

Instalación de Horizon 7

MARZO DE 2020

VMware Horizon 7 7.12



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 © 2011-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Instalación de Horizon 7 8

1 Requisitos del sistema para componentes del servidor 9

- Requisitos del servidor de conexión de Horizon 9
 - Requisitos de hardware para el servidor de conexión de Horizon 10
 - Sistemas operativos compatibles con el servidor de conexión de Horizon 10
 - Requisitos del software de virtualización para el servidor de conexión de Horizon 11
 - Requisitos de red de las instancias replicadas del servidor de conexión de Horizon 11
- Requisitos de Horizon Administrator 11
- Requisitos de Horizon Console 12
- Requisitos de View Composer 13
 - Sistemas operativos compatibles con View Composer 13
 - Requisitos de hardware para un View Composer independiente 14
 - Requisitos de base de datos para View Composer y para bases de datos de eventos 15

2 Requisitos del sistema para sistemas operativos invitados 16

- Requisitos y consideraciones para Horizon Agent 16
- Sistemas operativos compatibles con Standalone Horizon Persona Management 17
- Compatibilidad del software y protocolo de visualización remota 17
 - PCoIP 18
 - Microsoft RDP 20
 - VMware Blast Extreme 21

3 Instalar Horizon 7 en un entorno IPv6 26

- Configurar Horizon 7 en un entorno IPv6 26
- Versiones de Active Directory, de base de datos y de vSphere admitidas en un entorno IPv6 27
- Sistemas operativos compatibles con Horizon 7 Servers en un entorno IPv6 27
- Sistemas operativos Windows compatibles con hosts RDS y escritorios en un entorno IPv6 28
- Clientes admitidos en un entorno IPv6 28
- Protocolos de comunicación remota admitidos en un entorno IPv6 29
- Tipos de autenticación admitidos en un entorno IPv6 29
- Otras funciones admitidas en un entorno IPv6 29

4 Instalar Horizon 7 en modo FIPS 32

- Información general sobre la configuración de Horizon 7 en modo FIPS 32
- Requisitos del sistema para el modo FIPS 33

5 Preparar Active Directory 35

Configurar dominios y relaciones de confianza	36
Relaciones de confianza y filtros de dominio	37
Crear una OU para los escritorios remotos	37
Crear OU y grupos para cuentas cliente en modo de pantalla completa	38
Crear grupos para usuarios	38
Crear una cuenta de usuario para vCenter Server	38
Crear una cuenta de usuario para un servidor View Composer independiente	39
Crear una cuenta de usuario para operaciones en AD de View Composer	39
Crear una cuenta de usuario para operaciones de clones instantáneos	40
Configurar la directiva Grupos restringidos	41
Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7	42
Preparar Active Directory para la autenticación con tarjeta inteligente	43
Agregar UPN para usuarios de tarjetas inteligentes	43
Agregar el certificado raíz a las entidades de certificación raíz de confianza	44
Agregar un certificado intermedio a las entidades de certificación intermedias	45
Agregar el certificado raíz al almacén Enterprise NTAAuth	46
Deshabilitar cifrados débiles en SSL/TLS	47

6 Instalar View Composer 48

Preparar una base de datos de View Composer	48
Crear una base de datos SQL Server para View Composer	49
Crear una base de datos de Oracle para View Composer	54
Configurar un certificado SSL para View Composer	58
Instalar el servicio de View Composer	59
Habilitar TLSv1.0 en vCenter y conexiones ESXi desde View Composer	61
Configurar la infraestructura de View Composer	62
Configurar el entorno de vSphere para View Composer	62
Prácticas recomendadas adicionales para View Composer	63

7 Instalar el servidor de conexión de Horizon 64

Instalar el software del servidor de conexión de Horizon	64
Requisitos de instalación del servidor de conexión de Horizon	65
Instalar el servidor de conexión de Horizon con una nueva configuración	66
Instalar el servidor de conexión de Horizon de forma silenciosa	70
Propiedades de instalación silenciosa para una instalación estándar del servidor de conexión de Horizon	72
Habilitar TLSv1.0 en conexiones de vCenter desde el servidor de conexión	73
Instalar una instancia replicada del servidor de conexión de Horizon	74
Instalar una instancia replicada del servidor de conexión de Horizon de forma silenciosa	78
Propiedades de instalación silenciosa para una instancia replicada del servidor de conexión de Horizon	81
Configurar una contraseña de emparejamiento para el servidor de seguridad	82

Instalar un servidor de seguridad	83
Instalar un servidor de seguridad de forma silenciosa	87
Propiedades de instalación silenciosa para un servidor de seguridad	89
Eliminar las reglas IPsec del servidor de seguridad	91
Ventajas de los dispositivos Unified Access Gateway sobre la VPN	92
Reglas de firewall para el servidor de conexión de Horizon	94
Configurar que un firewall back-end admita IPsec	95
Volver a instalar el servidor de conexión de Horizon con una configuración de seguridad	96
Opciones de la línea de comandos de Microsoft Windows Installer	98
Desinstalar los componentes de Horizon 7 de forma silenciosa con las opciones de la línea de comandos MSI	101

8 Configurar los certificados TLS de los servidores de Horizon 7 103

Comprender los certificados TLS para Horizon 7 Server	104
Información general de las tareas para configurar certificados TLS	105
Obtener un certificado TLS firmado de una CA	107
Obtener un certificado firmado por una CA empresarial o de dominio de Windows	108
Configurar el servidor de conexión de Horizon, el servidor de seguridad o View Composer para usar un nuevo certificado TLS	109
Agregar el complemento Certificado a MMC	110
Importar un certificado del servidor SSL a un almacén de certificados de Windows	110
Modificar el Nombre descriptivo del certificado	112
Importar un certificado raíz e intermedios al almacén de certificados de Windows	112
Enlazar un nuevo certificado TLS al puerto usado por View Composer	114
Configurar endpoints cliente para confiar en el certificado raíz y los intermedios	115
Configurar Horizon Client para Mac para confiar en el certificado raíz y los intermedios	117
Configurar Horizon Client para iOS para confiar en el certificado raíz y los intermedios	117
Configurar la comprobación de la revocación de los certificados del servidor	118
Configurar la puerta de enlace segura de PCoIP para usar un nuevo certificado TLS	119
Verificar que el nombre del servidor coincida con el nombre del sujeto del certificado de la PSG	121
Configurar un certificado PSG en el almacén de certificados de Windows	121
Establecer el nombre descriptivo del certificado PSG en el Registro de Windows	123
Forzar el uso de un certificado firmado por una CA para las conexiones al PSG	124
Configurar Horizon Administrator para que confíe en un certificado de View Composer o de vCenter Server	125
Beneficios de usar certificados TLS firmados por una CA	125
Solucionar problemas de los certificados en el servidor de conexión de Horizon y el servidor de seguridad	126

9 Configurar Horizon 7 por primera vez 128

Configurar cuentas de usuario para vCenter Server, View Composer y clones instantáneos	128
Dónde utilizar el usuario de vCenter Server y los usuarios de View Composer	129

Configurar un usuario de vCenter Server para Horizon 7 y View Composer	129
Privilegios necesarios para el usuario de vCenter Server	131
Privilegios de clones instantáneos y View Composer necesarios para el usuario de vCenter Server	132
Configurar el servidor de conexión de Horizon por primera vez	134
Horizon Administrator y el servidor de conexión de Horizon	134
Iniciar sesión en Horizon Administrator	135
Instalar la clave de licencia del producto	136
Agregar instancias de vCenter Server a Horizon 7	137
Configurar las opciones de View Composer	139
Configurar los dominios de View Composer	140
Agregar un administrador de dominio de clones instantáneos	141
Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados	142
Configurar el acelerador de almacenamiento de View para vCenter Server	143
Límites de operaciones simultáneas para vCenter Server y View Composer	145
Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto	146
Aceptar la huella digital de un certificado TLS predeterminado	147
Configurar conexiones de Horizon Client	149
Configurar la puerta de enlace segura PCoIP y las conexiones de túnel seguro	150
Configurar la puerta de enlace segura Blast	151
Configurar URL externas para conexiones seguras de puerta de enlace y túnel.	153
Configurar las URL externas de una instancia del servidor de conexión	154
Modificar las URL externas de un servidor de seguridad	155
Otorgar preferencia a nombres DNS cuando el servidor de conexión de Horizon devuelve información de direcciones	157
Permitir HTML Access a través de un equilibrador de carga	158
Permitir HTML Access a través de una puerta de enlace	158
Reemplazar los puertos predeterminados para los servicios de Horizon 7	159
Reemplazar las NIC o los puertos HTTP predeterminados para las instancias del servidor de conexión de Horizon y los servidores de seguridad	159
Reemplazar los puertos predeterminados o las NIC para la puerta de enlace segura PCoIP en las instancias del servidor de conexión de Horizon y en los servidores de seguridad	161
Reemplazar el puerto de control predeterminado para la puerta de enlace segura PCoIP en las instancias del servidor de conexión y en los servidores de seguridad	162
Reemplazar el puerto predeterminado para View Composer	163
Cambiar el número de puerto para el redireccionamiento HTTP al servidor de conexión	164
Evitar el redireccionamiento HTTP para las conexiones cliente al servidor	165
Habilitar el acceso remoto para los contadores de rendimiento de Horizon 7 en los servidores de conexión	165
Configuración de tamaño de Windows Server para admitir la implementación	166
Cambiar el tamaño de la memoria del servidor de conexión de Horizon	166
Configurar las opciones de los archivos de paginación del sistema	167

10 Configurar informes de eventos 168

[Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7](#) 168

[Preparar una base de datos SQL Server para los informes de eventos](#) 169

[Configurar la base de datos de eventos](#) 170

[Configurar el registro de eventos para servidores Syslog](#) 172

Instalación de Horizon 7

Instalación de Horizon 7 explica cómo instalar el servidor y los componentes cliente de VMware Horizon[®] 7.

Público al que se dirige

Este documento está dirigido a cualquier persona que desee instalar VMware Horizon 7. La información está escrita para administradores de sistemas Linux o Windows que están familiarizados con la tecnología de máquinas virtuales y operaciones de los centros de datos.

Requisitos del sistema para componentes del servidor

1

Los hosts que ejecuten componentes de Horizon 7 Server deben cumplir requisitos de software y hardware específicos.

Este capítulo incluye los siguientes temas:

- [Requisitos del servidor de conexión de Horizon](#)
- [Requisitos de Horizon Administrator](#)
- [Requisitos de Horizon Console](#)
- [Requisitos de View Composer](#)

Requisitos del servidor de conexión de Horizon

El servidor de conexión de Horizon actúa como un agente para las conexiones cliente al autenticar y, a continuación, dirigir las solicitudes de los usuarios a las aplicaciones y los escritorios remotos apropiados. El servidor de conexión de Horizon tiene requisitos específicos de hardware, de sistema operativo, de instalación y de software admitido.

- [Requisitos de hardware para el servidor de conexión de Horizon](#)

Debe instalar todos los tipos de instalaciones del servidor de conexión de Horizon, incluidas las instalaciones estándar, réplica, del servidor de seguridad y del servidor de inscripciones, en una máquina virtual o en un equipo físico dedicados que cumplan los requisitos específicos de hardware.
- [Sistemas operativos compatibles con el servidor de conexión de Horizon](#)

Debe instalar el servidor de conexión de Horizon en un sistema operativo Windows Server compatible.
- [Requisitos del software de virtualización para el servidor de conexión de Horizon](#)

El servidor de conexión de Horizon requiere algunas versiones del software de virtualización de VMware.

■ Requisitos de red de las instancias replicadas del servidor de conexión de Horizon

Al instalar instancias replicadas del servidor de conexión de Horizon, normalmente debe configurarlas en la misma ubicación física y conectarlas a una red LAN de alto rendimiento. De lo contrario, los problemas de latencia podrían provocar inconsistencias en las configuraciones LDAP de View de las instancias del servidor de conexión de Horizon. Si la configuración de una instancia del servidor de conexión de Horizon no está actualizada, es posible que se rechace el acceso del usuario cuando este se conecta.

Requisitos de hardware para el servidor de conexión de Horizon

Debe instalar todos los tipos de instalaciones del servidor de conexión de Horizon, incluidas las instalaciones estándar, réplica, del servidor de seguridad y del servidor de inscripciones, en una máquina virtual o en un equipo físico dedicados que cumplan los requisitos específicos de hardware.

Tabla 1-1. Requisitos de hardware del servidor de conexión de Horizon

Componente de hardware	Obligatorio	Recomendado
Procesador	Procesador Pentium IV de 2 GHz o superior	4 CPU
Adaptador de red	NIC de 100 Mbps	NIC de 1 Gbps
Memoria Windows Server 2008 R2 de 64 bits	4 GB de RAM o superior	Al menos 10 GB de RAM o superior para implementaciones de 50 o más escritorios remotos
Memoria Windows Server 2012 R2 de 64 bits	4 GB de RAM o superior	Al menos 10 GB de RAM o superior para implementaciones de 50 o más escritorios remotos

Estos requisitos también se aplican a las instancias del servidor de conexión de Horizon de réplica y del servidor de seguridad que instala para obtener alta disponibilidad o acceso externo.

Importante La máquina virtual o el equipo físico que aloje el servidor de conexión de Horizon debe tener una dirección IP que no cambie. En un entorno IPv4, configure una dirección IP estática. En un entorno IPv6, los equipos obtienen automáticamente direcciones IP que no cambian.

Sistemas operativos compatibles con el servidor de conexión de Horizon

Debe instalar el servidor de conexión de Horizon en un sistema operativo Windows Server compatible.

Los siguientes sistemas operativos admiten todos los tipos de instalación del servidor de conexión de Horizon, incluidas las instalaciones del servidor de seguridad, de réplica y estándar.

Tabla 1-2. Sistemas operativos compatibles con el servidor de conexión de Horizon

Sistema operativo	Versión	Edición
Windows Server 2008 R2 SP1	64 bits	Standard Enterprise Datacenter
Windows Server 2012 R2	64 bits	Standard Datacenter
Windows Server 2016	64 bits	Standard Datacenter
Windows Server 2019	64 bits	Standard Datacenter

Nota Ya no se admite Windows Server 2008 R2 sin Service Pack.

Requisitos del software de virtualización para el servidor de conexión de Horizon

El servidor de conexión de Horizon requiere algunas versiones del software de virtualización de VMware.

Si usa vSphere, debe usar una versión compatible de host ESXi/vSphere ESX y de vCenter Server.

Si desea obtener más detalles sobre las versiones de Horizon que son compatibles con las versiones de vCenter Server y ESXi, consulte Matrices de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Requisitos de red de las instancias replicadas del servidor de conexión de Horizon

Al instalar instancias replicadas del servidor de conexión de Horizon, normalmente debe configurarlas en la misma ubicación física y conectarlas a una red LAN de alto rendimiento. De lo contrario, los problemas de latencia podrían provocar inconsistencias en las configuraciones LDAP de View de las instancias del servidor de conexión de Horizon. Si la configuración de una instancia del servidor de conexión de Horizon no está actualizada, es posible que se rechace el acceso del usuario cuando este se conecta.

Importante Para utilizar un grupo de instancias replicadas del servidor de conexión a través de una WAN, una MAN (red de área metropolitana) u otras redes que no sean LAN, en escenarios en los que una implementación de Horizon debe abarcar centros de datos, debe utilizar la función Arquitectura de Cloud Pod. Para obtener más información, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

Requisitos de Horizon Administrator

Los administradores utilizan Horizon Administrator para configurar Horizon Connection Server, implementar y administrar aplicaciones y escritorios remotos, controlar la autenticación de usuario, iniciar

y examinar eventos del sistema, y realizar actividades analíticas. Los sistemas cliente que ejecutan Horizon Administrator deben cumplir determinados requisitos.

Horizon Administrator es una aplicación basada en Web que se instala con el servidor de conexión. Puede acceder y utilizar Horizon Administrator con los siguientes navegadores web:

- Internet Explorer 9 (no recomendado)
- Internet Explorer 10
- Internet Explorer 11
- Firefox (últimas versiones admitidas)
- Chrome (últimas versiones admitidas)
- Safari 6 y versiones posteriores
- Microsoft Edge (Windows 10)

Para usar Horizon Administrator con su navegador web, debe instalar Adobe Flash Player 10.1 o versiones posteriores. Su sistema cliente debe tener acceso a Internet para permitir la instalación de Adobe Flash Player.

El equipo en el que inicie Horizon Administrator debe confiar en el certificado raíz y en los intermedios del servidor que aloja el servidor de conexión. Los navegadores admitidos ya incluyen algunos certificados para todas las entidades de certificación (CA) conocidas. Si los certificados proceden de una CA que no es conocida, debe seguir las siguientes instrucciones en [Configurar endpoints cliente para confiar en el certificado raíz y los intermedios](#).

Para que el texto se muestre correctamente, Horizon Administrator requiere fuentes específicas de Microsoft. Si su navegador web se ejecuta en un sistema operativo que no es de Windows, como Linux, UNIX o Mac, compruebe que las fuentes específicas de Microsoft estén instaladas en su equipo.

Actualmente, el sitio web de Microsoft no distribuye fuentes de Microsoft, pero puede descargarlas desde sitios web independientes.

Requisitos de Horizon Console

Los administradores utilizan Horizon Console para configurar Horizon Connection Server, implementar y administrar aplicaciones y escritorios remotos, controlar la autenticación de usuario, iniciar y examinar eventos del sistema, y realizar actividades analíticas. Los sistemas cliente que ejecutan Horizon Console deben cumplir determinados requisitos.

Horizon Console es una aplicación web que se instala con el servidor de conexión. Puede acceder y utilizar Horizon Console con los siguientes navegadores web:

- Internet Explorer 11
- Firefox (últimas versiones admitidas)
- Chrome (últimas versiones admitidas)
- Safari (últimas versiones admitidas)

- Microsoft Edge (Windows 10)

El equipo en el que inicie Horizon Console debe confiar en el certificado raíz y en los intermedios del servidor que aloja el servidor de conexión. Los navegadores admitidos ya incluyen algunos certificados para todas las entidades de certificación (CA) conocidas. Si los certificados proceden de una CA que no es conocida, debe seguir las siguientes instrucciones en [Configurar endpoints cliente para confiar en el certificado raíz y los intermedios](#).

Para que el texto se muestre correctamente, Horizon Console requiere fuentes específicas de Microsoft. Si su navegador web se ejecuta en un sistema operativo que no es de Windows, como Linux, UNIX o Mac, compruebe que las fuentes específicas de Microsoft estén instaladas en su equipo.

Actualmente, el sitio web de Microsoft no distribuye fuentes de Microsoft, pero puede descargarlas desde sitios web independientes.

Requisitos de View Composer

Con View Composer, puede implementar varios escritorios de clones vinculados desde una imagen de base centralizada. View Composer tiene requisitos específicos de almacenamiento e instalación.

- [Sistemas operativos compatibles con View Composer](#)

View Composer admite sistemas operativos de 64 bits con limitaciones y requisitos específicos. Puede instalar View Composer en la misma máquina virtual o el mismo equipo físico que vCenter Server o en un servidor independiente.

- [Requisitos de hardware para un View Composer independiente](#)

Si instala View Composer en una máquina virtual o en un equipo físico diferentes de la usada para vCenter Server, debe usar una máquina dedicada que cumpla los requisitos de hardware específicos.

- [Requisitos de base de datos para View Composer y para bases de datos de eventos](#)

View Composer necesita una base de datos SQL para almacenar datos. La base de datos debe residir o estar disponible en el host del servidor de View Composer. Puede configurar de forma opcional una base de datos de eventos para registrar información desde Horizon Connection Server sobre los eventos de Horizon.

Sistemas operativos compatibles con View Composer

View Composer admite sistemas operativos de 64 bits con limitaciones y requisitos específicos. Puede instalar View Composer en la misma máquina virtual o el mismo equipo físico que vCenter Server o en un servidor independiente.

Tabla 1-3. Sistemas operativos compatibles con View Composer

Sistema operativo	Versión	Edición
Windows Server 2008 R2 SP1	64 bits	Standard Enterprise Datacenter
Windows Server 2012 R2	64 bits	Standard Datacenter
Windows Server 2016	64 bits	Standard Datacenter
Windows Server 2019	64 bits	Standard Datacenter

Nota Ya no se admite Windows Server 2008 R2 sin Service Pack.

Si tiene pensado instalar View Composer en una máquina virtual o un equipo físico en los que no se encuentre vCenter Server, consulte [Requisitos de hardware para un View Composer independiente](#).

Para obtener más información sobre cómo solucionar problemas de una instalación de View Composer en una máquina virtual con Windows Server 2016 o Windows Server 2019, consulte el artículo <https://kb.vmware.com/s/article/59633> de la base de conocimientos de VMware.

Requisitos de hardware para un View Composer independiente

Si instala View Composer en una máquina virtual o en un equipo físico diferentes de la usada para vCenter Server, debe usar una máquina dedicada que cumpla los requisitos de hardware específicos.

Una instalación de View Composer independiente funciona con vCenter Server instalado en un equipo Windows Server o con el dispositivo de vCenter Server basado en Linux. VMware recomienda tener una asignación uno a uno entre el servicio View Composer y la instancia de vCenter Server.

Tabla 1-4. Requisitos de hardware para View Composer

Componente de hardware	Obligatorio	Recomendado
Procesador	Intel 64 de 1,4 GHz o más potente, o bien procesador AMD 64 con 2 CPU	2 GHz o más potente y 4 CPU
Red	Una o varias tarjetas de interfaz de red (NIC) de 10/100 Mbps	NIC de 1 Gbps
Memoria	4 GB de RAM o superior	8 GB de RAM o superior para implementaciones de 50 o más escritorios remotos
Espacio de disco	40 GB	60 GB

Importante La máquina virtual o el equipo físico que aloje View Composer debe tener una dirección IP que no cambie. En un entorno IPv4, configure una dirección IP estática. En un entorno IPv6, los equipos obtienen automáticamente direcciones IP que no cambian.

Requisitos de base de datos para View Composer y para bases de datos de eventos

View Composer necesita una base de datos SQL para almacenar datos. La base de datos debe residir o estar disponible en el host del servidor de View Composer. Puede configurar de forma opcional una base de datos de eventos para registrar información desde Horizon Connection Server sobre los eventos de Horizon.

Si una instancia del servidor de la base de datos ya existe para vCenter Server, View Composer puede usar esa instancia existente si es una de las versiones que aparece en la página de matrices de interoperabilidad de productos de VMware http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Si no existe ninguna instancia del servidor de la base de datos, debe instalar una.

View Composer admite un subconjunto de servidores de la base de datos que vCenter Server admite. Si ya utiliza vCenter Server con un servidor de la base de datos que View Composer no admita, continúe usando el servidor de la base de datos para vCenter Server e instale un servidor de la base de datos independiente para usar View Composer.

Importante Si crea la base de datos de View Composer en la misma instancia de SQL Server que vCenter Server, no sobrescriba la base de datos de vCenter Server.

Para la mayor parte de la información actualizada sobre las bases de datos admitidas, consulte Matrices de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. En el apartado de la **interoperabilidad entre la base de datos y la solución**, después de seleccionar el producto y la versión (en el paso para agregar una base de datos), si desea consultar una lista de todas las bases de datos compatibles, seleccione **Cualquiera** y haga clic en **Agregar**.

Requisitos del sistema para sistemas operativos invitados

2

Los sistemas que ejecutan Horizon Agent u Horizon Persona Management deben cumplir algunos requisitos de hardware y de software.

Este capítulo incluye los siguientes temas:

- [Requisitos y consideraciones para Horizon Agent](#)
- [Sistemas operativos compatibles con Standalone Horizon Persona Management](#)
- [Compatibilidad del software y protocolo de visualización remota](#)

Requisitos y consideraciones para Horizon Agent

El componente Horizon Agent (denominado View Agent en versiones anteriores) asiste al usuario gracias a la administración de las sesiones, de Single Sign-On y el redireccionamiento de los dispositivos, entre otras funciones. Debe instalar Horizon Agent en todas las máquinas virtuales, equipos físicos y hosts RDS.

Los tipos y ediciones de los sistemas operativos compatibles dependen de la versión de Windows. Para obtener una lista actualizada de los sistemas operativos Windows 10 compatibles, consulte el artículo <http://kb.vmware.com/kb/2149393> de la base de conocimientos (KB) de VMware. Para sistemas operativos Windows que no sean Windows 10, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150295>.

Para consultar una lista de funciones de experiencia remota específicas que son compatibles con los sistemas operativos Windows en los que Horizon Agent está instalado, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150305>.

Para usar la opción de configuración de Horizon Persona Management con Horizon Agent, debe instalar Horizon Agent en máquinas virtuales Windows 10, Windows 8, Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2008 R2 o Windows Server 2016. Esta opción no funciona en equipos físicos ni en hosts RDS.

Puede instalar la versión independiente de Horizon Persona Management en los equipos físicos. Consulte [Sistemas operativos compatibles con Standalone Horizon Persona Management](#).

Nota Para usar el protocolo de visualización VMware Blast, debe instalar Horizon Agent en una máquina virtual de sesión única o en un host RDS. El host RDS puede ser un equipo físico o una máquina virtual. El protocolo de visualización VMware Blast no funciona en máquinas físicas de usuario único, excepto en la edición Enterprise de Windows 10 RS4 y compilaciones posteriores.

Para proporcionar una seguridad mejorada, VMware recomienda configurar los conjuntos de claves de cifrado para que eliminen las vulnerabilidades conocidas. Para obtener instrucciones sobre cómo configurar una directiva de dominio en los conjuntos de claves de cifrado para los equipos Windows que ejecuten View Composer u Horizon Agent, consulte [Deshabilitar cifrados débiles en SSL/TLS](#).

Sistemas operativos compatibles con Standalone Horizon Persona Management

El software Standalone Horizon Persona Management ofrece administración de identidades para máquinas virtuales y equipos físicos independientes que no tienen Horizon Agent instalado. Cuando los usuarios inician sesión, sus perfiles se descargan de forma dinámica desde un repositorio de perfil remoto en sus sistemas independientes.

Nota Para configurar Persona Management para escritorios de Horizon, instale Horizon Agent con la opción de configuración **Administración de identidades**. El software Standalone Persona Management está destinado para su uso únicamente en sistemas que no sean Horizon.

Para obtener una lista de sistemas operativos compatibles con el software Standalone Horizon Persona Management, consulte el artículo de la base de conocimientos de VMware (KB) <http://kb.vmware.com/kb/2150295>.

El software Standalone Persona Management no es compatible con los Servicios de Escritorios remotos de Microsoft.

Compatibilidad del software y protocolo de visualización remota

Los protocolos y el software de visualización remota proporcionan acceso a aplicaciones y escritorios remotos. El tipo de protocolo de visualización remota varía según el dispositivo cliente, si desea

conectarse a una aplicación o escritorio remoto y el modo en que el administrador configura el grupo de escritorios o aplicaciones.

- **PCoIP**

PCoIP (PC over IP) ofrece una experiencia de escritorio optimizada para enviar una aplicación publicada o un entorno de escritorio remoto completo, con aplicaciones, imágenes y contenido de audio y vídeo, a un amplio grupo de usuarios a través la red LAN o WAN. PCoIP puede compensar el aumento de la latencia o la disminución del ancho de banda para garantizar que el rendimiento de los usuarios finales sea productivo independientemente de las condiciones de la red.

- **Microsoft RDP**

El Protocolo de escritorios remotos es el mismo protocolo multicanal que muchos usuarios ya utilizan para acceder al equipo de trabajo desde el equipo personal. La conexión a Escritorio remoto de Microsoft (RDC) usa RDP para enviar datos.

- **VMware Blast Extreme**

Optimizado para la nube móvil, VMware Blast Extreme admite el rango más amplio de dispositivos cliente que son compatibles con H.264. De los protocolos de visualización, VMware Blast ofrece el menor consumo de CPU para obtener una mayor duración de la batería de los dispositivos móviles. VMware Blast Extreme puede compensar un aumento en la latencia o una reducción en el ancho de banda y puede aprovechar los transportes de redes UDP y TCP.

PCoIP

PCoIP (PC over IP) ofrece una experiencia de escritorio optimizada para enviar una aplicación publicada o un entorno de escritorio remoto completo, con aplicaciones, imágenes y contenido de audio y vídeo, a un amplio grupo de usuarios a través la red LAN o WAN. PCoIP puede compensar el aumento de la latencia o la disminución del ancho de banda para garantizar que el rendimiento de los usuarios finales sea productivo independientemente de las condiciones de la red.

El protocolo de visualización PCoIP se puede utilizar con aplicaciones publicadas y escritorios remotos que usen máquinas virtuales, máquinas físicas que contengan tarjetas de host Teradici o escritorios de sesión compartida en un host RDS.

Funciones de PCoIP

Entre las funciones principales del protocolo PCoIP se incluyen las siguientes:

- Los usuarios que se encuentran fuera del firewall corporativo pueden utilizar este protocolo con la red privada virtual (VPN) de su compañía. También pueden establecer conexiones seguras y cifradas con un servidor de seguridad o dispositivo de Access Point de la red perimetral (DMZ) corporativa.
- El cifrado de 128 bits de Estándar de cifrado avanzado (AES) es compatible y se activa de forma predeterminada, pero puede cambiarlo a AES-256.
- Son compatibles las conexiones a escritorios Windows con las versiones de sistema operativo de Horizon Agent que se incluyen en [Requisitos y consideraciones para Horizon Agent](#).
- Las conexiones desde todos los tipos de dispositivos cliente.

- Controles de optimización para reducir el uso del ancho de banda en las redes LAN y WAN.
- Las pantallas virtuales admiten color de 32 bits.
- Compatible con fuentes ClearType.
- Redirección de audio con ajuste de calidad de audio dinámico para LAN y WAN.
- Audio y vídeo en tiempo real para usar cámaras web y micrófonos en algunos tipos de cliente.
- Opción de copiar y pegar texto (y también imágenes en algunos clientes) entre el sistema operativo cliente y una aplicación publicada o escritorio remoto. En otros tipos de cliente, solo se puede copiar texto sin formato. No es posible copiar y pegar objetos del sistema, como carpetas y archivos, de un sistema a otro.
- En algunos tipos de cliente, se pueden utilizar varios monitores. En algunos casos, puede usar hasta 4 monitores con una resolución de hasta 2560 x 1600 en cada uno o 3 monitores con una resolución de 4K (3840 x 2160) para escritorios remotos de Windows 7 en los que se deshabilite Aero. También son compatibles las opciones de autoajustar y rotar la pantalla.

Al habilitar la función 3D, se admiten hasta 2 monitores con una resolución de hasta 1920 x 1200 o un único monitor con una resolución de 4K (3840 x 2160).

- En algunos tipos de cliente, se admite el redireccionamiento USB.
- El redireccionamiento MMR es compatible con algunos sistemas operativos cliente Windows y algunos sistemas operativos de escritorio remoto (que tengan instalado Horizon Agent).

Para obtener información sobre los sistemas operativos de escritorio compatibles con funciones específicas de PCoIP, consulte el documento *Planificación de la arquitectura de Horizon 7*.

Acceda a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html> para obtener información sobre los dispositivos cliente compatibles con funciones específicas de PCoIP.

Configuración recomendada para los sistemas operativos invitados

Se recomienda 1 GB o más de RAM y una CPU dual para reproducir en alta definición, modo en pantalla completa, o bien vídeos de 720p o con un formato superior. Si desea utilizar Virtual Dedicated Graphics Acceleration para aplicaciones con gráficos avanzados, como aplicaciones CAD, necesita 4 GB de RAM.

Requisitos de calidad de vídeo

Vídeo con formato de 480p

Puede reproducir vídeo con una resolución nativa de 480p o inferior si el escritorio remoto tiene una única CPU virtual. Si desea reproducir el vídeo en Flash de alta definición o en modo de pantalla completa, el escritorio requiere una CPU virtual dual. Incluso con un escritorio que tenga doble CPU virtual, es posible que el vídeo con formato de 360p que se reproduce en modo de pantalla completa se retrase con respecto al audio, sobre todo en el caso de clientes Windows.

Vídeo con formato de 720p

Puede reproducir vídeo de 720p en resoluciones nativas si el escritorio remoto tiene una CPU virtual doble. El rendimiento puede verse afectado si

reproduce vídeos en 720p en alta definición o en modo de pantalla completa.

Vídeo con formato de 1080p

Si el escritorio remoto tiene una CPU virtual doble, puede reproducir vídeo con formato de 1080p, aunque es posible que el reproductor deba ajustarse a una ventana más pequeña.

Procesamiento 3D

Puede configurar escritorios remotos para que utilicen gráficos de aceleración de hardware o software. La función de gráficos de aceleración de software le permite ejecutar aplicaciones de OpenGL 2.1 y DirectX9 sin necesidad de una unidad de procesamiento de gráficos (GPU) física. Las funciones de gráficos de aceleración de hardware permiten que las máquinas virtuales compartan sus GPU (unidades de procesamiento gráfico) físicas en un host de vSphere o bien dediquen una GPU física a un único escritorio de máquina virtual.

Para las aplicaciones 3D, se admiten hasta 2 monitores y la resolución de pantalla máxima es 1920 x 1200. El sistema operativo invitado en los escritorios remotos debe ser Windows 7 o posterior.

Requisitos de hardware para los sistemas cliente

Para obtener información sobre los requisitos del procesador y la memoria, consulte el tipo de escritorio o dispositivo cliente móvil específico en el documento "Uso de VMware Horizon Client". Visite <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Microsoft RDP

El Protocolo de escritorios remotos es el mismo protocolo multicanal que muchos usuarios ya utilizan para acceder al equipo de trabajo desde el equipo personal. La conexión a Escritorio remoto de Microsoft (RDC) usa RDP para enviar datos.

Microsoft RDP es un protocolo de visualización compatible con los escritorios remotos que usan máquinas virtuales, equipos físicos o escritorios de sesión compartida en un host RDS. (Únicamente los protocolos de visualización VMware Blast y PCoIP se admiten en las aplicaciones publicadas). Microsoft RDP proporciona las siguientes funciones:

- RDP 7 es compatible con varios monitores de confianza, admitiendo hasta 16 monitores.
- Puede copiar y pegar texto y objetos del sistema como carpetas y archivos entre el sistema local y el escritorio remoto.
- Las pantallas virtuales admiten color de 32 bits.
- RDP admite el cifrado de 128 bits.
- Los usuarios que se encuentren fuera del firewall empresarial pueden usar este protocolo con la red privada virtual (VPN) de su compañía o pueden establecer conexiones cifradas y seguras al servidor de seguridad de View en la DMZ empresarial.

Para admitir las conexiones TLSv1.1 y TLSv1.2 en Windows 7 y Windows Server 2008 R2, debe aplicar la revisión de Microsoft KB3080079.

Requisitos de hardware para los sistemas cliente

Para obtener más información sobre los requisitos del sistema y del procesador, consulte el documento "Uso de VMware Horizon Client" para el tipo específico de sistema cliente. Visite <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Nota Los dispositivos cliente móviles 3.x únicamente usan el protocolo de visualización PCoIP. Los dispositivos cliente móviles 4.x solo usan el protocolo de visualización PCoIP o el protocolo de visualización VMware Blast.

VMware Blast Extreme

Optimizado para la nube móvil, VMware Blast Extreme admite el rango más amplio de dispositivos cliente que son compatibles con H.264. De los protocolos de visualización, VMware Blast ofrece el menor consumo de CPU para obtener una mayor duración de la batería de los dispositivos móviles. VMware Blast Extreme puede compensar un aumento en la latencia o una reducción en el ancho de banda y puede aprovechar los transportes de redes UDP y TCP.

El protocolo de visualización VMware Blast se puede usar para las aplicaciones publicadas y para los escritorios remotos que usan máquinas virtuales o escritorios de sesión compartida en un host RDS. El host RDS puede ser un equipo físico o una máquina virtual. El protocolo de visualización VMware Blast no funciona en máquinas físicas de usuario único, excepto en la edición Enterprise de Windows 10 RS4 y compilaciones posteriores.

Nota No se admiten aplicaciones de películas y TV en las máquina físicas con Windows 10 RS4.

Funciones de VMware Blast Extreme

Las funciones clave de VMware Blast Extreme incluyen las siguientes:

- Los usuarios que se encuentran fuera del firewall corporativo pueden utilizar este protocolo con la red privada virtual (VPN) corporativa. También pueden establecer conexiones seguras y cifradas con un servidor de seguridad o dispositivo de Access Point de la red perimetral (DMZ) corporativa.
- El cifrado de 128 bits de Estándar de cifrado avanzado (AES) es compatible y se activa de forma predeterminada, pero puede cambiarlo a AES-256.
- Son compatibles las conexiones a escritorios Windows con las versiones de sistema operativo de Horizon Agent que se incluyen en [Requisitos y consideraciones para Horizon Agent](#).
- Las conexiones desde todos los tipos de dispositivos cliente.
- Controles de optimización para reducir el uso del ancho de banda en las redes LAN y WAN.

- Los contadores de rendimiento mostrados mediante PerfMon en agentes de Windows proporcionan una representación exacta del estado actual del sistema que también se actualiza a un ritmo constante para lo siguiente:
 - Sesión de Blast
 - Imágenes
 - Audio
 - CDR
 - USB: Los contadores de USB que aparecen cuando utiliza PerfMon en agentes de Windows son válidos si el tráfico USB está configurado para utilizar VMware Virtual Channel (VVC).
 - Skype Empresarial: Los contadores son solo para controlar el tráfico.
 - Portapapeles
 - RTAV
 - Funciones de redireccionamiento del escáner y del puerto serie
 - Impresión virtual
 - MMR HTML5
 - Windows Media (MMR): Los contadores de rendimiento aparecen solo si se configuró esta función para que use VMware Virtual Channel (VVC).
- Continuidad de red durante una pérdida de red momentánea en clientes Windows.
- Las pantallas virtuales admiten color de 32 bits.
- Compatible con fuentes ClearType.
- Redirección de audio con ajuste de calidad de audio dinámico para LAN y WAN.
- Audio y vídeo en tiempo real para usar cámaras web y micrófonos en algunos tipos de cliente.
- Opción de copiar y pegar texto (y también imágenes en algunos clientes) entre el sistema operativo cliente y una aplicación publicada o escritorio remoto. En otros tipos de cliente, solo se puede copiar texto sin formato. No es posible copiar y pegar objetos del sistema, como carpetas y archivos, de un sistema a otro.
- En algunos tipos de cliente, se pueden utilizar varios monitores. En algunos casos, puede usar hasta cuatro monitores con una resolución de hasta 2560 x 1600 en cada uno o tres monitores con una resolución de 4K (3840 x 2160) para escritorios remotos de Windows 7 en los que se deshabilite Aero. También son compatibles las opciones de autoajustar y rotar la pantalla.

Al habilitar la función 3D, se admiten hasta dos monitores con una resolución de hasta 1920 x 1200 o un único monitor con una resolución de 4K (3840 x 2160).
- En algunos tipos de cliente, se admite el redireccionamiento USB.
- El redireccionamiento MMR se admite en algunos sistemas operativos cliente Windows y en algunos sistemas operativos de escritorio remoto (con Horizon Agent instalado).

- Las conexiones a equipos físicos sin monitores son compatibles con las tarjetas gráficas NVIDIA. Para obtener un mejor rendimiento, utilice una tarjeta gráfica que admita la codificación H.264.

Si tiene una GPU discreta adicional y una GPU integrada, es posible que se utilice el sistema operativo predeterminado para la GPU integrada. Para solucionar este problema, puede deshabilitar o eliminar el dispositivo en el Administrador de dispositivos. Si el problema persiste, puede instalar el controlador de gráficos WDDM para la GPU integrada o deshabilitar la GPU integrada en la BIOS del sistema. Consulte la documentación del sistema sobre cómo deshabilitar la GPU integrada.

Precaución Al deshabilitar la GPU integrada, es posible que se pierda el acceso a determinadas funciones como, por ejemplo, el acceso de la consola a la configuración del BIOS o al cargador de arranque NT.

- El códec Blast mejora el rendimiento de Adaptive y de los codificadores H.264 en el uso de escritorios al mostrar fuentes e imágenes más nítidas, y funciona como un códec de vídeo con detección de movimiento, vectores de movimiento y macrobloques interpredecibles. Se admite en los siguientes entornos y está deshabilitado de forma predeterminada:
 - Agentes Windows y Linux. Para habilitar el códec:
 - En agentes Windows, establezca la clave de registro: HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1
 - En agentes Linux, establezca RemoteDisplay.allowBlastCodec=TRUE en /etc/vmware/config
 - Deshabilite H.264 en la configuración del cliente Windows, Linux y MacOS. Esta función no es compatible con los clientes móviles ni con Web Client.
- Un conmutador de codificador dinámico permite alternar entre un codificador optimizado de vídeo (H.264 4:2:0 o H.264 4:4:4) y un codificador optimizado de texto (códec Blast o Adaptive). Este conmutador ayuda a mostrar vídeos y textos nítidos con un uso de ancho de banda reducido. Para usar esta función, habilite el conmutador del codificador:
 - En agentes Windows, establezca la clave de registro HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1
 - En agentes Linux, establezca RemoteDisplay.allowSwitchEncoder=TRUE en /etc/vmware/config
 - Habilite el códec Blast, que está deshabilitado de forma predeterminada. Si el códec Blast no está habilitado, el codificador del conmutador utilizará Adaptive para la codificación optimizada de texto.
 - Habilite H.264 en la configuración del cliente Windows, Linux o MacOS. Esta función no es compatible con los clientes móviles ni con Web Client.

Nota El conmutador de codificador solo utiliza software H.264 y no admite gráficos acelerados por hardware.

Para obtener más información sobre los dispositivos cliente que admiten funciones específicas de VMware Blast Extreme, diríjase a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Wake-on-LAN

Wake-on-LAN se admite en máquinas físicas con la edición Enterprise de Windows 10 RS4 y compilaciones posteriores. Esta función permite a los usuarios reactivar máquinas físicas cuando se conectan con Horizon Connection Server. La función Wake-on-LAN tiene estos requisitos previos:

- Wake-on-LAN (WoL) solo se admite en entornos IPv4.
- La máquina física debe estar configurada para reactivarse al recibir paquetes de Wake-on-LAN si la función Wake-on-LAN está habilitada en la configuración de la BIOS y de la tarjeta de red.
- Se debe utilizar el puerto de destino 9 para los paquetes de WoL procedentes del servidor de conexión.
- Los paquetes de WoL son paquetes de difusión orientados a direcciones IP que deben ser capaces de llegar a Horizon Agent cuando se envían desde Horizon Connection Server. Wake-on-LAN funciona en los siguientes casos:
 - El servidor de conexión y Horizon Agent en la máquina física están en la misma subred dentro de un entorno LAN.
 - Todos los enrutadores entre el servidor de conexión y Horizon Agent están configurados para permitir los paquetes de difusión orientados a direcciones IP en la subred de destino de la máquina física que desea reactivar.

Nota La función Wake-on-LAN no es compatible con grupos de asignaciones flotantes de un agente Windows 10 físico. El paquete de WoL solo se envía a grupos de asignaciones dedicados con la autorización de un usuario en particular.

Configuración recomendada para los sistemas operativos invitados

Se recomienda 1 GB o más de RAM y una CPU dual para reproducir en alta definición, en modo de pantalla completa, o bien vídeos de 720p o con un formato superior. Si desea utilizar Virtual Dedicated Graphics Acceleration para aplicaciones con gráficos avanzados, como aplicaciones CAD, necesita 4 GB de RAM.

Requisitos de calidad de vídeo

Vídeo con formato de 480p

Puede reproducir vídeo con una resolución nativa de 480p o inferior si el escritorio remoto tiene una única CPU virtual. Si desea reproducir el vídeo en Flash de alta definición o en modo de pantalla completa, el escritorio requiere una CPU virtual dual. Incluso con un escritorio que tenga doble CPU virtual, es posible que el vídeo con formato de 360p que se reproduce en modo de pantalla completa se retrase con respecto al audio, sobre todo en el caso de clientes Windows.

Vídeo con formato de 720p

Puede reproducir vídeo de 720p en resoluciones nativas si el escritorio remoto tiene una CPU virtual doble. El rendimiento puede verse afectado si reproduce vídeos en 720p en alta definición o en modo de pantalla completa.

Vídeo con formato de 1080p

Si el escritorio remoto tiene una CPU virtual doble, puede reproducir vídeo con formato de 1080p, aunque es posible que el reproductor deba ajustarse a una ventana más pequeña.

Procesamiento 3D

Puede configurar escritorios remotos para que utilicen gráficos de aceleración de hardware o software. La función de gráficos de aceleración de software le permite ejecutar aplicaciones de OpenGL 2.1 y DirectX9 sin necesidad de una unidad de procesamiento de gráficos (GPU) física. Las funciones de gráficos de aceleración de hardware permiten que las máquinas virtuales compartan sus GPU (unidades de procesamiento gráfico) físicas en un host de vSphere, o bien dediquen una GPU física a un único escritorio virtual.

Para las aplicaciones 3D, se admiten hasta dos monitores y la resolución de pantalla máxima es 1920 x 1200. El sistema operativo invitado en los escritorios remotos debe ser Windows 7 o posterior.

Requisitos de hardware para los sistemas cliente

Para obtener más información sobre los requisitos de memoria y de procesamiento para el tipo específico de escritorio o dispositivo móvil cliente, acceda a <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Instalar Horizon 7 en un entorno IPv6

3

Horizon 7 admite IPv6 como alternativa a IPv4. El entorno debe ser únicamente IPv6 o únicamente IPv4. Horizon 7 no admite un entorno IPv6 y IPv4 mixto.

No todas las funciones de Horizon 7 admitidas en un entorno IPv4 se admiten en un entorno IPv6. Horizon 7 no admite la actualización de un entorno IPv4 a un entorno IPv6. Además, Horizon 7 no admite la migración entre entornos IPv4 e IPv6.

Importante Para ejecutar Horizon 7 en un entorno IPv6, debe especificar IPv6 cuando instale todos los componentes de Horizon 7.

Este capítulo incluye los siguientes temas:

- [Configurar Horizon 7 en un entorno IPv6](#)
- [Versiones de Active Directory, de base de datos y de vSphere admitidas en un entorno IPv6](#)
- [Sistemas operativos compatibles con Horizon 7 Servers en un entorno IPv6](#)
- [Sistemas operativos Windows compatibles con hosts RDS y escritorios en un entorno IPv6](#)
- [Clientes admitidos en un entorno IPv6](#)
- [Protocolos de comunicación remota admitidos en un entorno IPv6](#)
- [Tipos de autenticación admitidos en un entorno IPv6](#)
- [Otras funciones admitidas en un entorno IPv6](#)

Configurar Horizon 7 en un entorno IPv6

Para ejecutar Horizon 7 en un entorno IPv6, debe conocer los requisitos y las opciones que son específicas para IPv6 cuando realice algunas tareas administrativas.

Antes de instalar Horizon 7, debe tener un entorno IPv6 en funcionamiento. Las siguientes tareas administrativas de Horizon 7 tienen opciones que son específicas para IPv6.

- Instalar el servidor de conexión de Horizon. Consulte [Instalar el servidor de conexión de Horizon con una nueva configuración](#).

- Instalar el servidor de réplica de View. Consulte [Instalar una instancia replicada del servidor de conexión de Horizon](#).
- Instalar el servidor de seguridad de View. Consulte [Instalar un servidor de seguridad](#).
- Configurar la URL externa de PCoIP. Consulte [Configurar URL externas para conexiones seguras de puerta de enlace y túnel.](#)
- Establecer la URL externa de PCoIP. Consulte [Configurar las URL externas de una instancia del servidor de conexión](#).
- Modificar la URL externa de PCoIP. Consulte [Configurar las URL externas de una instancia del servidor de conexión](#).
- Instalar Horizon Agent. Consulte los temas sobre la instalación de Horizon Agent en el documento *Configurar grupos de aplicaciones y escritorios*.
- Instalar Horizon Client. Consulte [Clientes admitidos en un entorno IPv6](#).

Nota Horizon 7 no necesita que introduzca una dirección IPv6 en ninguna tarea administrativa. En los casos en los que pueda especificar un nombre de dominio completo (FQDN) o una dirección IPv6, se recomienda que introduzca un FQDN para evitar errores potenciales.

Versiones de Active Directory, de base de datos y de vSphere admitidas en un entorno IPv6

En un entorno IPv6, Horizon 7 admite versiones de Active Directory, del servidor de la base de datos y de vSphere específicas.

Los entornos IPv6 admite bases de datos SQL Server 2012 y Oracle 11g (y versiones posteriores). Para obtener la información más actualizada sobre las bases de datos y las versiones de vSphere y Active Directory compatibles en entornos IPv6, consulte las matrices de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Sistemas operativos compatibles con Horizon 7 Servers en un entorno IPv6

En un entorno IPv6, debe instalar Horizon 7 Servers en sistemas operativos Windows Server específicos.

Los servidores de Horizon 7 incluyen instancias del servidor de conexión, servidores de réplica, servidores de seguridad e instancias de Horizon 7 Composer.

Sistema operativo	Edición
Windows Server 2016	Standard, Enterprise
Windows Server 2008 R2 SP1	Standard, Enterprise
Windows Server 2012 R2	Standard

Sistemas operativos Windows compatibles con hosts RDS y escritorios en un entorno IPv6

En un entorno IPv6, Horizon 7 admite sistemas operativos Windows específicos para equipos de escritorios y hosts RDS. Los hosts RDS proporcionan a los usuarios aplicaciones y escritorios basados en sesiones.

Los tipos y ediciones de los sistemas operativos compatibles dependen de la versión de Windows. Para obtener una lista actualizada de los sistemas operativos Windows 10 compatibles, consulte el artículo <http://kb.vmware.com/kb/2149393> de la base de conocimientos (KB) de VMware. Para sistemas operativos Windows que no sean Windows 10, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150295>.

Para consultar una lista de funciones de experiencia remota específicas que son compatibles con los sistemas operativos Windows en los que Horizon Agent está instalado, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2150305>.

Clientes admitidos en un entorno IPv6

En un entorno IPv6, Horizon 7 admite clientes que se ejecutan en sistemas operativos de escritorio específicos.

Tabla 3-1. Sistemas operativos Windows admitidos

Sistema operativo	Versión	Edición
Windows 7 y Windows 7 SP1	32 o 64 bits	Home, Enterprise, Professional y Ultimate
Windows 8 y Windows 8.1	32 o 64 bits	Pro, Enterprise e Industry Embedded
Windows 10	32 o 64 bits	Home, Pro, Pro for Workstations, Enterprise e IoT Enterprise

En dispositivos iOS, iOS 9.2 y las versiones posteriores son compatibles con Horizon Client 4.1 para iOS y versiones posteriores.

En dispositivos macOS, se requiere Horizon Client 4.9 para Mac o una versión posterior.

En dispositivos Android, se requiere Horizon Client 4.9 para Android o una versión posterior.

En dispositivos Chromebook, se requiere Horizon Client 5.1 para Android o una versión posterior.

No se admiten los siguientes clientes.

- Horizon Client para Linux, Horizon Client para Chrome, Horizon Client para Chrome OS, Horizon Client para Windows 10 UWP y Horizon Client para Tienda Windows.
- PCoIP Zero Client

Protocolos de comunicación remota admitidos en un entorno IPv6

En un entorno IPv6, Horizon 7 admite protocolos remotos específicos.

Se admiten los siguientes protocolos de comunicación remota:

- RDP
- RDP con túnel seguro
- PCoIP
- PCoIP a través de la puerta de enlace segura PCoIP
- VMware Blast
- VMware Blast a través de la puerta de enlace segura Blast
- Blast Extreme Adaptive Transport (BEAT)

Tipos de autenticación admitidos en un entorno IPv6

En un entorno IPv6, Horizon 7 admite tipos de autenticación específicos.

Se admiten los siguientes tipos de autenticación:

- Autenticación de contraseña con Active Directory
- Tarjeta inteligente
- Single Sign-On

No se admiten los siguientes tipos de autenticación:

- SecurID
- RADIUS
- SAML

Otras funciones admitidas en un entorno IPv6

En un entorno IPv6, Horizon 7 admite algunas funciones que no aparecen en los temas anteriores.

Se admiten las siguientes funciones:

- Grupos de aplicaciones
- Salida de audio
- Grupos de escritorios automatizados de máquinas virtuales completas, clones instantáneos o clones vinculados de Horizon 7 Composer
- Blast Extreme Adaptive Transport (BEAT)
- Programa de mejora de la experiencia de cliente (CEIP)

- Recuperación de espacio de disco
- Eventos
- Seguimiento del rendimiento de Horizon
- Redireccionamiento multimedia HTML5
- Grupos de escritorios de clones instantáneos
- Copia de seguridad de LDAP
- Grupo de escritorios manuales, incluidas las máquinas virtuales de vCenter Server, los equipos físicos y las máquinas virtuales que no están administradas por vCenter Server
- Snapshots NFS nativas (VAAI)
- Administración de identidades
- Audio/vídeo en tiempo real (RTAV)
- grupos de escritorios RDS
- Hosts RDS 3D
- Administración basada en funciones
- Session Collaboration
- Single Sign-On, incluida la función Iniciar sesión como usuario actual
- Panel de control de estado del sistema
- ThinApp
- Unity Touch
- Redireccionamiento USB
- Horizon 7 Composer Agent
- Acelerador de almacenamiento de Horizon 7
- Copia de seguridad de la base de datos de Horizon 7 Composer
- Impresión virtual
- VMware audio
- VMware video
- VMware Virtualization Pack para Skype Empresarial (solo Windows)

No se admiten las siguientes funciones:

- Redireccionamiento de unidades cliente
- Transparencia de IP de cliente (solo 64 bits)
- Arquitectura de Cloud Pod
- Device Bridge

- Asociación de archivos
- Redireccionamiento URL Flash
- HTML Access
- Log Insight
- Lync
- PCoIP con grupos de clones instantáneos de RDSH
- Redireccionamiento de escáner
- Redireccionamiento del puerto serie
- Syslog
- Tarjeta de host Teradici TERA
- TSMMR
- Redireccionamiento de URL
- vSAN
- Virtual Volumes
- Agente de escritorios vRealize Operations

Instalar Horizon 7 en modo FIPS

4

Horizon 7 puede realizar operaciones de cifrado usando algoritmos conformes a la norma FIPS (Estándar federal de procesamiento de información) 140-2. Puede instalar Horizon 7 en modo FIPS para habilitar el uso de estos algoritmos.

No todas las funciones de Horizon 7 se admiten en modo FIPS. Además, Horizon 7 no admite la actualización de una instalación que no sea FIPS a una que sí lo sea.

Nota Para asegurar que Horizon 7 se ejecute en modo FIPS, debe habilitar FIPS cuando instale todos los componentes de Horizon 7.

Este capítulo incluye los siguientes temas:

- [Información general sobre la configuración de Horizon 7 en modo FIPS](#)
- [Requisitos del sistema para el modo FIPS](#)

Información general sobre la configuración de Horizon 7 en modo FIPS

Para configurar Horizon 7 en modo FIPS, en primer lugar debe habilitar este modo en el entorno de Windows. A continuación, instale todos los componentes de Horizon 7 en modo FIPS.

La opción para instalar Horizon 7 en modo FIPS solo está disponible si se habilita este modo en el entorno de Windows. Para obtener más información sobre cómo habilitar el modo FIPS en Windows, acceda a <https://support.microsoft.com/en-us/kb/811833>.

Nota Horizon Administrator no indica si Horizon 7 se está ejecutando en modo FIPS.

Para instalar Horizon 7 en modo FIPS, realice las siguientes tareas administrativas.

- Al instalar el servidor de conexión, seleccione la opción del modo FIPS. Consulte [Instalar el servidor de conexión de Horizon con una nueva configuración](#).
- Al instalar el servidor de réplica, seleccione la opción del modo FIPS. Consulte [Instalar una instancia replicada del servidor de conexión de Horizon](#).

- Antes de instalar un servidor de seguridad, anule la selección de la opción global **Usar IPsec para las conexiones del servidor de seguridad** en Horizon Administrator y configure IPsec manualmente. Consulte <http://kb.vmware.com/kb/2000175>.
- Al instalar el servidor de seguridad, seleccione la opción del modo FIPS. Consulte [Instalar un servidor de seguridad](#).
- Cuando un sistema de Windows está configurado para que FIPS funcione y Horizon 7 está configurado para comunicar un servidor de conexión y un servidor de seguridad mediante IPsec, no se puede instalar el servidor de seguridad. En el caso de un entorno IPv4, especifique la URL externa de PCoIP como una dirección IP y el número de puerto 4172. En el caso de un entorno IPv6, puede especificar la dirección IP o el nombre de dominio plenamente cualificado y el número de puerto 4172. En ambos casos, no incluya el nombre del protocolo.

Por ejemplo, en un entorno IPv4: 10.20.30.40:4172

Los clientes deben poder usar la URL para alcanzar el servidor de seguridad.

- Deshabilite los cifrados débiles para las máquinas de View Composer y Horizon Agent. Consulte [Deshabilitar cifrados débiles en SSL/TLS](#).
- Al instalar View Composer, seleccione la opción del modo FIPS. Consulte [Capítulo 6 Instalar View Composer](#).
- Al instalar Horizon Agent, seleccione la opción del modo FIPS. Consulte los temas sobre la instalación de Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7 o Configurar aplicaciones y escritorios publicados en Horizon 7*.
- En clientes Windows, habilite el modo FIPS en el sistema operativo cliente y seleccione la opción del modo FIPS cuando instale Horizon Client para Windows. Consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*.
- En clientes de Linux, habilite el modo FIPS en el sistema operativo cliente. Consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Linux*.

Requisitos del sistema para el modo FIPS

Para admitir el modo FIPS, la implementación de Horizon 7 debe cumplir los siguientes requisitos.

vSphere

- vCenter Server 6.0 o posterior
- ESXi 6.0 o posterior

Escritorio remoto

- Cualquier plataforma de Windows con un certificado FIPS. Para obtener más información, consulte el artículo sobre la validación FIPS 140 en el sitio web Microsoft TechNet.
- View Agent 6.2 o Horizon Agent 7.0 o versiones posteriores de ambos productos únicamente para plataformas Windows

Horizon Client

- Cualquier plataforma de Windows con un certificado FIPS. Para obtener más información, consulte el artículo sobre la validación FIPS 140 en el sitio web Microsoft TechNet.
- Horizon Client para Windows 3.5 o posterior

Protocolo criptográfico

- TLSv1.2

Preparar Active Directory

5

Horizon 7 utiliza la infraestructura de su infraestructura de Active Directory de Microsoft para la administración y la autenticación del usuario. Debe realizar algunas tareas para preparar Active Directory si quiere utilizarlo con Horizon 7.

Horizon 7 es compatible con estos niveles funcionales de dominios de Active Directory Domain Services (AD DS):

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Este capítulo incluye los siguientes temas:

- [Configurar dominios y relaciones de confianza](#)
- [Crear una OU para los escritorios remotos](#)
- [Crear OU y grupos para cuentas cliente en modo de pantalla completa](#)
- [Crear grupos para usuarios](#)
- [Crear una cuenta de usuario para vCenter Server](#)
- [Crear una cuenta de usuario para un servidor View Composer independiente](#)
- [Crear una cuenta de usuario para operaciones en AD de View Composer](#)
- [Crear una cuenta de usuario para operaciones de clones instantáneos](#)
- [Configurar la directiva Grupos restringidos](#)
- [Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7](#)
- [Preparar Active Directory para la autenticación con tarjeta inteligente](#)
- [Deshabilitar cifrados débiles en SSL/TLS](#)

Configurar dominios y relaciones de confianza

Debe conectar cada host del servidor de conexión a un dominio de Active Directory. El host no debe ser un controlador de dominio.

Active Directory también administra las máquinas Horizon Agent, incluidos los host RD y las máquinas de un solo usuario, así como los usuarios y grupos de la implementación de Horizon 7. Puede autorizar usuarios y grupos para que utilicen aplicaciones y escritorios remotos, además de seleccionarlos para que sean administradores en Horizon Administrator.

Puede colocar máquinas Horizon Agent, servidores de View Composer, usuarios y grupos en los siguientes dominios de Active Directory:

- El dominio del servidor de conexión
- Un dominio diferente que tiene una relación de confianza bidireccional con el dominio del servidor de conexión.
- Un dominio en un bosque diferente al del dominio del servidor de conexión. Este último debe confiar de manera unidireccional y externa en él o debe existir una relación de confianza entre el dominio y un dominio kerberos.
- Un dominio en un bosque diferente al del dominio del servidor de conexión. Este último debe confiar de manera unidireccional en él o debe existir una relación de confianza transitiva bidireccional entre ambos.

Active Directory autentica los usuarios en el dominio del servidor de conexión y en otros dominios de usuario adicionales con los que exista un acuerdo de confianza.

Si los usuarios y los grupos se encuentran en dominios de confianza unidireccional, debe proporcionar credenciales secundarias para los usuarios administradores en Horizon Administrator. Los administradores deben poseer credenciales secundarias para darles acceso a los dominios de confianza unidireccionales. Un dominio de confianza unidireccional puede ser un dominio externo o un dominio en una confianza de bosque transitiva.

Las credenciales secundarias solo son necesarias para sesiones de Horizon Administrator, no para escritorios de usuarios finales ni sesiones de aplicaciones. Solo los usuarios administradores necesitan credenciales secundarias.

Puede proporcionar credencial secundarias si utiliza el comando `vdmadmin -T`.

- Configure credenciales secundarias para usuarios administradores individuales.
- En una confianza de bosque, puede configurar credenciales secundarias para el dominio raíz del bosque. A continuación, el servidor de conexión podrá enumerar dominios secundarios en la confianza de bosque.

Para obtener más información, consulte "Proporcionar credenciales secundarias para los administradores con la opción -T" en el documento *Administración de Horizon 7*.

En los dominios de confianza unidireccional no se admite la autenticación de usuarios tipo SAML o con tarjeta inteligente.

A partir de la versión 7.10 de Horizon 7, la función Iniciar sesión como usuario actual en Horizon Client para Windows es compatible con dominios de confianza unidireccional.

Nota Puesto que los servidores de seguridad no tienen acceso a los repositorios de autenticación, incluidos los de Active Directory, no es necesario que estén ubicados en un dominio de Active Directory.

Relaciones de confianza y filtros de dominio

Para determinar a qué dominios puede acceder, una instancia del servidor de conexión atraviesa las relaciones de confianza comenzando por su propio dominio.

En un conjunto de dominios reducido y conectado correctamente, el servidor de conexión puede determinar rápidamente la lista completa de dominios, pero la duración de este proceso aumenta a medida que lo hace el número de dominios o que disminuye la conectividad entre ellos. La lista también puede incluir los dominios que prefiera no ofrecer a los usuarios cuando se conecten a las aplicaciones y los escritorios remotos.

Puede usar el comando `vdadmin` para configurar los filtros de los dominios de forma que limiten los dominios en los que la instancia del servidor de conexión busca y que muestra a los usuarios. Consulte el documento *Administración de Horizon 7* para obtener más información.

Si una confianza de bosque está configurada con exclusiones de sufijos de los nombres, las exclusiones configuradas se utilizan para filtrar la lista de los dominios secundarios de bosques. Además de los filtros que se especifican con el comando `vdadmin`, se aplican los filtros de exclusión de sufijos de los nombres.

Crear una OU para los escritorios remotos

Debe crear una unidad organizativa (OU) específicamente para los escritorios remotos. Una OU es una subdivisión de Active Directory que contiene usuarios, grupos, equipos u otras OU.

Para evitar que se aplique la configuración de la directiva de grupo en otros servidores de Windows u otras estaciones de trabajo en el mismo dominio que los escritorios, puede crear un GPO para las directivas de grupo de Horizon 7 y vincularlo a la OU que contiene escritorios remotos. También puede delegar el control de la OU a los grupos subordinados, como, por ejemplo, los operadores de servidor o los usuarios individuales.

Si usa View Composer, debe crear un contenedor de Active Directory independiente para los escritorios de clonación vinculada que se basa en la OU del escritorio remoto. Los administradores con privilegios de OU en Active Directory pueden aprovisionar escritorios de clonación vinculada sin privilegios de administrador de dominio. Si cambia las credenciales de administrador en Active Directory, también puede actualizar la información de las credenciales en View Composer.

Crear OU y grupos para cuentas cliente en modo de pantalla completa

Un cliente en modo de pantalla completa es un cliente ligero o un equipo bloqueado que ejecuta el software cliente para conectarse a una instancia del servidor de conexión e iniciar una sesión de escritorio remoto. Si configura clientes en modo de pantalla completa, debe crear las OU y los grupos dedicados en Active Directory para las cuentas cliente en modo de pantalla completa.

La creación de las OU y de los grupos dedicados para las cuentas cliente en modo de pantalla completa divide los sistemas cliente frente a una intrusión no deseada y simplifica la administración y la configuración cliente.

Consulte el documento *Administración de Horizon 7* para obtener más información.

Crear grupos para usuarios

Debe crear grupos para diferentes tipos de usuarios en Active Directory. Por ejemplo, puede crear un grupo denominado Usuarios de Horizon 7 para los usuarios finales y otro grupo denominado Administradores de Horizon 7 para los usuarios que administrarán las aplicaciones y los escritorios remotos.

Crear una cuenta de usuario para vCenter Server

Debe crear una cuenta de usuario en Active Directory para usarla con vCenter Server. Especifique esta cuenta de usuario cuando agregue una instancia de vCenter Server en Horizon Administrator.

Debe otorgar privilegios de cuenta de usuario para realizar ciertas operaciones en vCenter Server. Puede crear una función de vCenter Server con los privilegios apropiados y asignar la función al usuario de vCenter Server. La lista de privilegios que agrega a la función vCenter Server varía, dependiendo de si usa Horizon 7 con o sin View Composer. Consulte [Configurar cuentas de usuario para vCenter Server, View Composer y clones instantáneos](#) para obtener más información sobre cómo configurar estos privilegios.

Si instala View Composer en el mismo equipo que vCenter Server, debe agregar el usuario de vCenter Server al grupo local Administradores en el equipo vCenter Server. Este requisito permite a Horizon 7 autenticarse en el servicio de View Composer.

Si instala View Composer en una máquina diferente a vCenter Server, no es necesario que el usuario de vCenter Server sea un administrador local en el equipo vCenter Server. Sin embargo, debe crear una cuenta independiente de usuario del servidor de View Composer que tenga la función de administrador local en el equipo View Composer.

Crear una cuenta de usuario para un servidor View Composer independiente

Si instala View Composer en una máquina diferente a la que utilizó para instalar vCenter Server, debe crear una cuenta de usuario del dominio en Active Directory que Horizon 7 pueda utilizar para autenticar el servicio View Composer en una máquina independiente.

La cuenta de usuario debe encontrarse en el mismo dominio que el host del servidor de conexión o en un dominio de confianza. Debe agregar la cuenta de usuario al grupo de administradores locales en la máquina View Composer independiente.

Especifique esta cuenta de usuario al configurar las opciones de View Composer en Horizon Administrator y seleccione **Servidor View Composer independiente**. Consulte [Configurar las opciones de View Composer](#).

Crear una cuenta de usuario para operaciones en AD de View Composer

Si usa View Composer, debe crear una cuenta de usuario en Active Directory que permita a View Composer realizar algunas operaciones en Active Directory. View Composer necesita que esta cuenta conecte las máquinas virtuales de clones vinculados con el dominio de Active Directory.

Para garantizar la seguridad, debe crear una cuenta de usuario independiente que se usará con View Composer. Al crear una cuenta independiente, puede garantizar que no tenga privilegios adicionales a los definidos para otros propósitos. Puede otorgar a la cuenta los privilegios mínimos necesarios para crear y eliminar objetos del equipo en un contenedor de Active Directory especificado. Por ejemplo, la cuenta de View Composer no necesita privilegios de administrador de dominio.

Procedimiento

- 1 En Active Directory, cree una cuenta de usuario en el mismo dominio que el host del servidor de conexión o en un dominio de confianza.
- 2 Agregue los permisos para **crear objetos de equipo, eliminar objetos de equipo y escribir todas las propiedades** en la cuenta del contenedor de Active Directory en el que se crearon las cuentas de los equipos de clones vinculados o al que estas se movieron.

La siguiente lista muestra todos los permisos necesarios para la cuenta de usuario, incluidos los permisos que se asignan de manera predeterminada:

- Mostrar contenido
- Leer todas las propiedades
- Escribir todas las propiedades
- Permisos de lectura
- Restablecer contraseña
- Crear objetos de equipo

- Eliminar objetos de equipo

Nota Se requieren menos permisos si selecciona la opción **Permitir la reutilización de cuentas de equipo existentes** para un grupo de escritorios. Asegúrese de que los siguientes permisos se asignaron a la cuenta de usuario:

- Mostrar contenido
 - Leer todas las propiedades
 - Permisos de lectura
 - Restablecer contraseña
-

- 3 Asegúrese de que los permisos de la cuenta de usuario se aplican al contenedor de Active Directory y a todos los objetos secundarios del contenedor.

Pasos siguientes

Especifique la cuenta en Horizon Administrator cuando configure los dominios de View Composer en el asistente Agregar vCenter Server y cuando configure e implemente los grupos de escritorios de clones vinculados.

Crear una cuenta de usuario para operaciones de clones instantáneos

Antes de implementar los clones instantáneos, debe crear una cuenta de usuario que tenga permiso para realizar ciertas operaciones en Active Directory.

Seleccione esta cuenta cuando agregue un administrador de dominio de clones instantáneos antes de implementar grupos de escritorios de clones instantáneos. Para obtener más información, consulte el apartado sobre cómo agregar un administrador de dominio de clones instantáneos en el documento *Configurar escritorios virtuales en Horizon 7*.

Procedimiento

- 1 En Active Directory, cree una cuenta de usuario en el mismo dominio que el servidor de conexión o en un dominio de confianza.
- 2 Agregue los permisos para **crear objetos de equipo**, **eliminar objetos de equipo** y **escribir todas las propiedades** en la cuenta del contenedor de las cuentas del equipo de clones instantáneos.

La siguiente lista muestra los permisos necesarios para la cuenta de usuario, incluidos los permisos que se asignan de manera predeterminada:

- Mostrar contenido
- Leer todas las propiedades
- Escribir todas las propiedades
- Permisos de lectura

- Restablecer contraseña
- Crear objetos de equipo
- Eliminar objetos de equipo

Asegúrese de que los permisos se apliquen al contenedor correcto y a todos los objetos secundarios del contenedor.

Configurar la directiva Grupos restringidos

Para poder conectarse a los escritorios remotos, los usuarios deben pertenecer al grupo Usuarios de escritorio remoto de dicho escritorio. Puede usar la directiva Grupos restringidos en Active Directory para agregar usuarios o grupos al grupo local Usuarios de escritorio remoto de cada escritorio remoto que está conectado al dominio.

La directiva Grupos restringidos establece la pertenencia del grupo local de equipos en el dominio que coincide con las opciones de la lista de pertenencia definida en la directiva Grupos restringidos. Los miembros del grupo de usuarios del escritorio remoto se agregan siempre al grupo Usuarios de escritorio remoto en cada escritorio remoto que se conecta al dominio. Cuando se agregan nuevos usuarios, solo es necesario que los agregue al grupo de usuarios del escritorio remoto.

Estos pasos se aplican al servidor de Active Directory en el dominio en el que se unen las aplicaciones y los escritorios virtuales o publicados de Horizon 7.

Requisitos previos

Cree un grupo para los usuarios del escritorio remoto en el dominio de Active Directory. Por ejemplo, cree un grupo denominado "Usuarios de Horizon".

Procedimiento

- 1 En el servidor de Active Directory, diríjase al complemento Administración de directivas de grupo.

Versión de AD	Ruta de navegación
Windows 2003	<ol style="list-style-type: none"> a Seleccione Inicio > Todos los programas > Herramientas administrativas > Usuarios y equipos de Active Directory. b Haga clic con el botón secundario en el dominio y, a continuación, en Propiedades. c En la pestaña Directiva de grupo, haga clic en Abrir para abrir el complemento Administración de directivas de grupo. d Haga clic con el botón secundario en Directiva predeterminada de dominio y seleccione Editar.
Windows 2008	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.

Versión de AD	Ruta de navegación
Windows 2012 R2	<ol style="list-style-type: none"> Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.
Windows 2016	<ol style="list-style-type: none"> Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.

- 2 Expanda la sección **Configuración del equipo** y abra **Configuración de Windows\Configuración de seguridad**.
- 3 Haga clic con el botón secundario en **Grupos restringidos**, seleccione **Agregar grupo** y agregue el grupo Usuarios de escritorio remoto.
- 4 Haga clic con el botón secundario en el grupo y agregue el nuevo grupo de usuarios de escritorio remoto a la lista de pertenencia a grupos.
Por ejemplo, agregue "Usuarios de Horizon" al grupo Usuarios de escritorio remoto.
- 5 Haga clic en **Aceptar** para guardar los cambios.

Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7

Horizon 7 incluye varios archivos de plantillas administrativas (ADMX) de directivas de grupo, específicos para los componentes.

Todos los archivos ADMX proporcionados por la configuración de las directivas de grupo para Horizon 7 están disponibles en VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip, donde x.x.x es la versión e yyyyyyy es el número de compilación. Puede descargar el archivo desde el sitio de descargas de VMware en <https://my.vmware.com/web/vmware/downloads>. En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el archivo ZIP.

Puede optimizar y asegurar los escritorios remotos al agregar la configuración de las directivas a estos archivos para un GPO nuevo o ya existente de Active Directory y, a continuación, vincular ese GPO a la OU que contiene los escritorios.

Consulte los documentos *Administración de Horizon 7* y *Configurar funciones de escritorios remotos en Horizon 7* para obtener información sobre cómo usar la configuración de las directivas de grupo de Horizon 7.

Preparar Active Directory para la autenticación con tarjeta inteligente

Es posible que deba realizar varias tareas en Active Directory al implementar la autenticación con tarjeta inteligente.

- **Agregar UPN para usuarios de tarjetas inteligentes**

Como los inicios de sesión de tarjetas inteligentes se basan en los nombres principales de usuarios (UPN), las cuentas de Active Directory de usuarios y administradores que usan tarjetas inteligentes para autenticarse en Horizon 7 deben tener un UPN válido.

- **Agregar el certificado raíz a las entidades de certificación raíz de confianza**

Si utiliza una entidad de certificación (CA) para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado raíz a la directiva de grupo Entidades de certificación raíz de confianza en Active Directory. No es necesario realizar este procedimiento si el controlador de dominio de Windows actúa como la CA raíz.

- **Agregar un certificado intermedio a las entidades de certificación intermedias**

Si utiliza una entidad de certificación intermedia (CA) para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado intermedio a la directiva de grupo Entidades de certificación en Active Directory.

- **Agregar el certificado raíz al almacén Enterprise NTAAuth**

Si utiliza una CA para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado raíz al almacén Enterprise NTAAuth en Active Directory. No es necesario realizar este procedimiento si el controlador de dominio de Windows actúa como la CA raíz.

Agregar UPN para usuarios de tarjetas inteligentes

Como los inicios de sesión de tarjetas inteligentes se basan en los nombres principales de usuarios (UPN), las cuentas de Active Directory de usuarios y administradores que usan tarjetas inteligentes para autenticarse en Horizon 7 deben tener un UPN válido.

Si el dominio en el que reside el usuario de tarjeta inteligente es distinto al dominio desde el que se emitió el certificado raíz, se debe establecer el UPN del usuario en el nombre alternativo del sujeto (SAN) que contiene el certificado raíz de la entidad de certificación de confianza. Si se expidió el certificado raíz desde un servidor del dominio actual del usuario de la tarjeta inteligente, no será necesario modificar el UPN del usuario.

Nota Es posible que necesite configurar el UPN de las cuentas de Active Directory integradas, aunque se expida el certificado desde el mismo dominio. Las cuentas integradas, incluido el administrador, no tienen un UPN establecido de forma predeterminada.

Requisitos previos

- Obtenga el SAN contenido en el certificado raíz de la CA de confianza viendo las propiedades del certificado.
- Si la utilidad Editor ADSI no se encuentra en el servidor de Active Directory, descargue e instale Herramientas de soporte de Windows desde el sitio web de Microsoft.

Procedimiento

- 1 En el servidor de Active Directory, inicie la utilidad Editor ADSI.
- 2 En el panel situado a la izquierda, expanda el dominio en el que el usuario está ubicado y haga doble clic en CN=Users.
- 3 En el panel situado a la derecha, haga clic con el botón secundario y luego haga clic en **Propiedades**.
- 4 Haga doble clic en el atributo userPrincipalName y escriba el valor SAN del certificado CA de confianza.
- 5 Haga clic en **Aceptar** para guardar la configuración del atributo.

Agregar el certificado raíz a las entidades de certificación raíz de confianza

Si utiliza una entidad de certificación (CA) para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado raíz a la directiva de grupo Entidades de certificación raíz de confianza en Active Directory. No es necesario realizar este procedimiento si el controlador de dominio de Windows actúa como la CA raíz.

Procedimiento

- 1 En el servidor de Active Directory, diríjase al complemento Administración de directivas de grupo.

Versión de AD	Ruta de navegación
Windows 2003	<ol style="list-style-type: none"> a Seleccione Inicio > Todos los programas > Herramientas administrativas > Usuarios y equipos de Active Directory. b Haga clic con el botón secundario en el dominio y, a continuación, en Propiedades. c En la pestaña Directiva de grupo, haga clic en Abrir para abrir el complemento Administración de directivas de grupo. d Haga clic con el botón secundario en Directiva predeterminada de dominio y seleccione Editar.
Windows 2008	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.

Versión de AD	Ruta de navegación
Windows 2012 R2	<ul style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.
Windows 2016	<ul style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.

- 2 Expanda la sección **Configuración del equipo** y abra **Configuración de Windows\Configuración de seguridad\Clave pública**.
- 3 Haga clic con el botón secundario en **Entidades de certificación raíz de confianza** y seleccione **Importar**.
- 4 Siga las instrucciones del asistente para importar el certificado intermedio (por ejemplo, rootCA.cer) y haga clic en **Aceptar**.
- 5 Cierre la ventana Directiva de grupo.

Resultados

Todos los sistemas que se encuentren en el dominio contarán con una copia del certificado raíz en el almacén raíz de confianza.

Pasos siguientes

Si una entidad de certificación intermedia (CA) expide certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, agregue el certificado intermedio a la directiva de grupo Entidades de certificación en Active Directory. Consulte [Agregar un certificado intermedio a las entidades de certificación intermedias](#).

Agregar un certificado intermedio a las entidades de certificación intermedias

Si utiliza una entidad de certificación intermedia (CA) para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado intermedio a la directiva de grupo Entidades de certificación en Active Directory.

Procedimiento

- 1 En el servidor de Active Directory, diríjase al complemento Administración de directivas de grupo.

Versión de AD	Ruta de navegación
Windows 2003	<ol style="list-style-type: none"> a Seleccione Inicio > Todos los programas > Herramientas administrativas > Usuarios y equipos de Active Directory. b Haga clic con el botón secundario en el dominio y, a continuación, en Propiedades. c En la pestaña Directiva de grupo, haga clic en Abrir para abrir el complemento Administración de directivas de grupo. d Haga clic con el botón secundario en Directiva predeterminada de dominio y seleccione Editar.
Windows 2008	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.
Windows 2012 R2	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.
Windows 2016	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.

- 2 Expanda la sección **Configuración del equipo** y abra la directiva de **Configuración de Windows \Configuración de seguridad\Clave pública**.
- 3 Haga clic con el botón secundario en **Entidades de certificación intermedias** y seleccione **Importar**.
- 4 Siga las instrucciones del asistente para importar el certificado intermedio (por ejemplo, intermediateCA.cer) y haga clic en **Aceptar**.
- 5 Cierre la ventana Directiva de grupo.

Resultados

Todos los sistemas que se encuentren en el dominio contarán con una copia del certificado intermedio en el almacén de entidades de certificación intermedias.

Agregar el certificado raíz al almacén Enterprise NTAUTH

Si utiliza una CA para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado raíz al almacén Enterprise NTAUTH en Active Directory. No es necesario realizar este procedimiento si el controlador de dominio de Windows actúa como la CA raíz.

Procedimiento

- ◆ En el servidor de Active Directory, use el comando `certutil` para publicar el certificado en el almacén Enterprise NTAAuth.

Por ejemplo: `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

Resultados

Ahora, la CA es de confianza para expedir certificados de este tipo.

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 y en View Composer 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 Composer y View Agent para que se aplique la nueva directiva de grupo.

Instalar View Composer

6

Para usar View Composer, cree una base de datos de View Composer, instale el servicio de View Composer y optimice la infraestructura de View para admitir este servicio. Puede instalar el servicio de View Composer en el mismo host que vCenter Server o en un host independiente.

View Composer es una función opcional. Instale View Composer si pretende implementar grupos de escritorios de clones vinculados.

Debe tener una licencia para instalar y usar la función View Composer.

Nota Antes de instalar View Composer, compruebe que preparó Active Directory.

Nota Si instala View Composer en la misma máquina en la que está instalado vCenter Server 6.5, el comportamiento de View Composer puede ser diferente en vCenter Server. Para obtener más información, consulte el artículo de la base de conocimientos de VMware <https://kb.vmware.com/s/article/2150066>.

Este capítulo incluye los siguientes temas:

- [Preparar una base de datos de View Composer](#)
- [Configurar un certificado SSL para View Composer](#)
- [Instalar el servicio de View Composer](#)
- [Habilitar TLSv1.0 en vCenter y conexiones ESXi desde View Composer](#)
- [Configurar la infraestructura de View Composer](#)

Preparar una base de datos de View Composer

Debe crear una base de datos y un nombre de origen de datos (DNS) para almacenar información de View Composer.

El servicio de View Composer no incluye una base de datos. Si no existe ninguna instancia de base de datos en su entorno de red, debe instalar una. Después de hacerlo, agregue la base de datos de View Composer a la instancia.

Puede agregarla a la instancia en la que se encuentra la base de datos de vCenter Server. La base de datos se puede configurar de forma local o remota en un equipo Windows Server, UNIX o Linux conectado a la red.

La base de datos de View Composer almacena información sobre las conexiones y los componentes que utiliza View Composer:

- Conexiones de vCenter Server
- Conexiones de Active Directory
- Escritorios de clones vinculados implementados por View Composer
- Réplicas creadas por View Composer

Cada instancia del servicio de View Composer debe tener su propia base de datos de View Composer. Varios servicios de View Composer no pueden compartir una base de datos de View Composer.

Para obtener una lista de versiones de bases de datos compatibles, consulte [Requisitos de base de datos para View Composer y para bases de datos de eventos](#).

Para agregar una base de datos de View Composer a una instancia de una base de datos instalada, elija uno de estos procedimientos.

- [Crear una base de datos SQL Server para View Composer](#)

View Composer puede almacenar información de los escritorios de clones vinculados en una base de datos SQL Server. Puede crear una base de datos de View Composer agregándola a SQL Server y configurando un origen de datos ODBC para ella.

- [Crear una base de datos de Oracle para View Composer](#)

View Composer puede almacenar información de los escritorios de clones vinculados en una base de datos Oracle 11g o 12c. Puede crear una base de datos de View Composer agregándola a una instancia de Oracle existente y configurando un origen de datos ODBC para ella. Puede agregar una nueva base de datos de View Composer usando el asistente de configuración de la base de datos de Oracle o ejecutando una instrucción SQL.

Crear una base de datos SQL Server para View Composer

View Composer puede almacenar información de los escritorios de clones vinculados en una base de datos SQL Server. Puede crear una base de datos de View Composer agregándola a SQL Server y configurando un origen de datos ODBC para ella.

Procedimiento

1 [Agregar una base de datos de View Composer a SQL Server](#)

Es posible agregar una nueva base de datos de View Composer a una instancia de Microsoft SQL Server ya existente para almacenar datos de clones vinculados en View Composer.

2 (opcional) Establecer los permisos de la base de datos SQL Server creando funciones de las bases de datos de forma manual

Al usar este método recomendado, el administrador de la base de datos de View Composer puede establecer que los permisos de los administradores de View Composer se otorguen a través de las funciones de la base de datos de Microsoft SQL Server.

3 Agregar un origen de datos ODBC a SQL Server

Después de agregar una base de datos de View Composer a SQL Server, debe configurar una conexión ODBC a la nueva base de datos para que el origen de datos sea visible para el servicio de View Composer.

Agregar una base de datos de View Composer a SQL Server

Es posible agregar una nueva base de datos de View Composer a una instancia de Microsoft SQL Server ya existente para almacenar datos de clones vinculados en View Composer.

Si una base de datos se encuentra en las instalaciones, en el sistema en el que View Composer se instalará, puede usar el modelo de seguridad Autenticación de Windows integrada. Si la base de datos se encuentra en un sistema remoto, no puede usar este método de autenticación.

Requisitos previos

- Compruebe que se instaló una versión compatible de SQL Server en el equipo en el que instalará View Composer o en el entorno de red. Para obtener más información, consulte [Requisitos de base de datos para View Composer y para bases de datos de eventos](#).
- Compruebe que usa SQL Server Management Studio para crear y administrar la base de datos. De forma alternativa, puede usar SQL Server Management Studio Express, que se puede descargar e instalar desde el siguiente sitio web.

<http://www.microsoft.com/en-us/download/details.aspx?id=7593>

Procedimiento

- 1 En el equipo de View Composer, seleccione **Inicio > Todos los programas > Microsoft SQL Server 2014, Microsoft SQL Server 2012 o Microsoft SQL Server 2008**.
- 2 Seleccione **SQL Server Management Studio** y conéctelo a la instancia de SQL Server.
- 3 En el panel Explorador de objetos, haga clic con el botón secundario en la entrada Base de datos y seleccione **Nueva base de datos**.

Puede usar los valores predeterminados para los parámetros `Initial size` y `Autogrowth` para la base de datos y los archivos de registro.
- 4 En el cuadro de diálogo Nueva base de datos, escriba un nombre en el cuadro de texto Nombre de base de datos.

Por ejemplo: **ViewComposer**

5 Haga clic en **Aceptar**.

SQL Server Management Studio agrega la base de datos a la entrada Bases de datos en el panel Explorador de objetos.

6 Cierre Microsoft SQL Server Management Studio.

Pasos siguientes

De forma opcional, siga las instrucciones que aparecen en [Establecer los permisos de la base de datos SQL Server creando funciones de las bases de datos de forma manual](#)

Siga las instrucciones de [Agregar un origen de datos ODBC a SQL Server](#).

Establecer los permisos de la base de datos SQL Server creando funciones de las bases de datos de forma manual

Al usar este método recomendado, el administrador de la base de datos de View Composer puede establecer que los permisos de los administradores de View Composer se otorguen a través de las funciones de la base de datos de Microsoft SQL Server.

VMware recomienda este método ya que elimina el requisito de establecer la función **db_owner** para los administradores de View Composer, quienes instalan y actualizan View Composer.

En este procedimiento, puede proporcionar los nombres que desee para inicio de sesión de la base de datos, para nombre de usuario y para las funciones de la base de datos. El usuario **[vcmpuser]** y las funciones de la base de datos **VCMP_ADMIN_ROLE** y **VCMP_USER_ROLE** son nombres de ejemplo. Al crear la base de datos de View Composer, también se crea el esquema **dbo**. Debe usar el nombre del esquema **dbo**.

Requisitos previos

- Compruebe que se creó una base de datos de View Composer. Consulte [Agregar una base de datos de View Composer a SQL Server](#).

Procedimiento

- 1 Inicie una sesión de Microsoft SQL Server Management Studio como administrador del sistema (SA) o con una cuenta con privilegios **sysadmin**.
- 2 Cree un usuario que reciba los permisos apropiados de la base de datos SQL Server.

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

- 3 En la base de datos de View Composer, cree la función **VCMP_ADMIN_ROLE**.
- 4 En la base de datos de View Composer, otorgue los privilegios a **VCMP_ADMIN_ROLE**.
 - a Otorgue los permisos del esquema **ALTER**, **REFERENCES** e **INSERT** en el esquema **dbo**.
 - b Otorgue los permisos **CREATE TABLE**, **CREATE VIEW** y **CREATE PROCEDURES**.
- 5 En la base de datos de View Composer, cree **VCMP_USER_ROLE**.
- 6 En la base de datos de View Composer, otorgue los permisos del esquema **SELECT**, **INSERT**, **DELETE**, **UPDATE** y **EXECUTE** en el esquema **dbo** de **VCMP_USER_ROLE**.
- 7 Otorgue **VCMP_USER_ROLE** al usuario **[vcmpuser]**.
- 8 Otorgue **VCMP_ADMIN_ROLE** al usuario **[vcmpuser]**.
- 9 En la base de datos de MSDB, cree la función **VCMP_ADMIN_ROLE**.
- 10 Otorgue privilegios a **VCMP_ADMIN_ROLE** en MSDB.
 - a En las tablas MSDB syscategories, sysjobsteps y sysjobs, otorgue el permiso **SELECT** al usuario **[vcmpuser]**.
 - b En los procedimientos almacenados de MSDB sp_add_job, sp_delete_job, sp_add_jobstep, sp_update_job, sp_add_jobserver, sp_add_jobschedule y sp_add_category, otorgue el permiso **EXECUTE** a la función **VCMP_ADMIN_ROLE**.
- 11 En la base de datos MSDB, otorgue **VCMP_ADMIN_ROLE** al usuario **[vcmpuser]**.
- 12 Cree el DSN de sistema ODBC usando el inicio de sesión de SQL Server **vcmpuser**.

Para obtener instrucciones, consulte [Agregar un origen de datos ODBC a SQL Server](#).
- 13 Instale View Composer.

Para obtener instrucciones, consulte [Instalar el servicio de View Composer](#).
- 14 En la base de datos MSDB, revoque **VCMP_ADMIN_ROLE** del usuario **[vcmpuser]**.

Después de revocar la función, puede dejarla como inactiva o eliminarla para obtener una mayor seguridad.

Agregar un origen de datos ODBC a SQL Server

Después de agregar una base de datos de View Composer a SQL Server, debe configurar una conexión ODBC a la nueva base de datos para que el origen de datos sea visible para el servicio de View Composer.

Cuando configura ODBC DNS para View Composer, proteja la conexión de la base de datos subyacente al nivel apropiado para su entorno. Para obtener más información sobre cómo proteger las conexiones de la base de datos, consulte la documentación SQL Server.

Si la conexión de la base de datos subyacente usa un cifrado SSL, le recomendamos que configure los servidores de la base de datos con certificados SSL firmados por una CA de confianza. Si usa certificados autofirmados, las conexiones de la base de datos pueden ser susceptibles de ataques de intermediarios.

Requisitos previos

Complete los pasos que se describen en [Agregar una base de datos de View Composer a SQL Server](#).

Procedimiento

- 1 En el equipo en el que se instalará View Composer, seleccione **Inicio > Herramientas administrativas > Orígenes de datos (ODBC)**.
- 2 Seleccione la pestaña **DSN de sistema**.
- 3 Haga clic en **Agregar** y, en la lista, seleccione **SQL Native Client**.
- 4 Haga clic en **Finalizar**.
- 5 En el asistente de configuración **Crear un nuevo origen de datos para SQL Server**, escriba un nombre y una descripción de la base de datos de View Composer.
Por ejemplo: **ViewComposer**
- 6 En el cuadro de texto Servidor, escriba el nombre de la base de datos SQL Server.
Use la forma *nombre_host\nombre_servidor*, donde *nombre_host* es el nombre del equipo y *nombre_servidor* es la instancia de SQL Server.
Por ejemplo: **VCHOST1\VIM_SQLEXP**
- 7 Haga clic en **Siguiente**.
- 8 Compruebe que esté seleccionada la casilla de verificación **Conectar con SQL Server para obtener la configuración predeterminada de las opciones de configuración adicionales** y seleccione una opción de autenticación.

Opción	Descripción
Autenticación de Windows integrada	Seleccione esta opción si utiliza una instancia local de SQL Server. Esta opción también se conoce como autenticación de confianza. Solo se admite la autenticación de Windows integrada si SQL Server se ejecuta en el equipo local.
Autenticación de SQL Server	Seleccione esta opción si utiliza una instancia remota de SQL Server. La autenticación de Windows NT no se admite en SQL Server remoto. Si configura de forma manual los permisos de la base de datos SQL Server y los asigna a un usuario, auténtíquese como ese usuario. Por ejemplo, auténtíquese como el usuario vcmpuser . De lo contrario, auténtíquese como el administrador del sistema (SA) o como una cuenta de usuario con privilegios sysadmin .

- 9 Haga clic en **Siguiente**.
- 10 Seleccione la casilla de verificación **Establecer la siguiente base de datos como predeterminada** y seleccione el nombre de la base de datos de View Composer de la lista.
Por ejemplo: **ViewComposer**
- 11 Si la conexión de SQL Server está configurada con SSL habilitado, diríjase a la página Configuración DSN de Microsoft SQL Server y seleccione **Usar cifrado de alta seguridad para los datos**.
- 12 Finalice y cierre el asistente **Administrador de orígenes de datos Microsoft ODBC**.

Pasos siguientes

Instale el nuevo servicio de View Composer. Consulte [Instalar el servicio de View Composer](#).

Crear una base de datos de Oracle para View Composer

View Composer puede almacenar información de los escritorios de clones vinculados en una base de datos Oracle 11g o 12c. Puede crear una base de datos de View Composer agregándola a una instancia de Oracle existente y configurando un origen de datos ODBC para ella. Puede agregar una nueva base de datos de View Composer usando el asistente de configuración de la base de datos de Oracle o ejecutando una instrucción SQL.

- [Agregar una base de datos de View Composer a Oracle 12c o 11g](#)

Puede usar el asistente de configuración de la base de datos de Oracle para agregar una nueva base de datos de View Composer a una instancia de Oracle 12c o 11g.

- [Usar una instrucción SQL para agregar una base de datos de View Composer a una instancia de Oracle](#)

- [Configurar un usuario de una base de datos de Oracle para View Composer](#)

De forma predeterminada, el usuario que ejecuta la base de datos de View Composer tiene permisos de administrador de sistema Oracle. Para restringir los permisos de seguridad del usuario que ejecuta la base de datos de View Composer, debe configurar una base de datos de Oracle con permisos específicos.

- [Agregar un origen de datos ODBC a Oracle 12c o 11g](#)

Después de agregar una base de datos de View Composer a una instancia de Oracle 12c o 11g, debe configurar una conexión ODBC a la nueva base de datos para que el origen de datos sea visible para el servicio de View Composer.

Agregar una base de datos de View Composer a Oracle 12c o 11g

Puede usar el asistente de configuración de la base de datos de Oracle para agregar una nueva base de datos de View Composer a una instancia de Oracle 12c o 11g.

Requisitos previos

Compruebe que esté instalada una versión compatible de Oracle 12c o 11g en el equipo local o remoto. Consulte [Requisitos de base de datos para View Composer y para bases de datos de eventos](#).

Procedimiento

- 1 Inicie el **Asistente de configuración de la base de datos** en el equipo en el que desea agregar la base de datos de View Composer.

Versión de la base de datos	Acción
Oracle 12c	Seleccione Inicio > Todos los programas > Oracle-OraDb12c_home > Herramientas de migración y configuración > Asistente de configuración de la base de datos.
Oracle 11g	Seleccione Inicio > Todos los programas > Oracle-OraDb11g_home > Herramientas de migración y configuración > Asistente de configuración de la base de datos.

- 2 En la página Operaciones, seleccione **Crear una base de datos**.
- 3 En la página Plantillas de base de datos, seleccione la plantilla **Uso general o procesamiento de transacción**.
- 4 En la página Identificación de la base de datos, escriba un Nombre de base de datos global y un prefijo SID (identificador de sistema de Oracle).

Por simplicidad, use el mismo valor para ambos elementos.
- 5 En la página Opciones de administración, haga clic en **Siguiente** para aceptar la configuración predeterminada.
- 6 En la página Credenciales de base de datos, seleccione **Usar la misma contraseña administrativa para todas las cuentas** y escriba una contraseña.
- 7 En el resto de páginas de configuración, haga clic en **Siguiente** para aceptar la configuración predeterminada.
- 8 En la página Opciones de creación, compruebe que **Crear base de datos** esté seleccionada y haga clic en **Finalizar**.
- 9 En la página Confirmación, revise las opciones y haga clic en **Aceptar**.

La herramienta de configuración crea la base de datos.
- 10 En la página Creación de base de datos completada, haga clic en **Aceptar**.

Pasos siguientes

Siga las instrucciones de [Agregar un origen de datos ODBC a Oracle 12c o 11g](#).

Usar una instrucción SQL para agregar una base de datos de View Composer a una instancia de Oracle

Cuando cree la base de datos, puede personalizar la ubicación de los datos y de los archivos de registro.

Requisitos previos

La base de datos de View Composer debe tener ciertos privilegios y espacios de tabla. Puede usar una instrucción SQL para crear la base de datos de View Composer en una instancia de la base de datos de Oracle 12c o 11g.

Compruebe que esté instalada una versión compatible de Oracle 12c o 11g en el equipo local o remoto. Para obtener más información, consulte [Requisitos de base de datos para View Composer y para bases de datos de eventos](#).

Procedimiento

- 1 Inicie sesión en una sesión SQL*Plus con la cuenta de sistema.
- 2 Ejecute la siguiente instrucción SQL para crear la base de datos.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

En este ejemplo, VCMP es el nombre de ejemplo de la base de datos de View Composer y vcmp01.dbf es el nombre del archivo de la base de datos.

Para una instalación en Windows, use las convenciones de Windows de la ruta del directorio en el archivo vcmp01.dbf.

Pasos siguientes

Si desea ejecutar la base de datos de View Composer con permisos de seguridad específicos, siga las instrucciones de [Configurar un usuario de una base de datos de Oracle para View Composer](#).

Siga las instrucciones de [Agregar un origen de datos ODBC a Oracle 12c o 11g](#)

Configurar un usuario de una base de datos de Oracle para View Composer

De forma predeterminada, el usuario que ejecuta la base de datos de View Composer tiene permisos de administrador de sistema Oracle. Para restringir los permisos de seguridad del usuario que ejecuta la base de datos de View Composer, debe configurar una base de datos de Oracle con permisos específicos.

Requisitos previos

Verifique que se creó una base de datos de View Composer en una instancia Oracle 11g o 12c.

Procedimiento

- 1 Inicie sesión en una sesión SQL*Plus con la cuenta de sistema.
- 2 Ejecute el siguiente comando SQL para crear un usuario de una base de datos de View Composer con los permisos adecuados.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE
"VCMP" ACCOUNT UNLOCK;
```



```
grant connect to VCMPADMIN;
grant resource to VCMPADMIN;
grant create view to VCMPADMIN;
grant create sequence to VCMPADMIN;
grant create table to VCMPADMIN;
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;
```

En este ejemplo, el nombre de usuario es VCMPADMIN y el nombre de la base de datos de View Composer es VCMF.

De forma predeterminada, la función recurso tiene los privilegios `crear procedimiento`, `crear tabla` y `crear secuencias` asignados. Si la función recurso no tiene esos privilegios, es necesario otorgárselos explícitamente al usuario de la base de datos de View Composer.

Agregar un origen de datos ODBC a Oracle 12c o 11g

Después de agregar una base de datos de View Composer a una instancia de Oracle 12c o 11g, debe configurar una conexión ODBC a la nueva base de datos para que el origen de datos sea visible para el servicio de View Composer.

Cuando configura ODBC DNS para View Composer, proteja la conexión de la base de datos subyacente al nivel apropiado para su entorno. Para obtener más información sobre cómo proteger las conexiones de la base de datos, consulte la documentación de las bases de datos de Oracle.

Si la conexión de la base de datos subyacente usa un cifrado SSL, le recomendamos que configure los servidores de la base de datos con certificados SSL firmados por una CA de confianza. Si usa certificados autofirmados, las conexiones de la base de datos pueden ser susceptible de ataques de intermediarios.

Requisitos previos

Compruebe que completó los pasos descritos en [Agregar una base de datos de View Composer a Oracle 12c o 11g](#) o en [Usar una instrucción SQL para agregar una base de datos de View Composer a una instancia de Oracle](#).

Procedimiento

- 1 En el equipo de la base de datos de View Composer, seleccione **Inicio > Herramientas administrativas > Orígenes de datos (ODBC)**.
- 2 En el asistente **Administrador de orígenes de datos Microsoft ODBC**, seleccione la pestaña **DSN de sistema**.
- 3 Haga clic en **Agregar** y seleccione en la lista el controlador de Oracle correspondiente.
Por ejemplo: **OraDb11g_home**
- 4 Haga clic en **Finalizar**.

- 5 En el cuadro de diálogo de la configuración del controlador ODBC de Oracle, escriba el DNS que usará con View Composer, una descripción del origen de datos y un ID de usuario para poder conectarse a la base de datos.

Si configuró un ID de usuario de una base de datos de Oracle con permisos de seguridad específicos, introduzca ese ID.

Nota Use el DSN cuando instale el servicio de View Composer.

- 6 Especifique un **Nombre de servicio TNS** seleccionando el nombre de la base de datos global en el menú desplegable.

El asistente de configuración de la base de datos de Oracle especifica el nombre de la base de datos global.

- 7 Para comprobar el origen de los datos, haga clic en **Probar conexión** y, a continuación, en **Aceptar**.

Pasos siguientes

Instale el nuevo servicio de View Composer. Consulte [Instalar el servicio de View Composer](#).

Configurar un certificado SSL para View Composer

De forma predeterminada, un certificado autofirmado se instala con View Composer. Puede usar el certificado predeterminado para realizar pruebas, pero para el uso de producción, debe reemplazarlo por un certificado firmado por una entidad de certificación (CA).

Puede configurar un certificado antes o después de instalar View Composer. En View 5.1 y versiones posteriores, configure un certificado importándolo en el almacén de certificados del equipo local Windows en el equipo Windows Server donde View Composer está instalado o se instalará.

- Si importa un certificado firmado por una CA antes de que instale View Composer, puede seleccionar el certificado firmado durante la instalación de View Composer. Este procedimiento elimina la tarea manual de reemplazar el certificado predeterminado después de la instalación.
- Si piensa reemplazar un certificado existente o el certificado autofirmado y predeterminado por uno nuevo después de instalar View Composer, debe importar el nuevo certificado y ejecutar la utilidad SviConfig ReplaceCertificate para enlazar el nuevo certificado al puerto que usa View Composer.

Para obtener más detalles sobre cómo configurar certificados SSL y usar la utilidad SviConfig ReplaceCertificate, consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

Si instala vCenter Server y View Composer en el mismo equipo Windows Server, pueden usar el mismo certificado SSL, pero debe configurar el certificado de forma independiente para cada componente.

Instalar el servicio de View Composer

Para usar View Composer, debe instalar el servicio de View Composer. Horizon 7 usa View Composer para crear e implementar escritorios de clonación vinculada en vCenter Server.

Puede instalar el servicio de View Composer en el equipo Windows Server en el que vCenter Server está instalado o en un equipo Windows Server independiente. Una instalación de View Composer independiente funciona con vCenter Server instalado en un equipo Windows Server y con vCenter Server Appliance basado en Linux.

El software de View Composer no puede coexistir en la misma máquina virtual ni en el mismo equipo físico con cualquier otro componente de software de Horizon 7, como un servidor de réplica, el servidor de seguridad, el servidor de conexión, Horizon Agent u Horizon Client.

Para proporcionar una seguridad mejorada, se recomienda configurar los conjuntos de claves de cifrado para que eliminen las vulnerabilidades conocidas. Para obtener instrucciones sobre cómo configurar una directiva de dominio en los conjuntos de claves de cifrado para los equipos Windows que ejecuten View Composer u Horizon Agent, consulte [Deshabilitar cifrados débiles en SSL/TLS](#).

Requisitos previos

- Verifique que la instalación cumpla los requisitos de View Composer descritos en [Requisitos de View Composer](#).
- Verifique que ningún otro componente de Horizon 7, incluidos el servidor de conexión, el servidor de seguridad, Horizon Agent u Horizon Client, esté instalado en el equipo en el que pretende instalar View Composer.
- Verifique que tenga una licencia para instalar y usar View Composer.
- Verifique que tenga el DNS, el nombre de usuario administrador y la contraseña que proporcionó en el asistente Administrador de orígenes de datos ODBC. Introduzca esta información cuando instale el servicio de View Composer.
- Si tiene pensado configurar un certificado SSL firmado por una CA para View Composer durante la instalación, verifique que el certificado se importó al almacén de certificados del equipo local Windows. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).
- Verifique que ninguna aplicación que se ejecute en el equipo de View Composer use las bibliotecas SSL de Windows que necesiten la versión 2 de SSL (SSLv2) proporcionada a través del paquete de seguridad del canal seguro de Microsoft (Schannel). El instalador de View Composer deshabilita SSLv2 en Schannel de Microsoft. Estas restricciones no afectan a las aplicaciones como Tomcat, que usa Java SSL, o Apache, que usa OpenSSL.
- Para ejecutar el instalador de View Composer, debe ser un usuario con privilegios de administrador en el sistema.

Procedimiento

- 1 Descargue el archivo instalador de View Composer de la página de productos de VMware, disponible en <http://www.vmware.com/products/> en el equipo Windows Server.

El nombre del archivo instalador es VMware-viewcomposer-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación e y.y.y es el número de la versión. El archivo instalador instala el servicio de View Composer en sistemas operativos Windows Server de 64 bits.

- 2 Para iniciar el programa de instalación de View Composer, haga clic con el botón secundario en el archivo instalador y seleccione **Ejecutar como administrador**.
- 3 Acepte los términos de licencia de VMware.
- 4 Acepte o cambie la carpeta de destino.
- 5 Escriba el DSN de la base de datos de View Composer que proporcionó en el asistente **Administrador de orígenes de datos ODBC** de Oracle o Microsoft.

Por ejemplo: **VMware View Composer**

Nota Si no configuró un DSN para la base de datos de View Composer, haga clic en **Configurar DSN de ODBC** para configurar un nombre en ese momento.

- 6 Escriba el nombre del usuario administrador y la contraseña que proporcionó en el asistente **Administrador de orígenes de datos ODBC**.

Si configuró un usuario de una base de datos de Oracle con permisos de seguridad específicos, introduzca ese nombre.

- 7 Escriba un número de puerto o acepte el predeterminado.

El servidor de conexión de View usa este puerto para comunicarse con el servicio de View Composer.

- 8 Proporcione un certificado SSL.

Opción	Acción
Crear un certificado SSL predeterminado	<p>Seleccione el botón de radio para crear un certificado SSL predeterminado para el servicio de View Composer.</p> <p>Después de la instalación, puede reemplazar el certificado predeterminado con un certificado SSL firmado por una CA.</p>
Usar un certificado SSL existente	<p>Seleccione este botón de radio si instaló un certificado SSL firmado que desee usar para el servicio de View Composer. Seleccione un certificado SSL de la lista.</p>

- 9 Haga clic en **Instalar y Finalizar** para completar la instalación del servicio de View Composer.

Resultados

Se inicia el servicio de VMware Horizon View Composer.

View Composer usa los conjuntos de claves de cifrado que proporciona el sistema operativo Windows Server. Debe seguir las directrices de su organización para administrar los conjuntos de claves de cifrado en los sistemas Windows Server. Si su organización no proporciona directrices, VMware recomienda que deshabilite los conjuntos de claves de cifrado débiles en el servidor de View Composer para mejorar la seguridad de su entorno de Horizon 7. Para obtener información sobre cómo administrar los conjuntos de claves de cifrado, consulte la documentación de Microsoft.

Pasos siguientes

Si tiene una versión anterior de vCenter Server, consulte [Habilitar TLSv1.0 en vCenter y conexiones ESXi desde View Composer](#).

Si estableció de forma manual los permisos de la base de datos SQL Server y los asignó a un usuario, puede revocar la función de administrador de la base de datos de ese usuario. Para obtener más detalles, consulte el último paso del procedimiento en [Establecer los permisos de la base de datos SQL Server creando funciones de las bases de datos de forma manual](#).

Habilitar TLSv1.0 en vCenter y conexiones ESXi desde View Composer

Horizon 7 y los componentes posteriores cuentan con el protocolo de seguridad TLSv1.0 deshabilitado de forma predeterminada. Si la implementación incluye una versión anterior de vCenter Server que solo admita TLSv1.0, es posible que necesite actualizar TLSv1.0 para las conexiones de View Composer después de instalar o actualizar a View Composer 7.0 o una versión posterior.

Algunas versiones de mantenimiento anteriores de vCenter Server 5.0, 5.1 y 5.5 solo admiten TLSv1.0 y este ya no está habilitado de forma predeterminada en Horizon 7 y versiones posteriores. Si no es posible actualizar vCenter Server a una versión que admita TLSv1.1 o TLSv1.2, puede habilitar TLSv1.0 para las conexiones de View Composer.

Si los hosts ESXi no ejecutan ESXi 6.0 U1b o una versión posterior y no puede actualizar, es posible que también necesite habilitar las conexiones de TLSv1.0 a los hosts ESXi desde View Composer.

Requisitos previos

- Verifique que tenga instalado View Composer 7.0 o una versión posterior.
- Verifique que pueda iniciar sesión en el equipo de View Composer como un administrador para usar el Editor del Registro de Windows.

Procedimiento

- 1 En el equipo que aloja a View Composer, abra el Editor del Registro de Windows (regedit.exe).
- 2 Diríjase a HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client.

Si esta clave aún no existe, créela.
- 3 Elimine el valor **Habilitado** si existe.

- 4 Cree o edite el valor **DWORDDisabledByDefault** y establézcalo a **0**.
- 5 Reinicie el servicio de VMware Horizon View Composer.
Ya están habilitadas las conexiones TLSv1.0 de View Composer a vCenter.
- 6 En el Registro de Windows del equipo de View Composer, diríjase a HKLM\SOFTWARE\VMware, Inc.\VMware View Composer.
- 7 Cree o edite el valor String **EnableTLS1.0** y establézcalo a **1**.
- 8 Si el host de View Composer está en un equipo de 64 bits, diríjase a HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware View Composer.
- 9 Cree o edite el valor String **EnableTLS1.0** y establézcalo a **1**.
- 10 Reinicie el servicio de VMware Horizon View Composer.
Ya están habilitadas las conexiones TLSv1.0 de View Composer a los hosts ESXi.

Configurar la infraestructura de View Composer

Puede aprovechar las ventajas de algunas funciones en vSphere, vCenter Server, Active Directory y otros componentes de la infraestructura para optimizar el rendimiento, la disponibilidad y la fiabilidad de View Composer.

Configurar el entorno de vSphere para View Composer

Para admitir View Composer, debe seguir algunas prácticas recomendadas cuando instale y configure vCenter Server, ESXi y otros componentes de vSphere.

Estas prácticas recomendadas permiten que View Composer trabaje eficientemente en el entorno de vSphere.

- Después de crear la información de la carpeta y la ruta para las máquinas virtuales de clonación vinculada, no cambie esta información en vCenter Server. En su lugar, use Horizon Administrator para cambiar la información de la carpeta.

Si cambia esta información en vCenter Server, Horizon 7 no puede buscar correctamente las máquinas virtuales en vCenter Server.

- Asegúrese de que las opciones de vSwitch del host ESXi estén configuradas con puertos suficientes para admitir el número total de NIC virtuales configuradas en las máquinas virtuales de clonación vinculada que se ejecutan en el host ESXi.
- Cuando implemente escritorios de clonación vinculada en un grupo de recursos, asegúrese de que el entorno de vSphere tenga CPU y memoria suficientes para alojar el número de escritorios que necesita. Use vSphere Client para supervisar el uso de la memoria y la CPU de los grupos de recursos.

- En vSphere 5.1 y versiones posteriores, un clúster que se usa para las clonaciones vinculadas de View Composer puede contener más de ocho hosts ESXi si los discos de réplica se almacenan en almacenes de datos VMFS5 o posteriores, o bien en almacenes de datos NFS. Si almacena réplicas en una versión de VMFS anterior a VMFS5, un clúster puede tener como máximo ocho hosts.
- Use vSphere DRS. DRS distribuye de forma eficiente las máquinas virtuales de clonación vinculada entre los hosts.

Nota Los escritorios de clonación vinculada no admiten Storage vMotion.

Prácticas recomendadas adicionales para View Composer

Para asegurarse de que View Composer funcione de forma eficiente, compruebe que el servicio de nombres dinámicos (DNS) funcione correctamente y realice exámenes del antivirus en intervalos de tiempo escalonados.

Al asegurarse de que la resolución DNS funcione correctamente, puede superar problemas intermitentes provocados por errores de DNS. El servicio de View Composer se basa en la resolución de un nombre dinámico para comunicarse con otros equipos. Para probar la operación de DNS, haga ping en los equipos de Active Directory del servidor de conexión de View por nombre.

Si escalona las horas de ejecución del antivirus, esto no afecta al rendimiento de los escritorios de clones vinculados. Si el antivirus se ejecuta en todos los clones vinculados al mismo tiempo, se produce un gran número de operaciones de entrada y salida por segundo (IOPS) en el subsistema de almacenamiento. Esta actividad excesiva puede afectar al rendimiento de los escritorios de clones vinculados.

Instalar el servidor de conexión de Horizon

7

Para usar el servidor de conexión, instale el software en equipos compatibles, configure los componentes necesarios y, de forma opcional, optimice los componentes.

Este capítulo incluye los siguientes temas:

- [Instalar el software del servidor de conexión de Horizon](#)
- [Requisitos de instalación del servidor de conexión de Horizon](#)
- [Instalar el servidor de conexión de Horizon con una nueva configuración](#)
- [Instalar una instancia replicada del servidor de conexión de Horizon](#)
- [Configurar una contraseña de emparejamiento para el servidor de seguridad](#)
- [Instalar un servidor de seguridad](#)
- [Ventajas de los dispositivos Unified Access Gateway sobre la VPN](#)
- [Reglas de firewall para el servidor de conexión de Horizon](#)
- [Volver a instalar el servidor de conexión de Horizon con una configuración de seguridad](#)
- [Opciones de la línea de comandos de Microsoft Windows Installer](#)
- [Desinstalar los componentes de Horizon 7 de forma silenciosa con las opciones de la línea de comandos MSI](#)

Instalar el software del servidor de conexión de Horizon

Según el rendimiento, la disponibilidad y las necesidades de seguridad de la implementación de Horizon 7, puede instalar una única instancia o instancias replicadas del servidor de conexión, así como servidores de seguridad. Debe instalar al menos una instancia del servidor de conexión.

Cuando instale el servidor de conexión, seleccione un tipo de instalación.

Instalación estándar

Genera una instancia del servidor de conexión con una nueva configuración LDAP de View.

Instalación de réplica

Genera una instancia del servidor de conexión con una configuración LDAP de View que se copia de una instancia existente.

Instalación del servidor de seguridad

Genera una instancia del servidor de conexión que agrega una capa adicional de seguridad entre Internet y la red interna.

Instalación del servidor de inscripciones

Instala un servidor de inscripciones que es necesario para la función True SSO (Single Sign-On), de forma que después de que los usuarios inicien sesión en VMware Identity Manager, puedan conectarse a una aplicación o un escritorio remotos sin tener que proporcionar las credenciales de Active Directory. El servidor de inscripciones solicita los certificados de corta duración que se usan para la autenticación.

Nota Como esta función necesita que también se configure una entidad de certificación y se realice una configuración específica, el proceso de instalación para el servidor de inscripciones aparece en el documento *Administración de Horizon 7*, en el capítulo sobre cómo autenticar usuarios sin necesitar credenciales, en lugar de en este documento de instalación.

Requisitos de instalación del servidor de conexión de Horizon

Antes de instalar el servidor de conexión, debe verificar que el entorno de instalación cumpla los requisitos específicos.

- Debe contar con una clave de licencia válida para Horizon 7.
- Debe conectar el host del servidor de conexión a un dominio de Active Directory. El servidor de conexión admite los siguientes niveles funcionales de dominios de Active Directory Domain Services (AD DS):
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016

El host del servidor de conexión no debe ser un controlador de dominio.

Nota El servidor de conexión no realiza ni necesita ninguna actualización de configuración o esquema para Active Directory.

- No instale el servidor de conexión en sistemas que tengan la función Windows Terminal Server instalada. Debe eliminar la función Windows Terminal Server de todos los sistemas en los que instale el servidor de conexión.
- No instale el servidor de conexión en un sistema que realice otras funciones. Por ejemplo, no utilice el mismo sistema para alojar vCenter Server.

- El sistema en el que instale el servidor de conexión debe tener una dirección IP que no cambie. En un entorno IPv4, configure una dirección IP estática. En un entorno IPv6, los equipos obtienen automáticamente direcciones IP que no cambian.
- Para ejecutar el instalador del servidor de conexión de Horizon, debe usar una cuenta de usuario de dominio con privilegios de administrador en el sistema.
- Cuando instale el servidor de conexión, autorice una cuenta Administradores. Puede especificar el grupo de administradores locales o una cuenta de un usuario o de un grupo de dominio. Horizon 7 asigna plenos derechos de administración, incluido el derecho para instalar instancias del servidor de conexión replicadas, únicamente a esta cuenta. Si especifica un grupo o un usuario de dominio, debe crear la cuenta en Active Directory antes de ejecutar el instalador.

Instalar el servidor de conexión de Horizon con una nueva configuración

Para instalar el servidor de conexión como un servidor único o como la primera instancia en un grupo de instancias del servidor de conexión replicadas, use la opción de instalación estándar.

Cuando selecciona la opción de instalación estándar, la instalación crea una nueva configuración LDAP de View local. La instalación carga las definiciones del esquema, la definición del árbol de información del directorio (DIT) y las ACL e inicia los datos.

Después de la instalación, puede administrar la mayor parte de los datos de configuración LDAP de View con Horizon Administrator. El servidor de conexión mantiene automáticamente algunas entradas LDAP de View.

El software del servidor de conexión no puede coexistir en la misma máquina virtual ni en el mismo equipo físico con cualquier otro componente de software de Horizon 7, como un servidor de réplica, el servidor de seguridad, View Composer, Horizon Agent u Horizon Client.

Cuando instale el servidor de conexión con una nueva configuración, puede participar en un programa de mejora de la experiencia de cliente. VMware recopila datos anónimos sobre su implementación con el fin de mejorar la respuesta de VMware a los requisitos de los usuarios. No se recopila ningún dato que identifique a su organización. Puede elegir no participar desmarcando esta opción durante la instalación. Si cambia de opinión después de la instalación, puede unirse al programa o descartar su participación editando la página Licencia y uso del producto en Horizon Administrator. Para revisar la lista de campos de los que se recopilan datos, incluidos los campos que son anónimos, consulte Información recopilada por el programa de mejora de la experiencia de cliente en el documento *Administración de Horizon 7*.

De forma predeterminada, el componente de HTML Access se instala en el host del servidor de conexión al instalar dicho servidor. Este componente configura la página del portal de usuario de Horizon 7 para mostrar un icono de HTML Access, además del icono de Horizon Client. El icono adicional permite que los usuarios seleccionen HTML Access cuando se conectan a sus escritorios.

Para obtener información general sobre cómo configurar el servidor de conexión para HTML Access, consulte el documento *Guía de instalación y configuración de VMware Horizon HTML Access* que se encuentra en la página Documentación de Horizon Client.

Requisitos previos

- Verifique que pueda iniciar sesión como un usuario de dominio con privilegios de administrador en el equipo Windows Server en el que instala el servidor de conexión.
- Verifique que la instalación cumpla con los requisitos descritos en [Requisitos del servidor de conexión de Horizon](#).
- Prepare su entorno para la instalación. Consulte [Requisitos de instalación del servidor de conexión de Horizon](#).
- Si pretende autorizar un grupo o un usuario de dominio como cuenta Administradores, verifique que creó la cuenta de dominio en Active Directory.
- Prepare una contraseña de Data Recovery. Cuando realiza una copia de seguridad del servidor de conexión, la configuración LDAP de View se exporta como datos LDIF cifrados. Para restaurar la configuración de Horizon 7 desde la copia de seguridad cifrada, 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.

Importante Necesitará la contraseña de Data Recovery para mantener Horizon 7 en funcionamiento y para evitar tiempo de inactividad en un escenario de continuidad empresarial y de recuperación ante desastres (BCDR). Puede proporcionar un recordatorio con la contraseña cuando instala el servidor de conexión.

- Familiarícese con los puertos de red que deben abrirse en el Firewall de Windows para las instancias del servidor de conexión. Consulte [Reglas de firewall para el servidor de conexión de Horizon](#).
- Si planea emparejar un servidor de seguridad con dicha instancia del servidor de conexión, verifique que el Firewall de Windows con seguridad avanzada esté **activado** en los perfiles activos. Se recomienda que esta opción esté **activada** en todos los perfiles. De forma predeterminada, las reglas IPsec rigen las conexiones entre el servidor de seguridad y el servidor de conexión, y requieren que se habilite el Firewall de Windows con seguridad avanzada.
- Si la topología de la red incluye un firewall back-end entre un servidor de seguridad y la instancia del servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte [Configurar que un firewall back-end admita IPsec](#).

Procedimiento

- 1 Descargue el archivo instalador del servidor de conexión desde el sitio de descargas de VMware disponible en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el servidor de conexión.

El nombre del archivo instalador es VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- 2 Para iniciar el programa de instalación del servidor de conexión, haga doble clic en el archivo instalador.

3 Acepte los términos de licencia de VMware.

4 Acepte o cambie la carpeta de destino.

5 Seleccione la opción de instalación **Servidor estándar de View**.

6 Seleccione la versión del protocolo de Internet (**IPv4** o **IPv6**).

Debe instalar todos los componentes de Horizon 7 con la misma versión de IP.

7 Seleccione si desea habilitar o deshabilitar el modo FIPS.

Esta opción estará disponible solo si el modo FIPS está habilitado en Windows.

8 Asegúrese de que la opción **Instale HTML Access** esté seleccionada si desea permitir a los usuarios conectarse a sus escritorios con un navegador web.

Si **IPv4** está seleccionado, esta opción se selecciona de forma predeterminada. Si **IPv6** está seleccionado, esta opción no aparece puesto que HTML Access no es compatible con el entorno IPv6.

9 Escriba la contraseña de Data Recovery y, de manera opcional, un recordatorio de contraseña.

10 Elija cómo configurar el servicio Firewall de Windows.

Opción	Acción
Configurar el Firewall de Windows automáticamente	Permita que el instalador configure el Firewall de Windows para autorizar las conexiones de red necesarias.
No configurar el Firewall de Windows	Configure las reglas del Firewall de Windows de forma manual. Seleccione esta opción solo si la organización utiliza sus propias reglas predefinidas para configurar el Firewall de Windows.

11 Autorice una cuenta de Horizon Administrator.

Solo los miembros de esta cuenta puede iniciar sesión en Horizon Administrator, disfrutar de todos los derechos de administración e instalar instancias del servidor de conexión replicadas, así como otros servidores de Horizon 7.

Opción	Descripción
Autorizar al grupo de administradores local	Permite a los usuarios en el grupo Administradores local gestionar Horizon 7.
Autorizar un usuario de un dominio específico o un grupo de dominios	Permite al grupo o usuario de dominio especificado gestionar Horizon 7.

12 Si especificó una cuenta de Horizon Administrator de dominio y está ejecutando el instalador como un administrador local u otro usuario sin acceso a la cuenta de dominio, proporcione las credenciales para iniciar sesión en el dominio con una contraseña y un nombre de usuario autorizados.

Use *nombre de dominio\nombre de usuario* o el formato de nombre principal de usuario (UPN). El formato UPN puede ser *usuario@dominio.com*.

13 Elija si desea participar en el programa de mejora de la experiencia de cliente.

Si participa, puede seleccionar de forma opcional el tipo, el tamaño y la ubicación de la organización.

14 Complete el asistente para finalizar la instalación del servidor de conexión.

15 Busque nuevas revisiones en el equipo Windows Server y ejecute Windows Update, si fuera necesario.

La instalación podría tener habilitadas inicialmente algunas funciones del sistema operativo aunque se hayan instalado en el equipo Windows Server todas las revisiones existentes antes de instalar el servidor de conexión. En tal caso, es posible que deban realizarse revisiones adicionales.

Resultados

Se instalan los servicios de Horizon 7 en el equipo Windows Server:

- Servidor de conexión de VMware Horizon
- Componente del marco de VMware Horizon View
- Componente de bus de mensajería VMware Horizon View
- VMware Horizon View Script Host
- Componente de puerta de enlace de seguridad de VMware Horizon View
- Puerta de enlace segura PCoIP de VMware Horizon View
- Puerta de enlace segura de Blast VMware Horizon View
- Componente Web de VMware Horizon View
- VMware VDMDS, que proporciona los servicios de los directorios LDAP de View

Para obtener más información sobre estos servicios, consulte el documento *Administración de Horizon 7*.

Si la opción **Instalar HTML Access** estaba seleccionada durante la instalación, se instala el componente HTML Access en el equipo Windows Server. Este componente configura el icono HTML Access en la página del portal de usuario de Horizon 7 y habilita la regla **Servidor de conexión VMware Horizon View (integrado en Blast)** en el firewall de Windows. Esta regla del firewall permite a los navegadores web de los dispositivos cliente conectarse al servidor de conexión en el puerto TCP 8443.

Pasos siguientes

Configure los certificados del servidor SSL para el servidor de conexión. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

Si tiene una versión anterior de vCenter Server, consulte [Habilitar TLSv1.0 en conexiones de vCenter desde el servidor de conexión](#).

Realice la configuración inicial en el servidor de conexión. Consulte [Capítulo 9 Configurar Horizon 7 por primera vez](#).

Si tiene pensado incluir instancias del servidor de conexión replicadas y servidores de seguridad en la implementación, debe instalar cada instancia del servidor ejecutando el archivo instalador del servidor de conexión.

Si vuelve a instalar el servidor de conexión y cuenta con un recopilador de datos configurado para supervisar los datos de rendimiento, detenga el recopilador y vuelva a iniciarlo.

Instalar el servidor de conexión de Horizon de forma silenciosa

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

La instalación silenciosa le permite implementar los componentes de Horizon 7 correctamente en una empresa de gran tamaño.

Requisitos previos

- Verifique que pueda iniciar sesión como un usuario de dominio con privilegios de administrador en el equipo Windows Server en el que instala el servidor de conexión.
- Verifique que la instalación cumpla con los requisitos descritos en [Requisitos del servidor de conexión de Horizon](#).
- Prepare su entorno para la instalación. Consulte [Requisitos de instalación del servidor de conexión de Horizon](#).
- Si pretende autorizar un grupo o un usuario de dominio como la cuenta de Horizon Administrator, verifique que creó la cuenta de dominio en Active Directory.
- Si utiliza autenticación MIT Kerberos para iniciar sesión en un equipo con Windows Server 2008 R2 en el que esté instalando el servidor de conexión, instale la revisión de Microsoft que se describe en KB 978116 en <http://support.microsoft.com/kb/978116>.
- Familiarícese con los puertos de red que deben abrirse en el Firewall de Windows para las instancias del servidor de conexión. Consulte [Reglas de firewall para el servidor de conexión de Horizon](#).
- Si planea emparejar un servidor de seguridad con dicha instancia del servidor de conexión, verifique que el Firewall de Windows con seguridad avanzada esté **activado** en los perfiles activos. Se recomienda que esta opción esté **activada** en todos los perfiles. De forma predeterminada, las reglas IPsec rigen las conexiones entre el servidor de seguridad y el servidor de conexión, y requieren que se habilite el Firewall de Windows con seguridad avanzada.
- Si la topología de la red incluye un firewall back-end entre un servidor de seguridad y la instancia del servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte [Configurar que un firewall back-end admita IPsec](#).
- Verifique que el equipo Windows en el que instala el servidor de conexión cuente con la versión 2.0 o posterior del motor en tiempo de ejecución MSI. Para obtener más información, consulte el sitio web de Microsoft.
- Familiarícese con las opciones de la línea de comandos del instalador MSI. Consulte [Opciones de la línea de comandos de Microsoft Windows Installer](#).

- Familiarícese con las propiedades de instalación silenciosa disponibles con una instalación estándar del servidor de conexión. Consulte [Propiedades de instalación silenciosa para una instalación estándar del servidor de conexión de Horizon](#).

Procedimiento

- 1 Descargue el archivo instalador del servidor de conexión desde el sitio de descargas de VMware disponible en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el servidor de conexión.

El nombre del archivo instalador es VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- 2 Abra una ventana del símbolo del sistema en el equipo Windows Server.
- 3 Escriba el comando de instalación en una línea.

Por ejemplo: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn

```
VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini
VDM_SERVER_RECOVERY_PWD_REMINDER=""First car""
```

Importante Cuando realiza una instalación silenciosa, la línea de comandos al completo, incluida la contraseña de Data Recovery, se registra en el archivo vminst.log del instalador. Después de completar la instalación, elimine este archivo de registro o cambie la contraseña de Data Recovery usando Horizon Administrator.

- 4 Busque nuevas revisiones en el equipo Windows Server y ejecute Windows Update, si fuera necesario.

La instalación podría tener habilitadas inicialmente algunas funciones del sistema operativo aunque se hayan instalado en el equipo Windows Server todas las revisiones existentes antes de instalar el servidor de conexión. En tal caso, es posible que deban realizarse revisiones adicionales.

Resultados

Se instalan los servicios de Horizon 7 en el equipo Windows Server:

- Servidor de conexión de VMware Horizon
- Componente del marco de VMware Horizon View
- Componente de bus de mensajería VMware Horizon View
- VMware Horizon View Script Host
- Componente de puerta de enlace de seguridad de VMware Horizon View
- Puerta de enlace segura PCoIP de VMware Horizon View
- Puerta de enlace segura de Blast VMware Horizon View
- Componente Web de VMware Horizon View

- VMware VDMDS, que proporciona los servicios de los directorios LDAP de View

Si la opción **Instalar HTML Access** estaba seleccionada durante la instalación, se instala el componente HTML Access en el equipo Windows Server. Este componente configura el icono HTML Access en la página del portal de usuario de Horizon 7 y habilita la regla **Servidor de conexión VMware Horizon View (integrado en Blast)** en el firewall de Windows. Esta regla del firewall permite a los navegadores web de los dispositivos cliente conectarse al servidor de conexión en el puerto TCP 8443.

Para obtener más información sobre estos servicios, consulte el documento *Administración de Horizon 7*.

Pasos siguientes

Configure los certificados del servidor SSL para el servidor de conexión. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

Si tiene una versión anterior de vCenter Server, consulte [Habilitar TLSv1.0 en conexiones de vCenter desde el servidor de conexión](#).

Si está configurando Horizon 7 por primera vez, realice la configuración inicial en el servidor de conexión. Consulte [Capítulo 9 Configurar Horizon 7 por primera vez](#).

Propiedades de instalación silenciosa para una instalación estándar del servidor de conexión de Horizon

Puede incluir propiedades específicas del servidor de conexión cuando realice una actualización o instalación silenciosa desde la línea de comandos. Debe usar el formato *PROPIEDAD=valor* para que Microsoft Windows Installer (MSI) pueda interpretar las propiedades y los valores. En las actualizaciones silenciosas se utilizan los mismos comandos de instalación.

Tabla 7-1. Propiedades MSI para instalar de forma silenciosa el servidor de conexión en una instalación estándar

Propiedad MSI	Descripción	Valor predeterminado
INSTALLDIR	La ruta y la carpeta en las que el software del servidor de conexión está instalado. Por ejemplo: INSTALLDIR=""D:\abc\my folder"" Si se incluyen comillas dobles que abran y cierren la ruta, el instalador MSI puede interpretar el espacio como parte válida de la ruta.	%ProgramFiles%\VMware\VMware View Server
VDM_SERVER_INSTANCE_TYPE	El tipo de instalación de Horizon Server: <ul style="list-style-type: none">■ 1. Instalación estándar■ 2. Instalación de réplica■ 3. Instalación del servidor de seguridad■ 5. Instalación del servidor de inscripciones Por ejemplo, para realizar una instalación estándar, defina VDM_SERVER_INSTANCE_TYPE=1	1
FWCHOICE	La propiedad MSI que determina si desea configurar un firewall para la instancia del servidor de conexión. El valor 1 configura un firewall. El valor 2 no configura ningún firewall. Por ejemplo: FWCHOICE=1	1

Tabla 7-1. Propiedades MSI para instalar de forma silenciosa el servidor de conexión en una instalación estándar (continuación)

Propiedad MSI	Descripción	Valor predeterminado
VDM_INITIAL_ ADMIN_SID	El SID del grupo o del usuario de Horizon Administrator inicial que está autorizado con derechos de administración completos en Horizon. El valor predeterminado es el SID del grupo de administradores local del equipo del servidor de conexión. Puede especificar un SID de una cuenta de grupo o de usuario de dominio.	S-1-5-32-544
VDM_SERVER_ RECOVERY_PWD	La contraseña de recuperación de datos. Si la contraseña de recuperación de datos no está establecida en LDAP de Horizon, esta propiedad es obligatoria. La contraseña debe tener entre 1 y 128 caracteres. Siga las prácticas recomendadas de la organización para generar contraseñas seguras.	Ninguno
VDM_SERVER_RECOVERY_ PWD_REMINDER	El recordatorio de la contraseña de recuperación de datos. Esta propiedad es opcional.	Ninguno
VDM_IP_PROTOCOL_ USAGE	Especifica la versión de IP que los componentes de Horizon usan para comunicarse. Los valores posibles son IPv4 e IPv6 .	IPv4
VDM_FIPS_ENABLED	Especifica si desea habilitar o deshabilitar el modo FIPS. El valor 1 habilita el modo FIPS. El valor 0 deshabilita el modo FIPS. Si esta propiedad se establece en 1 y Windows no está en modo FIPS, el instalador se detiene.	0
HTMLACCESS	Controla la instalación del complemento HTML Access. Establezca esta propiedad en 1 para configurar HTML Access u omita la propiedad si HTML Access no es necesario.	1

Habilitar TLSv1.0 en conexiones de vCenter desde el servidor de conexión

Horizon 7 y los componentes posteriores cuentan con el protocolo de seguridad TLSv1.0 deshabilitado de forma predeterminada. Si la implementación incluye una versión anterior de vCenter Server que solo admita TLSv1.0, es posible que necesite habilitar TLSv1.0 para las conexiones del servidor de conexión después de instalar la versión 7.0 o una versión posterior del servidor de conexión o actualizar a dicha versión.

Algunas versiones de mantenimiento anteriores de vCenter Server 5.1 y 5.5 solo admiten TLSv1.0, pero este ya no está habilitado de forma predeterminada en Horizon 7 y versiones posteriores. Si no es posible actualizar vCenter Server a una versión que admita TLSv1.1 o TLSv1.2, puede habilitar TLSv1.0 para las conexiones del servidor de conexión.

Requisitos previos

- Si está actualizando a Horizon 7, realice este procedimiento antes de actualizar para reducir el número de veces que debe reiniciar el servicio. Durante una actualización, se reinicia el servicio del servidor de conexión y es necesario reiniciar para que se apliquen los cambios descritos en este procedimiento. Si actualiza antes de realizar este procedimiento, tendrá que volver a reiniciar el equipo por segunda vez.
- Visite el sitio web de Microsoft TechNet si desea obtener información sobre cómo utilizar la utilidad Editor ADSI en la versión que utilice del sistema operativo Windows.

Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión.
- 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 panel del equipo, seleccione o escriba **localhost:389** o bien el nombre de dominio completo (FQDN) del host del servidor de conexión seguido por el puerto 389.

Por ejemplo: **localhost:389** o **miequipo.ejemplo.com:389**
- 5 Amplíe el árbol del Editor ADSI, amplíe **OU=Properties**, seleccione **OU=Global** y haga doble clic en **CN=Common** en el panel derecho.
- 6 En el cuadro de diálogo Propiedades, edite el atributo **pae-ClientSSLSecureProtocols** para agregar los valores siguientes

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

Verifique que incluya la barra invertida al principio de la línea.
- 7 Haga clic en **Aceptar**.
- 8 Si se trata de una instalación nueva, reinicie el servicio del servidor de conexión en cada instancia del servidor de conexión para aplicar el cambio de la configuración.

Si tiene pensado realizar una actualización, no es necesario que reinicie el servicio, ya que el proceso de actualización lo reinicia automáticamente.

Instalar una instancia replicada del servidor de conexión de Horizon

Para ofrecer alta disponibilidad y equilibrio de carga, puede instalar una o varias réplicas de instancias del servidor de conexión. Tras instalar la réplica, las instancias del servidor de conexión originales y las recién instaladas son idénticas.

Al instalar una instancia replicada, Horizon 7 copia los datos de configuración LDAP de View de la instancia existente del servidor de conexión.

Tras la instalación, los datos de configuración LDAP de View se mantienen en todas las instancias del servidor de conexión en el grupo replicado. Cuando se realiza un cambio en una instancia, la información actualizada se copia al resto de instancias.

Si se produce un error en una instancia replicada, el resto de instancias del grupo siguen funcionando. Cuando la instancia con el error reanuda su función, la configuración se actualiza con los cambios que se realizaron durante la interrupción.

Nota View LDAP proporciona la función de réplica, para lo que utiliza la misma tecnología de réplica que Active Directory.

El software del servidor de réplica no puede coexistir en la misma máquina virtual o física con cualquier otro componente de software de Horizon 7, como un servidor de seguridad, el servidor de conexión, View Composer, Horizon Agent u Horizon Client.

De forma predeterminada, el componente de HTML Access se instala en el host del servidor de conexión al instalar dicho servidor. Este componente configura la página del portal de usuario de Horizon 7 para mostrar un icono de HTML Access, además del icono de Horizon Client. El icono adicional permite que los usuarios seleccionen HTML Access cuando se conectan a sus escritorios.

Para obtener información general sobre cómo configurar el servidor de conexión para HTML Access, consulte el documento *Guía de instalación y configuración de VMware Horizon HTML Access* que se encuentra en la página Documentación de Horizon Client.

Requisitos previos

- Compruebe que al menos una instancia del servidor de conexión esté instalada y configurada en la red.
- Para instalar la instancia replicada, debe iniciar sesión como usuario con funciones de administradores. Cuando instale la primera instancia del servidor de conexión, especifique la cuenta o el grupo con la funciones de administradores. Las funciones pueden asignarse al grupo de administradores locales o al usuario o grupo de dominio. Consulte [Instalar el servidor de conexión de Horizon con una nueva configuración](#).
- Si la instancia del servidor de conexión existente se encuentra en un dominio diferente al de la instancia replicada, el usuario del dominio debe poseer también privilegios de administrador en el equipo Windows Server donde esté instalada la instancia original.
- Si utiliza autenticación MIT Kerberos para iniciar sesión en un equipo con Windows Server 2008 R2 en el que esté instalando el servidor de conexión, instale la revisión de Microsoft que se describe en KB 978116 en <http://support.microsoft.com/kb/978116>.
- Verifique que la instalación cumpla con los requisitos descritos en [Requisitos del servidor de conexión de Horizon](#).
- Compruebe que los equipos donde se instalan las instancias replicadas del servidor de conexión estén conectados a una red LAN de alto rendimiento. Consulte [Requisitos de red de las instancias replicadas del servidor de conexión de Horizon](#).

- Prepare su entorno para la instalación. Consulte [Requisitos de instalación del servidor de conexión de Horizon](#).
- Si instala una instancia replicada del servidor de conexión cuya versión sea Horizon 7 5.1 o una posterior, y la instancia original tiene instalado Horizon 7 5.0.x o una versión anterior, prepare una contraseña de Data Recovery. Consulte [Instalar el servidor de conexión de Horizon con una nueva configuración](#).
- Familiarícese con los puertos de red que deben abrirse en el Firewall de Windows para las instancias del servidor de conexión. Consulte [Reglas de firewall para el servidor de conexión de Horizon](#).
- Si planea emparejar un servidor de seguridad con dicha instancia del servidor de conexión, verifique que el Firewall de Windows con seguridad avanzada esté **activado** en los perfiles activos. Se recomienda que esta opción esté **activada** en todos los perfiles. De forma predeterminada, las reglas IPsec rigen las conexiones entre el servidor de seguridad y el servidor de conexión, y requieren que se habilite el Firewall de Windows con seguridad avanzada.
- Si la topología de la red incluye un firewall back-end entre un servidor de seguridad y la instancia del servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte [Configurar que un firewall back-end admita IPsec](#).

Procedimiento

- 1 Descargue el archivo instalador del servidor de conexión desde el sitio de descargas de VMware disponible en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el servidor de conexión.

El nombre del archivo instalador es VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- 2 Para iniciar el programa de instalación del servidor de conexión, haga doble clic en el archivo instalador.

- 3 Acepte los términos de licencia de VMware.

- 4 Acepte o cambie la carpeta de destino.

- 5 Seleccione la opción de instalación **Servidor de réplica de View**.

- 6 Seleccione la versión del protocolo de Internet (**IPv4 o IPv6**).

Debe instalar todos los componentes de Horizon 7 con la misma versión de IP.

- 7 Seleccione si desea habilitar o deshabilitar el modo FIPS.

Esta opción estará disponible solo si el modo FIPS está habilitado en Windows.

- 8 Asegúrese de que la opción **Instalar HTML Access** está seleccionada si pretende permitir a los usuarios conectarse a sus escritorios con HTML Access.

Si **IPv4** está seleccionado, esta opción se selecciona de forma predeterminada. Si **IPv6** está seleccionado, esta opción no aparece puesto que HTML Access no es compatible con el entorno IPv6.

- 9 Introduzca el nombre del host o la dirección IP de la instancia del servidor de conexión que esté replicando.

- 10 Escriba la contraseña de Data Recovery y, de manera opcional, un recordatorio de contraseña.

Se le solicita una contraseña de Data Recovery solo si la instancia del servidor de conexión que está replicando tiene instalado Horizon 7 5.0 x o una versión anterior.

- 11 Elija cómo configurar el servicio del Firewall de Windows.

Opción	Acción
Configurar el Firewall de Windows automáticamente	Permita que el instalador configure el Firewall de Windows para autorizar las conexiones de red necesarias.
No configurar el Firewall de Windows	Configure las reglas del Firewall de Windows de forma manual. Seleccione esta opción solo si la organización utiliza sus propias reglas predefinidas para configurar el Firewall de Windows.

- 12 Complete el asistente para finalizar la instalación de la instancia replicada.

- 13 Busque nuevas revisiones en el equipo Windows Server y ejecute Windows Update, si fuera necesario.

La instalación podría tener habilitadas inicialmente algunas funciones del sistema operativo aunque se hayan instalado en el equipo Windows Server todas las revisiones existentes antes de instalar el servidor de conexión. En tal caso, es posible que deban realizarse revisiones adicionales.

Resultados

Se instalan los servicios de Horizon 7 en el equipo Windows Server:

- Servidor de conexión de VMware Horizon
- Componente del marco de VMware Horizon View
- Componente de bus de mensajería VMware Horizon View
- VMware Horizon View Script Host
- Componente de puerta de enlace de seguridad de VMware Horizon View
- Puerta de enlace segura PCoIP de VMware Horizon View
- Puerta de enlace segura de Blast VMware Horizon View
- Componente Web de VMware Horizon View
- VMware VDMDS, que proporciona los servicios de los directorios LDAP de View

Para obtener más información sobre estos servicios, consulte el documento *Administración de Horizon 7*.

Si la opción **Instalar HTML Access** estaba seleccionada durante la instalación, se instala el componente HTML Access en el equipo Windows Server. Este componente configura el icono HTML Access en la página del portal de usuario de Horizon 7 y habilita la regla **Servidor de conexión VMware Horizon View (integrado en Blast)** en el firewall de Windows. Esta regla del firewall permite a los navegadores web de los dispositivos cliente conectarse al servidor de conexión en el puerto TCP 8443.

Pasos siguientes

Configure un certificado de servidor SSL para la instancia del servidor de conexión. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

No tiene que realizar una configuración inicial de Horizon 7 en una instancia replicada del servidor de conexión. La instancia replicada hereda su configuración de la instancia original del servidor de conexión.

Sin embargo, es posible que tenga que configurar las opciones de conexión de cliente para esta instancia del servidor de conexión y modificar la configuración de Windows Server para permitir una implementación grande. Consulte [Configurar conexiones de Horizon Client](#) y [Configuración de tamaño de Windows Server para admitir la implementación](#).

Si vuelve a instalar el servidor de conexión y cuenta con un recopilador de datos configurado para supervisar los datos de rendimiento, detenga el recopilador y vuelva a iniciarlo.

Instalar una instancia replicada del servidor de conexión de Horizon de forma silenciosa

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

La instalación silenciosa le permite implementar los componentes de Horizon 7 correctamente en una empresa de gran tamaño.

Requisitos previos

- Compruebe que al menos una instancia del servidor de conexión esté instalada y configurada en la red.
- Para instalar la instancia replicada, debe iniciar sesión como usuario con credenciales para acceder a la cuenta Administradores. La cuenta Administradores se especifica al instalar la primera instancia del servidor de conexión. La cuenta puede ser del grupo local Administradores o una cuenta de un usuario o grupo de dominio. Consulte [Instalar el servidor de conexión de Horizon con una nueva configuración](#).
- Si la instancia del servidor de conexión existente se encuentra en un dominio diferente al de la instancia replicada, el usuario del dominio debe poseer también privilegios de administrador en el equipo Windows Server donde esté instalada la instancia original.

- Si utiliza autenticación MIT Kerberos para iniciar sesión en un equipo con Windows Server 2008 R2 en el que esté instalando el servidor de conexión, instale la revisión de Microsoft que se describe en KB 978116 en <http://support.microsoft.com/kb/978116>.
- Verifique que la instalación cumpla con los requisitos descritos en [Requisitos del servidor de conexión de Horizon](#).
- Compruebe que los equipos donde se instalan las instancias replicadas del servidor de conexión estén conectados a una red LAN de alto rendimiento. Consulte [Requisitos de red de las instancias replicadas del servidor de conexión de Horizon](#).
- Prepare su entorno para la instalación. Consulte [Requisitos de instalación del servidor de conexión de Horizon](#).
- Familiarícese con los puertos de red que deben abrirse en el Firewall de Windows para las instancias del servidor de conexión. Consulte [Reglas de firewall para el servidor de conexión de Horizon](#).
- Si planea emparejar un servidor de seguridad con dicha instancia del servidor de conexión, verifique que el Firewall de Windows con seguridad avanzada esté **activado** en los perfiles activos. Se recomienda que esta opción esté **activada** en todos los perfiles. De forma predeterminada, las reglas IPsec rigen las conexiones entre el servidor de seguridad y el servidor de conexión, y requieren que se habilite el Firewall de Windows con seguridad avanzada.
- Si la topología de la red incluye un firewall back-end entre un servidor de seguridad y la instancia del servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte [Configurar que un firewall back-end admita IPsec](#).
- Familiarícese con las opciones de la línea de comandos del instalador MSI. Consulte [Opciones de la línea de comandos de Microsoft Windows Installer](#).
- Familiarícese con las propiedades de instalación silenciosa disponibles con una instalación de réplica del servidor de conexión. Consulte [Propiedades de instalación silenciosa para una instancia replicada del servidor de conexión de Horizon](#).

Procedimiento

- 1 Descargue el archivo instalador del servidor de conexión desde el sitio de descargas de VMware disponible en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el servidor de conexión.

El nombre del archivo instalador es VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- 2 Abra una ventana del símbolo del sistema en el equipo Windows Server.
- 3 Escriba el comando de instalación en una línea.

Por ejemplo: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn
VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com
VDM_INITIAL_ADMIN_SID=S-1-5-32-544"

Si instala una instancia del servidor de conexión replicada cuya versión sea View 5.1 o una posterior, y la instancia original tiene instalado View 5.0.x o una versión anterior, debe especificar una contraseña de Data Recovery y agregar un recordatorio. Por ejemplo: VMware–
viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2
ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544
VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car""

Importante Cuando realiza una instalación silenciosa, la línea de comandos al completo, incluida la contraseña de Data Recovery, se registra en el archivo `vminst.log` del instalador. Después de completar la instalación, elimine este archivo de registro o cambie la contraseña de Data Recovery usando Horizon Administrator.

- 4 Busque nuevas revisiones en el equipo Windows Server y ejecute Windows Update, si fuera necesario.

La instalación podría tener habilitadas inicialmente algunas funciones del sistema operativo aunque se hayan instalado en el equipo Windows Server todas las revisiones existentes antes de instalar el servidor de conexión. En tal caso, es posible que deban realizarse revisiones adicionales.

Resultados

Se instalan los servicios de Horizon 7 en el equipo Windows Server:

- Servidor de conexión de VMware Horizon
- Componente del marco de VMware Horizon View
- Componente de bus de mensajería VMware Horizon View
- VMware Horizon View Script Host
- Componente de puerta de enlace de seguridad de VMware Horizon View
- Puerta de enlace segura PCoIP de VMware Horizon View
- Puerta de enlace segura de Blast VMware Horizon View
- Componente Web de VMware Horizon View
- VMware VDMDS, que proporciona los servicios de los directorios LDAP de View

Para obtener más información sobre estos servicios, consulte el documento *Administración de Horizon 7*.

Si la opción **Instalar HTML Access** estaba seleccionada durante la instalación, se instala el componente HTML Access en el equipo Windows Server. Este componente configura el icono HTML Access en la página del portal de usuario de Horizon 7 y habilita la regla **Servidor de conexión VMware Horizon View (integrado en Blast)** en el firewall de Windows. Esta regla del firewall permite a los navegadores web de los dispositivos cliente conectarse al servidor de conexión en el puerto TCP 8443.

Pasos siguientes

Configure un certificado de servidor SSL para la instancia del servidor de conexión. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

No tiene que realizar una configuración inicial de Horizon 7 en una instancia replicada del servidor de conexión. La instancia replicada hereda su configuración de la instancia original del servidor de conexión.

Sin embargo, es posible que tenga que configurar las opciones de conexión de cliente para esta instancia del servidor de conexión y modificar la configuración de Windows Server para permitir una implementación grande. Consulte [Configurar conexiones de Horizon Client](#) y [Configuración de tamaño de Windows Server para admitir la implementación](#).

Propiedades de instalación silenciosa para una instancia replicada del servidor de conexión de Horizon

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

Tabla 7-2. Propiedades MSI para instalar de forma silenciosa una instancia replicada del servidor de conexión de Horizon

Propiedad MSI	Descripción	Valor predeterminado
INSTALLDIR	<p>La ruta y la carpeta en las que el software del servidor de conexión está instalado.</p> <p>Por ejemplo: <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>Si se incluyen comillas dobles que abran y cierren la ruta, el instalador MSI puede interpretar el espacio como parte válida de la ruta.</p> <p>La propiedad MSI es opcional.</p>	<p>%ProgramFiles%\VMware\VMware View\Server</p>
VDM_SERVER_INSTANCE_TYPE	<p>El tipo de instalación del servidor de conexión:</p> <ul style="list-style-type: none"> ■ 1. Instalación estándar ■ 2. Instalación de réplica ■ 3. Instalación del servidor de seguridad <p>Para instalar una instancia replicada, defina <code>VDM_SERVER_INSTANCE_TYPE=2</code></p> <p>Esta propiedad MSI es obligatoria cuando se instala una réplica.</p>	1
ADAM_PRIMARY_NAME	<p>El nombre del host o la dirección IP de la instancia del servidor de conexión que esté replicando.</p> <p>Por ejemplo: <code>ADAM_PRIMARY_NAME=cs1.companydomain.com</code></p> <p>Esta propiedad MSI es obligatoria.</p>	Ninguna
FWCHOICE	<p>La propiedad MSI que determina si desea configurar un firewall para la instancia del servidor de conexión.</p> <p>El valor 1 configura un firewall. El valor 2 no configura ningún firewall.</p> <p>Por ejemplo: <code>FWCHOICE=1</code></p> <p>La propiedad MSI es opcional.</p>	1

Tabla 7-2. Propiedades MSI para instalar de forma silenciosa una instancia replicada del servidor de conexión de Horizon (continuación)

Propiedad MSI	Descripción	Valor predeterminado
VDM_SERVER_RECOVERY_PWD	<p>La contraseña de recuperación de datos. Si la contraseña de recuperación de datos no está establecida en LDAP de View, esta propiedad es obligatoria.</p> <p>Nota La contraseña de recuperación de datos no se establece en el LDAP de View si la instancia del servidor de conexión que esté replicando tiene la versión 5.0 de View o una anterior. Si la instancia del servidor de conexión que está replicando tiene la versión 5.1 de View o una posterior, no es necesario que proporcione esta propiedad.</p> <p>La contraseña debe tener entre 1 y 128 caracteres. Siga las prácticas recomendadas de la organización para generar contraseñas seguras.</p>	Ninguna
VDM_SERVER_RECOVERY_PWD_REMINDER	El recordatorio de la contraseña de recuperación de datos. Esta propiedad es opcional.	Ninguna
VDM_IP_PROTOCOL_USAGE	Especifica la versión IP que los componentes de Horizon 7 usan para comunicarse. Los valores posibles son IPv4 e IPv6	IPv4
VDM_FIPS_ENABLED	Especifica si desea habilitar o deshabilitar el modo FIPS. El valor 1 habilita el modo FIPS. El valor 0 deshabilita el modo FIPS. Si esta propiedad se establece en 1 y Windows no está en modo FIPS, el instalador se detiene.	0

Configurar una contraseña de emparejamiento para el servidor de seguridad

Antes de que pueda instalar un servidor de seguridad, debe configurar una contraseña de emparejamiento para el servidor de seguridad. Cuando instala un servidor de seguridad con el programa de instalación del servidor de conexión, el programa le solicita esta contraseña durante el proceso de instalación.

La contraseña de emparejamiento del servidor de seguridad es una contraseña de un solo uso que permite que un servidor de seguridad se empareje con una instancia del servidor de conexión. La contraseña no es válida después de introducirla en el programa de instalación del servidor de conexión.

Nota No puede emparejar una versión anterior del servidor de seguridad con la versión actual del servidor de conexión. Si configura una contraseña de emparejamiento en la versión actual del servidor de conexión e intenta instalar una versión anterior del servidor de seguridad, la contraseña de emparejamiento no será válida.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña Servidores de conexión, seleccione la instancia del servidor de conexión que desee emparejar con el servidor de seguridad.

- 3 En el menú desplegable **Más comandos**, seleccione **Especificar contraseña para emparejar al servidor de seguridad**.
- 4 Escriba la contraseña en los cuadros de texto Emparejando contraseña y Confirmar contraseña y especifique un valor de tiempo de espera de contraseña.

Debe usar la contraseña dentro del periodo de tiempo de espera especificado.
- 5 Haga clic en **Aceptar** para configurar la contraseña.

Pasos siguientes

Instale un servidor de seguridad. Consulte [Instalar un servidor de seguridad](#).

Importante Si no proporciona la contraseña de emparejamiento del servidor de seguridad en el programa de instalación del servidor de conexión dentro del límite de tiempo para la contraseña, esta pasa a no ser válida y debe configurar una nueva contraseña.

Instalar un servidor de seguridad

Un servidor de seguridad es una instancia del servidor de conexión que agrega una capa adicional de seguridad entre Internet y la red interna. Puede instalar uno o varios servidores de seguridad para conectarse a una instancia del servidor de conexión.

El software del servidor de seguridad no puede coexistir en la misma máquina virtual ni en el mismo equipo físico con cualquier otro componente de software de Horizon 7, como un servidor de réplica, un servidor de conexión, View Composer, Horizon Agent u Horizon Client.

Requisitos previos

- Determine el tipo de topología que se debe utilizar. Por ejemplo, determine qué solución de equilibrio de carga se debe utilizar. Decida si las instancias del servidor de conexión que están emparejadas a los servidores de seguridad se dedicarán a los usuarios de la red externa. Para obtener más información, consulte el documento *Planificación de la arquitectura de Horizon 7*.

Importante Si utiliza un equilibrador de carga, este debe tener una dirección IP que no cambie. En un entorno IPv4, configure una dirección IP estática. En un entorno IPv6, los equipos obtienen automáticamente direcciones IP que no cambian.

- Verifique que la instalación cumpla con los requisitos descritos en [Requisitos del servidor de conexión de Horizon](#).
- Prepare su entorno para la instalación. Consulte [Requisitos de instalación del servidor de conexión de Horizon](#).
- Compruebe que la instancia del servidor de conexión que debe estar conectada al servidor de seguridad esté instalada, configurada y ejecutando una versión del servidor de conexión compatible con la versión del servidor de seguridad. Consulte el apartado sobre la matriz de compatibilidad de los componentes de Horizon 7 en el documento *Actualizaciones de Horizon 7*.

- Compruebe que se pueda acceder a la instancia del servidor de conexión que se conecta al servidor de seguridad desde el equipo en el que tiene planificado instalar el servidor de seguridad.

Nota Después de actualizar un servidor de conexión a la versión 7.5 de Horizon 7, los servidores de seguridad con IPsec deshabilitado se deben volver a instalar. Si la dirección IP de un servidor de seguridad cambia, se debe volver a instalar. El emparejamiento de los servidores de seguridad no funciona correctamente si el servidor de seguridad se encuentra tras un NAT dinámico.

- Configure una contraseña de emparejamiento para el servidor de seguridad. Consulte [Configurar una contraseña de emparejamiento para el servidor de seguridad](#).
- Familiarícese con el formato de las URL externas. Consulte [Configurar URL externas para conexiones seguras de puerta de enlace y túnel..](#)
- Verifique que el Firewall de Windows con seguridad avanzada esté **activado** en los perfiles activos. Se recomienda que esta opción esté **activada** en todos los perfiles. De forma predeterminada, las reglas IPsec rigen las conexiones entre el servidor de seguridad y el servidor de conexión de View y requieren que se habilite el Firewall de Windows con seguridad avanzada.
- Familiarícese con los puertos de red que deben abrirse en el Firewall de Windows para un servidor de seguridad. Consulte [Reglas de firewall para el servidor de conexión de Horizon](#).
- Si la topología de la red incluye un firewall back-end entre un servidor de seguridad y la instancia del servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte [Configurar que un firewall back-end admita IPsec](#).
- Si está actualizando o volviendo a instalar el servidor de seguridad, verifique que las reglas IPsec existentes para el servidor de seguridad se hayan suprimido. Consulte [Eliminar las reglas IPsec del servidor de seguridad](#).
- Si está instalando Horizon 7 en modo FIPS, debe anular la selección de la opción de configuración global **Usar IPsec para las conexiones del servidor de seguridad** en Horizon Administrator, ya que en modo FIPS, debe configurar IPsec manualmente tras instalar el servidor de seguridad.

Procedimiento

- 1 Descargue el archivo instalador del servidor de conexión desde el sitio de descargas de VMware disponible en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el servidor de conexión.

El nombre del archivo instalador es VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- 2 Para iniciar el programa de instalación del servidor de conexión, haga doble clic en el archivo instalador.
- 3 Acepte los términos de licencia de VMware.
- 4 Acepte o cambie la carpeta de destino.
- 5 Seleccione la opción de instalación **Servidor de seguridad de View**.

- 6 Seleccione la versión del protocolo de Internet (**IPv4** o **IPv6**).

Debe instalar todos los componentes de Horizon 7 con la misma versión de IP.

- 7 Seleccione si desea habilitar o deshabilitar el modo FIPS.

Esta opción estará disponible solo si el modo FIPS está habilitado en Windows.

- 8 Escriba el nombre de dominio completo o la dirección IP de la instancia del servidor de conexión para emparejar con el servidor de seguridad en el cuadro de texto **Servidor**.

El servidor de seguridad reenvía el tráfico de red a dicha instancia del servidor de conexión.

- 9 Escriba la contraseña de emparejamiento del servidor de seguridad en el cuadro de texto **Contraseña**.

Si la contraseña caducó, puede utilizar Horizon Administrator para configurar una nueva contraseña y escribirla en el programa de instalación.

- 10 En el cuadro de texto **URL externa**, escriba la URL externa del servidor de seguridad. Esto es necesario para todos los clientes, independientemente del protocolo de visualización que usen.

La URL debe incluir el identificador de protocolo (https), el nombre de servidor de seguridad que pueda resolver el cliente y el número de puerto (443).

Por ejemplo: https://view.example.com:443

Los clientes compatibles con el túnel que estén fuera de la red utilizarán la URL para acceder a las máquinas que están dentro de la red a través del servidor de seguridad.

- 11 En el cuadro de texto **URL externa de PCoIP**, escriba la URL externa de la puerta de enlace PCoIP del servidor de seguridad. Esto es necesario para los clientes que usan el protocolo de visualización PCoIP para conectarse a escritorios remotos.

La URL relativa al protocolo debe contener la dirección IP del servidor de seguridad y el número de puerto (4172). En entornos IPv4, utilice una dirección IPv4. En entornos IPv6, utilice una dirección IPv6.

Por ejemplo, en un entorno IPv4: 10.20.30.40:4172

Los clientes compatibles con PCoIP que estén fuera de la red utilizarán la URL para acceder a las máquinas que están dentro de la red a través del servidor de seguridad.

Nota Aunque debe introducirse aquí una dirección IPv6 cuando se encuentre en un entorno IPv6, se puede reemplazar por un nombre que el cliente pueda resolver después de la instalación.

- 12 En el cuadro de texto **URL externa de Blast**, escriba la URL externa de la puerta de enlace Blast del servidor de seguridad. Esto es necesario para los clientes que usan el protocolo de visualización Blast o HTML Access para conectarse a escritorios remotos.

La URL debe incluir el identificador de protocolo (https), el nombre de servidor de seguridad que pueda resolver el cliente y el número de puerto (8443).

Por ejemplo, https://myserver.example.com:8443

Los clientes de HTML Access y compatibles con Blast que estén fuera de la red utilizarán la URL para acceder a las máquinas que están dentro de la red a través del servidor de seguridad.

13 Elija cómo configurar el servicio Firewall de Windows.

Opción	Acción
Configurar el Firewall de Windows automáticamente	Permita que el instalador configure el Firewall de Windows para autorizar las conexiones de red necesarias.
No configurar el Firewall de Windows	Configure las reglas del Firewall de Windows de forma manual. Seleccione esta opción solo si la organización utiliza sus propias reglas predefinidas para configurar el Firewall de Windows.

14 Complete el asistente para finalizar la instalación del servidor de seguridad.

Resultados

Se instalan los servicios de los servidores de seguridad en el equipo Windows Server:

- Servidor de seguridad de VMware Horizon View
- Componente del marco de VMware Horizon View
- Componente de puerta de enlace de seguridad de VMware Horizon View
- Puerta de enlace segura PCoIP de VMware Horizon View
- Puerta de enlace segura de VMware Blast

Para obtener más información sobre estos servicios, consulte el documento *Administración de Horizon 7*.

El servidor de seguridad aparece en el panel Servidores de seguridad en Horizon Administrator.

La regla **Servidor de conexión de VMware Horizon View (integrado en Blast)** está habilitada en el Firewall de Windows del servidor de seguridad. Esta regla del firewall permite a los navegadores web de los dispositivos cliente usar HTML Access para conectarse al servidor de seguridad en TCP puerto 8443.

Nota Si se cancela o aborta la instalación, tendrá que eliminar las reglas IPsec para el servidor de seguridad antes de comenzarla de nuevo. Realice este paso incluso si ya eliminó las reglas IPsec antes de volver a instalar o actualizar el servidor de seguridad. Para obtener más instrucciones sobre cómo eliminar regla IPsec, consulte [Eliminar las reglas IPsec del servidor de seguridad](#).

Pasos siguientes

Configure un certificado de servidor SSL para el servidor de seguridad. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

Es posible que tenga que configurar las opciones de conexión de cliente para el servidor de seguridad y ajustar la configuración de Windows Server para permitir una implementación grande. Consulte [Configurar conexiones de Horizon Client](#) y [Configuración de tamaño de Windows Server para admitir la implementación](#).

Si vuelve a instalar el servidor de seguridad y cuenta con un recopilador de datos configurado para supervisar los datos de rendimiento, detenga el recopilador y vuelva a iniciarlo.

Instalar un servidor de seguridad de forma silenciosa

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

La instalación silenciosa le permite implementar los componentes de Horizon 7 correctamente en una empresa de gran tamaño.

Requisitos previos

- Determine el tipo de topología que se debe utilizar. Por ejemplo, determine qué solución de equilibrio de carga se debe utilizar. Decida si las instancias del servidor de conexión que están emparejadas a los servidores de seguridad se dedicarán a los usuarios de la red externa. Para obtener más información, consulte el documento *Planificación de la arquitectura de Horizon 7*.

Importante Si utiliza un equilibrador de carga, este debe tener una dirección IP que no cambie. En un entorno IPv4, configure una dirección IP estática. En un entorno IPv6, los equipos obtienen automáticamente direcciones IP que no cambian.

- Verifique que la instalación cumpla con los requisitos descritos en [Requisitos del servidor de conexión de Horizon](#).
- Prepare su entorno para la instalación. Consulte [Requisitos de instalación del servidor de conexión de Horizon](#).
- Compruebe que la instancia del servidor de conexión que debe estar conectada al servidor de seguridad esté instalada, configurada y ejecutando una versión del servidor de conexión compatible con la versión del servidor de seguridad. Consulte el apartado sobre la matriz de compatibilidad de los componentes de Horizon 7 en el documento *Actualizaciones de Horizon 7*.
- Compruebe que se pueda acceder a la instancia del servidor de conexión que se conecta al servidor de seguridad desde el equipo en el que tiene planificado instalar el servidor de seguridad.

Nota Después de actualizar un servidor de conexión a la versión 7.5 de Horizon 7, los servidores de seguridad con IPSec deshabilitado se deben volver a instalar. Si la dirección IP de un servidor de seguridad cambia, se debe volver a instalar. El emparejamiento de los servidores de seguridad no funciona correctamente si el servidor de seguridad se encuentra tras un NAT dinámico.

- Configure una contraseña de emparejamiento para el servidor de seguridad. Consulte [Configurar una contraseña de emparejamiento para el servidor de seguridad](#).
- Familiarícese con el formato de las URL externas. Consulte [Configurar URL externas para conexiones seguras de puerta de enlace y túnel](#).
- Verifique que el Firewall de Windows con seguridad avanzada esté **activado** en los perfiles activos. Se recomienda que esta opción esté **activada** en todos los perfiles. De forma predeterminada, las reglas IPsec rigen las conexiones entre el servidor de seguridad y el servidor de conexión, y requieren que se habilite el Firewall de Windows con seguridad avanzada.

- Familiarícese con los puertos de red que deben abrirse en el Firewall de Windows para un servidor de seguridad. Consulte [Reglas de firewall para el servidor de conexión de Horizon](#).
- Si la topología de la red incluye un firewall back-end entre un servidor de seguridad y la instancia del servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte [Configurar que un firewall back-end admita IPsec](#).
- Si está actualizando o volviendo a instalar el servidor de seguridad, verifique que las reglas IPsec existentes para el servidor de seguridad se hayan suprimido. Consulte [Eliminar las reglas IPsec del servidor de seguridad](#).
- Familiarícese con las opciones de la línea de comandos del instalador MSI. Consulte [Opciones de la línea de comandos de Microsoft Windows Installer](#).
- Familiarícese con las propiedades de instalación silenciosa disponibles con un servidor de seguridad. Consulte [Propiedades de instalación silenciosa para un servidor de seguridad](#).
- Si está instalando Horizon 7 en modo FIPS, debe anular la selección de la opción de configuración global **Usar IPsec para las conexiones del servidor de seguridad** en Horizon Administrator, ya que en modo FIPS, debe configurar IPsec manualmente tras instalar el servidor de seguridad.

Procedimiento

- 1 Descargue el archivo instalador del servidor de conexión desde el sitio de descargas de VMware disponible en <https://my.vmware.com/web/vmware/downloads>.

En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el servidor de conexión.

El nombre del archivo instalador es VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- 2 Abra una ventana del símbolo del sistema en el equipo Windows Server.
- 3 Escriba el comando de instalación en una línea.

```
Por ejemplo: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn
VDM_SERVER_INSTANCE_TYPE=3 VDM_SERVER_NAME=cs1.internaldomain.com
VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443
VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172
VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_BSG_EXTURL=https://
view.companydomain.com:8443 VDM_SERVER_SS_PWD=secret"
```

Resultados

Se instalan los servicios de los servidores de seguridad en el equipo Windows Server:

- Servidor de seguridad de VMware Horizon View
- Componente del marco de VMware Horizon View
- Componente de puerta de enlace de seguridad de VMware Horizon View
- Puerta de enlace segura PCoIP de VMware Horizon View

■ Puerta de enlace segura de VMware Blast

Para obtener más información sobre estos servicios, consulte el documento *Administración de Horizon 7*.

El servidor de seguridad aparece en el panel Servidores de seguridad en Horizon Administrator.

La regla **Servidor de conexión de VMware Horizon View (integrado en Blast)** está habilitada en el Firewall de Windows del servidor de seguridad. Esta regla del firewall permite a los navegadores web de los dispositivos cliente usar HTML Access para conectarse al servidor de seguridad en TCP puerto 8443.

Nota Si se cancela o aborta la instalación, tendrá que eliminar las reglas IPsec para el servidor de seguridad antes de comenzarla de nuevo. Realice este paso incluso si ya eliminó las reglas IPsec antes de volver a instalar o actualizar el servidor de seguridad. Para obtener más instrucciones sobre cómo eliminar regla IPsec, consulte [Eliminar las reglas IPsec del servidor de seguridad](#).

Pasos siguientes

Configure un certificado de servidor SSL para el servidor de seguridad. Consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

Es posible que tenga que configurar las opciones de conexión de cliente para el servidor de seguridad y ajustar la configuración de Windows Server para permitir una implementación grande. Consulte [Configurar conexiones de Horizon Client](#) y [Configuración de tamaño de Windows Server para admitir la implementación](#).

Propiedades de instalación silenciosa para un servidor de seguridad

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

Tabla 7-3. Propiedades MSI para instalar de forma silenciosa un servidor de seguridad

Propiedad MSI	Descripción	Valor predeterminado
INSTALLDIR	<p>La ruta y la carpeta en las que el software del servidor de conexión está instalado.</p> <p>Por ejemplo: INSTALLDIR=""D:\abc\my folder""</p> <p>Si se incluyen comillas dobles que abran y cierren la ruta, el instalador MSI puede interpretar el espacio como parte válida de la ruta.</p> <p>La propiedad MSI es opcional.</p>	%ProgramFiles%\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	<p>El tipo de instalación del servidor de conexión:</p> <ul style="list-style-type: none"> ■ 1. Instalación estándar ■ 2. Instalación de réplica ■ 3. Instalación del servidor de seguridad <p>Para instalar un servidor de seguridad, defina VDM_SERVER_INSTANCE_TYPE=3</p> <p>Esta propiedad MSI es obligatoria cuando se instala un servidor de seguridad.</p>	1

Tabla 7-3. Propiedades MSI para instalar de forma silenciosa un servidor de seguridad (continuación)

Propiedad MSI	Descripción	Valor predeterminado
VDM_SERVER_NAME	El nombre del host o la dirección IP de la instancia del servidor de conexión que se empareja con el servidor de seguridad. Por ejemplo: VDM_SERVER_NAME=cs1.internaldomain.com Esta propiedad MSI es obligatoria.	Ninguna
VDM_SERVER_SS_EXTURL	La URL externa del servidor de seguridad. La URL debe incluir el protocolo, un nombre de servidor de seguridad que se pueda resolver de forma externa y el número de puerto Por ejemplo: VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443 Esta propiedad MSI es obligatoria.	Ninguno
VDM_SERVER_SS_PWD	La contraseña de emparejamiento del servidor de seguridad. Por ejemplo: VDM_SERVER_SS_PWD=secret Esta propiedad MSI es obligatoria.	Ninguna
FWCHOICE	La propiedad MSI que determina si desea configurar un firewall para la instancia del servidor de conexión. El valor 1 configura un firewall. El valor 2 no configura ningún firewall. Por ejemplo: FWCHOICE=1 La propiedad MSI es opcional.	1
VDM_SERVER_SS_PCOIP_IPADDR	La dirección IP externa de la puerta de enlace segura PCoIP. En un entorno IPv6, el FQDN de la puerta de enlace segura PCoIP también puede establecer esta propiedad. Solo se admite esta propiedad cuando el servidor de seguridad está instalado en Windows Server 2008 R2 o una versión posterior. Por ejemplo: VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 Esta propiedad es obligatoria si piensa usar el componente de la puerta de enlace segura PCoIP.	Ninguna
VDM_SERVER_SS_PCOIP_TCPPORT	El número de puerto TCP externo de la puerta de enlace segura PCoIP. Solo se admite esta propiedad cuando el servidor de seguridad está instalado en Windows Server 2008 R2 o una versión posterior. Por ejemplo: VDM_SERVER_SS_PCOIP_TCPPORT=4172 Esta propiedad es obligatoria si piensa usar el componente de la puerta de enlace segura PCoIP.	Ninguna
VDM_SERVER_SS_PCOIP_UDPPORT	El número de puerto UDP externo de la puerta de enlace segura PCoIP. Solo se admite esta propiedad cuando el servidor de seguridad está instalado en Windows Server 2008 R2 o una versión posterior. Por ejemplo: VDM_SERVER_SS_PCOIP_UDPPORT=4172 Esta propiedad es obligatoria si piensa usar el componente de la puerta de enlace segura PCoIP.	Ninguna

Tabla 7-3. Propiedades MSI para instalar de forma silenciosa un servidor de seguridad (continuación)

Propiedad MSI	Descripción	Valor predeterminado
VDM_SERVER_SS_BSG_EXTURL	La URL externa de la puerta de enlace segura Blast. La URL debe incluir el protocolo HTTPS, un nombre de servidor de seguridad que se pueda resolver de forma externa y el número de puerto Por ejemplo: VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443 El puerto predeterminado es el 8443. Para permitir a los usuarios establecer conexiones web a los escritorios de Horizon 7, se debe instalar una puerta de enlace segura de Blast en el servidor de seguridad.	Ninguna
VDM_SERVER_SS_FORCE_IPSEC	Obliga a utilizar IPsec entre el servidor de seguridad y la instancia del servidor de conexión de emparejada. De forma predeterminada, una instalación desatendida y un emparejamiento del servidor de seguridad con una instancia del servidor de conexión que tenga IPsec deshabilitado provocan un error en el emparejamiento. El valor predeterminado 1 obliga al emparejamiento con IPsec. Establezca este valor en 0 para permitir un emparejamiento sin IPsec.	1
VDM_IP_PROTOCOL_USAGE	Especifica la versión IP que los componentes de Horizon 7 usan para comunicarse. Los valores posibles son IPv4 e IPv6	IPv4
VDM_FIPS_ENABLED	Especifica si desea habilitar o deshabilitar el modo FIPS. El valor 1 habilita el modo FIPS. El valor 0 deshabilita el modo FIPS. Si esta propiedad se establece en 1 y Windows no está en modo FIPS, el instalador se detiene.	0

Eliminar las reglas IPsec del servidor de seguridad

Antes de que pueda actualizar o volver a instalar una instancia del servidor de seguridad, debe eliminar las reglas IPsec que dirigen la comunicación entre el servidor de seguridad y la instancia del servidor de conexión emparejada. Si no realiza este paso, se produce un error en la actualización o reinstalación.

De forma predeterminada, las reglas IPsec rigen la comunicación entre un servidor de seguridad y la instancia del servidor de conexión emparejada. Cuando vuelve a instalar o actualiza el servidor de seguridad y lo vuelve a emparejar con la instancia del servidor de conexión, se debe establecer un nuevo conjunto de reglas IPsec. Si no se eliminan las reglas IPsec existentes antes de actualizar o volver a instalar, se produce un error en el emparejamiento.

Debe realizar este paso cuando actualice o vuelva a instalar un servidor de seguridad y esté usando IPsec para proteger la comunicación entre el servidor de seguridad y el servidor de conexión.

Puede configurar un emparejamiento inicial del servidor de seguridad sin usar las reglas IPsec. Antes de instalar el servidor de seguridad, puede abrir Horizon Administrator y desmarcar la opción global **Usar IPsec para las conexiones del servidor de seguridad**, que está habilitada de forma predeterminada. Si las reglas IPsec no se aplican, no es necesario que las elimine antes de actualizar o reinstalar.

Nota No es necesario que elimine ningún servidor de seguridad de Horizon Administrator antes de actualizar o volver a instalar el servidor de seguridad. Elimine un servidor de seguridad de Horizon Administrator solo si pretende eliminar el servidor de seguridad de forma permanente del entorno de Horizon 7.

Con View 5.0.x y versiones anteriores, puede eliminar un servidor de seguridad desde la interfaz de usuario de Horizon Administrator o con el comando `vdmadmin -S` de la línea de comandos. En View 5.1 y versiones posteriores, debe usar `vdmadmin -S`. Consulte cómo eliminar una entrada de una instancia del servidor de conexión de Horizon o del servidor de seguridad con la opción `-S`, en el documento *Administración de Horizon 7*.

Precaución Si elimina las reglas IPsec de un servidor de seguridad activo, se pierde la comunicación con el servidor de seguridad hasta que actualice o vuelva a instalar este servidor. Por lo tanto, si usa un equilibrador de carga para administrar un grupo de servidores de seguridad, realice este procedimiento en el servidor y, a continuación, actualícelo antes de eliminar las reglas IPsec del siguiente servidor. Puede eliminar los servidores de la producción y agregarlos uno a uno para evitar que los usuarios finales entren en un tiempo de inactividad.

Procedimiento

- 1 En Horizon Administrator, haga clic en **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de seguridad**, seleccione un servidor de seguridad y haga clic en **Más comandos > Preparar para la actualización o para la reinstalación**.

Si deshabilitó las reglas IPsec antes de instalar el servidor de seguridad, esta opción no está activa. En este caso, no es necesario que elimine las reglas IPsec antes de volver a instalar o actualizar.
- 3 Haga clic en **Aceptar**.

Resultados

Las reglas IPsec se eliminan y la opción **Preparar para la actualización o para la reinstalación** se vuelve inactiva, lo que indica que puede volver a instalar o actualizar el servidor de seguridad.

Pasos siguientes

Actualice o vuelva a instalar el servidor de seguridad.

Ventajas de los dispositivos Unified Access Gateway sobre la VPN

Un dispositivo Unified Access Gateway es la puerta de enlace predeterminada para acceder de forma segura a aplicaciones y escritorios remotos desde fuera del firewall empresarial.

Para ver la documentación de la última versión de Unified Access Gateway, consulte el documento *Implementación y configuración de VMware Unified Access Gateway* en <https://docs.vmware.com/es/Unified-Access-Gateway/index.html>.

Un dispositivo Unified Access Gateway reside en una zona desmilitarizada de la red (DMZ) y actúa como un host de proxy para las conexiones en una red de confianza, proporcionando una capa adicional de seguridad que protege los escritorios virtuales, los hosts de las aplicaciones y los servidores de parte pública de Internet.

Configurar un dispositivo de Unified Access Gateway

Unified Access Gateway y las soluciones VPN genéricas son similares ya que ambos garantizan que el tráfico se reenvía a una red interna únicamente en nombre de usuarios con autenticación sólida.

Entre las ventajas de Unified Access Gateway sobre la VPN genérica se incluyen las siguientes:

- **Access Control Manager.** Unified Access Gateway aplica reglas de acceso automáticamente. Unified Access Gateway reconoce las autorizaciones de los usuarios y el direccionamiento requerido para conectarse internamente. Una VPN hace lo mismo, ya que la mayoría de las VPN permiten a un administrador configurar las reglas de conexión de red para cada usuario o grupo de usuarios individualmente. Al principio, esto funciona bien con una VPN, pero mantener las reglas necesarias exige un esfuerzo administrativo importante.
- **Interfaz de usuario.** Unified Access Gateway no modifica la clara interfaz de usuario de Horizon Client. Con Unified Access Gateway, cuando Horizon Client se inicia, los usuarios autenticados se encuentran en sus entornos de View y tienen acceso controlado a sus escritorios y aplicaciones. En una VPN, es obligatorio configurar primero el software de la VPN y autenticar por separado antes de iniciar Horizon Client.
- **Rendimiento.** Unified Access Gateway está diseñado para maximizar la seguridad y el rendimiento. Con Unified Access Gateway, PCoIP, HTML Access y los protocolos WebSocket están seguros sin necesidad de encapsulaciones adicionales. Las VPN se implementan como VPN SSL. Esta implementación cumple los requisitos de seguridad y, con TLS habilitado, se considera segura, pero el protocolo subyacente con SSL/TLS está basado simplemente en TCP. Los protocolos actuales de vídeo remoto aprovechan los transportes basados en UDP sin conexión, por lo que sus ventajas de rendimiento pueden verse mermadas si deben utilizar un transporte basado en TCP. Esto no se aplica a todas las tecnologías de VPN, ya que las que también funcionan con DTLS o IPsec en lugar de SSL/TLS ofrecen un buen rendimiento con los protocolos de escritorio de Horizon 7.

Mejorar la seguridad de Horizon con Unified Access Gateway

Un dispositivo de Unified Access Gateway mejora la seguridad superponiendo la capa de autenticación de la certificación del dispositivo encima de la autenticación del usuario para que el acceso se pueda limitar solo a los dispositivos conocidos y agregando otra capa de seguridad en la infraestructura de escritorio virtual.

Nota Esta función solo es compatible con Horizon Client para Windows.

- Consulte cómo configurar el certificado o la autenticación de tarjeta inteligente en el dispositivo Unified Access Gateway en el documento *Implementación y configuración de VMware Unified Access Gateway* disponible en <https://docs.vmware.com/es/Unified-Access-Gateway/index.html>.
- La función para comprobar el cumplimiento del endpoint proporciona una capa extra de seguridad para acceder a los escritorios de Horizon, además del resto de servicios de autenticación del usuario que están disponibles en Unified Access Gateway. Consulte cómo comprobar el cumplimiento del endpoint para Horizon en el documento *Implementación y configuración de VMware Unified Access Gateway* disponible en <https://docs.vmware.com/es/Unified-Access-Gateway/index.html>.

Importante Cuando un dispositivo Unified Access Gateway se configura para la autenticación de dos fases (RSA SecurID y RADIUS) y la coincidencia de nombres de usuario de Windows está habilitada y hay varios dominios de usuario, debe habilitar el servidor de conexión para enviar la lista de dominios, de modo que el usuario pueda seleccionar el dominio adecuado mientras utiliza el nombre de usuario y la contraseña de Windows para la autenticación.

DMZ de doble salto

En los casos en los que se requiera una DMZ de doble salto entre Internet y la red interna, puede implementar un dispositivo Unified Access Gateway en la DMZ externa como un proxy inverso de web con Unified Access Gateway en la DMZ interna para crear una configuración DMZ de doble salto. El tráfico pasará a través de un proxy inverso específico en cada capa de la DMZ y no podrá omitir una capa de la DMZ. Para obtener más información sobre esa configuración, consulte el documento *Implementación y configuración de VMware Unified Access Gateway*.

Reglas de firewall para el servidor de conexión de Horizon

Algunos puertos se deben abrir en el firewall para los servidores de seguridad y las instancias del servidor de conexión.

Cuando instale el servidor de conexión, el programa de instalación puede configurar de forma opcional las reglas del Firewall de Windows que necesita. Estas reglas abren los puertos que se utilizan de forma predeterminada. Si cambia los puertos predeterminados después de la instalación, debe configurar de forma manual el Firewall de Windows para que permita que los dispositivos de Horizon Client se conecten a Horizon 7 a través de los puertos actualizados.

La siguiente tabla muestra los puertos predeterminados que se pueden abrir de forma automática durante la instalación. Los puertos son de entrada a menos que se especifique lo contrario.

Tabla 7-4. Puertos abiertos durante la instalación del servidor de conexión de Horizon

Protocolo	Puertos	Tipo de instancia del servidor de conexión de Horizon
JMS	TCP 4001	Estándar y de réplica
JMS	TCP 4002	Estándar y de réplica
JMSIR	TCP 4100	Estándar y de réplica
JMSIR	TCP 4101	Estándar y de réplica
AJP13	TCP 8009	Estándar y de réplica
HTTP	TCP 80	Servidor de seguridad, de réplica y estándar
HTTPS	TCP 443	Servidor de seguridad, de réplica y estándar
PCoIP	TCP 4172 integrado UDP 4172 ambas direcciones	Servidor de seguridad, de réplica y estándar
HTTPS	TCP 8443 UDP 8443	Servidor de seguridad, de réplica y estándar. Después de establecer la conexión inicial a Horizon 7, el navegador web o un dispositivo cliente se conecta a la puerta de enlace segura de Blast en el puerto TCP 8443. La puerta de enlace segura de Blast se debe habilitar en una instancia del servidor de conexión de View o del servidor de seguridad para permitir que se produzca esta segunda conexión.
HTTPS	TCP 8472	Estándar y de réplica Para la función Arquitectura de Cloud Pod: usada para la comunicación entre pods.
HTTP	TCP 22389	Estándar y de réplica Para la función Arquitectura de Cloud Pod: usada para la replicación LDAP global.
HTTPS	TCP 22636	Estándar y de réplica Para la función Arquitectura de Cloud Pod: usada para la replicación LDAP global de seguridad.

Configurar que un firewall back-end admita IPsec

Si la topología de la red incluye un firewall back-end entre servidores de seguridad e instancias del servidor de conexión, tiene que configurar algunos protocolos y puertos en el firewall para que sean compatibles con IPsec. Sin la configuración adecuada, los datos enviados a través de un servidor de seguridad y la instancia del servidor de conexión no podrán pasar a través del firewall.

De forma predeterminada, las reglas IPsec rigen las conexiones entre los servidores de seguridad y las instancias del servidor de conexión. Para dar soporte a IPsec, el instalador del servidor de conexión puede configurar las reglas del firewall de Windows en los hosts de Windows Server donde estén instalados los servidores de Horizon 7. Para un firewall back-end, debe configurar las reglas usted mismo.

Nota Se recomienda que use IPsec. También puede deshabilitar la configuración global **Usar IPsec para las conexiones del servidor de seguridad** de Horizon Administrator.

Las siguientes reglas deben permitir el tráfico bidireccional. Es posible que tenga que especificar reglas independientes en el firewall para el tráfico entrante y el saliente.

Se aplican diferentes reglas a los firewalls que usan la traducción de direcciones de red (NAT) y a los que no la usan.

Tabla 7-5. Requisitos para que firewalls sin NAT admitan reglas IPsec

Origen	Protocolo	Puerto	Destino	Notas
Servidor de seguridad	ISAKMP	UDP 500	Servidor de conexión de Horizon	Los servidores de seguridad usan el puerto UDP 500 para negociar la seguridad IPsec.
Servidor de seguridad	ESP	No disponible	Servidor de conexión de Horizon	El protocolo ESP encapsula el tráfico cifrado de IPsec. No es necesario que especifique un puerto para ESP como parte de la regla. Si es necesario, puede especificar direcciones IP de origen y de destino para reducir el ámbito de la regla.

Las siguientes reglas se aplican a los firewalls que usan NAT.

Tabla 7-6. Requisitos para que los firewalls con NAT admitan reglas IPsec

Origen	Protocolo	Puerto	Destino	Notas
Servidor de seguridad	ISAKMP	UDP 500	Servidor de conexión de Horizon	Los servidores de seguridad usan el puerto UDP 500 para iniciar la negociación de seguridad IPsec.
Servidor de seguridad	NAT-T ISAKMP	UDP 4500	Servidor de conexión de Horizon	Los servidores de seguridad usan el puerto UDP 4500 para las NAT transversales y para negociar la seguridad IPsec.

Volver a instalar el servidor de conexión de Horizon con una configuración de seguridad

En determinadas situaciones, es necesario volver a instalar la versión actual de una instancia del servidor de conexión y restaurar la configuración existente de Horizon 7 mediante la importación de un archivo LDIF de seguridad que incluya los datos de configuración de LDAP de View.

Por ejemplo, como parte del plan de recuperación de desastre y de continuidad del negocio (business continuity and disaster recovery plan, BC/DR), es posible que quiera disponer de un procedimiento en caso de que el almacén de datos dejara de funcionar. El primer paso de dicho plan es asegurarse de que se guardó una copia de seguridad de la configuración LDAP de View en otra ubicación. El segundo paso es instalar el servidor de conexión en una nueva ubicación e importar la configuración de seguridad, como se describe en este procedimiento.

Puede que también sea necesario realizar este procedimiento al configurar un segundo centro de datos con la configuración de Horizon 7 existente. O bien, en el caso de que la implementación de Horizon 7 incluya una única instancia del servidor de conexión y se produzca un error con dicho servidor.

No es necesario seguir este procedimiento si posee varias instancias del servidor de conexión en un grupo replicado y solo una instancia falla. Basta con volver a instalar el servidor de conexión como una réplica. Durante la instalación, se proporciona la información de la conexión a otra instancia del servidor de seguridad y Horizon 7 restaura la configuración LDAP de View a partir de la otra instancia.

Requisitos previos

- Compruebe que una copia de seguridad de la configuración LDAP de View se haya incluido en un archivo LDIF cifrado.
- Familiarícese con los pasos para restaurar una configuración LDAP de View desde un archivo de seguridad LDIF con el comando `vdmimport`.

Consulte cómo realizar una copia de seguridad y restaurar los datos de la configuración de Horizon 7 en el documento *Administración de Horizon 7*.

- Familiarícese con los pasos para instalar la nueva instancia del servidor de conexión. Consulte [Instalar el servidor de conexión de Horizon con una nueva configuración](#).

Procedimiento

- 1 Instale el servidor de conexión con una nueva configuración.
- 2 Descifre el archivo LDIF cifrado.

Por ejemplo:

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

- 3 Importe el archivo LDIF descifrado para restaurar la configuración LDAP de View.

Por ejemplo:

```
vdmimport -f MyDecryptedexport.LDF
```

Nota En esta fase, aún no se puede acceder a la configuración de Horizon 7. Los clientes no pueden acceder al servidor de conexión ni conectarse a sus escritorios.

- 4 Desinstale el servidor de conexión del equipo con la herramienta de Windows **Agregar o quitar programas**.

No desinstale la configuración LDAP de View, la instancia llamada "AD LDS Instance VMwareVDMDS". Puede usar la herramienta **Agregar o quitar programas** para comprobar que la instancia "AD LDS Instance VMwareVDMDS" no fue eliminada del equipo Windows Server.

- 5 Vuelva a instalar el servidor de conexión.

En la ventana del instalador, acepte el directorio LDAP de View existente.

Pasos siguientes

Configure el servidor de conexión y el entorno de Horizon 7 de la misma forma que tras instalar una instancia del servidor de conexión con una nueva configuración.

Opciones de la línea de comandos de Microsoft Windows Installer

Para instalar silenciosamente los componentes de Horizon 7, debe usar las propiedades y las opciones de la línea de comandos de Microsoft Windows Installer (MSI). Los instaladores de los componentes de Horizon 7 son programas MSI y usan las funciones estándares de MSI.

Si desea obtener más información sobre MSI, consulte el sitio web de Microsoft. En cuanto a las opciones de la línea de comandos MSI, consulte el sitio web Microsoft Developer Network (MSDN) Library y busque las opciones de la línea de comandos MSI. Para consultar el uso de la línea de comandos MSI, puede abrir una ventana de símbolo del sistema en el equipo donde se encuentran los componentes de Horizon 7 e introducir `msiexec /?`.

Para ejecutar un instalador silencioso de un componente de Horizon 7, comience silenciando el programa de arranque que extrae el instalador en un directorio temporal e inicie una instalación interactiva.

En la línea de comando, debe introducir las opciones que controlan el programa de arranque del instalador.

Tabla 7-7. Opciones de línea de comandos del programa de arranque del componente de Horizon 7

Opción	Descripción
<code>/s</code>	<p>Deshabilita el cuadro de diálogo de extracción y la pantalla de presentación del arranque, lo que evita que aparezcan diálogos interactivos.</p> <p>Por ejemplo: <code>servidordeconexióndeview-VMware-y.y.y-xxxxxx.exe /s</code></p> <p>Es necesaria la opción <code>/s</code> para ejecutar una instalación silenciosa.</p>
<code>/v"</code> <i>opciones_de_línea_de_comando</i> <code>s_para_MSI"</code>	<p>Ordena al instalador que envíe la cadena entre comillas dobles que introdujo en la línea de comandos como un conjunto de opciones para que MSI las interprete. Debe escribir las entradas de la línea de comandos entre comillas dobles. Escriba comillas dobles después de <code>/v</code> y al final de la línea de comandos.</p> <p>Por ejemplo: <code>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"opciones_línea_comandos"</code></p> <p>Si desea que el instalador MSI interprete una cadena que contiene espacios, escriba dos grupos de comillas dobles en la cadena. Por ejemplo, es posible que quiera instalar el componente de Horizon 7 con un nombre de ruta de instalación que contenga espacios.</p> <p>Por ejemplo: <code>servidordeconexióndeview-VMware-y.y.y-xxxxxx.exe /s /v"opciones_línea_comandos INSTALLDIR=""d:\abc\mi carpeta"""</code></p> <p>En este ejemplo, el instalador MSI transmitirá la ruta del directorio de instalación y no intentará interpretar la cadena como dos opciones de la línea de comandos. Tenga en cuenta que las últimas comillas dobles cierran toda la línea de comandos.</p> <p>Es necesaria la opción <code>/v"opciones_de_línea_de_comandos"</code> para ejecutar una instalación silenciosa.</p>

Puede controlar el aviso de una instalación silenciosa al enviar las opciones de la línea de comandos y los valores de la propiedad MSI para el instalador MSI, `msiexec.exe`. El instalador MSI incluye el código de instalación del componente de Horizon 7. El instalador usa los valores y las opciones que introduzca en la línea de comandos para interpretar las opciones de configuración y las especificaciones de instalación que se aplican al componente de Horizon 7.

Tabla 7-8. Opciones de la línea de comandos y de las propiedades MSI

Propiedad u opción MSI	Descripción
/qn	<p>Envía instrucciones al instalador MSI para que no muestre las páginas del asistente de instalación. Por ejemplo, es posible que quiera instalar Horizon Agent de forma silenciosa y usar únicamente funciones y opciones de configuración predeterminadas:</p> <pre>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn"</pre> <p>También puede usar la opción /qb para visualizar un cuadro de diálogo de progreso básico durante una instalación no interactiva y automatizada.</p> <p>Son necesarias las opciones /qn o /qb para ejecutar una instalación silenciosa.</p> <p>Si desea obtener más información sobre los parámetros de /q adicionales, consulte el sitio web Centro de desarrollo de Windows.</p>
INSTALLDIR	<p>Especifica una ruta de instalación alternativa para el componente de Horizon 7.</p> <p>Use el formato <i>INSTALLDIR=path</i> para especificar una ruta de instalación. Puede ignorar esta propiedad MSI si desea instalar el componente de Horizon 7 en la ruta predeterminada.</p> <p>La propiedad MSI es opcional.</p>

Tabla 7-8. Opciones de la línea de comandos y de las propiedades MSI (continuación)

Propiedad u opción MSI	Descripción
ADDLOCAL	<p>Determina las opciones específicas del componente que se instalarán.</p> <p>En una instalación interactiva, el instalador de Horizon 7 muestra opciones de configuración personalizadas que puede seleccionar o desmarcar. En una instalación silenciosa, puede usar la propiedad ADDLOCAL para instalar de forma selectiva opciones de configuración individuales especificando las opciones en la línea de comandos. No se instalan las opciones que no especifique.</p> <p>Tanto en las instalaciones interactivas como en las silenciosas, el instalador de Horizon 7 instala automáticamente algunas funciones. No puede usar ADDLOCAL para controlar si desea instalar o no estas funciones que no son opcionales.</p> <p>Introduzca ADDLOCAL=ALL para instalar todas las opciones de configuración personalizadas que se puedan instalar durante una instalación interactiva, incluidas las que se instalan de forma predeterminada y las que debe seleccionar para que se instalen, excepto NGVC. NGVC y SVIAGent son mutuamente exclusivas.</p> <p>En el siguiente ejemplo, se instalan Core, BlastProtocol, PColP, UnityTouch, VmVideo, PSG y todas las funciones compatibles con el sistema operativo invitado: VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</p> <p>Si no usa la propiedad ADDLOCAL, se instalan tanto las opciones de configuración personalizadas que lo hacen de forma predeterminada como las funciones que lo hacen automáticamente. No se instalan las opciones de configuración personalizadas que no están seleccionadas de forma predeterminada.</p> <p>En el siguiente ejemplo, se instalan Core, BlastProtocol, PColP, UnityTouch, VmVideo, PSG y las opciones de configuración personalizadas activadas de forma predeterminada compatibles en el sistema operativo invitado: VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>Para especificar opciones individuales, escriba una lista separada por comas de los nombres de opciones de configuración. No use espacios entre los nombres. Use el formato ADDLOCAL=valor,valor,valor....</p> <p>Puede incluir Core cuando use la propiedad ADDLOCAL=valor,valor,valor....</p> <p>El siguiente ejemplo instala Horizon Agent con las funciones Core, BlastProtocol, PColP, UnityTouch, VmVideo, PSG, Instant Clone Agent y Virtual Printing:</p> <p>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"</p> <p>El ejemplo anterior no instala otros componentes, ni siquiera los que están instalados interactivamente de forma predeterminada.</p> <p>La propiedad MSI ADDLOCAL es opcional.</p>
REBOOT	<p>Puede usar la opción REBOOT=ReallySuppress para permitir que se completen las tareas de configuración del sistema antes de que este se reinicie.</p> <p>La propiedad MSI es opcional.</p>
/l*v archivo_de_registro	<p>Escribe la información de registro en el archivo de registro especificado con una salida detallada.</p> <p>Por ejemplo: /l*v ""%TEMP%\vmmsi.log""</p> <p>Este ejemplo genera un archivo de registro detallado que es similar al que se genera durante una instalación interactiva.</p> <p>Puede usar esta opción para registrar funciones personalizadas que únicamente se puedan aplicar a su instalación. Es posible utilizar la información guardada para especificar funciones de instalación en futuras instalaciones silenciosas.</p> <p>La opción /l*v es opcional.</p>

Desinstalar los componentes de Horizon 7 de forma silenciosa con las opciones de la línea de comandos MSI

Puede desinstalar los componentes de Horizon 7 mediante las opciones de la línea de comandos de Microsoft Windows Installer (MSI).

Sintaxis

```
msiexec.exe  
/qb  
/x  
código_producto
```

Opciones

La opción `/qb` muestra la barra de progreso de desinstalación. Para que deje de aparecer la barra de progreso de desinstalación, reemplace la opción `/qb` por la opción `/qn`.

La opción `/x` desinstala el componente de Horizon 7.

La cadena *código_producto* identifica los archivos de producto de los componentes de Horizon 7 en el desinstalador MSI. Puede encontrar la cadena *código_producto* si busca ProductCode en el archivo `%TEMP%\vmmsi.log` que se creó durante la instalación. Para encontrar la cadena *código_producto* que se aplica a versiones anteriores de los componentes de Horizon 7, consulte el artículo de la base de conocimientos (KB) de VMware, disponible en <http://kb.vmware.com/kb/2064845>.

Para obtener más información sobre la línea de comandos MSI, consulte [Opciones de la línea de comandos de Microsoft Windows Installer](#).

Ejemplo de desinstalación de Horizon Agent

Para desinstalar Horizon Agent versión 7.0.2 de 32 bits, introduzca el siguiente comando:

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

Para desinstalar Horizon Agent versión 7.0.2 de 64 bits, introduzca el siguiente comando:

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

Agregue un registro detallado al comando.

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

Si no aplica de forma explícita la opción `/l`, el archivo de registro detallado predeterminado se encuentra en `%TEMP%\MSI\nnnn.log`, donde *nnnn* es un GUID de cuatro caracteres.

El proceso de desinstalación de Horizon Agent mantiene algunas claves de registro. Estas claves son necesarias para conservar la información de configuración del servidor de conexión que habilita que el escritorio remoto siga emparejándose con el servidor de conexión, aunque el agente se desinstale y se vuelva a instalar. Al eliminar estas claves de registro, se interrumpe ese emparejamiento.

Se mantienen las siguientes claves de registro:

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs
- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

Configurar los certificados TLS de los servidores de Horizon 7

8

VMware recomienda que configure los certificados TLS para la autenticación de las instancias del servidor de conexión, los servidores de seguridad y las instancias del servicio de View Composer.

Se genera un certificado predeterminado del servidor TLS cuando instala las instancias del servidor de conexión, de View Composer o los servidores de seguridad. El certificado predeterminado se puede usar para hacer pruebas.

Los certificados usados para la comunicación entre los servidores de conexión y también entre los Horizon Agent y las instancias del servidor de conexión se reemplazan con un mecanismo automático y no se pueden sustituir manualmente. Para obtener más información, consulte el documento *Seguridad de Horizon 7*.

Importante Reemplace el certificado predeterminado lo antes posible. El certificado predeterminado no está firmado por una entidad de certificación (CA). El uso de certificados que no están firmados por una CA puede permitir que partes que no son de confianza intercepten el tráfico al simular ser su servidor.

Este capítulo incluye los siguientes temas:

- [Comprender los certificados TLS para Horizon 7 Server](#)
- [Información general de las tareas para configurar certificados TLS](#)
- [Obtener un certificado TLS firmado de una CA](#)
- [Configurar el servidor de conexión de Horizon, el servidor de seguridad o View Composer para usar un nuevo certificado TLS](#)
- [Configurar endpoints cliente para confiar en el certificado raíz y los intermedios](#)
- [Configurar la comprobación de la revocación de los certificados del servidor](#)
- [Configurar la puerta de enlace segura de PCoIP para usar un nuevo certificado TLS](#)
- [Configurar Horizon Administrator para que confíe en un certificado de View Composer o de vCenter Server](#)
- [Beneficios de usar certificados TLS firmados por una CA](#)
- [Solucionar problemas de los certificados en el servidor de conexión de Horizon y el servidor de seguridad](#)

Comprender los certificados TLS para Horizon 7 Server

Debe seguir algunas directrices para configurar los certificados TLS para Horizon 7 Server y los componentes relacionados.

Servidor de seguridad y servidor de conexión de Horizon

El certificado TLS es necesario para establecer conexiones cliente a un servidor. Las instancias del servidor de conexión para el cliente, los servidores de seguridad y los servidores intermedios que finalizan las conexiones TLS requieren certificados de servidor TLS.

De forma predeterminada, cuando instala el servidor de conexión o el servidor de seguridad, la instalación genera un certificado autofirmado para el servidor. Sin embargo, la instalación usa un certificado existente en los siguientes casos:

- Si ya existe un certificado válido con un nombre descriptivo vdm en el almacén de certificados de Windows.
- Si actualiza a Horizon 7 desde una versión anterior y un archivo válido de almacén de claves está configurado en el equipo Windows Server, la instalación extrae las claves y los certificados, y los importa al almacén de certificados de Windows.

vCenter Server y View Composer

Antes de agregar vCenter Server y View Composer a Horizon 7 en un entorno de producción, asegúrese que vCenter Server y View Composer usen certificados firmados por una CA.

Para obtener más información sobre cómo reemplazar el certificado predeterminado para vCenter Server, consulte cómo realizar esta acción en el sitio web de documentación técnica de VMware, disponible en <http://www.vmware.com/resources/techresources/>.

Si instala vCenter Server y View Composer en el mismo host de Windows Server, pueden usar el mismo certificado TLS, pero debe configurar el certificado de forma independiente para cada componente.

Puerta de enlace segura de PCoIP

Para cumplir las normas de seguridad de la jurisdicción o la industria, puede reemplazar el certificado TLS predeterminado que generó el servicio de la puerta de enlace segura de PCoIP (PSG) con un certificado firmado por una CA. Se recomienda configurar el servicio PSG para usar un certificado firmado por una CA, sobre todo en implementaciones que le obligan a usar exámenes de seguridad para realizar una prueba de cumplimiento. Consulte [Configurar la puerta de enlace segura de PCoIP para usar un nuevo certificado TLS](#).

Puerta de enlace segura de Blast

De forma predeterminada, la puerta de enlace segura de Blast (BSG) usa el certificado TLS que está configurado para la instancia del servidor de conexión o el servidor de seguridad en el que la BSG se está ejecutando. Si reemplaza el certificado autofirmado predeterminado por un servidor con un certificado firmado por una CA, la BSG también usa este certificado.

Autenticador SAML 2.0

VMware Identity Manager usa autenticadores SAML 2.0 para proporcionar una autenticación basada en web y una autorización a través de dominios de seguridad. Si desea que Horizon 7 delegue la autenticación en VMware Identity Manager, puede configurar Horizon 7 para aceptar sesiones autenticadas de SAML 2.0 desde VMware Identity Manager. Cuando VMware Identity Manager esté configurado para admitir Horizon 7, los usuarios de VMware Identity Manager pueden conectarse a los escritorios remotos si seleccionan los iconos de escritorio que se encuentran en el portal de usuarios de Horizon.

En Horizon Administrator puede configurar autenticadores SAML 2.0 para usarlos con las instancias del servidor de conexión.

Antes de agregar un autenticador SAML 2.0 en Horizon Administrator, asegúrese de que el autenticador SAML 2.0 utilice un certificado firmado por una CA.

Directrices adicionales

Para obtener información general sobre la solicitud y el uso de certificados TLS que estén firmados por una CA, consulte [Beneficios de usar certificados TLS firmados por una CA](#).

Cuando los endpoints cliente se conecten a una instancia del servidor de conexión o a un servidor de seguridad, se presentan con el certificado de servidor TLS con los que cuenta el servidor y todos los certificados intermedios de la cadena de confianza. Para confiar en el certificado del servidor, los sistemas cliente deben tener instalado el certificado raíz de la CA que lo firma.

Cuando el servidor de conexión se comunica con vCenter Server y View Composer, el servidor de conexión se presenta con los certificados de servidor TLS y los certificados intermedios de esos servidores. Para confiar en los servidores de View Composer y en vCenter Server, el equipo del servidor de conexión debe tener instalado el certificado raíz de la CA que lo firma.

De forma similar, si un autenticador SAML 2.0 está configurado para el servidor de conexión, el equipo de este servidor debe tener instalado el certificado raíz de la CA que firma el certificado del servidor SAML 2.0.

Información general de las tareas para configurar certificados TLS

Si desea configurar certificados de servidor TLS para servidores de Horizon 7, debe realizar varias tareas generales.

En un pod de instancias replicadas del servidor de conexión, debe realizar estas tareas en todas las instancias del pod.

En los temas siguientes se describen los procedimientos para realizar estas tareas.

- 1 Determine si debe obtener un nuevo certificado TLS firmado de una CA.

Si su organización ya tiene un certificado de servidor TLS válido, puede utilizarlo para sustituir el certificado predeterminado que se proporciona con el servidor de conexión, el servidor de seguridad o View Composer. Si desea utilizar un certificado existente, también necesita su clave privada.

Punto de partida	Acción
Su organización le proporcionó un certificado de servidor TLS válido.	Vaya directamente al paso 2.
No tiene un certificado de servidor TLS.	Obtenga un certificado de servidor TLS firmado de una CA.

- 2 Importe el certificado TLS al almacén de certificados del equipo local Windows en el host del servidor de Horizon 7.

- 3 Si se trata de instancias del servidor de conexión y servidores de seguridad, cambie el Nombre descriptivo del certificado a **vdm**.

Asigne el Nombre descriptivo **vdm** solo a un certificado de cada host del servidor de Horizon 7.

- 4 Si el host de Windows Server no confía en el certificado raíz de un equipo del servidor de conexión, impórtelo al almacén de certificados del equipo local Windows.

Además, si las instancias del servidor de conexión no confían en los certificados raíz de los certificados del servidor TLS configurados para los hosts del servidor de seguridad, de vCenter Server y de View Composer, también debe importar dichos certificados raíz. Siga estos pasos solo para las instancias del servidor de conexión. No es necesario que importe el certificado raíz a los hosts del servidor de seguridad, de vCenter Server o de View Composer.

- 5 Si el certificado del servidor lo firmó una CA intermedia, importe los certificados intermedios al almacén de certificados del equipo local Windows.

Para simplificar la configuración cliente, importe la cadena de certificados completa al almacén de certificados del equipo local Windows. Si en el servidor de Horizon 7 no hay certificados intermedios, deben estar configurados para clientes y equipos que inicien Horizon Administrator.

- 6 Para las instancias de View Composer, siga uno de estos pasos:

- Si importa el certificado al almacén de certificados del equipo local Windows antes de instalar View Composer, puede seleccionar su certificado durante la instalación de View Composer.
- Si piensa reemplazar un certificado existente o el certificado autofirmado predeterminado por uno nuevo después de instalar View Composer, ejecute la utilidad `SviConfig ReplaceCertificate` para enlazar el nuevo certificado al puerto que View Composer utiliza.

- 7 Si su CA no es muy conocida, configure los clientes para que confíen en los certificados raíz e intermedios.

Asegúrese también de que los equipos en los que inicia Horizon Administrator confíen en los certificados raíz e intermedios.

- 8 Determine si desea volver a configurar la comprobación de revocación de certificados.

El servidor de conexión lleva a cabo la comprobación de revocación de certificados en los servidores de Horizon 7, View Composer y vCenter Server. La mayoría de los certificados firmados por una CA incluyen información de revocación de certificados. Si su CA no incluye esta información, puede configurar el servidor para que no compruebe la revocación de certificados.

Si el autenticador SAML está configurado para que se utilice con una instancia del servidor de conexión, dicho servidor también realiza la comprobación de la revocación del certificado en el certificado del servidor SAML.

Obtener un certificado TLS firmado de una CA

Si su organización no le proporciona un certificado de servidor TLS, debe solicitar un nuevo certificado firmado por una CA.

Hay varios métodos para obtener un nuevo certificado firmado. Por ejemplo, puede usar la utilidad `certreq` de Microsoft para generar una solicitud de firma de certificado (CSR) y enviarla a una CA.

Consulte el documento *Escenarios para configurar certificados TLS para Horizon 7* para ver un ejemplo sobre cómo utilizar `certreq` para realizar esta tarea.

Si desea realizar pruebas, puede obtener un certificado temporal gratuito basado en una raíz que no sea de confianza de muchas CA.

Importante Cuando obtenga certificados TLS firmados de una CA, debe seguir determinadas reglas y directrices.

- Al generar una solicitud de firma de certificado (CSR) en un equipo, compruebe que se genera también una clave privada. Cuando obtenga el certificado de servidor TLS y lo importe al almacén de certificados del equipo local de Windows, debe acompañarlo de una clave privada que se corresponda con el certificado.
 - Para cumplir las recomendaciones de seguridad de VMware, use el nombre de dominio plenamente cualificado (FQDN) que utilizan los dispositivos cliente para conectarse al host. No utilice un simple nombre de servidor o dirección IP, ni siquiera para comunicaciones dentro de su dominio interno.
 - No cree certificados para servidores que utilicen una plantilla de certificado compatible únicamente con una CA empresarial de Windows Server 2008 o versiones posteriores.
 - No genere certificados para servidores con un valor de longitud de clave `KeyLength` inferior a 1024. Los endpoints cliente no validarán certificados de un servidor generado con un valor `KeyLength` inferior a 1024 y los clientes no podrán conectarse al servidor. El servidor de conexión tampoco validará los certificados, por lo que los servidores afectados se mostrarán en rojo en el panel de control de Horizon Administrator.
-

Para obtener información general sobre cómo obtener certificados, consulte la ayuda en línea de Microsoft disponible con el complemento Certificado de MMC. Si aún no lo tiene instalado en su equipo, consulte [Agregar el complemento Certificado a MMC](#).

Obtener un certificado firmado por una CA empresarial o de dominio de Windows

Para obtener un certificado firmado por una CA empresarial o de dominio de Windows, debe utilizar el asistente Inscripción de certificados de Windows del almacén de certificados de Windows.

Este método de solicitud de certificados resulta apropiado si las comunicaciones entre equipos se producen dentro de su dominio interno. Por ejemplo, podría ser útil obtener un certificado firmado de una CA de dominio de Windows en el caso de las comunicaciones de servidor a servidor.

Si sus clientes se conectan a los servidores de Horizon 7 desde una red externa, solicite certificados de servidor TLS firmados por una CA externa de confianza.

Requisitos previos

- Determine el nombre de dominio plenamente cualificado (FQDN) que utilizan los dispositivos cliente para conectarse al host.

Para cumplir las recomendaciones de seguridad de VMware, utilice el FQDN en lugar de una dirección IP o un nombre de servidor simple, ni siquiera para comunicaciones dentro de su dominio interno.

- Verifique que el complemento Certificado se agregó a MMC. Consulte [Agregar el complemento Certificado a MMC](#).
- Compruebe que disponga de las credenciales adecuadas para solicitar un certificado que se puede emitir para un equipo o servicio.

Procedimiento

- 1 En la ventana **MMC** del host de Windows Server, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal**.
- 2 En el menú **Acción**, acceda a **Todas las tareas > Solicitar un nuevo certificado** para mostrar el asistente **Inscripción de certificados**.
- 3 Seleccione una directiva de inscripción de certificados.
- 4 Elija los tipos de certificados que quiere solicitar, seleccione la opción **Hacer exportable la clave privada** y haga clic en **Inscribir**.
- 5 Haga clic en **Finalizar**.

Resultados

El nuevo certificado firmado se agregará a la carpeta **Personal > Certificados** del almacén de certificados de Windows.

Pasos siguientes

- Compruebe que el certificado del servidor y la cadena de certificados se importaron al almacén de certificados de Windows.

- Si se trata de una instancia del servidor de conexión o un servidor de seguridad, cambie el nombre descriptivo del certificado a **vdm**. Consulte [Modificar el Nombre descriptivo del certificado](#).
- En el caso de los servidores de View Composer, enlace el nuevo certificado al puerto que utiliza View Composer. Consulte [Enlazar un nuevo certificado TLS al puerto usado por View Composer](#).

Configurar el servidor de conexión de Horizon, el servidor de seguridad o View Composer para usar un nuevo certificado TLS

Para configurar una instancia del servidor de conexión, de View Composer o del servidor de seguridad para que usen un certificado TLS, debe importar el certificado del servidor y toda la cadena de certificados en el almacén del certificado del equipo local Windows en el host de View Composer, del servidor de seguridad o del servidor de conexión.

En un pod de instancias replicadas del servidor de conexión, debe importar el certificado del servidor y la cadena de certificados en todas las instancias del pod.

De forma predeterminada, la puerta de enlace segura de Blast (BSG) usa el certificado TLS que está configurado para la instancia del servidor de conexión o el servidor de seguridad en el que la BSG se está ejecutando. Si reemplaza el certificado autofirmado predeterminado por View Server con un certificado firmado por una CA, la BSG también usa este certificado.

Importante Si desea configurar el servidor de seguridad o el servidor de conexión para que use un certificado, debe cambiar el Nombre descriptivo del certificado a **vdm**. Además, el certificado debe tener una clave privada.

Si piensa reemplazar un certificado existente o el certificado autofirmado y predeterminado por uno nuevo después de instalar View Composer, debe ejecutar la utilidad SviConfig ReplaceCertificate para enlazar el nuevo certificado al puerto que usa View Composer.

Procedimiento

1 [Agregar el complemento Certificado a MMC](#)

Antes de poder agregar certificados al almacén de certificados de Windows, debe agregar el complemento Certificado a la consola Microsoft Management Console (MMC) en el host de Windows Server en el que está instalado el servidor de Horizon 7.

2 [Importar un certificado del servidor SSL a un almacén de certificados de Windows](#)

Debe importar el certificado del servidor TLS al almacén de certificados del equipo local Windows en el host de Windows Server en el que están instalados la instancia del servidor de conexión o el servicio del servidor de seguridad.

3 [Modificar el Nombre descriptivo del certificado](#)

Si desea configurar un servidor de seguridad o un servidor de conexión para que reconozca y use un certificado TLS, debe cambiar el Nombre descriptivo del certificado a **vdm**.

4 Importar un certificado raíz e intermedios al almacén de certificados de Windows

Si el host de Windows Server en el que está instalado el servidor de conexión no confía en el certificado raíz del servidor TLS firmado, debe importar el certificado raíz al almacén de certificados del equipo local Windows. Además, si el host del servidor de conexión no confía en los certificados raíz de los certificados del servidor TLS configurados para los hosts del servidor de seguridad, de vCenter Server y de View Composer, también debe importar esos certificados raíz.

5 Enlazar un nuevo certificado TLS al puerto usado por View Composer

Si configura un nuevo certificado TLS después de instalar View Composer, debe ejecutar la utilidad `SviConfig ReplaceCertificate` para reemplazar el certificado que está enlazado al puerto usado por View Composer. Esta utilidad anula el enlace del certificado existente y enlaza el nuevo certificado al puerto.

Agregar el complemento Certificado a MMC

Antes de poder agregar certificados al almacén de certificados de Windows, debe agregar el complemento Certificado a la consola Microsoft Management Console (MMC) en el host de Windows Server en el que está instalado el servidor de Horizon 7.

Requisitos previos

Verifique que la consola MMC y el complemento Certificado estén disponibles en el equipo Windows Server en el que está instalado el servidor de Horizon 7.

Procedimiento

- 1 En el equipo Windows Server, haga clic en **Inicio** y escriba `mmc.exe`.
- 2 En la ventana **MMC**, diríjase a **Archivo > Agregar o quitar complemento**.
- 3 En la ventana **Agregar o quitar complementos**, seleccione **Certificados** y haga clic en **Agregar**.
- 4 En la ventana **Complemento Certificados**, seleccione **Cuenta de equipo**, haga clic en **Siguiente**, seleccione **Equipo local** y, a continuación, haga clic en **Finalizar**.
- 5 En la ventana **Agregar o quitar complementos**, haga clic en **Aceptar**.

Pasos siguientes

Importe el certificado de servidor TLS al almacén de certificados de Windows.

Importar un certificado del servidor SSL a un almacén de certificados de Windows

Debe importar el certificado del servidor TLS al almacén de certificados del equipo local Windows en el host de Windows Server en el que están instalados la instancia del servidor de conexión o el servicio del servidor de seguridad.

También debe realizar esta tarea en el host de Windows Server donde el servicio de View Composer está instalado.

Según el formato del archivo de certificado, toda la cadena de certificados que se encuentra en el archivo del almacén de claves se podría importar al almacén de certificados del equipo local Windows. Por ejemplo, se podrían importar el certificado del servidor, el certificado intermedio y el certificado raíz.

Para otros tipos de archivos de certificado, solo se importa el certificado del servidor al almacén de certificados del equipo local Windows. En este caso, debe realizar pasos independientes para importar el certificado raíz y los certificados intermedios a la cadena de certificados.

Para obtener más información sobre los certificados, consulte la ayuda en línea de Microsoft disponible con el complemento Certificado de MMC.

Nota Si descarga conexiones TLS en un servidor intermedio, debe importar el mismo certificado del servidor TLS al servidor intermedio y al servidor de Horizon 7 descargado. Para obtener más información, consulte "Descargar conexiones TLS a servidores intermedios" en el documento *Administración de Horizon 7*.

Requisitos previos

Verifique que el complemento Certificado se agregó a MMC. Consulte [Agregar el complemento Certificado a MMC](#).

Procedimiento

- 1 En la ventana MMC del host de Windows Server, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal**.
- 2 En el panel Acciones, diríjase a **Más acciones > Todas las tareas > Importar**.
- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenado el certificado.
- 4 Seleccione el archivo del certificado y haga clic en **Abrir**.

Para visualizar el tipo de archivo del certificado, puede seleccionar su formato en el menú desplegable **Nombre de archivo**.

- 5 Escriba la contraseña de la clave privada que se incluye en el archivo del certificado.
- 6 Seleccione **Marcar esta clave como exportable**.
- 7 Seleccione **Incluir todas las propiedades extendidas**.

- 8 Haga clic en **Siguiente** y en **Finalizar**.

El nuevo certificado aparece en la carpeta **Certificados (equipo local) > Personal > Certificados**.

- 9 Verifique que el nuevo certificado contiene una clave privada.
 - a En la carpeta **Certificados (equipo local) > Personal > Certificados**, haga doble clic en el nuevo certificado.
 - b En la pestaña General del cuadro de diálogo Información del certificado, verifique que aparece la siguiente afirmación: Tiene una clave privada correspondiente a este certificado.

Pasos siguientes

Cambie el Nombre descriptivo a **vdm**.

Modificar el Nombre descriptivo del certificado

Si desea configurar un servidor de seguridad o un servidor de conexión para que reconozca y use un certificado TLS, debe cambiar el Nombre descriptivo del certificado a **vdm**.

No tiene que modificar el Nombre descriptivo de los certificados TLS que utiliza View Composer.

Requisitos previos

Verifique que el certificado del servidor se importó a la carpeta **Certificados (equipo local) > Personal > Certificados** del almacén de certificados de Windows. Consulte [Importar un certificado del servidor SSL a un almacén de certificados de Windows](#).

Procedimiento

- 1 En la ventana MMC del host de Windows Server, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal > Certificados**.
- 2 Haga clic con el botón secundario en el certificado aplicado al host del servidor de Horizon 7 y haga clic en **Propiedades**.
- 3 En la pestaña General, elimine el texto **Nombre descriptivo** y escriba **vdm**.
- 4 Haga clic en **Aplicar** y en **Aceptar**.
- 5 Verifique que ningún otro certificado del servidor de la carpeta **Personal > Certificados** tenga el Nombre descriptivo **vdm**.
 - a Busque cualquier otro certificado del servidor, haga clic en él con el botón secundario y seleccione **Propiedades**.
 - b Si su Nombre descriptivo es **vdm**, borre el nombre, haga clic en **Aplicar** y luego en **Aceptar**.

Pasos siguientes

Importe el certificado raíz y los certificados intermedios al almacén de certificados del equipo local Windows.

Una vez importados todos los certificados de la cadena, debe reiniciar el servicio del servidor de conexión o del servidor de seguridad para que se implementen los cambios.

Importar un certificado raíz e intermedios al almacén de certificados de Windows

Si el host de Windows Server en el que está instalado el servidor de conexión no confía en el certificado raíz del servidor TLS firmado, debe importar el certificado raíz al almacén de certificados del equipo local Windows. Además, si el host del servidor de conexión no confía en los certificados raíz de los certificados del servidor TLS configurados para los hosts del servidor de seguridad, de vCenter Server y de View Composer, también debe importar esos certificados raíz.

Si los certificados de vCenter Server, de View Composer, del servidor de seguridad y del servidor de conexión están firmados por una CA raíz que es conocida y en la que el host del servidor de conexión confía y no hay certificados intermedios en las cadenas de certificados, puede omitir esta tarea. Es probable que el host confíe en las entidades de certificación más usadas.

Debe importar los certificados raíz que no sean de confianza en todas las instancias del servidor de conexión replicadas en un pod.

Nota No es necesario que importe el certificado raíz en los hosts del servidor de seguridad, vCenter Server o View Composer.

Si un certificado del servidor está firmado por una CA intermedia, también debe importar cada certificado intermedio a la cadena de certificados. Para simplificar la configuración cliente, importe toda la cadena intermedia a los hosts de vCenter Server, View Composer y el servidor de seguridad, así como a los hosts del servidor de conexión. Si en el servidor de conexión o el servidor de seguridad no aparecen los certificados intermedios, deben estar configurados para clientes y equipos que inicien Horizon Administrator. Si en un host de vCenter Server o View Composer no aparecen los certificados intermedios, deben estar configurados para cada instancia del servidor de conexión.

Si ya verificó que toda la cadena de certificados se importó al almacén de certificados del equipo local Windows, puede omitir esta tarea.

Nota Si un autenticador SAML está configurado para que una instancia del servidor de conexión lo use, las mismas directrices se aplican al autenticador SAML 2.0. Si el host del servidor de conexión no confía en el certificado raíz configurado para una autenticación SAML o si una CA intermedia firma el certificado del servidor SAML, debe asegurarse de que la cadena de certificados se importe en el almacén de certificados del equipo local Windows.

Procedimiento

- 1 En la consola MMC del host de Windows Server, expanda el nodo **Certificados (equipo local)** y diríjase a la carpeta **Entidades de certificación raíz de confianza > Certificados**.
 - Si el certificado raíz está en esta carpeta y no existen certificados intermedios en la cadena de certificados, diríjase al paso 7.
 - Si el certificado raíz no se encuentra en esta carpeta, comience en el paso 2.
- 2 Haga clic con el botón secundario en la carpeta **Entidades de certificación raíz de confianza > Certificados** y, a continuación, en **Todas las tareas > Importar**.
- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenada el certificado CA raíz.
- 4 Seleccione el archivo del certificado CA raíz y haga clic en **Abrir**.
- 5 Haga clic en **Siguiente**, vuelva a hacer clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

- 6 Si el certificado del servidor lo firmó una CA intermedia, importe todos los certificados intermedios de la cadena de certificados al almacén de certificados del equipo local Windows.
 - a Diríjase a la carpeta **Certificados (equipo local) > Entidades de certificación intermedias > Certificados**.
 - b Repita del paso 3 al 6 para cada certificado intermedio que se deba importar.
- 7 Reinicie el servicio del servidor de conexión, del servidor de seguridad, de View Composer o de vCenter Server para que se apliquen los cambios.

Enlazar un nuevo certificado TLS al puerto usado por View Composer

Si configura un nuevo certificado TLS después de instalar View Composer, debe ejecutar la utilidad SviConfig ReplaceCertificate para reemplazar el certificado que está enlazado al puerto usado por View Composer. Esta utilidad anula el enlace del certificado existente y enlaza el nuevo certificado al puerto.

Si instala el nuevo certificado en el equipo Windows Server antes de instalar View Composer, no es necesario que ejecute la utilidad SviConfig ReplaceCertificate. Cuando ejecute el instalador de View Composer, puede seleccionar un certificado firmado por una CA en lugar del certificado autofirmado predeterminado. Durante la instalación, el certificado seleccionado se enlaza al puerto que usa View Composer.

Si pretende reemplazar un certificado existente o el certificado autofirmado predeterminado por un nuevo certificado, debe usar la utilidad SviConfig ReplaceCertificate.

Requisitos previos

Compruebe que el nuevo certificado se importó en el almacén de certificados del equipo local de Windows en el equipo Windows Server en el que View Composer esté instalado.

Procedimiento

- 1 Detenga el servicio de View Composer.
- 2 Abra una ventana de símbolo de sistema en el host de Windows Server donde View Composer se encuentra instalado.
- 3 Diríjase al archivo ejecutable SviConfig.
El archivo se encuentra con la aplicación View Composer. La ruta predeterminada es C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe.
- 4 Escriba el comando SviConfig ReplaceCertificate.

Por ejemplo:

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

donde `-delete` es un parámetro obligatorio que funciona en el certificado que se está reemplazando. Debe especificar `-delete=true` para eliminar el certificado antiguo del almacén de certificados del equipo local Windows, o bien `-delete=false` para mantener el certificado antiguo en el almacén de certificados de Windows.

La utilidad muestra una lista numerada de certificados TLS que están disponibles en el almacén de certificados del equipo local Windows.

- 5 Para seleccionar un certificado, escriba su número y pulse Intro.
- 6 Reinicie el servicio de View Composer para que se apliquen los cambios.

Ejemplo: SviConfig ReplaceCertificate

El siguiente ejemplo reemplaza el certificado que está enlazado al puerto de View Composer:

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

Configurar endpoints cliente para confiar en el certificado raíz y los intermedios

Si un certificado de un servidor de Horizon 7 está firmado por una CA en la que no confían los equipos cliente ni los equipos cliente que acceden a Horizon Administrator, puede configurar todos los sistemas cliente Windows en un dominio para confiar en el certificado raíz y en los intermedios. Para ello, debe agregar la clave pública del certificado raíz en la directiva de grupo Entidades de certificación raíz de confianza en Active Directory y agregar el certificado raíz en el almacén Enterprise NTAAuth.

Por ejemplo, es posible que deba realizar estos pasos si su organización usa un servicio de certificados interno.

No tiene que seguir estos pasos si el controlador de dominio de Windows actúa como la CA raíz o si una CA conocida firmó los certificados. Para las CA conocidas, los proveedores de los sistemas operativos preinstalan el certificado raíz en los sistemas cliente.

Si los certificados del servidor están firmados por una CA que no es muy conocida, debe agregar el certificado intermedio a la directiva de grupo Entidades de certificación intermedias en Active Directory.

Para los dispositivos cliente que usen otros sistemas operativos que no sean Windows, consulte las siguientes instrucciones para distribuir el certificado raíz y los intermedios que los usuarios pueden instalar:

- Para Horizon Client para Mac, consulte [Configurar Horizon Client para Mac para confiar en el certificado raíz y los intermedios](#).
- Para Horizon Client para iOS, consulte [Configurar Horizon Client para iOS para confiar en el certificado raíz y los intermedios](#).
- Para Horizon Client para Android, consulte la documentación en el sitio web de Google, como la *guía de usuario de Android 3.0*, por ejemplo.

- Para Horizon Client para Linux, consulte la documentación de Ubuntu.

Requisitos previos

Compruebe que el certificado del servidor se generó con un valor de KeyLength que sea 1024 o superior. Los endpoints cliente no validarán certificados de un servidor generado con un valor KeyLength inferior a 1024 y los clientes no podrán conectarse al servidor.

Procedimiento

- 1 En el servidor de Active Directory, use el comando `certutil` para publicar el certificado en el almacén Enterprise NTAAuth.

Por ejemplo: `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

- 2 En el servidor de Active Directory, diríjase al complemento Administración de directivas de grupo.

Versión de AD	Ruta de navegación
Windows 2003	<ol style="list-style-type: none"> a Seleccione Inicio > Todos los programas > Herramientas administrativas > Usuarios y equipos de Active Directory. b Haga clic con el botón secundario en el dominio y, a continuación, en Propiedades. c En la pestaña Directiva de grupo, haga clic en Abrir para abrir el complemento Administración de directivas de grupo. d Haga clic con el botón secundario en Directiva predeterminada de dominio y seleccione Editar.
Windows 2008	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.
Windows 2012 R2	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.
Windows 2016	<ol style="list-style-type: none"> a Seleccione Inicio > Herramientas administrativas > Administración de directivas de grupo. b Expanda el dominio, haga clic con el botón secundario en Directiva predeterminada de dominio y, a continuación, en Editar.

- 3 Expanda la sección **Configuración del equipo** y diríjase a **Configuración de Windows > Configuración de seguridad > Directivas de clave pública**.

4 Importe el certificado.

Opción	Descripción
Certificado raíz	<ol style="list-style-type: none"> Haga clic con el botón secundario en Entidades de certificación raíz de confianza y seleccione Importar. Siga las instrucciones del asistente para importar el certificado intermedio (por ejemplo, rootCA.cer) y haga clic en Aceptar.
Certificado intermedio	<ol style="list-style-type: none"> Haga clic con el botón secundario en Entidades de certificación intermedias y seleccione Importar. Siga las instrucciones del asistente para importar el certificado intermedio (por ejemplo, intermediateCA.cer) y haga clic en Aceptar.

5 Cierre la ventana **Directiva de grupo**.

Resultados

Todos los sistemas del dominio ya tienen la información del certificado en los almacenes del certificado raíz y de los intermedios que permiten que confíen en los certificados raíz e intermedios.

Configurar Horizon Client para Mac para confiar en el certificado raíz y los intermedios

Si un certificado de servidor está firmado por una CA que no es de confianza para los equipos que ejecutan Horizon Client para Mac, puede configurar estos equipos de forma que confíen en el certificado raíz y en los intermedios. Debe distribuir el certificado raíz y todos los certificados intermedios en la cadena de confianza de los equipos cliente.

Procedimiento

- 1 Distribuya el certificado raíz y los certificados intermedios en el equipo que ejecuta Horizon Client para Mac.
- 2 Abra el certificado raíz en el equipo Mac.

El certificado muestra el siguiente mensaje: ¿Desea que su ordenador confíe en los certificados firmados por *nombre de la CA* a partir de ahora?
- 3 Haga clic en **Confiar siempre**.
- 4 Introduzca la contraseña del usuario.
- 5 Repita del paso 2 al 4 para todos los certificados intermedios de la cadena de confianza.

Configurar Horizon Client para iOS para confiar en el certificado raíz y los intermedios

Si un certificado de servidor está firmado por una CA que no es de confianza para dispositivos iPad y iPhone que ejecutan Horizon Client para iOS, puede configurar el dispositivo para que confíe en el certificado raíz y en los intermedios. Debe distribuir el certificado raíz y todos los certificados intermedios en la cadena de confianza de los dispositivos.

Procedimiento

- 1 Envíe el certificado raíz y los intermedios como archivos adjuntos por correo electrónico al iPad.
- 2 Abra el archivo adjunto del certificado raíz y seleccione **Instalar**.

El certificado muestra el siguiente mensaje:

Perfil no verificable. La autenticidad de *Nombre de certificado* no se puede verificar. La instalación de este perfil cambiará la configuración de iPad. Certificado raíz. Al instalar el certificado *Nombre del certificado* se agregará a la lista de certificados en iPad.

- 3 Vuelva a seleccionar **Instalar**.
- 4 Repita los pasos 2 y 3 para todos los certificados intermedios de la cadena de confianza.

Configurar la comprobación de la revocación de los certificados del servidor

Cada instancia del servidor de conexión comprueba la revocación de certificados en su propio certificado y en los servidores de seguridad emparejados. Cada instancia comprueba también los certificados de los servidores de vCenter y View Composer cuando se conecta a ellos. De forma predeterminada, todos los certificados en la cadena se comprueban, excepto el certificado raíz. Sin embargo, puede cambiar este valor predeterminado.

Si el autenticador SAML 2.0 está configurado para que una instancia del servidor de conexión lo use, el servidor de conexión también realiza la comprobación de la revocación del certificado en el certificado del servidor SAML 2.0.

Horizon 7 admite varios medios de comprobación de revocación de certificados, como las listas de revocación de certificados (CRL) y el protocolo de estado de certificado en línea (OCSP). Una CRL es una lista de certificados revocados publicada por la autoridad de certificación que los emitió. OCSP es un protocolo de validación de certificados que se utiliza para obtener el estado de revocación de un certificado X.509.

Con las CRL, la lista de certificados revocados se descarga desde un punto de distribución de certificados (DP) que se suele especificar en el certificado. El servidor se dirige periódicamente a la URL de DP de CRL especificada en el certificado, descarga la lista y la revisa para determinar si se revocó el certificado del servidor. Con OCSP, el servidor envía una solicitud a un respondedor OCSP para determinar el estado de revocación del certificado.

Cuando obtiene un certificado de servidor desde una entidad de certificación (CA) de terceros, el certificado incluye uno o varios medios por el cual se puede determinar su estado de revocación, incluida, por ejemplo, una URL de DP de CRL o la URL de un respondedor OCSP. Si tiene su propia CA y genera un certificado pero no incluye la información de revocación en este certificado, se produce un error en la comprobación de la revocación del certificado. Un ejemplo de información de revocación para un certificado podría incluir, por ejemplo, una URL a un DP de una CRL basada en la Web de un servidor en el que aloja una CRL.

Si tiene su propia CA pero no incluye o no puede incluir la información de la revocación en el certificado, puede elegir no comprobar certificados para la revocación o comprobar únicamente ciertos certificados de una cadena. En el servidor, con el Editor del Registro de Windows, puede crear el valor de cadena (REG_SZ) **CertificateRevocationCheckType**, en HKLM\Software\VMware, Inc.\VMware VDM\Security y establecer este valor a uno de los siguientes valores de datos.

Valor	Descripción
1	No realiza la comprobación de revocación del certificado.
2	Comprueba únicamente el certificado del servidor. No comprueba ningún otro certificado de la cadena.
3	Comprueba todos los certificados de la cadena.
4	(Predeterminado) Comprueba todos los certificados, excepto el certificado raíz.

Si este valor de registro no está configurado o si el ya establecido no es válido (es decir, si el valor no es 1, 2, 3 o 4), todos los certificados se comprueban, excepto el certificado raíz. Establezca este valor de registro en cada servidor en el que pretende modificar la comprobación de la revocación. No es necesario reiniciar el sistema después de establecer este valor.

Nota Si su organización usa opciones de proxy para acceder a Internet, es posible que tenga que configurar los equipos del servidor de conexión de forma que usen las opciones de proxy para asegurar que esa comprobación de revocación del certificado se pueda realizar en los servidores de seguridad o las instancias del servidor de conexión que se usan para las conexiones cliente seguras. Si una instancia del servidor de conexión no puede acceder a Internet, se puede producir un error la comprobación de la revocación del certificado y la instancia del servidor de conexión o los servidores de seguridad emparejados pueden aparecer en rojo en el panel de control de Horizon Administrator. Para solucionar esta cuestión, consulte el apartado sobre cómo solucionar problemas relacionados con la comprobación de revocación de certificados de los servidores de seguridad en el documento *Administración de Horizon 7*.

Configurar la puerta de enlace segura de PColP para usar un nuevo certificado TLS

Para cumplir las normas de seguridad de la jurisdicción o la industria, puede reemplazar el certificado TLS predeterminado que generó el servicio de la puerta de enlace segura de PColP (PSG) con un certificado firmado por una CA.

En Horizon 7, el servicio de PSG crea un certificado TLS autofirmado y predeterminado cuando el servicio se inicia. El servicio de PSG presenta el certificado autofirmado a los clientes que ejecutan Horizon Client 2.0 (o Horizon Client 5.2 para Windows) o versiones posteriores que se conecten a la PSG.

La PSG también proporciona un certificado TLS heredado que se presenta a los clientes que ejecutan clientes antiguos o versiones anteriores que se conectan a la PSG.

Los certificados predeterminados proporcionan conexiones seguras desde el endpoint cliente a la PSG y no necesitan ningún tipo de configuración en Horizon Administrator. Sin embargo, se recomienda configurar el servicio PSG para usar un certificado firmado por una CA, particularmente en implementaciones que le obligan a usar exámenes de seguridad para realizar una prueba de cumplimiento.

Aunque no es obligatorio, es recomendable configurar los nuevos certificados TLS firmados por una CA en los servidores antes de reemplazar el certificado PSG predeterminado por uno firmado por una CA. El siguiente procedimiento asume que ya importó un certificado firmado por una CA en el almacén de certificados de Windows en el servidor en el que la PSG se está ejecutando.

Nota Si usa un examen de seguridad para realizar una prueba de cumplimiento, es posible que quiera comenzar configurando la PSG para que use el mismo certificado que el servidor y que examine el puerto de View antes del puerto de la PSG. Puede resolver los problemas de validación o de confianza que se produzcan durante el examen del puerto de View para asegurar que esos problemas no provoquen que la prueba del certificado y del puerto de la PSG no sea válida. A continuación, puede configurar un certificado único para la PSG y realizar otro examen.

Procedimiento

1 Verificar que el nombre del servidor coincida con el nombre del sujeto del certificado de la PSG

Cuando se instala una instancia del servidor de conexión o un servidor de seguridad, el instalador crea una opción de registro con un valor que contiene el FQDN del equipo. Debe verificar que este valor coincida con la parte de la URL del nombre del servidor que los escáneres de seguridad usan para alcanzar el puerto de la PSG. El nombre del servidor también debe coincidir con el nombre del sujeto o el nombre alternativo del sujeto (SAN) del certificado TLS que pretende utilizar para la PSG.

2 Configurar un certificado PSG en el almacén de certificados de Windows

Para reemplazar el certificado PSG por un certificado firmado por una CA, debe configurar el certificado y su clave privada en el almacén de certificados del equipo local Windows en el equipo del servidor de seguridad o del servidor de conexión en el que la PSG se está ejecutando.

3 Establecer el nombre descriptivo del certificado PSG en el Registro de Windows

La PSG identifica el certificado TLS que se debe usar con el nombre del servidor y el nombre descriptivo del certificado. Debe establecer el valor de Nombre descriptivo en el Registro de Windows del servidor de conexión o en el equipo del servidor de seguridad en el que se ejecuta la PSG.

4 (opcional) Forzar el uso de un certificado firmado por una CA para las conexiones al PSG

Puede garantizar que todas las conexiones cliente al PSG usen el certificado firmado por una CA en lugar del certificado heredado predeterminado. Este procedimiento no es necesario para configurar un certificado firmado por una CA para el PSG. Realice estos pasos solo si es necesario forzar el uso de un certificado firmado por una CA en la implementación de Horizon 7.

Verificar que el nombre del servidor coincida con el nombre del sujeto del certificado de la PSG

Cuando se instala una instancia del servidor de conexión o un servidor de seguridad, el instalador crea una opción de registro con un valor que contiene el FQDN del equipo. Debe verificar que este valor coincida con la parte de la URL del nombre del servidor que los escáneres de seguridad usan para alcanzar el puerto de la PSG. El nombre del servidor también debe coincidir con el nombre del sujeto o el nombre alternativo del sujeto (SAN) del certificado TLS que pretende utilizar para la PSG.

Por ejemplo, si un escáner se conecta a la PSG con la URL `https://view.customer.com:4172`, la opción del registro debe tener el valor `view.customer.com`. Tenga en cuenta que el FQDN del equipo del servidor de conexión o del servidor de seguridad que se configura durante la instalación puede que no sea el mismo que este nombre del servidor externo.

Procedimiento

- 1 Inicie el Editor del Registro de Windows en el servidor de conexión o en el host del servidor de seguridad donde se ejecuta la puerta de enlace segura PCoIP.
- 2 Diríjase a la opción del registro `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni`.
- 3 Compruebe que el valor de la opción `SSLCertPsgSni` coincida con el nombre del servidor de la URL que usarán los escáneres para conectarse a la PSG y que coincida con el nombre del sujeto o un nombre del sujeto alternativo del certificado TLS que pretende instalar para la PSG.

Si el valor no coincide, reemplácelo por el valor correcto.

- 4 Reinicie el servicio de la puerta de enlace segura PCoIP de VMware Horizon View para que se realicen los cambios.

Pasos siguientes

Importe el certificado firmado por la CA en el almacén de certificados del equipo local de Windows y configure el Nombre descriptivo del certificado.

Configurar un certificado PSG en el almacén de certificados de Windows

Para reemplazar el certificado PSG por un certificado firmado por una CA, debe configurar el certificado y su clave privada en el almacén de certificados del equipo local Windows en el equipo del servidor de seguridad o del servidor de conexión en el que la PSG se está ejecutando.

Si pretende que la PSG use un certificado único, debe importar el certificado al almacén de certificados del equipo local Windows con una clave privada exportable y establecer el nombre descriptivo apropiado.

Si pretende que la PSG use el mismo certificado que el servidor, no es necesario que siga este procedimiento. Sin embargo, en el Registro de Windows, debe configurar el nombre del servidor de forma que coincida con el nombre del sujeto y establezca el nombre descriptivo **vdm**.

Requisitos previos

- Compruebe que la longitud de la clave sea, al menos, de 1024 bits.
- Compruebe que el certificado TLS sea válido. La hora actual del equipo del servidor debe estar dentro de las fechas de inicio y finalización del certificado.
- Compruebe que el nombre del asunto del certificado o un nombre alternativo del asunto coincida con la opción SSLCertPsgSni en el Registro de Windows. Consulte [Verificar que el nombre del servidor coincida con el nombre del sujeto del certificado de la PSG](#).
- Verifique que el complemento Certificado se agregó a MMC. Consulte [Agregar el complemento Certificado a MMC](#).
- Familiarícese con el procedimiento de importación de un certificado en el almacén de certificados de Windows. Consulte [Importar un certificado del servidor SSL a un almacén de certificados de Windows](#).
- Familiarícese con el procedimiento de modificación del nombre descriptivo del certificado. Consulte [Modificar el Nombre descriptivo del certificado](#).

Procedimiento

- 1 En la ventana MMC del host de Windows Server, abra la carpeta **Certificados (equipo local) > Personal**.
- 2 Importe el certificado TLS que se expide para la PSG seleccionando **Más acciones > Todas las tareas > Importar**.

Seleccione las siguientes opciones en el asistente **Importación de certificado**:

- a **Marcar esta clave como exportable**
- b **Incluir todas las propiedades ampliables**

Complete el asistente para finalizar la importación del certificado en la carpeta **Personal**.

- 3 Verifique que el nuevo certificado contenga una clave privada siguiendo uno de estos pasos:
 - Compruebe que aparezca una clave amarilla en el icono del certificado.
 - Haga doble clic en el certificado y compruebe que aparezca la siguiente información en el cuadro de diálogo Información del certificado: Tiene una clave privada correspondiente a este certificado.
- 4 Haga clic con el botón secundario en el nuevo certificado y, a continuación, en **Propiedades**.
- 5 En la pestaña General, elimine el texto **Nombre descriptivo** y escriba el nombre descriptivo que seleccionó.
 Asegúrese de que introdujo exactamente el mismo nombre en la opción SSLCertWinCertFriendlyName en el Registro de Windows, como se describe en el siguiente procedimiento.
- 6 Haga clic en **Aplicar** y en **Aceptar**.

Resultados

La PSG presenta el certificado firmado por CA a los dispositivos cliente que se conectan al servidor a través de PCoIP.

Nota Este procedimiento no afecta a los dispositivos cliente heredados. La PSG sigue presentando el certificado heredado predeterminado a los dispositivos cliente heredados que se conectan al servidor a través de PCoIP.

Pasos siguientes

Configure el nombre descriptivo del certificado en el Registro de Windows.

Establecer el nombre descriptivo del certificado PSG en el Registro de Windows

La PSG identifica el certificado TLS que se debe usar con el nombre del servidor y el nombre descriptivo del certificado. Debe establecer el valor de Nombre descriptivo en el Registro de Windows del servidor de conexión o en el equipo del servidor de seguridad en el que se ejecuta la PSG.

Todas las instancias del servidor de conexión y los servidores de seguridad utilizan el nombre descriptivo del certificado **vdm**. Por el contrario, puede configurar su propio nombre descriptivo del certificado para el certificado PSG. Debe configurar una opción del Registro de Windows para habilitar la PSG de forma que el nombre correcto coincida con el nombre descriptivo que estableció en el almacén de certificados de Windows.

La PSG puede usar el mismo certificado TLS que el servidor en el que se está ejecutando. Si configura la PSG para usar el mismo certificado que el servidor, el nombre descriptivo debe ser **vdm**.

El valor del nombre descriptivo, tanto en el Registro de Windows como en el almacén de certificados, distingue entre mayúsculas y minúsculas.

Requisitos previos

- Compruebe que el Registro de Windows contenga el nombre del sujeto que se usa para alcanzar el puerto de la PSG y que coincida con el nombre del sujeto del certificado PSG o el nombre alternativo del sujeto. Consulte [Verificar que el nombre del servidor coincida con el nombre del sujeto del certificado de la PSG](#).
- Compruebe que el nombre descriptivo del certificado esté configurado en el almacén de certificados del equipo local Windows. Consulte [Configurar un certificado PSG en el almacén de certificados de Windows](#).

Procedimiento

- 1 Inicie el Editor del Registro de Windows en el servidor de conexión o en el equipo del servidor de seguridad donde se ejecuta la puerta de enlace segura PCoIP.
- 2 Diríjase a la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway.

- 3 Agregue un nuevo valor de cadena (REG_SZ), SSLCertWinCertFriendlyName, a esta clave de registro.
- 4 Modifique el valor SSLCertWinCertFriendlyName e introduzca el nombre descriptivo del certificado que debe usar la PSG.

Por ejemplo: **pcoip**

Si usa el mismo certificado que el servidor, el valor debe ser **vdm**.

- 5 Reinicie el servicio de la puerta de enlace segura PCoIP de VMware Horizon View para que se realicen los cambios.

Pasos siguientes

Compruebe que los dispositivos cliente sigan conectados a la PSG.

Si usa un examen de seguridad para realizar pruebas de cumplimiento, examine el puerto de la PSG.

Forzar el uso de un certificado firmado por una CA para las conexiones al PSG

Puede garantizar que todas las conexiones cliente al PSG usen el certificado firmado por una CA en lugar del certificado heredado predeterminado. Este procedimiento no es necesario para configurar un certificado firmado por una CA para el PSG. Realice estos pasos solo si es necesario forzar el uso de un certificado firmado por una CA en la implementación de Horizon 7.

En algunos casos, el PSG puede presentar el certificado heredado predeterminado en lugar del certificado firmado por una CA para un examen de seguridad, lo que hace que la prueba de conformidad en el puerto PSG no sea válida. Para resolver este problema, puede configurar el PSG para que no presente el certificado heredado predeterminado a ningún dispositivo que intente conectarse.

Importante Este procedimiento evita que todos los clientes heredados se conecten a este servidor a través de PCoIP.

Requisitos previos

Verifique que todos los dispositivos cliente que se conecten a este servidor, incluidos los clientes ligeros, ejecuten Horizon Client 5.2 para Windows o Horizon Client 2.0 o versiones posteriores. Debe actualizar los clientes heredados.

Procedimiento

- 1 Inicie el Editor del Registro de Windows en el servidor de conexión o en el equipo del servidor de seguridad donde se ejecuta la puerta de enlace segura PCoIP.
- 2 Diríjase a la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway.
- 3 Agregue un nuevo valor de cadena (REG_SZ), SSLCertPresentLegacyCertificate, a esta clave de registro.
- 4 Configure el valor de SSLCertPresentLegacyCertificate a **0**.

- 5 Reinicie el servicio de la puerta de enlace segura PCoIP de VMware Horizon View para que se realicen los cambios.

Configurar Horizon Administrator para que confíe en un certificado de View Composer o de vCenter Server

En el panel de control de Horizon Administrator, puede configurar Horizon 7 para que confíe en un certificado de View Composer o de vCenter Server que no sea de confianza.

VMware recomienda que configure vCenter Server y View Composer para que utilicen certificados TLS firmados por una CA. También puede aceptar la huella digital del certificado predeterminado en vCenter Server y View Composer.

Asimismo, VMware recomienda que configure los autenticadores SAML 2.0 para que utilicen certificados TLS firmados por una CA. De forma alternativa, en el panel de control de Horizon Administrator puede configurar Horizon 7 para que confíe en un certificado del servidor SAML 2.0 que no sea de confianza para aceptar la huella digital del certificado predeterminado.

Beneficios de usar certificados TLS firmados por una CA

Una entidad de certificación es una entidad de confianza que garantiza la identidad del certificado y de su creador. Cuando una entidad de certificación firma un certificado, los usuarios dejan de recibir mensajes en los que se les pide que comprueben el certificado y de esta forma, los dispositivos del cliente ligero pueden conectarse sin necesidad de configuración adicional.

Puede solicitar un certificado de servidor TLS que sea específico de un dominio web, como `www.mycorp.com`, o bien puede solicitar un certificado de servidor TLS comodín que se use a través de un dominio como `*.mycorp.com`. Para simplificar la administración, debe seleccionar solicitar un certificado comodín si necesita instalar el certificado en varios servidores o en diferentes subdominios.

Normalmente, los certificados específicos de dominio se usan en instalaciones seguras y las CA suelen garantizar más protección frente a pérdidas con los certificados específicos de dominio que con los certificados comodines. Si utiliza un certificado comodín compartido con otros servicios, la seguridad del producto Horizon 7 dependerá también de la seguridad de esos otros servicios. Si usa un certificado comodín, debe asegurarse de que la clave privada se pueda transferir entre servidores.

Cuando reemplace el certificado predeterminado por su propio certificado, los clientes usan su certificado para autenticar el servidor. Si el certificado está firmado por una CA, el propio certificado se incrusta en el navegador o se ubica en una base de datos de confianza a la que el cliente puede acceder. Después de que un cliente acepte el certificado, este responde enviando una clave secreta que está cifrada con la clave pública que contiene el certificado. La clave secreta se usa para cifrar el tráfico entre el cliente y el servidor.

Solucionar problemas de los certificados en el servidor de conexión de Horizon y el servidor de seguridad

Los problemas de los certificados en un servidor de Horizon 7 no le permiten conectarse a Horizon Administrator o hacen que se muestre un indicador de estado rojo en un servidor.

Problema

No puede conectarse a Horizon Administrator en la instancia del servidor de conexión que tiene el problema. Cuando se conecta a Horizon Administrator en otra instancia del servidor de conexión que se encuentra en el mismo pod, puede ver que el indicador de estado del panel de control de la instancia del servidor de conexión con el problema se encuentra en rojo.

En la otra instancia del servidor de conexión, haga clic en el indicador de estado rojo que muestra Certificado SSL: no válido y Estado: (vacío), indicando que no se encuentra un certificado válido. El archivo de registro Horizon 7 contiene una entrada del tipo ERROR con el siguiente mensaje: No existe ningún certificado aplicable en el almacén de claves.

La información de registro de Horizon 7 se encuentra en la ruta C:\ProgramData\VMware\VDM\Logs\log-*.txt de la instancia del servidor de conexión.

Causa

Es posible que un certificado no se instale correctamente en Horizon 7 Server por alguna de las siguientes razones:

- El certificado no está en la carpeta Personal en el almacén de certificados del equipo local Windows.
- El almacén de certificados no tiene ninguna clave privada del certificado.
- El nombre descriptivo del certificado no es **vdm**.
- El certificado se generó desde una plantilla de certificados v3 para Windows Server 2008 o un servidor posterior. Horizon 7 no puede detectar una clave privada, pero si usa el complemento Certificados para examinar el almacén de certificados de Windows, el almacén indica que existe una clave privada.

Solución

- ◆ Compruebe que el certificado no está importado en la carpeta Personal en el almacén de certificados del equipo local Windows.
Consulte [Importar un certificado del servidor SSL a un almacén de certificados de Windows](#).
- ◆ Compruebe que el certificado contenga una clave privada.
Consulte [Importar un certificado del servidor SSL a un almacén de certificados de Windows](#).
- ◆ Compruebe que el nombre descriptivo del certificado sea **vdm**.
Consulte [Modificar el Nombre descriptivo del certificado](#).

- ◆ Si el certificado se generó desde una plantilla de certificados v3, obtenga un certificado firmado y válido desde una CA que no use una plantilla v3.

Consulte [Obtener un certificado TLS firmado de una CA](#).

Configurar Horizon 7 por primera vez

9

Después de instalar el software de Horizon 7 Server y configurar los certificados SSL para los servidores, debe realizar algunos pasos adicionales para configurar un entorno de Horizon 7 de trabajo.

Configure las cuentas de usuario de vCenter Server y View Composer, instale una clave de licencia de Horizon 7, agregue vCenter Server y View Composer al entorno de Horizon 7, configure la puerta de enlace segura PCoIP y el túnel seguro y, de forma opcional, ajuste la configuración de Windows Server para que admita el entorno de Horizon 7.

Este capítulo incluye los siguientes temas:

- [Configurar cuentas de usuario para vCenter Server, View Composer y clones instantáneos](#)
- [Configurar el servidor de conexión de Horizon por primera vez](#)
- [Configurar conexiones de Horizon Client](#)
- [Reemplazar los puertos predeterminados para los servicios de Horizon 7](#)
- [Configuración de tamaño de Windows Server para admitir la implementación](#)

Configurar cuentas de usuario para vCenter Server, View Composer y clones instantáneos

Para usar vCenter Server con Horizon 7, debe configurar una cuenta de usuario con los privilegios vCenter Server apropiados. Puede crear una función de vCenter Server con los privilegios apropiados y asignar dicha función a la cuenta de usuario de vCenter Server.

Si instala View Composer en una máquina diferente a la que utilizó para instalar vCenter Server, debe crear una cuenta de usuario en Active Directory que Horizon 7 pueda utilizar para autenticar el servicio View Composer en una máquina independiente.

Si usa View Composer, debe crear una tercera cuenta de usuario en Active Directory que permita a View Composer realizar algunas operaciones en Active Directory. View Composer necesita que esta cuenta conecte las máquinas virtuales de clones vinculados con el dominio de Active Directory. Consulte [Crear una cuenta de usuario para operaciones en AD de View Composer](#).

Si usa clones instantáneos, debe crear una cuenta de usuario en Active Directory que permita al servidor de conexión realizar algunas operaciones en Active Directory. El servidor de conexión necesita que esta cuenta conecte las máquinas virtuales de clones instantáneos al dominio de Active Directory. Consulte [Crear una cuenta de usuario para operaciones de clones instantáneos](#).

En resumen, cuando configure Horizon 7 por primera vez, proporcione estas cuentas de usuario en Horizon Administrator:

- El usuario de vCenter Server permite a Horizon 7 y View Composer realizar operaciones en vCenter Server.
- El servidor de View Composer independiente permite a Horizon 7 autenticarse en el servicio de View Composer en un equipo independiente.

Si instala View Composer en la misma máquina que vCenter Server, el usuario de vCenter Server realiza las dos funciones anteriores y no utiliza un usuario del servidor de View Composer independiente.

- El usuario de View Composer para las operaciones de AD permite a View Composer realizar algunas operaciones en Active Directory.
- El usuario de clones instantáneos para las operaciones de AD permite al servidor de conexión realizar algunas operaciones en Active Directory.

Dónde utilizar el usuario de vCenter Server y los usuarios de View Composer

Después de crear y configurar estas cuentas de usuario, especifique los nombres en Horizon Administrator.

- Especifique un usuario de vCenter Server al agregar vCenter Server a Horizon 7.
- Especifique un usuario de un servidor independiente de View Composer al configurar las opciones de View Composer y seleccione **Servidor View Composer independiente**.
- Especifique un usuario de View Composer para las operaciones de AD cuando configure los dominios de View Composer.
- Especifique el usuario de View Composer para las operaciones de AD cuando cree los grupos de clonación vinculada.

Configurar un usuario de vCenter Server para Horizon 7 y View Composer

Para configurar una cuenta de usuario que permita a Horizon 7 realizar operaciones en vCenter Server, debe asignar una función de vCenter Server con los privilegios apropiados a dicho usuario.

La lista de privilegios que debe agregar en la función vCenter Server varía, dependiendo de si usa Horizon 7 con o sin View Composer. El servicio View Composer realiza operaciones en vCenter Server que necesitan privilegios además de los básicos.

Si instala View Composer en el mismo equipo que vCenter Server, debe hacer que el usuario de vCenter Server sea un administrador de sistema local en el equipo vCenter Server. Este requisito permite a Horizon 7 autenticarse en el servicio de View Composer.

Si instala View Composer en una máquina diferente a vCenter Server, no es necesario que el usuario de vCenter Server sea un administrador local en el equipo vCenter Server. Sin embargo, debe crear una cuenta independiente de usuario del servidor de View Composer que tenga la función de administrador local en el equipo View Composer.

Requisitos previos

- En Active Directory, cree un usuario en el dominio del servidor de conexión o en un dominio de confianza. Consulte [Crear una cuenta de usuario para vCenter Server](#).
- Familiarícese con los privilegios de vCenter Server que son obligatorios para la cuenta de usuario. Consulte [Privilegios necesarios para el usuario de vCenter Server](#).
- Si usa View Composer, familiarícese con los privilegios obligatorios adicionales. Consulte [Privilegios de clones instantáneos y View Composer necesarios para el usuario de vCenter Server](#).

Procedimiento

- 1 En vCenter Server, prepare una función con los privilegios obligatorios del usuario.
 - Puede usar la función Administrador predefinida en vCenter Server. Esta función puede realizar todas las operaciones en vCenter Server.
 - Si usa View Composer, puede crear una función limitada con los privilegios mínimos que View Composer y el servidor de conexión necesitan para realizar operaciones de vCenter Server.
 En vSphere Client, haga clic en **Inicio > Funciones > Agregar función**, introduzca un nombre de función como **Administrador de View Composer** y seleccione los privilegios de la función.
 Esta función debe tener todos los privilegios que el servidor de conexión y View Composer necesitan para funcionar en vCenter Server.
 - Si usa Horizon 7 sin View Composer, puede crear una función limitada con los privilegios mínimos que el servidor de conexión necesita para realizar operaciones de vCenter Server.
 En vSphere Client, haga clic en **Inicio > Funciones > Agregar función**, introduzca un nombre de función como **Administrador de View Manager** y seleccione los privilegios de la función.
 - Si usa clones instantáneos, puede crear una función limitada con los privilegios mínimos que el servidor de conexión necesita para realizar operaciones de vCenter Server.
 En vSphere Client, haga clic en **Inicio > Funciones > Agregar función**, introduzca un nombre de función como **Administrador de clones instantáneos de View Manager** y seleccione los privilegios de la función. Para más información sobre los privilegios de los clones instantáneos, consulte [Privilegios de clones instantáneos y View Composer necesarios para el usuario de vCenter Server](#).

- 2 En vSphere Client, haga clic con el botón secundario en el vCenter Server situado en el nivel superior del inventario y haga clic en **Agregar permiso** y agregue el usuario de vCenter Server.

Nota Debe definir el usuario del vCenter Server en el nivel de vCenter Server.

- 3 En el menú desplegable, seleccione la función Administrador, o bien la función de View Composer o View Manager que creó y asígnela al usuario de vCenter Server.
- 4 Si instala View Composer en el mismo equipo que vCenter Server, agregue la cuenta de usuario de vCenter Server como miembro del grupo Administradores del sistema local en el equipo vCenter Server.

Este paso no es necesario si instala View Composer en un equipo diferente al vCenter Server.

Pasos siguientes

En Horizon Administrator, cuando agrega vCenter Server a Horizon 7, especifique el usuario de vCenter Server. Consulte [Agregar instancias de vCenter Server a Horizon 7](#).

Privilegios necesarios para el usuario de vCenter Server

Los usuarios de vCenter Server deben tener suficientes privilegios de vCenter Server para habilitar Horizon 7 para realizar operaciones en vCenter Server. Cree una función View Manager para el usuario de vCenter Server con los privilegios necesarios.

Tabla 9-1. Privilegios necesarios para la función View Manager

Grupo de privilegios	Privilegios que se deben habilitar
Carpeta	Crear carpeta
	Eliminar carpeta
Almacén de datos	Asignar espacio

Tabla 9-1. Privilegios necesarios para la función View Manager (continuación)

Grupo de privilegios	Privilegios que se deben habilitar
Máquina virtual	<p>En Configuración:</p> <ul style="list-style-type: none"> ■ Agregar o eliminar dispositivo ■ Avanzado ■ Modificar la configuración del dispositivo <p>En Interacción:</p> <ul style="list-style-type: none"> ■ Apagar ■ Encender ■ Restablecer ■ Suspender ■ Realizar operaciones de reducción o borrado <p>En Inventario:</p> <ul style="list-style-type: none"> ■ Crear nuevo ■ Crear a partir de uno existente ■ Eliminar <p>En Aprovisionamiento:</p> <ul style="list-style-type: none"> ■ Personalizar ■ Implementar plantilla ■ Leer las especificaciones de personalización ■ Clonar plantilla ■ Clonar máquina virtual
Recurso	Asignar una máquina virtual a un grupo de recursos
Global	<p>Actuar como vCenter Server</p> <p>El usuario de vCenter Server necesita este privilegio aunque no utilice el acelerador de almacenamiento de View.</p>
Host	<p>El siguiente privilegio Host es necesario para implementar el acelerador de almacenamiento de View, que habilita el almacenamiento en caché del host ESXi. Si no utiliza el acelerador de almacenamiento de View, el usuario de vCenter Server no necesita este privilegio.</p> <p>En Configuración:</p> <ul style="list-style-type: none"> ■ Configuración avanzada
Almacenamiento controlado por los perfiles (si utiliza almacenes de datos vSAN o Virtual Volumes)	(todo)

Privilegios de clones instantáneos y View Composer necesarios para el usuario de vCenter Server

Para dar soporte a View Composer o clones instantáneos, el usuario de vCenter Server debe tener ciertos privilegios además de los necesarios para dar soporte a Horizon 7.

Privilegios de clones instantáneos y View Composer muestra el supraconjunto de privilegios necesarios para View Manager, View Composer y clones instantáneos.

Tabla 9-2. Privilegios de clones instantáneos y View Composer

Grupo de privilegios de vCenter Server	Privilegios que se deben habilitar
Carpeta	<p>Crear carpeta</p> <p>Eliminar carpeta</p>
Almacén de datos	<p>Asignar espacio</p> <p>Examinar almacén de datos</p> <p>Operaciones de archivos de nivel inferior</p>
Host	<p>En Inventario:</p> <ul style="list-style-type: none"> ■ Modificar clúster
Máquina virtual	<p>En Configuración (todos)</p> <p>En Interacción:</p> <ul style="list-style-type: none"> ■ Apagar ■ Encender ■ Restablecer ■ Suspender ■ Realizar operaciones de reducción o borrado ■ Conexión del dispositivo <p>En Inventario (todos)</p> <p>En Administración de snapshots (todo)</p> <p>En Aprovisionamiento:</p> <ul style="list-style-type: none"> ■ Personalizar ■ Implementar plantilla ■ Leer las especificaciones de personalización ■ Clonar plantilla ■ Clonar máquina virtual ■ Permitir acceso de disco
Recurso	<p>Asignar una máquina virtual a un grupo de recursos</p> <p>El siguiente privilegio es necesario si desea realizar operaciones para volver a equilibrar View Composer.</p> <p>Migrar las máquinas virtuales desconectadas</p>
Global	<p>Habilitar métodos</p> <p>Deshabilitar métodos</p> <p>Etiqueta del sistema</p> <p>Administrar atributos personalizados</p> <p>Configurar atributo personalizado</p> <p>El privilegio siguiente es necesario para implementar el acelerador de almacenamiento de View, que habilita el almacenamiento en caché del host ESXi. El usuario de vCenter Server necesita este privilegio aunque no utilice el acelerador de almacenamiento de View.</p> <p>Actuar como vCenter Server</p>
Red	(todo)
Almacenamiento realizado por el perfil	(todo, en caso de utilizar almacenes de datos vSAN o Virtual Volumes)

Tabla 9-2. Privilegios de clones instantáneos y View Composer (continuación)

Grupo de privilegios de vCenter Server	Privilegios que se deben habilitar
Vistas de almacenamiento	View
Operaciones criptográficas	<p>Los siguientes privilegios son necesarios si se utilizan clones instantáneos de máquinas virtuales con un dispositivo Trusted Platform Module (vTPM).</p> <ul style="list-style-type: none"> ■ Clonar ■ Descifrar ■ Acceso directo ■ Cifrar ■ Administrar KMS ■ Migrar ■ Registrar host

Configurar el servidor de conexión de Horizon por primera vez

Después de instalar el servidor de conexión, debe instalar una licencia de producto y agregar los servicios de vCenter Server y de View Composer a Horizon 7. También puede permitir que los hosts ESXi recuperen el espacio de disco de las máquinas virtuales y configurar estos hosts para almacenar en caché los datos de disco de la máquina virtual.

Si instala servidores de seguridad, estos se agregan a Horizon 7 y aparecen automáticamente en Horizon Administrator.

Horizon Administrator y el servidor de conexión de Horizon

Horizon Administrator proporciona una interfaz de administración basada en Web para Horizon 7.

El servidor de conexión de Horizon puede tener varias instancias que funcionan de servidores de réplica o servidores de seguridad. En función de la implementación de Horizon 7, puede obtener una interfaz de Horizon Administrator con cada instancia de un servidor de conexión.

Utilice las siguientes prácticas recomendadas para usar Horizon Administrator con un servidor de conexión:

- Use el nombre de host y la dirección IP del servidor de conexión para iniciar sesión en Horizon Administrator. Use la interfaz de Horizon Administrator para administrar el servidor de conexión, así como cualquier servidor de seguridad asociado o servidor de réplica.
- En un entorno de pod, compruebe que todos los administradores utilicen el nombre de host y la dirección IP del mismo servidor de conexión para iniciar sesión en Horizon Administrator. No utilice el nombre de host ni la dirección IP del equilibrador de carga para acceder a la página web de Horizon Administrator.

- Para identificar el nombre del clúster o el pod de la CPA del servidor de conexión con el que está trabajando, puede consultar el nombre en el encabezado Horizon Administrator y en la pestaña Navegador web.

Nota Si usa dispositivos de Unified Access Gateway en lugar de servidores de seguridad, debe usar la REST API de Unified Access Gateway para administrar los dispositivos de Unified Access Gateway. Las versiones anteriores de Unified Access Gateway se denominan Access Point. Si desea obtener más información, consulte *Implementación y configuración de Unified Access Gateway*.

Iniciar sesión en Horizon Administrator

Para realizar tareas iniciales de configuración, debe iniciar sesión en Horizon Administrator.

Requisitos previos

Verifique que esté usando un navegador web compatible con Horizon Administrator. Consulte [Requisitos de Horizon Administrator](#).

Procedimiento

- 1 Abra el navegador web e introduzca la siguiente URL, donde *servidor* es el nombre del host de la instancia del servidor de conexión.

`https://servidor/admin`

Nota Puede usar la dirección IP si tiene que acceder a la instancia del servidor de conexión cuando el nombre del host no se puede resolver. Sin embargo, el host con el que contacta no coincide con el certificado TLS que está configurado para la instancia del servidor de conexión, lo cual resulta en un acceso bloqueado o un acceso con seguridad reducida.

El acceso a Horizon Administrator depende del tipo de certificado que esté configurado en el equipo del servidor de conexión. Si abre el navegador web en el host del servidor de conexión, use **`https://127.0.0.1`** para conectarse en lugar de **`https://localhost`**. Este método mejora la seguridad evitando ataques DNS potenciales en la resolución `hostlocal`.

Opción	Descripción
Configuró un certificado firmado por una CA para el servidor de conexión de Horizon.	Cuando se conecte por primera vez, el navegador web mostrará la página Bienvenidos a VMware Horizon 7 .
Se configura el certificado autofirmado y predeterminado proporcionado con el servidor de conexión de Horizon.	Cuando se conecte por primera vez, el navegador web puede mostrar una página que advierte que ninguna entidad de certificación expidió el certificado de seguridad asociado a la dirección. Haga clic en Ignorar para continuar usando el certificado TLS actual.

- 2 En Horizon Administrator, haga clic en **Iniciar**.

3 Inicie sesión con una cuenta que tenga la función Administradores.

Debe realizar una asignación inicial a la función Administradores cuando instale una instancia del servidor de conexión independiente o la primera instancia del servidor de conexión en un grupo replicado. De forma predeterminada, se selecciona la cuenta que use para instalar el servidor de conexión, pero puede cambiar esta cuenta al grupo local de administradores o a un grupo global de dominio.

Si selecciona el grupo de administradores locales, puede usar cualquier usuario de dominio agregado a este grupo directamente o mediante la pertenencia al grupo global. No puede usar usuarios locales que estén agregados a este grupo.

Resultados

Después de iniciar sesión en Horizon Administrator, puede usar **Configuración de View > Administradores** para cambiar la lista de usuarios y grupos que tengan la función Administradores.

Instalar la clave de licencia del producto

Antes de poder utilizar el servidor de conexión, debe introducir una clave de licencia.

Nota La clave de licencia del producto no es obligatoria si tiene una licencia de suscripción de Horizon 7. Para obtener más información sobre las licencias de suscripción, consulte [#unique_129](#).

La primera vez que inicia sesión, Horizon Administrator muestra la página Licencia y uso del producto.

Después de instalar la clave de licencia, Horizon Administrator muestra la página del panel de control cuando inicia sesión.

No es necesario configurar una clave de licencia cuando instala una instancia del servidor de conexión replicada o un servidor de seguridad. Las instancias replicadas y los servidores de seguridad usan la clave de licencia común almacenada en la configuración LDAP de View.

Nota El servidor de conexión necesita una clave de licencia válida. La clave de licencia del producto tiene 25 caracteres.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Licencia y uso del producto**.
- 2 En el panel **Licencia**, haga clic en **Editar licencia**.
- 3 Introduzca el número de serie de la licencia y haga clic en **Aceptar**.
- 4 Verifique la fecha de caducidad de la licencia.

- 5 Verifique que las licencias de View Composer, de escritorio y de aplicaciones remotas estén habilitadas o deshabilitadas, según la edición de VMware Horizon 7 que la licencia de producto le permita utilizar.

No todas las funciones y características de VMware Horizon 7 están disponibles en todas las ediciones. Si desea obtener más información sobre los conjuntos de funciones de cada edición, consulte <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

Agregar instancias de vCenter Server a Horizon 7

Debe configurar Horizon 7 para conectarse a las instancias de vCenter Server en la implementación de Horizon 7. vCenter Server crea y administra las máquinas virtuales que Horizon 7 utiliza en grupos de escritorios.

Si ejecuta instancias de vCenter Server en un grupo Linked Mode, debe agregar cada instancia de vCenter Server a Horizon 7 de forma independiente.

Horizon 7 se conecta a la instancia de vCenter Server mediante un canal seguro (SSL).

Requisitos previos

- Instale la clave de licencia del servidor de conexión.
- Prepare un usuario de vCenter Server con permiso para realizar las operaciones necesarias en vCenter Server para admitir Horizon 7. Para usar View Composer, otorgue al usuario privilegios adicionales.

Consulte [Configurar un usuario de vCenter Server para Horizon 7 y View Composer](#).

- Compruebe que el host de vCenter Server tenga instalado un certificado de servidor TLS/SSL. En entornos de producción, instale un certificado válido firmado por una autoridad de certificación (AC). En entornos de pruebas, puede usar el certificado predeterminado instalado en vCenter Server, pero debe aceptar la huella digital del certificado cuando agregue vCenter Server a Horizon 7.
- Compruebe que todas las instancias del servidor de conexión en el grupo replicado confíen en el certificado raíz de CA para el certificado del servidor instalado en el host de vCenter Server. Asegúrese de que el certificado raíz de CA se encuentre en la carpeta **Autoridades de certificación raíz de confianza > Certificados** en el almacén de certificados local de Windows de los hosts del servidor de conexión. En caso contrario, importe el certificado raíz de AC en el almacén de certificados del equipo local de Windows.

Consulte [Importar un certificado raíz e intermedios al almacén de certificados de Windows](#).

- Compruebe que la instancia de vCenter Server contenga hosts ESXi. Si no se configuraron hosts en la instancia de vCenter Server, no podrá agregar la instancia a Horizon 7.
- Si actualiza a la versión vSphere 5.5 o una posterior, compruebe que un usuario local vCenter Server haya otorgado permisos específicos para iniciar sesión en vCenter Server a la cuenta de administrador de dominio que utiliza como usuario de dicho servicio.

- Si piensa utilizar Horizon 7 en modo FIPS, compruebe que tenga instalado vCenter Server 6.0 y hosts ESXi 6.0 o versiones posteriores.

Si desea obtener más información, consulte [Capítulo 4 Instalar Horizon 7 en modo FIPS](#).

- Familiarícese con la configuración que determina el número máximo de operaciones para vCenter Server y View Composer. Consulte [Límites de operaciones simultáneas para vCenter Server y View Composer](#) y [Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **vCenter Servers**, haga clic en **Agregar**.
- 3 En el cuadro de texto **Dirección del servidor** en la configuración de vCenter Server, escriba el nombre de dominio plenamente cualificado (fully qualified domain name, FQDN) de la instancia de vCenter Server.

El FQDN incluye el nombre de host y el de dominio. Por ejemplo: en el FQDN

myserverhost.companydomain.com, *myserverhost* es el nombre de host y *companydomain.com* es el dominio.

Nota Si ingresa en un servidor con un nombre DNS o una URL, Horizon 7 no realiza una búsqueda DNS para comprobar si el administrador añadió anteriormente este servidor a Horizon 7 con su dirección IP. Si agrega un servidor vCenter Server con su nombre DNS y dirección IP, se produce un conflicto.

- 4 Escriba el nombre del usuario vCenter Server.
Por ejemplo, *domain\user* o *user@domain.com*
- 5 Escriba la contraseña del usuario vCenter Server.
- 6 (opcional) Escriba una descripción para esta instancia de vCenter Server.
- 7 Escriba el número de puerto TCP.
El puerto predeterminado es 443.
- 8 En Configuración avanzada, establezca el límite de las operaciones simultáneas en vCenter Server y View Composer.
- 9 Haga clic en **Siguiente** para mostrar la página de Configuración de View Composer.

Pasos siguientes

Configure las opciones de View Composer.

- Si la instancia de vCenter Server se configura con un certificado SSL firmado y el servidor de conexión confía en el certificado raíz, el asistente para agregar vCenter Server muestra la página Configuración de View Composer.

- Si la instancia de vCenter Server se configura con un certificado predeterminado, primero debe determinar si acepta la huella digital del certificado existente. Consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

Si Horizon 7 utiliza varias instancias de vCenter Server, repita este procedimiento para agregar las demás instancias de vCenter Server.

Configurar las opciones de View Composer

Para usar View Composer, debe configurar las opciones que permiten al servidor de conexión conectarse al servicio View Composer. View Composer se puede instalar en su propio equipo independiente o en el mismo que vCenter Server.

VMware recomienda tener una asignación uno a uno entre el servicio View Composer y la instancia de vCenter Server.

Requisitos previos

- Compruebe que el servidor de conexión esté configurado para conectarse a vCenter Server. A tal efecto, debe completar la página de Información de vCenter Server en el asistente para Agregar vCenter Server. Consulte [Agregar instancias de vCenter Server a Horizon 7](#).
- Compruebe que el servicio View Composer aún no esté configurado para conectarse a otra instancia de vCenter Server.
- Si instaló View Composer en un equipo independiente, compruebe que creó una cuenta de usuario de View Composer. Esta cuenta de usuario del dominio debe ser miembro del grupo local Administradores del equipo View Composer.

Procedimiento

- 1 En Horizon Administrator, complete la página Información de vCenter Server en el asistente Agregar vCenter Server.
 - a Haga clic en **Configuración de View > Servidores**.
 - b En la pestaña vCenter Servers, haga clic en **Agregar** y configure las opciones de vCenter Server.
- 2 En la página de Configuración de View Composer, si no está utilizando dicho componente, seleccione **No utilizar View Composer**.

Si selecciona **No utilizar View Composer**, el resto de opciones de configuración de View Composer quedan inactivas. Al hacer clic en **Siguiente**, el asistente para Agregar vCenter Server muestra la página de Configuración de almacenamiento. No incluye la página de Dominios de View Composer.

- 3 Si está utilizando View Composer, seleccione la ubicación del equipo de View Composer.

Opción	Descripción
View Composer está instalado en el mismo equipo que vCenter Server.	<p>a Seleccione View Composer instalado conjuntamente con vCenter Server.</p> <p>b Asegúrese de que el número de puerto es el mismo que se especificó cuando se instaló el servicio View Composer en vCenter Server. El puerto predeterminado es el 18443.</p>
View Composer está instalado en su propio equipo independiente.	<p>a Seleccione Servidor View Composer independiente.</p> <p>b En el cuadro de texto de la dirección del servidor de View Composer, escriba el nombre de dominio plenamente cualificado (fully qualified domain name, FQDN) en el equipo de View Composer.</p> <p>c Introduzca el nombre de una cuenta de usuario del dominio que se pueda autenticar en el servicio View Composer.</p> <p>La cuenta debe ser miembro del grupo local Administradores en el equipo de View Composer independiente.</p> <p>Por ejemplo, domain.com\user o user@domain.com</p> <p>d Introduzca la contraseña de esta cuenta de usuario del dominio.</p> <p>e Asegúrese de que el número de puerto es el mismo que se especificó cuando se instaló el servicio View Composer. El puerto predeterminado es el 18443.</p>

- 4 Haga clic en **Siguiente** para mostrar la página de Dominios de View Composer.

Pasos siguientes

Configure los dominios de View Composer.

- Si la instancia de View Composer está configurada con un certificado SSL firmado y el servidor de conexión confía en el certificado raíz, el asistente Agregar vCenter Server muestra la página Dominios de View Composer.
- Si la instancia de View Composer está configurada con un certificado predeterminado, debe determinar primero si acepta la huella digital del certificado existente. Consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

Configurar los dominios de View Composer

Debe configurar un dominio de Active Directory en el que View Composer implemente escritorios de clonación vinculada. Puede configurar varios dominios en View Composer. Después de agregar por primera vez la configuración de View Composer y vCenter Server a View, puede agregar más dominios de View Composer editando la instancia de vCenter Server en Horizon Administrator.

Requisitos previos

- El administrador de Active Directory debe crear un usuario de View Composer para las operaciones de AD. Este usuario de dominio debe tener permiso para agregar y eliminar máquinas virtuales del dominio de Active Directory que incluya clones vinculados. Para obtener más información sobre los permisos necesarios para este usuario, consulte [Crear una cuenta de usuario para operaciones en AD de View Composer](#).

- En Horizon Administrator, compruebe que completó las páginas Información de vCenter Server y Configuración de View Composer en el asistente Agregar vCenter Server.

Procedimiento

- 1 En la página Dominios de View Composer, haga clic en **Agregar** para agregar el usuario de View Composer que se usará en las operaciones de AD de información de cuenta.
- 2 Introduzca el nombre de dominio de Active Directory.
Por ejemplo: **domain.com**
- 3 Introduzca el nombre de usuario del dominio, del usuario de View Composer incluido el nombre de dominio.
Por ejemplo: **domain.com\admin**
- 4 Introduzca la contraseña de la cuenta.
- 5 Haga clic en **Aceptar**.
- 6 Para agregar cuentas de usuario del dominio con privilegios en otros dominios de Active Directory en el que implementa grupos de clonación vinculada, repita los pasos anteriores.
- 7 Haga clic en **Siguiente** para mostrar la página de Configuración de almacenamiento.

Pasos siguientes

Habilite la reclamación de espacio de disco de la máquina virtual y configure el acelerador de almacenamiento de View para Horizon 7.

Agregar un administrador de dominio de clones instantáneos

Antes de crear un grupo de escritorios de clones instantáneos, debe agregar un administrador de dominio de clones instantáneos a Horizon 7.

El administrador de dominio de clones instantáneos debe tener ciertos privilegios de dominio de Active Directory. Consulte "Privilegios de clones instantáneos y View Composer necesarios para el usuario de vCenter Server" en el documento *Instalación de Horizon 7*.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Adminis. del dominio de Instant Clone**.
- 2 Haga clic en **Agregar**.
- 3 Introduzca el nombre y la contraseña de inicio de sesión del administrador de dominio de clones instantáneos.

Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados

En vSphere 5.1 y versiones posteriores, puede habilitar la función de recuperación de espacio de disco de Horizon 7. A partir de vSphere 5.1, Horizon 7 crea máquinas virtuales de clones vinculados con formato de disco eficiente. Dicho formato permite que los hosts ESXi recuperen espacio de disco sin usar en los clones vinculados, con lo que se reduce el espacio de almacenamiento total necesario para los clones vinculados.

A medida que los usuarios interactúan con escritorios de clones vinculados, los discos de SO clonados crecen y pueden incluso usar tanto espacio de disco como los escritorios de clones completos. La recuperación de espacio de disco reduce el tamaño de los discos de SO sin necesidad de actualizar o recomponer los clones vinculados. Se puede recuperar el espacio mientras las máquinas virtuales están encendidas y los usuarios interactúan con sus escritorios remotos.

La recuperación de espacio de disco es especialmente útil para implementaciones que no pueden aprovechar las ventajas que ofrecen las estrategias de ahorro de almacenamiento, como actualizar al cerrar sesión. Por ejemplo, los trabajadores de conocimiento que instalan aplicaciones de usuario en escritorios remotos dedicados pueden perder sus aplicaciones personales si los escritorios remotos se actualizan o recomponen. Con la recuperación de espacio de disco, Horizon 7 puede mantener los clones vinculados casi al tamaño reducido con el que empezaron cuando se aprovisionaron por primera vez.

Esta función tiene dos componentes: formato de disco eficiente de espacio y operaciones de recuperación de espacio.

En vSphere 5.1 y entornos con una versión posterior, cuando la versión del hardware virtual de una máquina principal es 9 o posterior, Horizon 7 crea clones vinculados con discos de SO eficientes, estén o no habilitadas las operaciones de recuperación de espacio.

Debe usar Horizon Administrator para habilitar la recuperación de espacio en vCenter Server y recuperar espacio de disco de las máquinas virtuales para los grupos de escritorios individuales. La configuración de recuperación de espacio en vCenter Server presenta la opción de deshabilitar la función en todos los grupos de escritorios administrados por la instancia de vCenter Server. Al deshabilitar la función de vCenter Server, se anula la configuración a nivel de grupos de escritorios.

Las siguientes instrucciones se aplican a la función de recuperación de espacio:

- Solo funciona en discos de SO eficientes de clones vinculados.
- No afecta a los discos persistentes de View Composer.
- Funciona solo con vSphere 5.1 o una versión posterior en máquinas virtuales cuyo hardware virtual tenga la versión 9 o una posterior.
- No funciona en escritorios de clones completos.
- Funciona en máquinas virtuales con controladores SCSI. Los controladores IDE no son compatibles.

La función Array Integration de View Composer (VCAI) no es compatible con los grupos que incluyen máquinas virtuales con discos eficientes de espacio. VCAI usa la tecnología de snapshots NFS nativas vStorage APIs - Array Integration (VAAI) para clonar máquinas virtuales.

Requisitos previos

- Compruebe que la versión de vCenter Server y los hosts ESXi, incluidos todos los hosts ESXi de un clúster, sea 5.1 y que de la revisión de descarga ESXi 5.1 sea ESXi510-201212001 o una versión posterior.

Procedimiento

- 1 En Horizon Administrator, complete las páginas del asistente Agregar vCenter Server que preceden a la página de Configuración de almacenamiento.
 - a Seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, haga clic en **Agregar**.
 - c Complete las páginas de Información de vCenter Server, Configuración de View Composer y Dominios de View Composer.

- 2 En la página de Configuración de almacenamiento, asegúrese de que esté seleccionado **Habilitar recuperación de espacio**.

La recuperación de espacio está seleccionada de forma predeterminada si está realizando una instalación nueva de Horizon 7 5.2 o una versión posterior. Debe seleccionar **Habilitar recuperación de espacio** si está actualizando a Horizon 7 5.2 o una versión posterior desde Horizon 7 5.1 o una versión anterior.

Pasos siguientes

En la página de Configuración de almacenamiento, configure el Acelerador de almacenamiento de View.

Configure la recuperación de espacio de disco en grupos de escritorios para finalizar la configuración en Horizon 7.

Configurar el acelerador de almacenamiento de View para vCenter Server

En vSphere 5.1 y versiones posteriores, puede configurar los hosts ESXi para almacenar en caché datos del disco de la máquina virtual. Esta función, denominada Acelerador de almacenamiento de View, usa la función de almacenamiento de caché de lectura basada en el contenido (CBRC) en los hosts ESXi. El acelerador de almacenamiento de View mejora el rendimiento de Horizon 7 durante procesos de E/S masivos, que tienen lugar cuando varias máquinas virtuales se inician o realizan exámenes de antivirus a la vez. Esta función también es útil cuando los administradores o los usuarios cargan aplicaciones o datos frecuentemente. En lugar de leer todo el SO o toda la aplicación desde el sistema de almacenamiento una y otra vez, un host puede leer bloques de datos comunes desde la caché.

Al reducir el número de IOPS durante los arranques masivos, el acelerador de almacenamiento de View disminuye la demanda de la matriz de almacenamiento, que le permite usar menos ancho de banda E/S de almacenamiento para que admita la implementación de Horizon 7.

Puede habilitar el almacenamiento en caché de los hosts ESXi seleccionando la opción Acelerador de almacenamiento de View en el asistente de vCenter Server en Horizon Administrator, como se describe en este procedimiento.

Asegúrese de que el acelerador de almacenamiento de View también esté configurado en grupos de escritorios individuales. Para realizar operaciones en un grupo de escritorios, el acelerador de almacenamiento de View debe estar habilitado en vCenter Server y en el grupo de escritorios individual.

De forma predeterminada, el acelerador de almacenamiento de View está habilitado para grupos de escritorios. La función puede estar deshabilitada o habilitada cuando cree o edite un grupo. Lo más recomendable es habilitar esta función cuando cree un grupo de escritorios por primera vez. Si habilita la función al editar un grupo existente, debe asegurarse de que se hayan creado una nueva réplica y sus discos resumen antes de que se aprovisionen los clones vinculados. Puede crear una nueva réplica volviendo a componer el grupo en una snapshot nueva o volviendo a equilibrar el grupo en un nuevo almacén de datos. Los archivos de resumen solo se pueden configurar en las máquinas virtuales en un grupo de escritorios cuando están desconectados.

Puede habilitar el acelerador de almacenamiento de View en grupos de escritorios que contengan clones vinculados y grupos que contengan máquinas virtuales completas.

No se admite la tecnología de snapshot NFS nativa (VAAI) en grupos que están habilitados para el acelerador de almacenamiento de View.

El acelerador de almacenamiento de View ya está cualificado para trabajar en configuraciones que usen niveles de réplica de Horizon 7, cuyas réplicas estén almacenadas en almacenes de datos independientes de los clones vinculados. Aunque los beneficios de rendimiento del uso del acelerador de almacenamiento de View con niveles de réplica de Horizon 7 no sea significativo, algunos beneficios relacionados con la capacidad se deben realizar almacenando las réplicas en un almacén de datos independiente. Se probó esta combinación y se admite.

Importante Si tiene pensado usar esta función y está usando varios pods de Horizon 7 que comparten algunos hosts ESXi, debe habilitar la función Horizon Storage Accelerator en todos los pods que se encuentren en los hosts ESXi compartidos. Las configuraciones inconsistentes en varios pods puede causar inestabilidad en las máquinas virtuales de los hosts ESXi compartidos.

Requisitos previos

- Compruebe que vCenter Server y los hosts ESXi tengan la versión 5.1 o una versión posterior.
En un clúster ESXi, compruebe que todos los hosts cuenten con la versión 5.1 o posterior.
- Verifique que el usuario de vCenter Server tenga asignado el privilegio **Host > Configuración > Configuración avanzada** en vCenter Server.
Consulte [Configurar cuentas de usuario para vCenter Server, View Composer y clones instantáneos](#).

Procedimiento

- 1 En Horizon Administrator, complete las páginas del asistente Agregar vCenter Server que preceden a la página de Configuración de almacenamiento.
 - a Seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, haga clic en **Agregar**.
 - c Complete las páginas de Información de vCenter Server, Configuración de View Composer y Dominios de View Composer.
- 2 En la página Configuración de almacenamiento, asegúrese de que la casilla de verificación **Habilitar el acelerador de almacenamiento de View** esté seleccionada.
Esta casilla de verificación está seleccionada de forma predeterminada.
- 3 Especifique un tamaño de la caché del host predeterminado.
El tamaño de la memoria caché predeterminado se aplica a todos los hosts ESXi administrados por esta instancia de vCenter Server.
El valor predeterminado es 1.024MB. El tamaño de la caché debe estar entre 100 MB y 2.048 MB.
- 4 Para especificar un tamaño de la caché diferente para un host ESXi individual, seleccione un host ESXi y haga clic en **Editar tamaño de caché**.
 - a En el cuadro de diálogo Tamaño de caché del host seleccione **Omitir el tamaño de caché del host predeterminado**.
 - b Introduzca un valor **Tamaño de caché del host** entre 100 MB y 2.048 MB y haga clic en **Aceptar**.
- 5 En la página Configuración de almacenamiento, haga clic en **Siguiente**.
- 6 Haga clic en **Finalizar** para agregar la configuración de almacenamiento, de vCenter Server y de View Composer a Horizon 7.

Pasos siguientes

Para configurar la puerta de enlace segura de PCoIP, el túnel de seguridad y las URL externas para las conexiones cliente, consulte [Configurar conexiones de Horizon Client](#).

Para completar la configuración del acelerador de almacenamiento de View en Horizon 7, configure el acelerador de almacenamiento de View en los grupos de escritorios. Consulte "Configurar el acelerador de almacenamiento de View para los grupos de escritorios" en el documento *Configurar escritorios virtuales en Horizon 7*.

Límites de operaciones simultáneas para vCenter Server y View Composer

Cuando agrega vCenter Server a Horizon 7 o edita su configuración, puede establecer el número máximo de operaciones simultáneas que realizan vCenter Server y View Composer.

Configure estas opciones en el panel Configuración avanzada en la página de información de vCenter Server.

Tabla 9-3. Límites de operaciones simultáneas para vCenter Server y View Composer

Configuración	Descripción
Número máximo de operaciones de aprovisionamiento de vCenter simultáneas	<p>Determina el número máximo de solicitudes simultáneas que el servidor de conexión puede realizar para aprovisionar y eliminar máquinas virtuales completas en esta instancia de vCenter Server.</p> <p>El valor predeterminado es 20.</p> <p>Esta configuración se aplica únicamente a las máquinas virtuales completas.</p>
Máximo número de operaciones de alimentación simultáneas	<p>Determina el número máximo de operaciones de alimentación simultáneas (iniciar, apagar, suspender, etc.) que pueden tener lugar en máquinas virtuales administradas por el servidor de conexión en esta instancia de vCenter Server.</p> <p>El valor predeterminado es 50.</p> <p>Para obtener más instrucciones sobre cómo calcular el valor de esta opción, consulte Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto.</p> <p>Esta configuración se aplica a las máquinas virtuales completas y a los clones vinculados.</p>
Operaciones de mantenimiento simultáneas máximas de View Composer	<p>Determina el número máximo de operaciones simultáneas de actualización, para volver a componer y a equilibrar View Composer que pueden realizarse en clones vinculados administradas por esta instancia de View Composer.</p> <p>El valor predeterminado es 12.</p> <p>Es necesario que se cierren las sesiones activas de los escritorios remotos antes de que pueda comenzar una operación de mantenimiento. Si obliga a los usuarios a cerrar sesión cuando la operación de mantenimiento comienza, el número máximo de operaciones simultáneas en los escritorios remotos para las que son necesarias que se cierren las sesiones es la mitad del valor configurado. Por ejemplo, si configura esta opción en 24 y obliga a los usuarios a cerrar sesión, el número máximo de operaciones simultáneas en los escritorios para las que son necesarias que se cierren las sesiones es 12.</p> <p>Esta opción se aplica únicamente a los clones vinculados.</p>
Operaciones de aprovisionamiento simultáneas máximas de View Composer	<p>Determina el número máximo de operaciones simultáneas de creación y eliminación que pueden realizarse en clones vinculados administradas por esta instancia de View Composer.</p> <p>El valor predeterminado es 8.</p> <p>Esta opción se aplica únicamente a los clones vinculados.</p>

Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto

La opción **Máximo número de operaciones de alimentación simultáneas** establece el número máximo de opciones de alimentación simultáneas que se pueden producir en las máquinas virtuales del escritorio remoto en una instancia de vCenter Server. Este límite se establece en 50 de forma predeterminada. Puede cambiar este valor para que admita velocidades de encendido máximas cuando muchos usuarios inician sesión en los escritorios al mismo tiempo.

Como práctica recomendada, puede realizar una fase piloto para determinar el valor correcto de esta opción. Para obtener directrices de planificación, consulte el apartado que contiene las directrices de planificación y los elementos de diseño de arquitectura en el documento *Planificación de la arquitectura de Horizon 7*.

El número requerido de operaciones de alimentación simultáneas se basa en la velocidad máxima a la que se encienden los escritorios y en la cantidad de tiempo que tardan los escritorios en encenderse, iniciarse y estar disponibles para establecer una conexión. En general, el límite de operaciones de alimentación recomendado es el tiempo total que tardan los escritorios en iniciarse multiplicado por la velocidad máxima de encendido.

Por ejemplo, el escritorio medio tarda de dos a tres minutos en iniciarse. Por lo tanto, el límite de operaciones de alimentación simultáneas debe ser 3 veces la velocidad máxima de encendido. Se espera que la opción predeterminada de 50 admita una velocidad máxima de encendido de 16 escritorios por minuto.

El sistema espera un máximo de cinco minutos para que se inicie un escritorio. Si tarda más en iniciarse, es probable que se produzcan otros errores. Para ser conservador, puede configurar un límite de operaciones de alimentación que sea 5 veces la velocidad máxima de encendido. Con un procedimiento conservador, la opción predeterminada de 50 admite una velocidad máxima de encendido de 10 escritorios por minuto.

Los inicios de sesión y, por lo tanto, las operaciones de encendido de los escritorios, suelen suceder de forma distribuida a través de una ventana de tiempo determinada. Puede aproximar la velocidad máxima de encendido asumiendo que ocurra en la mitad de la ventana de tiempo, durante la cual cerca del 40% de las operaciones de encendido se producen en una sexta parte de la ventana de tiempo. Por ejemplo si los usuarios inician sesión entre las 8:00 y las 9:00, la ventana de tiempo es una hora y el 40% de los inicios de sesión se producen en los 10 minutos comprendidos entre las 8:25 y las 8:35. Si hay 2.000 usuarios, y el 20% tiene sus escritorios desconectados, el 40% de las 400 operaciones de encendido de los escritorios se producen en esos 10 minutos. La velocidad máxima de encendido es 16 escritorios por minuto.

Aceptar la huella digital de un certificado TLS predeterminado

Cuando agregue las instancias de vCenter Server y de View Composer a Horizon 7, debe asegurarse de que los certificados TLS que se usan para las instancias de vCenter Server y de View Composer sean válidos y que el servidor de conexión confíe en ellos. Si los certificados predeterminados instalados con vCenter Server y View Composer están aún en las instalaciones, debe determinar si desea aceptar las huellas digitales de los certificados.

Si una instancia de vCenter Server o de View Composer está configurada con un certificado firmado por una CA y el servidor de conexión confía en el certificado raíz, no es necesario que acepte la huella digital del certificado. No es necesaria ninguna acción.

Si reemplaza un certificado predeterminado por uno firmado por una CA, pero el servidor de conexión no confía en el certificado raíz, debe determinar si desea aceptar la huella digital del certificado. Una huella digital es un hash criptográfico de un certificado. La huella digital se usa para determinar rápidamente si un certificado presentado es igual a otro, como, por ejemplo, el certificado que se aceptó previamente.

Nota Si instala vCenter Server y View Composer en el mismo host de Windows Server, pueden usar el mismo certificado TLS, pero debe configurar el certificado de forma independiente para cada componente.

Para obtener más información sobre cómo configurar certificados TLS, consulte [Capítulo 8 Configurar los certificados TLS de los servidores de Horizon 7](#).

Primero agregue vCenter Server y View Composer en Horizon Administrator usando el asistente Agregar vCenter Server. Si un certificado no es de confianza y no acepta la huella digital, no puede agregar vCenter Server ni View Composer.

Después de agregar estos servidores, puede volver a configurarlos en el cuadro de diálogo Editar vCenter Server.

Nota También debe aceptar una huella digital de certificado cuando actualice una versión anterior y un certificado de vCenter Server o de View Composer no sea de confianza, o bien si reemplaza un certificado de confianza por uno que no lo sea.

En el panel de control de Horizon Administrator, el icono de vCenter Server o de View Composer se vuelve rojo y aparece el cuadro de diálogo Se detectó un certificado no válido. En Horizon Administrator, haga clic en **Configuración de View > Servidores** y edite la entrada de vCenter Server asociada al servicio de View Composer. A continuación, haga clic en **Editar** en la configuración de vCenter Server y siga las indicaciones para verificar y aceptar el certificado autofirmado.

De forma similar, en Horizon Administrator puede configurar un autenticador SAML para que lo use una instancia del servidor de conexión. Si el servidor de conexión no confía en el certificado del servidor SAML, debe determinar si desea aceptar la huella digital del certificado. Si no acepta la huella digital, no puede configurar el autenticador SAML en Horizon 7. Después de configurar un autenticador SAML, puede volver a configurarlo en el cuadro de diálogo Editar servidor de conexión.

Procedimiento

- 1 Cuando aparezca el cuadro de diálogo Se detectó un certificado no válido en Horizon Administrator, haga clic en **Ver certificado**.
- 2 Examine la huella digital del certificado en la ventana Información del certificado.
- 3 Examine la huella digital del certificado que se configuró para la instancia de View Composer o vCenter Server.
 - a En el host de View Composer o de vCenter Server, inicie el complemento MMC y abra el almacén de certificados de Windows.
 - b Diríjase al certificado de vCenter Server o de View Composer.
 - c Haga clic en la pestaña Información del certificado para mostrar la huella digital del certificado.

De forma similar, examine la huella digital del certificado de un autenticador SAML. Si es necesario, lleve a cabo los pasos anteriores en el host del autenticador SAML.

- 4 Compruebe que la huella digital de la ventana Información del certificado coincida con la huella digital de la instancia de vCenter Server o de View Composer.

De forma similar, compruebe que las huellas digitales coincidan con un autenticador SAML.

- 5 Determine si desea aceptar la huella digital del certificado.

Opción	Descripción
La huella digital coincide.	Haga clic en Aceptar para usar el certificado predeterminado.
Las huellas digitales no coinciden.	Haga clic en Rechazar . Solucione los problemas con los certificados que no coinciden. Por ejemplo, es posible que haya proporcionado una dirección IP incorrecta para vCenter Server o View Composer.

Configurar conexiones de Horizon Client

Los endpoints cliente se comunican con un host del servidor de seguridad o del servidor de conexión a través de conexiones seguras.

La conexión cliente inicial, que se usa para autenticar al usuario y seleccionar aplicaciones y escritorios remotos, se crea mediante HTTPS cuando un usuario proporciona un nombre de dominio de Horizon Client. Si un firewall y un software de equilibrio de carga están configurados correctamente en el entorno de red, esta solicitud llega al host del servidor de seguridad o del servidor de conexión. Con esta conexión, los usuarios se autentican y se selecciona un escritorio o una aplicación, pero los usuarios aún no se conectan a esta aplicación o este escritorio remotos.

Cuando los usuarios se conectan a aplicaciones y escritorios remotos, de forma predeterminada, el cliente establece una segunda conexión al host del servidor de seguridad o del servidor de conexión de View. Esta conexión se denomina conexión de túnel porque proporciona un túnel seguro para enviar RDP y otros datos mediante HTTPS.

Cuando los usuarios se conectan a aplicaciones y escritorios remotos con el protocolo de visualización PCoIP, el cliente puede establecer otra conexión a la puerta de enlace segura PCoIP en el host del servidor de seguridad o del servidor de conexión. La puerta de enlace segura PCoIP asegura que solo los usuarios autenticados puedan comunicarse con las aplicaciones y los escritorios remotos mediante PCoIP.

También puede proporcionar conexiones seguras para que los usuarios se conecten a las aplicaciones y los escritorios remotos con el protocolo de visualización VMware Blast y para que los usuarios externos que usan HTML Access se conecten a los escritorios remotos. La puerta de enlace segura Blast asegura que solo los usuarios autenticados puedan comunicarse con los escritorios remotos.

Dependiendo del tipo de dispositivo cliente que se utilice, se establecen canales adicionales para llevar otro tráfico, como los datos de redireccionamiento USB, al dispositivo cliente. Estos canales de datos enrutan el tráfico a través del túnel seguro si este está establecido.

Cuando el túnel seguro y las puertas de enlace seguras estén habilitadas, las sesiones de aplicaciones y de escritorios se establecen directamente entre el dispositivo cliente y el equipo remoto, omitiendo el host del servidor de seguridad o del servidor de conexión. Este tipo de conexión se denomina conexión directa.

Las sesiones de aplicaciones y de escritorios que usan conexiones directas siguen conectadas aunque el servidor de conexión ya no se ejecute.

Normalmente, para proporcionar conexiones seguras a los clientes externos que se conectan a un host del servidor de conexión o del servidor de seguridad a través de una WAN, es necesario que habilite el túnel seguro, la puerta de enlace segura PCoIP y la puerta de enlace segura de Blast. Puede deshabilitar el túnel seguro y las puertas de enlace seguras para permitir que los clientes internos y conectados a través de LAN establezcan conexiones directas a las aplicaciones y los escritorios remotos.

Si solo habilita el túnel seguro o una puerta de enlace segura, una sesión puede usar una conexión directa para algunos tráfico, pero envía los otros a través del host del servidor de seguridad o del servidor de conexión, dependiendo del tipo de cliente que se utilice.

SSL es obligatorio para todas las conexiones cliente a los hosts del servidor de seguridad y del servidor de conexión.

Configurar la puerta de enlace segura PCoIP y las conexiones de túnel seguro

Utilice Horizon Administrator para configurar el uso del túnel seguro y la puerta de enlace segura PCoIP. Estos componentes aseguran que solo los usuarios autenticados puedan comunicarse con escritorios remotos y aplicaciones.

Los clientes que usen un protocolo de visualización PCoIP pueden utilizar la puerta de enlace segura PCoIP. Los clientes que usen un protocolo de visualización RDP pueden utilizar el túnel seguro.

Para obtener más información sobre cómo configurar la puerta de enlace segura Blast, consulte [Configurar la puerta de enlace segura Blast](#).

Importante Una configuración de red típica que proporcione conexiones seguras a clientes externos incluye un servidor de seguridad. Para habilitar o deshabilitar el túnel seguro y la puerta de enlace segura PCoIP en un servidor de seguridad, debe editar la instancia del servidor de conexión emparejada con el servidor de seguridad.

En una configuración de red en la que los clientes externos se conecten directamente a un host del servidor de conexión, puede habilitar o deshabilitar el túnel seguro y la puerta de enlace segura PCoIP si edita la instancia del servidor de conexión en Horizon Administrator.

Requisitos previos

- Si planea habilitar la puerta de enlace segura PCoIP, compruebe que la instancia del servidor de conexión y el servidor de seguridad emparejado tengan instalados View 4.6 o una versión posterior.

- Si empareja un servidor de seguridad con una instancia del servidor de conexión en el que esté ya habilitada la puerta de enlace segura PCoIP, compruebe que el servidor de seguridad tenga instalado View 4.6 o una versión posterior.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En el panel Servidores de conexión, seleccione una instancia del servidor de conexión y haga clic en **Editar**.
- 3 Configure el uso del túnel seguro.

Opción	Descripción
Deshabilitar el túnel seguro	Anule la selección Usar la conexión de túnel seguro con la máquina .
Habilitar el túnel seguro	Seleccione Usar la conexión de túnel seguro con la máquina .

El túnel seguro se habilita de forma predeterminada.

- 4 Configure el uso de la puerta de enlace segura PCoIP.

Opción	Descripción
Habilitar la puerta de enlace segura PCoIP	Seleccione Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina .
Deshabilitar la puerta de enlace segura PCoIP	Anule la selección Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina .

La puerta de enlace segura PCoIP está deshabilitada de forma predeterminada.

- 5 Haga clic en **Aceptar** para guardar los cambios.

Configurar la puerta de enlace segura Blast

En Horizon Administrator, puede configurar el uso de la puerta de enlace segura Blast para proporcionar acceso seguro a las aplicaciones y a los escritorios remotos, a través de HTML Access o a través de conexiones cliente que usan el protocolo de visualización VMware Blast.

La puerta de enlace segura de Blast incluye redes Blast Extreme Adaptive Transport (BEAT), que se ajustan dinámicamente a las condiciones de la red, como los cambios de velocidad y la pérdida de paquetes.

- La puerta de enlace segura Blast admite las redes BEAT solo cuando se ejecutan en un dispositivo de Unified Access Gateway.
- Los Horizon Clients que usen IPv4 y los Horizon Clients que usen IPv6 se pueden gestionar a la vez en el puerto TCP 8443 y en el puerto UDP 8443 (para BEAT) cuando se conecte al dispositivo Unified Access Gateway versión 3.3 o posterior.

- Los Horizon Clients que usen una condición típica de la red deben conectarse a un servidor de conexión (BSG deshabilitada), a un servidor de seguridad (BSG deshabilitada) o a versiones posteriores a la 2.8 de un dispositivo Unified Access Gateway. Si Horizon Client usa una condición típica de la red para conectarse a un servidor de conexión (BSG habilitada), a un servidor de seguridad (BSG habilitada) o a versiones anteriores a la 2.8 de un dispositivo Unified Access Gateway, el cliente detecta automáticamente la condición de la red y vuelve a la red TCP.
- Los Horizon Clients que usen una condición mala de la red deben conectarse a la versión 2.9 o a una versión posterior de un dispositivo Unified Access Gateway (con Servidor del túnel UDP habilitado). Si Horizon Client usa una condición mala de la red para conectarse al servidor de conexión (BSG habilitada), al servidor de seguridad (BSG habilitada) o a versiones anteriores a la 2.8 de un dispositivo Unified Access Gateway, el cliente detecta automáticamente la condición de la red y vuelve a la red TCP.
- Los Horizon Clients que usen una mala condición de la red para conectarse al servidor de conexión (BSG habilitada), al servidor de seguridad (BSG habilitada), a versiones posteriores a la 2.9 de un dispositivo Unified Access Gateway (sin Servidor del túnel UDP habilitado) o a la versión 2.8 del dispositivo Unified Access Gateway, el cliente detecta automáticamente la condición de la red y vuelve a la condición típica.

Para obtener más información, consulte la documentación de Horizon Client disponible en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Nota También puede usar los dispositivos de Unified Access Gateway, en lugar de los servidores de seguridad, para el acceso externo seguro a los servidores y los escritorios de Horizon 7. Si usa dispositivos Unified Access Gateway, debe deshabilitar las puertas de enlace seguras en las instancias del servidor de conexión y habilitar estas puertas de enlace en los dispositivos de Unified Access Gateway. Si desea obtener más información, consulte *Implementación y configuración de Unified Access Gateway*.

Cuando la puerta de enlace segura Blast no está habilitada, los dispositivos cliente y los navegadores web cliente usan el protocolo VMware Blast Extreme para establecer conexiones directas a aplicaciones y máquinas virtuales de escritorio remoto, omitiendo la puerta de enlace segura Blast.

Importante Una configuración de red típica que proporcione conexiones seguras a usuarios externos incluye un servidor de seguridad. Para habilitar o deshabilitar la puerta de enlace segura Blast en un servidor de seguridad, debe editar la instancia del servidor de conexión emparejada con el servidor de seguridad. Si los usuarios externos se conectan directamente a un host del servidor de conexión, habilite o deshabilite la puerta de enlace segura Blast al editar esa instancia del servidor de conexión.

Requisitos previos

Si los usuarios seleccionan los escritorios remotos usando VMware Identity Manager, verifique que VMware Identity Manager esté instalado y configurado para usar con un servidor de conexión y que ese servidor de conexión esté emparejado con un servidor de autenticación SAML 2.0.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor de conexión y haga clic en **Editar**.
- 3 Configure el uso de la puerta de enlace segura Blast.

Opción	Descripción
Habilitar la puerta de enlace segura Blast	Seleccione Usar la puerta de enlace segura Blast en las conexiones Blast de la máquina
Habilitar la puerta de enlace segura de Blast para HTML Access	Seleccione Usar la puerta de enlace segura Blast solo en las conexiones HTML Access de la máquina
Deshabilitar la puerta de enlace segura de Blast	Seleccione No usar la puerta de enlace segura de Blast

La puerta de enlace segura Blast está habilitada de forma predeterminada.

- 4 Haga clic en **Aceptar** para guardar los cambios.

Configurar URL externas para conexiones seguras de puerta de enlace y túnel.

Para usar el túnel seguro, el sistema cliente debe tener acceso a una dirección IP, o bien a un nombre de dominio completo (FQDN) que pueda resolver una dirección IP que permita al cliente alcanzar un host del servidor de seguridad o del servidor de conexión.

Para usar la puerta de enlace segura PCoIP, un cliente se conecta a un host del servidor de conexión o del servidor de seguridad utilizando una URL. En un entorno IPv4, la URL debe identificar a un host por su dirección IP. En un entorno IPv6, la URL puede identificar a un host por su dirección IP o su FQDN.

Para usar la puerta de enlace segura de Blast, un dispositivo endpoint de usuario debe tener acceso a un FQDN que pueda resolver una dirección IP que permita al equipo o al navegador web del usuario alcanzar un host del servidor de conexión o un servidor de seguridad.

Usar las conexiones de túnel para ubicaciones externas

De forma predeterminada, solo se puede contactar con un host del servidor de seguridad o del servidor de conexión a través de clientes de túnel que residen dentro de la misma red y que, por lo tanto, pueden encontrar el host solicitado.

Muchas organizaciones necesitan que los usuarios se puedan conectar desde una ubicación externa usando una dirección IP específica o un nombre de dominio que el cliente pueda resolver, así como un puerto específico. Esta información podría o no podría parecerse al número de puerto y a la dirección reales del host del servidor de seguridad o del servidor de conexión. Esta información se proporciona al sistema cliente en forma de URL. Por ejemplo:

- `https://view-example.com:443`
- `https://view.example.com:443`

- `https://example.com:1234`
- `https://10.20.30.40:443`

Para usar direcciones como las anteriores en Horizon 7, debe configurar el host del servidor de conexión o del servidor de seguridad de forma que devuelva una URL externa en lugar del FQDN del host.

Configurar URL externas

Configure más de una URL externa. La primera URL permite a los sistemas cliente realizar conexiones en túnel. Una segunda URL permite a los clientes que usan PCoIP establecer conexiones seguras a través de la puerta de enlace segura PCoIP. En un entorno IPv4, la URL debe identificar a un host por su dirección IP. En un entorno IPv6, la URL puede identificar a un host por su dirección IP o su FQDN. La URL permite que los clientes se conecten desde una ubicación externa.

Una tercera URL permite a los usuarios establecer conexiones seguras desde los dispositivos cliente o los navegadores web a través de la puerta de enlace segura Blast.

Si la configuración de red incluye servidores de seguridad, proporcione URL externas para los servidores de seguridad. Las URL externas no son obligatorias en las instancias del servidor de conexión que están emparejadas con los servidores de seguridad.

El proceso de configuración de las URL externas es diferente para los servidores de seguridad y los servidores de conexión.

- En una instancia del servidor de conexión, configure las URL externas editando las opciones del servidor de conexión en Horizon Administrator.
- En un servidor de seguridad, configure las URL externas cuando ejecute el programa de instalación del servidor de conexión. Puede usar Horizon Administrator para modificar una URL externa de un servidor de seguridad.

Configurar las URL externas de una instancia del servidor de conexión

Horizon Administrator permite configurar las URL externas para una instancia del servidor de conexión.

La URL externa del túnel seguro, la URL externa de PCoIP y la URL externa de Blast deben ser direcciones que los sistemas cliente utilicen para alcanzar esta instancia del servidor de conexión.

Requisitos previos

- Compruebe que las conexiones del túnel seguro y la puerta de enlace segura PCoIP estén habilitadas en la instancia del servidor de conexión. Consulte [Configurar la puerta de enlace segura PCoIP y las conexiones de túnel seguro](#).
- Para establecer la URL externa de Blast, compruebe que la puerta de enlace segura de Blast esté habilitada en la instancia del servidor de conexión. Consulte [Configurar la puerta de enlace segura Blast](#).

Procedimiento

- 1 En Horizon Administrator, haga clic en **Configuración de View > Servidores**.

- 2 Seleccione la pestaña Servidores de conexión; a continuación, seleccione una instancia del servidor de conexión y haga clic en **Editar**.

- 3 Escriba la URL externa del túnel seguro en el cuadro de texto **URL externa**.

La URL debe incluir el protocolo, un nombre de host que pueda resolver el cliente y el número de puerto.

Por ejemplo: **https://myserver.example.com:443**

Nota Puede usar la dirección IP si tiene que acceder a la instancia del servidor de conexión cuando el nombre del host no se puede resolver. Sin embargo, el host con el que contacta no coincide con el certificado TLS que está configurado para la instancia del servidor de conexión, lo cual resulta en un acceso bloqueado o un acceso con seguridad reducida.

- 4 Escriba la URL externa de la puerta de enlace segura PCoIP en el cuadro de texto **URL externa de PCoIP**.

En el caso de un entorno IPv4, especifique la URL externa de PCoIP como una dirección IP y el número de puerto 4172. En el caso de un entorno IPv6, puede especificar la dirección IP o el nombre de dominio plenamente cualificado y el número de puerto 4172. En ambos casos, no incluya el nombre del protocolo.

Por ejemplo, en un entorno IPv4: **10.20.30.40:4172**

Los clientes deben poder usar la URL para alcanzar el servidor de seguridad.

- 5 Escriba la URL externa de la puerta de enlace segura Blast en el cuadro de texto **URL externa de Blast**.

La URL debe incluir el protocolo HTTPS, un nombre de host que pueda resolver el cliente y el número de puerto.

Por ejemplo, **https://myserver.example.com:8443**

De forma predeterminada, la URL incluye el FQDN de la URL externa del túnel seguro y el número del puerto predeterminado, 8443. La URL debe contener el FQDN y el número de puerto que un sistema cliente puede utilizar para alcanzar este host del servidor de conexión.

- 6 Compruebe que todas las direcciones de este cuadro de diálogo permitan a los sistemas cliente alcanzar esta instancia del servidor de conexión.

- 7 Haga clic en **Aceptar**.

Modificar las URL externas de un servidor de seguridad

Puede usar Horizon Administrator para modificar las URL externas de un servidor de seguridad.

Estas URL externas se configuran inicialmente al instalar un servidor de seguridad en el programa de instalación del servidor de conexión.

La URL externa del túnel de seguridad, la URL externa de PCoIP y la URL externa de Blast deben ser direcciones que los sistemas cliente usen para alcanzar el servidor de seguridad.

Requisitos previos

- Verifique que las conexiones de túnel de seguridad y la puerta de enlace segura PCoIP estén habilitadas en la instancia del servidor de conexión vinculada con el servidor de seguridad. Consulte [Configurar la puerta de enlace segura PCoIP y las conexiones de túnel seguro](#).
- Para establecer la URL externa de Blast, verifique que la puerta de enlace segura de Blast esté habilitada en la instancia del servidor de conexión vinculada con el servidor de seguridad. Consulte [Configurar la puerta de enlace segura Blast](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.

- 2 En la pestaña Servidores de seguridad, seleccione el servidor de seguridad y haga clic en **Editar**.

- 3 Escriba la URL externa del túnel seguro en el cuadro de texto **URL externa**.

La URL debe incluir el protocolo, un nombre del host del servidor de seguridad que pueda resolver el cliente y el número de puerto.

Por ejemplo: `https://myserver.example.com:443`

Nota Puede usar la dirección IP si tiene acceso al servidor de seguridad cuando el nombre del host no se puede resolver. Sin embargo, el host que contacta no coincide con el certificado TLS que se configura para el servidor de seguridad, lo que deriva en un acceso bloqueado o un acceso con seguridad reducida.

- 4 Escriba la URL externa de la puerta de enlace segura PCoIP en el cuadro de texto **URL externa de PCoIP**.

En el caso de un entorno IPv4, especifique la URL externa de PCoIP como una dirección IP y el número de puerto 4172. En el caso de un entorno IPv6, puede especificar la dirección IP o el nombre de dominio y el número de puerto 4172. En ambos casos, no incluya el nombre del protocolo.

Por ejemplo, en un entorno IPv4: `10.20.30.40:4172`

Los clientes deben poder usar la URL para alcanzar el servidor de seguridad.

- 5 Escriba la URL externa de la puerta de enlace segura Blast en el cuadro de texto **URL externa de Blast**.

La URL debe incluir el protocolo HTTPS, un nombre de host que pueda resolver el cliente y el número de puerto.

Por ejemplo, `https://myserver.example.com:8443`

De forma predeterminada, la URL incluye el FQDN de la URL externa del túnel seguro y el número del puerto predeterminado, 8443. La URL debe contener el FQDN y el número de puerto que un sistema cliente puede usar para alcanzar el servidor de seguridad.

- 6 Verifique que todas las direcciones en este cuadro de diálogo permiten que los sistemas cliente alcancen este host del servidor de seguridad.
- 7 Haga clic en **Aceptar** para guardar los cambios.

Resultados

Horizon Administrator envía las URL externas actualizadas al servidor de seguridad. No necesita reiniciar el servidor de seguridad para que se apliquen los cambios.

Otorgar preferencia a nombres DNS cuando el servidor de conexión de Horizon devuelve información de direcciones

De forma predeterminada, cuando se envían las direcciones de equipos de escritorio y hosts RDS a clientes y puertas de enlace, el servidor de conexión de Horizon otorga preferencia a las direcciones IP. Puede cambiar este comportamiento predeterminado con un atributo LDAP de Horizon 7 que informe al servidor de conexión de Horizon que debe dar preferencia a los nombres DNS. En algunos entornos, se puede obtener una flexibilidad adicional para diseñar una infraestructura de red gracias a que el servidor de conexión devuelve nombres DNS a clientes y puertas de enlace.

Nota Este atributo LDAP de Horizon 7 reemplaza la funcionalidad por escritorios que proporcionó la opción de la directiva de grupo, `Connect using DNS Name`, en Horizon 6.0.x y versiones anteriores.

Los atributos LDAP de Horizon 7 afectan a clientes que ejecutan Horizon Client 3.3 para Windows o versiones posteriores, HTML Access 3.5 o versiones posteriores y puertas de enlace seguras en las instancias del servidor de conexión (no en servidores de seguridad).

Requisitos previos

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.
- 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 seguido del puerto 389.
 Por ejemplo: `localhost:389` o `miequipo.midominio.com:389`
- 5 En el objeto **CN=Common, OU=Global, OU=Properties**, establezca el valor del atributo **pae-PreferDNS** en 1.

Cuando este atributo está configurado en 1, el servidor de conexión devuelve un nombre DNS si está disponible y el destinatario tiene soporte para la resolución de nombres. De lo contrario, el servidor de conexión devuelve una dirección IP, si está disponible una dirección IP del tipo correcto según su entorno (IPv4 o IPv6).

Cuando este atributo no está configurado o está establecido en 0, el servidor de conexión devuelve una dirección IP, si está disponible una dirección IP del tipo correcto. De lo contrario, se devuelve un error de compatibilidad con la dirección IP.

Permitir HTML Access a través de un equilibrador de carga

Las instancias del servidor de conexión y los servidores de seguridad que se encuentran directamente detrás de un equilibrador de carga o una puerta de enlace de carga equilibrada deben conocer la dirección por la que los navegadores se conectarán al equilibrador de carga cuando los usuarios utilicen HTML Access.

Para las instancias del servidor de conexión y los servidores de seguridad que se encuentran detrás de una puerta de enlace, realice el procedimiento descrito en [Permitir HTML Access a través de una puerta de enlace](#).

Debe realizar este procedimiento en cada servidor de Horizon 7 que se encuentre detrás del equilibrador de carga o de la puerta de enlace de carga equilibrada.

Procedimiento

- 1 Cree o edite el archivo `locked.properties` en la carpeta de configuración de la puerta de enlace SSL en el host del servidor de seguridad o del servidor de conexión.

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

- 2 Agregue la propiedad `balancedHost` y configúrela para la dirección de la puerta de enlace.

Por ejemplo, si los usuarios escriben `https://view.example.com` en un navegador para llegar a cualquiera de los servidores de Horizon 7 de carga equilibrada, agregue `balancedHost=view.example.com` al archivo `locked.properties`.

- 3 Guarde el archivo `locked.properties`.
- 4 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Permitir HTML Access a través de una puerta de enlace

Las instancias del servidor de conexión y los servidores de seguridad que se encuentran directamente detrás de una puerta de enlace, como Access Point, deben conocer la dirección por la que los navegadores se conectarán a la puerta de enlace cuando los usuarios utilicen HTML Access.

Para las instancias del servidor de conexión y los servidores de seguridad que se encuentran detrás de un equilibrador de carga o una puerta de enlace de carga equilibrada, realice el procedimiento descrito en [Permitir HTML Access a través de un equilibrador de carga](#).

Debe realizar este procedimiento en cada servidor de Horizon 7 que se encuentre detrás de la puerta de enlace.

Procedimiento

- 1 Cree o edite el archivo `locked.properties` en la carpeta de configuración de la puerta de enlace SSL en el host del servidor de seguridad o del servidor de conexión.

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

- 2 Agregue la propiedad `portalHost` y configúrela para la dirección de la puerta de enlace.

Por ejemplo, si `https://view-gateway.example.com` es la dirección que los navegadores usan para acceder a Horizon 7 a través de la puerta de enlace, agregue `portalHost=view-gateway.example.com` al archivo `locked.properties`.

Si la instancia del servidor de conexión o el servidor de seguridad se encuentra detrás de varias puertas de enlace, puede especificar cada puerta de enlace simplemente agregando un número a la propiedad `portalHost`, por ejemplo:

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

También debe especificar varias propiedades `portalHost` si un único equipo de puerta de enlace se conoce por más de un nombre.

- 3 Guarde el archivo `locked.properties`.
- 4 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Reemplazar los puertos predeterminados para los servicios de Horizon 7

Durante la instalación, se configuran de forma predeterminada los servicios de View para la escucha en puertos de la red. En algunas organizaciones, estos puertos se cambian para cumplir las directivas de la organización o para evitar la contención. Puede cambiar los puertos predeterminados que usan los servicios de View Composer, de la puerta de enlace segura PCoIP, del servidor de seguridad y del servidor de conexión.

El cambio de puertos es una tarea de configuración opcional. Use los puertos predeterminados si la implementación no requiere que los cambie.

Para consultar una lista de los puertos TCP y UDP predeterminados que usan los servidores de Horizon 7, consulte el documento *Seguridad de Horizon 7*.

Reemplazar las NIC o los puertos HTTP predeterminados para las instancias del servidor de conexión de Horizon y los servidores de seguridad

Puede reemplazar las NIC o los puertos HTTP predeterminados para una instancia del servidor de conexión o el servidor de seguridad editando el archivo `locked.properties` en el equipo del servidor.

Es posible que la organización necesite que realice estas tareas para cumplir con sus directivas o para evitar la contención.

El puerto SSL predeterminado es 443. El puerto sin SSL predeterminado es 80.

El puerto que se especificó en la URL externa de túnel seguro no se modifica como resultado de los cambios que realice en los puertos siguiendo este procedimiento. Dependiendo de la configuración de red, es posible que también tenga que cambiar el puerto de la URL externa del túnel seguro.

Si el equipo del servidor tiene varias NIC, el equipo las escucha a todas de forma predeterminada. Puede seleccionar una NIC para que escuche el puerto configurado especificando la dirección IP que está enlazada a esa NIC.

Durante la instalación, Horizon 7 configura el Firewall de Windows para abrir los puertos predeterminados necesarios. Si cambia un número de puerto o la NIC que escucha, debe volver a configurar el Firewall de Windows para que abra los puertos predeterminados, de forma que los dispositivos cliente puedan conectarse al servidor.

Si cambia el número de puerto SSL y necesita que el redireccionamiento HTTP siga funcionando, también debe cambiar el número de puerto de este redireccionamiento. Consulte [Cambiar el número de puerto para el redireccionamiento HTTP al servidor de conexión](#).

Requisitos previos

Compruebe que el puerto que se especificó en la URL externa para esta instancia del servidor de conexión o del servidor de seguridad continuará siendo válido después de cambiar los puertos siguiendo este procedimiento.

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\locked.properties`

Las propiedades del archivo `locked.properties` distinguen entre mayúsculas y minúsculas.

- 2 Agregue la propiedad `serverPort`, `serverPortNonSsl` o ambas al archivo `locked.properties`.

Por ejemplo:

```
serverPort=4443
serverPortNonSsl=8080
```

- 3 (opcional) Si el equipo del servidor tiene varias NIC, seleccione una para que escuche a los puertos configurados.

Agregue las propiedades `serverHost` y `serverHostNonSsl` para especificar la dirección IP que está enlazada a la NIC designada.

Por ejemplo:

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

Normalmente, los agentes de escucha SSL y sin SSL están configurados para que usen la misma NIC. Sin embargo, si utiliza la propiedad `serverProtocol=http` para descargar SSL en las conexiones cliente, puede establecer la propiedad `serverHost` en una NIC independiente para proporcionar conexiones SSL en sistemas que se usan para iniciar Horizon Administrator.

Si configura las conexiones SSL y sin SSL para que usen la misma NIC, los puertos SSL y sin SSL no deben ser el mismo.

- 4 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Pasos siguientes

Si es necesario, configure manualmente el Firewall de Windows para abrir los puertos actualizados.

Reemplazar los puertos predeterminados o las NIC para la puerta de enlace segura PCoIP en las instancias del servidor de conexión de Horizon y en los servidores de seguridad

Puede reemplazar los puertos predeterminados o las NIC que usa un servicio de la puerta de enlace segura PCoIP que se ejecuta en la instancia del servidor de conexión o en el servidor de seguridad. Es posible que la organización necesite que realice estas tareas para cumplir con sus directivas o para evitar la contención.

Para las conexiones UDP y TCP del cliente, la puerta de enlace segura PCoIP escucha el puerto 4172 de forma predeterminada. Para las conexiones UDP del escritorio remoto, la puerta de enlace segura PCoIP escucha el puerto 55000 de forma predeterminada.

El puerto que se especificó en la URL externa de PCoIP no se modifica como resultado de los cambios que realice en los puertos siguiendo este procedimiento. Dependiendo de la configuración de red, es posible que también tenga que cambiar el puerto de la URL externa de PCoIP.

Si el equipo en el que la puerta de enlace segura PCoIP se está ejecutando tiene varias NIC, el equipo escucha a todas las NIC de forma predeterminada. Puede seleccionar una NIC para que escuche los puertos configurados especificando la dirección IP que está enlazada a esa NIC.

Requisitos previos

Compruebe que el puerto que se especificó en la URL externa de PCoIP en la instancia del servidor de conexión o del servidor de seguridad continuará siendo válido después de cambiar los puertos siguiendo este procedimiento.

Procedimiento

- 1 Inicie el Editor del Registro de Windows en el servidor de conexión o en el equipo del servidor de seguridad donde se ejecuta la puerta de enlace segura PCoIP.

- 2 Diríjase a la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway.
- 3 En esta clave de registro, agregue uno o varios de los siguientes valores de la cadena (REG_SZ) cuando actualice los números de puerto.

Por ejemplo:

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

- 4 (opcional) Si el equipo en el que la puerta de enlace segura PCoIP se está ejecutando tiene varias NIC, seleccione una para escuchar los puertos configurados.

En la misma clave de registro, agregue los siguientes valores de la cadena (REG_SZ) para especificar la dirección IP que está enlazada a la NIC designada.

Por ejemplo:

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

Si configura las conexiones externas e internas para que usen la misma NIC, los puertos UDP interno y externo no deben ser el mismo.

- 5 Reinicie el servicio de la puerta de enlace segura PCoIP de VMware Horizon View para que se realicen los cambios.

Reemplazar el puerto de control predeterminado para la puerta de enlace segura PCoIP en las instancias del servidor de conexión y en los servidores de seguridad

Puede reemplazar el puerto predeterminado que controla el servicio de la puerta de enlace segura PCoIP (PSG) que se ejecuta en una instancia del servidor de conexión o en un servidor de seguridad. Es posible que deba realizar esta tarea para evitar la contención del puerto.

La puerta de enlace segura PCoIP escucha las conexiones de control en el puerto TCP local 50060 de forma predeterminada.

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 en el que se esté ejecutando la puerta de enlace segura PCoIP.

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

Las propiedades del archivo `locked.properties` distinguen entre mayúsculas y minúsculas.

- 2 Agregue la propiedad `psgControlPort` al archivo `locked.properties`.

Por ejemplo:

```
psgControlPort=52060
```

- 3 Inicie el Editor del registro de Windows en el mismo equipo.
- 4 Diríjase a la clave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.
- 5 En la clave del registro, agregue el siguiente valor de cadena (REG_SZ) con su número de puerto actualizado.

Por ejemplo:

```
TCPControlPort "52060"
```

Nota El número de puerto para `TCPControlPort` es el mismo que para `psgControlPort`.

- 6 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Reemplazar el puerto predeterminado para View Composer

El certificado SSL que usa el servicio de View Composer está enlazado a un puerto de forma predeterminada. Puede reemplazar el puerto predeterminado con la utilidad `SviConfig ChangeCertificateBindingPort`.

Cuando especifique un nuevo puerto con la utilidad `SviConfig ChangeCertificateBindingPort`, la utilidad anula el enlace del certificado de View Composer a ese puerto y lo enlaza al puerto nuevo.

Durante la instalación, View Composer configura el Firewall de Windows para abrir el puerto predeterminado necesario. Si cambia el puerto, debe volver a configurar de forma manual el Firewall de Windows para que abra el puerto actualizado y asegure la conectividad al servicio de View Composer.

Requisitos previos

Compruebe que el puerto que especifique esté disponible.

Procedimiento

- 1 Detenga el servicio de View Composer.
- 2 Abra una ventana de símbolo de sistema en el host de Windows Server donde View Composer se encuentra instalado.
- 3 Diríjase al archivo ejecutable `SviConfig`.

El archivo se encuentra con la aplicación View Composer. La ruta predeterminada es `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

- 4 Escriba el comando `SvcConfig ChangeCertificateBindingPort`.

Por ejemplo:

```
svconfig -operation=ChangeCertificateBindingPort
        -Port=número de puerto
```

donde `-port=número de puerto` es el nuevo puerto al que View Composer enlaza el certificado. El parámetro `-port=número de puerto` es obligatorio.

- 5 Reinicie el servicio de View Composer para que se apliquen los cambios.

Pasos siguientes

Si es necesario, vuelva a configurar de forma manual el Firewall de Windows en el servidor View Composer para que abra el puerto actualizado.

Cambiar el número de puerto para el redireccionamiento HTTP al servidor de conexión

Si reemplaza el puerto predeterminado 443 en un servidor de Horizon 7 y desea permitir el redireccionamiento HTTP para los Horizon Client que intenten conectarse al puerto 80, debe configurar el archivo `locked.properties` en un servidor de Horizon 7.

Nota Este procedimiento no tiene efecto si descarga SSL en un dispositivo intermedio. Con la descarga SSL en las instalaciones, el puerto HTTP del servidor de Horizon 7 proporciona servicio a los clientes.

Requisitos previos

Compruebe que estableció un número diferente de puerto predeterminado al 443. Si usa los valores predeterminados que se configuraron durante la instalación, no es necesario que realice este procedimiento para conservar la regla de redireccionamiento HTTP.

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\locked.properties`

Las propiedades del archivo `locked.properties` distinguen entre mayúsculas y minúsculas.

- 2 Agregue las siguientes líneas al archivo `locked.properties`:

```
frontMappingHttpDisabled.1=5:*:moved:https::puerto
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

En las líneas anteriores, la variable `puerto` es el número de puerto al que el cliente se debe conectar.

Si no agrega las líneas anteriores, el `puerto` sigue siendo el 443.

- 3 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Evitar el redireccionamiento HTTP para las conexiones cliente al servidor

Los intentos de Horizon Client de conectarse a servidores de Horizon 7 a través de HTTP se redireccionan de forma silenciosa a HTTPS. En algunas implementaciones, es posible que desee evitar que los usuarios introduzcan **http://** en sus navegadores web y obligarles a usar HTTPS. Para evitar el redireccionamiento HTTP de Horizon Client, debe configurar el archivo `locked.properties` en el servidor de Horizon 7.

Nota Este procedimiento no tiene efecto si descarga SSL en un dispositivo intermedio. Con la descarga SSL en las instalaciones, el puerto HTTP del servidor de Horizon 7 proporciona servicio a los clientes.

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\locked.properties`

Las propiedades del archivo `locked.properties` distinguen entre mayúsculas y minúsculas.

- 2 Agregue las siguientes líneas al archivo `locked.properties`:

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

- 3 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Habilitar el acceso remoto para los contadores de rendimiento de Horizon 7 en los servidores de conexión

Los contadores de rendimiento de Horizon 7 están disponibles de forma local en un servidor de conexión, pero devuelven el valor 0 cuando se accede a ellos desde otro equipo. Para habilitar el acceso remoto a los contadores de rendimiento de Horizon 7 en los servidores de conexión, debe configurar el puerto del entorno del servidor de conexión en el registro.

Procedimiento

- 1 Inicie el Editor del Registro de Windows.
- 2 Diríjase a la clave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager`.
- 3 Agregue un nuevo valor de cadena (REG_SZ), Puerto de administración.
- 4 Establezca el valor Puerto de administración a **32111**.

Configuración de tamaño de Windows Server para admitir la implementación

Para admitir una implementación mayor de escritorios remotos, puede configurar los equipos Windows Server en los que instale el servidor de conexión. En cada uno, puede elegir el tamaño del archivo de paginación.

En los equipos Windows Server 2008 R2 y Windows Server 2012 R2, la configuración de tamaño de la máquina virtual Java, los puertos efímeros y la tabla hash de CPS está establecida de forma predeterminada. Estos ajustes garantizan que los equipos tengan los recursos adecuados para funcionar correctamente con carga de usuarios esperada.

Cambiar el tamaño de la memoria del servidor de conexión de Horizon

En un equipo del servidor de conexión, son necesarios 10 GB de memoria para las implementaciones de 50 escritorios remotos o más. Un equipo Windows Server con al menos 10 GB de memoria se configura automáticamente para admitir aproximadamente 2.000 sesiones de túnel simultáneas, el número máximo que el servidor de conexión puede admitir.

Configure menos de 10 GB de memoria solo para implementaciones pequeñas y de prueba de conceptos. Con la memoria mínima de 4 GB, una configuración puede admitir aproximadamente 500 sesiones de túnel simultáneas, valor adecuado para las implementaciones pequeñas y de prueba de conceptos.

Sin embargo, como la implementación puede aumentar a medida que se agregan usuarios al entorno, VMware recomienda que configure siempre al menos 10 GB de memoria. Realice una excepción solo cuando sepa que el entorno no crecerá y la memoria no esté disponible.

Si instala el servidor de conexión con menos de 10 GB de memoria, Horizon 7 proporciona recomendaciones de memoria mediante la generación de mensajes de advertencia una vez completada la instalación. Un evento que se activa cada 12 horas indica que la instancia del servidor de conexión de View está configurada con una pequeña cantidad de memoria física.

Si aumenta la memoria del equipo a 10 GB para admitir una implementación más grande, reinicie el servidor de conexión para asegurarse de que el tamaño de la pila de la JVM aumente automáticamente hasta llegar al valor recomendado. No es necesario que reinstale el servidor de conexión.

Importante No cambie el tamaño de la pila de la JVM en equipos Windows Server de 64 bits. El cambio de este valor puede hacer que el comportamiento del servidor de conexión sea inestable. En equipos de 64 bits, el servicio del servidor de conexión establece el tamaño de la pila de la JVM de acuerdo con la memoria física.

Para obtener información adicional sobre los requisitos de memoria y de hardware del servidor de conexión, consulte [Requisitos de hardware para el servidor de conexión de Horizon](#).

Si desea obtener recomendaciones de memoria y hardware para utilizar el servidor de conexión en una implementación grande, consulte el apartado sobre los máximos del servidor de conexión y la configuración de las máquinas virtuales en *Planificación de la arquitectura de Horizon 7*.

Configurar las opciones de los archivos de paginación del sistema

Puede cambiar la configuración de los archivos de paginación del sistema para optimizar la memoria virtual en los equipos Windows Server en los cuales están instaladas las instancias del servidor de conexión.

Cuando Windows Server está instalado, Windows calcula un tamaño de archivo de paginación máximo e inicial basado en la memoria física instalada en el equipo. Estas opciones predeterminadas se mantienen aunque reinicie el equipo.

Si el equipo Windows Server es una máquina virtual, puede cambiar el tamaño de la memoria a través de vCenter Server. Sin embargo, si Windows usa la opción predeterminada, el tamaño de archivo de paginación del sistema no se ajusta al nuevo tamaño de la memoria.

Procedimiento

- 1 En el equipo Windows Server en el que se instaló el servidor de conexión, diríjase al cuadro de diálogo Memoria virtual.

De forma predeterminada, la opción **Personalizar tamaño** está seleccionada. Aparece un tamaño de archivo de paginación inicial y máximo.

- 2 Haga clic en **Tamaño administrado por el sistema**.

Resultados

Windows recalcula continuamente el tamaño del archivo de paginación del sistema basado en el uso de la memoria actual y de la memoria disponible.

Configurar informes de eventos

10

Puede crear una base de datos de eventos para registrar información sobre los eventos de Horizon 7. Además, si utiliza un servidor syslog, puede configurar el servidor de conexión para que envíe eventos a un servidor syslog o crear un archivo plano de eventos en formato syslog.

Este capítulo incluye los siguientes temas:

- [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7](#)
- [Preparar una base de datos SQL Server para los informes de eventos](#)
- [Configurar la base de datos de eventos](#)
- [Configurar el registro de eventos para servidores Syslog](#)

Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7

Para crear una base de datos de eventos, agréguela al servidor de una base de datos existente. A continuación, puede utilizar un software de informe empresarial para analizar los eventos en la base de datos.

Implemente el servidor de base de datos para la base de datos de eventos en un servidor dedicado, de modo que el registro de eventos no afecte al aprovisionamiento u otras actividades críticas para las implementaciones de Horizon 7.

Nota No es necesario crear un origen de datos ODBC para esta base de datos.

Requisitos previos

- Compruebe que posee un servidor de base de datos de Oracle o Microsoft SQL Server compatible con el sistema al que la instancia del servidor de conexión tiene acceso. Para obtener una lista de versiones de bases de datos compatibles, consulte [Requisitos de base de datos para View Composer y para bases de datos de eventos](#).
- Compruebe que posea los privilegios necesarios para crear una base de datos y un usuario en el servidor de la base de datos.

- Si no está familiarizado con el proceso para crear bases de datos en los servidores de base de datos de Microsoft SQL Server, revise los pasos en [Agregar una base de datos de View Composer a SQL Server](#).
- Si no está familiarizado con el proceso para crear bases de datos en servidores de base de datos de Oracle, revise los pasos en [Agregar una base de datos de View Composer a Oracle 12c o 11g](#).

Procedimiento

- 1 Agregue una nueva base de datos al servidor y asígnele un nombre descriptivo, por ejemplo, EventosHorizon.

En el caso de bases de datos de Oracle 12c u 11g, asigne también un identificador de sistema de Oracle (SID) para configurar la base de datos de eventos en Horizon Administrator.

- 2 Agregue un usuario para esta base de datos con permiso para crear tablas, vistas y, en el caso de Oracle, desencadenadores y secuencias, además de permiso para leer y escribir en estos objetos.

En el caso de una base de datos de Microsoft SQL Server, no utilice el modelo de seguridad de autenticación integrada de Windows. Asegúrese de utilizar el método de autenticación de SQL Server.

Resultados

Se creará la base de datos, pero no se instalará el esquema hasta que configure la base de datos en Horizon Administrator.

Pasos siguientes

Siga las instrucciones de [Configurar la base de datos de eventos](#).

Preparar una base de datos SQL Server para los informes de eventos

Si desea utilizar Horizon Administrator para configurar una base de datos de eventos en Microsoft SQL Server, debe configurar las propiedades de TCP/IP adecuadas y verificar que el servidor utilice la autenticación de SQL Server.

Requisitos previos

- Crear una base de datos SQL Server para los informes de eventos. Consulte [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7](#).
- Compruebe que disponga de los privilegios de base de datos necesarios para configurar la base de datos.
- Compruebe que el servidor de la base de datos utilice el método de autenticación de SQL Server. No utilice la autenticación de Windows.

Procedimiento

- 1 Abra el administrador de configuración de SQL Server y expanda **SQL Server AAAA Configuración de red**.
- 2 Seleccione **Protocolos de nombre_servidor**.
- 3 En la lista de protocolos, haga clic con el botón secundario en **TCP/IP** y seleccione **Propiedades**.
- 4 Elija **Sí** para la propiedad **Habilitada**.
- 5 Compruebe que haya un puerto asignado o asigne uno si es necesario.
Para obtener información sobre los puertos dinámicos y estáticos y cómo asignarlos, consulte la ayuda en línea del administrador de configuración de SQL Server.
- 6 Compruebe que el puerto no esté bloqueado por un firewall.

Pasos siguientes

Utilice Horizon Administrator para conectar la base de datos al servidor de conexión. Siga las instrucciones de [Configurar la base de datos de eventos](#).

Configurar la base de datos de eventos

La base de datos de eventos almacena información sobre los eventos de Horizon 7 en forma de registros en una base de datos en lugar de hacerlo en un archivo de registro.

Configure una base de datos de eventos después de instalar una instancia del servidor de conexión. Solo es necesario configurar un host en un grupo de servidores de conexión. El resto de hosts del grupo están configurados de forma automática.

Nota La seguridad de la conexión de la base de datos entre el servidor de conexión y una base de datos externa es responsabilidad del administrador, aunque se limite el tráfico de eventos a la información sobre el estado del entorno de Horizon 7. Si desea tomar más precauciones, puede asegurar este canal a través de IPsec u otros medios, o bien puede implementar la base de datos de forma local en el equipo del servidor de conexión.

Puede usar las herramientas de informe de la base de datos de Oracle o Microsoft SQL Server para examinar los eventos de las tablas de la base de datos. Para obtener más información, consulte el documento *Integración de Horizon 7*.

También puede generar eventos de Horizon 7 en formato syslog para que los software de análisis de terceros puedan acceder a los datos de eventos. Puede usar el comando `vdmadmin` con la opción `-I` para registrar mensajes de eventos de Horizon 7 en formato syslog en archivos de registro de eventos. Consulte "Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción `-I`" en el documento *Administración de Horizon 7*.

Requisitos previos

Necesita la siguiente información para configurar una base de datos de eventos:

- La dirección IP o nombre de DNS del servidor de base de datos.
- El tipo del servidor de la base de datos: Oracle o Microsoft SQL Server. Para obtener más información sobre los servidores de base de datos compatibles, consulte [Versiones de Active Directory, de base de datos y de vSphere admitidas en un entorno IPv6](#).
- El número de puerto que se usa para acceder al servidor de la base de datos. El predeterminado es 1521 para Oracle y 1433 para SQL Server. Para SQL Server, si el servidor de la base de datos es una instancia con nombre o si usa SQL Server Express, es posible que necesite determinar el número de puerto. Consulte el artículo de la KB de Microsoft sobre cómo conectarse a una instancia con nombre de SQL Server, disponible en <http://support.microsoft.com/kb/265808>.
- El nombre de la base de datos del evento que creó en el servidor de la base de datos. Consulte [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7](#).

En el caso de bases de datos de Oracle 12c u 11g, debe usar un identificador de sistema de Oracle (SID) como el nombre de la base de datos cuando configure la base de datos de eventos en Horizon Administrator.

- El nombre y la contraseña del usuario que creó para esta base de datos. Consulte [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7](#).

Use la autenticación de SQL Server para este usuario. No use el método de autenticación del modelo de seguridad de autenticación integrada de Windows.

- Un prefijo para las tablas de la base de datos de eventos, por ejemplo, VE_. El prefijo habilita que se comparta la base de datos en las instalaciones de Horizon 7.

Nota Debe introducir caracteres válidos para el software de la base de datos que está utilizando. No se comprueba la sintaxis del prefijo cuando completa el cuadro de diálogo. Si introduce caracteres que no son válidos para el software de la base de datos que está utilizando, se produce un error cuando el servidor de conexión intenta conectarse al servidor de la base de datos. El archivo de registro muestra todos los errores, incluidos este y otros que devuelva el servidor de la base de datos si el nombre de la base de datos no es válido.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración de eventos**.
- 2 En la sección **Base de datos de eventos**, haga clic en **Editar**, introduzca la información en los campos proporcionados y haga clic en **Aceptar**.

- 3 (opcional) En la ventana Configuración de evento, haga clic en **Editar**, cambie el tiempo establecido para mostrar los eventos y el número de días para clasificar los eventos como nuevos y, a continuación, haga clic en **Aceptar**.

Estas opciones pertenecen al tiempo durante el cual los eventos aparecen en la interfaz de Horizon Administrator. Después, los eventos solo están disponibles en las tablas históricas de la base de datos.

La ventana de la configuración de la base de datos muestra la configuración actual de la base de datos del evento.

- 4 Seleccione **Supervisión > Eventos** para verificar que la conexión a la base de datos del evento sea correcta.

Si la conexión no es correcta, aparece un mensaje de error. Si usa SQL Express o si usa una instancia con nombre de SQL Server, es posible que necesite determinar el número de puerto correcto, como se mencionó en los requisitos.

Resultados

En el Panel de Horizon Administrator, el estado del componente del sistema muestra el servidor de la base de datos de eventos bajo el encabezado de la base de datos de informes.

Configurar el registro de eventos para servidores Syslog

Puede generar eventos de Horizon 7 en formato syslog para que los software de análisis puedan acceder a los datos de eventos.

Solo es necesario configurar un host en un grupo de servidores de conexión. El resto de hosts del grupo están configurados de forma automática.

Si habilita el registro de eventos basados en archivo, los eventos se acumulan en un archivo de registro local. Si especifica un recurso compartido de archivo, estos archivos de registros se mueven a ese recurso.

- Si usa un archivo local solo para solucionar problemas de forma rápida durante la configuración, antes de que se configure la base de datos de eventos, tendrá diversas maneras de ver los eventos.

El tamaño máximo del directorio local para los registros de eventos es 300 MB, incluidos los archivos de registro cerrados, antes de que se eliminen los archivos más antiguos. El destino predeterminado de la salida syslog es %PROGRAMDATA%\VMware\VDM\events\.

- Use una ruta UNC para guardar los archivos de registro de eventos a largo plazo, si no tiene un servidor syslog o si el servidor syslog actual no cumple sus necesidades.

Puede usar un comando `vdmadmin` para configurar el registro de eventos basados en archivo en formato syslog. Consulte el tema sobre la generación de mensajes de registro de eventos de Horizon 7 en formato syslog con la opción `-I` del comando `vdmadmin`, en el documento *Administración de Horizon 7*.

Importante Los datos syslog se envían a través de la red sin ningún cifrado basado en software y pueden contener información confidencial, como los nombres de usuarios. VMware recomienda el uso de la seguridad de nivel de vínculo, como IPSEC, para evitar la posibilidad de que estos datos se puedan supervisar a través de la red.

Requisitos previos

Necesita la siguiente información para configurar el servidor de conexión de forma que los eventos se puedan registrar en formato syslog, que se envíen a un servidor syslog o ambas opciones:

- Si tiene pensado usar un servidor syslog para escuchar los eventos de Horizon 7 en un puerto UDP, debe tener el nombre DNS o la dirección IP del servidor syslog y el número de puerto UDP. El puerto UDP predeterminado es el 514.
- Si tiene pensado recopilar registros en formato de archivo plano, debe tener la ruta UNC al recurso compartido de archivo y la carpeta en la que se almacenan los archivos de registro. También debe tener el nombre de usuario, de dominio y la contraseña de una cuenta que tenga permiso para escribir en el recurso compartido de archivo.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración de eventos**.
- 2 (opcional) En el área **Syslog**, para configurar que los servidores de conexión envíen eventos a un servidor syslog, haga clic en **Agregar** junto a **Enviar a servidores syslog** y proporcione el nombre del servidor o la dirección IP y el número de puerto UDP.
- 3 (opcional) En el área **Eventos del sistema de archivos**, elija si desea habilitar o no la generación y el almacenamiento de los mensajes de registro de eventos en los archivos de registro y en formato syslog.

Opción	Descripción
Always	Siempre genera y almacena los mensajes de registro de eventos en los archivos de registro y en formato syslog.
Registrar en archivo en caso de error (predeterminada)	Registra los eventos de auditoría en un archivo de registro cuando se produce un problema al escribir eventos en la base de datos de eventos o en el servidor syslog. Esta opción está habilitada de forma predeterminada.
Never	Nunca genera ni almacena los mensajes de registro de eventos en los archivos de registro en formato Syslog.

Los archivos de registro se utilizan de forma local si no especifica una ruta UNC a un recurso compartido de archivo.

- 4 (opcional) Para almacenar los mensajes de registro de eventos de Horizon 7 en un recurso compartido de archivos, haga clic en **Agregar**, situado junto a **Copiar a ubicación** y proporcione la ruta UNC a la carpeta y al archivo de recurso compartido en el que se almacenan los archivos de registro además del nombre de usuario, el nombre de dominio y la contraseña de una cuenta que tenga permiso para escribir en el recurso compartido de archivos.

Un ejemplo de una ruta UNC es:

```
\\syslog-server\folder\file
```