Seguridad en Horizon Client y Agent

Horizon Client 3.x/4.x y View Agent 6.2.x/Horizon Agent 7.2/7.1/7.0.x

VMware Horizon 7 7.2

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Contenido

Seguridad en Horizon Client y Agent

Seguridad en Horizon Client y Agent proporciona una referencia concisa sobre las funciones de seguridad de VMware Horizon® Client™ y Horizon Agent (para Horizon 7) o VMware View Agent® (para Horizon 6). Esta guía acompaña a la guía *Seguridad de View*, que se elabora para cada versión principal y secundaria de VMware Horizon™ 6 y Horizon 7. La guía *Seguridad en Horizon Client y Agent* se actualiza cada trimestre, con las versiones trimestrales del software de cliente y agente.

Horizon Client es la aplicación que inician los usuarios finales desde sus dispositivos cliente para conectarse a una aplicación o escritorio remotos. View Agent (para Horizon 6) u Horizon Agent (para Horizon 7) es el software agente que se ejecuta en el sistema operativo del escritorio remoto o host de Microsoft RDS que proporciona aplicaciones remotas. Esta guía incluye la siguiente información:

- Cuentas necesarias para iniciar sesión en el sistema. ID de inicio de sesión de las cuentas creadas durante la instalación/el arranque del sistema e instrucciones sobre cómo cambiar los valores predeterminados.
- Opciones y configuración que tienen implicaciones de seguridad.
- Los recursos que deben estar protegidos, como los archivos y las contraseñas de configuración relevantes para la seguridad, y los controles de acceso recomendados para realizar un funcionamiento seguro.
- Ubicación de los archivos de registro y su finalidad.
- Privilegios asignados a usuarios del servicio.
- Interfaces externas, puertos y servicios que se deben abrir o habilitar para que funcione correctamente el cliente y el agente.
- Información sobre cómo pueden obtener y aplicar los clientes la actualización o la revisión de seguridad más recientes.

Audiencia prevista

Esta información está dirigida a las personas encargadas de la toma de decisiones de TI, a arquitectos, administradores y a otras personas que necesiten familiarizarse con los componentes de seguridad de Horizon 6 u Horizon 7, incluyendo el cliente y el agente.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario de términos que quizás desconozca. Para ver la definición de los términos que se utilizan en la documentación técnica de VMware, visite http://www.vmware.com/support/pubs.

Puertos externos 1

Para el correcto funcionamiento del producto y dependiendo de las funciones que desee utilizar, se deben abrir varios puertos para que se puedan comunicar entre sí los clientes y el agente en los escritorios remotos.

Este capítulo cubre los siguientes temas:

Comprender los protocolos de comunicaciones de Horizon 7

Los componentes de Horizon 7 intercambian mensajes utilizando diferentes protocolos distintos.

Tabla 1-1 enumera los puertos predeterminados que se utilizan para cada protocolo. Si fuese necesario para cumplir las directivas de la organización o para evitar la contención, puede cambiar los números de puerto que se utilizan.

Tabla 1-1. Puertos predeterminados

Protocolo	Puerto
JMS	Puerto TCP 4001 Puerto TCP 4002
HTTP	Puerto TCP 80
HTTPS	Puerto TCP 443
MMR/CDR	Para el redireccionamiento multimedia y de la unidad cliente, se utiliza el puerto TCP 9427.
RDP	Puerto TCP 3389
PCoIP	Puerto TCP 4172 Puertos UDP 4172, 50002, 55000
Redireccionamiento USB	Puerto TCP 32111. Este puerto también se utiliza para la sincronización de la zona horaria.
VMware Blast Extreme	Puerto TCP 8443, 22443 Puertos UDP 443, 8443, 22443
HTML Access	Puerto TCP 8443, 22443

Reglas de firewall de Horizon Agent

El programa de instalación de Horizon Agent configura de forma opcional las reglas del firewall de Windows en los escritorios remotos y los hosts RDS para abrir los puertos de red predeterminados. Los puertos son de entrada a menos que se especifique lo contrario.

El programa de instalación del agente configura la regla del firewall local para que las conexiones RDP entrantes coincidan con el puerto RDP actual del sistema operativo del host, que suele ser 3389.

Si indica al programa de instalación del agente que no habilite la compatibilidad con escritorios remotos, no abrirá los puertos 3389 y 32111, y deberá abrirlos manualmente.

Si cambia el número de puerto RDP tras la instalación, deberá modificar las reglas del firewall asociadas. Si cambia un puerto predeterminado después de la instalación, debe volver a configurar de forma manual las reglas del firewall de Windows para permitir el acceso al puerto actualizado. Consulte "Reemplazar los puertos predeterminados para los servicios de View" en el documento *Instalación de View*.

Las reglas de firewall de Windows para Horizon Agent en hosts RDS muestran un bloque de 256 puertos UDP contiguos abiertos para el tráfico entrante. Este bloque de puertos es para el uso interno de VMWare Blast Extreme en Horizon Agent. Un controlador especial firmado de Microsoft sobre hosts RDS bloquea el tráfico entrante que llega a estos puertos de fuentes externas. Este controlador causa que el firewall de Windows trate los puertos como cerrados.

Si utiliza una plantilla de máquina virtual como origen de escritorio, las excepciones del firewall solo se aplican en los escritorios implementados si la plantilla es un miembro del dominio de escritorio. Puede utilizar la configuración de directiva de grupo de Microsoft para administrar las excepciones de firewall local. Consulte el artículo 875357 de la Microsoft Knowledge Base (KB) para obtener más información.

Tabla 1-2. Puertos TCP y UDP abiertos durante la instalación del agente

Protocolo	Puertos
RDP	Puerto TCP 3389
Redireccionamiento USB y sincronización de la zona horaria	Puerto TCP 32111
MMR (redireccionamiento multimedia) y CDR (redireccionamiento de la unidad cliente)	Puerto TCP 9427
PCoIP	Puerto TCP 4172 Puerto UDP 4172 (bidireccional)
VMware Blast Extreme	Puerto TCP 22443 Puerto UDP 22443 (bidireccional) **NOTA:** UDP no se utiliza en escritorios Linux.
HTML Access	Puerto TCP 22443

Puertos TCP y UDP utilizados por clientes y agentes

View Agent (para Horizon 6), Horizon Agent (para Horizon 7) y Horizon Client utilizan puertos TCP y UDP para el acceso en red entre ellos y a varios componentes de servidor de Horizon 7.

Tabla 1-3. Puertos UDP y TCP que usa View Agent o Horizon Agent

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Horizon Client	*	View Agent/Horizon Agent	3389	TCP	Tráfico de Microsoft RDP a los escritorios de View si se usan conexiones directas en lugar de conexiones en túnel.
Horizon Client	*	View Agent/Horizon Agent	9427	TCP	Redireccionamiento Windows Media MMR y redireccionamiento de la unidad cliente, si se usan las conexiones directas en lugar de las conexiones en túnel. **NOTA:** No es necesario para CDR cuando se utiliza VMware Blast Extreme.
Horizon Client	*	View Agent/Horizon Agent	32111	TCP	Redireccionamiento USB y sincronización de la zona horaria si se usan conexiones directas en lugar de conexiones en túnel.
Horizon Client	*	View Agent/Horizon Agent	4172	TCP y UDP	PCoIP si no se usa la puerta de enlace segura de PCoIP. **NOTA:** Como el puerto de origen varía, consulte la nota que aparece bajo esta tabla.
Horizon Client	*	Horizon Agent	22443	TCP y UDP	VMware Blast Extreme si se utilizan conexiones directas en lugar de conexiones en túnel. **NOTA:** UDP no se utiliza en escritorios Linux.
Navegador	*	View Agent/Horizon Agent	22443	TCP	HTML Access si se utilizan conexiones directas en lugar de conexiones en túnel.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	View Agent/Horizon Agent	3389	TCP	Tráfico de Microsoft RDP a los escritorios de View cuando se usan conexiones en túnel.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	View Agent/Horizon Agent	9427	TCP	Redireccionamiento Windows Media MMR y redireccionamiento de la unidad cliente cuando se usan conexiones en túnel.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	View Agent/Horizon Agent	32111	TCP	Redireccionamiento USB y sincronización de la zona horaria cuando se usan conexiones en túnel.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	55000	View Agent/Horizon Agent	4172	UDP	PCoIP (no SALSA20) si se usa la puerta de enlace segura de PCoIP.

Tabla 1-3. Puertos UDP y TCP que usa View Agent o Horizon Agent (Continua)

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	View Agent/Horizon Agent	4172	TCP	PCoIP si se usa la puerta de enlace segura de PCoIP.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	Horizon Agent	22443	TCP y UDP	VMware Blast Extreme si se usa la puerta de enlace segura de Blast. **NOTA:** UDP no se utiliza en escritorios Linux.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	View Agent/Horizon Agent	22443	TCP	HTML Access si se usa la puerta de enlace segura de Blast.
View Agent/Horizon Agent	*	Servidor de conexión de View	4001, 4002	TCP	Tráfico SSL de JMS.
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP si no se usa la puerta de enlace segura de PCoIP. **NOTA:** Como el puerto de destino varía, consulte la nota que aparece bajo esta tabla.
View Agent/Horizon Agent	4172	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	55000	UDP	PCoIP (no SALSA20) si se usa la puerta de enlace segura de PCoIP.

NOTA: El número de puerto UDP que usan los agentes para PCoIP puede cambiar. Si el puerto 50002 se está utilizando, el agente usará el puerto 50003. Si el puerto 50003 se está utilizando, el agente usará el puerto 50004, y así sucesivamente. Debe configurar el firewall con la opción ANY donde aparece un asterisco (*) en la tabla.

Tabla 1-4. Puertos UDP y TCP usados por Horizon Client

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Horizon Client	*	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	443	TCP	HTTPS para iniciar sesión en View. (Este puerto también se usa en los túneles de las conexiones en túnel). **NOTA:** Horizon Client 4.4 y versiones posteriores son compatibles con el puerto UDP 443 (consulte la información a continuación).
Horizon Client 4.4 o posterior	*	Dispositivo Unified Access Gateway 2.9 o versiones posteriores	443	UDP	HTTPS para iniciar sesión en View, si se utiliza la puerta de enlace segura Blast y si el Servidor del túnel UDP está habilitado. (Este puerto también se usa en los túneles de las conexiones en túnel).

Tabla 1-4. Puertos UDP y TCP usados por Horizon Client (Continua)

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Dispositivo Unified Access Gateway 2.9 o versiones posteriores	443	Horizon Client 4.4 o posterior	*	UDP	HTTPS para iniciar sesión en View, si se utiliza la puerta de enlace segura Blast y si el Servidor del túnel UDP está habilitado. (Este puerto también se usa en los túneles de las conexiones en túnel).
Horizon Client	*	View Agent/Horizon Agent	22443	TCP	HTML Access y VMware Blast Extreme si no se usa la puerta de enlace segura de Blast.
Horizon Client	*	Horizon Agent	22443	UDP	VMware Blast Extreme si no se usa la puerta de enlace segura de Blast. **NOTA:** No se utiliza cuando se conecta a los escritorios Linux.
Horizon Agent	22443	Horizon Client	*	UDP	VMware Blast Extreme si no se usa la puerta de enlace segura de Blast. **NOTA:** No se utiliza cuando se conecta a los escritorios Linux.
Horizon Client	*	View Agent/Horizon Agent	3389	TCP	Tráfico de Microsoft RDP a los escritorios de View si se usan conexiones directas en lugar de conexiones en túnel.
Horizon Client	*	View Agent/Horizon Agent	9427	TCP	Redireccionamiento Windows Media MMR y redireccionamiento de la unidad cliente, si se usan las conexiones directas en lugar de las conexiones en túnel. **NOTA:** No es necesario para CDR cuando se utiliza VMware Blast Extreme.
Horizon Client	*	View Agent/Horizon Agent	32111	TCP	Redireccionamiento USB y sincronización de la zona horaria si se usan conexiones directas en lugar de conexiones en túnel.
Horizon Client	*	View Agent/Horizon Agent	4172	TCP y UDP	PCoIP si no se usa la puerta de enlace segura de PCoIP. **NOTA:** Como el puerto de origen varía, consulte la nota que aparece bajo esta tabla.
Horizon Client	*	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	4172	TCP y UDP	PCoIP (no SALSA20) si se usa la puerta de enlace segura de PCoIP. **NOTA:** Como el puerto de origen varía, consulte la nota que aparece bajo esta tabla.
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP si no se usa la puerta de enlace segura de PCoIP. **NOTA:** Como el puerto de destino varía, consulte la nota que aparece bajo esta tabla.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	4172	Horizon Client	*	UDP	PCoIP (no SALSA20) si se usa la puerta de enlace segura de PCoIP. **NOTA:** Como el puerto de destino varía, consulte la nota que aparece bajo esta tabla.

Tabla 1-4. Puertos UDP y TCP usados por Horizon Client (Continua)

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Horizon Client	*	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	8443	TCP	HTML Access y VMware Blast Extreme si se usa la puerta de enlace segura de Blast.
Horizon Client	*	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	8443	UDP	VMware Blast Extreme si se usa la puerta de enlace segura de Blast. **NOTA:** No se utiliza cuando se conecta a un escritorio Linux.
Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	8443	Horizon Client	*	UDP	VMware Blast Extreme si se usa la puerta de enlace segura de Blast. **NOTA:** No se utiliza cuando se conecta a un escritorio Linux.

NOTA: El número de puerto UDP que utilizan los clientes para PCoIP y VMware Blast Extreme puede cambiar. Si se usa el puerto 50002, el cliente usará 50003. Si se usa el puerto 50003, el cliente usará el puerto 50004 y sucesivamente. Debe configurar el firewall con la opción ANY donde aparece un asterisco (*) en la tabla.

Procesos, demonios y servicios instalados 2

Cuando ejecuta el instalador de cliente o agente, se instalan varios componentes.

Este capítulo cubre los siguientes temas:

Servicios instalados por View Agent o el instalador de Horizon Agent en máquinas Windows

La operación de las aplicaciones y los escritorios remotos depende de varios servicios de Windows.

Tabla 2-1. Servicios de View Agent (para Horizon 6) o Horizon Agent (para Horizon 7)

Nombre del servicio	Tipo de inicio	Descripción
VMware Blast	Automático	Proporciona servicios para HTML Access y para usar el protocolo VMware Blast Extreme para conectar con clientes nativos.
VMware Horizon View Agent	Automático	Proporciona servicios para View Agent/Horizon Agent.
VMware Horizon View Composer Guest Agent Server	Automático	Proporciona servicios si esta máquina virtual forma parte de un grupo de escritorios de clon vinculado de View Composer.
VMware Horizon View Persona Management	Automático si la función está habilitada; de lo contrario, Deshabilitado.	Proporciona servicios para la función VMware Persona Management.
VMware Horizon View Script Host	Deshabilitada	Proporciona soporte para ejecutar scripts de inicio de sesión, si los hubiese, para configurar directivas de seguridad de escritorio antes de que comience una sesión de escritorio. Las políticas se basan en el dispositivo de cliente y la ubicación del usuario.
Servicio de supervisor de VMware Netlink	Automático	Para admitir la función de redireccionamiento de escáner y la función de redireccionamiento del puerto serie, proporciona servicios de supervisión para transferir información entre los procesos de espacio de usuarios y kernel.
Servicio de cliente de redireccionamiento del escáner de VMware	Automático	(View Agent 6.0.2 y versiones posteriores) Proporciona servicios para la función de redireccionamiento del escáner.

Tabla 2-1. Servicios de View Agent (para Horizon 6) o Horizon Agent (para Horizon 7) (Continua)

Nombre del servicio	Tipo de inicio	Descripción
Servicio de cliente de comunicaciones serie de VMware	Automático	(View Agent 6.1.1 y versiones posteriores) Proporciona servicios para la función de redireccionamiento del puerto serie.
VMware Snapshot Provider	Manual	Proporciona servicios para snapshots de máquinas virtuales, que se utilizan para clonar.
VMware Tools	Automático	Proporciona soporte para sincronizar objetos entre los sistemas operativos de invitado y host, que mejora el rendimiento del sistema operativo de invitado de máquinas virtuales y la gestión de la máquina virtual.
Servicio de arbitraje USB de VMware	Automático	Enumera los diversos dispositivos USB conectados al cliente y determina qué dispositivos conectar al cliente y cuáles conectar al escritorio remoto.
VMware View USB	Automático	Proporciona servicios para la función de redireccionamiento USB.

Servicios instalados en el cliente de Windows

La operación de Horizon Client depende de varios servicios de Windows.

Tabla 2-2. Servicios de Horizon Client

Nombre del servicio	Tipo de inicio	Descripción
VMware Horizon Client	Automático	Proporciona servicios de Horizon Client.
Servicio de supervisor de VMware Netlink	Automático	Para admitir la función de redireccionamiento de escáner y la función de redireccionamiento del puerto serie, proporciona servicios de supervisión para transferir información entre los procesos de espacio de usuarios y kernel.
Servicio de cliente de redireccionamiento del escáner de VMware	Automático	(Horizon Client 3.2 y versiones posteriores) Proporciona servicios para la función de redireccionamiento del escáner.
Servicio de cliente de comunicaciones serie de VMware	Automático	(Horizon Client 3.4 y versiones posteriores) Proporciona servicios para la función de redireccionamiento del puerto serie.
Servicio de arbitraje USB de VMware	Automático	Enumera los diversos dispositivos USB conectados al cliente y determina qué dispositivos conectar al cliente y cuáles conectar al escritorio remoto.
VMware View USB	Automático	Proporciona servicios para la función de redireccionamiento USB. **NOTA:** En Horizon Client 4.4 y versiones posteriores, este servicio se elimina y el servicio USBD se envía al proceso `vmware-remotemks.exe`.

Demonios instalados en otros clientes y en el escritorio Linux

Por motivos de seguridad, es importante saber si Horizon Client ha instalado demonios o procesos.

Tabla 2-3. Servicios, procesos o demonios instalados por Horizon Client ordenados por Tipo de cliente

Tipo	Servicio, proceso o demonio
Cliente Linux	■ `vmware-usbarbitrator`, que numera los diversos dispositivos USB conectados al cliente y determina qué dispositivos conectar al cliente y cuáles conectar al escritorio remoto. ■ `vmware-view-used`, que proporciona servicios para la función de redireccionamiento USB. **NOTA:** Estos demonios se inician de forma automática si, durante la instalación, hace clic en la casilla **Registrar e iniciar los servicios tras la instalación**. Estos procesos se ejecutan como raíz.
Cliente Mac	Horizon Client no crea ningún demonio.

Tabla 2-3. Servicios, procesos o demonios instalados por Horizon Client ordenados por Tipo de cliente (Continua)

Tipo	Servicio, proceso o demonio
Cliente Chrome	Horizon Client se ejecuta en un proceso de Android. Horizon Client no crea ningún demonio.
Cliente iOS	Horizon Client no crea ningún demonio.
Cliente Android	Horizon Client se ejecuta en un proceso de Android. Horizon Client no crea ningún demonio.
Cliente de la Tienda Windows	Horizon Client no crea ni activa ningún servicio de sistema.
Escritorio Linux	■ `StandaloneAgent`, que se ejecuta con privilegios de raíz y se inicia cuando el sistema Linux está listo y en funcionamiento. `StandaloneAgent` se comunica con el servidor de conexión de Horizon para realizar la administración de sesiones de escritorios remotos (establece y anula la sesión, actualizando el estado del escritorio remoto al agente en el servidor de conexión). ■ `VMwareBlastServer`, que inicia `StandaloneAgent` cuando el servidor de conexión recibe una solicitud `StartSession`. El demonio `VMwareBlastServer` se ejecuta con privilegio `vmwblast` (una cuenta de sistema creada al instalar Linux Agent) . Se comunica con `StandaloneAgent` a través de un canal `MKSControl` interno y con Horizon Client mediante el protocolo Blast.

Recursos a proteger 3

Entre estos recursos se incluyen los archivos de configuración relevantes, las contraseñas y los controles de acceso.

Este capítulo cubre los siguientes temas:

Implementar procedimientos recomendados para proteger sistemas de cliente

Implemente estos procedimientos recomendados para proteger sistemas cliente.

- Asegúrese de que los sistemas de cliente estén configurados para entrar en suspensión tras un período de inactividad y que los usuarios deban introducir una contraseña para que el equipo se reactive.
- Exija a los usuarios que escriban un nombre de usuario y una contraseña al iniciar sistemas de cliente. No configure los sistemas de cliente de modo que permitan inicios de sesión automáticos.
- Para los sistemas de cliente Mac, considere establecer otras contraseñas para la cuenta de usuario y el llavero. Si las contraseñas son distintas, se pregunta a los usuarios antes de que el sistema introduzca en su nombre una contraseña. Asimismo, debería considerar el activar la protección FileVault.

Ubicaciones de archivos de configuración

Los recursos que requieren protección incluyen archivos de configuración relativos a la seguridad.

Tabla 3-1. Ubicación de archivos de configuración por tipo de cliente

Tipo	Ruta de acceso del directorio
Cliente Linux	Cuando se inicia Horizon Client, las opciones de configuración se procesan desde varias ubicaciones en el siguiente orden: 1 `/etc/vmware/view-default-config` 2 `~/.vmware/view-preferences` 3 `/etc/vmware/view-mandatory-config` Si una opción se define en varias ubicaciones, el valor que se utiliza es el que se obtiene de la última lectura de la opción de línea de comandos o del archivo.
Cliente de Windows	La configuración de usuario que puede incluir algo de información privada se encuentra en el siguiente archivo: `C:\Usuarios\`*`nombre-de-usuario`*`\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt`

Tabla 3-1. Ubicación de archivos de configuración por tipo de cliente (Continua)

Tipo	Ruta de acceso del directorio
Cliente Mac	Algunos archivos de configuración generados tras el arranque del cliente Mac. ■ `$HOME/Library/Preferences/com.vmware.horizon.plist` ■ `$HOME/Library/Preferences/com.vmware.vmrc.plist` ■ `$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist` ■ `/Library/Preferences/com.vmware.horizon.plist`
Cliente Chrome	La configuración de seguridad aparece en la interfaz de usuario en lugar de en archivos de configuración. No hay archivos de configuración visibles para ningún usuario.
Cliente iOS	La configuración de seguridad aparece en la interfaz de usuario en lugar de en archivos de configuración. No hay archivos de configuración visibles para ningún usuario.
Cliente Android	La configuración de seguridad aparece en la interfaz de usuario en lugar de en archivos de configuración. No hay archivos de configuración visibles para ningún usuario.
Cliente de la Tienda Windows	La configuración de seguridad aparece en la interfaz de usuario en lugar de en archivos de configuración. No hay archivos de configuración visibles para ningún usuario.
View Agent o Horizon Agent (escritorio remoto con sistema operativo Windows)	La configuración de seguridad solo aparece en el Registro de Windows.
Escritorio Linux	Puede utilizar un editor de texto para abrir el siguiente archivo de configuración y especificar la configuración de SSL. `/etc/vmware/viewagent-custom.conf`

Cuentas

Los usuarios cliente deben tener cuentas en Active Directory.

Cuentas de usuario de Horizon Client

Configure en Active Directory las cuentas de los usuarios que tengan acceso a las aplicaciones y a los escritorios remotos. Las cuentas de usuario deben ser miembros del grupo Usuarios de escritorios remotos si pretende utilizar el protocolo RDP.

Por lo general, los usuarios finales no deben ser administradores de Horizon. Si un administrador de Horizon necesita verificar la experiencia del usuario, cree y autorice una cuenta de prueba independiente. En el escritorio, los usuarios finales de Horizon no deben ser miembros de grupos con privilegios, como es el caso del grupo Administradores, ya que, de serlo, podrían modificar archivos de configuración bloqueados y el Registro de Windows.

Cuentas de sistema creadas durante la instalación

La aplicación Horizon Client no crea ninguna cuenta de usuario de servicio en ningún tipo de cliente. Para los servicios creados por Horizon Client para Windows, el ID de inicio de sesión es Sistema local.

En el primer inicio en un cliente Mac el usuario debe conceder privilegios de acceso de administrador local para iniciar los servicios de Virtual Printing (ThinPrint) y USB. Una vez que se hayan iniciado por primera vez estos servicios, el usuario estándar tendrá privilegios de ejecución sobre ellos. De forma similar, en el cliente Linux, los demonios `vmware-usbarbitrator` y `vmware-view-used` se inician automáticamente si hace clic en la casilla **Registrar e iniciar los servicios tras la instalación** durante la instalación. Estos procesos se ejecutan como raíz.

Ni View Agent ni Horizon Agent crean cuentas de usuarios de servicios en escritorios de Windows. En los escritorios de Linux se crea una cuenta de sistema denominada `vmwblast`. En los escritorios de Linux el demonio `StandaloneAgent` se ejecuta con privilegios de raíz y el demonio `VmwareBlastServer` se ejecuta con privilegios `vmwblast`.

Configuración de seguridad para el cliente y el agente

4

Hay disponibles varias configuraciones de cliente y agente para ajustar la seguridad de la configuración. Puede acceder a la configuración del escritorio remoto y los clientes de Windows utilizando objetos de directiva de grupo o editando la configuración del Registro de Windows.

Para obtener información sobre los parámetros relacionados con la recopilación de registros, consulte Capítulo 6, "Ubicaciones de archivos de registros de clientes y agente," página 49. Para obtener información sobre los parámetros relacionados con protocolos de seguridad y conjuntos de claves de cifrado, consulte Capítulo 5, "Configurar protocolos de seguridad y conjuntos de claves de cifrado," página 39.

Este capítulo cubre los siguientes temas:

Configurar la comprobación del certificado

Los administradores pueden configurar el modo de verificación del certificado para que, por ejemplo, siempre se realice una verificación completa. Los administradores también pueden configurar si los usuarios finales pueden elegir si las conexiones de cliente se rechazan en caso de que se produzca un error en una o varias comprobaciones de los certificados del servidor.

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

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

La verificación de los certificados incluye las siguientes comprobaciones:

- ¿Se revocó el certificado?
- ¿El certificado persigue otro objetivo que no sea verificar la identidad del remitente y el cifrado de las comunicaciones del servidor? Es decir, ¿es el tipo de certificado correcto?
- ¿Expiró el certificado o solo será válido en el futuro? Es decir, ¿el certificado es válido según el reloj del equipo?
- ¿El nombre común del certificado coincide con el nombre de host del servidor que lo envía? Se produce un error de coincidencia cuando un equilibrador de carga redirecciona Horizon Client a un servidor que tiene un certificado que no coincide con el nombre de host introducido en Horizon Client. También puede producirse un error de coincidencia si introduce una dirección IP distinta al nombre de host en el cliente.
- ¿El certificado está firmado por una entidad de certificación desconocida o que no es de confianza? Los certificados autofirmados no son certificados de confianza.

  Para superar esta comprobación, la cadena de confianza del certificado debe especificar la raíz en el almacén de certificados local del dispositivo.

Si desea obtener información sobre cómo configurar la comprobación de certificados en un tipo de cliente específico, consulte el documento *Uso de VMware Horizon Client* para el tipo específico de cliente. Los documentos están disponibles en la página de documentación de Horizon Client en https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html. Estos documentos también contienen información sobre el uso de certificados autofirmados.

Configuración de seguridad de la plantilla de configuración de Horizon Agent

La configuración de seguridad se proporciona en archivos de plantilla ADMX para Horizon Agent. Los archivos de plantilla ADMX se denominan `vdm_agent.admx`. Salvo que se indique lo contrario, los parámetros solo incluyen un parámetro de configuración de equipo.

La configuración de seguridad se guarda en el registro de la máquina invitada bajo `HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration`.

Tabla 4-1. La configuración de seguridad de la plantilla de configuración de View Agent (para Horizon 6) o Horizon Agent (para Horizon 7)

Ajuste	Descripción
`AllowDirectRDP`	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. 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`. De forma predeterminada, mientras un usuario tenga la sesión iniciada en la sesión del escritorio de Horizon 7, puede usar RDP para conectarse a la máquina virtual desde fuera de Horizon 7. La conexión RDP finaliza la sesión del escritorio de Horizon 7 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`. **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. Esta configuración está habilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `AllowDirectRDP`.
`AllowSingleSignon`	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. Esta configuración está habilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `AllowSingleSignon`.
`CommandsToRunOnConnect`	Especifica una lista de comandos o scripts de comandos que se ejecutarán al conectar una sesión por primera vez. No se especifica ninguna lista de forma predeterminada. El valor equivalente en el Registro de Windows es `CommandsToRunOnConnect`.
`CommandsToRunOnDisconnect`	Especifica una lista de comandos o scripts de comandos que se ejecutarán al desconectar una sesión. No se especifica ninguna lista de forma predeterminada. El valor equivalente en el Registro de Windows es `CommandsToRunOnReconnect`.
`CommandsToRunOnReconnect`	Especifica una lista de comandos o scripts de comandos que se ejecutarán al volver a conectar una sesión después de una desconexión. No se especifica ninguna lista de forma predeterminada. El valor equivalente en el Registro de Windows es `CommandsToRunOnDisconnect`.

Tabla 4-1. La configuración de seguridad de la plantilla de configuración de View Agent (para Horizon 6) o Horizon Agent (para Horizon 7) (Continua)

Ajuste	Descripción
`ConnectionTicketTimeout`	Especifica la cantidad de tiempo en segundos durante los que es válido el ticket de conexión de Horizon. 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. El valor equivalente en el Registro de Windows es `VdmConnectionTicketTimeout`.
`CredentialFilterExceptions`	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. No se especifica ninguna lista de forma predeterminada. El valor equivalente en el Registro de Windows es `CredentialFilterExceptions`.

Para obtener más información sobre estas opciones y sus implicaciones de seguridad, consulte el documento *Administración de View*.

Opciones de configuración en los archivos de configuración de un escritorio Linux

Puede configurar determinadas opciones agregando entradas a los archivos `/etc/vmware/config` o `/etc/vmware/viewagent-custom.conf`.

Durante la instalación de View Agent o Horizon Agent, el instalador copia dos archivos de plantilla de configuración, `config.template` y `viewagent-custom.conf.template`, en `/etc/vmware`. Además, si los archivos `/etc/vmware/config` y `/etc/vmware/viewagent-custom.conf` no existen, el instalador copia `config.template` en `config` y `viewagent-custom.conf.template` en `viewagent-custom.conf`. En los archivos de plantilla, se enumeran y documentan todas las opciones de configuración. Para establecer una opción, tan solo tiene que eliminar el comentario y cambiar el valor según corresponda.

Después de hacer cambios de configuración, reinicie Linux para que los cambios surtan efecto.

Opciones de configuración en /etc/vmware/config

VMwareBlastServer y sus complementos asociados utilizan el archivo de configuración `/etc/vmware/config`.

NOTA: La siguiente tabla incluye la descripción de cada opción de directiva aplicada por el agente para las conexiones USB en el archivo de configuración de Horizon Agent. Horizon Agent usa la configuración para decidir si un USB se puede reenviar al equipo del host. Horizon Agent también envía la configuración a Horizon Client para su interpretación y su aplicación en función de si desea especificar el modificador merge**(m)** para aplicar la opción de la directiva de filtro de Horizon Agent, además de la opción de directiva de filtro de Horizon Client o el modificador override**(o)** para usar la opción de la directiva de filtro de Horizon Agent en lugar de la opción de la directiva de filtro de Horizon Client.

Tabla 4-2. Opciones de configuración en `/etc/vmware/config`

Opción	Valor/Formato	Predeterminado	Descripción
VVC.ScRedir.Enable	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar el redireccionamiento de tarjetas inteligentes.
VVC.logLevel	`fatal` `error`, `warn`, `info`, `debug` o `trace`	`info`	Utilice esta opción para establecer el nivel de registro del nodo proxy VVC.
VVC.RTAV.Enable	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar la entrada de audio.
Clipboard.Direction	`0, 1, 2,` o `3`	`2`	Esta opción determina la directiva de redireccionamiento del portapapeles. ■ 0 - Deshabilitar el redireccionamiento del portapapeles. ■ 1 - Habilitar el redireccionamiento del portapapeles en ambas direcciones. ■ 2 -Habilitar el redireccionamiento del portapapeles solo de cliente a escritorio remoto. ■ 3 - Habilitar el redireccionamiento del portapapeles solo de escritorio remoto a cliente.
cdrserver.logLevel	`error`, `warn`, `info`, `debug`, `trace`o `verbose`	`info`	Utilice esta opción para establecer el nivel de registro para `vmware-CDRserver.log`
cdrserver.forcedByAdmin	`true` o `false`	`false`	Establezca esta opción para permitir o no que el cliente comparta otras carpetas que no se especifican con la opción `cdrserver.shareFolders`.
cdrserver.sharedFolders	***ruta_archivo1*`,R;`*ruta-archivo2*`,;`*ruta_archivo3*`,R; ...`**	no definida	Especifique una o varias rutas a las carpetas que el cliente pueda compartir con el escritorio Linux. Por ejemplo: ■ para un cliente Windows: **`C:\spreadsheets,;D:\ebooks,R`** ■ para un cliente que no sea Windows:**`/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R`**

Tabla 4-2. Opciones de configuración en `/etc/vmware/config` (Continua)

Opción	Valor/Formato	Predeterminado	Descripción
cdrserver.permissions	`R`	`RW`	Utilice esta opción para aplicar los permisos de lectura o de escritura que Horizon Agent tenga en las carpetas que comparte Horizon Client. Por ejemplo: ■ Si la carpeta que comparte Horizon Client tiene los permisos `read` y `write` y establece **`cdrserver.permissions=R`**, entonces Horizon Agent solo tiene permisos `read` de acceso. ■ Si la carpeta que comparte Horizon Client solo tiene permisos `read` y establece **`cdrserver.permissions=RW`**, Horizon Agent sigue teniendo derechos `read` de acceso únicamente. Horizon Agent no puede cambiar el atributo solo `read` que estableció Horizon Client. Lo único que Horizon Agent puede hacer es eliminar los derechos de acceso de escritura. Los usos más habituales son: ■ **`cdrserver.permissions=R`** ■ **`#cdrserver.permissions=R`** (por ejemplo, puede agregar un comentario o eliminar la entrada)
cdrserver.cacheEnable	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar la función de caché de escritura en el agente a través del lado del cliente.
UsbRedirPlugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace` o `verbose`	`info`	Utilice esta opción para establecer el nivel de registro del complemento Redireccionamiento USB.
UsbRedirServer.log.logLevel	`error`, `warn`, `info`, `debug`, `trace` o `verbose`	`info`	Utilice esta opción para establecer el nivel de registro del servidor Redireccionamiento USB.
viewusb.AllowAutoDeviceSplitting	**`{m|o}: {true|false}`**	no definida, lo que es igual a `false`	Establezca esta opción para permitir o no la división de un dispositivo USB compuesto. Ejemplo: **`m:true`**
viewusb.SplitExcludeVidPid	**`{m|o}:vid–`*`xxx1`*`_pid–`*`yyy1`*`[;vid–`*`xxx2`*`_pid–`*`yyy2`*`;...]`**	no definida	Utilice esta opción para incluir un dispositivo USB compuesto y especificado en la división por ID de producto o de proveedor, o bien para excluirlo. El formato de la configuración es **`vid–`*`xxx1`*`_pid–`*`yyy1`*`[;vid–`*`xxx2`*`_pid–`*`yyy2`*`;...]`**. Debe especificar los números del ID en formato hexadecimal. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID. Ejemplo: **`m:vid–0f0f_pid–55**`**

Tabla 4-2. Opciones de configuración en `/etc/vmware/config` (Continua)

Opción	Valor/Formato	Predeterminado	Descripción
viewusb.SplitVidPid	**{m|o}: vid-*xxxx*_pid-*yyyy*([exintf:*zz*[;exintf:*ww*]])[;...]**	no definida	Establezca esta opción para tratar los componentes de un dispositivo USB compuesto y especificado según los ID del producto y del proveedor como dispositivos independientes. El formato de la opción es **vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*])** Puede usar la palabra clave **exintf** para excluir componentes del redireccionamiento al especificar el número de interfaz. Debe especificar números ID de forma hexadecimal. Además, los números de interfaz en decimales deben incluir un cero a la izquierda. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID. Ejemplo: **o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)** **NOTA:** Horizon no incluye automáticamente los componentes que no ha excluido explícitamente. Debe especificar una directiva de filtrado, como **Incluir dispositivo VidPid** para incluir estos componentes.
viewusb.AllowAudioIn	**{m|o}: {true|false}**	no definida, lo que es igual a `true`	Utilice esta opción para permitir o no el redireccionamiento de dispositivos de entrada de audio. Ejemplo: **o:false**
viewusb.AllowAudioOut	**{m|o}: {true|false}**	no definida, lo que es igual a `false`	Establezca esta opción para permitir o no el redireccionamiento de dispositivos de salida de audio.
viewusb.AllowHIDBootable	**{m|o}: {true|false}**	no definida, lo que es igual a `true`	Utilice esta opción para permitir o no el redireccionamiento de los dispositivos de entrada que no sean los dispositivos de teclado o de mouse disponibles en el momento de arranque, también conocidos como dispositivos con arranque HID.
viewusb.AllowDevDescFailsafe	**{m|o}: {true|false}**	no definida, lo que es igual a `false`	Establezca esta opción para permitir o no que se redireccionen los dispositivos, aunque Horizon Client no pueda obtener la configuración o los descriptores del dispositivo. Para admitir un dispositivo, aunque no se pueda obtener su configuración o sus descriptores, inclúyalo en los filtros de inclusión como **IncludeVidPid** o **IncludePath**.
viewusb.AllowKeyboardMouse	**{m|o}: {true|false}**	no definida, lo que es igual a `false`	Utilice esta opción para permitir o no el redireccionamiento de teclados con dispositivos de señalización (como un mouse, una bola de seguimiento o un panel táctil).
viewusb.AllowSmartcard	**{m|o}: {true|false}**	no definida, lo que es igual a `false`	Utilice esta opción para permitir o no el redireccionamiento de dispositivos de tarjetas inteligentes.
viewusb.AllowVideo	**{m|o}: {true|false}**	no definida, lo que es igual a `true`	Use esta opción para permitir o no el redireccionamiento de dispositivos de vídeo.

Tabla 4-2. Opciones de configuración en `/etc/vmware/config` (Continua)

Opción	Valor/Formato	Predeterminado	Descripción
viewusb.DisableRemoteConfig	**{m|o}: {true|false}**	no definida, lo que es igual a `false`	Establezca esta opción para habilitar o deshabilitar el uso de la configuración de Horizon Agent cuando realice el filtrado de dispositivos USB.
viewusb.ExcludeAllDevices	**{true|false}**	no definida, lo que es igual a `false`	Utilice esta opción para excluir o incluir el redireccionamiento de todos los dispositivos USB. Si está configurado como **true**, puede usar otras opciones de directivas para permitir el redireccionamiento de dispositivos o familias de dispositivos específicas. Si está configurado como **false**, puede usar otras opciones de directivas para evitar el redireccionamiento de dispositivos o familias de dispositivos específicas. Si establece el valor de **ExcludeAllDevices** en **true** en Horizon Agent y se envía esta configuración a Horizon Client, la configuración del agente sustituye a la de Horizon Client.
viewusb.ExcludeFamily	**{m|o}:*nombre_familia_1*[;nombre_familia_2;...]**	no definida	Use esta opción para excluir el redireccionamiento de familias de dispositivos. Por ejemplo: **m:bluetooth;smart-card** Si habilitó la división automática de dispositivo, Horizon examinará la familia de dispositivos de cada interfaz de un dispositivo USB compuesto para decidir cuál debe excluir. Si deshabilitó la división automática del dispositivo, Horizon examinará la familia del dispositivo de todo el dispositivo USB compuesto. **NOTA:** Sin embargo, el teclado y el mouse se excluyen del redireccionamiento de forma predeterminada y no es necesario excluirlos mediante esta opción.
viewusb.ExcludeVidPid	**{m|o}:vid-*xxx1*_ pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;..]**	no definida	Establezca esta opción para excluir el redireccionamiento de dispositivos con los ID de producto y de proveedor especificados. 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- ****;vid-0561_pid-554c**
viewusb.ExcludePath	**{m|o}:bus-*x1*[/*y1*].../port-*z1*[;bus-*x2*[/*y2*].../port-*z2*;...]**	no definida	Utilice esta opción para excluir el redireccionamiento de dispositivos de rutas de puertos o de un concentrador específicos. Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta. Por ejemplo: **m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff**
viewusb.IncludeFamily	**{m|o}:*nombre_familia_1*[;*nombre_familia_2*]...**	no definida	Establezca esta opción para incluir familias de dispositivos que se pueden redireccionar. Por ejemplo: **o:storage; smart-card**

Tabla 4-2. Opciones de configuración en `/etc/vmware/config` (Continua)

Opción	Valor/Formato	Predeterminado	Descripción
viewusb.IncludePath	**{m|o}:bus-*x1*[/*y1*].../port-*z1*[;bus-*x2*[/*y2*].../portz2;...]**	no definida	Utilice esta opción para incluir el redireccionamiento de dispositivos en rutas de puertos o en un concentrador específicos. Debe especificar los números de puerto y bus en hexadecimal. No puede usar el carácter comodín en la ruta. Por ejemplo: **m:bus-1/2_port- 02;bus-1/7/1/4_port-0**f
viewusb.IncludeVidPid	**{m|o}:vid-*xxx1*_ pid-*yyy1*[;vid-*xxx2*_pid-*yyy2;...*]**	no definida	Establezca esta opción para incluir el redireccionamiento de dispositivos con los ID de producto y de proveedor especificados. Debe especificar los números ID en hexadecimales. Puede utilizar el carácter comodín (*) en lugar de dígitos individuales en un ID. Por ejemplo: **o:vid-***_pid-0001;vid-0561_pid-554c**
mksVNCServer.useXExtButton Mapping	`true` o `false`	`false`	Establezca esta opción para habilitar o deshabilitar la compatibilidad con un ratón para zurdos en SLED 11 SP3.
mksvhan.clipboardSize	Un número entero	1024	Utilice esta opción para especificar el tamaño máximo del portapapeles para copiar y pegar.
RemoteDisplay.maxBandwidth Kbps	Un número entero	4096000	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 y el canal virtual. El valor máximo es de 4 Gbps (4096000).
RemoteDisplay.maxFPS	Un número entero	60	Especifica la velocidad máxima de actualizaciones de pantalla. Utilice esta opción para administrar el ancho de banda medio que consumen los usuarios. Un valor válido debería ser de entre 3 y 60. El valor predeterminado es de 60 actualizaciones por segundo.
RemoteDisplay.enableStats	`true` o `false`	`false`	Habilite o deshabilite las estadísticas de protocolo Blast en el registro de mks, como ancho de banda, FPS, RTT, etc.
RemoteDisplay.allowH264	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar la codificación H.264.
vdpservice.log.logLevel	`fatal` `error`, `warn`, `info`, `debug` o `trace`	`info`	Utilice esta opción para establecer el nivel de registro del vdpservice.
RemoteDisplay.qpmaxH264	rango disponible de valores: 0-51	36	Use esta opción para establecer el parámetro de cuantificación de H264minQP, que especifica la mejor calidad de imagen para la pantalla remota configurada para utilizar la codificación H.264. Establezca el valor en un valor superior al establecido para RemoteDisplay.qpminH264.
RemoteDisplay.qpminH264	rango disponible de valores: 0-51	10	Use esta opción para establecer el parámetro de cuantificación de H264maxQP, que especifica la calidad de imagen más baja para la pantalla remota configurada para utilizar la codificación H. 264. Establezca el valor en un valor inferior al establecido para RemoteDisplay.qpmaxH264.

Tabla 4-2. Opciones de configuración en `/etc/vmware/config` (Continua)

Opción	Valor/Formato	Predeterminado	Descripción
RemoteDisplay.minQualityJPEG	rango disponible de valores: 1-100	25	Especifica la calidad de imagen de la pantalla del escritorio para la codificación JPEG/PNG. 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.
RemoteDisplay.midQualityJPEG	rango disponible de valores: 1-100	35	Especifica la calidad de imagen de la pantalla del escritorio para la codificación JPEG/PNG. Utilice esta opción para establecer las opciones de calidad media de la pantalla del escritorio.
RemoteDisplay.maxQualityJPEG	rango disponible de valores: 1-100	90	Especifica la calidad de imagen de la pantalla del escritorio para la codificación JPEG/PNG. Las opciones de alta calidad se proporcionan para las áreas más estáticas de la pantalla, lo que ofrece una mejor calidad de la imagen.

Opciones de configuración en /etc/vmware/viewagent-custom.conf

Java Standalone Agent utiliza el archivo de configuración `/etc/vmware/viewagent-custom.conf`.

Tabla 4-3. Opciones de configuración en `/etc/vmware/viewagent-custom.conf`

Opción	Valor	Predeterminado	Descripción
Subred	`NULL` o dirección de red y máscara en formato de dirección IP/CIDR	`NULL`	Si hay varias direcciones IP locales con diferentes subredes, utilice esta opción para establecer la subred que proporciona Linux Agent al servidor de conexión de View. Cuando se detectan varias configuraciones de subred en una máquina Linux Agent, esta opción se requiere para especificar la subred correcta que debe utilizar el Linux Agent. Por ejemplo, si instaló Docker en la máquina Linux, será introducido como un adaptador de red virtual. Para evitar que Linux Agent utilice Docker como adaptador de red virtual, debe establecer esta opción para que utilice el adaptador de red física real. Debe especificar el valor en formato de dirección IP/CIDR. Por ejemplo, Subred=192.168.1.0/24. NULL implica que Linux Agent selecciona la dirección IP de forma aleatoria.
SSOEnable	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar Single Sign-On (SSO).
SSOUserFormat	Una cadena de texto	[nombredeusuario]	Utilice esta opción para especificar el formato del nombre de inicio de sesión para Single Sign-On. El valor predeterminado es el nombre del usuario solamente. Establezca esta opción si también se requiere el nombre del dominio. Por lo general, el nombre de inicio de sesión es el nombre de dominio más un carácter especial seguido por el nombre de usuario. Si el carácter especial es la barra diagonal inversa, debe escapar con otra barra diagonal inversa. Ejemplos de formatos de nombre de inicio de sesión: ■ SSOUserFormat=[dominio]\\[nombredeusuario] ■ SSOUserFormat=[dominio]+[nombredeusuario] ■ SSOUserFormat=[nombredeusuario]@[dominio]

Tabla 4-3. Opciones de configuración en `/etc/vmware/viewagent-custom.conf` (Continua)

Opción	Valor	Predeterminado	Descripción
CDREnable	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar la función Redireccionamiento de unidades cliente (CDR).
USBEnable	`true` o `false`	`true`	Establezca esta opción para habilitar o deshabilitar la función Redireccionamiento USB.
KeyboardLayoutSync	`true` o `false`	`true`	Utilice esta opción para especificar si desea sincronizar una lista de configuración regional del sistema del cliente y la distribución del teclado con Horizon Agent para escritorios Linux. Cuando esta opción está habilitada o no está configurada, se permite la sincronización. Cuando esta opción está deshabilitada, no se permite la sincronización. Esta función solo es compatible con Horizon Client para Windows y para las siguientes configuraciones regionales: alemán, chino simplificado, chino tradicional, coreano, español, francés, inglés y japonés.
StartBlastServerTimeout	Un número entero	20	Esta opción determina la cantidad de tiempo en segundos de que dispone el proceso VMwareBlastServer para su inicialización. Si el proceso no está listo antes de que finalice el tiempo de espera establecido, no se realizará el inicio de sesión del usuario.
SSLCiphers	Una cadena de texto	!aNULL:kECDH +AESGCM:ECDH +AESGCM:RSA +AESGCM:kECDH +AES:ECDH+AES:RSA +AES	Use esta opción para especificar la lista de cifrados. Debe utilizar el formato que se define en https://www.openssl.org/docs/manmaster/man1/ciphers.html.
SSLProtocols	Una cadena de texto	TLSv1_1:TLSv1_2	Use esta opción para especificar los protocolos de seguridad. Los protocolos compatibles son TLSv1.0, TLSv1.1 y TLSv1.2.
SSLCipherServerPreference	`true` o `false`	`true`	Use esta opción para habilitar o deshabilitar la opción SSL_OP_CIPHER_SERVER_PREFERENCE. Si desea obtener más información, consulte https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html.
UseGnomeFlashback	`true` o `false`	`false`	Esta opción determina si se debe usar el entorno de escritorio GNOME Flashback (Metacity) si se encuentra instalado en un sistema Ubuntu 14.04 o Ubuntu 16.04. Esta opción se aplica independientemente de si la función SSO está habilitada o no. Después de que esta opción se establezca como **`TRUE`**, el entorno de escritorio GNOME Flashback (Metacity) se utiliza siempre en lugar del entorno de escritorio predeterminado. **Tip** Para mejorar el rendimiento del sistema, establezca **`UseGnomeFlashback=TRUE`** después de instalar el escritorio GNOME Flashback (Metacity) en el sistema Ubuntu 14.04 o en el sistema Ubuntu 16.04.
LogCnt	Un número entero	-1	Use esta opción para establecer el número de archivos de registro que se conservan en `/tmp/vmware-root`. ■ -1: conservar todos ■ 0: eliminar todos ■ > 0: número de registros que se conservan.

Tabla 4-3. Opciones de configuración en `/etc/vmware/viewagent-custom.conf` (Continua)

Opción	Valor	Predeterminado	Descripción
RunOnceScript			Use esta opción para volver a unir la máquina virtual clonada a AD. Establezca la ejecución del script una vez que haya cambiado el nombre del host. El script especificado solo se ejecuta una vez después del primer cambio de nombre de host. El script se ejecuta como permiso de raíz cuando se inicia el servicio de agente y el nombre de host ha cambiado después de que se instalase el agente. Por ejemplo, para la solución winbind, debe unir la máquina virtual (VM) base a AD con winbind y establecer esta opción en una ruta de acceso de script. Esta debe contener el comando de unirse de nuevo al dominio `/usr/bin/net ads join –U <ADUserName> %<ADUserPassword>`. Tras la clonación de la VM, la personalización del sistema operativo cambia el nombre del host. Cuando se inicia el servicio de agente, se ejecuta el script para unir la VM clonada a AD.
RunOnceScriptTimeout		120	Utilice esta opción para establecer el tiempo de espera en segundos de la opción RunOnceScript. Por ejemplo, establezca `RunOnceScriptTimeout=120`

NOTA: Las tres opciones de seguridad, SSLCiphers, SSLProtocols y SSLCipherServerPreference, son para el proceso VMwareBlastServer. Cuando se inicia el proceso VMwareBlastServer, Java Standalone Agent pasa estas opciones como parámetros. Si está habilitada la puerta de enlace segura de Blast (BSG), estas opciones afectan a la conexión entre BSG y el escritorio Linux. Si BSG está deshabilitada, estas opciones afectan a la conexión entre el cliente y el escritorio Linux.

Configuración de directiva de grupo para HTML Access

La configuración de la directiva de grupo para HTML Access se especifica en los archivos de plantilla. El archivo de plantilla ADMX se denomina `vdm_blast.admx`. Las plantillas son para el protocolo de visualización VMware Blast, que es el único protocolo de visualización que utiliza HTML Access.

Para HTML Access 4.0 y Horizon 7.0, la configuración de la directiva de grupo de VMware Blast se describe en la sección "Configuración de la directiva de VMware Blast" del documento *Configurar funciones de escritorios remotos en Horizon 7*.

Si tiene HTML Access 3.5 o anterior y Horizon 6.2.x o anterior, la siguiente tabla describe la configuración de directiva de grupo que se aplica a HTML Access. En Horizon 7.0 o versiones posteriores, están disponibles más configuraciones de la directiva de grupo VMware Blast.

Tabla 4-4. Configuración de directiva de grupo para HTML Access 3.5 y versiones anteriores

Configuración	Descripción
Pantalla en blanco	Controla si la máquina virtual remota se puede ver desde fuera de Horizon 7 durante una sesión de HTML Access. Por ejemplo, un administrador podría usar vSphere Web Client para abrir una consola en la máquina virtual mientras un usuario esté conectado al escritorio a través de HTML Access. Si esta opción está habilitada o no está configurada y alguien intenta acceder a la máquina virtual remota desde fuera de Horizon 7 mientras hay una sesión de HTML Access activa, la máquina virtual remota muestra una pantalla en blanco.
Recopilación de elementos no utilizados de la sesión	Controla la recopilación de elementos no utilizados de las sesiones remotas abandonadas. Si esta opción está habilitada, puede configurar el intervalo y el umbral de recopilación de elementos no utilizados. El intervalo controla la frecuencia con la que se ejecuta el recopilador de elementos no utilizados. Este intervalo se define en milisegundos. El umbral determina cuánto tiempo debe pasar después de que se haya abandonado una sesión para que cumpla los requisitos para ser eliminada. El umbral se define en segundos.
Configurar el redireccionamiento del portapapeles	Determina la dirección en la que se permite el redireccionamiento del portapapeles. Solo se puede copiar y pegar texto. Puede seleccionar uno de estos valores: ■ **Habilitado solo de cliente a servidor** (Esto es, permitir el copiado y el pegado solo desde el sistema de cliente al escritorio remoto). ■ **Deshabilitado en ambas direcciones** ■ **Habilitado en ambas direcciones** ■ **Habilitado solo de servidor a cliente** (Esto es, permitir el copiado y el pegado solo desde el escritorio remoto al sistema de cliente). Esta opción solo se aplica a View Agent o Horizon Agent. Si esta opción está deshabilitada o no configurada, el valor predeterminado es **Habilitado solo de cliente a servidor**.
Servicio HTTP	Le permite cambia el puerto TCP seguro (HTTPS) por el servicio de Blast Agent. El puerto predeterminado es 22443. Habilite esta opción para cambiar el número de puerto. Si cambia esta opción, también debe actualizar la configuración en el firewall de los escritorios remotos afectados (donde esté instalado View Agent o Horizon Agent).

Configuración de seguridad en las plantillas de configuración de Horizon Client

Se proporcionan opciones de seguridad en la sección Seguridad y en la sección Definiciones de scripting de los archivos de plantilla ADMX para Horizon Client. El archivo de plantilla ADMX se denomina `vdm_client.admx`. Salvo que se indique lo contrario, los parámetros solo incluyen un parámetro de configuración de equipo. Si hay disponible una opción de Configuración de usuario y define un valor para ella, invalida la opción equivalente Configuración del equipo.

En la siguiente tabla se describen las opciones de la sección Seguridad de los archivos de plantilla ADMX.

Tabla 4-5. Plantilla de configuración de Horizon Client : configuración de seguridad

Ajuste	Descripción
`Allow command line credentials` (Parámetro de configuración de equipos)	Determina si se pueden proporcionar credenciales de usuario con opciones de línea de comandos de Horizon Client. Si esta configuración está deshabilitada, las opciones `smartCardPIN` y `password` no estarán disponibles cuando los usuarios ejecuten Horizon Client desde la línea de comandos. Esta configuración está habilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `AllowCmdLineCredentials`.
`Servers Trusted For Delegation` (Parámetro de configuración de equipos)	Especifica las instancias del servidor de conexión que aceptan la información de credencial e identidad de usuario que se transmite cuando un usuario selecciona la casilla de verificación **Iniciar sesión como usuario actual**. Si no especifica ninguna instancia del servidor de conexión, todas ellas aceptan esta información. Para agregar una instancia del servidor de conexión, use uno de los siguientes formatos: ■ **`dominio\sistema$`** ■ **`sistema$@dominio.com`** ■ El nombre de entidad de seguridad de servicio (SPN) del servicio del servidor de conexión. El valor equivalente en el Registro de Windows es `BrokersTrustedForDelegation`.
`Certificate verification mode` (Parámetro de configuración de equipos)	Configura el nivel de comprobación de certificados que realiza Horizon Client. Puede seleccionar uno de estos modos: ■ `No Security`. Sin comprobación de certificados. ■ `Warn But Allow`. Se muestra una advertencia si el host del servidor de conexión presenta un certificado autofirmado, aunque el usuario podrá conectarse igualmente al servidor de conexión. El nombre del certificado no es necesario que coincida con el nombre del servidor de conexión proporcionado por el usuario en Horizon Client. Si se produce cualquier otra situación de error relacionada con certificados, se muestra un cuadro de diálogo de error y se impide al usuario conectarse al servidor de conexión. `Warn But Allow` es el valor predeterminado. ■ `Full Security`. Si se produce cualquier tipo de error relacionado con los certificados, el usuario no podrá conectarse al servidor de conexión. El usuario ve los errores de los certificados. Cuando se define esta configuración de directiva de grupo, los usuarios pueden consultar el modo de verificación de certificados seleccionado en Horizon Client, aunque no pueden configurarla. El cuadro de diálogo de configuración de SSL informa a los usuarios de que el administrador ha bloqueado la configuración. Cuando esta configuración no está definida o está deshabilitada, los usuarios de Horizon Client pueden seleccionar un modo de verificación de certificados. Si no desea configurar la verificación de certificados como una directiva de grupo, puede también habilitarla mediante la modificación de los valores del Registro de Windows.

Tabla 4-5. Plantilla de configuración de Horizon Client : configuración de seguridad (Continua)

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

Tabla 4-5. Plantilla de configuración de Horizon Client : configuración de seguridad (Continua)

Ajuste	Descripción
`Configures SSL protocols and cryptographic algorithms` (Parámetro de configuración de usuarios y equipos)	Configura la lista de cifrado para restringir el uso de ciertos protocolos y algoritmos criptográficos antes de establecer una conexión SSL cifrada. La lista de cifrado consta de una o más cadenas de cifrado separadas por dos puntos. **NOTA:** Todas las cadenas de cifrado distinguen mayúsculas y minúsculas. ■ El valor predeterminado de Horizon Client 4.2 y de las versiones posteriores es **!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH +AES:ECDH+AES:RSA+AES**. ■ El valor predeterminado de las versiones de Horizon Client 4.0.1 y 4.1 es **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA +AES:@STRENGTH**. ■ El valor predeterminado de Horizon Client 4.0 es **TLSv1.1:TLSv1.2:! aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**. ■ El valor predeterminado de Horizon Client 3.5 es **TLSv1:TLSv1.1:TLSv1.2:! aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**. ■ El valor predeterminado de Horizon Client 3.3 y 3.4 es **TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. ■ El valor de Horizon Client 3.2 y versiones anteriores es **SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. Esto significa que en Horizon Client 4.0.1 y 4.1, se han habilitado TLSv1.0, TLSv1.1 y TLSv1.2. (Se han eliminado SSL v2.0 y v3.0). Puede deshabilitar TLSv1.0 si no se requiere la compatibilidad de TLSv1.0 con el servidor. En Horizon Client 4.0, se han habilitado TLS v1.1 y TLS v1.2. (Se ha habilitado TLS v1.0. Se han eliminado SSL v2.0 y v3.0). En Horizon Client 3.5, se han habilitado TLS v1.0, TLS v1.1 y TLS v1.2. (Se han deshabilitado SSL v2.0 y v3.0). En Horizon Client 3.3 y 3.4, se han habilitado TLS v1.0 y TLS v1.1. (Se han deshabilitado SSL v2.0 y v3.0, y TLS v1.2). En Horizon Client 3.2 y versiones anteriores, se ha habilitado también SSL v3.0. (Se han deshabilitado SSL v2.0 y TLS v1.2). Los paquetes de cifrado usan AES de 128 o 256 bits, eliminan los algoritmos DH anónimos y, a continuación, ordenan la lista de cifrado actual de acuerdo con la longitud de la clave del algoritmo de cifrado. Vínculo de referencia para la configuración: http://www.openssl.org/docs/apps/ciphers.html El valor equivalente en el Registro de Windows es `SSLCipherList`. Si no desea configurar este parámetro como una directiva de grupo, también puede habilitarlo mediante la adición del nombre de valor `SSLCipherList` a una de las claves de registro siguiente en el equipo cliente: ■ Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware VDM\Client\Security` ■ Para Windows de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware,Inc.\VMware VDM\Client\Security`
`Enable Single Sign-On for smart card authentication` (Parámetro de configuración de equipos)	Determina si Single Sign-On está habilitado para la autenticación de tarjeta inteligente. Cuando Single Sign-On está habilitado, Horizon Client almacena el PIN de la tarjeta inteligente cifrada en una memoria temporal antes de enviarlo al servidor de conexión. Cuando está deshabilitado, Horizon Client no muestra un cuadro de diálogo de PIN deshabilitado. El valor equivalente en el Registro de Windows es `EnableSmartCardSSO`.
`Ignore bad SSL certificate date received from the server` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con fechas de certificado de servidor no válidas. Estos errores se producen cuando un servidor envía un certificado con una fecha ya pasada. El valor equivalente en el Registro de Windows es `IgnoreCertDateInvalid`.

Tabla 4-5. Plantilla de configuración de Horizon Client : configuración de seguridad (Continua)

Ajuste	Descripción
`Ignore certificate revocation problems` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con un certificado de servidor revocado. Estos errores se producen cuando el servidor envía un certificado que se ha revocado y cuando el cliente no puede verificar un estado de revocación de un certificado. Esta opción está deshabilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `IgnoreRevocation`.
`Ignore incorrect SSL certificate common name (host name field)` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con nombres comunes de certificado de servidor incorrectos. Estos errores se producen cuando el nombre común del certificado no coincide con el nombre de host del servidor que lo envía. El valor equivalente en el Registro de Windows es `IgnoreCertCnInvalid`.
`Ignore incorrect usage problems` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con el uso incorrecto de un certificado de servidor. Estos errores se producen cuando el servidor envía un certificado con un objetivo diferente al de verificar la identidad del remitente y cifrar las comunicaciones del servidor. El valor equivalente en el Registro de Windows es `IgnoreWrongUsage`.
`Ignore unknown certificate authority problems` (Parámetro de configuración de equipos)	(View 4.6 y versiones anteriores solamente) Determina si se ignoran los errores asociados con una entidad de certificación desconocida (CA) en el certificado de servidor. Estos errores se producen cuando el servidor envía un certificado firmado por una entidad de certificación que no es de confianza. El valor equivalente en el Registro de Windows es `IgnoreUnknownCa`.

En la siguiente tabla se describen las opciones de la sección Definiciones de scripting de los archivos de plantilla ADMX.

Tabla 4-6. Opciones de seguridad en la sección Definiciones de scripting

Ajuste	Descripción
`Connect all USB devices to the desktop on launch`	Determina si todos los dispositivos USB disponibles en el sistema cliente se conectan al escritorio al iniciarlo. Esta opción está deshabilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `connectUSBOnStartup`.
`Connect all USB devices to the desktop when they are plugged in`	Determina si los dispositivos USB se conectan al escritorio cuando se insertan en el sistema cliente. Esta opción está deshabilitada de forma predeterminada. El valor equivalente en el Registro de Windows es `connectUSBOnInsert`.
`Logon Password`	Especifica la contraseña que Horizon Client usa en el inicio de sesión. Active Directory almacena la contraseña en texto sin formato. Esta opción no está definida de forma predeterminada. El valor equivalente en el Registro de Windows es `Password`.

Para obtener más información sobre estas opciones y sus implicaciones de seguridad, consulte el documento *Uso de VMware Horizon Client para Windows*.

Configurar el modo de verificación del certificado de Horizon Client

Puede configurar el modo de verificación del certificado de Horizon Client agregando el nombre de valor `CertCheckMode` a una clave del registro en el equipo de cliente de Windows.

En los sistemas de Windows de 32 bits, la clave del registro es `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`. En los sistemas de Windows de 64 bits, la clave del registro es `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`.

Use uno de los siguientes valores en las claves del registro:

- `0`: implementa la opción **No comprobar los certificados de identidad de los servidores**.
- `1`: implementa la opción **Advertirme antes de conectarme a servidores que no sean de confianza**.
- `2`: implementa la opción **No conectarse nunca a servidores que no sean de confianza**.

También puede configurar el modo de verificación del certificado de Horizon Client mediante la configuración de directiva de grupo `Modo de verificación del certificado`. Si configura tanto la opción de la directiva de grupo como la de `CertCheckMode` en la clave de registro, la opción de la directiva de grupo tiene prioridad sobre el valor de la clave de registro.

Cuando se define la configuración de directiva de grupo o la configuración del registro, los usuarios pueden ver el modo de verificación de certificados seleccionado en Horizon Client, aunque no pueden configurarla.

Si desea obtener información sobre cómo definir la configuración de directiva de grupo `Modo de verificación del certificado`, consulte "Configuración de seguridad en las plantillas de configuración de Horizon Client," página 33.

Configurar la protección de autoridad de seguridad local

Horizon Client y Horizon Agent admiten la protección de autoridad de seguridad local (LSA). La protección de LSA impide que los usuarios con credenciales sin proteger puedan leer la memoria ni insertar códigos.

Para obtener más información sobre la configuración de la protección de LSA, consulte la documentación de Microsoft Windows Server.

Cuando se configura la protección de LSA para Horizon Client 4.4 y versiones anteriores, se produce un error en esta función:

- Iniciar sesión como usuario actual

Cuando se configura la protección de LSA para las versiones de Horizon Agent anteriores a la versión 7.2 de Horizon 7, se produce un error en estas funciones:

- Autenticación con tarjeta inteligente
- True SSO

Configurar protocolos de seguridad y conjuntos de claves de cifrado 5

Puede configurar los protocolos de seguridad y los conjuntos de cifrado que se acepten y propongan entre Horizon Client, View Agent/Horizon Agent y los componentes de servidor de View.

Este capítulo cubre los siguientes temas:

Directivas globales predeterminadas para los protocolos de seguridad y los conjuntos de claves de cifrado

Las directivas de propuesta y aceptación globales habilitan ciertos protocolos de seguridad y conjuntos de claves de cifrado de forma predeterminada.

En las siguientes tablas, se enumeran los protocolos y conjuntos de claves de cifrado que se habilitan de forma predeterminada para Horizon Client 4.4, 4.3, 4.2, 4.1, 4.0.1, 4.0 y 3.x en sistemas de cliente de Windows, Linux, Mac, iOS, Android y Chrome. En Horizon Client 3.1 (y versiones posteriores) para Windows, Linux y Mac, estos conjuntos de claves de cifrado y protocolos también se utilizan para cifrar el canal USB (la comunicación entre el demonio de servicios USB y View Agent o Horizon Agent). Para las versiones de Horizon Client anteriores a la 4.0, el demonio de servicios USB agrega `RC4 ( :RC4-SHA: +RC4 )` al final de la cadena de control de cifrado cuando se conecta a un escritorio remoto. RC4 dejó de agregarse desde Horizon Client 4.0.

Horizon Client 4.2

NOTA: No se produjo ningún cambio de Horizon Client 4.2 a Horizon Client 4.4.

Tabla 5-1. Protocolos de seguridad y conjuntos de claves de cifrado habilitados de forma predeterminada en Horizon Client 4.2

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

TLS 1.0 se habilita de forma predeterminada para garantizar que, de forma predeterminada, Horizon Client se pueda conectar a los servidores de VMware Horizon Air. La cadena de cifrado predeterminada es !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. Puede deshabilitar TLS 1.0 si no se requiere compatibilidad de TLS 1.0 con el servidor.

Horizon Client 4.0.1 y 4.1

Tabla 5-2. Protocolos de seguridad y conjuntos de claves de cifrado habilitados de forma predeterminada en Horizon Client 4.0.1 y 4.1

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

TLS 1.0 se habilita de forma predeterminada para garantizar que, de forma predeterminada, Horizon Client se pueda conectar a los servidores de VMware Horizon Air. La cadena de cifrado predeterminada es TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. Puede deshabilitar TLS 1.0 si no se requiere compatibilidad de TLS 1.0 con el servidor.

Horizon Client 4.0

Tabla 5-3. Protocolos de seguridad y conjuntos de claves de cifrado habilitados de forma predeterminada en Horizon Client 4.0

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

IMPORTANTE: TLS 1.0 se deshabilita de forma predeterminada. Se ha eliminado SSL 3.0.

Horizon Client 3.5

Tabla 5-4. Protocolos de seguridad y conjuntos de claves de cifrado habilitados de forma predeterminada en Horizon Client 3.5

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Horizon Client 3.3 y 3.4.

Tabla 5-5. Protocolos de seguridad y conjuntos de claves de cifrado habilitados de forma predeterminada en Horizon Client 3.3 y 3.4

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
■ `TLS 1.1` ■ `TLS 1.0`	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

NOTA: `TLS 1.2` también se admite, aunque no se habilita de forma predeterminada. Para habilitar `TLS 1.2`, siga las instrucciones proporcionadas en VMware KB 2121183, tras lo cual se admitirán los conjuntos de claves de cifrado enumerados en Tabla 5-4.

Horizon Client 3.0, 3.1 y 3.2

Tabla 5-6. Protocolos de seguridad y conjuntos de claves de cifrado habilitados de forma predeterminada en Horizon Client 3.0, 3.1 y 3.2

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
■ `TLS 1.1` ■ `TLS 1.0` ■ `SSL 3.0` (solo habilitado en clientes de Windows)	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022) ■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f) ■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

NOTA: `TLS 1.2` también se admite, aunque no se habilita de forma predeterminada. Para habilitar `TLS 1.2`, siga las instrucciones proporcionadas en VMware KB 2121183, tras lo cual se admitirán los conjuntos de claves de cifrado enumerados en Tabla 5-4.

Configurar protocolos de seguridad y conjuntos de claves de cifrado para tipos de cliente específicos

Cada tipo de cliente tiene su propio método para configurar los protocolos y conjuntos de claves de cifrado utilizados.

Solo debe cambiar los protocolos de seguridad en Horizon Client si su servidor de View no admite la configuración actual. Si configura un protocolo de seguridad para Horizon Client que no está habilitado en el servidor de View al que el cliente se conecta, se produce un error TLS/SSL y de conexión.

Para cambiar los valores predeterminados de los protocolos y cifrados, utilice el siguiente mecanismo de cliente específico:

- En los sistemas de cliente de Windows, puede utilizar una configuración de directiva de grupo o una configuración del Registro de Windows. Para obtener información, consulte el documento *Uso de VMware Horizon Client para Windows*.
- En los sistemas de cliente de Linux, puede utilizar las propiedades del archivo de configuración u opciones de la línea de comandos. Para obtener información, consulte el documento *Uso de VMware Horizon Client para Linux*.
- En los sistemas de cliente Mac, puede utilizar una configuración de Preferencias en Horizon Client. Para obtener información, consulte el documento *Uso de VMware Horizon Client para Mac*.
- En los sistemas de cliente de iOS, Android y Chrome OS, puede utilizar una configuración de Opciones SSL avanzadas en la configuración de Horizon Client. Para obtener información, consulte el documento aplicable: *Uso de VMware Horizon Client para iOS*, *Uso de VMware Horizon Client para Android* o *Uso de VMware Horizon Client para Chrome OS*.

Los documentos están disponibles en la página de documentación de Horizon Client en https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html.

Deshabilitar cifrados débiles en SSL/TLS

Para conseguir una mayor seguridad, puede configurar el objeto de directiva de grupo (GPO) de forma que los equipos basados en Windows que ejecutan View Agent o Horizon Agent no usen cifrados débiles cuando se comuniquen con el protocolo SSL/TLS.

Procedimiento

1. En el servidor de Active Directory, para editar el GPO seleccionando, seleccione **Inicio > Herramientas administrativas > Administración de directivas de grupo**, haga clic en el GPO y seleccione **Editar**.
2. En el Editor de administración de directivas de grupo, diríjase a **Configuración del equipo > Directivas > Plantillas administrativas > Red > Opciones de configuración SSL**.
3. Haga doble clic en **Orden de conjuntos de cifrado SSL**.
4. En la ventana Orden de conjuntos de cifrado SSL, haga clic en **Habilitado**.
5. En el panel Opciones, reemplace todo el contenido del cuadro de texto Conjunto de claves de cifrado SSL por la siguiente lista de cifrado:

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
```

```
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

Los conjuntos de claves de cifrado aparecen en la parte superior en líneas separadas para que se puedan leer con facilidad. Cuando copie la lista en el cuadro de texto, los conjuntos de claves de cifrado deben estar en una línea y sin espacios después de las comas.

6 Salga del Editor de administración de directivas de grupo.

7 Reinicie los equipos Horizon Agent o View Agent para que se aplique la nueva directiva de grupo.

Configurar protocolos de seguridad y conjuntos de claves de cifrado para agente HTML Access

Desde View Agent 6.2 puede configurar los conjuntos de claves de cifrado que utiliza HTML Access Agent mediante la edición del Registro de Windows. Desde View Agent 6.2.1 también puede configurar los protocolos de seguridad utilizados. También puede especificar las configuraciones en un objeto de directiva de grupo (GPO).

Con View Agent 6.2.1 y las versiones posteriores, de forma predeterminada, el HTML Access Agent solo utiliza TLS 1.1 y TLS 1.2. Los protocolos permitidos son, de más bajo a más alto, TLS 1.0, TLS 1.1 y TLS 1.2. Nunca se admiten protocolos más antiguos, como SSLv3 y versiones anteriores. Dos valores del registro, `SslProtocolLow` y `SslProtocolHigh`, determinan el rango de protocolos que aceptará el agente HTML Access. Por ejemplo, configurar `SslProtocolLow=tls_1.0` y `SslProtocolHigh=tls_1.2`, hará que el agente HTML Access acepte TLS 1.0, TLS 1.1 y TLS 1.2. Las opciones predeterminadas son `SslProtocolLow=tls_1.1` y `SslProtocolHigh=tls_1.2`.

Debe especificar la lista de cifrados mediante el formato que se define en https://www.openssl.org/docs/manmaster/man1/ciphers.html, en la sección sobre el formato de la lista de cifrados. La siguiente lista de cifrados es la predeterminada:

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

Procedimiento

1 Inicie el Editor del Registro de Windows.

2 Diríjase a la clave del registro `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

3 Agregue dos nuevos valores de cadena (REG_SZ), `SslProtocolLow` y `SslProtocolHigh`, para especificar el rango de protocolos.

Los datos de los valores de registro deben ser `tls_1.0`, `tls_1.1` o `tls_1.2`. Para habilitar un solo protocolo, especifique el mismo protocolo para ambos valores de registro. Si no existe alguno de los dos valores de registro o si sus datos no se establecen en uno de los tres protocolos, se utilizarán los protocolos predeterminados.

4 Agregue un nuevo valor de cadena (REG_SZ), `SslCiphers`, para especificar una lista de conjuntos de claves de cifrado.

Escriba o pegue la lista de conjuntos de claves de cifrado en el campo de datos del valor del registro. Por ejemplo,

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

5 Reinicie el servicio de Windows VMware Blast.

Para volver a usar la lista de cifrados predeterminados, elimine el valor del registro `SslCiphers` y reinicie el servicio de Windows VMware Blast. No elimine simplemente los datos del valor, ya que el agente HTML Access tratará entonces a todos los cifrados como no aceptables, según la definición del formato de la lista de cifrados OpenSSL.

Cuando se inicia el HTML Access Agent, escribe el protocolo y la información de cifrado en su archivo de registro. Puede examinar el archivo de registro para determinar los valores que se están aplicando.

Los conjuntos de claves de cifrado y protocolos predeterminados pueden cambiar en el futuro para adaptarse a los procedimientos recomendados de VMware en lo relativo a seguridad de redes, que evolucionan constantemente.

Configurar directivas de propuesta en escritorios de View

Puede controlar la seguridad de las conexiones del bus de mensajería al servidor de conexión de View si configura las directivas de propuesta en los escritorios de View que ejecuten Windows.

Asegúrese de que el servidor de conexión de View esté configurado para aceptar las mismas directivas para evitar un error de conexión.

Procedimiento

1 Inicie el Editor del registro de Windows en el escritorio de View.

2 Diríjase a la clave de registro `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`.

3 Agregue un nuevo valor de cadena (REG_SZ), `ClientSSLSecureProtocols`.

4 Establezca el valor para una lista de conjuntos de claves de cifrado en el formato **\LIST:*protocol_1,protocol_2,...***.

   Lista de protocolos con el protocolo más reciente en primer lugar. Por ejemplo:

   ```
   \LIST:TLSv1.2,TLSv1.1,TLSv1
   ```

5 Agregue un nuevo valor de cadena (REG_SZ), `ClientSSLCipherSuites`.

6 Establezca el valor a una lista de conjuntos de claves de cifrado en el formato **\LIST:*cipher_suite_1,cipher_suite_2,...***.

   La lista debe aparecer en orden de preferencia, con el conjunto de claves de cifrado preferido en primer lugar. Por ejemplo:

   ```
   \LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
   ```

Ubicaciones de archivos de registros de clientes y agente 6

Los clientes y el agente crean archivos de registro que registran la instalación y operación de sus componentes.

Este capítulo cubre los siguientes temas:

Horizon Client para registros de Windows

Los archivos de registro pueden ayudar a solucionar problemas de instalación, protocolo de visualización y varios componentes destacados. Puede utilizar opciones de directiva de grupo para configurar la ubicación, el nivel de detalle y el período de retención de algunos archivos de registros.

Ubicación del registro

Para los nombres de archivo de la siguiente tabla, *YYYY* representa el año, *MM* el mes, *DD* el día y *XXXXXX* es un número.

Tabla 6-1. Archivos de registros de Horizon Client para Windows

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Instalación	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp`	`vminst.log_XXXXXX_XXXXXX.txt` `vmmsi.log_XXXXXX_XXXXXX.txt`
Cliente PCoIP Desde el proceso `vmware-remotemks.exe`	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp`	`pcoip_client_AAAA_MM_DD_XXXXXX.txt` **NOTA:** Puede utilizar un objeto de directiva de grupo (GPO) para configurar el nivel de detalle del registro del 0 al 3 (siendo el 3 el más detallado). Use el archivo de plantilla ADMX de variables de sesiones del cliente PCoIP de View (`pcoip.admx`). La opción se denomina **Configurar nivel de detalle de registro de eventos PCoIP**.

Tabla 6-1. Archivos de registros de Horizon Client para Windows (Continua)

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Interfaz de usuario (IU) de Horizon Client Desde el proceso `vmware-view.exe`	`C:\Usuarios\%nombredeusuario%\AppData\Local\VMware\VDM\Logs`	`vmware-horizon-viewclient-AAAA-MM-DD-XXXXXX.txt` **NOTA:** Puede utilizar un GPO para configurar la ubicación del registro. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.
Registros de Horizon Client Desde el proceso `vmware-view.exe`	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp\vmware-nombredeusuario-XXXXXX`	`vmware-crtbora-XXXXXX.log`
Marco de mensaje	`C:\Usuarios\%nombredeusuario%\AppData\Local\VMware\VDM\Logs`	`log-AAAA-MM-DD-XXXXXX.txt` `debug-AAAA-MM-DD-XXXXXX.txt`

Registros de MKS (ratón-teclado-pantalla) remoto
Desde el proceso `vmware-remotemks.exe`
	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp\vmware-nombredeusuario`	`ViewMP-Client-XXXXXX.log`
		`vmware-mks-XXXXXX.log`
		`vmware-rdeSvc-XXXXXX.log`
		`vmware-vvaClient-XXXXXX.log`

Cliente Tsdr Desde el proceso `vmware-remotemks.exe`	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp\vmware-nombredeusuario`	`vmware-ViewTsdr-Client-XXXXXX.log`
Cliente Tsmmr Desde el proceso `vmware-remotemks.exe`	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp\vmware-nombredeusuario`	`vmware-ViewTsmmr-Client-XXXXXX.log`
Cliente VdpService Desde el proceso `vmware-remotemks.exe`	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp\vmware-nombredeusuario`	`vmware-vdpServiceClient-XXXXXX.log`
Servicio WSNM Desde el proceso `wsnm.exe`	`C:\ProgramData\VMware\VDM\logs`	`debug-aaaa-mm-dd-XXXXXX.txt` **NOTA:** Puede utilizar un GPO para configurar la ubicación del registro. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.
Redireccionamiento USB Desde los procesos `vmware-view-usbd.exe` o `vmware-remotemks.exe`	`C:\ProgramData\VMware\VDM\logs`	`debug-aaaa-mm-dd-XXXXXX.txt` En Horizon Client 4.4 y versiones posteriores, se elimina el proceso `vmware-view-usbd.exe` y el proceso USBD se envía al proceso `vmware-remotemks.exe`. **NOTA:** Puede utilizar un GPO para configurar la ubicación del registro. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.
Redireccionamiento del puerto serie Desde el proceso `vmwsprrdpwks.exe`	`C:\ProgramData\VMware\VDM\Logs`	`Serial*.txt` `Netlink*.txt`
Redireccionamiento del escáner Desde el proceso `ftscanmgr.exe`	`C:\ProgramData\VMware\VDM\Logs`	`Scanner*.txt` `Netlink*.txt`

Configuración de registro

Puede utilizar los ajustes de directivas de grupos para hacer algunos cambios en la configuración:

- Puede utilizar registros de clientes de PCoIP, puede configurar el nivel de detalle del registro de 0 a 3 (siendo 3 el nivel más detallado). Use el archivo de plantilla ADMX de variables de sesiones del cliente PCoIP de View (`pcoip.admx`). La opción se denomina **Configurar nivel de detalle de registro de eventos PCoIP**.
- Para los registros de IU de cliente, configure la ubicación del registro, el nivel de detalle y la directiva de retención. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.
- Para los registros de redireccionamiento USB, configure la ubicación del registro, el nivel de detalle y la directiva de retención. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.
- Para los registros de servicio WSNM, configure la ubicación del registro, el nivel de detalle y la directiva de retención. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.

También puede utilizar un comando de línea de comando para establecer un nivel de detalle. Vaya al directorio `C:\Archivos de programa (x86)\VMware\VMware Horizon View Client\DCT` e introduzca el siguiente comando:

```
support.bat loglevels
```

Se mostrará una nueva ventana de símbolo del sistema y se le pedirá que seleccione un nivel de detalle.

Recopilar un paquete de registros

Puede utilizar la IU de cliente o un comando de línea de comandos para reunir los registros en un archivo .zip que podrá enviar al servicio de soporte técnico de VMware.

- En la ventana Horizon Client, del menú Opciones, seleccione **Información de soporte técnico** y en el cuadro de diálogo que aparezca, haga clic en **Recopilar datos del soporte técnico**.
- Desde la línea de comandos vaya al directorio `C:\Archivos de programa (x86)\VMware\VMware Horizon View Client\DCT` e introduzca el siguiente comando: `support.bat`.

Horizon Client para registros de Mac

Los archivos de registro pueden ayudar a solucionar problemas de instalación, protocolo de visualización y varios componentes destacados. Puede crear un archivo de configuración para configurar el nivel de detalle.

Ubicación del registro

Tabla 6-2. Archivos de registros de Horizon Client para Mac

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Interfaz de usuario (IU) de Horizon Client	`~/Library/Logs/VMware Horizon Client`	
Cliente PCoIP	`~/Library/Logs/VMware Horizon Client`	
Audio/vídeo en tiempo real	`~/Library/Logs/VMware`	`vmware-RTAV-pid.log`
Redireccionamiento USB	`~/Library/Logs/VMware`	
VChan	`~/Library/Logs/VMware Horizon Client`	

Tabla 6-2. Archivos de registros de Horizon Client para Mac (Continua)

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Registros de MKS (ratón-teclado-pantalla) remoto	`~/Library/Logs/VMware`	
Crtbora	`~/Library/Logs/VMware`	

Configuración de registro

En Horizon Client 3.1 y versiones posteriores, Horizon Client genera archivos de registro en el directorio `~/Library/Logs/VMware Horizon Client` en el cliente Mac. Los administradores pueden configurar el número máximo de archivos de registro y el número máximo de días durante los que se guardarán al configurar las claves del archivo `/Library/Preferences/com.vmware.horizon.plist` en un cliente Mac.

Tabla 6-3. Claves plist para la recopilación de archivos de registro

Clave	Descripción
`MaxDebugLogs`	Número máximo de archivos de registro. El valor máximo es 100.
`MaxDaysToKeepLogs`	Número máximo de días durante los que se guardarán los archivos de registro. Este valor no está limitado.

Se eliminan los archivos que no coinciden con estos criterios cuando inicia Horizon Client.

Si las claves `MaxDebugLogs` o `MaxDaysToKeepLogs` no se configuran en el archivo `com.vmware.horizon.plist`, el número predeterminado de archivos de registro es 5 y el número predeterminado de días durante los que se guardarán los archivos de registro es 7.

Registros de Horizon Client para Linux

Los archivos de registro pueden ayudar a solucionar problemas de instalación, protocolo de visualización y varios componentes destacados. Puede crear un archivo de configuración para configurar el nivel de detalle.

Ubicación del registro

Tabla 6-4. Archivos de registros de Horizon Client para Linux

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Instalación	`/tmp/vmware-root/`	`.vmware-installer-pid.log` `vmware-vmis-pid.log`
Interfaz de usuario (IU) de Horizon Client	`/tmp/vmware-`*`nombredeusuario`*`/`	`vmware-horizon-client-pid.log`
Cliente PCoIP	`/tmp/teradici-`*`nombredeusuario`*`/`	`pcoip_client_`*`AAAA_MM_DD_XXXXXX`*`.log`
Audio/vídeo en tiempo real	`/tmp/vmware-`*`nombredeusuario`*`/`	`vmware-RTAV-pid.log`
Redireccionamiento USB	`/tmp/vmware-root/`	`vmware-usbarb-pid.log` `vmware-view-usbd-pid.log`
VChan	`/tmp/vmware-`*`nombredeusuario`*`/`	`VChan-Client.log` **NOTA:** Este registro se crea cuando habilita los registros de RDPVCBridge estableciendo "`export VMW_RDPVC_BRIDGE_LOG_ENABLED=1`".

Registros de MKS (ratón-teclado-pantalla) remoto	`/tmp/vmware-`*`nombredeusuario`*`/`	`vmware-mks-pid.log`
		`vmware-MKSVchanClient-pid.log`
		`vmware-rdeSvc-pid.log`

Tabla 6-4. Archivos de registros de Horizon Client para Linux (Continua)

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Cliente VdpService	`/tmp/vmware-`*`nombredeusuario`*`/`	`vmware-vdpServiceClient-pid.log`
Cliente Tsdr	`/tmp/vmware-`*`nombredeusuario`*`/`	`vmware-ViewTsdr-Client-pid.log`

Configuración de registro

Puede utilizar una propiedad de configuración (`view.defaultLogLevel`) para establecer el nivel de detalle de los registros de cliente de 0 (recopilar todos los eventos) a 6 (recopilar solo los eventos fatales).

Para registros específicos de USB puede utilizar los siguientes comandos de línea de comandos:

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

Recopilar un paquete de registros

El recopilador de registros se encuentra en `/usr/bin/vmware-view-log-collector` . Para utilizar el recopilador de registros, debe disponer de permisos de ejecución. Puede establecer los permisos desde la línea de comandos de Linux escribiendo el siguiente comando:

```
chmod +x /usr/bin/vmware-view-log-collector
```

Puede ejecutar el recopilador de registros desde la línea de comandos de Linux escribiendo el siguiente comando:

```
/usr/bin/vmware-view-log-collector
```

Registros de Horizon Client en dispositivos móviles

Puede que tenga que instalar en los dispositivos móviles un programa de terceros para acceder al directorio en el que se guardan los archivos de los registros. Los clientes móviles tienen opciones de configuración para enviar paquetes de registros a VMware. Dado que los registros pueden afectar al rendimiento, solo debe habilitarlos cuando necesite solucionar un problema.

Registros de cliente de iOS

En los clientes de iOS, los archivos de registros se encuentran en los directorios `tmp` y `Documents` bajo *`User Programs`*`/Horizon/`. Para acceder a estos directorios, debe instalar una aplicación de terceros como iFunbox.

Puede habilitar los registros habilitando la opción **Registro** en la configuración de Horizon Client. Con esta opción habilitada, si el cliente se cierra de forma inesperada o si usted cierra el cliente y lo vuelve a iniciar, los archivos de registros se combinan y se comprimen en un único archivo GZ. A continuación puede enviar mediante correo electrónico el paquete a VMware. Si el dispositivo está conectado a un PC o Mac, también puede utilizar iTunes para recuperar archivos de registro.

registros de cliente de Android

En los clientes Android, los archivos de registros se pueden encontrar en el siguiente directorio: `Android/data/com.vmware.view.client.android/files/`. Para acceder a este directorio, debe instalar una aplicación de terceros como File Explorer o My Files.

De forma predeterminada los registros solo se crean si la aplicación se cierra de forma inesperada. Puede cambiar este valor predeterminado habilitando la opción **Habilitar registro** en la configuración de Horizon Client. Para enviar un paquete de registros a VMware mediante correo electrónico, puede enviar la opción **Enviar el registro** en la Configuración general del cliente.

Registros de cliente de Chrome

En los clientes de Chrome los registros están disponibles únicamente a través de la consola JavaScript.

Registros de cliente de la Tienda Windows

En el caso de los clientes de la Tienda Windows que tengan instalado Horizon Client para la Tienda Windows, en lugar de Horizon Client para Windows, los archivos de registros se encuentran en el siguiente directorio: `C:\Usuarios\%nombredeusuario%\AppData\Local\Packages\VMwareInc.VMwareViewClient_23chmsjxv380w\LocalState\logs`.

Puede habilitar los registros habilitando la opción **Habilitar registro avanzado** en la Configuración general del cliente y, a continuación, utilizando el botón **Recopilar información de soporte técnico**. Se le pedirá que seleccione una carpeta para los registros. Puede comprimir la carpeta en formato Zip como lo haría con cualquier otra carpeta.

Registros de Horizon Agent desde equipos de Windows

Los archivos de registro pueden ayudar a solucionar problemas de instalación, protocolo de visualización y varios componentes destacados. Puede utilizar opciones de directiva de grupo para configurar la ubicación, el nivel de detalle y el período de retención de algunos archivos de registros.

Ubicación del registro

Para los nombres de archivo de la siguiente tabla, *YYYY* representa el año, *MM* el mes, *DD* el día y *XXXXXX* es un número.

Tabla 6-5. Archivos de registros de Horizon Client para Windows

Tipo de registros	Ruta de acceso del directorio	Nombre de archivo
Instalación	`C:\Usuarios\%nombredeusuario%\AppData\Local\Temp`	`vminst.log_XXXXXX_XXXXXX.txt` `vmmsi.log_XXXXXX_XXXXXX.txt`

View Agent (para Horizon 6) o Horizon Agent (para Horizon 7)	`<Letra de la unidad>:\ProgramData\VMware\VDM\logs`	`pcoip_agent_AAAA_MM_DD_XXXXXX.txt`
		`pcoip_agent_AAAA_MM_DD_XXXXXX.txt`
		`vmware-vdpServiceServer-XXXXXX.log`
		`Serial*.txt`
		`Scanner*.txt`
		`Netlink*.txt`
		`debug-aaaa-mm-dd-XXXXXX.txt`
		NOTA: Puede utilizar un GPO para configurar la ubicación del registro. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.

Configuración de registro

Hay varios métodos para configurar las opciones de registro.

- Puede utilizar la configuración de directiva de grupo para configurar la ubicación, el nivel de detalle y el período de retención de algunos archivos de registros. Utilice el archivo de plantilla ADMX de configuración común de View `vdm_common.admx`.
- Puede utilizar un comando de línea de comando para establecer un nivel de detalle. Vaya al directorio `C:\Archivos de programa\VMware\VMware View\Agent\DCT` e introduzca el siguiente comando: `support.bat loglevels`. Se mostrará una nueva ventana de símbolo del sistema y se le pedirá que seleccione un nivel de detalle.

- Puede utilizar el comando `vdmadmin` con la opción `–A` para configurar los registros que realiza View Agent o Horizon Agent. Para obtener instrucciones, consulte el documento *Administración de View*.

Recopilar un paquete de registros

Puede utilizar un comando de línea de comandos para reunir los registros en un archivo .zip que podrá enviar al servicio de soporte técnico de VMware. Desde la línea de comandos vaya al directorio `C:\Archivos de programa\VMware\VMware View\Agent\DCT` e introduzca el siguiente comando: `support.bat`.

Registros de escritorios Linux

Los archivos de registro pueden ayudar a solucionar problemas de instalación, protocolo de visualización y varios componentes destacados. Puede crear un archivo de configuración para configurar el nivel de detalle.

Ubicación del registro

Tabla 6-6. Archivos de registros de escritorios Linux

Tipo de registros	Ruta de acceso del directorio
Instalación	`/tmp/vmware-root`
View Agent (para Horizon 6) o Horizon Agent (para Horizon 7)	`/var/log/vmware`
View Agent (para Horizon 6) o Horizon Agent (para Horizon 7)	`/usr/lib/vmware/viewagent/viewagent-debug.log`

Configuración de registro

Edite el archivo `/etc/vmware/config` para configurar el registro.

Recopilar un paquete de registros

Puede crear un paquete de herramientas de recopilación de datos (DCT) que recopile los registros y la información de configuración de la máquina en un archivo tar comprimido. Abra un símbolo del sistema en el escritorio Linux y ejecute el script `dct-debug.sh`.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

El archivo tar se genera en el directorio desde el que se ejecutó el script (el directorio de trabajo actual). El nombre de archivo incluye el sistema operativo, la marca de tiempo y otro tipo de información, por ejemplo: `ubuntu-12-vdm-sdct-20150201-0606-agent.tgz`

Este comando recopila archivos de registro desde los directorios `/tmp/vmware-root` y `/var/log/vmware`. Asimismo, recopila la los siguientes archivos de configuración y registros del sistema:

- `/var/log/messages*`
- `/var/log/syslog*`
- `/var/log/boot*.log`
- `/proc/cpuinfo`, `/proc/meminfo`, `/proc/vmstat`, `/proc/loadavg`
- `/var/log/audit/auth.log*`
- `/etc/hosts`
- `/etc/resolv.conf`
- `/etc/nsswitch.conf`
- `/var/log/Xorg*`

- `/etc/X11/xorg.conf`
- Archivos principales en `/usr/lib/vmware/viewagent`
- Todos los archivos de bloqueos en `/var/crash/_usr_lib_vmware_viewagent*`

Aplicar revisiones de seguridad 7

Las versiones de revisión pueden incluir instaladores de los siguientes componentes de Horizon 7: View Composer, servidor de conexión de Horizon, View Agent o Horizon Agent, y varios clientes. Los componentes de revisión que debe aplicar dependen del número de correcciones de problemas que requiere la implementación de Horizon 7.

Dependiendo de las correcciones de errores que necesite, instale los componentes de Horizon 7 necesarios en el siguiente orden:

1 View Composer

2 Servidor de conexión

3 View Agent (para Horizon 6) o Horizon Agent (para Horizon 7)

4 Horizon Client

Si desea obtener instrucciones para aplicar revisiones para los componentes de servidor, consulte el documento *Actualizaciones de View*.

Este capítulo cubre los siguientes temas:

Aplicar una revisión a View Agent o Horizon Agent

Si desea aplicar una revisión, este proceso incluye la descarga y la ejecución de la versión de revisión.

Es necesario realizar los siguientes pasos en la máquina virtual principal, en los grupos de escritorios de clonación vinculada o en cada escritorio de la máquina virtual de un grupo de clonación completa, o bien en máquinas virtuales de escritorio individuales para grupos que contienen únicamente un escritorio de máquina virtual.

Prerequisitos

Compruebe que tenga una cuenta de usuario del dominio con privilegios de administrador en los hosts que utilizará para ejecutar el instalador de revisión.

Procedimiento

1 Descargue el archivo instalador de la versión de revisión de View Agent (para Horizon 6) o Horizon Agent (para Horizon 7) en todas las máquinas virtuales principales, en las máquinas virtuales usadas para plantillas de clonación completa, en los clones completos de un grupo y en las máquinas virtuales agregadas de forma manual.

   Si se pone en contacto con VMware, le proporcionaremos instrucciones para realizar esta descarga.

2 Ejecute el instalador de la versión de revisión de View Agent o de Horizon Agent que descargó.

Para obtener información sobre la ejecución del instalador de agente, consulte el documento *Configurar escritorios virtuales en Horizon 7*.

NOTA: En Horizon 6 versión 6.2 y versiones posteriores no necesita desinstalar la versión anterior antes de instalar la revisión.

3 Si deshabilitó el aprovisionamiento de las nuevas máquinas virtuales mientras preparaba View Composer para aplicar una revisión, vuelva a habilitarlo.

4 En las máquinas virtuales principales que se usan para crear grupos de escritorios de clonación vinculada, realice una snapshot de la máquina virtual.

Si desea obtener información sobre cómo realizar snapshots, consulte la ayuda en línea de vSphere Client.

5 En los grupos de escritorios de clonación vinculada, utilice la snapshot que creó para recomponer los grupos de escritorios.

6 Compruebe que puede iniciar sesión en los grupos de escritorios revisados con Horizon Client.

7 Si canceló cualquier operación de recomposición o de actualización en algún grupo de escritorios de clonación vinculada, vuelva a programar las tareas.

Aplicar una revisión a Horizon Client

En los dispositivos cliente, si desea aplicar una revisión, este proceso incluye la descarga y la ejecución de la versión de revisión. En clientes móviles, si desea aplicar una revisión, este proceso incluye simplemente la instalación de la actualización desde un sitio web que venda aplicaciones, como Google Play, Tienda Windows o Apple App Store.

Procedimiento

1 En cada sistema cliente, descargue el archivo instalador de la versión de revisión de Horizon Client.

Si se pone en contacto con VMware, le proporcionaremos instrucciones para realizar esta descarga. O bien, puede dirigirse a la página de descarga del cliente en http://www.vmware.com/go/viewclients. Como se mencionó anteriormente, para algunos clientes, puede obtener la versión de revisión desde una tienda de aplicaciones.

2 Si el dispositivo cliente es un equipo o un escritorio Mac o Linux, elimine la versión actual del software cliente del dispositivo.

Use el método de métricas específico del dispositivo para eliminar aplicaciones.

NOTA: Con Horizon Client 3.5 para Windows y versiones posteriores, no necesita desinstalar la versión anterior antes de instalar la revisión en los clientes de Windows. Con Horizon Client 4.1 para Windows y versiones posteriores, puede habilitar la función Actualizar Horizon Client en línea para actualizar Horizon Client en línea en clientes de Windows. Si desea obtener información, consulte el documento *Utilizar VMware Horizon Client* para Windows. Con Horizon Client para Mac 4.4 y versiones posteriores, puede habilitar la función Actualizar Horizon Client en línea para actualizar Horizon Client en línea en clientes de Mac.

3 Si es necesario, ejecute el instalador de la versión de revisión de Horizon Client que descargó.

Si obtuvo la revisión desde Apple App Store o Google Play, la aplicación se suele instalar cuando la descarga y no es necesario que ejecute un instalador.

4 Compruebe que pueda iniciar sesión en los grupos de escritorios revisados con el Horizon Client revisado recientemente.

Índice

U

V