

Seguridad de View

Modificado para Horizon 7 7.3.2
VMware Horizon 7 7.3



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2009-2017 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Seguridad de View 5

1 Cuentas, recursos y archivos de registro de Horizon 7 6

Cuentas de Horizon 7 6

Recursos de Horizon 7 7

Archivos de registro de Horizon 7 8

2 Configuración de seguridad de View 10

Opciones globales relacionadas con la seguridad de View Administrator 10

Opciones del servidor relacionadas con la seguridad en View Administrator 13

Opciones relacionadas con la seguridad en LDAP de View 13

3 Puertos y servicios 15

Puertos UDP y TCP de View 15

Redireccionamiento HTTP en View 19

Servicios en un host del servidor de conexión de View 20

Servicios de un servidor de seguridad 21

4 Configurar protocolos de seguridad y conjuntos de claves de cifrado en una instancia del servidor de conexión de View o en un servidor de seguridad 23

Directivas globales predeterminadas para los protocolos de seguridad y los conjuntos de claves de cifrado 24

Configurar las directivas de propuesta y de aceptación globales 24

Directivas de propuesta y de aceptación globales definidas en el LDAP de View 24

Cambiar las directivas globales de propuesta y de aceptación 25

Configurar directivas de aceptación en servidores individuales 26

Configurar directivas de propuesta en escritorios remotos 27

Cifrados y protocolos antiguos deshabilitados en View 28

5 Configurar los protocolos de seguridad y los conjuntos de claves de cifrado para la puerta de enlace segura de Blast 30

Configurar los protocolos de seguridad y los conjuntos de claves de cifrado para la puerta de enlace segura de Blast (BSG) 30

6 Implementar dispositivos USB en un entorno de Horizon 7 seguro 32

Deshabilitar el redireccionamiento USB en todos los tipos de dispositivos 32

Deshabilitar el redireccionamiento USB de dispositivos específicos 34

7 Medidas de protección HTTP en los servidores de conexión y de seguridad 36

Estándares del Grupo de trabajo de ingeniería de Internet	36
Estándares del Consorcio World Wide Web	37
Compartir recursos de distintos orígenes	37
Directiva de seguridad de contenido	39
Otras medidas de protección	40
Reducir los riesgos de seguridad de tipo MIME	40
Disminuir ataques de scripts de sitios	40
Comprobar el tipo de contenido	40
Supervisión de protocolo de enlace	41
Listas blancas de agentes de usuarios	42
Configurar las medidas de protección HTTP	43

Seguridad de View

La guía *Seguridad de View* supone una referencia concisa de las funciones de seguridad de VMware Horizon 7.

- Cuentas de inicio de sesión necesarias de las bases de datos y del sistema.
- 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.
- Interfaces externas, puertos y servicios que se deben abrir o habilitar para que View funcione correctamente.

Público al que se dirige

Esta información va dirigida a responsables de toma de decisiones, arquitectos y administradores de TI así como a otros usuarios que se deben familiarizar con los componentes de seguridad de View.

Cuentas, recursos y archivos de registro de Horizon 7

1

Si tiene diferentes cuentas para componentes específicos, esto supone una protección para no otorgar a los usuarios más permisos y accesos de los que necesitan. Además, si conoce la ubicación de los archivos de configuración y otros archivos con datos confidenciales, esto ayuda a configurar la seguridad en varios sistemas de hosts.

Nota A partir de la Horizon 7.0, View Agent se denomina Horizon Agent.

Este capítulo incluye los siguientes temas:

- [Cuentas de Horizon 7](#)
- [Recursos de Horizon 7](#)
- [Archivos de registro de Horizon 7](#)

Cuentas de Horizon 7

Debe establecer cuentas de la base de datos y del sistema para administrar los componentes de Horizon 7.

Tabla 1-1. Cuentas de sistema de Horizon 7

Componentes de Horizon	Cuentas necesarias
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 parte del grupo Usuarios de escritorio remoto, pero estas cuentas no necesitan privilegios de Horizon Administrator.
vCenter Server	Configure una cuenta de usuario en Active Directory con permiso para realizar las operaciones necesarias en vCenter Server para admitir Horizon 7. Para obtener más información sobre los privilegios necesarios, consulte el documento <i>Instalación de View</i> .

Componentes de Horizon	Cuentas necesarias
View Composer	<p>Cree una cuenta de usuario en Active Directory para usarla con View Composer. View Composer necesita que esta cuenta conecte los escritorios de clonación vinculada con el dominio de Active Directory.</p> <p>La cuenta de usuario no debe ser una cuenta administrativa de Horizon. Otorgue a la cuenta los privilegios mínimos necesarios para crear y eliminar objetos del equipo en un contenedor de Active Directory especificado. Por ejemplo, esta cuenta no necesita privilegios de administrador de dominio. Para obtener más información sobre los privilegios necesarios, consulte el documento <i>Instalación de View</i>.</p>
Servidor de conexión	<p>Cuando instala Horizon 7, puede especificar un usuario de dominio, el grupo de Administradores locales o un grupo de usuarios de dominio específico como administradores de Horizon. Le recomendamos que cree un grupo de usuarios de dominio dedicado de administradores de Horizon. El predeterminado es el usuario con la sesión ya iniciada.</p> <p>En Horizon Administrator, puede usar Configuración de View > Administradores para cambiar la lista de los administradores de Horizon.</p> <p>Consulte el documento <i>Administración de View</i> para obtener más información sobre los privilegios necesarios.</p>

Tabla 1-2. Cuentas de la base de datos de Horizon

Componentes de Horizon	Cuentas necesarias
Base de datos de View Composer	<p>Una base de datos de Oracle o SQL Server almacena los datos de View Composer. Cree una cuenta administrativa para la base de datos que pueda asociar con la cuenta de usuario de View Composer.</p> <p>Para obtener más información sobre la configuración de una base de datos de View Composer, consulte el documento <i>Instalación de View</i>.</p>
Base de datos de eventos que usa el servidor de conexión de Horizon	<p>Una base de datos de Oracle o de SQL Server almacena los datos de eventos de Horizon. Cree una cuenta administrativa para la base de datos que Horizon Administrator pueda usar para acceder a los datos de los eventos.</p> <p>Para obtener más información sobre la configuración de una base de datos de View Composer, consulte el documento <i>Instalación de View</i>.</p>

Para reducir el riesgo de vulnerabilidades de seguridad, realice las siguientes acciones:

- Configure las bases de datos de Horizon 7 en servidores que estén separados de otros servidores de bases de datos que use su organización.
- No permita que una cuenta de usuario único acceda a varias bases de datos.
- Configure cuentas independientes para acceder a las bases de datos de eventos y de View Composer.

Recursos de Horizon 7

Horizon 7 incluye varios archivos de configuración y recursos similares que deben protegerse.

Tabla 1-3. Recursos del servidor de seguridad y del servidor de conexión de Horizon

Recurso	Ubicación	Protección
Configuración de LDAP	No aplicable.	Los datos de LDAP se protegen automáticamente como parte del control de acceso según la función.
Archivos de copia de seguridad de seguridad de LDAP	%ProgramData%\VMware\VDM\backups	Protegidos por el control de acceso.
locked.properties (archivo de configuración de la puerta de enlace segura)	directorio_instalación\VMware\VMware View\Server\sslgateway\conf	Asegúrese de que este archivo esté protegido de forma que no puedan acceder a él otros usuarios que no sean los administradores de Horizon.
absg.properties (archivo de configuración de la puerta de enlace segura de Blast)	directorio_instalación\VMware\VMware View\Server\appblastgateway	Asegúrese de que este archivo esté protegido de forma que no puedan acceder a él otros usuarios que no sean los administradores de Horizon.
Archivos de registro	Consulte Archivos de registro de Horizon 7	Protegidos por el control de acceso.
web.xml (Archivo de configuración de Tomcat)	directorio_instalación\VMware View\Server\broker\web apps\ROOT\Web INF	Protegidos por el control de acceso.

Archivos de registro de Horizon 7

Horizon 7 crea archivos de registros de la instalación y el funcionamiento de sus componentes.

Nota El equipo de soporte de VMware usa los archivos de registro de Horizon 7. VMware le recomienda que configure y use la base de datos de eventos para supervisar Horizon 7. Para obtener más información, consulte los documentos *Instalación de View* e *Integración de View*.

Tabla 1-4. Archivos de registro de Horizon 7

Componentes de Horizon	Ruta de acceso al archivo y otra información
Todos los componentes (registros de instalación)	%TEMP%\vminst.log_fecha _ marcadetiempo %TEMP%\vmmsi.log_fecha _ marcadetiempo
Horizon Agent	<p><Letra de la unidad>:\ProgramData\VMware\VDM\logs</p> <p>Para acceder a los archivos de registro de Horizon 7 que se almacenan en <Letra de la unidad>:\ProgramData\VMware\VDM\logs, debe abrir los registros desde un programa con privilegios de administrador elevados. Haga clic en el botón secundario y seleccione Ejecutar como administrador.</p> <p>Si un disco de datos de usuario (UDD) está configurado, <Letra de la unidad> debe coincidir con el UDD.</p> <p>Los registros de PCoIP reciben el nombre pcoip_agent*.log y pcoip_server*.log.</p>

Componentes de Horizon	Ruta de acceso al archivo y otra información
Aplicaciones publicadas	<p>La base de datos de eventos de View configurada en un servidor de base de datos Oracle o SQL Server.</p> <p>Registros de eventos de aplicación de Windows. Deshabilitado de forma predeterminada.</p>
View Composer	<p>%system_drive% \Windows\Temp\vmware-viewcomposer-ga-new.log en el escritorio de clonación vinculada.</p> <p>El registro de View Composer contiene información sobre la ejecución de los scripts QuickPrep y Sysprep. El registro almacena el tiempo de inicio y de finalización de la ejecución de un script y todas las salidas o mensajes de error.</p>
Servidor de seguridad o el servidor de conexión	<p><Letra de la unidad>:\ProgramData\VMware\VDM\logs.</p> <p>El directorio de registros se puede configurar en las opciones de configuración del registro en el archivo de plantilla ADMX de la configuración común de View (vdm_common.admx).</p> <p>Los registros de la puerta de enlace segura de PCoIP se escriben en archivos denominados SecurityGateway_*.log en el subdirectorio Puerta de enlace segura PCoIP.</p> <p>Los registros de la puerta de enlace segura de Blast se escriben en archivos denominados absg*.log en el subdirectorio Puerta de enlace segura de Blast.</p>
Servicios de Horizon	<p>La base de datos de eventos de Horizon configurada en un servidor de base de datos Oracle o SQL Server.</p> <p>Registros de eventos de sistema de Windows.</p>

Configuración de seguridad de View

2

View incluye varias opciones que puede usar para establecer la seguridad de la configuración. Puede acceder a la configuración con View Administrator o con la utilidad del Editor ADSI, según corresponda.

Nota Para obtener información sobre la configuración de seguridad de Horizon Client y de Horizon Agent, consulte el documento *Seguridad en Horizon Client y Agent*.

Este capítulo incluye los siguientes temas:

- [Opciones globales relacionadas con la seguridad de View Administrator](#)
- [Opciones del servidor relacionadas con la seguridad en View Administrator](#)
- [Opciones relacionadas con la seguridad en LDAP de View](#)

Opciones globales relacionadas con la seguridad de View Administrator

Se puede acceder a las opciones globales relacionadas con la seguridad de las conexiones y las sesiones cliente a través de **Configuración de View > Configuración global** en View Administrator.

Tabla 2-1. Opciones globales relacionadas con la seguridad

Configuración	Descripción
Cambiar contraseña de recuperación de datos	<p>La contraseña es necesaria cuando restaura la configuración LDAP de View desde una copia de seguridad cifrada.</p> <p>Cuando instala el servidor de conexión de View versión 5.1 o posterior, proporcione una contraseña de Data Recovery. Después de la instalación, puede cambiar esta contraseña en View Administrator.</p> <p>Cuando realiza una copia de seguridad del servidor de conexión de View, la configuración LDAP de View se exporta como datos LDIF cifrados. Para restaurar la copia de seguridad cifrada con la utilidad vdmimport, debe proporcionar la contraseña de Data Recovery. La contraseña debe tener entre 1 y 128 caracteres. Siga las prácticas recomendadas de la organización para generar contraseñas seguras.</p>
Modo de seguridad Mensaje	<p>Determina el mecanismo de seguridad que se usa cuando los mensajes JMS se envían entre los componentes de View.</p> <ul style="list-style-type: none"> ■ Si está establecida como Deshabilitado, el modo de seguridad del mensaje está deshabilitado. ■ Si está establecido como Habilitado, se produce la firma del mensaje heredado y la verificación de los mensajes JMS. Los componentes de View rechazan los mensajes no firmados. Este modo admite una combinación de SSL y conexiones JMS sin formato. ■ Para cifrar todos los mensajes, si está establecido como Mejorado, se usa SSL para todas las conexiones JMS. El control de los accesos también está habilitado para restringir los temas JMS a los que los componentes de View pueden enviar mensajes y de los que pueden recibirlos. ■ Si está establecido como Mixto, el modo de seguridad de los mensajes está habilitado, pero no mejorado para los componentes de View anteriores a View Manager 3.0. <p>La opción predeterminada es Mejorado en las nuevas instalaciones. Si actualiza una versión anterior, se mantiene la opción utilizada en la versión anterior.</p> <p>Importante VMware recomienda establecer el modo de seguridad de los mensajes a Mejorado después de actualizar a esta versión todas las instancias del servidor de conexión de View, los servidores de seguridad y los escritorios de View. La opción Mejorado proporciona mejoras de seguridad importantes y actualizaciones de MQ (cola de mensajes).</p>
Estado de seguridad mejorada (solo lectura)	<p>Campos de solo lectura que aparecen cuando la opción Modo de seguridad Mensaje se cambia de Habilitado a Mejorado. Como el cambio se hace en fases, este campo muestra el progreso en las diferentes fases:</p> <ul style="list-style-type: none"> ■ La opción Esperar el reinicio del bus de mensajería es la primera fase. Este estado aparece hasta que reinicie de forma manual todas las instancias del servidor de conexión en el pod o en el servicio del componente del bus de mensajería de VMware Horizon View en todos los hosts del servidor de conexión del pod. ■ La opción Mejora pendiente es el siguiente estado. Después de que se reinicien todos los servicios del componente de bus de mensajería de View, el sistema comienza a cambiar el modo de seguridad de los mensajes a Mejorado de todos los escritorios y servidores de seguridad. ■ La opción Mejorado es el estado final, que indica que todos los componentes están usando el modo de seguridad de los mensajes Mejorado.

Configuración	Descripción
Volver a autenticar las conexiones de túnel seguro después de la interrupción en la red	<p>Determina si las credenciales del usuario deben volver a autenticarse después de una interrupción de red cuando Horizon Client usa conexiones de túnel seguras con las aplicaciones y los escritorios de View.</p> <p>Esta opción proporciona más seguridad. Por ejemplo, si se roba un equipo y se lleva a una red diferente, el usuario no puede acceder automáticamente a las aplicaciones y los escritorios de View porque la conexión de red se interrumpió de forma temporal.</p> <p>Esta configuración está deshabilitada de forma predeterminada.</p>
Desconectar usuarios de forma forzada	<p>Desconecta todos los escritorios y todas las aplicaciones después de que transcurra el número de minutos especificado desde que el usuario inició sesión en View. Todos los escritorios y todas las aplicaciones se desconectarán al mismo tiempo, sin tener en cuenta cuándo el usuario los inició.</p> <p>El valor predeterminado es 600 minutos.</p>
Para clientes que admiten aplicaciones. Si el usuario deja de usar el teclado y el mouse, desconecte las aplicaciones y descarte las credenciales SSO	<p>Protege las sesiones de las aplicaciones donde no hay actividad de teclado ni mouse en el dispositivo cliente. Si está establecido como Después de ... minutos, View desconecta todas las aplicaciones y descarta las credenciales SSO después del número de minutos especificado sin actividad del usuario. Se desconectan las sesiones de escritorio. Los usuarios deben iniciar sesión de nuevo para volver a conectar todas las aplicaciones que se desconectaron o iniciar una nueva aplicación o un nuevo escritorio.</p> <p>Si está establecido como Nunca, View no desconecta nunca las aplicaciones ni descarta las credenciales SSO debido a la inactividad de usuario.</p> <p>El valor predeterminado es Nunca.</p>
Otros clientes. Descartar credenciales SSO	<p>Descarta las credenciales SSO después de un periodo de tiempo. Esta opción está destinada a clientes que no admiten la comunicación remota de aplicaciones. Si está establecida como Después de... minutos, los usuarios deben iniciar sesión de nuevo para conectarse a un escritorio después de que pase el número de minutos determinado desde que el usuario inició sesión en View, sin tener en cuenta la actividad del usuario en el dispositivo cliente.</p> <p>El valor predeterminado es Después de 15 minutos.</p>
Habilitar IPSec para el emparejamiento del servidor de seguridad	<p>Determina si se debe usar el Protocolo de seguridad de Internet (IPSec) para las conexiones entre los servidores de seguridad y las instancias del servidor de conexión de View. Esta opción debe deshabilitarse antes de instalar un servidor de seguridad en modo FIPS; de lo contrario, se producirá un error en el emparejamiento.</p> <p>De forma predeterminada, se encuentra habilitada IPSec para las conexiones del servidor de seguridad.</p>
Tiempo de espera de la sesión de View Administrator	<p>Determina durante cuánto tiempo continua una sesión inactiva de View Administrator antes de que la sesión caduque.</p> <p>Importante Al establecer el tiempo de espera de la sesión de View Administrator a un número elevado de minutos, aumenta el riesgo de que View Administrator se use de forma no autorizada. Si desea permitir una sesión inactiva durante un tiempo prolongado, hágalo con precaución.</p> <p>De forma predeterminada, el tiempo de espera de la sesión de View Administrator es 30 minutos. Puede establecer el tiempo de espera de la sesión de 1 a 4320 minutos.</p>

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

Nota SSL es necesario para todas las conexiones de Horizon Client y de View Administrator con View. Si la implementación de View usa equilibradores de carga u otros servidores intermedios para el cliente, puede descargar SSL en ellos y configurar conexiones SSL en instancias individuales del servidor de conexión de View y los servidores de seguridad. Consulte "Descargar conexiones SSL a servidores intermedios" en el documento *Administración de View*.

Opciones del servidor relacionadas con la seguridad en View Administrator

Se puede acceder a las opciones del servidor relacionadas con la seguridad en **Configuración de View > Servidores** en View Administrator.

Tabla 2-2. opciones del servidor relacionadas con la seguridad

Configuración	Descripción
Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina	<p>Determina si Horizon Client establece una conexión más segura con el servidor de conexión de View o el host del servidor de seguridad cuando los usuarios se conectan a las aplicaciones y a los escritorios de View con el protocolo de visualización PCoIP.</p> <p>Si esta opción está deshabilitada, la sesión de la aplicación o del escritorio se establece directamente entre el cliente y el escritorio de View o el host de los Servicios de Escritorio remoto (RDS), derivando el servidor de conexión de View o el host del servidor de seguridad.</p> <p>Esta configuración está deshabilitada de forma predeterminada.</p>
Usar la conexión de túnel seguro con la máquina	<p>Determina si Horizon Client establece una conexión HTTPS con el servidor de conexión de View o el host del servidor de seguridad cuando los usuarios se conectan a las aplicaciones y a los escritorios de View.</p> <p>Si esta opción está deshabilitada, la sesión de la aplicación o del escritorio se establece directamente entre el cliente y el escritorio de View o el host de los Servicios de Escritorio remoto (RDS), derivando el servidor de conexión de View o el host del servidor de seguridad.</p> <p>Esta configuración está habilitada de forma predeterminada.</p>
Usar la puerta de enlace segura de Blast en las conexiones Blast de la máquina	<p>Determina si los clientes que usan el protocolo de visualización Blast Extreme o el navegador web para acceder a los escritorios usan la puerta de enlace segura de Blast para establecer un túnel seguro al servidor de conexión de View.</p> <p>Si no está habilitado, los clientes que usan sesiones de Blast Extreme y navegadores web establecen conexiones directas a escritorios de View, derivando el servidor de conexión de View.</p> <p>Esta configuración está deshabilitada de forma predeterminada.</p>

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

Opciones relacionadas con la seguridad en LDAP de View

LDAP de View proporciona opciones relacionadas con la seguridad en la ruta de acceso del objeto `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`. Puede usar la utilidad Editor ADSI para cambiar el valor de estas opciones en una instancia del servidor de conexión de View. El

cambio se propaga automáticamente a todas las instancias del servidor de conexión de View de un grupo.

Tabla 2-3. Opciones relacionadas con la seguridad en LDAP de View

Par valores y nombres	Descripción
cs-allowunencryptedstartsession	<p>El atributo es <code>pae-NameValuePair</code>.</p> <p>Este atributo controla si es necesario un canal seguro entre la instancia del servidor de conexión de View y un escritorio cuando se inicie una sesión remota de usuario.</p> <p>Cuando View Agent 5.1 o una versión posterior, o bien Horizon Agent 7.0 o una versión posterior, estén instalados en un equipo de escritorio, este atributo no tiene efecto y siempre se solicita un canal de seguridad. Cuando está instalada una versión de View Agent anterior a View 5.1, no se puede establecer un canal de seguridad si el equipo de escritorio no es miembro de un dominio con una confianza bidireccional al dominio de la instancia del servidor de conexión de View. En este caso, el atributo es importante para determinar si se puede iniciar una sesión remota de usuario sin un canal seguro.</p> <p>En todos los casos, las credenciales de usuario y vales de autorización están protegidas por una clave estática. Un canal seguro proporciona un mayor control de confidencialidad a través de claves dinámicas.</p> <p>Si se establece a 0, no se iniciará una sesión remota de usuario si no se puede establecer un canal seguro. Esta opción es útil si todos los escritorios se encuentran en dominios de confianza o si todos los escritorios tienen instalados View Agent 5.1 o una versión posterior.</p> <p>Si se establece a 1, se puede iniciar una sesión remota de usuario aunque no se pueda establecer un canal seguro. Esta opción es útil si algunos escritorios tienen instaladas versiones más antiguas de View Agents y no se encuentran en dominios de confianza.</p> <p>La opción predeterminada es 1.</p>

Puertos y servicios

Se deben abrir algunos puertos TCP y UDP para que los componentes de View se puedan comunicar entre ellos. Si se conoce los servicios de Windows que se ejecutan en cada tipo de View Server, esto ayudará a identificar los servicios que no pertenezcan al servidor.

Este capítulo incluye los siguientes temas:

- [Puertos UDP y TCP de View](#)
- [Servicios en un host del servidor de conexión de View](#)
- [Servicios de un servidor de seguridad](#)

Puertos UDP y TCP de View

View usa los puertos TCP y UDP entre sus componentes para acceder a la red.

Durante la instalación, View puede configurar de forma opcional reglas del firewall de Windows para abrir los puertos que se usan de forma predeterminada. Si cambia los puertos predeterminados después de la instalación, debe volver a configurar de forma manual las reglas del firewall de Windows para permitir el acceso a los puertos actualizados. Consulte "Reemplazar los puertos predeterminados para los servicios de View" en el documento *Instalación de View*.

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

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	55000	Horizon Agent	4172	UDP	PCoIP (no SALSA20) si se usa la puerta de enlace segura de PCoIP.
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.					

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Servidor de seguridad	500	Servidor de conexión de View	500	UDP	Tráfico de negociación de IPsec.
Servidor de seguridad	*	Servidor de conexión de View	4001	TCP	Tráfico JMS.
Servidor de seguridad	*	Servidor de conexión de View	4002	TCP	Tráfico SSL de JMS.
Servidor de seguridad	*	Servidor de conexión de View	8009	TCP	Tráfico web reenviado por AJP13, si no se usa IPsec.
Servidor de seguridad	*	Servidor de conexión de View	*	ESP	Tráfico web reenviado por AJP13, al usar IPsec sin NAT.
Servidor de seguridad	4500	Servidor de conexión de View	4500	UDP	Tráfico web reenviado por AJP13, al usar IPsec a través de un dispositivo NAT.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	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	*	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	*	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	*	Horizon Agent	4172	TCP	PCoIP si se usa la puerta de enlace segura de PCoIP.

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	Horizon Agent	22443	TCP	VMware Blast Extreme si se usa la puerta de enlace segura de Blast.
Servidor de seguridad, servidor de conexión de View o dispositivo Unified Access Gateway	*	Horizon Agent	22443	TCP	HTML Access si se usa la puerta de enlace segura de Blast.
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.
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.
Horizon Agent	4172	Dispositivo de Unified Access Gateway	*	UDP	PCoIP. Las aplicaciones y escritorios de View devuelven datos PCoIP a los dispositivos Unified Access Gateway desde el puerto UDP 4172. El puerto UDP de destino será el puerto de origen de los paquetes UDP recibidos y, como se trata de datos de respuesta, no suele ser necesario agregar ninguna regla de firewall específica para ello.
Horizon Client	*	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	80	TCP	SSL (acceso HTTPS) está habilitado de forma predeterminada para las conexiones cliente, pero el puerto 80 (acceso HTTP) se puede usar en ciertos casos. Consulte Redireccionamiento HTTP en View .
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).

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Horizon Client	*	Servidor de conexión de View, servidor de seguridad o dispositivo Unified Access Gateway	4172	TCP y UDP	PCoIP si se usa la puerta de enlace segura de PCoIP.
Horizon Client	*	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	*	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.
Horizon Client	*	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	*	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
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.
Navegador web	*	Servidor de seguridad o dispositivo Unified Access Gateway	8443	TCP	HTML Access.
Servidor de conexión de View	*	Servidor de conexión de View	48080	TCP	Para la comunicación interna entre los componentes del servidor de conexión de View.
Servidor de conexión de View	*	vCenter Server o View Composer	80	TCP	Mensajes SOAP si SSL está deshabilitado para acceder a vCenter Server o View Composer.
Servidor de conexión de View	*	vCenter Server	443	TCP	Mensajes SOAP si SSL está habilitado para acceder a vCenter Server.
Servidor de conexión de View	*	View Composer	18443	TCP	Mensajes SOAP si SSL está habilitado para acceder a View Composer.

Origen	Puerto	Destino	Puerto	Protocolo	Descripción
Servidor de conexión de View	*	Servidor de conexión de View	4100	TCP	Tráfico entre enrutadores JMS.
Servidor de conexión de View	*	Servidor de conexión de View	4101	TCP	Tráfico entre enrutadores SSL JMS.
Servidor de conexión de View	*	Servidor de conexión de View	8472	TCP	Para una comunicación entre los pods en una arquitectura Cloud Pod.
Servidor de conexión de View	*	Servidor de conexión de View	22389	TCP	Para una replicación LDAP global en la arquitectura Cloud Pod.
Servidor de conexión de View	*	Servidor de conexión de View	22636	TCP	Para una replicación LDAP global segura en la arquitectura Cloud Pod.
Servidor de conexión de View	*	Servidor de conexión de View	32111	TCP	Tráfico de claves compartidas.
Dispositivo de Unified Access Gateway	*	Servidor de conexión de View o equilibrador de carga	443	TCP	Acceso HTTPS. Los dispositivos de Unified Access Gateway se conectan al puerto TCP 443 para comunicarse con una instancia del servidor de conexión de View o un equilibrador de carga frente a varias instancias de servidor de conexión de View.
Servicio de View Composer	*	Host de ESXi	902	TCP	Se usa cuando View Composer personaliza discos de clonación vinculada, incluidos los discos internos de View Composer y, si se especifican, los discos persistentes y los discos descartables del sistema.

Nota El número de puerto UDP que el cliente usa para PCoIP 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 así sucesivamente. Debe configurar el firewall con la opción ANY donde aparece un asterisco (*) en la tabla.

Nota Microsoft Windows Server requiere que se abra un rango de puertos dinámico entre todos los servidores de conexión del entorno de Horizon 7. Microsoft Windows necesita estos puertos para el funcionamiento normal de llamadas a procedimientos remotos (RPC) y réplicación de Active Directory. Para obtener más información sobre el rango de puertos dinámico, consulte la documentación de Microsoft Windows Server.

Redireccionamiento HTTP en View

Los intentos de conexión mediante HTTP se redireccionan de forma silenciosa a HTTPS, excepto los intentos de conexión a View Administrator. El redireccionamiento HTTP no es necesario con las versiones más recientes de Horizon Client porque establecen conexiones HTTPS de forma

predeterminada, pero es útil cuando los usuarios se conectan con un navegador web para descargar Horizon Client, por ejemplo.

El problema del redireccionamiento HTTPS es que no se trata de un protocolo seguro. Si un usuario no tiene la costumbre de escribir **https://** en la barra de direcciones, un atacante puede poner en peligro el navegador web, instalar malware o robar credenciales, aunque la página se muestre correctamente.

Nota El redireccionamiento HTTP de las conexiones externas pueden producirse únicamente si configura el firewall externo para que permita el tráfico entrante al puerto TCP 80.

No se redireccionan los intentos de conexión mediante HTTP a View Administrator. En su lugar, aparece un mensaje de error para informarle que debe usar HTTPS.

Para evitar el redireccionamiento en todas los intentos de conexión HTTPS, consulte "Evitar el redireccionamiento HTTP en las conexiones cliente al servidor de conexión" en el documento *Instalación de View*.

Las conexiones al puerto 80 de una instancia del servidor de conexión de View o del servidor de seguridad también pueden tener lugar si descarga las conexiones cliente SSL a un dispositivo intermedio. Consulte "Descargar conexiones SSL a servidores intermedios" en el documento *Administración de View*.

Para permitir el redireccionamiento HTTP cuando se cambia el número de puerto SSL, consulte "Cambiar el número de puerto para el redireccionamiento HTTPS al servidor de conexión" en el documento *Instalación de View*.

Servicios en un host del servidor de conexión de View

La operación de View depende de varios dispositivos que se ejecutan en el host del servidor de conexión de View.

Tabla 3-2. Servicios de los hosts del servidor de conexión de View

Nombre del servicio	Tipo de inicio	Descripción
Puerta de enlace segura de Blast VMware Horizon View	Automático	Proporciona servicios HTML Access y Blast Extreme seguros. Este servicio debe ejecutarse si los clientes se conectan al servidor de conexión de View a través de la puerta de enlace segura de Blast.
Servidor de conexión de VMware Horizon View	Automático	Proporciona los servicios del agente de conexión. Este servicio siempre debe estar en ejecución. Al iniciar o detener este servicio, también se inician o se detienen los servicios web, de la puerta de enlace de seguridad, del bus de mensajería y del marco de trabajo. Este servicio no inicia ni detiene el servicio VMwareVDMDS ni el servicio del host de script de VMware Horizon View.
Componente de marco de trabajo VMware Horizon View	Manual	Proporciona servicios de registro de eventos, seguridad y marco de trabajo COM+. Este servicio siempre debe estar en ejecución.

Nombre del servicio	Tipo de inicio	Descripción
Componente de bus de mensajería VMware Horizon View	Manual	Proporciona servicios de mensajería entre los componentes de View. Este servicio siempre debe estar en ejecución.
Puerta de enlace segura PCoIP de VMware Horizon View	Manual	Proporciona servicios de la puerta de enlace segura de PCoIP. Este servicio debe ejecutarse si los clientes se conectan al servidor de conexión de View a través de la puerta de enlace segura de PCoIP.
VMware Horizon View Script Host	Deshabilitada	Proporciona compatibilidad para que los scripts de terceros se ejecuten cuando elimina máquinas virtuales. Este servicio está deshabilitado de forma predeterminada. Debe habilitar este servicio si desea ejecutar los scripts.
Componente de puerta de enlace de seguridad de VMware Horizon View	Manual	Proporciona servicios de puerta de enlace común. Este servicio siempre debe estar en ejecución.
Componente Web de VMware Horizon View	Manual	Proporciona servicios web. Este servicio siempre debe estar en ejecución.
VMwareVDMDS	Automático	Proporciona servicios del directorio LDAP. Este servicio siempre debe estar en ejecución. Durante las actualizaciones de View, este servicio asegura que los datos existentes se migren correctamente.

Servicios de un servidor de seguridad

La operación de View depende de varios dispositivos que se ejecutan en el servidor de seguridad.

Tabla 3-3. Servicios del servidor de seguridad

Nombre del servicio	Tipo de inicio	Descripción
Puerta de enlace segura de Blast VMware Horizon View	Automático	Proporciona servicios HTML Access y Blast Extreme seguros. Este servicio debe ejecutarse si los clientes se conectan a este servidor de seguridad a través de la puerta de enlace segura de Blast.
Servidor de seguridad de VMware Horizon View	Automático	Proporciona servicios del servidor de seguridad. Este servicio siempre debe estar en ejecución. Al iniciar o detener este servicio, también se inician o se detienen los servicios de la puerta de enlace de seguridad y el marco de trabajo.
Componente de marco de trabajo VMware Horizon View	Manual	Proporciona servicios de registro de eventos, seguridad y marco de trabajo COM+. Este servicio siempre debe estar en ejecución.

Nombre del servicio	Tipo de inicio	Descripción
Puerta de enlace segura PColP de VMware Horizon View	Manual	Proporciona servicios de la puerta de enlace segura de PColP. Este servicio debe ejecutarse si los clientes se conectan a este servidor de seguridad a través de la puerta de enlace segura de PColP.
Componente de puerta de enlace de seguridad de VMware Horizon View	Manual	Proporciona servicios de puerta de enlace común. Este servicio siempre debe estar en ejecución.

Configurar protocolos de seguridad y conjuntos de claves de cifrado en una instancia del servidor de conexión de View o en un servidor de seguridad

4

Puede configurar los protocolos de seguridad y los conjuntos de claves de cifrado que acepta el servidor de conexión de View. Puede definir una directiva de aceptación global que se aplique a todas las instancias del servidor de conexión de View en un grupo replicado, o bien puede definir una directiva de aceptación para instancias del servidor de conexión de View y servidores de seguridad individuales.

También puede configurar los protocolos de seguridad y los conjuntos de claves de cifrado que las instancias del servidor de conexión de View proponen al conectarse a vCenter Server y View Composer. Puede definir una directiva de propuesta global que se aplique a todas las instancias del servidor de conexión de View de un grupo replicado. No puede definir que se excluyan instancias individuales de una directiva de propuesta global.

Nota La configuración de seguridad del servidor de conexión de View no se aplica a la puerta de enlace segura de Blast (BSG). Debe configurar la seguridad de BSG por separado. Consulte [Capítulo 5 Configurar los protocolos de seguridad y los conjuntos de claves de cifrado para la puerta de enlace segura de Blast](#).

Los archivos de la directiva Unlimited Strength Jurisdiction (Jurisdicción de intensidad ilimitada) de Oracle se incluyen como estándares, permitiendo claves de 256 bits de forma predeterminada.

Este capítulo incluye los siguientes temas:

- [Directivas globales predeterminadas para los protocolos de seguridad y los conjuntos de claves de cifrado](#)
- [Configurar las directivas de propuesta y de aceptación globales](#)
- [Configurar directivas de aceptación en servidores individuales](#)
- [Configurar directivas de propuesta en escritorios remotos](#)
- [Cifrados y protocolos antiguos deshabilitados en View](#)

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.

Tabla 4-1. Directivas globales predeterminadas

Protocolos de seguridad predeterminados	Conjuntos de claves de cifrado predeterminados
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	■ TLS_RSA_WITH_AES_128_CBC_SHA
	■ TLS_RSA_WITH_AES_256_CBC_SHA

De forma predeterminada, los conjuntos de claves de cifrado GCM no están habilitados por motivos de rendimiento.

Configurar las directivas de propuesta y de aceptación globales

Las directivas de propuesta y de aceptación globales se definen en los atributos del LDAP de View. Estas directivas se aplican a todas las instancias del servidor de conexión de View y a los servidores de seguridad en un grupo replicado. Para cambiar una directiva global, puede editar el LDAP de View en cualquier instancia del servidor de conexión de View.

Cada directiva es un atributo de un solo valor en la siguiente ubicación del LDAP de View:
cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int

Directivas de propuesta y de aceptación globales definidas en el LDAP de View

Los atributos del LDAP de View que definen las directivas de propuesta y de aceptación globales se pueden editar.

Directivas de aceptación globales

La siguiente lista de atributos muestra los protocolos de seguridad. Para ordenar la lista, coloque el protocolo más reciente en primer lugar:

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

El siguiente atributo muestra los conjuntos de claves de cifrado. Este ejemplo muestra una lista abreviada:

```
pae-ServerSSLCipherSuites = \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```


El siguiente atributo controla la prioridad de los conjuntos de claves de cifrado. Normalmente, no es importante el orden del servidor de los conjuntos de claves de cifrado y se utiliza el del cliente. Para usar el orden de los conjuntos de claves de cifrado en su lugar, establezca el siguiente atributo:

```
pae-ServerSSLHonorClientOrder = 0
```

Directivas de propuesta globales

La siguiente lista de atributos muestra los protocolos de seguridad. Para ordenar la lista, coloque el protocolo más reciente en primer lugar:

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

El siguiente atributo muestra los conjuntos de claves de cifrado. Esta lista debe aparecer por orden de preferencia. Coloque el conjunto de claves de cifrado preferente en primer lugar, el siguiente en segundo lugar y sucesivamente. Este ejemplo muestra una lista abreviada:

```
pae-ClientSSLCipherSuites = \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Cambiar las directivas globales de propuesta y de aceptación

Para cambiar las directivas globales de propuesta y de aceptación para los conjuntos de claves de cifrado y los protocolos de seguridad, debe utilizar la utilidad Editor ADSI para editar los atributos del LDAP de View.

Requisitos previos

- Familiarícese con los atributos del LDAP de View que definen las directivas de propuesta y de aceptación. Consulte [Directivas de propuesta y de aceptación globales definidas en el LDAP de View](#).
- Visite el sitio web de Microsoft TechNet si desea obtener información sobre cómo utilizar la utilidad Editor ADSI en su versión del sistema operativo de Windows Server.

Procedimiento

- 1 Inicie la utilidad Editor ADSI en el equipo del servidor de conexión de View.
- 2 En el árbol de la consola, seleccione la opción **Conectar a**.
- 3 En el cuadro de texto para **seleccionar o escribir un nombre distinguido o el contexto de nomenclatura**, escriba el nombre distinguido **DC=vdi**, **DC=vmware**, **DC=int**.
- 4 En el cuadro de texto **Seleccione o escriba un dominio o servidor**, seleccione o escriba **localhost:389** o el nombre de dominio completo (FQDN) del equipo del servidor de conexión de View seguido del puerto 389.

Por ejemplo: **localhost:389** o **miequipo.midominio.com:389**

- 5 Amplíe el árbol del Editor ADSI y, a continuación, amplíe **OU=Properties**, seleccione **OU=Global** y, por último, seleccione **OU=Common** en el panel derecho.

- 6 En el objeto **CN=Common, OU=Global, OU=Properties**, seleccione los atributos que desee cambiar y escriba la nueva lista de los protocolos de seguridad o los conjuntos de claves de cifrado.
- 7 Reinicie el componente de puerta de enlace de seguridad de VMware Horizon View en cada instancia del servidor de conexión y el servidor de seguridad si modificó `pae-ServerSSLSecureProtocols`.

No es necesario que reinicie ningún servicio después de modificar `pae-ClientSSLSecureProtocols`.

Configurar directivas de aceptación en servidores individuales

Para especificar una directiva de aceptación local en un servidor de seguridad o una instancia del servidor de conexión, debe agregar propiedades al archivo `locked.properties`. Si el archivo `locked.properties` no existe aún en el servidor, debe crearlo.

Agregue una entrada `secureProtocols.n` en cada protocolo de seguridad que desee configurar. Use la siguiente sintaxis `secureProtocols.n=security_protocol`.

Agregue una entrada `enabledCipherSuite.n` en cada conjunto de claves de cifrado que desee configurar. Use la siguiente sintaxis `enabledCipherSuite.n=cipher_suite`.

La variable *n* es un número entero que debe agregar secuencialmente (1, 2, 3) en cada tipo de entrada.

Agregue una entrada `honorClientOrder` para controlar la prioridad de los conjuntos de claves de cifrado. Normalmente, no es importante el orden del servidor de los conjuntos de claves de cifrado y se utiliza el del cliente. Para usar el orden de los conjuntos de cifrado del servidor en su lugar, utilice la siguiente sintaxis:

```
honorClientOrder=false
```

Asegúrese de que las entradas del archivo `locked.properties` tengan la sintaxis correcta y los nombres del conjunto de claves de cifrado y los protocolos de seguridad estén escritos correctamente. Cualquier error en el archivo puede causar un error en la negociación entre el cliente y el servidor.

Procedimiento

- 1 Cree o edite el archivo `locked.properties` en la carpeta de configuración de la puerta de enlace SSL en el equipo del servidor de seguridad o del servidor de conexión.
Por ejemplo: `install_directory\VMware\VMware View\Server\sslgateway\conf\`
- 2 Agregue las entradas `secureProtocols.n` y `enabledCipherSuite.n`, incluidos los protocolos de seguridad asociados y los conjuntos de claves de cifrado.
- 3 Guarde el archivo `locked.properties`.
- 4 Reinicie el servicio del servidor de conexión VMware Horizon View o el servicio del servidor de seguridad VMware Horizon View para que se realicen los cambios.

Ejemplo: Directivas de aceptación predeterminadas en un servidor individual

El ejemplo siguiente muestra las entradas del archivo `locked.properties` que son necesarias para especificar las directivas predeterminadas:

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2
secureProtocols.2=TLSv1.1

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
enabledCipherSuite.4=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
enabledCipherSuite.5=TLS_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.6=TLS_RSA_WITH_AES_256_CBC_SHA

# Use the client's ordering of cipher suites (ignores the ordering given above):

honorClientOrder=true
```

Configurar directivas de propuesta en escritorios remotos

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

Asegúrese de que el servidor de conexión esté configurado para aceptar las mismas directivas, de forma que se puedan evitar errores de conexión.

Procedimiento

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

Cifrados y protocolos antiguos deshabilitados en View

Algunos cifrados y protocolos antiguos que ya no se consideran seguros se deshabilitan en View de forma predeterminada. Si es necesario, puede habilitarlos de forma manual.

Conjuntos de cifrado DHE

Si desea obtener más información, consulte <http://kb.vmware.com/kb/2121183>. Los conjuntos de cifrado que son compatibles con certificados DSA usan las claves efímeras Diffie-Hellman y, además, estos conjuntos ya no están habilitados de forma predeterminada desde la versión 6.2 de Horizon 6.

Para las instancias del servidor de conexión, los servidores de seguridad y los escritorios de View, puede habilitar estos conjuntos de cifrado editando la base de datos LDAP de View, el archivo `locked.properties` o el registro, tal como se describe en esta guía. Consulte [Cambiar las directivas globales de propuesta y de aceptación](#), [Configurar directivas de aceptación en servidores individuales](#) y [Configurar directivas de propuesta en escritorios remotos](#). Puede definir una lista de conjuntos de cifrado que incluyan uno o varios de los siguientes conjuntos, en este orden:

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (únicamente TLS 1.2, no FIPS)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (únicamente TLS 1.2, no FIPS)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (únicamente TLS 1.2)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (únicamente TLS 1.2)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

Para los equipos View Composer y View Agent Direct-Connection (VADC), puede habilitar los conjuntos de claves de cifrado DHE al agregar los siguientes valores a la lista de cifrados mientras realiza el procedimiento "Deshabilitar cifrados débiles en SSL/TLS para equipos View Composer y Horizon Agent" en el documento *Instalación de View*.

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

Nota No es posible habilitar la compatibilidad con certificados ECDSA. Estos certificados nunca se admitieron.

SSLv3

En Horizon 7, se eliminó la versión 3.0 de SSL.

Si desea obtener más información, consulte <http://tools.ietf.org/html/rfc7568>.

RC4

Si desea obtener más información, consulte <http://tools.ietf.org/html/rfc7465>.

Para las instancias del servidor de conexión, los servidores de seguridad y los escritorios de View, puede habilitar RC4 en el servidor de conexión, el servidor de seguridad o el equipo de Horizon Agent editando el archivo de configuración `C:\Program Files\VMware\VMware View\Server\jre\lib\security\jdk.tls.legacyAlgorithms`. Al final del archivo, se encuentra una entrada multilínea denominada `jdk.tls.legacyAlgorithms`. Elimine de la entrada `RC4_128` y la coma que aparece a continuación y reinicie el servidor de conexión, el servidor de seguridad o el equipo de Horizon Agent, dependiendo del caso.

Para los equipos View Composer y View Agent Direct-Connection (VADC), puede habilitar RC4 al agregar los siguientes valores a la lista de cifrados mientras realiza el procedimiento "Deshabilitar cifrados débiles en SSL/TLS para equipos View Composer y Horizon Agent" en el documento *Instalación de View*.

```
TLS_RSA_WITH_RC4_128_SHA
```

TLS 1.0

En Horizon 7, TLS 1.0 está deshabilitado de forma predeterminada.

Para obtener más información, consulte https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf y <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>. Para obtener instrucciones sobre cómo habilitar TLS 1.0, consulte las secciones "Habilitar TLSv1 en las conexiones vCenter del servidor de conexión" y "Habilitar TLSv1 en las conexiones ESXi y vCenter de View Composer" en el documento *Actualizaciones de View*.

Configurar los protocolos de seguridad y los conjuntos de claves de cifrado para la puerta de enlace segura de Blast

5

La configuración de seguridad del servidor de conexión de View no se aplica a la puerta de enlace segura de Blast (BSG). Debe configurar la seguridad de BSG por separado.

Este capítulo incluye los siguientes temas:

- [Configurar los protocolos de seguridad y los conjuntos de claves de cifrado para la puerta de enlace segura de Blast \(BSG\)](#)

Configurar los protocolos de seguridad y los conjuntos de claves de cifrado para la puerta de enlace segura de Blast (BSG)

Para configurar los protocolos de seguridad y los conjuntos de claves de cifrado que el agente de escucha del lado cliente de la BSG acepta, edite el archivo `absg.properties`.

Los protocolos permitidos son, de menor a mayor, `tls1.0`, `tls1.1` y `tls1.2`. No se admiten protocolos más antiguos como `SSLv3` y versiones anteriores. Dos propiedades, `localHttpsProtocolLow` y `localHttpsProtocolHigh`, determinan el rango de los protocolos que aceptará el agente de escucha BSG. Por ejemplo, configurar `localHttpsProtocolLow=tls1.0` y `localHttpsProtocolHigh=tls1.2` hará que el agente de escucha acepte `tls1.0`, `tls1.1` y `tls1.2`. Las opciones predeterminadas son `localHttpsProtocolLow=tls1.1` y `localHttpsProtocolHigh=tls1.2`. Puede examinar el archivo `absg.log` de BSG para detectar los valores que se ejecutan en una instancia de BSG específica.

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 En la instancia del servidor de conexión, edite el archivo *install_directory\VMware\VMware View\Server\appblastgateway\absg.properties*.

De forma predeterminada, el directorio de instalación es *%ProgramFiles%*.

- 2 Edite las propiedades `localHttpsProtocolLow` y `localHttpsProtocolHigh` para especificar un rango de protocolos.

Por ejemplo,

```
localHttpsProtocolLow=tls1.0  
localHttpsProtocolHigh=tls1.2
```

Para habilitar un solo protocolo, especifique el mismo protocolo para `localHttpsProtocolLow` y `localHttpsProtocolHigh`.

- 3 Edite la propiedad `localHttpsCipherSpec` para especificar una lista de conjuntos de claves de cifrado.

Por ejemplo,

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

- 4 Reinicie la puerta de enlace segura de Blast de VMware HorizonView del servicio de Windows.

Implementar dispositivos USB en un entorno de Horizon 7 seguro

6

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

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

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

Este capítulo incluye los siguientes temas:

- [Deshabilitar el redireccionamiento USB en todos los tipos de dispositivos](#)
- [Deshabilitar el redireccionamiento USB de dispositivos específicos](#)

Deshabilitar el redireccionamiento USB en todos los tipos de dispositivos

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

Use la estrategia más adecuada según su situación:

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

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

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

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

Tabla 6-1. Efecto de combinar las directivas de exclusión de todos los dispositivos

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

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

Estas directivas se incluyen en el archivo de plantilla ADMX de la configuración de Horizon Agent (`vdm_agent.admx`). Para obtener más información, consulte "Configuración USB en la plantilla ADMX de configuración de Horizon Agent" en *Configurar funciones de escritorios remotos en Horizon 7*.

Deshabilitar el redireccionamiento USB de dispositivos específicos

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

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

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

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

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

<code>ExcludeAllDevices</code>	<code>Enabled</code>
<code>IncludeVidPid</code>	<code>o:vid-0123_pid-abcd</code>

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

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

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

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

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

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

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

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

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

Estas directivas se incluyen en el archivo de plantilla ADMX de la configuración de Horizon Agent (`vdm_agent.admx`). Si desea obtener más información, consulte *Configurar funciones de escritorios remotos en Horizon 7*.

Medidas de protección HTTP en los servidores de conexión y de seguridad

7

Horizon 7 emplea ciertas medidas para proteger la comunicación que usa el protocolo HTTP.

Este capítulo incluye los siguientes temas:

- [Estándares del Grupo de trabajo de ingeniería de Internet](#)
- [Estándares del Consorcio World Wide Web](#)
- [Otras medidas de protección](#)
- [Configurar las medidas de protección HTTP](#)

Estándares del Grupo de trabajo de ingeniería de Internet

El servidor de conexión y el servidor de seguridad cumplen algunos estándares del Grupo de trabajo de ingeniería de Internet (IETF).

- La seguridad de la capa de transporte (TLS) RFC 5746: extensión de la indicación de renegociación, también conocida como renegociación segura, está habilitada de forma predeterminada.

Nota La renegociación iniciada por el cliente está deshabilitada de forma predeterminada en los servidores de conexión y de seguridad. Para habilitarla, edite el valor de registro [HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions y elimine `-Djdk.tls.rejectClientInitiatedRenegotiation=true` de la cadena.

- La seguridad de transporte estricta con HTTP RFC 6797 (HSTS), también conocida como seguridad de transporte, está habilitada de forma predeterminada. No se puede deshabilitar esta opción.
- Las opciones del marco X del campo del encabezado HTTP RFC7034, también conocidas como secuestro de clic de contadores, están habilitadas de forma predeterminada. Para deshabilitarlas, agregue la entrada `x-frame-options=OFF` al archivo `locked.properties`. Para obtener más información sobre cómo agregar propiedades al archivo `locked.properties`, consulte [Configurar las medidas de protección HTTP](#).

Nota En versiones anteriores a la 7.2 de Horizon 7, si esta opción cambiaba, no afectaba a las conexiones de HTML Access.

- La comprobación del origen RFC 6454, que ofrece protección contra la falsificación de solicitud en sitios cruzados, está habilitada de forma predeterminada. Para deshabilitarla, agregue la entrada `checkOrigin=false` a `locked.properties`. Si desea obtener más información, consulte [Compartir recursos de distintos orígenes](#).

Nota En versiones anteriores, esta protección estaba deshabilitada de forma predeterminada.

Estándares del Consorcio World Wide Web

El servidor de conexión y el servidor de seguridad cumplen con algunos estándares del Consorcio World Wide Web (W3C).

- La opción para compartir recursos de distintos orígenes (CORS), que limita las solicitudes de distintos orígenes del cliente, está habilitada de forma predeterminada. Para deshabilitarla, agregue la entrada `enableCORS=false` a `locked.properties`.
- La directiva de seguridad de contenido (CSP), que reduce un gran número de vulnerabilidades de inserción de contenido, está habilitada de forma predeterminada. Para deshabilitarla, agregue la entrada `enableCSP=false` a `locked.properties`.

Compartir recursos de distintos orígenes

La función para compartir recursos de distintos orígenes (CORS) regula las solicitudes de diferentes orígenes del cliente. Para ello, proporciona declaraciones de directivas al cliente a demanda y comprueba que cumplen la directiva. Esta función está habilitada de forma predeterminada.

Las directivas incluyen el conjunto de métodos HTTP que se aceptan, los posibles orígenes de las solicitudes y los tipos de contenido válidos. Estos varían en función de la URL de solicitud y se pueden reconfigurar según sea necesario. Para ello, agregue entradas a `locked.properties`.

Los puntos suspensivos después de un nombre de propiedad indican que esta puede aceptar una lista.

Tabla 7-1. Propiedades CORS

Propiedad	Tipo de valor	Principal predeterminado	Otros valores predeterminados
<code>enableCORS</code>	<code>true</code> <code>false</code>	<code>true</code>	n/a
<code>acceptContentType...</code>	<code>http-content-type</code>	<code>application/x-www-form-urlencoded,application/xml,text/xml</code>	<ul style="list-style-type: none"> ■ <code>admin=application/x-amf</code> ■ <code>helpdesk=application/json,application/text,application/x-www-form-urlencoded</code> ■ <code>view-vlsi-rest=application/json</code>
<code>acceptHeader...</code>	<code>http-header-name</code>	*	n/a
<code>exposeHeader...</code>	<code>http-header-name</code>	*	n/a

Propiedad	Tipo de valor	Principal predeterminado	Otros valores predeterminados
filterHeaders	true false	true	n/a
checkOrigin	true false	true	n/a
allowCredentials	true false	false	admin=true broker=true helpdesk=true misc=true portal=true saml=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET, HEAD, POST	misc=GET, HEAD saml=GET, HEAD
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	OFF	n/a

Ejemplo de propiedades CORS del archivo `locked.properties`:

```
enableCORS = true
allowPreflight = true
checkOrigin = true
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

Comprobación del origen

La comprobación del origen está habilitada de forma predeterminada. Cuando está habilitada, se aceptan solicitudes sin origen o con un origen igual a la dirección proporcionada en la URL externa, la dirección `balancedHost`, cualquier dirección `portalHost`, cualquier hash `chromeExtension`, `null` o `localhost`. Si el origen no es una de estas posibilidades, se registra el error "Origen inesperado" y devuelve el estado 404.

Si varios servidores de conexión o servidores de seguridad tienen la carga equilibrada, debe especificar la dirección del equilibrador de carga agregando una entrada `balancedHost` a `locked.properties`. Se supone que en esta dirección el puerto es el 443.

Si los clientes necesitan conectarse a través de Unified Access Gateway u otra puerta de enlace, debe especificar todas las direcciones de puerta de enlace. Para ello, agregue entradas `portalHost` a `locked.properties`. Se supone que en estas direcciones el puerto también es el 443. Realice la misma acción si desea proporcionar acceso a un servidor de conexión o a un servidor de seguridad con un nombre diferente del especificado en la URL externa.

Los clientes de la extensión de Chrome asignan su origen inicial a su propia identidad. Para que las conexiones se realicen correctamente, agregue una entrada `chromeExtension` a `locked.properties` para registrar la extensión.

Directiva de seguridad de contenido

La función de la directiva de seguridad de contenido (CSP) reduce un gran número de vulnerabilidades de inserción de contenido, como la creación de scripts entre sitios (XSS), con directivas para los navegadores compatibles. Esta función está habilitada de forma predeterminada. Puede agregar entradas a `locked.properties` para reconfigurar las directivas.

Tabla 7-2. Propiedades CSP

Propiedad	Tipo de valor	Principal predeterminado	Otros valores predeterminados
<code>enableCSP</code>	<code>true</code> <code>false</code>	<code>true</code>	n/a
<code>content-security-policy</code>	<code>directives-list</code>	<code>default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data::style-src 'self' 'unsafe-inline';font-src 'self' data:</code>	<code>portal=child-src 'self' blob::default-src 'self';connect-src 'self' wss::font-src 'self' data:;img-src 'self' data: blob::media-src 'self' blob::object-src 'self' blob::script-src 'self' 'unsafe-inline' 'unsafe-eval' data::style-src 'self' 'unsafe-inline';frame-ancestors 'self'</code>
<code>x-frame-options</code>	<code>OFF</code> specification	<code>deny</code>	<code>portal=sameorigin</code>
<code>x-content-type-options</code>	<code>OFF</code> specification	<code>nosniff</code>	n/a
<code>x-xss-protection</code>	<code>OFF</code> specification	<code>1; mode=block</code>	n/a

Puede agregar propiedades CSP al archivo `locked.properties`. Propiedades CSP de ejemplo:

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' data:
content-security-policy-portal = default-src 'self';frame-ancestors 'self'
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

Otras medidas de protección

Además de los estándares del Grupo de trabajo de ingeniería de Internet y de W3, Horizon 7 emplea otras medidas para proteger la comunicación que usa el protocolo HTTP.

Reducir los riesgos de seguridad de tipo MIME

De forma predeterminada, Horizon 7 envía el encabezado `x-content-type-options: nosniff` en sus respuestas HTTP para ayudar a evitar ataques basados en la confusión de tipo MIME.

Puede deshabilitar esta función agregando la siguiente entrada al archivo `locked.properties`:

```
x-content-type-options=OFF
```

Disminuir ataques de scripts de sitios

De forma predeterminada, Horizon 7 emplea el filtro de script de sitios (XSS) para disminuir los ataques de scripts de sitios al enviar el encabezado `x-xss-protection=1; mode=block` en sus respuestas HTTP.

Puede deshabilitar esta función agregando la siguiente entrada al archivo `locked.properties`:

```
x-xss-protection=OFF
```

Comprobar el tipo de contenido

De forma predeterminada, Horizon 7 acepta solicitudes solamente con los siguientes tipos de contenidos declarados:

- `application/x-www-form-urlencoded`
- `application/xml`
- `text/xml`

Nota En versiones anteriores, esta protección estaba deshabilitada de forma predeterminada.

Para restringir los tipos de contenidos que View acepta, agregue la siguiente entrada al archivo `locked.properties`:

```
acceptContentType.1=content-type
```


Por ejemplo:

```
acceptContentType.1=x-www-form-urlencoded
```

Para aceptar otro tipo de contenido, agregue la entrada `acceptContentType.2=content-type`.

Para aceptar solicitudes con cualquier tipo de contenido declarado, especifique `acceptContentType=*`.

Nota En versiones anteriores a la 7.2 de Horizon 7, no afecta a las conexiones de Horizon Administrator si cambia esta lista.

Supervisión de protocolo de enlace

Los protocolos de enlace TLS del puerto 443 deben completarse en un periodo de tiempo configurable; de lo contrario, se forzará su cierre. De forma predeterminada, este periodo es 10 segundos. Si se habilita la autenticación con tarjeta inteligente, los protocolos de enlace TLS del puerto 443 podrán completarse en 100 segundos.

Si es necesario, puede ajustar el tiempo de los protocolos de enlace TLS del puerto 443. Para ello, agregue la siguiente propiedad al archivo `locked.properties`:

```
handshakeLifetime = lifetime_in_seconds
```

Por ejemplo:

```
handshakeLifetime = 20
```

De forma opcional, el cliente responsable de un protocolo de enlace TLS que se ejecute en exceso puede agregarse automáticamente a una lista negra. Las conexiones nuevas de los clientes que estén en una lista negra se retrasan durante un periodo de tiempo configurable antes de que se procesen para dar prioridad a otros clientes. Para habilitar esta función, agregue la siguiente propiedad al archivo `locked.properties`:

```
secureHandshakeDelay = delay_in_milliseconds
```

Por ejemplo:

```
secureHandshakeDelay = 2000
```

Para que las conexiones HTTPS no se agreguen a una lista negra, elimine la entrada `secureHandshakeDelay` o asígnele el valor 0.

La dirección IP de un cliente que tiene un comportamiento erróneo se agrega a la lista negra durante un periodo de tiempo mínimo igual a la suma de `handshakeLifetime` y `secureHandshakeDelay`.

Tomando como ejemplo los valores anteriores, el período mínimo para la dirección IP de un cliente que tiene un comportamiento erróneo es de 22 segundos.

```
(20 * 1000) + 2000 = 22 seconds
```

El período mínimo se amplía cada vez que una conexión de la misma dirección IP tenga un comportamiento erróneo. La dirección IP se elimina de la lista negra después de que caduque el periodo mínimo y de que se procese la última conexión que se retrasó desde esa dirección IP.

La ejecución en exceso de un protocolo de enlace TLS no es la única razón para añadir un cliente a la lista negra. Otros motivos son las series de conexiones abandonadas o las series de solicitudes que acaban en error (por ejemplo, varios intentos de acceso a URL que no existen). Estos activadores tienen diferentes periodos mínimos para agregarse a una lista negra. Para ampliar la supervisión de estos activadores adicionales al puerto 80, agregue la siguiente entrada al archivo `locked.properties`:

```
insecureHandshakeDelay = delay_in_milliseconds
```

Por ejemplo:

```
insecureHandshakeDelay = 1000
```

Para que las conexiones HTTP no se agreguen a una lista negra, elimine la entrada `insecureHandshakeDelay` o asígnele el valor 0.

Listas blancas de agentes de usuarios

Establezca una lista blanca para restringir los agentes de usuarios que pueden interactuar con Horizon 7. De forma predeterminada, se aceptan todos los agentes de usuarios.

Nota Esto no es estrictamente una función de seguridad. La detección de los agentes de usuarios se basa en el encabezado de la solicitud de agente de usuarios proporcionada por el cliente o navegador que se conecta, que pueden ser falsos. Algunos navegadores permiten que los usuarios modifiquen el encabezado de la solicitud.

Los agentes de usuarios se especifican por su nombre y una versión mínima. Por ejemplo:

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

Esto significa que solo la versión 14 y posteriores de Google Chrome y la 5.1 y posteriores de Safari se pueden conectar mediante HTML Access. Todos los navegadores pueden conectarse a otros servicios.

Puede introducir los siguientes nombres de agentes de usuarios reconocidos:

- Android
- Chrome
- Edge
- Internet Explorer
- Firefox
- Opera

- Safari

Nota Algunos de estos agentes de usuarios no son compatibles con Horizon 7. Estos son solo ejemplos.

Configurar las medidas de protección HTTP

Para configurar las medidas de protección HTTP, debe crear o editar el archivo `locked.properties` en la carpeta de configuración de la puerta de enlace SSL en la instancia del servidor de seguridad o el servidor de conexión.

Por ejemplo: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- Utilice la siguiente sintaxis para configurar una propiedad en `locked.properties`:

```
myProperty = newValue
```

- El nombre de la propiedad siempre distingue entre mayúsculas y minúsculas y el valor puede hacerlo también. El espacio en blanco alrededor del signo `=` es opcional.
- Para las propiedades CORS y CSP, es posible establecer valores específicos del servicio, así como un valor principal. Por ejemplo, el servicio de administración se encarga de administrar las solicitudes de Horizon Administrator y es posible asignar una propiedad a este servicio sin que afecte a otros. Para ello, agregue `-admin` después del nombre de propiedad.

```
myProperty-admin = newValueForAdmin
```

- Si se especifican un valor principal y otro específico del servicio, se aplica el valor específico a ese servicio y el principal, al resto. La única excepción es el valor especial "OFF" (Desactivado). Si se asigna el valor principal "OFF" (Desactivado) a la propiedad, se ignoran todos los valores específicos del servicio para esta propiedad.

Por ejemplo:

```
myProperty = OFF
myProperty-admin = newValueForAdmin ; ignored
```

- Algunas propiedades aceptan una lista de valores.

Para establecer un valor único, introduzca la siguiente propiedad:

```
myProperty = newValue
myProperty-admin = newValueForAdmin
```

Para asignar varios valores a una propiedad que acepta valores de una lista, especifique cada valor en una línea distinta:

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- Para determinar el nombre del servicio correcto que desee usar cuando realice una configuración específica del servicio, busque líneas que contengan la siguiente secuencia en los registros de depuración:

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

En este ejemplo, el nombre del servicio es `admin`. Puede utilizar los siguientes nombres de servicio comunes:

- `admin` para Horizon Administrator
- `broker` para el servidor de conexión
- `docroot` para servidores de archivos locales
- `helpdesk` para el departamento de soporte técnico
- `portal` para HTML Access
- `saml` para la comunicación SAML (vIDM)
- `tunnel` para el túnel seguro
- `view-vlsi` para la API de View
- `misc` para otros servicios