

Actualizaciones de Horizon 7

13 de diciembre de 2018
VMware Horizon 7 7.7



vmware®

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

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

El sitio web de VMware también ofrece las actualizaciones de producto más recientes.

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2009–2018 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y marca comercial](#).

Contenido

Actualizaciones de Horizon 7	5
1 Descripción general de la actualización de Horizon 7	6
2 Aplicar una rama ampliada del servicio	9
3 Actualizar la aplicación cliente	10
4 Requisitos del sistema para las actualizaciones de Horizon 7 Server	12
Matriz de compatibilidad para varias versiones de los componentes de Horizon 7	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
Actualizar requisitos para View Composer	15
Requisitos del servidor de conexión de Horizon	16
Requisitos de hardware para el servidor de conexión de Horizon	16
Sistemas operativos compatibles con el servidor de conexión de Horizon	17
Requisitos para actualizar el servidor de conexión de Horizon	17
Sistemas operativos compatibles con Horizon Agent	19
5 Actualizar los componentes de Horizon 7 Server	21
Actualizar View Composer	21
Preparar vCenter Server y View Composer para una actualización	22
Actualizar View Composer	24
Habilitar TLSv1.0 en vCenter y conexiones ESXi desde View Composer	25
Habilitar la autenticación implícita de acceso para View Composer	26
Actualizar de forma manual la base de datos de View Composer	27
Migrar View Composer a otro equipo	30
Actualizar el servidor de conexión de Horizon	37
Preparar el servidor de conexión para una actualización	37
Actualizar los servidores de conexión en un grupo replicado	38
Habilitar TLSv1.0 en conexiones de vCenter desde el servidor de conexión	42
Actualizar a la versión más reciente del servidor de conexión en un equipo diferente	43
Crear un grupo replicado después de revertir un servidor de conexión a una snapshot	44
Actualizar los servidores de seguridad	45
Preparar el servidor de seguridad para una actualización	45
Actualizar los servidores de seguridad y sus servidores de conexión emparejados	46

- Reemplazar un servidor de seguridad por un dispositivo Unified Access Gateway 49
 - Actualizar un entorno de Arquitectura de Cloud Pod 50
 - Actualizar Horizon 7 Servers para permitir HTML Access 51
 - Actualizar vCenter Server 51
 - Aceptar la huella digital de un certificado TLS predeterminado 53
 - Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7 54
- 6 Actualizar los hosts ESXi y sus máquinas virtuales 56**
- 7 Actualizar escritorios virtuales y publicados 59**
 - Requisitos relacionados con la seguridad para actualizar los escritorios 59
 - Actualizar hosts RDS que proporcionan escritorios basados en sesión 59
 - Actualizar View Agent o Horizon Agent 61
 - Actualizar grupos de escritorios de View Composer 63
 - Actualizar grupos de escritorios de clones instantáneos 65
- 8 Actualizar el dispositivo virtual Horizon 7 Cloud Connector 68**
 - Solucionar problemas de la actualización del dispositivo virtual Horizon 7 Cloud Connector 69
- 9 Tareas posteriores a la actualización para habilitar nuevas funciones en la configuración de Horizon 71**
 - Cambiar el modo de seguridad del mensaje JMS a Mejorada 71
 - Tareas de actualización de grupos de escritorios para usar la recuperación de espacio 73
 - Actualizar tareas si usa los almacenes de datos VMware vSAN 74
 - Actualizar de un almacén de datos sin vSAN a un almacén de datos con vSAN 74
 - Actualizar desde la versión 1 del formato de disco vSAN 75
 - Actualizar desde Horizon View 5.3.x en un almacén de datos vSAN 77
 - Configurar la página del portal web de VMware Horizon para los usuarios finales 79
- 10 Actualizar los componentes de vSphere independientemente en un entorno de Horizon 7 84**

Actualizaciones de Horizon 7

El documento *Actualizaciones de Horizon 7* proporciona instrucciones para actualizar las últimas versiones de mantenimiento de Horizon View 5.3, VMware Horizon™ 6 (con View), o bien VMware Horizon 6 versión 6.1 o 6.2 a VMware Horizon 7. También puede usar esta guía cuando actualice a las versiones de mantenimiento de Horizon 7.

Si también está actualizando la versión de VMware vSphere®, esta guía le proporcionará información sobre qué pasos de esa actualización debe realizar en varias etapas de la actualización de Horizon 7.

Público al que se dirige

Esta guía está dirigida a cualquier usuario que necesite actualizar a la última versión de este producto. Asimismo, está destinada a administradores de sistemas Microsoft Windows o Linux con experiencia que estén familiarizados con la tecnología de las máquinas virtuales y las operaciones de los centros de datos.

Descripción general de la actualización de Horizon 7

1

La actualización de una implementación de Horizon 7 empresarial incluye varias tareas de nivel elevado. La actualización es un proceso de varias fases en el que los procedimientos se deben realizar siguiendo un orden determinado. Actualice View Composer antes de actualizar Horizon Connection Server y el resto de Horizon 7 Servers.

Importante Con la versión 6.2 y posteriores de Horizon 6, puede instalar los componentes de Horizon 7 para que se ejecuten en modo FIPS. Horizon 7 no admite la actualización de una instalación que no sea FIPS a una que sí lo sea. Horizon admite la actualización de la versión 6.2 de Horizon 6 en modo FIPS a Horizon 7 en modo FIPS. Si necesita realizar una instalación nueva, consulte "Instalar Horizon 7 en modo FIPS" en el documento *Instalación de Horizon 7*.

Durante una actualización, Horizon 7 no admite las operaciones de mantenimiento y aprovisionamiento de View Composer. Las operaciones como el aprovisionamiento y la recomposición de escritorios de clones vinculados no se admiten durante el periodo de transición cuando algún servidor de Horizon 7 sigue ejecutando una versión anterior. Puede realizar correctamente estas operaciones únicamente cuando todas las instancias del servidor de conexión y de View Composer estén actualizadas.

Debe completar el proceso de actualización siguiendo un orden específico. El orden también es importante en cada fase de actualización.

Nota Esta descripción general hace referencia a las actualizaciones de versiones de mantenimiento, secundarias y principales.

La cantidad de las siguientes tareas que necesita completar depende de los componentes de Horizon 7 que use en la implementación.

- 1 Actualice el software Horizon Client que se ejecuta en los dispositivos cliente de los usuarios finales. Consulte [Capítulo 3 Actualizar la aplicación cliente](#).
- 2 En las máquinas virtuales o los equipos físicos que alojan View Composer y VMware® vCenter Server™, realice copias de seguridad y detenga de forma temporal algunas tareas programadas. Consulte [Preparar vCenter Server y View Composer para una actualización](#).

Si tiene un View Composer independiente, que está instalado en un equipo separado de vCenter Server, es necesario que haga una copia de seguridad únicamente de la base de datos de View Composer y del certificado TLS/SSL de View Composer. Puede programar una actualización de vCenter Server de forma independiente, si también desea actualizar 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.

- 3 Actualice View Composer en el host existente o mígrelo a un equipo nuevo. Consulte [Actualizar View Composer](#).
- 4 En las máquinas virtuales o en los equipos físicos que alojan las instancias del servidor de conexión, realice las copias de seguridad y registre varias opciones del sistema y de configuración. Consulte [Preparar el servidor de conexión para una actualización](#).

Si tiene varias instancias del servidor de conexión en un grupo replicado, realice las copias de seguridad y registre las opciones de configuración solamente para una instancia del grupo. Para otras tareas de preparación, puede realizarlas en una instancia al mismo tiempo, antes de realizar la actualización de esa instancia del servidor.

- 5 Actualice las instancias del servidor de conexión que no están emparejadas con los servidores de seguridad. Consulte [Actualizar los servidores de conexión en un grupo replicado](#).

En un entorno de producción típico que consta de dos o más instancias del servidor de conexión dirigida por un equilibrador de carga, si necesita minimizar el tiempo de inactividad, puede eliminar las instancias del servidor de conexión del clúster de carga equilibrada una a una mientras las actualiza.

Importante Tras actualizar una instancia del servidor de conexión a la versión más reciente, no puede cambiar dicha instancia a una versión anterior. Tras actualizar todas las instancias del servidor de conexión de un grupo replicado, no puede agregar otra instancia que se ejecute en una versión anterior.

- 6 Si usa servidores de seguridad, realice las copias de seguridad y registre varias opciones de sistema y de configuración. Consulte [Preparar el servidor de seguridad para una actualización](#).

Para minimizar el tiempo de inactividad, puede realizar estas tareas en un servidor de seguridad al mismo tiempo, antes de realizar la actualización de ese servidor.
- 7 Si usa servidores de seguridad, actualice cada servidor de seguridad y su instancia del servidor de conexión emparejada. Si actualiza estas parejas una a una, puede conseguir que no haya tiempo de inactividad al eliminar cada servidor de seguridad del grupo de carga equilibrada, actualizar la pareja y, a continuación, volver a agregar el servidor de seguridad al grupo. Consulte [Actualizar los servidores de seguridad y sus servidores de conexión emparejados](#).
- 8 Actualice las directivas de grupo usadas en Active Directory. Consulte [Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7](#).
- 9 Si también está actualizando los componentes de VMware vSphere, consulte vCenter Server. Consulte [Actualizar vCenter Server](#).

Durante la actualización de vCenter Server, no se desconectarán las sesiones de las aplicaciones y los escritorios remotos existentes. Los escritorios remotos que están en estado de aprovisionamiento no se encenderán durante la actualización de vCenter Server y los nuevos escritorios no se iniciarán, así como las operaciones de View Composer no se permiten durante la actualización de vCenter Server.

- 10 Si también está actualizando vSphere, actualice los hosts y las máquinas virtuales de VMware[®] ESXi[™]. Consulte [Capítulo 6 Actualizar los hosts ESXi y sus máquinas virtuales](#).

Los hosts ESXi se pueden actualizar sin tiempo de inactividad utilizando vMotion para asignar las máquinas virtuales a otro host del clúster, si los hosts están configurados en un entorno de clústeres.

- 11 Si actualmente usa servidores de Windows Terminal Services como orígenes de los escritorios, actualice a Windows Server 2008 R2 o a una versión posterior y compruebe que la función Host RDS esté instalada. Consulte [Actualizar hosts RDS que proporcionan escritorios basados en sesión](#)
- 12 Actualice el software Horizon[™] Agent o el software View Agent[™] que se ejecuta en las máquinas virtuales o en el equipo físico que se usan como orígenes de los escritorios, como escritorios de clones vinculados de un grupo y como los escritorios individuales de un grupo manual. Consulte [Actualizar View Agent o Horizon Agent](#).
- 13 Use los orígenes del escritorio de la máquina virtual actualizada recientemente para crear grupos de escritorios actualizados. Consulte [Actualizar grupos de escritorios de View Composer](#).
- 14 Si usa la función Arquitectura de Cloud Pod, consulte [Actualizar un entorno de Arquitectura de Cloud Pod](#).

Como algunos comandos pueden actualizar simultáneamente más de una etapa, VMware le recomienda que sea consciente de los cambios irreversibles que se producen en cada etapa antes de que actualice los entornos de producción.

Importante La función VMware View[®] Client with Local Mode, para usar los escritorios sin conexión, se eliminó y, por lo tanto, esta descripción general no incluye los pasos necesarios para actualizar las instancias del servidor de transferencias de View y View Client with Local Mode. En lugar de la función Modo local, VMware recomienda que use VMware[®] Mirage[™], que se incluye con VMware Horizon 6.0 y versiones posteriores. Para obtener más información, consulte las notas de la versión de Horizon 7, disponibles en <https://docs.vmware.com/es/VMware-Horizon-7/index.html>.

Aplicar una rama ampliada del servicio

2

Una rama ampliada del servicio (ESB) es una opción disponible a partir de Horizon 7.5, VMware App Volumes 2.14 y VMware User Environment Manager 9.4.0. Contiene actualizaciones periódicas de Service Pack (SP), que incluyen soluciones de problemas importantes y correcciones de seguridad.

Si decide no actualizar a la última versión de Horizon y prefiere seguir utilizando la misma versión, puede implementar una ESB y seguir recibiendo soluciones de problemas y correcciones de seguridad. Las actualizaciones de SP no incluyen nuevas funciones, por lo que puede basar sus implementaciones importantes en una plataforma de Horizon estable.

Hay disponibles ESB independientes una vez al año para la plataforma Horizon central, VMware App Volumes y VMware User Environment Manager. Las ESB se admiten durante 24 meses con tres actualizaciones de SP programadas: SP1 se publicará seis meses después de la versión inicial, SP2 se publicará tres meses después de SP1 y SP3 se publicará seis meses después de SP2.

Para obtener más información, consulte las preguntas frecuentes sobre: Horizon 7, App Volumes y ramas de servicios ampliados (ESB) de UEM, disponibles en <https://kb.vmware.com/s/article/52845>.

Actualizar la aplicación cliente

Actualice a la versión más reciente de Horizon Client y actualice el firmware en los dispositivos de cliente ligero si los usa.

Se eliminó la función Modo local para Horizon Client. En su lugar, VMware recomienda el uso de Mirage, que se incluye en VMware Horizon 7. Para obtener más información, consulte las notas de la versión de Horizon 7, disponibles en <https://docs.vmware.com/es/VMware-Horizon-7/index.html>.

Importante La actualización incluye ejecutar la nueva versión del instalador de Horizon Client sin eliminar en primer lugar la versión anterior de la aplicación cliente. Si los usuarios finales tienen View Client 4.6.0 basado en Windows o una versión posterior, envíeles instrucciones para eliminar el software cliente antes de descargar y ejecutar el instalador de Horizon Client más reciente.

Requisitos previos

- Compruebe que tenga una cuenta de usuario del dominio con privilegios de administrador en los hosts que utilizará para ejecutar el instalador y realizar la actualización.
- Compruebe que el teléfono, la tableta, el equipo portátil o el equipo de escritorio cliente cumplan con los requisitos de sistema operativo y los requisitos de hardware de Horizon Client. Consulte el documento "Uso de Horizon Client" para el tipo especificado de dispositivo cliente móvil o de escritorio. Visite <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Procedimiento

- 1 Haga que los usuarios finales actualicen a la versión más reciente de Horizon Client.

Opción	Acción
Horizon Client	<p>Descargue y envíe los instaladores de Horizon Client a los usuarios finales o publíquelos en un sitio web y solicite a los usuarios que descarguen el instalador y que lo ejecuten. Puede descargar los instaladores o solicitar a los usuarios finales que los descarguen del sitio web de VMware disponible en https://www.vmware.com/go/viewclients.</p> <p>Para clientes móviles, puede solicitar a los usuarios finales que obtengan la versión más reciente de Horizon Client de otros sitios web que vendan aplicaciones, incluidos Apple App Store, Google Play, Amazon y Tienda Windows.</p>
Portal web de usuario de VMware Horizon	<p>Los usuarios finales pueden abrir un navegador y dirigirse a una instancia del servidor de conexión. La página web que aparece se denomina Portal web de usuario de VMware Horizon y contiene vínculos para descargar el archivo instalador de Horizon Client.</p> <p>Nota Los vínculos predeterminados de la página web se dirigen al sitio de descargas de Horizon Client. Puede modificar los vínculos predeterminados para que se dirijan a otro lugar. Consulte Configurar la página del portal web de VMware Horizon para los usuarios finales.</p>
Cliente ligero	<p>Actualice el firmware del cliente ligero e instale el nuevo software de Horizon Client en los dispositivos cliente de los usuarios finales. Los partners de VMware proporcionan los clientes ligeros y los clientes cero.</p>

- 2 Solicite a los usuarios finales que comprueben que puedan iniciar sesión y conectarse a los escritorios remotos.

Requisitos del sistema para las actualizaciones de Horizon 7 Server

4

Los hosts y las máquinas virtuales de una implementación de Horizon 7 deben cumplir requisitos del sistema operativo y de hardware específicos.

Este capítulo incluye los siguientes temas:

- [Matriz de compatibilidad para varias versiones de los componentes de Horizon 7](#)
- [Requisitos de View Composer](#)
- [Requisitos del servidor de conexión de Horizon](#)
- [Sistemas operativos compatibles con Horizon Agent](#)

Matriz de compatibilidad para varias versiones de los componentes de Horizon 7

Como las grandes empresas deben realizar actualizaciones en fases, los componentes se diseñan para que sean compatibles con versiones anteriores y posteriores, al menos durante las actualizaciones.

Para actualizar a Horizon 7, se admiten las siguientes versiones:

- Última versión de mantenimiento de Horizon View 5.3
- Última versión de mantenimiento de VMware Horizon 6.0 (con View)
- Última versión de mantenimiento de VMware Horizon 6 versión 6.1
- Última versión de mantenimiento de VMware Horizon 6 versión 6.2

Para determinar la última versión de mantenimiento de un componente en concreto, consulte las notas de la versión correspondiente, disponibles en <https://docs.vmware.com/en/VMware-Horizon-7/index.html>

La compatibilidad del servidor de conexión de Horizon con Horizon Agent está limitada a la interoperabilidad durante una actualización del servidor de conexión. Debe actualizar Horizon Agent o View Agent cuanto antes para que coincidan con la versión del servidor de conexión que los administra.

La siguiente tabla muestra los componentes y si son compatibles con otros componentes cuya versión es diferente.

Tabla 4-1. Matriz de compatibilidad de VMware Horizon 7 y versiones anteriores de los componentes de View

	Servidor de conexión: versión anterior	Servidor de seguridad: versión anterior	View Composer: versión anterior	View Agent: versión anterior	Horizon Client (Windows): versión anterior
Servidor de conexión 7.0	Solo durante la actualización	Solo si se emparejó antes de la actualización	No	Solo durante la actualización	Sí
Servidor de seguridad 7.0 (PCoIP y RDP)	No	No disponible	No	Solo durante la actualización	Sí
View Composer 7.0	Solo durante la actualización	Solo durante la actualización	No disponible	Solo durante la actualización	No disponible
Horizon Agent 7.0	Solo durante la actualización (consulte la excepción en la nota que aparece tras esta tabla)	No	No	No disponible	Solo durante la actualización
Horizon Client 4.0	Sí	Sí	Sí	Sí	No disponible



Precaución Durante una actualización, las operaciones de mantenimiento y de aprovisionamiento de View Composer no son compatibles. Las operaciones como el aprovisionamiento y la recomposición de escritorios de clonación vinculada no se admiten durante el periodo de transición cuando algún servidor de Horizon 7 sigue ejecutando una versión anterior. Solo puede realizar estas operaciones correctamente cuando todas las instancias del servidor de conexión y View Composer se actualizaron a la última versión.

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 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.

Tabla 4-2. 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

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](#).

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 4-3. 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**.

Actualizar requisitos para View Composer

El proceso de actualización de View Composer tiene limitaciones y requisitos especiales.

Para ejecutar el instalador de View Composer, debe ser un usuario de dominio con privilegios de administrador en el sistema.

Requisitos relacionados con la seguridad

- View Composer requiere un certificado TLS firmado por una CA (entidad de certificación). 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.

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

Para obtener una información completa sobre los requisitos del certificado de seguridad, consulte "Configurar certificados SSL en View Server", disponible en el documento *Instalación de Horizon 7*.

- Los certificados para vCenter Server, View Composer, y Horizon 7 Servers deben incluir las listas de revocación de certificados (CRL). Para obtener más información, consulte "Configurar la comprobación de la revocación de los certificados del servidor" en la guía *Instalación 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. SSLv3, TLSv1.0 y RC4 también están deshabilitados de forma predeterminada. Para obtener más información, consulte "Cifrados y protocolos anteriores deshabilitados en View" en el documento de *Seguridad de Horizon 7*.
- Para mejorar la seguridad de View Composer, deshabilite los conjuntos de claves de cifrado débiles en el equipo Windows Server en el que esté instalado el servicio de View Composer. Consulte la sección "Deshabilitar cifrados débiles en SSL/TLS" que aparece en el documento *Instalación de Horizon 7*.
- Es posible que necesite realizar cambios en la configuración del protocolo para que siga siendo compatible con vSphere. Si es posible, aplique revisiones a ESXi y a vCenter Server para que admitan TLSv1.1 y TLSv1.2 antes de actualizar View Composer. Si no puede aplicar las revisiones, vuelva a habilitar TLSv1.0 en View Composer antes de la actualización. Si desea obtener más información, consulte [Habilitar TLSv1.0 en vCenter y conexiones ESXi desde View Composer](#).
- A partir de la versión 7.0.3 de Horizon 7, puede habilitar la autenticación implícita de acceso para View Composer para mejorar la seguridad. Si desea obtener más información, consulte [Habilitar la autenticación implícita de acceso para 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.

Tabla 4-4. 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

Tabla 4-4. Requisitos de hardware del servidor de conexión de Horizon (Continuación)

Componente de hardware	Obligatorio	Recomendado
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 4-5. 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

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

Requisitos para actualizar el servidor de conexión de Horizon

El proceso de actualización del servidor de conexión de Horizon tiene limitaciones y requisitos especiales.

- El servidor de conexión requiere una clave de licencia válida para esta última versión.
- La cuenta de usuario del dominio que use para instalar la nueva versión del servidor de conexión debe tener privilegios administrativos en el host del servidor de conexión. El administrador del servidor de conexión debe tener credenciales administrativas para vCenter Server.

- Al ejecutar el instalador, autoriza una cuenta de Administradores. Puede especificar el grupo Administradores local o una cuenta de un usuario o de un grupo de dominio. Horizon 7 asigna plenos derechos de Horizon Administrator, 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.
- 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.

Requisitos relacionados con la seguridad

- El servidor de conexión requiere un certificado TLS firmado por una CA (entidad de certificación) y que los clientes pueden validar. Aunque se genere un certificado autofirmado predeterminado en ausencia de un certificado firmado por una CA cuando instala el servidor de conexión, debe reemplazar el certificado autofirmado predeterminado cuanto antes. Los certificados autofirmados aparecen como no válidos en Horizon Administrator.

Además, los clientes actualizados esperan que se comunique la información sobre el certificado del servidor como parte del protocolo de enlace TLS entre el cliente y el servidor. Los clientes actualizados no suelen confiar en los certificados autofirmados.

Para obtener una información completa sobre los requisitos del certificado de seguridad, consulte "Configurar los certificados TLS para los Horizon 7 Server", disponible en la guía *Instalación de Horizon 7*. Consulte también el documento *Escenarios para configurar certificados TLS para Horizon 7*, que describe la configuración de los servidores intermedios que realiza tareas, como equilibrar cargas y descargar conexiones SSL.

Nota Si los servidores originales ya tienen certificados TLS firmados por una CA, durante la actualización, Horizon 7 importa el certificado firmado por la CA al almacén de certificados de Windows Server.

- Los certificados de vCenter Server, View Composer y Horizon 7 Servers deben incluir las listas de revocación de certificados (CRL). Para obtener más información, consulte "Configurar la comprobación de la revocación de los certificados del servidor" en el documento *Instalación de Horizon 7*.

Importante Si la empresa utiliza una configuración del proxy para acceder a Internet, debe tener configurados los hosts del servidor de conexión para que usen el proxy. Este paso asegura que los servidores puedan acceder a los sitios de la comprobación de revocación del certificado a través de Internet. Puede usar los comandos de Microsoft Netshell para importar la configuración del proxy al servidor de conexión. Para obtener más información, consulte cómo solucionar problemas relacionados con la comprobación de revocación de certificados de Horizon 7 Server en el documento *Administración de Horizon 7*.

- 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 red incluye un firewall entre un servidor de seguridad y la instancia de un servidor de conexión, tiene que configurar el firewall para que sea compatible con IPsec. Consulte el documento *Instalación de Horizon 7*.
- Es posible que necesite realizar cambios en la configuración del protocolo para que siga siendo compatible con vSphere. Si es posible, aplique revisiones a ESXi y a vCenter Server para que admitan TLSv1.1 y TLSv1.2 antes de actualizar el servidor de conexión. Si no puede aplicar las revisiones, vuelva a habilitar TLSv1.0 en el servidor de conexión antes de actualizar. Si desea obtener más información, consulte [Habilitar TLSv1.0 en conexiones de vCenter desde el servidor de conexión](#).
- Si utiliza Horizon 7 Server con una versión de View Agent anterior a la versión 6.2, deberá habilitar TLSv1.0 para las conexiones PCoIP. Las versiones de View Agent anteriores a 6.2 admiten el protocolo de seguridad TLSv1.0 solo para PCoIP. Horizon 7 Server, incluidos los servidores de conexión y los de seguridad, tienen deshabilitado de forma predeterminada TLSv1.0. Puede habilitar TLSv1.0 para las conexiones PCoIP en estos servidores siguiendo las instrucciones que aparecen en <http://kb.vmware.com/kb/2130798> de la base de conocimientos de VMware.

Si tiene pensado realizar nuevas instalaciones de las instancias del servidor de conexión en máquinas virtuales o equipos físicos adicionales, consulte la lista completa de los requisitos de instalación en el documento *Instalación de Horizon 7*.

Sistemas operativos compatibles con 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 proporcionar una seguridad mejorada, VMware recomienda configurar los conjuntos de claves de cifrado para que eliminen las vulnerabilidades conocidas. Si desea obtener instrucciones sobre cómo configurar una directiva de dominio en los conjuntos de claves de cifrado para equipos Windows que ejecutan View Composer o Horizon Agent, consulte el tema sobre cómo deshabilitar claves de cifrado en Horizon Agent o View Composer en el documento *Instalación de Horizon 7*.

Actualizar los componentes de Horizon 7 Server

5

Entre los componentes del servidor que debe actualizar, se incluyen Horizon Connection Server, servidores replicados y servidores de seguridad. En función de los componentes opcionales que use, es posible que también necesite actualizar View Composer.

Si realiza las tareas de actualización en varias ventanas de mantenimiento, puede verificar que se complete correctamente o identificar problemas en cada fase del proceso. VMware le recomienda actualizar todos los componentes del servidor durante la primera ventana de mantenimiento.

Este capítulo incluye los siguientes temas:

- [Actualizar View Composer](#)
- [Actualizar el servidor de conexión de Horizon](#)
- [Actualizar los servidores de seguridad](#)
- [Actualizar un entorno de Arquitectura de Cloud Pod](#)
- [Actualizar Horizon 7 Servers para permitir HTML Access](#)
- [Actualizar vCenter Server](#)
- [Aceptar la huella digital de un certificado TLS predeterminado](#)
- [Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7](#)

Actualizar View Composer

Durante una actualización, Horizon 7 no admite las operaciones de mantenimiento y aprovisionamiento de View Composer. Las operaciones como el aprovisionamiento y la recomposición de escritorios de clones vinculados no se admiten durante el periodo de transición cuando algún servidor de Horizon 7 sigue ejecutando una versión anterior. Solo realizará correctamente estas operaciones cuando todas las instancias de Horizon Connection Server y de View Composer estén actualizadas.

Nota Antes de que pueda usar la función de View Composer 6.2 para crear granjas automáticas de hosts RDS de clones vinculados, debe actualizar todos los componentes de Horizon a la versión 6.2 o posterior de Horizon 6.

Preparar vCenter Server y View Composer para una actualización

Dado que vCenter Server y View Composer se suelen instalar en la misma máquina virtual o el mismo equipo físico, algunas tareas de preparación se aplican a ambos.

Prepararse para las actualizaciones que incluyen vSphere

Si va a actualizar vCenter Server además de actualizar a la última versión de Horizon 7, debe consultar la *Guía de actualización de VMware vSphere* y realizar las siguientes tareas en el siguiente orden:

- 1 Compruebe que el equipo físico o la máquina virtual cumplan los requisitos del sistema para la versión de vCenter Server a la que desee actualizar.
- 2 Compruebe que la máquina virtual o el equipo físico donde está instalada la instancia actual de View Composer cumpla los requisitos de seguridad de la nueva versión.

Consulte [Actualizar requisitos para View Composer](#).

- 3 Si vCenter Server está instalado en una máquina virtual, realice una snapshot de dicha máquina virtual.

Para obtener más instrucciones sobre cómo realizar una snapshot, consulte la ayuda en línea de vSphere Client™.

- 4 Si el nombre del equipo tiene más de 15 caracteres, acórtelo a 15 o menos caracteres.
- 5 Realice una copia de seguridad de la base de datos de vCenter Server y de View Composer.

Para obtener más instrucciones sobre cómo realizar una copia de seguridad de la base de datos, consulte la documentación del proveedor de la base de datos.

- 6 Compruebe que el servidor de la base de datos sea compatible con la versión de vCenter Server que tiene pensado utilizar.

Por ejemplo, si el servidor de la base de datos es Oracle 9i, debe actualizarlo.

- 7 Compruebe que la base de datos sea compatible con la nueva versión de View Composer.

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 base de datos que View Composer no admite, continúe utilizando dicho servidor de base de datos para vCenter Server e instale otro para utilizar View Composer y los eventos de la base de datos de Horizon 7.

- 8 Realice una copia de la carpeta que contiene los certificados TLS.

Esta carpeta está ubicada en %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.

- 9 Anote la dirección IP y el nombre del sistema de la máquina en la que vCenter Server está instalado.
- 10 En todos los grupos de escritorios de clones instantáneos y clones vinculados, use Horizon Administrator para deshabilitar el aprovisionamiento de nuevas máquinas virtuales.

En los clones vinculados, dado que View Composer se podría actualizar durante una ventana de mantenimiento distinta a la de sus grupos de escritorios, el aprovisionamiento se debe posponer hasta que se actualicen ambos componentes.

- 11 Si algún grupo de escritorios de clones instantáneos o de escritorios de clones vinculados se configura para actualizar el disco del sistema operativo al cerrar sesión, utilice Horizon Administrator para editar la configuración **Escritorio/Grupos** de ese grupo y establezca **Eliminar o actualizar la máquina al cerrar sesión** en **Nunca**.

En los clones vinculados, esta opción evita que se produzca un error cuando la instancia de View Composer que se actualizó recientemente intenta actualizar un escritorio en el que Horizon Agent aún no se actualizó.

- 12 Si se programa que cualquier grupo de escritorios de clones instantáneos o clones vinculados realice una operación de publicación de imagen, de recomposición o de actualización, use Horizon Administrator para cancelar estas tareas.

Prepararse solamente para las actualizaciones de View Composer

Si solo está actualizando View Composer y no vCenter Server, debe realizar las siguientes tareas:

- 1 Compruebe que la máquina virtual o el equipo físico donde está instalada la instancia actual de View Composer cumpla los requisitos de seguridad de la nueva versión.

Consulte [Actualizar requisitos para View Composer](#).

- 2 Si View Composer está instalado en una máquina virtual, realice una snapshot de dicha máquina virtual.

Para obtener más instrucciones sobre cómo realizar una snapshot, consulte la ayuda en línea de vSphere Client.

- 3 Realice una copia de seguridad de la base de datos de View Composer.

Para obtener más instrucciones sobre cómo realizar una copia de seguridad de la base de datos, consulte la documentación del proveedor de la base de datos.

- 4 Compruebe que la base de datos sea compatible con la nueva versión de View Composer.

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 base de datos que View Composer no admite, continúe utilizando dicho servidor de base de datos para vCenter Server e instale otro para utilizar View Composer y los eventos de la base de datos de Horizon 7.

- 5 Anote la dirección IP y el nombre del sistema de la máquina en la que vCenter Server está instalado.
- 6 En todos los grupos de escritorios de clones vinculados, use Horizon Administrator para deshabilitar el aprovisionamiento de nuevas máquinas virtuales.

Dado que View Composer se podría actualizar durante una ventana de mantenimiento distinta a la de sus grupos de escritorios, el aprovisionamiento se debe posponer hasta que se actualicen ambos componentes.

- 7 Si algún grupo de escritorios se configura para actualizar el disco del sistema operativo al cerrar sesión, utilice Horizon Administrator para editar la configuración **Escritorio/Grupos** de ese grupo y establezca **Eliminar o actualizar la máquina al cerrar sesión en Nunca**.

Esta opción evita que se produzca un error cuando la instancia de View Composer que se actualizó recientemente intenta actualizar un escritorio en el que View Agent aún no se actualizó.

- 8 Si se programó alguna operación de recomposición o de actualización en los grupos de escritorios, use Horizon Administrator para cancelar estas tareas.

Actualizar View Composer

En la primera ventana de mantenimiento, actualizará View Composer. Las operaciones como aprovisionar y recomponer escritorios de clones vinculados no se admiten hasta que todos los servidores de Horizon 7 estén actualizados.

Requisitos previos

- Determine cuándo realizar este procedimiento. Elija una ventana de mantenimiento del escritorio que esté disponible. Asigne de 15 minutos a media hora.
- Complete las tareas que aparecen en [Prepararse solamente para las actualizaciones de View Composer](#).
- Compruebe que el servidor en el que View Composer está instalado tenga instalado y configurado un certificado del servidor TLS/SSL firmado por una CA (entidad de certificación). Después de actualizar Horizon Connection Server, si View Composer no usa un certificado firmado por una CA, el certificado autofirmado predeterminado aparece como no válido en Horizon Administrator.
- Compruebe que tenga una cuenta de usuario del dominio con privilegios de administrador en los hosts que utilizará para ejecutar el instalador y realizar la actualización.
- Determine si desea permitir que el asistente del instalador actualice la base de datos de View Composer si es necesaria una actualización del esquema. Puede seleccionar si desea ejecutar manualmente la utilidad de la línea de comandos SviConfig después de que el asistente termine de actualizar el esquema de la base de datos y crear un registro de la actualización.

Procedimiento

- 1 En la máquina virtual o el equipo físico donde View Composer está instalado, descargue y ejecute el instalador de View Composer.

Puede descargar el instalador desde el sitio web de VMware.

Puede encontrar instrucciones paso a paso para ejecutar el instalador en el documento *Instalación de Horizon 7*.

- 2 Especifique si desea que el asistente actualice el esquema de la base de datos si fuera necesaria una actualización.

Si aparece un cuadro de diálogo con el mensaje "Se completó la actualización de la base de datos con advertencias", puede hacer clic en **Aceptar** e ignorar el mensaje de forma segura.

- 3 Cuando el asistente solicite el número de puerto de View Composer, compruebe que esté establecido en 18443.

Pasos siguientes

Si necesita realizar una actualización manual del esquema de la base de datos, consulte [Ejecutar SviConfig para actualizar de forma manual la base de datos](#).

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

En la siguiente ventana de mantenimiento, continúe con la actualización de Horizon 7. Consulte [Actualizar los servidores de conexión en un grupo replicado](#).

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 **DWORD DisabledByDefault** 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.

Habilitar la autenticación implícita de acceso para View Composer

A partir de la versión 7.0.3 de Horizon 7, View Composer tiene el método básico de autenticación de acceso para garantizar la seguridad web que está habilitado de forma predeterminada. Para mejorar la seguridad, puede habilitar el método de autenticación implícita de acceso para View Composer.

Requisitos previos

- Verifique que tenga instalado View Composer 7.0.3 o una versión posterior.
- Verifique que pueda iniciar sesión en el equipo View Composer como un administrador.
- Verifique que tenga instalado la versión 7.0.3 o una versión posterior del servidor de conexión.

Procedimiento

- 1 Diríjase al directorio en el que View Composer está instalado.
- 2 Edite el archivo SviWebservice.exe.config.
- 3 En la opción de configuración SslPoxBinding, establezca authenticationScheme="Digest".
- 4 En la opción de configuración SslBasicAuth, establezca clientCredentialType="Digest".
- 5 Guarde y cierre el archivo SviWebservice.exe.config.
- 6 Edite el archivo SviConfig.exe.config.
- 7 En la opción de configuración SslSviBinding, establezca clientCredentialType="Digest".
- 8 Guarde y cierre el archivo SviConfig.exe.config.
- 9 Reinicie el servicio View Composer.
 - a Introduzca `services.msc` en la ventana del símbolo del sistema para iniciar la herramienta de Windows Service.
 - b En la lista de servicios, haga clic con el botón secundario en el servicio que desea reiniciar. Por ejemplo, haga clic con el botón secundario en VMware Horizon Composer 7.0.3.
 - c Haga clic en **Reiniciar**.

Actualizar de forma manual la base de datos de View Composer

En lugar de permitir que el instalador de View Composer actualice la base de datos cuando es necesaria una actualización de esquema, puede actualizar la base de datos de forma manual. Puede usar la utilidad SviConfig cuando necesite observar el proceso de actualización detenidamente o cuando las tareas de actualización se deban distribuir a los administradores TI con diferentes responsabilidades.

Cuando actualice View Composer a una versión con un esquema de base de datos actualizado, un instalador le pedirá si desea que el asistente actualice la base de datos. Si decide no usar el asistente del instalador, debe usar la utilidad SviConfig para actualizar la base de datos y migrar los datos existentes.

El uso de la utilidad de la línea de comandos SviConfig tiene las siguientes ventajas:

- Esta utilidad devuelve códigos de resultado y crea un registro de la actualización de la base de datos para simplificar la solución de problemas si se produce un error de la actualización.
- Puede separar las tareas de actualización. vSphere o un administrador de Horizon 7 pueden ejecutar el instalador de View Composer para actualizar el software. Un administrador de base de datos (DBA) puede usar SviConfig para actualizar la base de datos de View Composer.
- La actualización del software y la actualización de la base de datos pueden realizarse durante diferentes ventanas de mantenimiento. Por ejemplo, su sitio puede ejecutar operaciones de mantenimiento de la base de datos solo los fines de semanas, mientras las tareas de mantenimiento del software se pueden realizar durante la semana.

Ejecutar SviConfig para actualizar de forma manual la base de datos

La utilidad de la línea de comandos SviConfig permite actualizar la base de datos de View Composer independientemente del software de View Composer. Esta utilidad también crea un archivo de registro para simplificar la solución de problemas si se produce un error en la actualización.

Importante Solo los administradores de View Composer con experiencia deben usar la utilidad SviConfig. Esta utilidad está destinada a solucionar problemas relacionados con el servicio de View Composer.

Requisitos previos

- Realice una copia de seguridad de la base de datos de View Composer. Para obtener más instrucciones, consulte la documentación del servidor de la base de datos.
- Compruebe que sepa el nombre de origen de la base de datos (DNS) de la base de datos de View Composer.
- Compruebe que sepa el nombre de usuario y la contraseña de la cuenta de administrador de esta base de datos.

Procedimiento

- 1 En la máquina virtual o el equipo físico de vCenter Server, abra una ventana de símbolo de sistema de Windows y 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.

- 2 Introduzca el comando para detener VMware View Composer.

net stop svid

- 3 Ejecute el comando SviConfig databaseupgrade.

```
sviconfig -operation=databaseupgrade
          -DsnName=DSN_destino
          -Username=nombredeusuario_administrador_basededatos
```

Por ejemplo:

```
sviconfig -operation=databaseupgrade -dsname=LinkedClone
          -username=Admin
```

- 4 Cuando se le solicite, proporcione la contraseña.

Si todo es correcto, se mostrará un archivo de salida con los pasos de la actualización.

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

- 5 Introduzca el comando para iniciar View Composer.

net start svid

Se creará un registro completo del proceso de actualización que se ubicará en C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log.

Pasos siguientes

Si se produce algún error durante la actualización de la base de datos, consulte [Solucionar un error de actualización de la base de datos de View Composer](#).

Si el código de resultado es un número distinto a 0, que significa que la operación se realizó correctamente, consulte [Códigos de resultado para una actualización del esquema de la base de datos manual](#).

Códigos de resultado para una actualización del esquema de la base de datos manual

Cuando actualiza de forma manual la base de datos de View Composer, el comando `sviconfig databaseupgrade` muestra un código de resultado.

Tabla 5-1 Muestra los códigos de resultado de `sviconfig databaseupgrade`.

Tabla 5-1. Códigos de resultado del comando `databaseupgrade`

Código	Descripción
0	La operación finalizó correctamente.
1	No se encuentra el DSN proporcionado.
2	Se proporcionaron credenciales de administrador de la base de datos no válidas.
3	La unidad de la base de datos no es compatible.
4	Se produjo un problema inesperado y el comando no se completó.
14	Hay otra aplicación utilizando el servicio de View Composer. Desconecte el servicio antes de ejecutar el comando.
15	Se produjo un problema durante el proceso de restauración. Los detalles aparecen en la salida del registro en pantalla.
17	No se pudieron actualizar los datos de la base de datos.
18	No se puede conectar con el servidor de la base de datos.

Solucionar un error de actualización de la base de datos de View Composer

Cuando actualiza el servicio de View Composer con el instalador de este producto o ejecuta el comando `SviConfig databaseupgrade`, se puede producir un error en la operación para actualizar la base de datos de View Composer.

Problema

La operación `SviConfig databaseupgrade` muestra el código de error 17, o bien el instalador de View Composer muestra un mensaje de advertencia.

La actualización de la base de datos se completó con advertencias

Causa

El software de actualización de la base de datos se pone en contacto con vCenter Server para obtener información adicional sobre los escritorios. Se puede producir un error en la actualización de la base de datos si los escritorios no están disponibles, el host ESXi no se está ejecutando o vCenter Server no está disponible.

Solución

- 1 Consulte el archivo de registro SviConfig de View Composer para obtener más información.

La ubicación predeterminada de este archivo es C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log. El script de actualización registra un mensaje de cada error.

- 2 Examine los registros para identificar los escritorios en los que se produjo un error de actualización.

Opción	Acción
El escritorio existe, pero no está disponible.	Vuelva a hacer que el escritorio esté disponible. En función de la causa del error, es posible que tenga que reiniciar el host ESXi o vCenter Server, o bien realizar otra acción.
El escritorio no existe.	Ignore el mensaje de registro.
	Nota Puede aparecer un escritorio eliminado como existente en Horizon Administrator si un administrador elimina la máquina virtual de escritorio directamente en vSphere.

- 3 Vuelva a ejecutar el comando SviConfig databaseupgrade.

Migrar View Composer a otro equipo

En algunas situaciones, es posible que necesite migrar un servicio de VMware Horizon View Composer a una nueva máquina virtual o a un equipo físico Windows Server. Por ejemplo, puede migrar View Composer y vCenter Server a un nuevo host ESXi o a un clúster para ampliar la implementación de Horizon 7. Además, no es necesario que View Composer y vCenter Server estén instalados en el mismo equipo Windows Server.

Puede migrar View Composer del equipo vCenter Server a un equipo independiente o de un equipo independiente al equipo vCenter Server.

Importante Estos temas se refieren a la migración de la última versión de View Composer a otro equipo. Debe actualizar la versión anterior de View Composer antes de realizar estas tareas.

Si la versión actual de View Composer está instalada en un equipo que no cumpla los requisitos del sistema necesarios para la nueva versión de View Composer, no puede usar estos procedimientos. Después de migrar View Composer a un sistema con un sistema operativo Windows Server que sea compatible con esta versión, puede realizar una actualización inmediata a la última versión de View Composer.

■ [Directrices para migrar View Composer](#)

Los pasos que realice para migrar el servicio de VMware Horizon View Composer dependen de si pretende conservar las máquinas virtuales de clones vinculados existentes.

■ [Migrar View Composer con una base de datos existente](#)

Al migrar View Composer a otra máquina virtual o física, si planea preservar las máquinas virtuales de clones vinculados actuales, el nuevo servicio VMware Horizon View Composer continúa usando la base de datos de View Composer existente.

- **Migrar View Composer sin máquinas virtuales de clones vinculados**

Si el servicio actual de VMware Horizon View Composer no administra ninguna máquina virtual de clones vinculados, puede migrar View Composer a una máquina virtual o a un equipo físico sin migrar las claves RSA a la nueva máquina. El servicio de VMware Horizon View Composer migrado puede conectarse a la base de datos de View Composer original o puede preparar una nueva base de datos para View Composer.

- **Preparar Microsoft .NET Framework para migrar las claves RSA**

Para utilizar una base de datos de View Composer existente, debe migrar el contenedor de claves RSA de una máquina a otra. Para ello, utilice la herramienta de registro de IIS de ASP.NET que incluye Microsoft .NET Framework.

- **Migrar el contenedor de claves RSA al nuevo servicio de View Composer**

Para usar una base de datos de View Composer existente, debe migrar el contenedor de claves RSA de la máquina virtual o del equipo físico de origen donde reside el servicio de VMware Horizon View Composer al equipo donde desee instalar el nuevo servicio de VMware Horizon View Composer.

Directrices para migrar View Composer

Los pasos que realice para migrar el servicio de VMware Horizon View Composer dependen de si pretende conservar las máquinas virtuales de clones vinculados existentes.

Para conservar las máquinas virtuales de clones vinculados en la implementación, el servicio de VMware Horizon View Composer que instale en la nueva máquina virtual o en el equipo físico debe continuar usando la base de datos de View Composer. La base de datos de View Composer contiene datos que son necesarios para crear, aprovisionar, mantener y eliminar los clones vinculados.

Al migrar el servicio VMware Horizon View Composer, también puede migrar la base de datos de View Composer a una nueva máquina.

Migre o no la base de datos de View Composer, la base de datos debe estar configurada en una máquina disponible en el mismo dominio que la nueva máquina en la que instala el servicio de VMware Horizon View o en un dominio de confianza.

View Composer crea pares de claves RSA para cifrar y descifrar la información de autenticación almacenada en la base de datos de View Composer. Para que este origen de datos sea compatible con el nuevo servicio de VMware Horizon View Composer, debe migrar el contenedor de claves RSA que creó el servicio de VMware Horizon View original. Debe importar el contenedor de claves RSA a la máquina en la que instala el nuevo servicio.

Si el servicio de VMware Horizon View Composer actual no administra ninguna máquina virtual de clones vinculados, puede migrar el servicio sin usar la base de datos de View Composer existente. No es necesario migrar las claves RSA, use o no la base de datos existente.

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

Migrar View Composer con una base de datos existente

Al migrar View Composer a otra máquina virtual o física, si planea preservar las máquinas virtuales de clones vinculados actuales, el nuevo servicio VMware Horizon View Composer continúa usando la base de datos de View Composer existente.

Siga los pasos de este procedimiento al migrar View Composer en cualquiera de las siguientes direcciones:

- De una máquina vCenter Server a una máquina independiente
- De una máquina independiente a una máquina vCenter Server
- De una máquina independiente a una máquina independiente
- De una máquina vCenter Server a una máquina vCenter Server

Al migrar el servicio VMware Horizon View Composer, también puede migrar la base de datos de View Composer a una nueva ubicación. Por ejemplo, es posible que sea necesario migrar la base de datos de View Composer si la base de datos actual está ubicada en una máquina vCenter Server que también desee migrar.

Al instalar el servicio VMware Horizon View Composer en una nueva máquina, debe configurar el servicio para conectarse a la base de datos de View Composer.

Requisitos previos

- Familiarícese con los requisitos de migración de View Composer. Consulte [Directrices para migrar View Composer](#).
- Familiarícese con los pasos para migrar el contenedor de claves RSA al nuevo servicio VMware Horizon View Composer. Consulte [Preparar Microsoft .NET Framework para migrar las claves RSA y Migrar el contenedor de claves RSA al nuevo servicio de View Composer](#).
- Familiarícese con la instalación del servicio VMware Horizon View Composer en el documento *Instalación de Horizon 7*.
- Familiarícese con la configuración del certificado TLS para View Composer en el documento *Instalación de Horizon 7*.
- Familiarícese con la configuración de View Composer en Horizon Administrator. Consulte los temas sobre cómo configurar View Composer y sus dominios en el documento *Administración de Horizon 7*.
- Como práctica recomendada, verifique que las máquinas de origen y de destino que use para migrar View Composer son idénticas y comparten las mismas credenciales de administrador. Al migrar View Composer desde una máquina independiente a una máquina de vCenter Server que ya tenga View Composer instalado, se puede producir un error al configurar View Composer si las credenciales usadas en las dos máquinas son diferentes.

Procedimiento

- 1 Deshabilite el aprovisionamiento de la máquina virtual en la instancia de vCenter Server que esté asociada con el servicio VMware Horizon View Composer.

- a En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- b En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server y haga clic en **Deshabilitar aprovisionamiento**.

- 2 (opcional) Migre la base de datos de View Composer a una nueva ubicación.

Si necesita realizar este paso, consulte al administrador de base de datos para obtener instrucciones sobre la migración.

- 3 Desinstale el servicio VMware Horizon View Composer de la máquina actual.

- 4 (opcional) Migre el contenedor de claves RSA a la nueva máquina.

- 5 Instale el servicio VMware Horizon View Composer en la nueva máquina.

Durante la instalación, especifique el DSN de la base de datos que utilizó el servicio original VMware Horizon View Composer. Especifique también el nombre de usuario de administrador del dominio y la contraseña que se proporcionaron para el origen de datos ODBC de dicha base de datos.

Si migró la base de datos, el DSN y la información del origen de datos se dirigen a la nueva ubicación de la base de datos. Independientemente de que se migrara o no la base de datos, el nuevo servicio VMware Horizon View Composer debe tener acceso a la información de la base de datos original sobre los clones vinculados.

- 6 Configure un certificado de servidor SSL para View Composer en la nueva máquina.

Puede copiar el certificado que se instaló para View Composer en la máquina original o instalar uno nuevo.

- 7 En Horizon Administrator, establezca la nueva configuración de View Composer.

- a En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- b En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server que esté asociada con dicho servicio de View Composer y haga clic en **Editar**
- c En el panel Configuración del servidor View Composer, haga clic en **Editar** e introduzca la nueva configuración de View Composer.

Si está instalando View Composer con vCenter Server en una máquina nueva, seleccione **View Composer instalado conjuntamente con vCenter Server**.

Si está instalando View Composer en una máquina independiente, seleccione **Servidor View Composer independiente** e introduzca el FQDN de la máquina View Composer y el nombre y contraseña de usuario de View Composer.

- d En el panel Dominios, haga clic en **Verificar información del servidor** y agregue o edite los dominios de View Composer según sea necesario.
- e Haga clic en **Aceptar**.

Migrar View Composer sin máquinas virtuales de clones vinculados

Si el servicio actual de VMware Horizon View Composer no administra ninguna máquina virtual de clones vinculados, puede migrar View Composer a una máquina virtual o a un equipo físico sin migrar las claves RSA a la nueva máquina. El servicio de VMware Horizon View Composer migrado puede conectarse a la base de datos de View Composer original o puede preparar una nueva base de datos para View Composer.

Requisitos previos

- Familiarícese con la instalación del servicio VMware Horizon View Composer en el documento *Instalación de Horizon 7*.
- Familiarícese con la configuración de un certificado TLS para View Composer en el documento *Instalación de Horizon 7*.
- Familiarícese con los pasos para eliminar View Composer de Horizon Administrator. Consulte los temas sobre cómo eliminar View Composer de Horizon Administrator en el documento *Administración de Horizon 7*.

Antes de eliminar View Composer, verifique que ya no administre ninguna máquina virtual de clones vinculados. Si aparece alguno, debe eliminarlo.

- Familiarícese con la configuración de View Composer en Horizon Administrator. Consulte los temas sobre cómo configurar View Composer y sus dominios en el documento *Administración de Horizon 7*.

Procedimiento

- 1 En Horizon Administrator, elimine View Composer desde Horizon Administrator.
 - a Seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server que esté asociada con el servicio de View Composer y haga clic en **Editar**.
 - c En el panel Configuración del servidor View Composer, haga clic en **Editar**.
 - d Seleccione **No utilizar View Composer** y haga clic en **Aceptar**.

- 2 Desinstale el servicio VMware Horizon View Composer de la máquina actual.

- 3 Instale el servicio VMware Horizon View Composer en la nueva máquina.

Durante la instalación, configure View Composer para que se conecte al DNS de la base de datos original o nueva de View Composer.

- 4 Configure un certificado de servidor TLS para View Composer en la nueva máquina.

Puede copiar el certificado que se instaló para View Composer en la máquina original o instalar uno nuevo.

- 5 En Horizon Administrator, establezca la nueva configuración de View Composer.
 - a En Horizon Administrator, seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server que esté asociada con dicho servicio de View Composer y haga clic en **Editar**
 - c En el panel Configuración del servidor View Composer, haga clic en **Editar**.
 - d Proporcione la nueva configuración de View Composer.

Si está instalando View Composer con vCenter Server en una máquina nueva, seleccione **View Composer instalado conjuntamente con vCenter Server**.

Si está instalando View Composer en una máquina independiente, seleccione **Servidor View Composer independiente** e introduzca el FQDN de la máquina View Composer y el nombre y contraseña de usuario de View Composer.
 - e En el panel Dominios, haga clic en **Verificar información del servidor** y agregue o edite los dominios de View Composer según sea necesario.
 - f Haga clic en **Aceptar**.

Preparar Microsoft .NET Framework para migrar las claves RSA

Para utilizar una base de datos de View Composer existente, debe migrar el contenedor de claves RSA de una máquina a otra. Para ello, utilice la herramienta de registro de IIS de ASP.NET que incluye Microsoft .NET Framework.

Requisitos previos

Descargue .NET Framework y consulte información sobre la herramienta de registro de IIS de ASP.NET. Visite <http://www.microsoft.com/net>.

Procedimiento

- 1 Instale .NET Framework en la máquina virtual o física en la que esté instalado el servicio de VMware Horizon View Composer asociado a la base de datos existente.
- 2 Instale .NET Framework en la máquina de destino en la que desee instalar el nuevo servicio de VMware Horizon View Composer.

Pasos siguientes

Migre el contenedor de claves RSA a la máquina de destino. Consulte [Migrar el contenedor de claves RSA al nuevo servicio de View Composer](#).

Migrar el contenedor de claves RSA al nuevo servicio de View Composer

Para usar una base de datos de View Composer existente, debe migrar el contenedor de claves RSA de la máquina virtual o del equipo físico de origen donde reside el servicio de VMware Horizon View Composer al equipo donde desee instalar el nuevo servicio de VMware Horizon View Composer.

Debe realizar este procedimiento antes de instalar el nuevo servicio de VMware Horizon View Composer.

Requisitos previos

Verifique que la herramienta de registro IIS de ASP.NET y Microsoft .NET Framework estén instalados en los equipos de origen y de destino. Consulte [Preparar Microsoft .NET Framework para migrar las claves RSA](#).

Procedimiento

- 1 En el equipo de origen donde reside el servicio de VMware Horizon View Composer existente, abra una ventana de símbolo de sistema y diríjase al directorio %windir%\Microsoft.NET\Framework\v2.0xxxxx.

- 2 Escriba el comando `aspnet_regiis` para guardar el par de claves RSA en un archivo local.

`aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri`

La herramienta de registro IIS de ASP.NET exporta el par de claves privada y pública RSA del contenedor SviKeyContainer al archivo `keys.xml` y guarda el archivo de forma local.

- 3 Copie el archivo `keys.xml` en el equipo de destino en el que desea instalar el nuevo servicio de VMware Horizon View Composer.
- 4 En el equipo de destino, abra una ventana de símbolo de sistema y diríjase al directorio %windir%\Microsoft.NET\Framework\v2.0xxxxx.
- 5 Escriba el comando `aspnet_regiis` para migrar los datos del par de claves RSA.

`aspnet_regiis -pi "SviKeyContainer" "ruta\keys.xml" -exp`

donde *ruta* es la ruta del archivo exportado.

La opción `-exp` crea un par de claves exportables. Si es necesaria una migración en el futuro, las claves se pueden exportar de este equipo e importarse a otro. Si migró previamente las claves a esta máquina sin usar la opción `-exp`, puede volver a importar las claves con la opción `-exp` para poder exportar las claves en el futuro.

La herramienta de registro importa los datos del par de claves en el contenedor de claves local.

Pasos siguientes

Instale el nuevo servicio VMware Horizon View Composer en la máquina de destino. Proporcione la información de origen de los datos ODBC y DSN que permite a VMware Horizon View Composer conectarse a la misma información de la base de datos que usó el servicio de VMware Horizon View Composer original. Para obtener más instrucciones, consulte "Instalar View Composer" en el documento *Instalación de Horizon 7*.

Complete los pasos para migrar View Composer a un nuevo equipo y usar la misma base de datos. Consulte [Migrar View Composer con una base de datos existente](#).

Actualizar el servidor de conexión de Horizon

Si la implementación usa equilibradores de carga para administrar varias instancias del servidor de conexión, se puede realizar una actualización de la infraestructura del servidor de conexión sin tiempo de espera.

Nota Para poder utilizar la función de Horizon 6 versión 6.2 para clonar un grupo de escritorios, debe actualizar todas las instancias del servidor de conexión de un pod a Horizon 6 versión 6.2 o una versión posterior.

Después de realizar una instalación desde cero o actualizar todas las instancias de servidor de conexión a Horizon 7 versión 7.2, no se puede cambiar la versión de dichas instancias a una versión anterior a la 7.2 de Horizon 7, ya que cambiaron las claves que se utilizan para proteger los datos LDAP.

Para seguir teniendo la posibilidad de cambiar las instancias del servidor de conexión a una versión anterior mientras planifica una actualización a la versión 7.2 de Horizon 7, debe realizar una copia de seguridad de las instancias del servidor de conexión antes de comenzar la actualización. Si necesita cambiar las instancias del servidor de conexión a una versión anterior, debe realizar este procedimiento en todas las instancias del servidor de conexión y, a continuación, aplicar la copia de seguridad al servidor de conexión que se modificó a una versión anterior.

Preparar el servidor de conexión para una actualización

Antes de actualizar el servidor de conexión o cualquiera de los componentes de vSphere de los que dicho servidor depende, debe realizar varias tareas para asegurarse de que la actualización se realice correctamente.

Tareas a realizar en una única instancia de un grupo replicado

Antes de empezar a actualizar cualquier instancia del servidor de conexión, realice las siguientes tareas únicamente con una de las instancias. Como las instancias están replicadas, la configuración de una instancia es la misma que la del resto:

- Si el servidor de conexión está instalado en una máquina virtual, realice una snapshot de dicha máquina virtual.

Para obtener más instrucciones sobre cómo realizar una snapshot, consulte la ayuda en línea de vSphere Client. Si alguna vez necesita revertir a esta snapshot y tiene otras instancias del servidor de conexión en un grupo replicado, debe desinstalarlas antes de revertir la principal a la snapshot. Tras la reversión, puede volver a instalar las instancias replicadas y dirigirse a la que revirtió.

Puede etiquetar la snapshot como Fase de preparación de la actualización.

- Abra Horizon Administrator y registre toda la configuración general y la de los escritorios y grupos: las secciones de grupos y de escritorios del árbol de inventario y la sección Configuración Global del árbol de configuración de View.

Por ejemplo, haga una captura de pantalla de la configuración correspondiente.

- La utilidad `vdmexport.exe` le permitirá realizar una copia de seguridad de la base de datos de LDAP. Para obtener instrucciones, consulte la guía de administración de la versión actual del documento *Administración de Horizon 7*.

Tareas a realizar con cada instancia justo antes de la actualización

- Compruebe que la máquina virtual o física donde está instalada la instancia actual del servidor de conexión cumpla los requisitos del sistema de la nueva versión.
Consulte [Requisitos del servidor de conexión de Horizon](#).
- Registre la dirección IP y el nombre del sistema del equipo en el que el servidor de conexión está instalado.
- Determine si su compañía escribió archivos por lotes o scripts que se ejecutan en la base de datos de View de la instancia del servidor de conexión. Si es así, registre sus nombres y ubicaciones.
- Abra Horizon Administrator y registre toda la configuración específica de la instancia.
Por ejemplo, acceda a **Configuración de View > Servidores > Servidores de conexión**, seleccione la instancia del servidor de conexión en la tabla y haga clic en **Editar**. Puede hacer una captura de pantalla de cada pestaña en el cuadro de diálogo **Editar configuración del servidor de conexión**.

Actualizar los servidores de conexión en un grupo replicado

Este procedimiento describe la actualización de las instancias del servidor de conexión que no están emparejadas con los servidores de seguridad. Por ejemplo, este procedimiento se aplica a los servidores de conexión que están configurados para establecer conexiones con los clientes que están dentro del firewall corporativo.

Para las instancias del servidor de conexión que están emparejadas con los servidores de seguridad, use el procedimiento que se describe en [Actualizar los servidores de seguridad y sus servidores de conexión emparejados](#).

No es necesario que reinicie el servidor de conexión después de acabar la actualización.

Nota Este proceso describe una actualización local. Para migrar a otra máquina, consulte [Actualizar a la versión más reciente del servidor de conexión en un equipo diferente](#).

Requisitos previos

- Determine cuándo realizar este procedimiento. Elija una ventana de mantenimiento del escritorio que esté disponible. La cantidad de tiempo que tarda la actualización en realizarse depende del número de instancias del servidor de conexión del grupo. Asigne de 15 minutos a media hora para cada instancia.
- Si usa View Composer, compruebe que se actualizó. Consulte [Actualizar View Composer](#). Después de actualizar el servidor de conexión, debe agregar View Composer utilizando Horizon Administrator.

- Familiarícese con los requisitos de seguridad de Horizon 7 y compruebe que dichos requisitos se cumplan. Consulte [Requisitos para actualizar el servidor de conexión de Horizon](#). Es posible que necesite obtener e instalar un certificado del servidor SSL firmado por una CA que incluya información sobre la revocación del certificado, verificar que el Firewall de Windows con seguridad avanzada esté establecido en **activo** y configurar los firewalls back-ends para que admitan IPsec.
- Compruebe que el servidor en el que vCenter Server está instalado tenga un certificado del servidor SSL firmado por una CA (entidad de certificación) instalado y configurado. Después de actualizar el servidor de conexión, si vCenter Server no usa un certificado firmado por una CA, el certificado autofirmado predeterminado aparece como no válido en Horizon Administrator y un mensaje indica que vCenter Server no está disponible.
- Complete las tareas que aparecen en [Preparar el servidor de conexión para una actualización](#).
- Compruebe que tenga una licencia que sea válida para la nueva versión.

Nota Cuando actualiza de 6.0.x o 6.1.x a 6.2, la licencia anterior continuará funcionando y el modelo de uso se establecerá en **Usuario simultáneo**. Un nuevo modelo de licencia denominado Usuario con nombre se agregó a partir de la versión 6.2 de Horizon 6. Tiene la opción de cambiar el modelo de licencia a **Usuario con nombre**. Si desea obtener más información, consulte <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

- Compruebe que tenga una cuenta de usuario del dominio con privilegios de administrador en los hosts que utilizará para ejecutar el instalador y realizar la actualización.
- Si no está familiarizado con la utilidad `vdmexport.exe`, imprima las instrucciones sobre cómo usarla que aparecen en el documento *Administración de Horizon 7*. Esta utilidad le servirá para realizar una copia de seguridad de la base de datos de LDAP de View como parte del procedimiento de actualización.

No es necesario cambiar la configuración de los equilibradores de carga existentes.

Procedimiento

- 1 Si utiliza un equilibrador de carga para administrar un grupo de instancias del servidor de conexión, deshabilite el servidor que aloja la instancia que está a punto de actualizar.
 - a Inicie sesión en Horizon Administrator.
 - b Diríjase a **Configuración de View > Servidores** y haga clic en la pestaña **Servidores de conexión**.
 - c Seleccione la instancia del servidor de conexión en la lista y haga clic en el botón **Deshabilitar** en la parte superior de la tabla.
 - d Haga clic en **Aceptar** para confirmar que desea deshabilitar el servidor.

- 2 En el host de la instancia del servidor de conexión, descargue y ejecute el instalador de la nueva versión del 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. No es necesario que detenga los servicios antes de realizar la actualización. El instalador detiene y reinicia los servicios según sea necesario. De hecho, el servicio VMware VDMDS debe estar en ejecución para actualizar la base de datos de LDAP de View.

El instalador determina que ya está instalada una versión anterior y realiza la actualización. El instalador muestra menos opciones de instalación que durante una instalación nueva.

También se actualiza el LDAP de View.

Nota Antes de actualizar, el instalador comprueba el estado de replicación para determinar si el servidor se puede comunicar con los otros servidores en el grupo replicado y si puede recuperar las actualizaciones de LDAP a partir de otros servidores del grupo. Si se produce un error en la comprobación del estado, no se realiza la actualización.

- 3 Compruebe que el servicio del servidor de conexión de VMware Horizon se reinicie después de que el asistente del instalador se cierre.
- 4 Inicie sesión en Horizon Administrator y habilite la instancia del servidor de conexión que acaba de actualizar.
 - a Diríjase a **Configuración de View > Servidores** y haga clic en la pestaña **Servidores de conexión**.
 - b Seleccione la instancia del servidor de conexión en la lista y haga clic en el botón **Habilitado** en la parte superior de la tabla.
 - c En la columna Versión, compruebe que aparece la nueva versión.
- 5 Diríjase a **Configuración de View > Uso y licencia del producto**, haga clic en **Editar licencia**, introduzca la clave de licencia y haga clic en **Aceptar**.
- 6 Si utiliza un equilibrador de carga para administrar esta instancia del servidor de conexión, habilite el servidor que acaba de actualizar.
- 7 Compruebe que pueda iniciar sesión en un escritorio remoto.
- 8 Repita los pasos previos para actualizar cada instancia del servidor de conexión en el grupo.

Importante Si no actualiza todas las instancias del servidor de conexión en un grupo replicado, los indicadores de estado del panel de control de Horizon Administrator pueden mostrar una o más instancias en estado de error. Esta situación se produce porque diferentes versiones proporcionan diferentes tipos de datos. La solución es actualizar todas las instancias en el grupo replicado.

- 9 Utilice la herramienta `vdmexport.exe` para realizar una copia de seguridad de la base de datos de LDAP de View actualizada recientemente.

Si cuenta con varias instancias del servidor de conexión en un grupo replicado, solo es necesario que exporte la información desde una instancia.

- 10 Inicie sesión en Horizon Administrator y examine el panel de control para comprobar que los iconos de vCenter Server y de View Composer aparezcan en color verde.

Si alguno de estos iconos aparecen en color rojo y se muestra un cuadro de diálogo para informar de que se detectó un certificado no válido, debe hacer clic en **Verificar** y aceptar la huella digital del certificado que no es de confianza (como se describe en los pasos que debe seguir a continuación), o bien instalar un certificado SSL firmado por una entidad de certificación.

Para obtener más información sobre cómo reemplazar el certificado predeterminado en vCenter Server, consulte el documento *Ejemplos y escenarios de VMware vSphere*.

- 11 Compruebe que los iconos del panel de control de las instancias del servidor de conexión también aparezcan en color verde.

Si alguna instancia aparece con el icono en color rojo, haga clic en dicha instancia para determinar el estado de replicación. Es posible que la replicación se vea afectada por las siguientes razones:

- Un firewall puede estar bloqueando la comunicación
- Es posible que el servicio de VMware VDMDS se detuviera en una instancia del servidor de conexión
- Las opciones de VMware VDMS DSA pueden bloquear las replicaciones
- Se produjo un problema en la red

Pasos siguientes

Para usar un certificado autofirmado o uno predeterminado desde vCenter Server o View Composer, consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

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

Si se produce un error al actualizar una o varias instancias del servidor de conexión, consulte [Crear un grupo replicado después de revertir un servidor de conexión a una snapshot](#).

Importante Si tiene pensado utilizar el modo seguro de mensajes mejorado para los mensajes JMS, asegúrese de que los firewall permitan que las instancias del servidor de conexión reciban el tráfico JMS entrante en el puerto 4002 desde los servidores de seguridad y escritorios. Abra también el puerto 4101 para aceptar las conexiones desde otras instancias del servidor de conexión.

Si vuelve a instalar en algún momento el servidor de conexión en un servidor que cuente con un recopilador de datos configurado para supervisar los datos de rendimiento, detenga el recopilador de datos y vuelva a iniciarlo.

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.

Actualizar a la versión más reciente del servidor de conexión en un equipo diferente

Como parte de la actualización, puede migrar el servidor de conexión a un nuevo equipo.

Requisitos previos

- Actualice al menos una instancia del servidor de conexión existente a la versión más reciente. Consulte [Actualizar los servidores de conexión en un grupo replicado](#). Durante esta actualización, se actualizará el LDAP de View existente.
- Verifique que la nueva máquina virtual o el nuevo equipo físico cumplan los requisitos del sistema para instalar el servidor de conexión. Consulte [Sistemas operativos compatibles con el servidor de conexión de Horizon](#) y [Requisitos de hardware para el servidor de conexión de Horizon](#).
- Familiarícese con los requisitos de seguridad de Horizon 7 y compruebe que dichos requisitos se cumplan. Consulte [Requisitos para actualizar el servidor de conexión de Horizon](#).
- Determine cuándo realizar este procedimiento. Elija una ventana de mantenimiento del escritorio que esté disponible. Asigne de 15 minutos a media hora para cada instancia.
- Compruebe que tenga una cuenta de usuario de dominio con privilegios administrativos en el host que usará para ejecutar el instalador.
- Familiarícese con el procedimiento para instalar una instancia replicada. Consulte el documento *Instalación de Horizon 7*. Instale una instancia replicada como parte de este procedimiento.

No es necesario cambiar la configuración de los equilibradores de carga existentes.

Procedimiento

- 1 Compruebe que se esté ejecutando una instancia actualizada del servidor de conexión y que sea accesible para el nuevo equipo en el que tenga pensado instalar el servidor de conexión.
Cuando instale el servidor de conexión en el nuevo host, se le dirigirá a esta instancia existente.
- 2 En el nuevo equipo, instale una instancia replicada del servidor de conexión.
El LDAP de View de la nueva instancia será una réplica del LDAP de la instancia de origen actualizada.
- 3 Si corresponde, desinstale el servidor de conexión del host antiguo con la herramienta de Windows **Agregar o quitar programas**.
- 4 En Horizon Administrator, diríjase a la pestaña **Configuración de View > Servidores > Servidores de conexión** y determine si la instancia del servidor de conexión que se desinstaló aún aparece en la lista.

- 5 Si la instancia del servidor de conexión que se desinstaló aún aparece en la lista, utilice el comando `vdmadmin` para eliminarla.

```
vdmadmin.exe -S -s nombre_servidor -r
```

En este ejemplo, *nombre_servidor* es el nombre del host o la dirección IP del host del servidor de conexión. Para obtener más información sobre la herramienta `vdmadmin` de la línea de comandos, consulte el documento *Administración de Horizon 7*.

Se agrega una nueva instancia del servidor de conexión a un grupo y se elimina una instancia antigua.

Pasos siguientes

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

Actualice los otros componentes del servidor de Horizon 7.

Si vuelve a instalar en algún momento el servidor de conexión en un servidor que cuente con un recopilador de datos configurado para supervisar los datos de rendimiento, detenga el recopilador de datos y vuelva a iniciarlo.

Crear un grupo replicado después de revertir un servidor de conexión a una snapshot

Si se produce un error en una actualización o si, por otra razón, debe revertir a una snapshot una máquina virtual que aloja el servidor de conexión, debe desinstalar las otras instancias del servidor de conexión del grupo y volver a crear el grupo replicado.

Si revierte una máquina virtual del servidor de conexión a una snapshot, los objetos LDAP de View de la base de datos de esa máquina virtual ya no son coherentes con los de las bases de datos de otras instancias replicadas. Después de revertir a una snapshot, se registra el siguiente evento en el Registro de eventos de Windows, en el evento VMwareVDMDS (ID del evento 2103): Se restauró la base de datos de los Servicios de directorio ligero de Active Directory mediante un procedimiento de restauración no compatible. La máquina virtual revertida deja de replicar su LDAP de View.

Si considera necesario revertir a una snapshot, debe desinstalar las otras instancias del servidor de conexión y el LDAP de View en esas máquinas virtuales y, a continuación, volver a instalar las instancias de réplica.

Requisitos previos

Determine la instancia que debe ser el nuevo servidor de conexión estándar o principal. Este servidor de conexión tiene los datos de configuración de Horizon 7 deseados.

Procedimiento

- 1 En todas las instancias del servidor de conexión, excepto en la elegida para ser la nueva instancia estándar, desinstale el servidor de conexión y la instancia LDAP de View.

La instancia LDAP de View se denomina "AD LDS Instance VMwareVDMDS".

- 2 En la máquina virtual que aloja la instancia del servidor de conexión estándar o principal, abra un símbolo de sistema e introduzca el siguiente comando para comprobar que no se deshabilitó la replicación.

```
repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL -DISABLE_INBOUND_REPL
```

- 3 En las máquinas virtuales que se encargan de alojar las instancias de réplica del servidor de conexión, ejecute el instalador del servidor de conexión, seleccione la opción de instalación **Servidor de réplica de View** y especifique el nombre del host o la dirección IP de la instancia estándar del servidor de conexión.

El grupo replicado de las instancias del servidor de conexión se vuelve a crear y los objetos LDAP de View son coherentes.

Actualizar los servidores de seguridad

Si la implementación usa equilibradores de carga para administrar varios servidores de seguridad, una actualización de la infraestructura del servidor de conexión se puede realizar sin tiempo de espera.

Nota Para utilizar los dispositivos de Unified Access Gateway en lugar de los servidores de seguridad, debe actualizar las instancias del servidor de conexión a la versión 6.2 de Horizon 6 o a una versión posterior antes de instalar y configurar los dispositivos de Unified Access Gateway, de forma que se dirijan a instancias del servidor de conexión o al equilibrador de carga que se dirige a las instancias. Si desea obtener más información, consulte [Reemplazar un servidor de seguridad por un dispositivo Unified Access Gateway](#).

Preparar el servidor de seguridad para una actualización

Antes de actualizar los servidores de seguridad, realice estas tareas para crear copias de seguridad y guardar las opciones de configuración.

- Compruebe que la máquina virtual o el equipo físico donde está instalada la instancia actual del servidor de seguridad cumpla los requisitos del sistema de la nueva versión.

Consulte [Requisitos del servidor de conexión de Horizon](#).

- Si el servidor de seguridad está instalado en una máquina virtual, realice una snapshot de dicha máquina virtual.

Para obtener más instrucciones sobre cómo realizar una snapshot, consulte la ayuda en línea de vSphere Client. Puede etiquetar la snapshot como Fase de preparación de la actualización.

- Abra Horizon Administrator y anote las opciones de este servidor de seguridad. Diríjase a **Configuración de View > Servidores** y haga clic en la pestaña **Servidores de seguridad**.

Por ejemplo, seleccione el servidor de seguridad, haga clic en **Editar** y realice una captura de pantalla de la configuración.

- Anote la dirección IP y el nombre del sistema de la máquina en la que el servidor de seguridad está instalado.

- Si utiliza equilibradores de carga para los servidores de seguridad, anote las opciones de configuración de dichos equilibradores.

Nota Este tema no describe el comando de Horizon Administrator denominado **Preparar para la actualización o para la reinstalación**, que está disponible en la pestaña **Servidores de seguridad**. Este comando elimina las reglas IPsec del servidor de seguridad, que detiene toda la comunicación entre el servidor de seguridad y la instancia del servidor de conexión emparejada. Por lo tanto, deberá utilizar el comando durante el procedimiento de actualización, inmediatamente antes de actualizar el servidor de seguridad, tal y como se describe en [Actualizar los servidores de seguridad y sus servidores de conexión emparejados](#).

Actualizar los servidores de seguridad y sus servidores de conexión emparejados

Use este procedimiento si la instancia del servidor de conexión que tiene pensado actualizar está emparejada con un servidor de seguridad.

Este procedimiento está diseñado para actualizar un servidor de seguridad y su instancia del servidor de conexión antes de pasar a actualizar el siguiente servidor de seguridad y su instancia del servidor de conexión emparejada. Esta estrategia permite que no se produzca ningún tiempo de inactividad. Si la instancia no está emparejada con un servidor de seguridad, use el procedimiento [Actualizar los servidores de conexión en un grupo replicado](#).

Los primeros pasos de este procedimiento incluyen actualizar la instancia del servidor de conexión. Después de actualizar el servidor de conexión, pero antes de actualizar el servidor de seguridad, uno de estos pasos describe cómo eliminar las reglas IPsec del servidor de seguridad. Cuando 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 el servidor de seguridad.

De forma predeterminada, las reglas IPsec rigen la comunicación entre un servidor de seguridad y la instancia del servidor de conexión emparejada. Si las reglas IPsec existentes no se eliminaron antes de volver a instalar o actualizar, se produce un error en el emparejamiento entre el servidor de seguridad y el servidor de conexión, y no se puede establecer un nuevo grupo de reglas IPsec después de la actualización.

Requisitos previos

- Determine cuándo realizar este procedimiento. Elija una ventana de mantenimiento del escritorio que esté disponible. Asigne de 15 a 30 minutos en cada servidor de seguridad y su instancia del servidor de conexión.
- Si usa View Composer, compruebe que se actualizó. Consulte [Actualizar View Composer](#). Después de actualizar el servidor de conexión, debe agregar View Composer utilizando Horizon Administrator.

- Familiarícese con los requisitos de seguridad de Horizon 7 y compruebe que dichos requisitos se cumplan. Consulte [Requisitos para actualizar el servidor de conexión de Horizon](#). Es posible que necesite obtener e instalar un certificado del servidor TLS firmado por una CA que incluya información sobre la revocación del certificado, verificar que el Firewall de Windows con seguridad avanzada esté establecido como **activo** y configurar los firewalls back-ends para que admitan IPsec.
- Compruebe que las máquinas virtuales y los equipos físicos en los que las instancias del servidor de conexión y el servidor de seguridad actual están instalados cumplan los requisitos del sistema. Consulte [Requisitos del servidor de conexión de Horizon](#).
- Complete las tareas que aparecen en [Preparar el servidor de conexión para una actualización](#).
- Compruebe que tenga una licencia para la nueva versión.
- Compruebe que tenga una cuenta de usuario con privilegios de administrador en los hosts que utilizará para ejecutar el instalador y realizar la actualización.
- Compruebe que se pueda acceder a la instancia del servidor de conexión que se desea emparejar con el 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.

Procedimiento

- 1 Si utiliza un equilibrador de carga para administrar servidores de seguridad emparejados con instancias del servidor de conexión, deshabilite el servidor de seguridad que está emparejado con la instancia que está a punto de actualizar.
- 2 Actualice la instancia del servidor de conexión que está emparejada con el servidor de seguridad. Realice del paso 2 al 6 de [Actualizar los servidores de conexión en un grupo replicado](#).
- 3 Elimine las reglas IPsec del servidor de seguridad emparejado con la instancia del servidor de conexión que acaba de actualizar.
 - a En Horizon Administrator, haga clic en **Configuración de View > Servidores**.
 - b 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.
 - c Haga clic en **Aceptar**.

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.

- 4 Configure una contraseña de emparejamiento de servidores de seguridad usando la última versión de Horizon Administrator. Consulte "Configurar una contraseña de emparejamiento para el servidor de seguridad" en el documento *Instalación de Horizon 7*.

- 5 En el host del servidor de seguridad, descargue y ejecute el instalador para la versión del servidor de conexión más reciente.

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. El instalador determina que ya está instalada una versión anterior y realiza la actualización. El instalador muestra menos opciones de instalación que durante una instalación nueva.

Se le solicitará que proporcione la contraseña de emparejamiento del servidor de seguridad.

Es posible que se le solicite que descarte un cuadro de mensaje que le notifica que se detuvo el servidor de seguridad. El instalador detiene el servicio para prepararlo para la actualización.

- 6 Después de que el asistente del instalador finalice, compruebe que el servicio del servidor de seguridad de VMware Horizon View comience.
- 7 Si utiliza un equilibrador de carga para administrar este servidor de seguridad, vuelva a agregarlo al grupo de carga equilibrada.
- 8 Inicie sesión en Horizon Administrator, seleccione el servidor de seguridad en el panel de control y compruebe que este servidor tenga la última versión.
- 9 Compruebe que pueda iniciar sesión en un escritorio remoto.
- 10 En Horizon Administrator, diríjase a la pestaña **Configuración de View > Servidores > Servidores de seguridad** y elimine de la lista los servidores de seguridad duplicados.

El mecanismo de emparejamiento del servidor de seguridad automático puede producir entradas duplicadas en la lista **Servidores de seguridad** si el nombre del sistema completo no coincide con el nombre que se asignó cuando el servidor de seguridad se creó.

- 11 Utilice la herramienta vdmexport.exe para realizar una copia de seguridad de la base de datos de LDAP de View actualizada recientemente.

Si cuenta con varias instancias del servidor de conexión en un grupo replicado, solo es necesario que exporte la información desde una instancia.

- 12 Inicie sesión en Horizon Administrator y examine el panel de control para comprobar que los iconos de vCenter Server y de View Composer aparezcan en color verde.

Si alguno de estos iconos aparecen en color rojo y se muestra un cuadro de diálogo para informar de que se detectó un certificado no válido, debe hacer clic en **Verificar** y aceptar la huella digital del certificado que no es de confianza (como se describe en los pasos que debe seguir a continuación), o bien instalar un certificado SSL firmado por una entidad de certificación.

Para obtener más información sobre cómo reemplazar el certificado predeterminado en vCenter Server, consulte el documento *Ejemplos y escenarios de VMware vSphere*.

- 13** Compruebe que los iconos del panel de control de las instancias del servidor de conexión también aparezcan en color verde.

Si alguna instancia aparece con el icono en color rojo, haga clic en dicha instancia para determinar el estado de replicación. Es posible que la replicación se vea afectada por las siguientes razones:

- Un firewall puede estar bloqueando la comunicación
- Es posible que el servicio de VMware VDMS se detuviera en una instancia del servidor de conexión
- Las opciones de VMware VDMS DSA pueden bloquear las replicaciones
- Se produjo un problema en la red

Pasos siguientes

Para usar un certificado autofirmado o uno predeterminado desde vCenter Server o View Composer, consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

Si se produce un error al actualizar una o varias instancias del servidor de conexión, consulte [Crear un grupo replicado después de revertir un servidor de conexión a una snapshot](#).

Importante Si tiene pensado utilizar el modo seguro de mensajes mejorado para los mensajes JMS, asegúrese de que los firewall permitan que las instancias del servidor de conexión reciban el tráfico JMS entrante en el puerto 4002 desde los servidores de seguridad y escritorios. Abra también el puerto 4101 para aceptar las conexiones desde otras instancias del servidor de conexión.

Si vuelve a instalar en algún momento el servidor de conexión en un servidor que cuente con un recopilador de datos configurado para supervisar los datos de rendimiento, detenga el recopilador de datos y vuelva a iniciarlo.

Reemplazar un servidor de seguridad por un dispositivo Unified Access Gateway

Puede reemplazar un servidor de seguridad por un dispositivo Unified Access Gateway.

Requisitos previos

Para utilizar los dispositivos de Unified Access Gateway en lugar de los servidores de seguridad, debe actualizar las instancias del servidor de conexión a la versión 6.2 de Horizon 6 o a una versión posterior antes de instalar y configurar los dispositivos de Unified Access Gateway, de forma que se dirijan a instancias del servidor de conexión o al equilibrador de carga que se dirige a las instancias.

Procedimiento

- 1 Desinstale el software del servidor de seguridad.
- 2 Elimine la configuración IPsec del servidor de seguridad. Consulte *Eliminar las reglas IPsec del servidor de seguridad* en el documento *Instalación de Horizon 7*.

- 3 Elimine la entrada LDAP del servidor de seguridad. Consulte *Eliminar una entrada de una instancia del servidor de conexión o del servidor de seguridad con la opción -S* en el documento *Administración de Horizon 7*.
- 4 En Horizon Administrator, registre el dispositivo Unified Access Gateway.
- 5 En el firewall de red entre Unified Access Gateway y el servidor de conexión, elimine las reglas del firewall asociadas al servidor de seguridad eliminado y agregue las reglas del firewall asociadas al Unified Access Gateway entrante. Unified Access Gateway necesita comunicarse con el servidor de conexión del puerto TCP 443.

Las reglas del firewall de back-end del servidor de seguridad para el servidor de conexión son las siguientes:

Origen	Puerto predeterminado	Protocolo	Destino	Puerto predeterminado	Notas
Servidor de seguridad	UDP 500	ISAKMP	Servidor de conexión	UDP 500	Negociación de la fase 1 de IPsec.
Servidor de seguridad	UDP 4500	NAT-T	Servidor de conexión	UDP 4500	Tráfico AJP13 encapsulado cuando se utiliza NAT.
Servidor de seguridad		ESP	Servidor de conexión		Tráfico AJP13 encapsulado cuando no se requiere circulación NAT. ESP es el protocolo IP 50. No se especifican los números de puerto.
Servidor de seguridad		AJP13	Servidor de conexión	TCP 8009	Tráfico AJP13 sin IPsec y durante el emparejamiento.
Servidor de seguridad		JMS	Servidor de conexión	TCP 4001	Canal de mensajería para la negociación de la clave.
Servidor de seguridad		JMS-TLS	Servidor de conexión	TCP 4002	Canal de mensajería para la administración.

- 6 Configure e inicie el dispositivo 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>.

Actualizar un entorno de Arquitectura de Cloud Pod

La función Arquitectura de Cloud Pod usa componentes estándar de Horizon 7 para proporcionar administración de centro de datos cruzados. Con la función Arquitectura de Cloud Pod, puede vincular varios pods para ofrecer un único entorno de administración de aplicaciones y escritorios de gran tamaño. Un pod consta de un grupo de instancias del servidor de conexión, un almacenamiento compartido, un servidor de la base de datos e infraestructuras de red y de vSphere necesarias para alojar grupos de aplicaciones y escritorios.

Utilice el siguiente proceso para actualizar un entorno de Arquitectura de Cloud Pod.

- 1 Actualice todas las instancias del servidor de conexión en un pod, según el proceso usual para actualizar una instancia del servidor de conexión.
- 2 Repita el paso anterior en los otros pods de la federación de pods, actualizando los pods uno a uno.

Durante el proceso de actualización, algunas instancias del servidor de conexión utilizan la versión más reciente de Horizon 7 y otros utilizan una versión anterior. A pesar de que este entorno con varias versiones se admite a partir de la versión 7.4 de Horizon 7, las funciones nuevas no funcionan en un entorno mixto. Por ejemplo, una función nueva que esté visible en el Horizon Administrator de un servidor actualizado no estará visible en el Horizon Administrator de un servidor que no se actualizó.

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

Actualizar Horizon 7 Servers para permitir HTML Access

Cuando actualice las instancias del servidor de conexión o los servidores de seguridad que se encuentran tras un equilibrador de carga o una puerta de enlace como Unified Access Gateway, debe realizar cambios en la configuración para continuar usando HTML Access.

Para obtener más información, consulte "Permitir HTML Access a través de un equilibrador de carga" y "Permitir HTML Access a través de una puerta de enlace" en el documento *Instalación de Horizon 7*.

Actualizar vCenter Server

Realice una actualización de vCenter Server como parte de la misma ventana de mantenimiento durante la que actualiza otros componentes de Horizon 7 Server. Antes de actualizar vCenter Server, debe realizar una copia de seguridad de algunos datos de Horizon 7. Tras la actualización, si View Composer se ejecuta en el mismo servidor, debe reiniciar el servicio de View Composer.

Nota Durante la actualización de vCenter Server, las sesiones de las aplicaciones y escritorios remotos existentes no se desconectan, pero la siguiente funcionalidad no está disponible durante la actualización de vCenter Server:

- Los escritorios remotos que están en estado de aprovisionamiento no se encenderán.
 - No se pueden iniciar los nuevos escritorios.
 - Las operaciones de View Composer no están permitidas.
-

Requisitos previos

- Determine cuándo realizar este procedimiento. Elija una ventana de mantenimiento del escritorio que esté disponible. Para obtener más información sobre cuánto tiempo es necesario, consulte la *Guía de actualización de VMware vSphere*.
- Realice una copia de seguridad de la base de datos de vCenter Server y de View Composer.
- Realice una copia de seguridad de la base de datos LDAP de View desde una instancia del servidor de conexión mediante la utilidad `vdmexport.exe`.

Para obtener instrucciones, consulte el documento *Administración de Horizon 7*. Si cuenta con varias instancias del servidor de conexión en un grupo replicado, es necesario que exporte la información desde una única instancia.

- Realice las tareas que aparecen en [Prepararse para las actualizaciones que incluyen vSphere](#).
- Compruebe que el servidor en el que vCenter Server está instalado tenga un certificado de servidor TLS firmado por una CA (entidad de certificación) instalado y configurado. Después de actualizar el servidor de conexión, si vCenter Server no usa un certificado firmado por una CA, el certificado autofirmado predeterminado aparece como no válido en Horizon Administrator y un mensaje indica que vCenter Server no está disponible.
- Complete los requisitos previos que aparecen en la *Guía de actualización de VMware vSphere* mediante la versión de la guía que corresponda a la versión de vSphere que tiene pensado actualizar.
- Para actualizar vCenter Server mientras los clones instantáneos están en uso, consulte los pasos del artículo <https://kb.vmware.com/s/article/52573> de la base de conocimientos de VMware.

Procedimiento

- 1 Actualice vCenter Server como se describe en la *Guía de actualización de VMware vSphere*.

Importante Si los clústeres contienen almacenes de datos vSAN, consulte además el capítulo sobre cómo actualizar el clúster de vSAN en el documento *Administrar VMware vSAN*. Este capítulo contiene un tema sobre cómo actualizar vCenter Server.

- 2 Si View Composer se instala en el mismo host, reinicie el servicio de View Composer.
- 3 Inicie sesión en Horizon Administrator y revise el panel de control para comprobar que los iconos de vCenter Server y de View Composer aparezcan en color verde.

Si alguno de estos iconos aparecen en color rojo y se muestra un cuadro de diálogo para informar de que se detectó un certificado no válido, debe hacer clic en **Verificar** y aceptar la huella digital del certificado que no es de confianza (como se describe en los pasos que debe seguir a continuación), o bien instalar un certificado SSL firmado por una entidad de certificación.

Para obtener más información sobre cómo reemplazar el certificado predeterminado en vCenter Server, consulte el documento *Ejemplos y escenarios de VMware vSphere*.

Pasos siguientes

Para usar un certificado autofirmado o predeterminado de vCenter Server o View Composer, consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

Si terminó de actualizar los componentes de Horizon 7 Server, en la siguiente ventana de mantenimiento, continúe con la actualización de Horizon 7.

- Si también está actualizando los componentes de vSphere, consulte [Capítulo 6 Actualizar los hosts ESXi y sus máquinas virtuales](#).

- Si solo está actualizando los componentes de Horizon 7, consulte [Actualizar View Agent o Horizon Agent](#).

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 la configuración de los certificados TLS, consulte cómo configurar certificados TLS en View Server, disponible en el documento *Instalación 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.

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

Horizon 7 proporciona varios archivos de plantillas administrativas ADMX de directivas de grupo, específicos para los componentes. Puede optimizar y asegurar las aplicaciones y los escritorios remotos al agregar la configuración de la directiva de los archivos de plantilla ADMX a un GPO nuevo o ya existente de Active Directory.

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

Para actualizar las directivas de grupo, use el Editor de objetos de directiva de grupo en el servidor de Active Directory para agregar la nueva versión de los archivos de plantilla.

Los archivos de plantilla ADMX de Horizon 7 contienen tanto las directivas de grupo Configuración de usuario como las de Configuración del equipo.

- Las directivas Configuración del equipo establecen directivas que se aplican a todos los escritorios remotos, sin tener en cuenta quién se conecta al escritorio.
- Las directivas Configuración de usuario establecen directivas que se aplican a todos los usuarios, independientemente de la aplicación o el escritorio remotos al que se conectan. Las directivas Configuración de usuario sobrescriben las equivalentes de Configuración del equipo.

Microsoft Windows aplica las directivas cuando el escritorio se inicia y cuando los usuarios inician sesión.

Actualizar los hosts ESXi y sus máquinas virtuales

6

El proceso de actualización de los hosts ESXi y las máquinas virtuales es el que más tiempo consume durante esta fase intermedia de una actualización de Horizon 7.

Este procedimiento proporciona una descripción general de las tareas que debe realizar durante la segunda ventana de mantenimiento y las siguientes. Para completar algunas de estas tareas, es posible que necesite las instrucciones paso a paso que aparecen en la *Guía de actualización de VMware vSphere* y en el documento *Administración de Horizon 7*.

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.

Importante La siguiente tabla describe las funciones de Horizon 7 que dependen de versiones específicas del hardware virtual y, por lo tanto, pueden necesitar que se actualicen las máquinas virtuales.

Tabla 6-1. Versiones del hardware virtual necesarias para funciones específicas

Función	Versión del hardware virtual	Versión de vSphere correspondiente
Formato de disco eficiente de espacio para grupos de clones vinculados	9 o posterior	vSphere 5.1 o posterior
Almacenes de datos VMware® vSAN®, primera versión	10 o posterior	vSphere 5.5 Update 1 o posterior
Almacenes de datos VMware vSAN, segunda versión	11 o posterior	vSphere 6.0 o posterior
Almacenes de datos VMware Virtual Volumes	11 o posterior	vSphere 6.0 o posterior
Tecnología de snapshot NFS nativas (VAAI)	9 o posterior	vSphere 5.1 o posterior
Aceleración de gráficos virtuales compartidos	8 o posterior	vSphere 5.0 o posterior
Aceleración de gráficos virtuales dedicados	9 o posterior	vSphere 5.1 o posterior
Aceleración de gráficos NVIDIA GRID vGPU	11 o posterior	vSphere 6.0 o posterior

Requisitos previos

- Complete el procedimiento que se describe en [Actualizar los servidores de conexión en un grupo replicado](#).

- Realice las tareas de preparación de la actualización de ESXi que aparecen en la *Guía de actualización de VMware vSphere*.

Procedimiento

1 Actualizar los hosts ESXi, clúster a clúster.

Para obtener más instrucciones, consulte la *Guía de actualización de VMware vSphere*. Si los clústeres contienen almacenes de datos vSAN, consulte además el capítulo sobre cómo actualizar el clúster de vSAN en el documento *Administrar VMware vSAN*. Este capítulo contiene un tema sobre cómo actualizar los hosts ESXi.

Si tiene varios clústeres, es posible que sean necesarias varias ventanas de mantenimiento para que se complete este paso. La actualización de los hosts ESXi puede incluir las siguientes tareas:

- a Use VMware vSphere® vMotion® para mover las máquinas virtuales fuera del host ESXi.
- b Ponga el host en modo de mantenimiento.
- c Realice la actualización.
- d Use vMotion para volver a enviar las máquinas virtuales al host.
- e Realice las tareas necesarias después de la actualización en los hosts ESXi.

Todos los hosts deben ser miembros de un clúster, como se mencionó en los requisitos.

2 Si un host actualizado no se vuelve a conectar a vCenter Server, use vSphere Client para volver a conectar el host a vCenter Server.

3 Si usa View Composer, después de que se actualicen todos los hosts ESXi, reinicie el servicio de View Composer en el host de vCenter Server.

4 (opcional) Actualice VMware® Tools™ y las máquinas virtuales en todas las máquinas virtuales principales, en las plantillas de máquinas virtuales y en las máquinas virtuales que alojan los componentes de Horizon 7 Server, como las instancias del servidor de conexión.

- a Planifique que esta acción se desarrolle durante un tiempo de inactividad, como se describe en la *Guía de actualización de VMware vSphere*.
- b Actualice VMware Tools y el hardware de las máquinas virtuales que se usarán como orígenes de los escritorios remotos.

Para obtener instrucciones paso a paso si no tiene pensado usar VMware vSphere® Update Manager™, consulte el capítulo sobre cómo actualizar las máquinas virtuales en el documento *Administración de máquinas virtuales de VMware vSphere*.

Si usa VMware vSphere Update Manager, puede actualizar VMware Tools y, a continuación, la versión del hardware virtual siguiendo el orden apropiado para todas las máquinas virtuales de una carpeta concreta. Consulte la *Guía de actualización de VMware vSphere*.

- 5 (opcional) Si usa escritorios de clones vinculados completa, en cada máquina virtual, actualice VMware Tools y el hardware virtual de las máquinas virtuales que se usarán como orígenes de los escritorios remotos.

Para obtener instrucciones paso a paso si no tiene pensado usar VMware vSphere® Update Manager™, consulte el capítulo sobre cómo actualizar las máquinas virtuales en el documento *Administración de máquinas virtuales de VMware vSphere*.

Si usa vSphere Update Manager, puede actualizar VMware Tools y, a continuación, la versión del hardware virtual siguiendo el orden apropiado para todas las máquinas virtuales de una carpeta concreta. Consulte la *Guía de actualización de VMware vSphere*.

Pasos siguientes

Actualice el software agente. Consulte [Actualizar View Agent o Horizon Agent](#).

Actualizar escritorios virtuales y publicados

7

Actualice los escritorios publicados, los escritorios virtuales y Horizon Agent, que se ejecuta en los sistemas operativos de los escritorios virtuales y los hosts Microsoft RDS.

Importante Este capítulo no contiene información sobre cómo actualizar Horizon Agent en una máquina virtual Linux. Para obtener esa información, consulte *Configurar escritorios de Horizon 7 for Linux*.

Este capítulo incluye los siguientes temas:

- [Requisitos relacionados con la seguridad para actualizar los escritorios](#)
- [Actualizar hosts RDS que proporcionan escritorios basados en sesión](#)
- [Actualizar View Agent o Horizon Agent](#)
- [Actualizar grupos de escritorios de View Composer](#)
- [Actualizar grupos de escritorios de clones instantáneos](#)

Requisitos relacionados con la seguridad para actualizar los escritorios

RC4, SSLv3 y TLSv1.0 aparecen deshabilitados de forma predeterminada en los componentes de Horizon 7. Si necesita volver a habilitar RC4, SSLv3 o TLSv1.0 en un escritorio virtual o publicado, consulte el apartado sobre protocolos antiguos y cifrados deshabilitados en Horizon 7 que aparecen el documento *Seguridad de Horizon 7*.

Para obtener información completa sobre las funciones de seguridad de View Agent, Horizon Agent y Horizon Client, consulte el documento *Seguridad en Horizon Client y Agent*.

Actualizar hosts RDS que proporcionan escritorios basados en sesión

En los hosts RDS con Windows Server 2008 R2 o sistema operativo posterior, puede actualizar el software Horizon Agent o View Agent y editar la configuración de grupo de forma que el host RDS pueda proporcionar aplicaciones remotas basadas en Windows y escritorios remotos.

Con VMware Horizon 6.0 y versiones posteriores, puede usar hosts RDS de Microsoft para proporcionar aplicaciones remotos, además de escritorios remotos. Con esta nueva funcionalidad, el nombre de la granja de servidores previamente oculto ahora se muestra en Horizon Administrator.

Requisitos previos

- Compruebe que se actualizó al menos una instancia del servidor de conexión de Horizon en el grupo replicado. El servidor de conexión se debe actualizar en primer lugar para que el mecanismo de emparejado JMS seguro pueda funcionar con Horizon Agent.
- Verifique que el host RDS que actualmente aloja los escritorios remotos esté ejecutando Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2. Windows Server 2008 (Terminal Services) era compatible con las versiones anteriores de Horizon 7, pero no es compatible con esta versión. Si no tiene un sistema operativo Windows Server compatible, debe realizar una nueva instalación en lugar de una actualización. Para obtener una lista de sistemas operativos compatibles, consulte [Sistemas operativos compatibles con Horizon Agent](#).
- Compruebe que la función del host RDS esté instalado en el sistema operativo. Consulte el procedimiento sobre cómo instalar los Servicios de Escritorio remoto en Windows Server 2008 R2 en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Familiarícese con el procedimiento para ejecutar el instalador de Horizon Agent. Consulte el procedimiento "Instalar Horizon Agent en un host de los Servicios de Escritorio remoto" en *Configurar aplicaciones y escritorios publicados en Horizon 7*, disponible al hacer clic en el botón **Ayuda** en Horizon Administrator.
- Verifique que haya cerrado sesión en todas las aplicaciones y todos los escritorios remotos.
- Compruebe que tenga una cuenta de usuario del dominio con privilegios de administrador en los hosts que utilizará para ejecutar el instalador y realizar la actualización.

Procedimiento

- 1 En Horizon Administrator, edite la configuración de este grupo de escritorios para deshabilitarlo.

Acceda a **Catálogo > Grupos de escritorios**, seleccione el grupo y haga clic en **Editar**.

- 2 En el host RDS, descargue y ejecute el instalador para la nueva versión de Horizon Agent.

Puede descargar el instalador desde el sitio web de VMware.

- 3 En Horizon Administrator, edite la configuración de la granja y establezca el protocolo de visualización predeterminado en **PCoIP** o **VMware Blast**.

Acceda a **Recursos > Granjas**, seleccione la granja y haga clic en **Editar**.

También puede usar una configuración que permita al usuario final seleccionar el protocolo. Para usar aplicaciones remotas, el protocolo debe ser PCoIP o VMware Blast. Las aplicaciones remotas no son compatibles con RDP.

- 4 En Horizon Administrator, edite la configuración del grupo de escritorios para habilitarlo.

Este host puede ahora proporcionar aplicaciones remotas, además de escritorios remotos. En Horizon Administrator, si accede a **Catálogo > Grupos de escritorios**, verá que el tipo de grupo es **Grupo de escritorios RDS**. Si accede a **Recursos > Granjas**, verá un ID de granja en la lista que se corresponde con el ID de grupo.

Pasos siguientes

Actualice los clientes. Consulte [Capítulo 3 Actualizar la aplicación cliente](#).

Actualizar View Agent o Horizon Agent

La estrategia para actualizar el software del agente depende del tipo de origen del escritorio.

Nota Para actualizar el sistema operativo en un escritorio de máquina virtual de Windows 8 a Windows 8.1, debe desinstalar Horizon Agent, actualizar el sistema operativo de Windows 8 a Windows 8.1 y, a continuación, volver a instalar Horizon Agent. De forma alternativa, puede realizar una nueva instalación de Windows 8.1 y volver a instalar Horizon Agent.

Este procedimiento proporciona una visión general de las tareas que debe realizar para actualizar el software del agente en las máquinas virtuales que se utilizan como orígenes de los escritorios. Para completar algunas de estas tareas, es posible que necesite las instrucciones paso a paso que se encuentran en la ayuda en línea de vSphere Client o en *Configurar escritorios virtuales en Horizon 7*, disponible al hacer clic en el botón **Ayuda** en Horizon Administrator. Para actualizar el software del agente en un host Terminal Services o host RDS de Microsoft, consulte [Actualizar hosts RDS que proporcionan escritorios basados en sesión](#). Para actualizar el software del agente en una máquina virtual Linux, consulte el documento independiente *Configurar escritorios de Horizon 7 for Linux*.

Si tiene pensado implementar clones instantáneos, puede usar este procedimiento para crear una máquina virtual principal para un grupo de escritorios de clones instantáneos. Cuando actualice Horizon Agent en una máquina virtual principal, solo tiene que seleccionar la opción adecuada para un grupo de escritorios de clones instantáneos.

Importante El instalador de Horizon Agent ahora incluye todos los componentes que se incluyeron previamente en Remote Experience Agent, que era parte de VMware Horizon™ View™ Feature Pack. Para actualizar funciones que se instalaron con Remote Experience Agent, puede ejecutar el instalador de Horizon Agent. Este instalador elimina Remote Experience Agent antes de realizar la actualización. Si, por alguna razón, decide eliminar de forma manual Remote Experience Agent, asegúrese de hacerlo antes de ejecutar el instalador de la nueva versión de Horizon Agent.

Requisitos previos

- Compruebe que se actualizó al menos una instancia del servidor de conexión en el grupo replicado. El servidor de conexión se debe actualizar en primer lugar para que el mecanismo de emparejado JMS seguro pueda funcionar con Horizon Agent.
- Si está actualizando los hosts ESXi y las máquinas virtuales, complete el procedimiento que se describe en [Capítulo 6 Actualizar los hosts ESXi y sus máquinas virtuales](#).

- Compruebe que tenga una cuenta de usuario del dominio con privilegios de administrador en los hosts que utilizará para ejecutar el instalador y realizar la actualización.

Procedimiento

- 1 Si tiene pensado implementar clones instantáneos o clones vinculados de View Composer, actualice el software del agente en una máquina virtual principal y cree un grupo de escritorios en el que realizar pruebas.

- a Descargue y ejecute la nueva versión del instalador de Horizon Agent en una máquina virtual principal.

Puede descargar el instalador desde el sitio web de VMware.

- b Cree un grupo pequeño de escritorios a partir de esta máquina virtual.
 - c Pruebe un escritorio de la máquina virtual desde el grupo de escritorios para comprobar que todos los escenarios de uso funcionen correctamente.

Por ejemplo, cree un grupo de escritorios que contenga un escritorio de la máquina virtual y compruebe que pueda usar Horizon Client para iniciar sesión en ese escritorio.

Puede encontrar instrucciones paso a paso para ejecutar el instalador de Horizon Agent y para crear grupos de escritorios en *Configurar escritorios virtuales en Horizon 7*, disponible al hacer clic en el botón **Ayuda** en Horizon Administrator.

Importante Si actualiza desde View 5.1.x o una versión anterior, utiliza Sysprep y los usuarios finales conectarán los dispositivos USB a sus escritorios remotos, debe seguir el procedimiento descrito en la base de conocimientos de VMware, disponible en <http://kb.vmware.com/kb/2051801>. De lo contrario, después de actualizar el software del agente, es posible que la función del redireccionamiento USB no funcione.

- 2 En las otras máquinas virtuales y las plantillas de las máquinas virtuales, descargue y ejecute el instalador de la nueva versión de Horizon Agent.

Puede encontrar instrucciones paso a paso para ejecutar el instalador de Horizon Agent y para crear grupos de escritorios en *Configurar escritorios virtuales en Horizon 7*, disponible al hacer clic en el botón **Ayuda** en Horizon Administrator.

- 3 Si tiene pensado crear grupos de escritorios de clones vinculados de View Composer o de clones instantáneos, realice una snapshot de cada máquina virtual principal actualizada.

Use la nueva snapshot para crear un grupo de escritorios de clones vinculados o de clones instantáneos, o bien para recomponer un grupo de escritorios de clones vinculados ya existente.

Para obtener más instrucciones sobre cómo realizar una snapshot, consulte la ayuda en línea de vSphere Client.

- 4 Si usa escritorios de clones completos u otras máquinas virtuales que agregó como escritorios individuales o como parte de un grupo manual, actualice el software del agente mediante las herramientas de terceros que suele utilizar para las actualizaciones de software.

- 5 Para los grupos de Windows 7 y 8 automáticos y manuales que no son de clones vinculados ni de clones instantáneos, para activar la función del procesamiento 3D, edite el grupo y encienda y apague los escritorios de la máquina virtual.

- a Configure las siguientes opciones del grupo:
 - Establezca que el grupo use el protocolo de visualización PCoIP o el protocolo de visualización VMware Blast.
 - Establezca **Permitir que los usuarios elijan el protocolo** en **No**.
 - Active la función **Procesamiento 3D**.
- b Apague cada máquina virtual y vuelva a encenderlas.

Si reinicia una máquina virtual, en lugar de encenderla y apagarla, la opción no se aplica.

- 6 Si usa máquinas virtuales o equipos físicos como los hosts RDS de Microsoft, para proporcionar aplicaciones o los escritorios remotos, descargue y ejecute el instalador de la nueva versión de Horizon Agent en estos equipos.

Puede descargar el instalador desde el sitio web de VMware.

Importante Cuando ejecute el instalador en un host RDS de una máquina virtual, se desmarca el componente **View Composer Agent**. No seleccione este componente durante una actualización. Si quiere usar este componente para crear una granja automática, que es una función que se introdujo con la versión 6.2 de Horizon 6, desinstale la versión anterior del software agente y vuelva a instalar la nueva versión con el componente **View Composer Agent** seleccionado.

- 7 Si usa equipos físicos como orígenes de los escritorios, descargue y ejecute el instalador de la nueva versión de Horizon Agent en esos equipos.

Puede descargar el instalador desde el sitio web de VMware.

- 8 Use un Horizon Client que no se actualizó para comprobar que pueda iniciar sesión en los orígenes de los escritorios remotos actualizados con el software del cliente anterior.

Pasos siguientes

Si usa los grupos de escritorios de View Composer, vuelva a componer o a crear los grupos. Consulte [Actualizar grupos de escritorios de View Composer](#).

Actualice los clientes. Consulte [Capítulo 3 Actualizar la aplicación cliente](#).

Actualizar grupos de escritorios de View Composer

Parte de la fase final de una actualización de Horizon incluye actualizar los grupos de escritorios de View Composer.

La actualización de los grupos que se crearon con View Composer requiere que use una snapshot que se tomó después de actualizar Horizon Agent en la máquina virtual principal.

Importante Si usa clones vinculados de View Composer y desea usar la función de recuperación del espacio disponible en las máquinas virtuales que cuentan con vSphere 5.1 y versiones posteriores, debe configurar algunas opciones en el LDAP de View y de Horizon Administrator, además de realizar los pasos que se indican en este procedimiento. Para obtener una lista completa de las tareas, consulte [Tareas de actualización de grupos de escritorios para usar la recuperación de espacio](#).

Nota Si también está actualizando la versión del hardware virtual, por ejemplo, a la versión 8 o a alguna versión posterior, que se incluye con vSphere 5 o versiones posteriores, las snapshots de la máquina virtual principal actualizada se usan para actualizar la versión del hardware virtual del resto de las máquinas virtuales en el grupo de clones vinculados.

Se admite este tipo de actualización, es decir, de una versión del hardware virtual (o nivel de compatibilidad) a una versión superior. Sin embargo, no puede volver a componer clones vinculados en una versión de hardware anterior a la actual. Por ejemplo, no puede volver a componer clones con una versión de hardware 8 a una máquina virtual principal cuya versión de hardware sea 7.

Requisitos previos

- Complete el procedimiento que se describe en [Actualizar View Composer](#).
- Complete el procedimiento que se describe en [Actualizar los servidores de conexión en un grupo replicado](#).
- Si también está actualizando los hosts ESXi y las máquinas virtuales, complete el procedimiento descrito en [Capítulo 6 Actualizar los hosts ESXi y sus máquinas virtuales](#).

Para obtener más información sobre las versiones de vSphere que son necesarias para varias funciones nuevas, consulte [Tabla 6-1](#).

- Complete el procedimiento descrito en [Actualizar View Agent o Horizon Agent](#) para actualizar el agente en la máquina virtual principal.

Importante Si actualiza desde View 5.1.x o una versión anterior, utiliza Sysprep y los usuarios finales conectarán los dispositivos USB a sus escritorios remotos, debe seguir el procedimiento descrito en la base de conocimientos de VMware, disponible en <http://kb.vmware.com/kb/2051801>. De lo contrario, después de actualizar el software del agente, es posible que la función del redireccionamiento USB no funcione.

- Planifique la ventana de mantenimiento con atención para que, al volver a crear y al volver a componer los grupos de escritorios, no se inunde la matriz de almacenamiento ni los hosts ESXi.

Procedimiento

- 1 Si deshabilitó el aprovisionamiento de las nuevas máquinas virtuales que estaba preparando para la actualización, vuelva a habilitarlo.

- 2 Para activar la función de procesamiento 3D, edite el grupo para configurar las siguientes opciones:
 - Establezca que el grupo use el protocolo de visualización PCoIP o el protocolo de visualización VMware Blast.
 - Establezca **Permitir que los usuarios elijan el protocolo** en **No**.
 - Active la función **Procesamiento 3D**.
- 3 Para habilitar la función de recuperación del espacio disponible en las máquinas virtuales que cuentan con vSphere 5.1, en la sección **Almacenamiento avanzado** de la configuración del grupo, seleccione **Reclamar espacio de disco de la máquina virtual** y establezca el umbral de la recuperación del disco en 1 GB.
- 4 Para habilitar el acelerador de almacenamiento de View, disponible en las máquinas virtuales con vSphere 5.0 o versiones posteriores, en la sección **Almacenamiento avanzado** de la configuración de los grupos, compruebe que la casilla **Usar el acelerador de almacenamiento de View** este seleccionada.

El acelerador de almacenamiento de View puede mejorar el rendimiento durante los arranques masivos y los exámenes antivirus de E/S en masa al permitir que los hosts ESXi almacenen en caché los datos comunes de los discos de las máquinas virtuales.

Importante Esta función está activada de forma predeterminada. El acelerador de almacenamiento de View requiere 1 GB de RAM por host ESXi.

- 5 Use la snapshot que creó después de actualizar la máquina virtual principal para volver a componer los grupos de escritorios.
- 6 Si cambió la opción **Actualizar el disco del SO al cerrar sesión** de un grupo a **Nunca** al preparar la actualización, vuelva a cambiar la opción para que refleje la directiva de actualización apropiada.
- 7 Si canceló cualquier operación de recomposición o de actualización en algún grupo de escritorios, vuelva a programar las tareas.

Pasos siguientes

Actualice los clientes. Consulte [Capítulo 3 Actualizar la aplicación cliente](#).

Realice las tareas que aparecen en [Capítulo 9 Tareas posteriores a la actualización para habilitar nuevas funciones en la configuración de Horizon](#) que se aplican a su configuración.

Actualizar grupos de escritorios de clones instantáneos

Si actualiza vCenter Server para usar vSphere 6.7, también debe actualizar el grupo de escritorios de clones instantáneos.

Requisitos previos

- Complete los requisitos del sistema para actualizar a la versión 7.5 de Horizon 7 o a una versión posterior.
- Complete los procedimientos que se describen en [Actualizar el servidor de conexión de Horizon](#).

- Complete el procedimiento descrito en [Actualizar View Agent o Horizon Agent](#) para actualizar el agente en la máquina virtual principal.
- Complete los requisitos que aparecen en la *Guía de actualización de VMware vSphere* mediante la versión de la guía que corresponda a la versión de vSphere que tiene pensado actualizar.

Nota Si actualiza vCenter Server a vSphere 6.7, todos o algunos hosts ESXi del clúster se deben actualizar a vSphere 6.7. Si no, es posible que los grupos de escritorios de clones instantáneos no funcionen correctamente.

- Identifique los hosts ESXi que quiere actualizar y verifique que tenga suficientes hosts en línea para los grupos de escritorios existentes.

Procedimiento

- 1 Realice una snapshot de la máquina virtual principal en la que actualiza Horizon Agent a Horizon 7 versión 7.5 o posterior. Esta snapshot es la imagen principal de los clones instantáneos.
- 2 Establezca el umbral de la migración de Storage Distributed Resource Scheduler (DRS) a 3 en el clúster.
- 3 Deshabilite el grupo de escritorios de clones instantáneos.
- 4 Actualice vCenter Server a vSphere 6.7.
- 5 Para poner los hosts que piensa actualizar en modo de mantenimiento, seleccione una de las siguientes opciones.
 - Ponga el host directamente en modo de mantenimiento desde vSphere Web Client y actualice el host a vSphere 6.7. Después de que acabe la actualización, use vSphere Web Client para cerrar el modo de mantenimiento.
 - Use la utilidad `icm maint.cmd` para marcar que un host entre en mantenimiento con la opción **ACTIVADO**. Al marcar un host para su mantenimiento, se eliminan las imágenes principales, que son las máquinas virtuales principales en vCenter Server del host ESXi. Ponga el host en modo de mantenimiento y actualice a vSphere 6.7 ESXi. Una vez finalizada la actualización, quite el host del modo de mantenimiento. A continuación, use `icm maint.cmd` para desmarcar el mantenimiento del host con la opción **DESACTIVADO**.
- 6 Habilite el grupo de escritorios de clones instantáneos.
- 7 Realice una operación de publicación de imagen para cada grupo de escritorios de clones instantáneos que usen la nueva snapshot.

Solo los hosts que están actualizados a vSphere 6.7 ESXi se usan para el aprovisionamiento. Los clones instantáneos creados durante la operación de publicación de imagen se pueden migrar a otros hosts que aún no estén en vSphere 6.7.
- 8 Verifique que todos los hosts del clúster estén actualizados a vSphere 6.7.

- 9 Si actualiza la máquina virtual principal desde una versión previa para que sea compatible con ESXi 6.7 y versiones posteriores (versión 14 de la máquina virtual), actualice VMware Tools en la máquina virtual principal. Debe realizar una nueva snapshot de la máquina virtual principal, que es la imagen principal para los clones instantáneos, y realizar una operación de publicación de imagen en todos los grupos de escritorios de clones instantáneos que usen la versión previa de esta imagen principal.
- 10 Si el conmutador virtual distribuido (vDS) se actualiza, encienda la máquina virtual principal para verificar que no existan problemas de red. Tras una actualización de vDS, debe realizar una nueva snapshot de la máquina virtual principal y realizar una operación de publicación de imagen en los grupos de escritorios de clones instantáneos.

Actualizar el dispositivo virtual Horizon 7 Cloud Connector

8

Actualice a la versión más reciente del dispositivo virtual Horizon 7 Cloud Connector para comunicar los pods de Horizon 7 con las funciones de VMware Horizon Cloud Service más recientes.

Requisitos previos

- Instale e implemente el dispositivo virtual Horizon 7 Cloud Connector. Consulte el documento *Instalación de Horizon 7*.
- Verifique que el nuevo dispositivo virtual Horizon 7 Cloud Connector y el dispositivo virtual Horizon 7 Cloud Connector existente que necesite actualizarse estén en la misma red, de forma que el nuevo dispositivo virtual pueda establecer una comunicación SSH con el dispositivo virtual existente.
- Utilice vSphere Web Client para realizar una snapshot del dispositivo virtual Horizon 7 Cloud Connector existente.
- Cuando ya exista un dominio de Active Directory que esté unido, verifique que tenga las credenciales para una cuenta de Active Directory en el dominio que tenga permisos de acceso.

Procedimiento

- 1 En vSphere Web Client, encienda el dispositivo Horizon 7 Cloud Connector existente.
Aparece la dirección IP de la interfaz de usuario del dispositivo Horizon 7 Cloud Connector.
- 2 Si va a actualizar desde la versión 1.0 del dispositivo virtual Horizon 7 Cloud Connector, inicie sesión como usuario raíz del vCenter Server al dispositivo virtual Horizon 7 Cloud Connector existente e introduzca el comando `chage -E -1 -M -1 tomcat8`.

Por ejemplo, introduzca el siguiente comando: `root@example.com [~]# chage -E -1 -M -1 tomcat8`

Nota Este paso no es necesario para la versión 1.1 y versiones posteriores del dispositivo virtual Horizon 7 Cloud Connector.

- 3 En un navegador web, introduzca la dirección IP del dispositivo virtual Horizon 7 Cloud Connector para iniciar sesión en la interfaz de usuario de Horizon 7 Cloud Connector.

Utilice sus credenciales de la cuenta My VMware para iniciar sesión. Este paso verifica que la conexión existente de Horizon Cloud se configuró correctamente con el servidor de conexión que está alojado en las instalaciones.

- 4 Implemente la versión más reciente del dispositivo virtual Horizon 7 Cloud Connector y use las credenciales de la cuenta My VMware para iniciar sesión.

Nota Si el entorno asociado a la cuenta de My VMware se unió a un dominio de Active Directory, aparecerá la ventana de inicio de sesión de Active Directory y deberá iniciar sesión con las credenciales de Active Directory.

- 5 Conecte la versión más reciente del dispositivo Horizon 7 Cloud Connector con la instancia del servidor de conexión en las instalaciones. En la casilla **Conectar al servidor de conexión Horizon 7**, introduzca el FQDN del servidor de conexión que se aloja en las instalaciones y haga clic en **Conectar**.

- 6 Haga clic en la casilla para verificar el certificado de huella digital para el servidor de conexión.

Nota Esta verificación se omite si el servidor de conexión tiene un certificado de CA raíz.

- 7 Introduzca el nombre de dominio, el nombre del usuario y la contraseña del servidor de conexión y haga clic en **Conectar**.

Nota Para optimizar la auditoría de las acciones de Horizon 7 Cloud Connector, utilice un nombre de usuario único y una contraseña en el servidor de conexión.

- 8 Haga clic en **Actualizar** en el cuadro de diálogo.
- 9 En el campo **Dirección antigua de Cloud Connector**, introduzca la dirección IP o el dispositivo virtual Horizon 7 Cloud Connector anterior y haga clic en **Conectar**.
- 10 Haga clic en la casilla para verificar la huella digital para la conexión SSH.
- 11 Haga clic en **Actualizar**.

El pod de Horizon 7 se actualiza y se empareja con VMware Horizon Cloud Service correctamente.

Solucionar problemas de la actualización del dispositivo virtual Horizon 7 Cloud Connector

La versión anterior del dispositivo virtual Horizon 7 Cloud Connector se deshabilita solo al final del proceso de actualización. Si hay algún problema de actualización, puede revertirla a la versión anterior del dispositivo virtual Horizon 7 Cloud Connector.

Nota Cuando realice cualquier tarea de solución de problemas, no desconecte la última versión implementada del dispositivo Horizon 7 Cloud Connector.

Procedimiento

- 1 Si la actualización falla y aún se puede acceder a la versión anterior del dispositivo virtual Horizon 7 Cloud Connector, puede seguir usando esta versión del dispositivo virtual. Después de comprobar los archivos de registro y verificar la información de configuración del nuevo dispositivo virtual Horizon 7 Cloud Connector, puede volver a realizar la tarea de actualización.
- 2 Si se produce un error en la actualización y no se puede acceder a la versión anterior del dispositivo virtual Horizon 7 Cloud Connector, realice estos pasos:
 - a Desconecte el nuevo dispositivo virtual Horizon 7 Cloud Connector.
 - b Revierta el dispositivo virtual Horizon 7 Cloud Connector existente a la snapshot del dispositivo virtual realizada antes de la actualización. Verifique que se pueda acceder al dispositivo virtual Horizon 7 Cloud Connector desde el navegador web y que muestre el estado emparejado.
 - c Realice la tarea de actualización para volver a implementar la versión más reciente del dispositivo Horizon 7 Cloud Connector. Si el problema persiste, póngase en contacto con el soporte de VMware.

Tareas posteriores a la actualización para habilitar nuevas funciones en la configuración de Horizon

9

Una vez que termine de actualizar los servidores, las máquinas virtuales y el software agente de los grupos de aplicaciones y escritorios, puede ajustar la configuración para utilizar algunas funciones nuevas.

Además utilizar Horizon Administrator para las tareas que se incluyen en los temas de este capítulo (si fuera pertinente), puede usarlo para editar opciones de almacenamiento avanzado de los grupos de escritorios y modificar el ámbito del uso compartido de páginas transparente. De forma predeterminada y como medida de seguridad, las máquinas virtuales de un host ESXi no pueden compartir memoria. Para obtener más información, consulte el tema "Modificar la configuración de un grupo de escritorios existente" del documento *Administración de Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Cambiar el modo de seguridad del mensaje JMS a Mejorada](#)
- [Tareas de actualización de grupos de escritorios para usar la recuperación de espacio](#)
- [Actualizar tareas si usa los almacenes de datos VMware vSAN](#)
- [Configurar la página del portal web de VMware Horizon para los usuarios finales](#)

Cambiar el modo de seguridad del mensaje JMS a Mejorada

Cuando actualiza, se mantiene la opción del modo de seguridad del mensaje JMS existente utilizada en la versión anterior. A partir de Horizon 6 versión 6.1, puede usar Horizon Administrator para cambiar esta opción a **Mejorada**.

Este procedimiento muestra cómo usar Horizon Administrator para cambiar el modo de seguridad del mensaje a **Mejorada** y supervisar el progreso del cambio en todos los componentes de Horizon. De forma alternativa, puede usar la utilidad de la línea de comandos `vdmutil` para cambiar el modo y supervisar el progreso. Consulte el documento *Administración de Horizon 7*.

Nota Con Horizon 6 versión 6.2 y versiones posteriores, puede usar los dispositivos de Access Point en lugar de los servidores de seguridad de Horizon. Access Point utiliza un protocolo HTTP(S) para comunicarse con el servidor de conexión. JMS, IPsec y AJP13 no se utilizan.

Para utilizar los dispositivos de Access Point en lugar de los servidores de seguridad de Horizon, debe actualizar las instancias del servidor de conexión a la versión 6.2 o a una versión posterior antes de instalar y configurar estos dispositivos de forma que se dirijan a instancias del servidor de conexión o al equilibrador de carga que se dirige a las instancias. Si desea obtener más información, consulte *Implementación y configuración de Unified Access Gateway*.

Requisitos previos

Verifique que actualizó todas las instancias de Horizon Connection Server, los servidores de seguridad y los escritorios de Horizon a Horizon 6 versión 6.1 o a una versión posterior. Los componentes de View que sean anteriores a la versión 6.1 de Horizon 6 no se pueden comunicar con una instancia del servidor de conexión 6.1 que usa el modo Mejorado.

Procedimiento

- 1 Configure reglas del firewall back-end de forma que permitan a los servidores de seguridad enviar tráfico JMS en el puerto 4002 a las instancias del servidor de conexión.
- 2 En Horizon Administrator, diríjase a **Configuración de View > Configuración global** y en la pestaña **Seguridad**, establezca **Modo de seguridad Mensaje a Mejorada**.
- 3 De forma manual, reinicie el servicio del componente del bus de mensajería de VMware Horizon en todos los hosts del servidor de conexión o reinicie las instancias del servidor de conexión.

Después de que se reinicien todos los servicios, las instancias del servidor de conexión vuelven a configurar el modo de seguridad del mensaje en todos los escritorios y los servidores de seguridad, cambiando el modo a **Mejorada**.

- 4 Para supervisar el progreso en Horizon Administrator, diríjase a **Configuración de View > Configuración global**.

En la pestaña **Seguridad**, el elemento **Estado de seguridad mejorada** mostrará **Mejorada** cuando todos los componentes hagan la transición al modo Mejorada.

Cuando los servidores se comuniquen con los clientes, estos servidores los configurarán para usar el modo de seguridad del mensaje mejorada.

Tareas de actualización de grupos de escritorios para usar la recuperación de espacio

A partir de vSphere 5.1, Horizon 7 crea máquinas virtuales de clones vinculados en un formato de disco eficiente que permite a los hosts ESXi recuperar el espacio de disco sin usar de los clones vinculados. La actualización de los grupos para usar esta función incluye cambiar la configuración de vCenter Server, de LDAP de View y de las opciones de grupo y, a continuación, recomponer el grupo.

Nota La función de recuperación de espacio no se admite si los escritorios de las máquinas virtuales se alojan en almacenes de datos vSAN o Virtual Volumes.

Aunque la función de recuperación de espacio reduce la cantidad de espacio de disco utilizada para una máquina virtual, solo puede recuperar el espacio que no se utilice. Esta función no puede recuperar el espacio de disco creado por máquinas virtuales que no se optimizaron. Para optimizar una imagen de sistema operativo, puede desactivar servicios de Windows como el servicio indizador, el servicio desfragmentador y los puntos de restauración. Para obtener más información, consulte los temas sobre cómo optimizar el rendimiento de los sistemas operativos invitados Windows, Windows 7 y Windows 8, así como el tema sobre cómo optimizar Windows 7 y Windows 8 para los escritorios de clones vinculados en el documento Configurar grupos de aplicaciones y escritorios en *Configurar escritorios virtuales en Horizon 7*.

Importante Como este procedimiento incluye la recomposición del grupo de escritorios, se perderán todos los cambios que los usuarios finales hagan en el sistema operativo.

- 1 Si no todas las instancias de vCenter Server y los hosts ESXi del grupo tienen la versión 5.1 o posterior de VMware vSphere, actualícelos.

Para obtener más instrucciones, consulte la *Guía de actualización de VMware vSphere*.

- 2 Si no todos los escritorios de las máquinas virtuales del grupo tienen VMware vSphere 5.1 (versión 9 del hardware virtual) o posterior, actualícelos.

- En la máquina virtual principal, actualice VMware Tools a VMware vSphere 5.1 o a una versión posterior y actualice la máquina virtual a la versión más reciente, que debe tener la versión 9 del hardware virtual o una versión posterior.

Para obtener más instrucciones, consulte la *Guía de actualización de VMware vSphere*.

- Realice una snapshot de la máquina virtual principal. Para obtener más instrucciones sobre cómo realizar una snapshot, consulte la ayuda en línea de vSphere Client.
- Use la snapshot de la máquina virtual principal que acaba de crear para recomponer el grupo de escritorios. Para obtener más instrucciones sobre cómo recomponer grupos, haga clic en el botón **Ayuda** de Horizon Administrator.

La recomposición del grupo desde una snapshot de una máquina virtual actualizada es solo un método para actualizar todas las máquinas virtuales en un grupo de clones vinculados. También puede actualizar las máquinas virtuales una a una.

- 3 Actualice el formato de disco usado para las máquinas virtuales.
 - En el host del servidor de conexión, use Editor ADSI para dirigirse al grupo de servidores que pertenece al grupo y cambie el valor del campo **pae-UseSeSparseFormat** de **0** a **1**.
 - Vuelva a componer el grupo de escritorios.
- 4 Use Horizon Administrator para editar la configuración de vCenter Server, diríjase a la pestaña **Almacenamiento** y seleccione **Reclamar espacio de disco de la máquina virtual**.

Para obtener más instrucciones sobre cómo editar la configuración de los servidores, haga clic en el botón **Ayuda** en Horizon Administrator.
- 5 Use Horizon Administrator para editar las opciones del grupo, diríjase a la sección **Almacenamiento avanzado**, seleccione **Reclamar espacio de disco de la máquina virtual** y establezca el umbral de recuperación de espacio en 1 GB.

Actualizar tareas si usa los almacenes de datos VMware vSAN

A partir de vSphere 5.5 Update 1, puede usar la función vSAN para la administración basada en directivas y el almacenamiento de alto rendimiento.

Con vSAN, los discos de almacenamiento físicos conectados que están disponibles en un clúster de los hosts vSphere se agregan a un almacén de datos virtual. Especifique este almacén de datos cuando cree un grupo de escritorios y los distintos componentes, como los archivos de la máquina virtual, las réplicas, los datos de usuario y los archivos del sistema operativo, se ubican en los discos de la unidad de estado sólido (SSD) o los discos duro de conexión directa (HDD).

Horizon 7 define los requisitos del almacenamiento de la máquina virtual, como la capacidad, el rendimiento y la disponibilidad, en forma de perfiles predeterminados de directivas de almacenamiento, según la configuración del grupo usada. El almacenamiento se aprovisiona y se configura automáticamente según las directivas asignadas.

Nota La función de recuperación de espacio no se admite si los escritorios de máquina virtual están alojados en almacenes de datos vSAN.

Actualizar de un almacén de datos sin vSAN a un almacén de datos con vSAN

La actualización de los grupos para que usen almacenes de datos VMware vSAN incluye cambiar una opción de escritorio y, a continuación, volver a equilibrar el grupo.

Las tareas detalladas de este procedimiento describen la actualización de un almacén de datos sin vSAN a uno con vSAN. No se admite la actualización desde un almacén de datos vSAN en un clúster de vSphere 5.5 o una versión anterior (una función de vista previa técnica).

Importante Como este procedimiento incluye la recomposición del grupo de escritorios, se perderán todos los cambios que los usuarios finales hagan en el sistema operativo.

Requisitos previos

- Compruebe que todos los hosts ESXi del clúster utilizado para el grupo estén actualizados a 5.5 Update 1 o a una versión posterior y que cumplan los requisitos del sistema para la función vSAN. VMware recomienda que actualice a vSphere 6.0 o una versión posterior, ya que la función vSAN disponible con vSphere 6.0 y versiones posteriores contiene muchas mejoras de rendimiento en comparación con la función que estaba disponible con vSphere 5.5 Update 1. Con vSphere 6.0, esta función también admite una compatibilidad de hardware (HCL) más amplia.

Para obtener más información sobre las actualizaciones, consulte [Capítulo 6 Actualizar los hosts ESXi y sus máquinas virtuales](#) y la *Guía de actualización de VMware vSphere*. Para obtener más información sobre las actualizaciones y los requisitos de vSAN, consulte el documento *Administrar VMware vSAN*.

- En vCenter Server, compruebe que se agregaron los siguientes privilegios a la función de Composer:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Procedimiento

- 1 Use vCenter Server 5.5 Update 1 o una versión posterior para habilitar vSAN en el clúster de vSphere.

Para obtener más información, consulte el documento *Almacenamiento de vSphere*.

- 2 Actualice el grupo de escritorios a la última versión, tal como se describe en [Actualizar grupos de escritorios de View Composer](#).

Este proceso incluye la instalación de la última versión de Horizon Agent en la máquina virtual principal y la realización de una snapshot.

- 3 Vuelva a componer el grupo en el almacén de datos sin vSAN con la snapshot de la máquina virtual principal que acaba de crear.

Para obtener más instrucciones sobre cómo recomponer grupos, haga clic en el botón **Ayuda** de Horizon Administrator.

- 4 Edite la configuración del grupo de escritorios recientemente actualizado para habilitar la opción de grupo **Usar VMware Virtual SAN**, cambie el almacén de datos desde uno sin vSAN a otro vSAN y use el comando **Reequilibrar**.

Para obtener más instrucciones sobre cómo editar la configuración de los servidores y cómo usar el comando **Reequilibrar**, haga clic en el botón **Ayuda** de Horizon Administrator.

Actualizar desde la versión 1 del formato de disco vSAN

Después de actualizar de VMware vSphere 5.5 Upgrade 1 a vSphere 6.0 o una versión posterior, debe actualizar también el formato del disco vSAN.

VMware recomienda que actualice a vSphere 6.0 o una versión posterior, ya que la función vSAN disponible con vSphere 6.0 y versiones posteriores contiene muchas mejoras de rendimiento en comparación con la función que estaba disponible con vSphere 5.5 Update 1. Con vSphere 6.0, esta función también admite una compatibilidad de hardware (HCL) más amplia.

Importante Este procedimiento describe un proceso de actualización para vSAN si tiene disponibles grupos de escritorios en almacenes de datos vSAN con vSphere 5.5 Update 1 o una versión de actualización posterior. Si los grupos de escritorios no usan almacenes de datos vSAN en ese momento, consulte [Actualizar de un almacén de datos sin vSAN a un almacén de datos con vSAN](#).

La actualización de un almacén de datos VMware vSAN es un proceso de varias fases que incluye la actualización del software vSphere en cada host ESXi y, a continuación, la actualización del formato del disco, realizando este proceso en un grupo de discos al mismo tiempo. Se dedica un capítulo completo al proceso de actualización en el documento de vSphere 6 *Administrar VMware vSAN*. Los pasos del siguiente procedimiento detallan el orden de las tareas que deben realizarse en el nivel del host ESXi en vCenter Server y en el nivel de grupos de escritorios en View Administrator.

Requisitos previos

- Compruebe que los grupos de escritorios utilicen View Agent 6.0 o una versión posterior. Si las máquinas virtuales usan View Agent 5.3.x en los almacenes de datos vSAN, consulte [Actualizar desde Horizon View 5.3.x en un almacén de datos vSAN](#).
- En vCenter Server, compruebe que se agregaron los siguientes privilegios a la función de Composer:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

- Familiarícese con el proceso de actualización de vSAN. Consulte el capítulo sobre cómo actualizar vSAN en el documento *Administrar VMware vSAN*, disponible en <https://docs.vmware.com/es/VMware-vSAN/index.html>.

Procedimiento

- 1 Actualice vCenter Server y los hosts ESXi a vSphere 6 o a una versión posterior, tal y como se describe en el capítulo sobre cómo actualizar el clúster vSAN en el documento *Administrar VMware vSAN*, disponible en el centro de documentación de vSphere 6.0.

En este punto, el grupo de escritorios aún se usa en el formato 1 del disco vSAN y las máquinas virtuales y VMware Tools no se actualizaron a la versión 11 del hardware virtual de vSphere 6.0.

- 2 Actualice el grupo de escritorios a la versión más reciente, tal y como se describe en [Actualizar View Agent o Horizon Agent](#) y en [Actualizar grupos de escritorios de View Composer](#).

Este proceso incluye la instalación de la versión más reciente de Horizon Agent en la máquina virtual principal, en la plantilla de la máquina virtual o en las máquinas virtuales de clones completos en el grupo. Para los grupos de clones vinculados, el proceso también incluye realizar una snapshot y volver a componer el grupo.

Las máquinas virtuales del grupo de escritorios ya tienen View Agent 6.1 o una versión posterior instalada y las máquinas virtuales aún residen en los almacenes de datos vSAN disponibles con vSphere 5.5 Update 1. En este punto, el grupo de escritorios está usando el formato 1 del disco vSAN.

- 3 Actualice la versión del formato del disco vSAN de la versión 1 a la versión 2.

Para obtener más instrucciones, consulte el tema sobre cómo actualizar el formato del disco vSAN que aparece en el capítulo de actualizaciones del documento *Administrar VMware vSAN*, disponible en <https://docs.vmware.com/es/VMware-vSAN/index.html>.

Puede usar la herramienta RVC de la línea de comandos para realizar esta actualización, o bien, si cuenta con vSphere 6 Update 1, puede usar vSphere Web Client. Ruby vSphere Console (RVC) es una consola de línea de comandos basada en Ruby para los hosts VMware ESXi y vCenter Server. RVC se incluye en las versiones de vCenter Server para Linux y para Windows. Para obtener más información sobre cómo usar los comandos RVC, consulte la *guía de referencia de la línea de comandos RVC*.

- 4 Después de que se actualicen los discos en todos los hosts ESXi del clúster en la máquina virtual principal, en la plantilla de la máquina virtual o en las máquinas virtuales completas del grupo, complete estas tareas en el siguiente orden.
 - a Si la máquina virtual principal está en un almacén de datos vSAN, elimine todas las snapshots.

La máquina virtual no puede empezar a usar el nuevo formato de la snapshot disponible con el formato 2 del disco vSAN hasta que se eliminen todas las snapshots anteriores basadas en redoLog. Si la máquina virtual no está en un almacén de datos vSAN, no es obligatorio que elimine las snapshots.
 - b Actualice el hardware de la máquina virtual a la versión 11 y actualice VMware Tools.
- 5 Para los grupos de clones vinculados, realice una nueva snapshot y vuelva a componer el grupo de escritorios mediante la nueva snapshot.

A partir de ese momento, el grupo de escritorios está usando el formato 2 del disco vSAN.

Actualizar desde Horizon View 5.3.x en un almacén de datos vSAN

Horizon 6.0 introdujo nuevas directivas de almacenamiento predeterminadas para vSAN. Estas directivas no se aplican automáticamente a los escritorios de máquinas virtuales existentes que Horizon 7 5.3.x creó en vSAN después de actualizar el grupo de escritorios.

Además, cuando actualiza desde Horizon 7 5.3.x, la opción de grupo **Usar VMware Virtual SAN** no se habilitará automáticamente, aunque el grupo esté en un almacén de datos vSAN. Tiene las siguientes opciones de actualización:

- Si continúa utilizando VMware vSphere 5.5 Update 1, después de actualizar, continúe usando las directivas de almacenamiento predeterminada que se usaron con Horizon 7 5.3.x. Si selecciona esta opción, edite las opciones de grupo de forma que la opción **Usar VMware Virtual SAN** esté habilitada.
- Use el procedimiento descrito en este tema para que el grupo de escritorios utilice las nuevas directivas predeterminadas de almacenamiento. Este procedimiento incluye volver a equilibrar el grupo de escritorios en un almacén de datos sin vSAN y, a continuación, actualizar y volver a equilibrar de nuevo en el almacén de datos vSAN.

Importante Las tareas detalladas en este procedimiento describen una actualización desde un grupo de escritorios Horizon 7 5.3.x con un almacén de datos vSAN en un clúster VMware vSphere 5.5 Update 1. No se admite la actualización desde un almacén de datos vSAN en un clúster VMware vSphere 5.5 o una versión anterior (una función de vista previa técnica).

Además, como este procedimiento incluye la recomposición del grupo de escritorios, se perderán todos los cambios que los usuarios finales hagan en el sistema operativo.

Requisitos previos

- Compruebe que todas las máquinas virtuales del grupo tengan la versión 5.5 de VMware vSphere Update 1 o una versión posterior. VMware recomienda que actualice a VMware vSphere 6.0 o una versión posterior, ya que la función vSAN disponible con vSphere 6.0 y versiones posteriores contiene muchas mejoras de rendimiento en comparación con la función que estaba disponible con vSphere 5.5 Update 1. Con vSphere 6.0, esta función también admite una compatibilidad de hardware (HCL) más amplia.

Para obtener más información sobre las actualizaciones, consulte [Capítulo 6 Actualizar los hosts ESXi y sus máquinas virtuales](#) y la *Guía de actualización de VMware vSphere*. Para obtener más información sobre las actualizaciones y los requisitos de vSAN, consulte el documento *Administrar VMware vSAN*.

- En vCenter Server, compruebe que se agregaron los siguientes privilegios a la función de Composer:

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Procedimiento

- 1 Edite la configuración del grupo de escritorios para cambiar el almacén de datos de uno vSAN a otro sin vSAN y use el comando **Reequilibrar**.

Para obtener más instrucciones sobre cómo editar la configuración de los servidores y cómo usar el comando **Reequilibrar**, haga clic en el botón **Ayuda** de View Administrator.

- 2 Actualice el grupo de escritorios a la última versión, tal como se describe en [Actualizar grupos de escritorios de View Composer](#).

Este proceso incluye la instalación de la última versión de Horizon Agent en la máquina virtual principal y la realización de una snapshot.

- 3 Vuelva a componer el grupo en el almacén de datos sin vSAN con la snapshot de la máquina virtual principal que acaba de crear.

Para obtener más instrucciones sobre cómo recomponer grupos, haga clic en el botón **Ayuda** de View Administrator.

- 4 Edite la configuración del grupo de escritorios que acaba de actualizar para cambiar el almacén de datos de uno sin vSAN a otro con vSAN y use el comando **Reequilibrar**.

Pasos siguientes

Si actualizó las máquinas virtuales a VMware vSphere 6.0, para actualizar de forma que pueda usar vSAN 2 en lugar de vSAN 1, consulte [Actualizar desde la versión 1 del formato de disco vSAN](#).

Configurar la página del portal web de VMware Horizon para los usuarios finales

Puede configurar esta página web para que muestre u oculte el icono para descargar Horizon Client o el icono para conectarse a un escritorio remoto a través de HTML Access. También puede configurar otros vínculos a esta página.

De forma predeterminada, este portal web muestra un icono para descargar e instalar Horizon Client nativo y otro icono para conectarse a través de HTML Access. El vínculo de descarga utilizado se determina a partir de los valores predeterminados definidos en el archivo `portal-links-html-access.properties`.

En algunos casos, sin embargo, es posible que desee que los vínculos dirijan a un servidor web interno o que quiera tener disponibles versiones específicas del cliente en su propio servidor. Puede reconfigurar la página del portal para que dirija a otra URL de descarga modificando el contenido del archivo `portal-links-html-access.properties`. Si ese archivo no está disponible o está vacío y existe el archivo `oslinks.properties`, el archivo `oslinks.properties` se utiliza para determinar el valor de vínculo del archivo de instalador.

El archivo `oslinks.properties` se instala en la carpeta *directorio-de-instalación\VMware\VMware View\Server\broker\webapps\portal\WEB-INF*. Si falta este archivo durante la sesión de HTML Access, el vínculo de descarga redirigirá a los usuarios de forma predeterminada a <https://www.vmware.com/go/viewclients>. El archivo contiene los siguientes valores predeterminados:

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
```



```
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Puede crear vínculos de instalador para sistemas operativos de cliente específicos en el archivo `portal-links-html-access.properties` u `oslinks.properties`. Por ejemplo, si se dirige a la página del portal desde un sistema Mac OS X, aparece el vínculo del instalador Mac OS X nativo. En el caso de los clientes Windows o Linux, puede crear vínculos independientes para instaladores de 32 o 64 bits.

Importante Si actualiza desde el servidor de conexión de View 5.x o una versión anterior y no cuenta con el componente HTML Access instalado y, además, editó previamente la página del portal para que descargue Horizon Client en su propio servidor, estas personalizaciones se podrían ocultar después de instalar el servidor de conexión 6.0 o una versión posterior. Con Horizon 6 o una versión posterior, el componente HTML Access se instala automáticamente durante una actualización del servidor de conexión.

Si ya instaló el componente HTML Access por separado para Horizon 7 5.x, se conservan todas las personalizaciones que realizó para la página web. Si no cuenta con el componente HTML Access instalado, se ocultan todas las personalizaciones. Las personalizaciones de las versiones anteriores se encuentran en el archivo `portal-links.properties`, que ya no se utiliza.

Procedimiento

- 1 En el host del servidor de conexión, abra el archivo `portal-links-html-access.properties` con un editor de texto.

La ubicación de este archivo es `CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties`. Para los sistemas operativos Windows Server 2008, el directorio `CommonAppDataFolder` es `C:\ProgramData`. Para que aparezca la carpeta `C:\ProgramData` en el Explorador de Windows, debe usar el cuadro de diálogo Opciones de carpeta para mostrar las carpetas ocultas.

Si no existe el archivo `portal-links-html-access.properties` y existe el archivo `oslinks.properties`, abra el archivo `<directorio-de-instalación>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` para modificar las URL para usar los archivos de instalador específicos de descarga.

Nota Las personalizaciones de Horizon 7 5.x y versiones anteriores se encuentran en el archivo `portal-links.properties`, que está en el mismo directorio `CommonAppDataFolder\VMware\VDM\portal\` que el archivo `portal-links-html-access.properties`.

2 Edite las propiedades de configuración para establecerlas correctamente.

De forma predeterminada, tanto el icono del instalador como el icono de HTML Access están habilitados y un vínculo lleva a la página de descargas del cliente en el sitio web de VMware. Para deshabilitar un icono, lo que supone que se elimine de la página web, configure la propiedad como `false`.

Nota El archivo `osLinks.properties` solo se puede utilizar para configurar los vínculos en los archivos de instalador específicos. No admite las otras opciones enumeradas debajo.

Opción	Configuración de propiedad
Deshabilitar HTML Access	<code>enable.webclient=false</code> Si esta opción aparece como <code>false</code> pero <code>enable.download</code> está configurada como <code>true</code> , se envía al usuario a una página web para que se descargue el instalador de Horizon Client nativo. Si ambas opciones aparecen como <code>false</code> , el usuario verá el siguiente mensaje: "Póngase en contacto con el administrador local para obtener instrucciones sobre cómo acceder a este servidor de conexión".
Deshabilitar la descarga de Horizon Client	<code>enable.download=false</code> Si esta opción aparece como <code>false</code> pero la opción <code>enable.webclient</code> está configurada como <code>true</code> , se envía al usuario a la página web de inicio de sesión de HTML Access. Si ambas opciones se han establecido como <code>False</code> , el usuario verá el siguiente mensaje: "Póngase en contacto con el administrador local para obtener instrucciones sobre cómo acceder a este servidor de conexión".
Cambiar la URL de la página web para descargar Horizon Client	<code>link.download=https://url_del_servidor_web</code> Use esta propiedad si piensa crear su propia página web.

Opción	Configuración de propiedad
Crear vínculos para instaladores específicos	<p>Los siguientes ejemplos muestran URL completas, pero puede usar URL relativas si coloca los archivos del instalador en el directorio downloads que se encuentra en el directorio C:\Program Files\VMware\VMware View\Server\broker\webapps\ del servidor de conexión, como se describe en el siguiente paso.</p> <ul style="list-style-type: none"> ■ Vínculo general para descargar el instalador: <pre>link.download=https://server/downloads</pre> ■ Instalador de Windows de 32 bits: <pre>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</pre> ■ Instalador para Windows de 64 bits: <pre>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</pre> ■ Instalador de Windows Phone: <pre>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</pre> ■ Instalador de Linux de 32 bits: <pre>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</pre> ■ Instalador de Linux de 64 bits: <pre>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</pre> ■ Instalador para Mac OS X: <pre>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</pre> ■ Instalador para iOS: <pre>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</pre> ■ Instalador para Android: <pre>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</pre> ■ Instalador de Chrome OS: <pre>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</pre>
Cambiar la URL para el vínculo Ayuda en la página de inicio de sesión	<pre>link.help</pre> <p>De forma predeterminada, este vínculo lleva a un sistema de ayuda alojado en el sitio web de VMware. El vínculo Ayuda aparece en la parte inferior de la página</p>

Opción	Configuración de propiedad
	de inicio de sesión.

- 3 Para hacer que los usuarios se descarguen instaladores de una ubicación diferente al sitio web de VMware, ponga los archivos del instalador en el servidor HTTP correspondiente.

Esta ubicación debe corresponderse con las URL que especificó en el archivo `portal-links-html-access.properties` o el archivo `oslinks.properties` durante el paso anterior. Por ejemplo, para situar los archivos en un directorio `downloads` en el host del servidor de conexión, use la siguiente ruta:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Los vínculos a los archivos del instalador pueden usar URL relativas con el formato `/downloads/nombre_archivo_instalador_de_cliente`.

- 4 Reinicie el servicio del componente web de Horizon.

Actualizar los componentes de vSphere independientemente en un entorno de Horizon 7

10

Si actualiza los componentes de vSphere independientemente de los componentes de Horizon 7, debe realizar copias de seguridad de algunos datos de Horizon 7 y volver a reinstalar ciertos software de Horizon 7.

En lugar de realizar una actualización integrada de los componentes de Horizon 7 y de vSphere, puede seleccionar actualizar en primer lugar todos los componentes de Horizon 7 y, a continuación, actualizar los de vSphere, o bien a la inversa. Es posible que quiera actualizar únicamente los componentes de vSphere cuando se publique una versión o actualización nueva de vSphere.

Cuando actualice los componentes de vSphere de forma separada de los componentes de Horizon 7, debe realizar las siguientes tareas adicionales:

- 1 Antes de actualizar vCenter Server, realice una copia de seguridad de la base de datos de vCenter Server y de View Composer.
- 2 Antes de actualizar vCenter Server, realice una copia de seguridad de la base de datos LDAP de Horizon desde una instancia de Horizon Connection Server usando la utilidad `vdmexport.exe`.

Para obtener instrucciones, consulte el documento *Administración de Horizon 7*. Si cuenta con varias instancias del servidor de conexión en un grupo replicado, es necesario que exporte la información desde una única instancia.

- 3 Si usa View Composer, después de actualizar todos los host ESXi que administra una instancia de vCenter Server en concreto, reinicie el servicio de View Composer en ese host.
- 4 Después de actualizar VMware Tools en las máquinas virtuales que se usan como escritorios remotos, vuelva a instalar Horizon Agent.

Al volver a instalar Horizon Agent, se garantiza que las unidades de la máquina virtual sigan siendo compatibles con el resto de componentes de Horizon 7.

Puede encontrar instrucciones paso a paso para ejecutar el instalador de Horizon Agent en el documento *Configurar escritorios virtuales en Horizon 7*.