad de transmisión máxima (MTU) de los paquetes UDP para una sesión PCoIP.</p> <p>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.</p> <p>El tamaño de MTU máximo es 1.500 bytes. El tamaño de MTU mínimo es 500 bytes. El valor predeterminado es 1.300 bytes.</p> <p>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.</p> <p>Esta opción se aplica a Horizon Agent y al cliente. Si los dos endpoints tienen opciones de tamaño de MTU diferentes, se utilizará el menor tamaño.</p> <p>Si esta opción está deshabilitada o no está configurada, el cliente usa el valor predeterminado en la negociación con Horizon Agent.</p>

Ajuste	Descripción
Configure the PCoIP session audio bandwidth limit	<p>Especifica el ancho de banda máximo que se puede usar para el audio (reproducción de sonido) en una sesión PCoIP.</p> <p>El procesamiento de audio supervisa el ancho de banda que se utiliza para el audio. Este proceso selecciona el algoritmo de compresión de audio que proporciona la mayor calidad de audio de acuerdo al uso actual de ancho de banda. Si se establece un límite para el ancho de banda, el proceso reduce la calidad cambiando la selección del algoritmo de compresión hasta que se alcanza el límite de ancho de banda. Si no se puede proporcionar la calidad de audio mínima con el límite especificado de ancho de banda, se deshabilita el audio.</p> <p>Para admitir audio en estéreo de alta calidad y descomprimido, establezca este valor a uno superior a 1.600 kbit/s. El valor 450 kbit/s, así como valores superiores, admiten audio en estéreo, comprimido y de alta calidad. Un valor que se encuentre entre 50 kbit/s y 450 kbit/s resulta en un audio con una calidad que se encuentra entre la de una radio FM y la de una llamada de teléfono. Un valor por debajo de 50 kbit/s puede resultar en que no se reproduzca el audio.</p> <p>Esta opción se aplica únicamente a Horizon Agent. Debe habilitar el audio en ambos endpoints para que esta opción se aplique.</p> <p>Además, esta opción no se aplica en los dispositivos de audio USB.</p> <p>Si esta opción está deshabilitada o no está configurada, se establece un límite predeterminado de ancho de banda de 500 kilobits por segundo para limitar el algoritmo de compresión de audio seleccionado. Si la opción está configurada, el valor se mide en kilobits por segundo, con un límite de ancho de banda de audio predeterminado de 500 kilobits por segundo.</p> <p>Esta opción se aplica en View 4.6 y versiones posteriores. No se aplica en versiones anteriores de View.</p> <p>Cuando esta opción se modifica durante una sesión PCoIP activa, el cambio se aplica de forma inmediata.</p>
Turn off Build-to-Lossless feature	<p>Especifica si desea activar o desactivar la función Compilación sin pérdida del protocolo PCoIP. Esta función está desactivada de forma predeterminada.</p> <p>Si esta opción está habilitada o no está configurada, la función Compilación sin pérdida está desactivada, y las imágenes y otros contenidos del escritorio y de la aplicación no se compilarán sin pérdidas. En entornos de red con ancho de banda limitado, desactivar la función Compilación sin pérdida puede suponer un ahorro de ancho de banda.</p> <p>Si esta función está deshabilitada, la función Compilación sin pérdida está activada. Se recomienda activar la función Compilación sin pérdida en entornos que requieran que las imágenes y otros contenidos del escritorio y de la aplicación se compilen sin pérdidas.</p> <p>Cuando esta opción se modifica durante una sesión PCoIP activa, el cambio se aplica de forma inmediata.</p> <p>Si desea obtener más información sobre la función Compilación sin pérdida de PCoIP, consulte Función Compilación sin pérdida de PCoIP.</p>

Configuración del teclado para PCoIP

El archivo de plantilla ADMX de PCoIP de View incluye la configuración de directiva de grupo que permite establecer valores de PCoIP que afectan al uso del teclado.

Todas estas configuraciones están en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que se puede sobrescribir** en el Editor de administración de directivas de grupo.

Todas estas configuraciones también están en la carpeta **Configuración de usuario > Directivas > Plantillas administrativas > Variables de las sesiones PCoIP > Configuración del administrador que no se puede sobrescribir** en el Editor de administración de directivas de grupo.

Tabla 5-12. Variables de las sesiones PCoIP de Horizon para el teclado

Ajuste	Descripción
Disable sending CAD when users press Ctrl+Alt+Del	<p>Cuando esta directiva está habilitada, los usuarios deben pulsar Ctrl+Alt+Insert en lugar de Ctrl+Alt+Supr para enviar una secuencia de aviso de seguridad (SAS) al escritorio remoto durante una sesión PCoIP.</p> <p>Es posible que quiera habilitar esta opción si los usuarios se confunden cuando pulsan Ctrl+Alt+Supr para bloquear el endpoint cliente y se envía una SAS al host y al invitado.</p> <p>Esta opción se aplica únicamente a Horizon Agent y no afecta a ningún cliente.</p> <p>Cuando esta directiva no está configurada o está deshabilitada, los usuarios pueden pulsar Ctrl+Alt+Supr o Ctrl+Alt+Insert para enviar una SAS al escritorio remoto.</p>
Use alternate key for sending Secure Attention Sequence	<p>Especifica una tecla alternativa, en lugar de la tecla Insert, para enviar una secuencia de aviso de seguridad (SAS).</p> <p>Puede usar esta opción para mantener la secuencia de teclas Ctrl+Alt+Insert en las máquinas virtuales que se inician desde un escritorio remoto durante una sesión PCoIP.</p> <p>Por ejemplo, un usuario puede iniciar un vSphere Client desde un escritorio PCoIP y abrir una consola en una máquina virtual vCenter Server. Si la secuencia Ctrl+Alt+Insert se usa dentro del sistema operativo invitado en la máquina virtual vCenter Server, se envía una SAS Ctrl+Alt+Supr a la máquina virtual. Esta opción permite que la secuencia Ctrl+Alt+<i>Tecla alternativa</i> envíe una SAS Ctrl+Alt+Supr al escritorio PCoIP.</p> <p>Cuando esta opción está habilitada, debe seleccionar una tecla alternativa del menú desplegable. No puede habilitar la opción sin especificar el valor.</p> <p>Cuando esta opción está deshabilitada o no está configurada, la secuencia de teclas Ctrl+Alt+Insert se utiliza como la SAS.</p> <p>Esta opción se aplica únicamente a Horizon Agent y no afecta a ningún cliente.</p>

Función Compilación sin pérdida de PCoIP

Puede configurar el protocolo de visualización PCoIP para que utilice un enfoque de cifrado denominado compilación progresiva o compilación sin pérdida, que ofrece una experiencia de usuario general óptima aunque las condiciones de la red sean restringidas. Esta función está desactivada de forma predeterminada.

La función de compilación sin pérdida proporciona una imagen inicial muy comprimida, denominada imagen con pérdidas, que se compila de forma progresiva hasta alcanzar un estado sin pérdida. En este estado, la imagen aparece con la fidelidad total esperada.

En una LAN, PCoIP siempre utiliza la compresión sin pérdida para mostrar texto. Si la función de compilación sin pérdida está activada y el ancho de banda disponible por sesión se reduce y es inferior a 1 Mbps, PCoIP muestra inicialmente una imagen de texto con pérdidas y compila rápidamente una imagen sin pérdida. Este enfoque permite que el escritorio siga respondiendo y muestre la mejor imagen posible cuando las condiciones de red sean inestables para ofrecer una experiencia óptima a los usuarios.

La función de compilación sin pérdida tiene las siguientes características:

- Ajusta la calidad de imagen de forma dinámica
- Reduce la calidad de imagen en redes colapsadas
- Disminuye la latencia de actualización de pantalla para mantener la capacidad de respuesta
- Recupera la máxima calidad de imagen cuando la red deja de estar saturada

Para activar la función Compilación sin pérdida, deshabilite la opción de la directiva de grupo Turn off Build-to-Lossless feature. Consulte [Configuración de ancho de banda de PCoIP](#).

Configuración de la directiva VMware Blast

El archivo de plantilla ADMX de la directiva de grupo VMware Blast `vdm_blast.admx` contiene la configuración de directivas del protocolo de visualización VMware Blast. Después de que se aplique la directiva, la configuración se almacena en la clave del registro `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config`.

Estas opciones se aplican a HTML Access y a todos los Horizon Clients.

Tabla 5-13. Configuración de la directiva VMware Blast

Ajuste	Descripción
Max Session Bandwidth	Especifica el ancho de banda máximo, en kilobits por segundo (kbps), para una sesión de VMware Blast. El ancho de banda incluye todo el tráfico de control de VMware Blast y de las imágenes, el audio, el canal virtual y USB. El valor predeterminado es 1 Gbps.
Min Session Bandwidth	Especifica el ancho de banda mínimo, en kilobits por segundo (kbps), reservado para una sesión de VMware Blast. El valor predeterminado es 256 kbps.
Max Bandwidth Slope for the Kbps Per Megapixel	Especifica la pendiente del ancho de banda máximo, en kilobits por segundo (kbps), reservado para una sesión de VMware Blast. El valor mínimo es 100. El valor máximo es 100000. El valor predeterminado es 6200.
Max Frame Rate	Especifica la velocidad máxima de actualizaciones de pantalla. Utilice esta opción para administrar el ancho de banda medio que consumen los usuarios. El valor predeterminado es de 30 actualizaciones por segundo.
UDP Protocol	Especifica si se debe usar el protocolo UDP o el protocolo TCP. El valor predeterminado es utilizar el protocolo UDP. Para esta opción, es necesario reiniciar la máquina de Horizon Agent en la que existe la clave del registro. Esta opción no se aplica a HTML Access, que siempre utiliza el protocolo TCP.

Ajuste	Descripción
H264	Especifica si se usa la codificación H.264 o la codificación JPEG/PNG. De forma predeterminada se usa la codificación H.264.
PNG	<p>Si habilita o no configura esta opción, la codificación PNG está disponible para las sesiones remotas. Si deshabilita esta opción, solo se usa la codificación JPEG para codificar en modo JPEG/PNG. Esta directiva no se aplica cuando el codificador H.264 está activo. Esta opción no está configurada de forma predeterminada.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Screen Blanking	Especifica si la consola de la máquina virtual de escritorio muestra el escritorio que el usuario ve o muestra una pantalla vacía cuando el escritorio tiene una sesión activa. De forma predeterminada, se muestra la pantalla vacía.
Cookie Cleanup Interval	Determina la frecuencia, en milisegundos, en la que se eliminan las cookies asociadas a las sesiones inactivas. El valor predeterminado es 100 ms.
Image Quality	<p>Especifica la calidad de imagen de la pantalla remota. Puede especificar dos opciones de baja calidad, dos opciones de alta calidad y una opción de calidad media. Las opciones de baja calidad se proporcionan para las áreas de la pantalla que cambian a menudo, como, por ejemplo, cuando se produce el desplazamiento. Las opciones de alta calidad se proporcionan para las áreas más estáticas de la pantalla, lo que ofrece una mejor calidad de la imagen. Puede especificar las siguientes opciones:</p> <ul style="list-style-type: none"> ■ Calidad JPEG baja (rango de valores disponibles: 1 - 100, predeterminado: 25) ■ Submuestreo de croma de JPEG de baja calidad (rango de valores disponibles: 4:1:0 (el más bajo) 4:1:1, 4:2:0, 4:2:2 y 4:4:4 (el más alto), predeterminado: 4:1:0) ■ Calidad JPEG media (rango de valores disponibles: 1 - 100, predeterminado: 35) ■ Calidad JPEG alta (rango de valores disponibles: 1 - 100, predeterminado: 90) ■ Submuestreo de croma de JPEG de alta calidad (rango de valores disponibles: 4:1:0 (el más bajo) 4:1:1, 4:2:0, 4:2:2 y 4:4:4 (el más alto), predeterminado: 4:4:4)
H.264 Quality	<p>Especifica la calidad de la imagen para la pantalla remota configurada para usar la codificación H.264. Puede especificar los valores de cuantificación mínimos y máximos que determinan el nivel de control sobre una imagen en cuanto a la compresión sin pérdida. Puede especificar un valor mínimo de cuantificación para obtener la mejor calidad de imagen. Puede especificar un valor máximo de cuantificación para obtener la calidad de imagen más baja. Puede especificar las siguientes opciones:</p> <ul style="list-style-type: none"> ■ H264maxQP (rango de valores disponibles: 0-51, predeterminado: 36) ■ H264minQP (rango de valores disponibles: 0-51, predeterminado: 10) <p>Para obtener la mejor calidad de imagen, establezca los valores de cuantificación entre +5 y -5 del rango disponible de valores.</p>
HTTP Service	Especifica el puerto que se usará para la comunicación segura (HTTPS) entre el servidor de seguridad o el dispositivo de Access Point y un escritorio. El firewall debe estar configurado para tener este puerto abierto. El valor predeterminado es 22443.
Audio playback	Especifica si la reproducción de audio está habilitada para los escritorios remotos. Esta opción se usa para habilitar la reproducción de audio.

Ajuste	Descripción
Configure clipboard redirection	<p>Especifica el comportamiento permitido para el redireccionamiento del portapapeles. Las opciones son:</p> <ul style="list-style-type: none"> ■ Habilitado en ambas direcciones ■ Deshabilitado en ambas direcciones ■ Habilitado solo de cliente a servidor (los usuarios pueden copiar y pegar solo desde el cliente al escritorio). ■ Habilitado solo de servidor a cliente (los usuarios pueden copiar y pegar solo desde el escritorio al cliente). <p>El predeterminado es Habilitado solo de cliente a servidor.</p>
Clipboard memory size on server(in kilobytes)	<p>Especifica el valor del tamaño de la memoria del portapapeles del servidor, en kilobytes. El cliente también tiene un valor del tamaño de la memoria del portapapeles. Una vez que se configura la sesión, el servidor envía el valor del tamaño de la memoria del portapapeles al cliente. El valor efectivo del tamaño de la memoria del portapapeles es el menor de los valores del tamaño de la memoria del portapapeles del cliente y del servidor.</p> <p>Puede especificar un valor mínimo de 512 kilobytes y un valor máximo de 16384 kilobytes. Si especifica 0 o no especifica ningún valor, el tamaño de la memoria del portapapeles del servidor es 1.024 kilobytes.</p> <p>Esta opción solo es compatible con la versión 7.0.1 y posteriores, y con los clientes Windows, Linux o Mac en los que esté instalado Horizon Client 4.1 o versiones posteriores. En versiones anteriores, el tamaño de la memoria del portapapeles es 1 MB.</p> <p>Nota En función de la red, si el tamaño de la memoria del portapapeles es muy grande, el rendimiento puede verse afectado de forma negativa. VMware le recomienda que no asigne al tamaño de memoria del portapapeles un valor superior a 16 MB.</p>
Keyboard locale synchronization	<p>Especifica si la lista de configuraciones locales del teclado y la configuración local por defecto del teclado se sincronizan con la aplicación o el escritorio remotos. Si esta opción está habilitada, se produce la sincronización. Esta opción solo se aplica a Horizon Agent.</p> <p>Nota Esta función solo es compatible con Horizon Client para Windows.</p>
Configure file transfer	<p>Especifica el comportamiento permitido para la transferencia de archivos entre un escritorio remoto y el cliente HTML Access. Puede seleccionar uno de estos valores:</p> <ul style="list-style-type: none"> ■ Carga y descarga deshabilitadas ■ Carga y descarga habilitadas ■ Solo carga de archivos habilitada (los usuarios solo pueden cargar archivos desde el sistema cliente al escritorio remoto). ■ Solo descarga de archivos habilitada (los usuarios solo pueden descargar archivos desde el escritorio remoto al sistema cliente). <p>El valor predeterminado es Solo carga de archivos habilitada.</p> <p>Esta opción solo se aplica a la versión 7.0.1 y a HTML Access 4.1 y sus respectivas versiones posteriores.</p>
Filter text out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos textuales a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>

Ajuste	Descripción
Filter Rich Text Format data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto enriquecido a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter images out of the incoming clipboard data	<p>Especifica si se deben filtrar las imágenes a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto de Microsoft Office (formato BIFF12) a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos de gráficos y SmartArt de Microsoft Office (Art::GVML ClipFormat) a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Text Effects data out of the incoming clipboard data	<p>Especifica si se deben filtrar los datos de efectos de texto de Microsoft Office (formato HTML) a partir de los datos del portapapeles que provienen del cliente y se dirigen al agente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter text out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos textuales de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Rich Text Format data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto enriquecido de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter images out of the outgoing clipboard data	<p>Especifica si se deben filtrar las imágenes de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Office text data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos en formato de texto Microsoft Office (formato BIFF12) de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>

Ajuste	Descripción
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos de gráficos y SmartArt de Microsoft Office (Art::GVML ClipFormat) de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>
Filter Microsoft Text Effects data out of the outgoing clipboard data	<p>Especifica si se deben filtrar los datos de efectos de texto de Microsoft Office (formato HTML) de los datos del portapapeles que provienen del agente y se dirigen al cliente. Cuando esta opción está habilitada y la casilla de verificación está seleccionada, los datos se filtran. Cuando esta opción está deshabilitada o no está configurada, los datos se incluyen.</p> <p>Esta opción se aplica a la versión 7.0.2 y posteriores.</p>

Aplicar la configuración de la directiva VMware Blast

Si las siguientes directivas de VMware Blast cambian durante una sesión cliente, Horizon Client detecta el cambio y aplica inmediatamente la nueva opción.

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

Para el resto de directivas de VMware Blast, se aplican las reglas de actualización del GPO de Microsoft. Los GPO se pueden actualizar de forma manual o reiniciando la máquina Horizon Agent. Para obtener más información, consulte la documentación de Microsoft.

Habilitar Compresión sin pérdida de información para VMware Blast

Puede habilitar el protocolo de visualización VMware Blast para que utilice un enfoque de cifrado denominado compilación progresiva o compilación sin pérdida. Esta función proporciona una imagen inicial muy comprimida, denominada imagen con pérdidas, que se compila de forma progresiva hasta alcanzar un estado sin pérdida. En este estado, la imagen aparece con la fidelidad total esperada.

Para habilitar la compresión sin pérdida para VMware Blast, establezca la clave EncoderBuildToPNG en 1 en la carpeta HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config del Registro de Windows en el equipo del agente. El valor predeterminado es 0 (deshabilitado), lo que significa que el códec no se compila a PNG, que es un formato sin pérdida.

Los cambios en la configuración de la clave `EncoderBuildToPNG` se aplican inmediatamente.

Nota Habilitar la compresión sin pérdida de información para VMware Blast provoca un aumento del ancho de banda y del uso de CPU. VMware le recomienda que use el protocolo de visualización PCoIP en lugar de VMware Blast si necesita compresión sin pérdida. Para obtener información sobre la configuración de la compresión sin pérdida para PCoIP, consulte [Función Compilación sin pérdida de PCoIP](#).

Usar Servicios de Escritorio remoto de directivas de grupo

Las directivas de grupo de Servicios de Escritorio remoto permiten controlar la configuración y el rendimiento de los hosts RDS y de las sesiones de aplicaciones y de escritorios RDS. Horizon 7 proporciona un archivo ADMX que contiene las directivas de grupo de RDS de Microsoft que son compatibles con Horizon 7.

Como práctica recomendada, configure las directivas de grupo proporcionadas en el archivo ADMX de Horizon 7, en lugar de usar las directivas de grupo de Microsoft correspondientes. Se certificó la compatibilidad de las directivas de grupo de Horizon 7 con su implementación de Horizon 7.

Agregar el archivo ADMX de Servicios de Escritorio remoto a Active Directory

Puede agregar la configuración de directiva del archivo ADMX de Servicios de Escritorio remoto a objetos de directivas de grupos (Group Policy Object, GPO) de Active Directory.

También puede instalar el archivo ADMX de Servicios de Escritorio remoto en hosts RDS individuales. En un host RDS individual, use el Editor de directivas de grupo local (`gpedit.msc`) para editar la configuración de directiva de grupo.

Requisitos previos

- Cree los GPO para la configuración de directiva de grupo de Servicios de Escritorio remoto y vincúlelos a la OU que contenga sus hosts RDS.
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Administración de directivas de grupo y MMC en su servidor de Active Directory.

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyyy*.zip, donde *x.x.x* es la versión y *yyyyyyyy* es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyyy*.zip y copie los archivos ADML y ADMX de Servicios de Escritorio remoto al servidor de Active Directory.
 - a Copie el archivo vmware_rdsh_server.admx a la carpeta C:\Windows\PolicyDefinitions del servidor de Active Directory.
 - b (opcional) Copie el archivo de recursos de idioma vmware_rdsh_server.adml a la subcarpeta adecuada en C:\Windows\PolicyDefinitions\ del servidor de Active Directory.
- 3 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo.

La configuración de directiva de grupo de Servicios de Escritorio remoto se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto**.

Algunas opciones de configuración de directiva de grupo de Servicios de Escritorio remoto también se instalan en la carpeta **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto**.
- 4 (opcional) Establezca la configuración de directiva de grupo en la carpeta **Servicios de Escritorio remoto > Host de sesión de Escritorio remoto**.

Configuración de compatibilidad de aplicación con RDS

La configuración de la directiva de grupo de compatibilidad de aplicación con RDS controla la compatibilidad con Windows Installer, la virtualización de IP de escritorio, la selección de adaptador de red y el uso de la dirección IP de host RDS.

Tabla 5-14. Configuración de la directiva de grupo de compatibilidad de aplicación con RDS

Ajuste	Descripción
Turn off Windows Installer RDS Compatibility	<p>Esta opción de directiva especifica si la compatibilidad de RDS con Windows Installer se ejecuta por usuario en las aplicaciones instaladas completamente. Windows Installer solo permite que se ejecute una instancia del proceso <code>msiexec</code> a la vez. De forma predeterminada, la compatibilidad de RDS con Windows Installer está activada.</p> <p>Si habilita esta opción de directiva, la compatibilidad de RDS con Windows Installer se desactiva, y solo puede ejecutarse una instancia del proceso <code>msiexec</code> a la vez.</p> <p>Si deshabilita o no configura esta opción de directiva, la compatibilidad de RDS con Windows Installer se activa, y el proceso <code>msiexec</code> pone en cola y gestiona las solicitudes de instalación de aplicaciones por usuario en el orden en el que se reciban.</p>
Turn on Remote Desktop IP Virtualization	<p>Esta opción de directiva especifica si la Virtualización de IP de escritorio remoto está activada.</p> <p>De forma predeterminada, la Virtualización de IP de escritorio remoto está desactivada.</p> <p>Si habilita esta opción de directiva, la Virtualización de IP de escritorio remoto se activará. Puede seleccionar el modo en el que se aplica esta opción. Si usa el modo Por programa, debe introducir una lista de programas para usar direcciones IP virtuales. Agregue cada programa en una línea independiente, sin dejar líneas en blanco entre programas. Por ejemplo:</p> <pre>explorer.exe mstsc.exe</pre> <p>Si deshabilita o no configura esta opción de directiva, la Virtualización de IP de escritorio remoto se desactivará.</p>

Ajuste	Descripción
Select the network adapter to be used for Remote Desktop IP Virtualization	<p>Esta opción de directiva especifica la dirección IP y la máscara de red que corresponden al adaptador de red utilizado para direcciones IP virtuales. Debe usar la notación de enrutamiento de interdominios sin clases para introducir la dirección IP y la máscara de red. Por ejemplo: 192.0.2.96/24.</p> <p>Si habilita esta opción de directiva, la dirección IP y la máscara de red especificadas se usarán para seleccionar el adaptador de red de las direcciones IP virtuales.</p> <p>Si deshabilita o no configura esta opción de directiva, la Virtualización de IP de escritorio remoto se desactivará. Para que la Virtualización de IP de escritorio remoto funcione, debe configurar un adaptador de red.</p>
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	<p>Esta configuración de directiva especifica si una sesión usa la dirección IP del host RDS si no hay ninguna dirección IP virtual disponible.</p> <p>Si habilita esta configuración de directiva, la dirección IP del host RDS no se usa si no hay ninguna IP virtual disponible. La sesión no tendrá conectividad de red.</p> <p>Si deshabilita o no configura esta configuración de directiva, la dirección IP del host RDS se usa si no hay ninguna IP virtual disponible.</p>

Configuración de conexiones RDS

La configuración de directiva de grupo de conexiones RDS permite a los usuarios establecer directivas para las conexiones a las sesiones en los hosts RDS.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Conexiones**.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Conexiones**.

Tabla 5-15. Configuración de la directiva de grupo de conexiones RDS

Ajuste	Descripción
Automatic reconnection	<p>Especifica si se debe permitir eliminar a los clientes de conexión a escritorio remoto para volver a conectarse automáticamente a las sesiones en un host RDS, en caso de que su conexión de red se pierde temporalmente. De forma predeterminada, se realiza un máximo de veinte intentos de reconexión en intervalos de cinco segundos.</p> <p>Si habilita esta directiva, se intentará volver a conectar automáticamente a todos los clientes que estén ejecutando la conexión a escritorio remoto cuando estos pierdan su conexión de red.</p> <p>Si deshabilita esta configuración de directiva, está prohibida la reconexión automática de los clientes.</p> <p>Si no establece esta configuración de directiva, no se especifica la reconexión automática en el nivel de directiva de grupo. Sin embargo, los usuarios pueden configurar la reconexión automática mediante la casilla de verificación Volver a conectar si se pierde la conexión en la pestaña Experiencia en la conexión a escritorio remoto.</p>
Allow users to connect remotely using Remote Desktop Services	<p>Esta configuración de directiva determina el acceso remoto a equipos con Servicios de Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, los usuarios que sean miembros del grupo de usuarios de Escritorio remoto en el equipo de destino se pueden conectar de forma remota al equipo de destino con Servicios de Escritorio remoto.</p> <p>Si deshabilita esta configuración de directiva, los usuarios no se pueden conectar de forma remota al equipo de destino con Servicios de Escritorio remoto. El equipo de destino mantendrá las conexiones actuales, pero no aceptará ninguna conexión entrante nueva.</p> <p>Si no establece esta configuración de directiva, Servicios de Escritorio remoto utilizará la configuración de Escritorio remoto en el equipo de destino para determinar si se permite la conexión remota. Esta configuración se encuentra en la pestaña Remoto en Propiedades del sistema. De forma predeterminada, no se permite la conexión remota.</p> <p>Nota Puede limitar qué clientes pueden conectarse de forma remota con los Servicios de Escritorio remoto si configura la configuración de directiva "Requerir la autenticación del usuario para las conexiones remotas mediante Autenticación a nivel de red" ubicada en la carpeta Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Seguridad. Puede limitar el número de usuarios que se pueden conectar simultáneamente si configura la opción Número máximo de conexiones en la pestaña Adaptador de red en la herramienta de configuración de host de sesión de Escritorio remoto o si configura la configuración de directiva "Limitar número de conexiones" ubicada en la carpeta Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Conexiones.</p>

Ajuste	Descripción
Deny logoff of an administrator logged in to the console session	<p>Esta configuración de directiva determina si un administrador que intenta conectarse de forma remota a la consola de un servidor puede cerrar la sesión de un administrador que tiene una sesión iniciada en la consola.</p> <p>Esta directiva es útil cuando el administrador que está conectado no desea que otro administrador le cierre la sesión. Si se cierra la sesión del administrador conectado, se perderán todos los datos que no se hayan guardado previamente.</p> <p>Si habilita esta configuración de directiva, no será posible cerrar la sesión del administrador conectado.</p> <p>Si deshabilita o no configura este ajuste de directiva, será posible cerrar la sesión del administrador conectado.</p> <p>Nota La sesión de la consola se conoce también como Sesión 0. Se puede obtener acceso a la consola mediante el conmutador / console desde el campo de nombre del equipo en Conexión a Escritorio remoto o desde la línea e comandos.</p>
Configure keep-alive connection interval	<p>Esta configuración de directiva permite especificar un intervalo entre mensajes de mantenimiento de conexión para garantizar que el estado de la sesión en el host RDS sea coherente con el estado del cliente.</p> <p>Después de que un cliente pierda la conexión a un host RDS, la sesión en dicho host RDS puede permanecer activa en lugar de desconectarse, incluso si el cliente se desconecta físicamente del host RDS. Si el cliente inicia sesión de nuevo en el mismo host RDS, puede establecerse una nueva sesión (si la configuración del host RDS permite varias sesiones) y la sesión original puede permanecer activa.</p> <p>Si habilita esta configuración de directiva, debe especificar un intervalo entre mensajes de mantenimiento de conexión. El intervalo entre mensajes de mantenimiento de conexión determina la frecuencia (en minutos) con la que el servidor comprueba el estado de la sesión. El intervalo de valores que se puede escribir es de 1 a 999.999.</p> <p>Si deshabilita o no configura este ajuste de directiva, no se establecerá ningún intervalo entre mensajes de mantenimiento de conexión y el servidor no comprobará el estado de la sesión.</p>

Ajuste	Descripción
Limit number of connections	<p>Especifica si Servicios de Escritorio remoto limita el número de conexiones simultáneas al servidor.</p> <p>Puede usar esta opción para restringir el número de sesiones remotas que pueden estar activas en un servidor. Si se excede este número, los demás usuarios que intenten conectarse recibirán un mensaje de error que indica que el servidor está ocupado para que lo vuelvan a intentar más tarde. La restricción del número de sesiones mejora el rendimiento porque hay menos sesiones que consumen recursos del sistema. De forma predeterminada, los host RDS permiten un número ilimitado de sesiones de Servicios de Escritorio remoto, y Escritorio remoto para administración permite dos sesiones de Servicios de Escritorio remoto.</p> <p>Para usar esta opción, escriba el número de conexiones que desea especificar como el número máximo para el servidor. Para especificar un número ilimitado de conexiones, escriba 9999999.</p> <p>Si habilita esta configuración de directiva, el número máximo de conexiones está limitado al número especificado coherente con la versión de Windows y el modo de Servicios de Escritorio remoto que se está ejecutando en el servidor.</p> <p>Si deshabilita o no configura este ajuste de directiva, los límites en el número de conexiones no se aplican en el nivel de directiva de grupo.</p> <p>Nota Esta opción de configuración está diseñada para usarse en hosts RDS, es decir, en servidores que ejecutan Windows con el servicio de rol de host de sesión de Escritorio remoto instalado.</p>
Set rules for remote control of Remote Desktop Services user sessions	<p>Utilice esta configuración de directiva para especificar el nivel de control remoto permitido en una sesión de Servicios de Escritorio remoto.</p> <p>Puede usar esta configuración de directiva para seleccionar uno de los dos niveles de control remoto: Ver sesión o Control total. Ver sesión permite que el usuario de control remoto visualice una sesión. Control total permite al administrador interactuar con la sesión. El control remoto puede establecerse con o sin permisos del usuario.</p> <p>Si se habilita esta configuración de directiva, los administradores pueden interactuar de forma remota con una sesión de Servicios de Escritorio remoto del usuario según las reglas especificadas. Para establecer dichas reglas, seleccione el nivel de control y permisos deseados en la lista Opciones. Para deshabilitar el control remoto, seleccione "Control remoto no permitido".</p> <p>Si se deshabilita o no se configura esta configuración de directiva, las reglas de control remoto se determinan mediante la configuración de la pestaña Control remoto en la herramienta de configuración de host de sesión de Escritorio remoto. De manera predeterminada, los usuarios de control remoto tienen total control de la sesión con permisos del usuario.</p> <p>Nota Esta configuración de directiva aparece tanto en Configuración del equipo como en Configuración de usuario. Si se establecen ambas configuraciones de directiva, tiene prioridad la de Configuración del equipo.</p>

Ajuste	Descripción
Restrict Remote Desktop Services users to a single Remote Desktop Services session	<p>Utilice esta configuración de directiva para restringir a los usuarios a una sola sesión de Servicios de Escritorio remoto.</p> <p>Si se habilita esta configuración de directiva, los usuarios que inician sesión de forma remota a través de Servicios de Escritorio remoto quedarán limitados a una sola sesión en ese servidor (activa o desconectada). Si el usuario abandona la sesión en estado de desconexión, se volverá a conectar automáticamente a esa sesión en el próximo inicio de sesión.</p> <p>Si deshabilita esta configuración de directiva, los usuarios podrán establecer un número ilimitado de conexiones remotas simultáneas mediante Servicios de Escritorio remoto.</p> <p>Si no se configura esta configuración de directiva, la configuración "Restringir cada usuario a una sesión" de la herramienta de configuración de host de sesión de Escritorio remoto, determinará si se restringe a los usuarios a una sola sesión remota.</p>
Allow remote start of unlisted programs	<p>Utilice esta configuración de directiva para especificar si los usuarios remotos pueden iniciar cualquier programa en host RDS cuando inician una sesión de Servicios de Escritorio remoto o si solo pueden iniciar los programas que aparecen en la lista Programas RemoteApp.</p> <p>Puede controlar qué programas se pueden iniciar remotamente en un host RDS usando la herramienta Administrador de RemoteApp para crear una lista de programas RemoteApp. De forma predeterminada, solo los programas de la lista de programas de RemoteApp pueden iniciarse cuando el usuario inicia una sesión de Servicios de Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, los usuarios remotos podrán iniciar cualquier programa en el host RDS cuando inicien una sesión de Servicios de Escritorio remoto. Por ejemplo, un usuario remoto puede iniciar cualquier programa si especifica la ruta de acceso del ejecutable del programa en el momento de la conexión mediante el cliente de Conexión a Escritorio remoto.</p> <p>Si deshabilita o no establece esta configuración de directiva, los usuarios remotos solo podrán iniciar los programas que se muestren en la lista de programas de RemoteApp cuando inicien una sesión de Servicios de Escritorio remoto.</p>
Turn off Fair Share CPU Scheduling	<p>La Programación de reparto justo de CPU distribuye de manera dinámica el tiempo de procesador a sesiones de Servicios de Escritorio remoto del mismo host RDS en función del número de sesiones y de la demanda de tiempo del procesador en cada una de ellas.</p> <p>Si habilita esta opción de directiva, la programación de reparto justo de CPU se desactivará.</p> <p>Si deshabilita o no configura esta opción de directiva, la programación de reparto justo de CPU se activará.</p>

Configuración de redirección de dispositivo o recurso de RDS

La configuración de la directiva de grupo de redirección de dispositivo o recurso de RDS controla el acceso a los dispositivos y a los recursos de un equipo cliente en sesiones de Servicios de Escritorio remoto.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Redirección de dispositivo o recurso**.

La configuración de directiva de grupo de RDS de Horizon 7 también se instala en la carpeta **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Redirección de dispositivo o recurso**.

Tabla 5-16. Configuración de la directiva de grupo Redirección de dispositivo o recurso de RDS

Ajuste	Descripción
Allow audio and video playback redirection	<p>Utilice esta configuración de directiva para especificar si los usuarios pueden redirigir la salida de audio y vídeo del equipo remoto durante una sesión de Servicios de Escritorio remoto.</p> <p>Para especificar dónde reproducir la salida de audio del equipo remoto, los usuarios pueden configurar las opciones de audio remoto en la pestaña Recursos locales de Conexión a Escritorio remoto (RDC). Los usuarios pueden elegir si quieren reproducir el audio remoto en el equipo remoto o en el equipo local. También pueden elegir no reproducir el audio. La reproducción de vídeo se puede configurar mediante la opción de reproducción de vídeo de un archivo .rdp (Protocolo de escritorio remoto). De forma predeterminada, la reproducción de vídeo está habilitada.</p> <p>También de forma predeterminada, no se permite la redirección de audio y vídeo cuando se conecta con un equipo que ejecuta Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003. La reproducción de audio y vídeo se permite de forma predeterminada cuando se conecta con un equipo que ejecuta Windows 7, Windows Vista o Windows XP Professional.</p> <p>Si habilita esta configuración de directiva, se permitirá la redirección de la reproducción de audio y vídeo.</p> <p>Si deshabilita esta configuración de directiva, no se permitirá la redirección de la reproducción de audio y vídeo, aunque se especifique la redirección de la reproducción de audio en RDC o de vídeo en el archivo .rdp.</p> <p>Si no configura esta directiva, la configuración de reproducción de audio y vídeo de la pestaña Configuración del cliente de la herramienta de configuración de host de sesión de Escritorio remoto será la que determine si se permite la redirección de la reproducción de audio y vídeo.</p>
Allow audio recording redirection	<p>Utilice esta configuración de directiva para especificar si los usuarios pueden grabar audio en un equipo remoto durante una sesión de Servicios de Escritorio remoto.</p> <p>Para especificar si graban audio en el equipo remoto, los usuarios pueden configurar las opciones de audio remoto en la pestaña Recursos locales de Conexión a Escritorio remoto (RDC). Los usuarios pueden grabar audio mediante un dispositivo de entrada de audio en el equipo local, como un micrófono integrado.</p> <p>De forma predeterminada, no se permite la redirección de la grabación de audio cuando se conecta con un equipo que ejecuta Windows Server 2008 R2. La redirección de la grabación de audio se permite de forma predeterminada cuando se conecta con un equipo que ejecuta Windows 7.</p> <p>Si habilita esta configuración de directiva, se permitirá la redirección de la grabación de audio.</p> <p>Si deshabilita esta configuración de directiva, no se permitirá la redirección de la grabación de audio, aunque se especifique la redirección de la grabación de audio en RDC.</p> <p>Si no configura esta directiva, la configuración de grabación de audio de la pestaña Configuración del cliente de la herramienta de configuración de host de sesión de Escritorio remoto será la que determine si se permite la redirección de la grabación de audio.</p>

Ajuste	Descripción
Limit audio playback quality	<p>Utilice esta configuración de directiva para limitar la calidad de la reproducción de audio durante una sesión de Servicios de Escritorio remoto. Limitar la calidad de la reproducción de audio puede mejorar el rendimiento de la conexión, en particular con vínculos lentos.</p> <p>Si habilita esta configuración de directiva, debe seleccionar una de las siguientes opciones: Alta, Media o Dinámica. Si selecciona Alta, el audio se enviará sin compresión y con latencia mínima. Esto requiere una gran cantidad de ancho de banda. Si selecciona Media, el audio se enviará con algo de compresión y con latencia mínima según determine el códec que se esté usando. Si selecciona Dinámica, el audio se enviará con el nivel de compresión que determine el ancho de banda de la conexión remota.</p> <p>La calidad de reproducción de audio que especifique en el equipo remoto mediante esta configuración de directiva es la calidad máxima que se podrá usar en una sesión de Servicios de Escritorio remoto, independientemente de la calidad de reproducción de audio configurada en el equipo cliente. Por ejemplo, si el nivel de calidad de reproducción de audio configurado en el equipo cliente es más alto que el configurado en el equipo remoto, se usará el nivel que sea más bajo.</p> <p>La calidad de reproducción de audio se puede configurar en el equipo cliente mediante la opción de modo de calidad de audio de un archivo de Protocolo de escritorio remoto (.rdp). De forma predeterminada, la calidad de reproducción de audio se establece en Dinámica.</p>
Do not allow clipboard redirection	<p>Especifica si se debe impedir el uso compartido del contenido del Portapapeles (redirección del Portapapeles) entre un equipo remoto y un equipo cliente durante una sesión de Servicios de Escritorio remoto.</p> <p>Puede usar esta configuración para impedir que los usuarios redirijan datos del Portapapeles a, y desde, el equipo remoto y el equipo local. De forma predeterminada, Servicios de Escritorio remoto permite la redirección del Portapapeles.</p> <p>Si habilita esta configuración de directiva, los usuarios no podrán redirigir los datos del Portapapeles.</p> <p>Si deshabilita esta configuración de directiva, Servicios de Escritorio remoto permitirá siempre la redirección del Portapapeles.</p> <p>Si no establece esta configuración de directiva, la redirección del Portapapeles no se especificará en el nivel de directiva de grupo. Sin embargo, un administrador podrá seguir deshabilitando la redirección del Portapapeles usando la herramienta de configuración de host de sesión de Escritorio remoto.</p>

Ajuste	Descripción
Do not allow COM port redirection	<p>Especifica si se impide o no la redirección de datos a los puertos COM de cliente desde el equipo remoto en una sesión de Servicios de Escritorio remoto.</p> <p>Puede utilizar esta configuración para impedir que los usuarios redirijan datos a periféricos de puertos COM o asignen puertos COM locales mientras mantienen una sesión de Servicios de Escritorio remoto. De forma predeterminada, Servicios de Escritorio remoto permite esta redirección de puertos COM.</p> <p>Si habilita esta configuración de directiva, los usuarios no podrán redirigir datos del servidor al puerto COM local.</p> <p>Si deshabilita esta configuración de directiva, Servicios de Escritorio remoto permitirá siempre la redirección al puerto COM.</p> <p>Si no establece esta configuración de directiva, la redirección al puerto COM no se especificará en el nivel de directiva de grupo. Sin embargo, un administrador podrá seguir deshabilitando la redirección de puertos COM usando la herramienta de configuración de host de sesión de Escritorio remoto.</p>
Do not allow drive redirection	<p>Especifica si se debe impedir la asignación de unidades cliente en una sesión de Escritorio remoto (redirección de unidad).</p> <p>De forma predeterminada, el servidor de host de sesión de Escritorio remoto asigna unidades cliente automáticamente al conectarse. Las unidades asignadas aparecen en el árbol de carpetas de sesión en el Explorador de Windows o en Equipo con el formato <letraDeUnidad> en <nombreDeEquipo>. Puede usar esta opción para invalidar este comportamiento.</p> <p>Si habilita esta configuración, no se permite la redirección de la unidad de cliente en sesiones de Servicios de Escritorio remoto.</p> <p>Si deshabilita esta configuración, se permite siempre la redirección de la unidad de cliente.</p> <p>Si no se establece esta configuración, la redirección de la unidad de cliente no se especificará en el nivel de directiva de grupo. Sin embargo, un administrador podrá seguir deshabilitando la redirección de unidad de cliente mediante la herramienta de configuración de host de sesión de Escritorio remoto.</p>

Ajuste	Descripción
Do not allow LTP Port redirection	<p>Especifica si se impide la redirección de datos a puertos LPT de cliente durante una sesión de Servicios de Escritorio remoto.</p> <p>Puede usar esta configuración para impedir a los usuarios asignar puertos LPT locales y redirigir datos desde el equipo remoto a periféricos de puertos locales LPT. De forma predeterminada, Servicios de Escritorio remoto permite la redirección de puertos LPT.</p> <p>Si habilita esta configuración de directiva, los usuarios de una sesión de Servicios de Escritorio remoto no pueden redirigir datos del servidor al puerto LPT local.</p> <p>Si deshabilita esta configuración de directiva, se permitirá siempre la redirección a puertos LPT.</p> <p>Si no establece esta configuración de directiva, la redirección de puertos LPT no se especificará en el nivel de directiva de grupo. Sin embargo, un administrador podrá seguir deshabilitando la redirección de puertos locales LPT usando la herramienta de configuración de host de sesión de Escritorio remoto.</p>
Do not allow supported Plug and Play device redirection	<p>Utilice esta configuración de directiva para controlar la redirección de los dispositivos Plug and Play compatibles, como los dispositivos portátiles de Windows, al equipo remoto de una sesión de Servicios de Escritorio remoto.</p> <p>De forma predeterminada, Servicios de Escritorio remoto permite el redireccionamiento de dispositivos Plug and Play compatibles. Los usuarios pueden utilizar la opción "Más" en la pestaña Recursos locales de conexión a Escritorio remoto para elegir los dispositivos Plug and Play compatibles para redirigir al equipo remoto.</p> <p>Si habilita esta configuración de directiva, los usuarios no pueden redireccionar sus dispositivos Plug and Play compatibles al equipo remoto.</p> <p>Si deshabilita o no establece esta configuración de directiva, los usuarios pueden redireccionar sus dispositivos Plug and Play compatibles al equipo remoto.</p> <p>Nota También puede impedir el redireccionamiento de dispositivos Plug and Play compatibles en la pestaña de configuración del cliente en la herramienta de configuración de host de sesión de Escritorio remoto. Se puede impedir el redireccionamiento de tipos específicos de dispositivos Plug and Play compatibles mediante la opción de opciones de directiva en la carpeta Configuración del equipo > Plantillas administrativas > Sistema > Instalación del dispositivo > Restricciones de instalación del dispositivo.</p>

Ajuste	Descripción
Do not allow smart card device redirection	<p>Utilice esta configuración de directiva para controlar la redirección de los dispositivos de tarjeta inteligente en una sesión de Servicios de Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, los usuarios de Servicios de Escritorio remoto no podrán usar una tarjeta inteligente para iniciar una sesión de Servicios de Escritorio remoto.</p> <p>Si deshabilita o no configura este ajuste de directiva, se permitirá la redirección de dispositivos de tarjeta inteligente. De forma predeterminada, Servicios de Escritorio remoto redirige automáticamente los dispositivos de tarjeta inteligente durante la conexión.</p> <hr/> <p>Nota El equipo cliente debe ejecutar como mínimo Microsoft Windows 2000 Server o Microsoft Windows XP Professional, y el servidor de destino debe estar unido a un dominio.</p>
Allow time zone redirection	<p>Esta opción de directiva determina si el equipo cliente redirecciona su configuración de zona horaria a la sesión de Servicios de Escritorio remoto.</p> <p>Si habilita esta opción de directiva, los clientes que puedan redirigir su zona horaria enviarán su información de zona horaria al servidor. La hora de base del servidor se usará entonces para calcular la hora de la sesión actual (hora de la sesión actual = hora de base del servidor + zona horaria del cliente).</p> <p>Si deshabilita o no configura esta opción de directiva, el equipo cliente no redirigirá su información de zona horaria y la zona horaria de la sesión será la misma que la del servidor.</p>

Configuración de licencias de RDS

La configuración de la directiva de grupo de licencias de RDS controla el orden en el que se encuentran los servidores de licencias, si se muestran avisos de problemas y si se usan licencias Por usuario o Por dispositivo para las licencias de acceso de cliente de Servicios de Escritorio remoto (CAL).

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Licencias**.

Tabla 5-17. Configuración de la directiva de grupo de licencias de RDS

Configuración	Descripción
Use the specified Remote Desktop license servers	<p>Esta configuración de directiva le permite especificar el orden en el que un servidor de host RDS busca los servidores de licencias del Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, un servidor de host RDS intenta primero encontrar los servidores de licencias que especifique. Si no puede encontrarlos, el servidor de host RDS intentará detectar servidores de licencias automáticamente.</p> <p>En el proceso de detección automática de servidores de licencias, un servidor de host RDS de un dominio basado en Windows Server intenta contactar con un servidor de licencias en el siguiente orden:</p> <ol style="list-style-type: none"> 1 Servidores de licencias especificados en la herramienta de configuración de host de sesión de Escritorio remoto. 2 Servidores de licencias publicados en los Servicios de dominio de Active Directory. 3 Servidores de licencias instalados en controladores de dominio en el mismo dominio que el host RDS. <p>Si deshabilita o no establece esta configuración de directiva, el host RDS usa el modo de detección de servidores de licencias especificado en la herramienta de configuración de host de sesión de Escritorio remoto.</p>
Hide notifications about RD Licensing problems that affect the RD Session Host server	<p>Esta configuración de directiva determina si se muestran notificaciones en un host RDS cuando se producen problemas con la licencia de Escritorio remoto que afecten al host RDS.</p> <p>Si se detectan problemas con la licencia de Escritorio remoto que afecten al host RDS, de forma predeterminada se mostrarán notificaciones en un host RDS después de que inicie sesión como administrador local. Si procede, también se mostrará una notificación con el número de días que quedan para que se agote el período de gracia de la licencia del host RDS.</p> <p>Si habilita esta configuración de directiva, estas notificaciones no se mostrarán en el host RDS.</p> <p>Si deshabilita o no establece esta configuración de directiva, estas notificaciones se mostrarán en el host RDS después de que inicie sesión como administrador local.</p>
Set the Remote Desktop licensing mode	<p>Esta configuración de directiva le permite especificar el tipo de licencia de acceso de cliente de Servicios de Escritorio remoto (CAL de Escritorio remoto) que se necesita para conectarse a este host RDS.</p> <p>Puede usar esta configuración de directiva para seleccionar uno de los dos modos de licencia: Por usuario o Por dispositivo.</p> <p>El modo de licencia Por usuario requiere que cada cuenta de usuario que se conecte a este host RDS tenga una CAL Por usuario de Escritorio remoto.</p> <p>El modo de licencia Por dispositivo requiere que cada dispositivo que se conecte a este host RDS tenga una CAL Por dispositivo de Escritorio remoto.</p> <p>Si habilita esta opción de directiva, el modo de licencia que especifique tiene preferencia sobre el modo de licencia que se especifique durante la instalación del host de sesión de Escritorio remoto o en la herramienta de configuración del host de sesión de Escritorio remoto.</p> <p>Si deshabilita o no configura esta opción de directiva, se utiliza el modo de licencia especificado durante la instalación del servicio de la función de host de sesión de Escritorio remoto o especificado en</p>

Configuración del redireccionamiento de la impresora RDS

La configuración de directiva de grupo del redireccionamiento de la impresora RDS permite a los usuarios configurar directivas para redireccionar la impresora.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Redirección de impresora**.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Redirección de impresora**.

Tabla 5-18. Configuración de directiva de grupo del redireccionamiento de la impresora RDS

Ajuste	Descripción
Do not set default client printer to be default printer in a session	<p>Utilice esta configuración de directiva para especificar si la impresora cliente predeterminada está configurada como impresora predeterminada de una sesión en un host RDS.</p> <p>De forma predeterminada, los Servicios de Escritorio remoto designan automáticamente la impresora cliente predeterminada como la impresora predeterminada de una sesión de un host RDS. Puede utilizar esta configuración de directiva para anular este comportamiento.</p> <p>Si habilita esta configuración de directiva, la impresora predeterminada es la especificada en el equipo remoto.</p> <p>Si deshabilita esta configuración de directiva, el host RDS asigna automáticamente la impresora cliente predeterminada y la establece como la impresora predeterminada de la conexión.</p> <p>Si no configura esta configuración de directiva, la impresora predeterminada no se especifica en el nivel Directiva de grupo. Sin embargo, un administrador puede configurar la impresora predeterminada para las sesiones de cliente usando la herramienta de configuración de host de sesión de Escritorio remoto.</p>
Do not allow client printer redirection	<p>Utilice esta configuración de directiva para especificar si desea evitar que se asignen impresoras cliente en las sesiones de Servicios de Escritorio remoto.</p> <p>Puede usar esta configuración de directiva para evitar que los usuarios redireccionen trabajos de impresión del equipo remoto a una impresora conectada al equipo local (cliente). De forma predeterminada, los Servicios de Escritorio remoto permiten esta asignación de impresora cliente.</p> <p>Si habilita esta configuración de directiva, los usuarios no pueden redireccionar los trabajos de impresión del equipo remoto a una impresora cliente local en las sesiones de Servicios de Escritorio remoto.</p> <p>Si deshabilita esta configuración de directiva, los usuarios pueden redireccionar trabajos de impresión con la asignación de impresora cliente.</p> <p>Si no configura esta configuración de directiva, la asignación de impresora cliente no se especifica en el nivel Directiva de grupo. Sin embargo, un administrador puede deshabilitar la asignación de impresora cliente usando la herramienta de configuración de host de sesión de Escritorio remoto.</p>

Ajuste	Descripción
Use Remote Desktop Easy Print printer driver first	<p data-bbox="810 226 1420 315">Utilice esta configuración de directiva para especificar si se utiliza en primer lugar el controlador de impresora Easy Print de Escritorio remoto para instalar todas las impresoras cliente.</p> <p data-bbox="810 327 1420 604">Si habilita o no establece esta configuración de directiva, el host RDS intenta en primer lugar usar el controlador de impresora Easy Print de Escritorio remoto para instalar todas las impresoras cliente. Si por algún motivo no se puede utilizar el controlador de impresora Easy Print de Escritorio remoto, se usará un controlador de impresora en el host RDS que coincida con la impresora cliente. Si el host RDS no tiene un controlador de impresora que coincida con la impresora cliente, esta no estará disponible en la sesión de Escritorio remoto.</p> <p data-bbox="810 617 1420 894">Si deshabilita esta configuración de directiva, el host RDS busca un controlador de impresora adecuado para instalar la impresora cliente. Si el host RDS no cuenta con un controlador de impresora que coincida con la impresora cliente, este host intenta usar el controlador de impresora Easy Print de Escritorio remoto para instalar dicha impresora. Si, por algún motivo, el controlador de impresora Easy Print de Escritorio remoto no se puede utilizar, la impresora cliente no está disponible para la sesión de Servicios de Escritorio remoto.</p> <p data-bbox="810 919 1420 1041">Nota Si la configuración de directiva "No permitir la redirección de impresoras de cliente" está habilitada, se ignora la configuración de directiva "Usar primero el controlador de impresora Easy Print de Escritorio remoto".</p>

Ajuste	Descripción
Specify RD Session Host Server fallback printer driver behavior	<p>Utilice esta configuración de directiva para especificar el comportamiento del controlador de la impresora de reserva del host RDS.</p> <p>De forma predeterminada, el controlador de la impresora de reserva del host RDS está deshabilitado. Si el host RDS no tiene un controlador de impresora que coincida con la impresora cliente, ninguna impresora estará disponible para la sesión de Servicios de Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, el controlador de la impresora de reserva está habilitado y el comportamiento predeterminado consiste en que el host RDS busque un controlador de impresora adecuado. Si no lo encuentra, la impresora cliente no estará disponible. Puede cambiar este comportamiento predeterminado. Las opciones disponibles son:</p> <ul style="list-style-type: none"> ■ Do nothing if one is not found. Si no coincide el controlador de impresora, el host RDS buscará un controlador adecuado. Si no se encuentra ninguno, la impresora cliente no estará disponible. Este es el comportamiento predeterminado. ■ Default to PCL if one is not found. Si no se encuentra ningún controlador de impresora adecuado, se utilizará de forma predeterminada el controlador de impresora de reserva Lenguaje de control de impresora (PCL). ■ Default to PS if one is not found. Si no se encuentra ningún controlador de impresora adecuado, se utilizará de forma predeterminada el controlador de impresora de reserva PostScript (PS). ■ Show both PCL and PS if one is not found. Si no se encuentra ningún controlador adecuado, aparecen los controladores de impresora de reserva basados en PCL y PS. <p>Si deshabilita esta configuración de directiva, el controlador de reserva del host RDS está deshabilitado y este host no usará el controlador de impresora de reserva.</p> <p>Si no establece esta configuración de directiva, el controlador de impresora de reserva estará desconectado de forma predeterminada.</p> <p>Nota Si la opción "No permitir la redirección de impresoras de cliente" está habilitada, esta configuración de directiva se ignorará y se deshabilitará el controlador de impresora de reserva.</p>
Redirect only the default client printer	<p>Utilice esta configuración de directiva para especificar si la impresora cliente predeterminada es la única impresora redireccionada de las sesiones de Servicios de Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, solo se redireccionará la impresora cliente predeterminada de las sesiones de Servicios de Escritorio remoto.</p> <p>Si deshabilita o no establece esta configuración de directiva, todas las impresoras cliente se redireccionarán en las sesiones de Servicios de Escritorio remoto.</p>

Configuración de perfiles RDS

La configuración de la directiva de grupo de perfiles RDS controla la configuración del perfil móvil y del directorio principal para sesiones de Servicios de Escritorio remoto.

Tabla 5-19. Configuración de la directiva de grupo de perfiles RDS

Ajuste	Descripción
Limit the size of the entire roaming user profile cache	<p>Esta opción de directiva le permite limitar el tamaño de toda la caché del perfil de usuario móvil en la unidad local. Esta opción de directiva solo se aplica a los equipos en los que esté instalado el servicio de la función de host de sesión de Escritorio remoto.</p> <p>Nota Si quiere limitar el tamaño de un perfil de usuario individual, use la opción de directiva <code>Limit profile size</code> que se encuentra en Configuración de usuario\Directivas\Plantillas administrativas\Sistema\Perfiles de usuario.</p> <p>Si habilita esta opción de directiva, deberá especificar un intervalo de supervisión (en minutos) y un tamaño máximo (en gigabytes) de toda la caché del perfil de usuario móvil. El intervalo de supervisión determina la frecuencia con la que se comprueba el tamaño de toda la caché del perfil de usuario móvil. Cuando el tamaño de toda la caché del perfil de usuario móvil supere el tamaño máximo que especificó, se eliminarán los perfiles de usuarios móviles más antiguos (menos usados recientemente) hasta que el tamaño de toda la caché del perfil de usuario móvil sea inferior al tamaño máximo especificado.</p> <p>Si deshabilita o no configura esta opción de directiva, no se establecerá ninguna restricción sobre el tamaño de toda la caché del perfil de usuario móvil en la unidad local.</p> <p>Nota: esta opción de directiva se ignorará si la opción de directiva <code>Prevent Roaming Profile changes from propagating to the server</code>, que se encuentra en Configuración de usuario\Directivas\Plantillas administrativas\Sistema\Perfiles de usuario, está habilitada.</p>
Set Remote Desktop Services User Home Directory	<p>Especifica si Servicios de Escritorio remoto usa el recurso compartido de red especificado o una ruta de directorio local como la raíz del directorio principal del usuario en una sesión de Servicios de Escritorio remoto.</p> <p>Para usar esta opción, seleccione la ubicación del directorio principal (local o de red) en la lista desplegable Ubicación. Si elige colocar el directorio en un recurso compartido de red, introduzca la ruta de acceso raíz del directorio principal de la siguiente forma: <code>\Nombredelequipo\Nombredele recursocompartido</code> y, después, seleccione la letra de unidad a la cual quiera asignar el recurso compartido de red.</p> <p>Si elige mantener el directorio principal en el equipo local, introduzca la ruta de acceso raíz del directorio principal de la siguiente forma: <code>Unidad:\Ruta</code>, sin variables de entorno ni puntos suspensivos. No debe especificar un marcador de posición para el alias de usuario, ya que Servicios de Escritorio remoto lo agrega automáticamente al iniciar sesión.</p> <p>Nota El campo Letra de unidad se ignorará si especifica una ruta de acceso local. Si especifica una ruta de acceso local pero, a continuación, introduce el nombre de un recurso compartido de red en la ruta de acceso raíz del directorio local, Servicios de Escritorio remoto coloca los directorios principales del usuario en la ubicación de red.</p> <p>Si el estado está establecido en Habilitado, Servicios de Escritorio remoto crea el directorio principal del usuario en la ubicación especificada en la red o en el equipo local. La ruta de acceso del directorio principal para cada usuario es la ruta de acceso raíz del directorio principal y el alias del usuario.</p>

Ajuste	Descripción
Use mandatory profiles on the RD Session Host server	<p>Esta configuración de directiva le permite especificar si Servicios de Escritorio remoto usa un perfil obligatorio para todos los usuarios que se conectan de forma remota al host RDS.</p> <p>Si habilita esta opción de directiva, Servicios de Escritorio remoto usa la ruta de acceso especificada en la opción de directiva Set path for Remote Desktop Services Roaming User Profile como carpeta raíz para el perfil de usuario obligatorio. Todos los usuarios que se conectan de manera remota al host RDS usan el mismo perfil de usuario.</p> <p>Si deshabilita o no establece esta configuración de directiva, los usuarios que se conectan de manera remota al host RDS no usarán perfiles de usuario obligatorios.</p> <p>Nota Para que se aplique esta opción de directiva, también debe habilitar y configurar la opción de directiva Set path for Remote Desktop Services Roaming User Profile.</p>
Set path for Remote Desktop Services Roaming User Profile	<p>Esta opción de directiva le permite especificar la ruta de acceso de red que usa Servicios de Escritorio remoto para los perfiles de usuario móvil.</p> <p>De forma predeterminada, Servicios de Escritorio remoto almacena todos los perfiles de usuario de forma local en el host RDS. Puede usar esta configuración de directiva para especificar un recurso compartido de red donde puedan almacenarse los perfiles de usuario de forma centralizada, lo que permite que los usuarios accedan a los mismos perfiles en cada sesión en todos los host RDS que estén configurados para usar el recurso compartido de red para perfiles de usuario.</p> <p>Si habilita esta opción de directiva, Servicios de Escritorio remoto usará la ruta de acceso especificada como directorio raíz para todos los perfiles de usuario. Los perfiles se incluyen en subcarpetas cuyo nombre es el mismo de la cuenta de cada usuario.</p> <p>Para configurar esta opción de directiva, introduzca la ruta de acceso al recurso compartido de red de la siguiente forma: \Nombredelequipo\Nombredelrecursocompartido. No especifique un marcador de posición para el nombre de la cuenta de usuario, ya que Servicios de Escritorio remoto lo agrega automáticamente cuando el usuario inicia sesión y se crea el perfil. Si el recurso compartido de red especificado no existe, la función Servicios de Escritorio remoto mostrará un mensaje de error en el host RDS y almacenará los perfiles de usuario de forma local en el host RDS.</p> <p>Si deshabilita o no establece esta configuración de directiva, los perfiles de usuario se almacenarán de forma local en el host RDS. Puede configurar una ruta de acceso de un perfil de usuario en la pestaña Perfil de Servicios de Escritorio remoto del cuadro de diálogo Propiedades de la cuenta de usuario.</p> <p>Notas:</p> <ol style="list-style-type: none"> Los perfiles de usuarios móviles habilitados por la opción de directiva solo se aplican a las conexiones de Servicios de Escritorio remoto. También es posible que un usuario tenga un perfil de usuario móvil configurado. El perfil de usuario móvil de Servicios de Escritorio remoto siempre tiene prioridad en una sesión de Servicios de Escritorio remoto. Para configurar un perfil de usuario móvil de Servicios de Escritorio remoto obligatorio para todos los usuarios que se conecten de forma remota al host RDS, use esta configuración

Configuración del servidor de conexión RDS

La configuración de directiva de grupo del servidor de conexión RDS permite a los usuarios configurar directivas para el servidor de conexión.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Agente de conexión**.

Tabla 5-20. Configuración de directiva de grupo del servidor de conexión RDS

Ajuste	Descripción
Join RD Connection Broker	<p>Utilice esta configuración de directiva para especificar si el host RDS debe unirse a una granja en el servidor de conexión que está instalado en un host RDS. El servidor de conexión de un host RDS realiza un seguimiento de las sesiones de usuario y permite que un usuario vuelva a conectar su sesión existente en una granja RDS de carga equilibrada. Para participar en el servidor de conexión de un host RDS, debe instalarse el servicio de la función de host de sesión de Escritorio remoto en el host RDS.</p> <p>Si está habilitada la configuración de directiva, el host RDS se une a la granja que se especifica en la opción "Configurar nombre de la granja del Agente de conexión a Escritorio remoto". La granja se encuentra en el servidor de conexión que se especifica en la configuración de la directiva "Configurar nombre del servidor del Agente de conexión a Escritorio remoto".</p> <p>Si deshabilita esta configuración de directiva, el host RDS no se une a una granja en el servidor de conexión y no se realiza el seguimiento de la sesión de usuario. Si la configuración está deshabilitada, no puede utilizar la herramienta de configuración de host de sesión de Escritorio remoto ni el proveedor WMI de Terminal Services para unir el host RDS al servidor de conexión.</p> <p>Si no se establece la configuración de directiva, la opción no se especifica en el nivel de la directiva de grupo. En este caso, puede configurar el host RDS para que se una al servidor de conexión en el host RDS mediante la herramienta de configuración de host de sesión de Escritorio remoto o el proveedor WMI de Terminal Services.</p> <p>Nota</p> <ol style="list-style-type: none"> Si habilita esta configuración, también debe habilitar las opciones de configuración de directiva "Configurar nombre de la granja del Agente de conexión a Escritorio remoto" y "Configurar nombre del servidor del Agente de conexión a Escritorio remoto" o configurar estas opciones mediante la herramienta de configuración de host de sesión de Escritorio remoto o el proveedor WMI de Terminal Services. Para Windows Server 2008, esta configuración de directiva es compatible con al menos Windows Server 2008 Standard.
Configure RD Connection Broker farm name	<p>Utilice esta configuración de directiva para especificar el nombre de una granja para que se una al servidor de conexión de un host RDS. El servidor de conexión utiliza el nombre de granja para determinar qué hosts RDS están en la misma granja RDS. Por lo tanto, debe utilizar el mismo nombre de granja para todos los hosts RDS en la misma granja de carga equilibrada. El nombre de granja no tiene que corresponder a un nombre de los Servicios de dominio de Active Directory.</p> <p>Si especifica un nombre de granja nuevo, se crea una nueva granja en el servidor de conexión para el host RDS. Si especifica un nombre de granja existente, el host RDS se une a esa granja en el servidor de conexión del host RDS.</p> <p>Si habilita esta configuración de directiva, debe especificar el nombre de una granja en el servidor de conexión para el host RDS.</p> <p>Si deshabilita o no establece esta configuración de directiva, la</p>

Ajuste	Descripción
Use IP Address Redirection	<p>Utilice esta configuración de directiva para especificar el método de redireccionamiento que se usará cuando un dispositivo cliente se vuelva a conectar a una sesión de Servicios de Escritorio remoto existente en una granja de servidores de host de sesión de Escritorio remoto de carga equilibrada. Esta opción se aplica a un host RDS que esté configurado para usar el servidor de conexión en un host RDS y no para el servidor de conexión de un escritorio remoto.</p> <p>Si habilita a esta configuración de directiva, un cliente de Servicios de Escritorio remoto consulta al servidor de conexión en el host RDS y es redireccionado a una sesión existente a través de la dirección IP del host RDS en el que se ubica la sesión. Para utilizar este método de redireccionamiento, los equipos cliente deben poder conectarse directamente a través de la dirección IP para el host RDS en la granja.</p> <p>Si deshabilita esta configuración de directiva, la dirección IP del host RDS no se envía al cliente. En su lugar, la dirección IP está integrada a un token. Cuando un cliente vuelve a conectarse al equilibrador de carga, se usa el token de enrutamiento para redireccionar al cliente a la sesión existente en el host RDS correcto de la granja. Deshabilite a esta opción solo cuando la solución de carga equilibrada de red sea compatible con el uso de los tokens de enrutamiento del servidor de conexión del host RDS y no desee que los clientes se conecten directamente a través de la dirección IP al host RDS en la granja de carga equilibrada.</p> <p>Si no establece esta configuración de directiva, se usa la opción "Usar redirección de direcciones IP" en la herramienta de configuración de host de sesión de Escritorio remoto. De manera predeterminada, esta opción de la herramienta de configuración de host de sesión de Escritorio remoto está habilitada.</p> <p>Nota Para Windows Server 2008, esta configuración de directiva es compatible con al menos Windows Server 2008 Standard.</p>

Ajuste	Descripción
Configure RD Connection Broker Server name	<p>Utilice esta configuración de directiva para especificar el servidor de conexión que el host RDS usa para realizar un seguimiento y redireccionar las sesiones de usuario de una granja RDS de carga equilibrada. El host RDS especificado debe estar ejecutando el servicio del servidor de conexión. Todos los hosts RDS en una granja de carga equilibrada deben utilizar el mismo servidor de conexión.</p> <p>Si habilita esta configuración de directiva, debe especificar el servidor de conexión para el host RDS mediante su nombre de host, dirección IP o nombre de dominio completo. Si especifica un nombre o dirección IP para el servidor de conexión que no sean válidos, se registrará un mensaje de error en el Visor de eventos del host RDS.</p> <p>Si deshabilita o no establece esta configuración de directiva, puede ajustar el nombre del servidor de conexión del host RDS o la dirección IP con la herramienta de configuración de host de sesión de Escritorio remoto o el proveedor WMI de Terminal Services.</p> <hr/> <p>Nota</p> <ul style="list-style-type: none"> ■ Para Windows Server 2008, esta configuración de directiva es compatible con Windows Server 2008 Standard. ■ Esta configuración de directiva no se hace efectiva a menos que se habilite la configuración de directiva "Unirse al Agente de conexión a Escritorio remoto" o se configure el host RDS para que se una al servidor de conexión del host RDS mediante la herramienta de configuración de host de sesión de Escritorio remoto o el proveedor WMI de Terminal Services. ■ Para ser miembro activo de una sesión habilitada de un servidor de conexión de una granja RDS, la cuenta del equipo para cada host RDS de la granja debe ser miembro del grupo local "Equipos de directorio de sesión" en el servidor de conexión para el host RDS.
Use RD Connection Broker load balancing	<p>Utilice esta configuración de directiva para especificar si se debe utilizar la función de equilibrador de carga en un servidor de conexión de un host RDS para equilibrar la carga entre los servidores de una granja RDS.</p> <p>Si habilita a esta configuración de directiva, el servidor de conexión de un host RDS redirecciona a los usuarios que no tienen una sesión existente al host RDS de la granja con el menor número de sesiones. El comportamiento del redireccionamiento para los usuarios con sesiones existentes no se verá afectado. Si el servidor está configurado para usar el servidor de conexión en un host RDS, los usuarios que tengan una sesión existente se redireccionan al host RDS en el que se ubica la sesión.</p> <p>Si deshabilita esta configuración de directiva, los usuarios que no tengan una sesión existente deberán iniciar sesión en el primer host RDS al que se conecten.</p> <p>Si no establece esta configuración de directiva, puede configurar el host RDS para que participe en el equilibrado de carga del servidor de conexión para el host RDS mediante la herramienta de configuración de host de sesión de Escritorio remoto o con el proveedor WMI de Terminal Services.</p>

Configuración del entorno de sesión remota de RDS

La directiva de grupo de entorno de sesión remota de RDS controla la configuración de la interfaz de usuario en las sesiones de Servicios de Escritorio remoto.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de escritorio remoto > Entorno de sesión remota**.

La configuración de directiva de grupo de RDS de Horizon 7 también se instala en la carpeta **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de escritorio remoto > Entorno de sesión remota**.

Tabla 5-21. Configuración de la directiva de grupo de entorno de sesión remota de RDS

Ajuste	Descripción
Limit maximum color depth	<p>Utilice esta configuración de directiva para especificar la resolución de color máxima (profundidad de color) para las conexiones de Servicios de Escritorio remoto.</p> <p>Puede usar esta configuración de directiva para establecer un límite de profundidad de color de cualquier conexión mediante RDP. La limitación de profundidad de color puede mejorar el rendimiento de la conexión, especialmente en vínculos de baja velocidad, y reducir la carga del servidor.</p> <p>Si habilita esta configuración de directiva, la profundidad de color especificada es la profundidad de color máxima para una conexión de usuario sobre RDP. La profundidad de color real para la conexión viene determinada por la compatibilidad de color disponible en el equipo cliente. Si selecciona "Compatible con el cliente", se usará la profundidad de color máxima compatible con el cliente.</p> <hr/> <p>Nota Una profundidad de color de 24 bits solo es compatible con Windows XP Professional y Windows Server 2003.</p> <hr/> <p>Si deshabilita o no establece esta configuración de directiva, la profundidad de color para las conexiones queda determinada por la opción "Limitar máxima profundidad de color" en la pestaña Configuración de cliente de la herramienta de configuración de host de sesión de Escritorio remoto, a menos que el usuario especifique un nivel inferior en el momento de la conexión.</p>
Enforce Removal of Remote Desktop Wallpaper	<p>Especifica si el papel tapiz del escritorio se muestra a clientes remotos que se conecten a través de Servicios de Escritorio remoto.</p> <p>Puede usar esta opción para exigir la eliminación de papel tapiz durante una sesión de Servicios de Escritorio remoto. De manera predeterminada, Windows XP Professional muestra el papel tapiz a los clientes remotos que se conectan a través de Escritorio remoto, dependiendo de la configuración del cliente. Consulte la pestaña Rendimiento en las opciones Conexión a Escritorio remoto para obtener más información. Los servidores que ejecutan Windows Server 2003 no muestran el papel tapiz de manera predeterminada en sesiones de Servicios de Escritorio remoto.</p> <p>Si habilita esta configuración, el papel tapiz nunca aparece en la sesión de Servicios de Escritorio remoto.</p> <p>Si deshabilita esta configuración, puede que aparezca el papel tapiz en la sesión de Servicios de Escritorio remoto, dependiendo de la configuración del cliente.</p> <p>Si no establece esta configuración, se aplica el comportamiento predeterminado.</p>

Ajuste	Descripción
Configure RemoteFX	<p>Utilice esta configuración de directiva para controlar la disponibilidad de RemoteFX en un servidor de host de Virtualización de Escritorio remoto (host de Virtualización de RD) y en un host RDS.</p> <p>Cuando RemoteFX se implementa en un servidor de host de Virtualización de Escritorio remoto, proporciona una experiencia de usuario rica mediante la representación del contenido del servidor por medio de unidades de procesamiento de gráficos (GPU) o hardware. De forma predeterminada, RemoteFX para host de virtualización de Escritorio remoto usa hardware o las GPU del servidor para proporcionar una experiencia de usuario enriquecida a través de conexiones LAN y RDP 7.1.</p> <p>Cuando RemoteFX se implementa en un host RDS, proporciona una experiencia de usuario rica mediante el uso de un esquema de compresión acelerado por hardware.</p> <p>Si habilita esta configuración de directiva, RemoteFX se usará para proporcionar una experiencia de usuario enriquecida a través de conexiones LAN y RDP 7.1.</p> <p>Si deshabilita esta configuración de directiva, RemoteFX se deshabilitará.</p> <p>Si no establece esta configuración de directiva, se usará el comportamiento predeterminado. De forma predeterminada, RemoteFX está habilitado para el host de virtualización de Escritorio remoto y deshabilitado para el host RDS.</p>
Limit maximum display resolution	<p>Utilice esta configuración de directiva para especificar la resolución máxima de pantalla que puede usar cada monitor que muestra una sesión de Servicios de Escritorio remoto. La limitación de la resolución usada para mostrar una sesión remota puede mejorar el rendimiento de la conexión, en particular con vínculos lentos, y reducir la carga del servidor.</p> <p>Si habilita esta configuración de directiva, deberá especificar un ancho y un alto de resolución. La resolución especificada será la máxima que podrá usar cada monitor que muestre una sesión de Servicios de Escritorio remoto.</p> <p>Si deshabilita o no define esta configuración de directiva, la resolución máxima de pantalla que puede usar cada monitor que muestra una sesión de Servicios de Escritorio remoto la determinan los valores especificados en la pestaña Configuración de pantalla de la herramienta de configuración de host de sesión de Escritorio remoto.</p>

Ajuste	Descripción
Limit maximum number of monitors	<p>Utilice esta configuración de directiva para limitar el número máximo de monitores que un usuario puede usar para mostrar una sesión de Servicios de Escritorio remoto. La limitación del número de monitores para mostrar una sesión de Servicios de Escritorio remoto puede mejorar el rendimiento de la conexión, en particular con vínculos lentos, y reducir la carga del servidor.</p> <p>Si habilita esta configuración de directiva, podrá especificar el número de monitores que se pueden usar para mostrar una sesión de Servicios de Escritorio remoto. Puede especificar un número de 1 a 10.</p> <p>Si deshabilita o no define esta configuración de directiva, el número de monitores que se pueden usar para mostrar una sesión de Servicios de Escritorio remoto lo determinará el valor especificado en el cuadro "Número máximo de monitores por sesión" en la pestaña Configuración de pantalla de la herramienta de configuración de host de sesión de Escritorio remoto.</p>
Remove "Disconnect" option from Shut Down dialog	<p>Utilice esta configuración de directiva para quitar la opción "Desconectar" del cuadro de diálogo Cerrar Windows en las sesiones de Servicios de Escritorio remoto.</p> <p>Puede usar esta configuración de directiva para impedir que los usuarios usen este método habitual para desconectar clientes de un host RDS.</p> <p>Si habilita esta configuración de directiva, "Desconectar" no aparecerá como una opción en la lista desplegable del cuadro de diálogo Cerrar Windows.</p> <p>Si deshabilita o no establece esta configuración de directiva, "Desconectar" seguirá apareciendo en la lista del cuadro de diálogo Cerrar Windows.</p> <p>Nota Esta configuración de directiva afecta solo al cuadro de diálogo Cerrar Windows. No impide que los usuarios usen otros métodos para desconectarse de una sesión de Servicios de Escritorio remoto. Además, esta configuración de directiva no impide las sesiones desconectadas en el servidor. Puede controlar el tiempo durante el cual una sesión desconectada continúa activa en el servidor si configura la configuración de directiva "Establecer el límite de tiempo para las sesiones desconectadas" en la carpeta Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Límites de tiempo de sesión.</p>

Ajuste	Descripción
Optimize visual experience when using RemoteFX	<p>Utilice esta configuración de directiva para especificar la experiencia visual que tendrán los usuarios remotos en conexiones de Conexión a Escritorio remoto (RDC) que usan RemoteFX. Puede usar esta directiva para equilibrar el uso del ancho de banda de red con el tipo de experiencia gráfica que se proporciona.</p> <p>En función de los requerimientos de los usuarios, puede reducir el uso del ancho de banda de red reduciendo de la velocidad de captura de pantalla. También puede reducir el uso del ancho de banda de red reduciendo la calidad de imagen (se aumenta el nivel de compresión de la imagen).</p> <p>Si cuenta con una red con ancho de banda superior al promedio, puede maximizar la utilización de ancho de banda seleccionando el valor más alto de la velocidad de captura de pantalla y el valor más alto de la calidad de imagen.</p> <p>De forma predeterminada, las sesiones de Conexión a Escritorio remoto que usan RemoteFX se optimizan para lograr una experiencia equilibrada en todas las condiciones de la LAN. Si deshabilita o no establece esta configuración de directiva, las sesiones de Conexión a Escritorio remoto que usan RemoteFX se desarrollarán como si estuviera seleccionados los valores de velocidad de captura de pantalla media y compresión de imagen media (comportamiento predeterminado).</p>
Set compression algorithm for RDP data	<p>Utilice esta configuración de directiva para especificar el algoritmo de compresión de Protocolo de escritorio remoto (RDP) que se usará.</p> <p>De manera predeterminada, los servidores usan un algoritmo de compresión RDP que se basa en la configuración de hardware del servidor.</p> <p>Si habilita esta configuración de directiva, puede especificar el algoritmo de compresión RDP que se usará. Si selecciona el algoritmo optimizado para usar menos memoria, esta opción usa menos memoria pero usa más ancho de banda de red. Si selecciona el algoritmo optimizado para usar menos ancho de banda de red, esta opción usa menos ancho de banda de red pero usa más memoria. Asimismo, está disponible una tercera opción que equilibra el uso de memoria y de ancho de banda de red.</p> <p>También puede elegir no usar un algoritmo de compresión de RDP. Si elige no usar un algoritmo de compresión de RDP, se usará más ancho de banda de red, lo que solo se recomienda si se usa un dispositivo de hardware diseñado para optimizar el tráfico de red. Aunque elija no usar un algoritmo de compresión de RDP, algunos datos gráficos de comprimirán.</p> <p>Si deshabilita o no establece esta configuración de directiva, se usará el algoritmo de compresión RDP predeterminado.</p>

Ajuste	Descripción
Optimize visual experience for Remote Desktop Services sessions	<p>Utilice esta configuración de directiva para especificar la experiencia visual que reciben los usuarios remotos en sesiones de Servicios de Escritorio remoto. Las sesiones remotas del equipo se optimizan para admitir esta experiencia visual.</p> <p>De forma predeterminada, las sesiones de Servicios de Escritorio remoto se optimizan para multimedia enriquecida, como las aplicaciones que usan Silverlight o Windows Presentation Foundation.</p> <p>Si habilita esta configuración de directiva, deberá seleccionar la experiencia visual para la cual desea optimizar las sesiones de Servicios de Escritorio remoto. Puede seleccionar Multimedia enriquecida o Texto.</p> <p>Si deshabilita o no define esta configuración de directiva, las sesiones de Servicios de Escritorio remoto se optimizan para multimedia enriquecida.</p>

Ajuste	Descripción
Start a program on connection	<p>Configura Servicios de Escritorio remoto para que ejecute automáticamente un programa especificado al conectarse.</p> <p>Puede usar esta configuración para especificar que determinado programa se ejecute automáticamente cuando un usuario inicie sesión en un equipo remoto.</p> <p>De forma predeterminada, las sesiones de Servicios de Escritorio remoto proporcionan acceso al escritorio completo de Windows, a menos que el administrador del servidor o el usuario hayan especificado algo distinto con este ajuste al configurar la conexión de cliente. Habilitar esta opción invalida la opción "Iniciar programa" establecida por el administrador del servidor o el usuario. El menú Inicio y el escritorio de Windows no se muestran y, cuando el usuario sale del programa, la sesión se cierra automáticamente.</p> <p>Para usar esta opción, en Nombre de archivo y ruta de acceso del programa, escriba el nombre de archivo completo y la ruta de acceso del archivo ejecutable que se va a ejecutar cuando el usuario inicie sesión. Si es necesario, en Directorio de trabajo, escriba la ruta de acceso completa del directorio de inicio del programa. Si deja Directorio de trabajo en blanco, el programa se ejecutará con su directorio de trabajo predeterminado. Si la ruta de acceso, nombre de archivo o directorio de trabajo del programa especificado no es un nombre de un directorio válido, se produce un error en la conexión del servidor host de sesión de Escritorio remoto y aparece un mensaje de error.</p> <p>Si el estado se establece en Habilitado, las sesiones de Servicios de Escritorio remoto ejecutan automáticamente el programa especificado y usan el directorio de trabajo especificado (o el directorio predeterminado del programa, si no se ha especificado el directorio de trabajo) como directorio de trabajo del programa.</p> <p>Si el estado se establece en Deshabilitado o No configurado, las sesiones de Servicios de Escritorio remoto se inician con el escritorio completo, a menos que el administrador del servidor o el usuario especifiquen lo contrario. Para obtener más información, consulte la configuración de directiva "Ejecutar estos programas cuando el usuario inicie la sesión" en la carpeta Configuración del equipo > Plantillas administrativas > Sistema > Iniciar sesión.</p> <p>Nota Esta opción aparece tanto en Configuración del equipo como en Configuración de usuario. Si se establecen ambas configuraciones, la opción Configuración del equipo sobrescribe la opción Configuración de usuario.</p>

Ajuste	Descripción
Always show desktop on connection	<p>Esta configuración de directiva determina si el escritorio se muestra siempre después de que un cliente se conecta a un equipo remoto o si un programa inicial se puede ejecutar. Utilice esta configuración para requerir que el escritorio se muestre después de que un cliente se conecte a un equipo remoto, incluso si ya se ha especificado un programa inicial en el perfil de usuario predeterminado, en Conexión a escritorio remoto, en el cliente de Servicios de Escritorio remoto o a través de directivas de grupo.</p> <p>Si habilita esta configuración de directiva, el escritorio se mostrará siempre cuando el cliente se conecte a un equipo remoto. Esta configuración de directiva invalida cualquier configuración de directiva de programa inicial.</p> <p>Si deshabilita o no configura este ajuste de directiva, se podrá especificar un programa inicial para ejecutarse en el equipo remoto después de que el cliente se conecte al equipo remoto. Si no se especifica un programa inicial, el escritorio siempre se muestra en el equipo remoto después de que el cliente se conecte a éste.</p> <p>Nota Si esta configuración de directiva está habilitada, se pasará por alto la configuración de directiva "Iniciar un programa al conectarse".</p>

Ajuste	Descripción
Allow desktop composition for remote desktop sessions	<p>Utilice esta configuración de directiva para especificar si la composición del escritorio está permitida para sesiones de escritorio remoto. Esta configuración de directiva no se aplica a sesiones de RemoteApp.</p> <p>La composición del escritorio proporciona los elementos de interfaz de usuario de Windows Aero, como las ventanas translúcidas, para sesiones de escritorio remoto. Puesto que Windows Aero requiere recursos de sistema y de ancho de banda adicionales, si se permite la composición del escritorio para sesiones de escritorio remoto se reducirá el rendimiento de la conexión, particularmente en vínculos de baja velocidad y aumentará la carga del equipo remoto.</p> <p>Si habilita esta configuración de directiva, la composición del escritorio se permitirá para sesiones de escritorio remoto. En el equipo cliente puede configurar la composición del escritorio en la pestaña Rendimiento en la Conexión a Escritorio remoto (RDC) o mediante la configuración "permitir la composición de escritorio" en un archivo de Protocolo de escritorio remoto (.rdp). De manera adicional, el equipo cliente debe disponer del hardware necesario para admitir las funciones de Windows Aero.</p> <hr/> <p>Nota Es posible que sea necesaria una configuración adicional en el equipo remoto para que las funciones de Windows Aero estén disponibles para las sesiones de escritorio remoto. Por ejemplo, la función Experiencia de uso debe estar instalada en el equipo remoto y la profundidad máxima de color en el equipo remoto debe establecerse en 32 bits por píxel. Además, el servicio Temas debe iniciarse en el equipo remoto.</p> <hr/> <p>Si deshabilita o no configura esta configuración de directiva, la composición del escritorio no estará permitida para sesiones de escritorio remoto, incluso si dicha composición está habilitada en la RDC o en el archivo .rdp.</p>

Ajuste	Descripción
Do not allow font smoothing	<p>Utilice esta configuración de directiva para especificar si el suavizado de fuentes está permitido para conexiones remotas.</p> <p>El suavizado de fuentes proporciona funcionalidad ClearType para una conexión remota. ClearType es una tecnología para mostrar fuentes en el equipo de una manera clara y suave, especialmente si está utilizando un monitor LCD. Puesto que el suavizado de fuentes requiere recursos de ancho de banda adicionales, si no se permite el suavizado de fuentes para conexiones remotas se mejorará el rendimiento de la conexión, particularmente en vínculos de baja velocidad.</p> <p>De manera predeterminada, el suavizado de fuentes está permitido para conexiones remotas. Puede configurar el suavizado de fuentes en la pestaña Rendimiento en la Conexión a Escritorio remoto (RDC) o mediante la configuración "permitir el suavizado de fuentes" en un archivo de Protocolo de escritorio remoto (.rdp).</p> <p>Si habilita esta configuración de directiva, el suavizado de fuentes no se permitirá para conexiones remotas, incluso si el suavizado de fuentes está habilitado en la RDC o en el archivo .rdp.</p> <p>Si deshabilita o no establece esta configuración de directiva, el suavizado de fuentes estará permitido en conexiones remotas.</p>
Remove Windows Security item from Start menu	<p>Especifica si se quita el elemento Seguridad de Windows del menú Configuración de los clientes de Escritorio remoto. Puede usar esta opción para impedir que usuarios inexpertos cierren una sesión de Servicios de Escritorio remoto inadvertidamente.</p> <p>Si el estado se establece en Habilitado, Seguridad de Windows no aparecerá en la Configuración del menú Inicio. Como resultado, los usuarios deben escribir una secuencia de aviso de seguridad, por ejemplo Ctrl+Alt+Fin, para abrir el cuadro de diálogo Seguridad de Windows en el equipo cliente.</p> <p>Si el estado se establece en Deshabilitado o No configurado, Seguridad de Windows permanecerá en el menú Configuración.</p>

Configuración de seguridad de RDS

La opción de directiva de grupo de seguridad de RDS controla si permitir que los administradores locales personalicen los permisos.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de escritorio remoto > Host de sesión de escritorio remoto > Seguridad**.

Tabla 5-22. Configuración de la directiva de grupo de seguridad de RDS

Ajuste	Descripción
Server Authentication Certificate Template	<p>Utilice esta configuración de directiva para especificar el nombre de la plantilla de certificado que determina qué certificado se selecciona de forma automática para autenticar un host RDS.</p> <p>Se necesita un certificado para autenticar un host RDS cuando se usa SSL (TLS 1.0) para dar seguridad a la comunicación entre un cliente y un host RDS durante las conexiones RDP.</p> <p>Si se habilita esta configuración de directiva, se debe especificar un nombre de plantilla de certificado. Cuando se selecciona automáticamente un certificado para autenticar un host RDS, solo se considerarán los certificados creados mediante la plantilla de certificado especificada. Solo se selecciona el certificado automáticamente si no se ha seleccionado un certificado específico.</p> <p>Si no se encuentra ningún certificado que haya sido creado con la plantilla de certificado especificada, el host RDS emitirá una solicitud de inscripción de certificado y usará el certificado actual hasta que la solicitud finalice. Si se encuentra más de un certificado creado con la plantilla de certificado especificada, se seleccionará el certificado con fecha de caducidad posterior y que coincida con el nombre actual del host RDS.</p> <p>Si se deshabilita o no se configura esta configuración de directiva, se usará un certificado autofirmado de forma predeterminada para autenticar el host RDS. Se puede seleccionar un certificado específico para autenticar el host RDS en la pestaña General de la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p>Nota Si selecciona un certificado específico para autenticar el host RDS, ese certificado tendrá prioridad sobre la configuración de directiva.</p>
Set client connection encryption level	<p>Especifica si es necesario usar un nivel de cifrado específico para proteger las comunicaciones entre clientes y hosts RDS durante las conexiones de Protocolo de escritorio remoto (RDP).</p> <p>Si habilita esta configuración, todas las comunicaciones entre clientes y hosts RDS realizadas durante conexiones remotas deben usar el método de cifrado aquí especificado. De forma predeterminada, el nivel de cifrado se establece en Alto. Los métodos de cifrado disponibles son:</p> <ul style="list-style-type: none"> ■ High. La opción Alto cifra los datos enviados desde el cliente al servidor y desde el servidor al cliente usando cifrado de alta seguridad de 128 bits. Use este nivel de cifrado en entornos que contengan únicamente clientes de 128 bits (por ejemplo, clientes que ejecuten Conexión a Escritorio remoto). Los clientes que no admitan este nivel de cifrado no podrán conectarse a los servidores host RDS. ■ Client Compatible. La opción Compatible con el cliente cifra los datos enviados entre el cliente y el servidor con la seguridad de clave máxima compatible con el cliente. Use este nivel de cifrado en entornos que contengan clientes no compatibles con el cifrado de 128 bits. ■ Low. La opción Bajo cifra únicamente los datos enviados desde el cliente al servidor usando cifrado de 56 bits. <p>Si deshabilita o no configura este ajuste, el nivel de cifrado que se usará en las conexiones remotas a host RDS no se aplicará mediante la directiva de grupo. Sin embargo, puede configurar un nivel de cifrado necesario para estas conexiones mediante la</p>

Ajuste	Descripción
Always prompt for password upon connection	<p>Especifica si Servicios de Escritorio remoto pide siempre al cliente una contraseña al conectarse.</p> <p>Puede usar esta opción para exigir la petición de una contraseña a los usuarios que se conecten a Servicios de Escritorio remoto, aunque ya hayan proporcionado la contraseña en el cliente de Conexión a Escritorio remoto.</p> <p>De forma predeterminada, Servicios de Escritorio remoto permite a los usuarios iniciar sesión de forma automática si especifican una contraseña en el cliente de Conexión a Escritorio remoto.</p> <p>Si habilita esta configuración de directiva, los usuarios no podrán iniciar sesión automáticamente en Servicios de Escritorio remoto mediante la especificación de su contraseña en el cliente de Conexión a Escritorio remoto. Se les pedirá una contraseña para iniciar sesión.</p> <p>Si deshabilita o no configura este ajuste de directiva, los usuarios podrán iniciar sesión siempre automáticamente en Servicios de Escritorio remoto mediante la especificación de su contraseña en el cliente de Conexión a Escritorio remoto.</p> <p>Si no establece esta configuración de directiva, el inicio de sesión automático no se especificará en el nivel de directiva de grupo. No obstante, un administrador podrá seguir aplicando la petición de contraseña con la herramienta de configuración de host de sesión de Escritorio remoto.</p>
Require secure RPC communication	<p>Especifica si un host RDS requiere comunicaciones RPC seguras con todos los clientes o permite comunicaciones no seguras.</p> <p>Puede usar esta opción para reforzar la seguridad de la comunicación RPC con los clientes al permitir solo peticiones autenticadas y cifradas.</p> <p>Si habilita esta configuración, Servicios de Escritorio remoto acepta peticiones de clientes RPC que admiten peticiones seguras y no permite la comunicación no segura con clientes que no sean de confianza.</p> <p>Si deshabilita esta configuración, Servicios de Escritorio remoto siempre solicita seguridad para todo el tráfico RPC. Sin embargo, se permite la comunicación no segura para los clientes RPC que no responden a la petición.</p> <p>Si no establece esta configuración, se permite la comunicación no segura.</p> <p>Nota La interfaz RPC se usa para administrar y configurar Servicios de Escritorio remoto.</p>

Ajuste	Descripción
Require use of specific security layer for remote (RDP) connections	<p>Especifica si es necesario usar un nivel de seguridad específico para proteger las comunicaciones entre clientes y hosts RDS durante las conexiones de Protocolo de escritorio remoto (RDP).</p> <p>Si habilita esta configuración de directiva, todas las comunicaciones entre clientes y hosts RDS realizadas durante las conexiones remotas deberán usar el método de seguridad especificado en esta configuración. Los métodos de seguridad disponibles son los siguientes:</p> <ul style="list-style-type: none"> ■ Negotiate. El método Negotiate aplica el método más seguro compatible con el cliente. Si se admite la versión 1.0 de Seguridad de la capa de transporte (TLS), se usa para autenticar el host RDS. Si no se admite TLS, se usa el cifrado de Protocolo de escritorio remoto (RDP) nativo para proteger las comunicaciones, pero no se autentica el host RDS. ■ RDP. El método RDP usa el cifrado RDP nativo para proteger las comunicaciones entre el cliente y el host RDS. Si selecciona esta configuración, el host RDS no se autentica. ■ SSL (TLS 1.0). El método SSL requiere el uso de TLS 1.0 para autenticar el host RDS. Si no se admite TLS, se producirá un error en la conexión. <p>Si deshabilita o no establece esta configuración, el método de seguridad que se debe usar para las conexiones remotas a los hosts RDS no se aplican mediante la directiva de grupo. Sin embargo, puede configurar un método de seguridad necesario para estas conexiones mediante la herramienta de configuración de host de sesión de Escritorio remoto.</p>

Ajuste	Descripción
Require user authentication for remote connections by using Network	<p>Utilice esta configuración de directiva para especificar si es necesaria la autenticación del usuario para conexiones remotas al host RDS mediante Autenticación a nivel de red. Esta configuración de directiva mejora la seguridad al requerir que la autenticación del usuario tenga lugar en un momento más temprano del proceso de conexión remota.</p> <p>Si habilita esta configuración de directiva, solo podrán conectarse al host RDS los equipos cliente que sean compatibles con Autenticación a nivel de red.</p> <p>Para determinar si un equipo cliente es compatible con Autenticación a nivel de red, inicie Conexión a Escritorio remoto en el equipo cliente, haga clic en el icono ubicado en el rincón superior izquierdo del cuadro de diálogo Conexión a Escritorio remoto y, a continuación, haga clic en Acerca de. En el cuadro de diálogo Acerca de Conexión a Escritorio remoto, busque la frase "Compatible con Autenticación a nivel de red".</p> <p>Si deshabilita o no configura este ajuste de directiva, no se requerirá Autenticación a nivel de red para la autenticación de usuario antes de permitir conexiones remotas al host RDS.</p> <p>Puede especificar que la Autenticación a nivel de red sea necesaria para la autenticación de usuarios mediante la herramienta de configuración de host de sesión de Escritorio remoto o la pestaña Acceso remoto en Propiedades del sistema.</p> <p>Importante Si se deshabilita o no se establece esta configuración de directiva, la seguridad se verá afectada, puesto que la autenticación de usuarios tendrá lugar más adelante en el proceso de conexión remota.</p>
Do not allow local administrators to customize permissions	<p>Especifica si se deshabilitan los derechos del administrador para personalizar los permisos de seguridad en la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p>Puede usar esta opción para evitar que los administradores cambien los grupos de usuarios en la pestaña Permisos de la herramienta de configuración de host de sesión de Escritorio remoto. De forma predeterminada, los usuarios pueden realizar tales cambios.</p> <p>Si el estado se establece en Habilitado, la pestaña Permisos de la herramienta de configuración de host de sesión de Escritorio remoto no se puede usar para personalizar los descriptores de seguridad por conexión ni para cambiar los descriptores de seguridad predeterminados para un grupo existente. Todos los descriptores de seguridad son de solo lectura.</p> <p>Si el estado se establece en Deshabilitado o No configurado, los administradores del servidor disponen de plenos privilegios de lectura/escritura con respecto a los descriptores de seguridad de la pestaña Permisos de la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p>Nota El método preferido para administrar el acceso de los usuarios es agregar un usuario al grupo Usuarios de Escritorio remoto.</p>

Límites de tiempo de sesión RDS

La configuración de la directiva de grupo de los límites de tiempo de sesión RDS permite a los usuarios establecer directivas para limitar el tiempo de las sesiones en los hosts RDS.

La configuración de directiva de grupo de RDS de Horizon 7 se instala en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de escritorio remoto > Límites de tiempo de sesión**.

La configuración de la directiva de grupo de RDS de Horizon 7 se instalan también en la carpeta **Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de escritorio remoto > Límites de tiempo de sesión**.

Tabla 5-23. Configuración de directiva de grupo de los límites de tiempo de la sesión RDS

Ajuste	Descripción
Set time limit for disconnected sessions	<p>Utilice esta configuración de directiva para configurar un límite de tiempo para las sesiones de Servicios de Escritorio remoto desconectadas.</p> <p>Puede usar esta configuración de directiva para especificar la cantidad máxima de tiempo que una sesión desconectada se mantiene activa en el servidor. De forma predeterminada, Servicios de Escritorio remoto permite a los usuarios desconectarse de una sesión de Servicios de Escritorio remoto sin cerrar sesión.</p> <p>Cuando una sesión está desconectada, los programas en ejecución se mantienen activos aunque el usuario ya no esté conectado de forma activa. De forma predeterminada, estas sesiones desconectadas se mantienen durante un tiempo ilimitado en el servidor.</p> <p>Si habilita esta configuración de directiva, las sesiones desconectadas se eliminarán del servidor una vez transcurrido el tiempo especificado. Para aplicar el comportamiento predeterminado que mantiene las sesiones desconectadas por tiempo ilimitado, seleccione "Nunca". En sesiones de la consola, los límites de tiempo de las sesiones desconectadas no se aplican.</p> <p>Si deshabilita o no establece esta configuración de directiva, las sesiones desconectadas se mantienen durante un tiempo ilimitado. Se pueden especificar límites de tiempo para sesiones desconectadas en la pestaña Sesiones de la herramienta de configuración de host de sesión de Escritorio remoto.</p> <hr/> <p>Nota Esta configuración de directiva aparece tanto en Configuración del equipo como en Configuración de usuario. Si se establecen ambas configuraciones de directiva, tiene prioridad la de Configuración del equipo.</p> <hr/>
Set time limit for active but idle Remote Desktop Services sessions	<p>Utilice esta configuración de directiva para especificar la cantidad máxima de tiempo durante el que una sesión activa de Servicios de Escritorio remoto puede estar inactiva (es decir, sin la intervención del usuario) antes de que se desconecte automáticamente.</p> <p>Si habilita esta configuración de directiva, debe seleccionar el límite de tiempo deseado en la lista desplegable Límite de la sesión inactiva. Servicios de Escritorio remoto desconectará automáticamente las sesiones activas que no se hayan usado en el tiempo límite especificado. El usuario recibe una advertencia dos minutos antes de que se desconecte la sesión, lo que le permite presionar una tecla o mover el mouse para mantener activa la sesión. En sesiones de la consola, los límites de tiempo de las sesiones inactivas no se aplican.</p> <p>Si deshabilita o no establece esta configuración de directiva, Servicios de Escritorio remoto permite mantener las sesiones activas pero sin usar durante un tiempo ilimitado. Se pueden especificar límites de tiempo para sesiones activas, pero en inactividad, en la pestaña Sesiones de la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p>Si desea que los Servicios de Escritorio remoto cierren una sesión, en lugar de desconectarla, puede establecer la configuración de directiva "Finalizar sesión cuando se alcancen los límites de tiempo" en la carpeta Configuración del equipo > Plantillas administrativas > Componentes de Windows ></p>

Ajuste	Descripción
Set time limit for active Remote Desktop Services sessions	<p data-bbox="810 226 1409 342">Utilice esta configuración de directiva para especificar la cantidad máxima de tiempo durante el que una sesión de Servicios de Escritorio remoto puede estar activa antes de que se desconecte automáticamente.</p> <p data-bbox="810 359 1417 636">Si habilita esta configuración de directiva, debe seleccionar el límite de tiempo deseado en la lista desplegable Límite de sesión activa. Servicios de Escritorio remoto desconectará automáticamente las sesiones activas una vez transcurrido el tiempo límite especificado. El usuario recibe una advertencia dos minutos antes de que se desconecte la sesión de Servicios de Escritorio remoto, lo que le permite guardar los archivos abiertos y cerrar programas. En sesiones de la consola, los límites de tiempo de las sesiones activas no se aplican.</p> <p data-bbox="810 653 1417 831">Si deshabilita o no establece esta configuración de directiva, Servicios de Escritorio remoto permite mantener activas las sesiones durante un tiempo ilimitado. Se pueden especificar límites de tiempo para sesiones activas en la pestaña Sesiones de la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p data-bbox="810 848 1417 1058">Si desea que los Servicios de Escritorio remoto cierren una sesión, en lugar de desconectarla, puede establecer la configuración de directiva "Finalizar sesión cuando se alcancen los límites de tiempo" en la carpeta Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de escritorio remoto > Límites de tiempo de sesión.</p> <p data-bbox="810 1087 1417 1203">Nota Esta configuración de directiva aparece tanto en Configuración del equipo como en Configuración de usuario. Si se establecen ambas configuraciones de directiva, tiene prioridad la de Configuración del equipo.</p>

Ajuste	Descripción
<p>Terminate session when time limits are reached</p>	<p>Especifica si se finaliza una sesión de Servicios de Escritorio remoto que ha agotado el tiempo de espera en lugar de desconectarla.</p> <p>Puede usar esta opción para que Servicios de Escritorio remoto finalice una sesión (es decir, se cierra la sesión de usuario y se elimina la sesión del servidor) cuando se alcance el límite de tiempo de sesiones activas o inactivas. De forma predeterminada, Servicios de Escritorio remoto desconecta sesiones que alcanzan sus límites de tiempo.</p> <p>Los límites de tiempo están establecidos localmente por el administrador del servidor o en directivas de grupo. Consulte "Establecer el límite de tiempo para las sesiones activas de Servicios de Escritorio remoto" y "Establecer el límite de tiempo para las sesiones activas, pero en inactividad, de Servicios de Escritorio remoto".</p> <p>Si habilita esta configuración, Servicios de Escritorio remoto finaliza cualquier sesión que alcance el límite de tiempo de espera.</p> <p>Si deshabilita esta configuración, Servicios de Escritorio remoto siempre desconecta una sesión que ha agotado el tiempo de espera, incluso si el administrador del servidor ha especificado otra acción.</p> <p>Si no establece esta configuración, Servicios de Escritorio remoto desconecta una sesión que ha agotado el tiempo de espera, a no ser que la configuración local especifique otra acción.</p> <p>Nota Esta configuración se aplica solo a los límites de tiempo de espera que se establecen deliberadamente (en la herramienta de configuración de host de sesión de Escritorio remoto o en la Consola de administración de directivas de grupo), no a eventos de tiempo de espera que ocurran debido a las condiciones de la conexión o de la red. Asimismo, tenga en cuenta que esta opción aparece tanto en Configuración del equipo como en Configuración de usuario. Si ambas opciones están configuradas, la opción de Configuración del equipo invalida la otra.</p>
<p>Set time limit for logoff of RemoteApp sessions</p>	<p>Utilice esta configuración de directiva para especificar cuánto tiempo permanecerá en estado desconectado una sesión de aplicación remota antes de que ésta se cierre desde el host RDS.</p> <p>De manera predeterminada, si un usuario cierra una aplicación remota, la sesión se desconecta desde el host RDS.</p> <p>Si habilita esta configuración de directiva, cuando un usuario cierre una aplicación remota, su sesión permanecerá en estado desconectado hasta que se alcance el límite de tiempo especificado. Cuando se alcanza el límite de tiempo especificado, la sesión de la aplicación remota se cierra desde el host RDS. Si el usuario inicia una aplicación remota antes de que se alcance el límite de tiempo, se volverá a conectar a la sesión desconectada en el host RDS.</p> <p>Si deshabilita o no establece esta configuración de directiva, cuando un usuario cierra una aplicación remota, la sesión se desconecta desde el host RDS.</p> <p>Nota Esta configuración de directiva aparece tanto en Configuración del equipo como en Configuración de usuario. Si se establecen ambas configuraciones de directiva, tiene</p>

Configuración de carpetas temporales de RDS

La opción de directiva de grupo de conexiones RDS controla la creación y la eliminación de carpetas temporales para sesiones de Servicios de Escritorio remoto.

Tabla 5-24. Configuración de la directiva de grupo de carpetas temporales de RDS

Configuración	Descripción
Do not delete temp folder upon exit	<p>Especifica si Servicios de Escritorio remoto conserva las carpetas temporales por sesión de un usuario al cerrar sesión.</p> <p>Puede usar esta opción para conservar las carpetas temporales específicas de la sesión de un usuario en un equipo remoto, aunque el usuario cierra sesión. De forma predeterminada, Servicios de Escritorio remoto elimina las carpetas temporales de un usuario cuando este cierra sesión.</p> <p>Si el estado se establece en Habilitado, las carpetas temporales por sesión de los usuarios se conservan cuando este cierra sesión.</p> <p>Si el estado se establece en Deshabilitado, las carpetas temporales se eliminan cuando un usuario cierra sesión, aunque el administrador especifique otra acción en la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p>Si el estado se establece en No configurado, Servicios de Escritorio remoto elimina las carpetas temporales del equipo remoto al cerrar sesión, a no ser que el administrador del servidor especificara otra acción.</p> <p>Nota Esta opción solo se aplica si se usan carpetas temporales por sesión en el servidor. Es decir que, si habilita la opción "No usar las carpetas temporales por sesión", esta configuración de directiva no tendrá efecto.</p>
Do not use temporary folders per session	<p>Esta opción de directiva permite evitar que Servicios de Escritorio remoto cree carpetas temporales específicas de la sesión.</p> <p>Puede usar esta opción de directiva para deshabilitar la creación de carpetas temporales separadas en un equipo remoto para cada sesión. De forma predeterminada, Servicios de Escritorio remoto crea una carpeta temporal separada para cada sesión activa que el usuario conserva en un equipo remoto. Estas carpetas temporales se crean en el equipo remoto, en una carpeta Temp en la carpeta de perfil del usuario, y se les asigna el nombre de sessionid.</p> <p>Si habilita esta opción de directiva, no se crean carpetas temporales por sesión. En lugar de ello, los archivos temporales de todas las sesiones del usuario en el equipo remoto se almacenan en una carpeta Temp común en la carpeta de perfil del usuario del equipo remoto.</p> <p>Si deshabilita esta opción de directiva, las carpetas temporales por sesión se crean siempre, aunque especifique otra acción en la herramienta de configuración de host de sesión de Escritorio remoto.</p> <p>Si no configura esta opción de directiva, las carpetas temporales por sesión se crean a no ser que especifique otra acción en la herramienta de configuración de host de sesión de Escritorio remoto.</p>

Filtrar las impresoras por impresión virtual

Cuando se habilita la función de impresión virtual, los usuarios pueden imprimir en cualquier impresora disponible en los sistemas cliente desde las aplicaciones y escritorios remotos. Puede usar la opción de directiva de grupo del agente **Especificar un filtro en el redireccionamiento de impresoras cliente** para que la función de impresión virtual no redirija impresoras cliente específicas a aplicaciones y escritorios remotos.

La opción de la directiva de grupo **Especificar un filtro en el redireccionamiento de impresoras cliente** se encuentra en el archivo de plantilla ADMX de redireccionamiento de impresora de VMware Horizon (vdm_agent_printing.admx) que, a su vez, se incluye en un paquete en el archivo VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip. Para obtener instrucciones de instalación, consulte [Agregar los archivos de plantilla ADMX a Active Directory](#).

Cuando habilita la opción de directiva de grupo **Especificar un filtro en el redireccionamiento de impresoras cliente**, debe escribir una regla de filtrado en el cuadro de texto **Nombre del valor de registro: PrinterFilterString**. La regla de filtrado es una expresión regular que especifica las impresoras que no se deben redireccionar (lista negra). Se redireccionan todas las impresoras que no coincidan con las que se encuentran en la regla de filtrado. De forma predeterminada, la regla de filtrado está vacía, lo que significa que se redireccionan todas las impresoras cliente.

La siguiente tabla muestra los atributos, los operadores y los caracteres comodín que puede usar en las reglas de filtrado.

Tabla 5-25. Atributos, operadores y caracteres comodín que se admiten en las reglas de filtrado

Atributos	Operadores	Caracteres comodín
DriverName, VendorName y PrinterName	AND, OR y NOT	* y ?

A continuación aparecen varios ejemplos de reglas de filtrado.

```
(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"
```

```
PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"
```

```
PrinterName!=".*PDFCreator.*"
```

Habilite la función de impresión virtual cuando instale Horizon Agent en un escritorio virtual o un host RDS. Si desea obtener instrucciones de instalación, consulte los documentos *Configurar escritorios virtuales en Horizon 7* y *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Configurar impresión según ubicación

La función de impresión según ubicación asigna impresoras que están físicamente cerca de los sistemas cliente a los escritorios remotos, lo que permite que los usuarios puedan imprimir en sus impresoras locales y de red desde sus escritorios remotos.

La función de impresión basada en la ubicación permite que las organizaciones de TI asignen escritorios remotos a la impresora más cercana al dispositivo cliente endpoint. Por ejemplo, si un doctor se mueve de una habitación a otra de un hospital, cada vez que el doctor imprima algo, el trabajo de impresión se envía a la impresora más cercana.

La función impresión según ubicación está disponible para Windows, Mac, Linux y dispositivos cliente móviles.

La impresión según ubicación se admite en las aplicaciones y los escritorios remotos siguientes:

- Escritorios que se implementan en equipos de usuario único, incluyendo escritorios Windows y equipos Windows Server
- Escritorios que se implementan en hosts RDS, donde los hosts RDS son máquinas virtuales
- Aplicaciones publicadas
- Las aplicaciones publicadas que se inician desde Horizon Client, dentro de los escritorios remotos

Para usar la función de impresión según ubicación, debe instalar la opción de configuración Impresión virtual con Horizon Agent e instalar los controladores de impresora correctos en el escritorio.

Configure la impresión según ubicación mediante la opción `AutoConnect Map Additional Printers for VMware View` de la directiva de grupo de Active Directory, que se encuentra en el Editor de objetos de directiva de grupo de Microsoft. Para acceder a ella, seleccione **Configuración del equipo** y abra la carpeta **Configuración de software**.

Nota `AutoConnect Map Additional Printers for VMware View` es una directiva específica del equipo. Las directivas específicas del equipo se aplican a todos los escritorios remotos, independientemente de la persona que se conecte al escritorio.

`AutoConnect Map Additional Printers for VMware View` se implementa como tabla de traducción de nombres. Cada fila de la tabla permite identificar una impresora específica y definir un conjunto de reglas de traducción para dicha impresora. Las reglas de traducción determinan si la impresora se asigna al escritorio remoto de un sistema cliente en concreto.

Cuando un usuario se conecta a un escritorio remoto, Horizon 7 compara el sistema cliente con las reglas de traducción asociadas a cada impresora de la tabla. Si el sistema cliente cumple todas las reglas de traducción establecidas para una impresora, o bien una impresora no tiene ninguna regla de traducción asociada, Horizon 7 asigna la impresora al escritorio remoto durante la sesión del usuario.

Puede definir reglas de traducción basadas en la dirección IP, el nombre y la dirección MAC del sistema cliente y en el nombre de usuario y su grupo. Puede especificar una regla de traducción o una combinación de varias reglas de traducción para una impresora en concreto.

La información usada para asignar la impresora al escritorio remoto se almacena en una entrada de registro en el escritorio remoto en `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

Configuración de impresoras para la impresión según ubicación

La configuración de impresoras para impresión según ubicación se conserva después de que un usuario cierre sesión o se desconecte del escritorio. Por ejemplo, es posible que un usuario establezca que una impresora según ubicación use el modo blanco y negro. Cuando el usuario cierra sesión y vuelve a iniciarla en el escritorio, la impresora según ubicación sigue usando el modo blanco y negro.

Para guardar la configuración de la impresora en diferentes sesiones de una aplicación publicada, el usuario debe seleccionar una impresora según ubicación en el cuadro de diálogo de impresión de la aplicación, hacer clic con el botón secundario en la impresora seleccionada y seleccionar **Preferencias de impresión**. La configuración de impresión no se guarda si el usuario selecciona una impresora y hace clic en el botón **Preferencias** del cuadro de diálogo de impresión de la aplicación.

No se admiten configuraciones persistentes para impresoras basadas en la ubicación si la configuración se guarda en el espacio privado del controlador de la impresora y no en la parte extendida DEVMODE del controlador de la impresora, tal como recomienda Microsoft. Para disponer de configuraciones persistentes, implemente impresoras que tengan guardada su configuración en la parte DEVMODE del controlador de la impresora.

Registrar el archivo DLL de la directiva de grupo de impresión según ubicación

Para poder configurar la opción de directiva de grupo para la impresión según ubicación, debe registrar el archivo DLL `TPVMGPoACmap.dll`.

Las versiones de 32 y 64 bits de `TPVMGPoACmap.dll` están disponibles en un paquete de archivos .zip llamado `VMware-Horizon-Extras-Paquete-x.x.x-yyyyyy.zip`, donde `x.x.x` es la versión y `yyyyyy` es el número de compilación. Puede descargar el archivo desde el sitio de descargas de VMware en <http://www.vmware.com/go/downloadview>.

Procedimiento

- 1 Copie la versión apropiada de `TPVMGPoACmap.dll` en su servidor de Active Directory o en el equipo dominio que use para configurar las directivas de grupo.
- 2 Mediante la utilidad `regsvr32`, registre el archivo `TPVMGPoACmap.dll`.

Por ejemplo: `regsvr32 "C:\TPVMGPoACmap.dll"`

Pasos siguientes

Configure la opción de directiva de grupo de impresión según ubicación.

Configurar la directiva de grupo de impresión según ubicación

Para configurar la impresión según ubicación, configure el ajuste de directiva de grupo `AutoConnect Map Additional Printers for VMware View`. La opción de directiva de grupo es una tabla de traducción de nombres que asigna impresoras a escritorios de Horizon.

Requisitos previos

- Compruebe que estén disponibles los complementos Editor de objetos de directiva de grupo y MMC de Microsoft en su servidor de Active Directory o en el equipo del dominio que usa para configurar directivas de grupo.
- Registre el archivo DLL TPVMGPoACmap.dll en su servidor de Active Directory o en el equipo del dominio que usa para configurar directivas de grupo. Consulte [Registrar el archivo DLL de la directiva de grupo de impresión según ubicación](#).
- Familiarícese con la sintaxis del ajuste de directiva de grupo AutoConnect Map Additional Printers for VMware View. Consulte [Sintaxis de la opción de la directiva de grupo de impresión según ubicación](#).
- Cree un GPO para la opción de directiva de grupo basada en ubicación y vincúlelo a la unidad organizativa que contenga sus escritorios de Horizon. Consulte [Crear GPO para directivas de grupo de Horizon 7](#) para ver un ejemplo de cómo crear GPO para directivas de grupo de Horizon.
- Compruebe que se haya instalado la opción de configuración de Impresión virtual con Horizon Agent en sus escritorios. Para verificarlo, compruebe si se han instalado el Servicio de autoconexión y el Servicio de puerta de enlace TP VC en el sistema operativo del escritorio.
- Como los trabajos de impresión se envían directamente desde el escritorio de Horizon a la impresora, compruebe que estén instalados en sus escritorios los controladores de impresora necesarios.

Procedimiento

- 1 En el servidor de Active Directory, edite el GPO.

Versión de AD	Ruta de navegación
Windows 2003	<ol style="list-style-type: none"> a Seleccione Inicio > Todos los programas > Herramientas administrativas > Usuarios y equipos de Active Directory. b Haga clic con el botón secundario en la unidad organizativa que contenga los escritorios de Horizon y seleccione Propiedades. c En la pestaña Directiva de grupo, haga clic en Abrir para abrir el complemento Administración de directivas de grupo. d En el panel derecho, haga clic con el botón secundario en el GPO que creó para el ajuste de directiva de grupo de impresión según ubicación y seleccione Editar.
Windows 2008	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda su dominio y haga clic con el botón secundario en el GPO que creó para el ajuste de directiva de grupo de impresión según ubicación y seleccione Editar.

Se abrirá la ventana del **Editor de objetos de directiva de grupo**.

- 2 Expanda **Configuración del equipo**, abra la carpeta **Configuración de software** y seleccione **Impresoras adicionales del mapa de conexión automática para VMware View**.

- 3 En el panel Directiva, haga doble clic en **Configurar impresoras adicionales del mapa de conexión automática**.

Se abre la ventana **Impresoras adicionales del mapa de conexión automática para VMware View**.

- 4 Seleccione **Habilitado** para habilitar el ajuste de directiva de grupo.

Los botones y los encabezados de la tabla de traducción se muestran en la ventana de la directiva de grupo.

Importante Si hace clic en **Deshabilitado**, se eliminan todas las entradas de la tabla. Como medida de precaución, guarde su configuración para poder importarla más adelante.

- 5 Agregue las impresoras que quiera asignar a escritorios de Horizon y defina sus reglas de traducción asociadas.
- 6 Haga clic en **Aceptar** para guardar los cambios.

Sintaxis de la opción de la directiva de grupo de impresión según ubicación

Utilice la opción de la directiva de grupo `AutoConnect Map Additional Printers for VMware View` para asignar impresoras a escritorios remotos.

`AutoConnect Map Additional Printers for VMware View` es una tabla de traducción de nombres que identifica impresoras y define reglas de traducción asociada. [Tabla 5-26. Valores y columnas de la tabla](#) describe la sintaxis de la tabla de traducción.

La impresión según ubicación asigna impresoras locales a escritorios remotos, pero no admite la asignación de impresoras de red que se configuren mediante rutas de acceso UNC.

Tabla 5-26. Valores y columnas de la tabla

Columna	Descripción
IP Range	<p>Regla de traducción que especifica un rango de direcciones IP para sistemas cliente.</p> <p>Para especificar direcciones IP de un rango específico, use la siguiente notación:</p> <p><i>dirección_ip-dirección_ip</i></p> <p>Por ejemplo: 10.112.116.0-10.112.119.255</p> <p>Para especificar todas las direcciones IP de una subred específica, use la siguiente notación:</p> <p><i>dirección_ip/bits_máscara_subred</i></p> <p>Por ejemplo: 10.112.4.0/22</p> <p>Esta notación especifica las direcciones IPv4 que se pueden utilizar desde 10.112.4.1 hasta 10.112.7.254.</p> <p>Introduzca un asterisco para que coincida con cualquier dirección IP.</p>
Client Name	<p>Regla de traducción que especifica un nombre de equipo.</p> <p>Por ejemplo: Equipo de María</p> <p>Introduzca un asterisco para que coincida con cualquier nombre de equipo.</p>
Mac Address	<p>Regla de traducción que especifica una dirección MAC. En el editor GPO, debe usar el mismo formato que use el sistema cliente. Por ejemplo:</p> <ul style="list-style-type: none"> ■ Los clientes Windows usan guiones: 01-23-45-67-89-ab ■ Los clientes Linux usan dos puntos: 01:23:45:67:89:ab <p>Introduzca un asterisco para que coincida con cualquier dirección MAC.</p>
User/Group	<p>Regla de traducción que especifica un nombre de usuario o de grupo.</p> <p>Para especificar un usuario o un grupo particular, use la siguiente notación:</p> <p><i>\\dominio\usuario_o_grupo</i></p> <p>Por ejemplo: \\midominio\María</p> <p>El nombre de dominio completo (FQDN) no es una notación válida para el nombre de dominio. Introduzca un asterisco para que coincida con cualquier nombre de usuario o de grupo.</p>
Printer Name	<p>El nombre de la impresora cuando está asignada al escritorio remoto.</p> <p>Por ejemplo: IMPRESORA-2-CLR</p> <p>El nombre asignado no tiene que coincidir con el nombre de la impresora en el sistema cliente.</p> <p>La impresora debe estar en el dispositivo cliente. No se puede asignar una impresora de red de una ruta de acceso UNC.</p>
Printer Driver	<p>El nombre del controlador que usa la impresora.</p> <p>Por ejemplo: HP Color LaserJet 4700 PS</p> <p>Importante El controlador de la impresora debe instalarse en el escritorio, ya que los trabajos de impresión se envían directamente desde el escritorio hasta la impresora.</p>

Columna	Descripción
IP Port/ThinPrint Port	<p>Para impresoras de red, la dirección IP de la impresora que se agrega al principio de IP_.</p> <p>Por ejemplo: IP_10.114.24.1</p> <p>El puerto predeterminado es 9100. Puede especificar un puerto no predeterminado si agrega el número de puerto a la dirección IP.</p> <p>Por ejemplo: IP_10.114.24.1:9104</p>
Default	Indica si la impresora es la predeterminada.

Use los botones que aparecen encima de los títulos de las columnas para agregar, eliminar y mover filas y guardar e importar entradas de la tabla. Cada botón tiene una combinación de teclas equivalente. Para ver una descripción de un botón así como su combinación de teclas equivalente, coloque el mouse encima de él. Por ejemplo, para insertar una fila al final de una tabla, haga clic en el primer botón de la tabla o pulse Alt+A. Haga clic en los dos últimos botones para importar y guardar las entradas de la tabla.

[Tabla 5-27. Ejemplo de la opción de la directiva de grupo de impresión según ubicación](#) muestra un ejemplo de dos traducciones de filas de tabla.

Tabla 5-27. Ejemplo de la opción de la directiva de grupo de impresión según ubicación

Rango de direcciones IP	Nombre de cliente	Dirección MAC	Usuario/Grupo	Nombre de impresora	Controlador de impresora	Puerto IP/Puerto ThinPrint	Predeterminado
*	*	*	*	IMPRESORA-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	IMPRESORA-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

La impresora de red especificada en la primera fila se asignará a un escritorio remoto de cualquier sistema cliente porque aparecen asteriscos en la traducción de las columnas de reglas. La impresora de red especificada en la segunda fila solo se asignará a un escritorio remoto si el sistema cliente tiene una dirección IP en el rango 10.112.116.140 hasta 10.112.116.145.

Ejemplo de directiva de grupo de Active Directory

Una forma de implementar directivas de grupo de Active Directory en Horizon 7 consiste en crear una unidad organizativa (Organizational Unit, OU) para las máquinas que suministren sesiones de escritorio remoto y vinculen uno o varios objetos de directiva de grupo (Group Policy Object, GPO). Puede utilizar estos GPO para aplicar los ajustes de directiva de grupo a sus máquinas de Horizon 7.

Puede vincular GPO directamente a un dominio si los ajustes de directiva se aplican a todos los equipos del dominio. Sin embargo, como práctica recomendada, la mayoría de las implementaciones deberían vincular los GPO a OU individuales para impedir que se procese la directiva en todos los equipos del dominio.

Puede configurar las directivas en su servidor de Active Directory o en cualquier equipo del dominio. En este ejemplo, se muestra cómo configurar las directivas directamente en su servidor de Active Directory.

Nota Puesto que cada entorno de Horizon 7 es diferente, puede que tenga que dar distintos pasos para satisfacer las necesidades específicas de su organización.

Crear una unidad organizativa (OU) para máquinas de Horizon 7

Para aplicar directivas de grupo a las máquinas que proporcionen sesiones de escritorios remotos sin afectar a otros equipos Windows que se encuentren en el mismo dominio de Active Directory, cree una unidad organizativa (OU) específicamente para sus máquinas de Horizon 7. Puede crear una OU para toda la implementación de Horizon 7 o crear unidades organizativas independientes para máquinas de escritorios virtuales y hosts RDS.

Procedimiento

- 1 En el servidor de Active Directory, seleccione **Inicio > Todos los programas > Herramientas administrativas > Usuarios y equipos de Active Directory**.
- 2 Haga clic con el botón secundario en el dominio que contenga sus máquinas de Horizon 7 y seleccione **Nuevo > Unidad organizativa**.
- 3 Escriba un nombre para la OU y haga clic en **Aceptar**.
La nueva OU se muestra en el panel izquierdo.
- 4 Agregue máquinas de Horizon 7 a la nueva OU.
 - a Haga clic en **Equipos** en el panel izquierdo.
Todos los objetos de equipo del dominio aparecen en el panel derecho.
 - b Haga clic con el botón secundario en el nombre del objeto de equipo que represente la máquina de Horizon 7 en el panel de la derecha y seleccione **Mover**.
 - c Seleccione la OU y haga clic en **Aceptar**.
Se mostrará la máquina de Horizon 7 en el panel derecho al seleccionar la OU.

Pasos siguientes

Cree GPO para directivas de grupo de Horizon 7.

Crear GPO para directivas de grupo de Horizon 7

Cree GPO para que contengan directivas de grupo de componentes de Horizon 7 y de impresión según ubicación y vincúelos a la unidad organizativa (organizational unit, OU) de sus máquinas de Horizon 7.

Requisitos previos

- Cree una OU para sus máquinas de Horizon 7
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.

- Compruebe que estén disponibles los complementos Administración de directivas de grupo y MMC en su servidor de Active Directory.

Procedimiento

- 1 En el servidor de Active Directory, abra la Consola de administración de directivas de grupo.
- 2 Expanda su dominio, haga clic con el botón secundario en la OU que contiene sus máquinas de Horizon 7 y seleccione **Crear un GPO en este dominio y vincularlo aquí**.
- 3 Escriba un nombre para el GPO y haga clic en **Aceptar**.

El nuevo GPO se muestra bajo la OU en el panel izquierdo.

- 4 (opcional) Aplique el GPO a las máquinas de Horizon 7 específicas de la OU.
 - a Seleccione el GPO en el panel izquierdo.
 - b Seleccione **Filtrado de seguridad > Agregar**.
 - c Escriba el nombre de equipo de las máquinas de Horizon 7 y haga clic en **Aceptar**.

Se mostrarán las máquinas de Horizon 7 en el panel Filtrado de seguridad. Los ajustes del GPO solo se aplican a estas máquinas.

Pasos siguientes

Agregue las plantillas ADMX de Horizon al GPO.

Agregar un archivo de plantilla ADMX Horizon 7 a un GPO

Para aplicar la configuración de directiva de grupo de los componentes de Horizon 7 a las aplicaciones y escritorios, agregue los archivos de plantilla ADMX a los GPO.

Requisitos previos

- Cree GPO para la configuración de directiva de grupo de componentes de Horizon 7 y vincúlelos a la OU que contenga sus máquinas de Horizon 7.
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Administración de directivas de grupo y MMC en su servidor de Active Directory.

Procedimiento

- 1 Descargue el paquete GPO de Horizon 7.zip del 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 paquete GPO.

Este archivo se llama VMware-Horizon-Extras-Bundle-*x.x.x-yyy-yyyyy*.zip, donde *x.x.x* es la versión y *yyy-yyyyy* es el número de compilación. Todos los archivos ADMX que proporcionan opciones de configuración de las directivas de grupo para Horizon 7 están disponibles en este archivo.

- 2 Descomprima el archivo VMware-Horizon-Extras-Bundle-*x.x.x-yyy-yyyyy*.zip y copie los archivos ADMX al servidor de Active Directory.
 - a Copie los archivos .admx y la carpeta en-US a la carpeta %systemroot%\PolicyDefinitions del servidor de Active Directory.
 - b Copie los archivos de recursos de idioma (.adml) a la subcarpeta adecuada en %systemroot%\PolicyDefinitions\ del servidor de Active Directory.
- 3 En el servidor de Active Directory, abra el Editor de administración de directivas de grupo y escriba la ruta de acceso a los archivos de plantilla en la que estos vayan a aparecer en el editor después de la instalación.

Pasos siguientes

Establezca la configuración de directiva de grupo y habilite el procesamiento de bucle invertido para las máquinas de Horizon 7.

Habilitar procesamiento de bucle invertido para escritorios remotos

Para hacer que la configuración de usuario que normalmente se aplica a un equipo se aplique también a todos los usuarios que inicien sesión en ese equipo, habilite el procesamiento de bucle invertido.

Requisitos previos

- Cree GPO para la configuración de directiva de grupo de componentes de Horizon 7 y vincúlelos a la OU que contenga sus máquinas de Horizon 7.
- Verifique que pueda iniciar sesión como usuario de dominio Administrador en la máquina que aloja su servidor Active Directory.
- Compruebe que estén disponibles los complementos Administración de directivas de grupo y MMC en su servidor de Active Directory.

Procedimiento

- 1 En el servidor de Active Directory, abra la Consola de administración de directivas de grupo.
- 2 Expanda su dominio, haga clic con el botón secundario en el GPO que creó para la configuración de la directiva de grupo y seleccione **Editar**.
- 3 En el Editor de administración de directivas de grupo, diríjase a **Configuración del equipo > Directivas > Plantillas administrativas: definición de directivas > Sistema > Directiva de grupo**.
- 4 En el panel derecho, haga doble clic en **Modo de procesamiento de bucle invertido de la directiva de grupo de usuario**.

- 5 Seleccione **Habilitado** y, a continuación, seleccione un modo de procesamiento de bucle invertido del menú desplegable **Modo**.

Opción	Acción
Combinar	La configuración de directivas de usuario aplicada es una combinación de aquellas que están incluidas tanto en el equipo como en los GPO de usuario. Cuando se produzca un conflicto, los GPO del equipo tendrán preferencia.
Reemplazar	Las directivas de usuario se definen totalmente a partir de los GPO asociados con el equipo. Cualquier GPO asociado con el usuario se ignorará.

- 6 Haga clic en **Aceptar** para guardar los cambios.