

Escenarios para configurar certificados TLS para Horizon 7

DICIEMBRE DE 2019
VMware Horizon 7 7.11



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2012-2019 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Escenarios para configurar certificados TLS para Horizon 7 4

1 Obtener certificados TLS de una entidad de certificación 5

- Determinar si este escenario se puede aplicar a su caso 5
- Seleccionar el tipo de certificado correcto 6
- Generar una solicitud de firma del certificado y obtener un certificado con la utilidad certreq de Microsoft 7
 - Crear un archivo de configuración CSR 8
 - Generar una CSR y solicitar un certificado firmado de una CA 10
 - Verificar que la CSR y su clave privada se almacenan en el almacén de certificados de Windows 12
 - Importar un certificado firmado mediante certreq 13
 - Configurar un certificado importado para un servidor de Horizon 7 13

2 Descargar conexiones TLS a servidores intermediarios 15

- Importar los certificados del servidor de descarga TLS a los servidores de Horizon 7 15
 - Descargar un certificado TLS del servidor intermedio 17
 - Descargar una clave privada desde el servidor intermedio 17
 - Convertir un archivo de certificado al formato PKCS#12 18
 - Importar un certificado del servidor SSL a un almacén de certificados de Windows 19
 - Modificar el Nombre descriptivo del certificado 20
 - Importar los certificados raíz e intermedios al almacén de certificados de Windows 21
- Configurar las URL externas del servidor de Horizon 7 para enviar los clientes a los servidores de descarga TLS 22
 - Configurar las URL externas de una instancia del servidor de conexión 22
 - Modificar las URL externas de un servidor de seguridad 23
- Permitir conexiones HTTP desde servidores intermedios 24

Escenarios para configurar certificados TLS para Horizon 7

Escenarios para configurar certificados TLS para Horizon 7 proporciona ejemplos sobre cómo configurar certificados TLS para que los servidores de Horizon 7 los usen. El primer escenario muestra cómo se pueden obtener certificados TLS firmados de una entidad de certificación y cómo se puede garantizar que los certificados estén en un formato que los servidores de Horizon 7 puedan usar. El segundo escenario muestra cómo configurar los servidores de Horizon 7 para descargar conexiones TLS en un servidor intermedio.

Público al que se dirige

Esta información está destinada a cualquier usuario que desee instalar Horizon 7 y necesite obtener certificados TLS que usen los servidores de Horizon 7, o bien para cualquier usuario que use servidores intermedios para descargar conexiones TLS en Horizon 7. La información está escrita para administradores de sistemas Linux o Windows que están familiarizados con la tecnología de máquinas virtuales y operaciones de los centros de datos.

Obtener certificados TLS de una entidad de certificación

1

VMware recomienda que configure certificados TLS firmados por una entidad de certificación (CA) válida para que las instancias del servidor de conexión de Horizon, de View Composer y los servidores de seguridad los utilicen.

Se generan certificados TLS predeterminados cuando instala las instancias de View Composer, del servidor de seguridad y del servidor de conexión. Aunque puede usar los certificados autofirmados predeterminados para realizar pruebas, reemplácelos cuanto antes. Los certificados predeterminados no están firmados por ninguna CA. El uso de certificados que no están firmados por una CA puede permitir que partes que no son de confianza intercepten el tráfico al simular ser su servidor.

En un entorno de Horizon 7, también debe reemplazar el certificado predeterminado que se instala con vCenter Server por un certificado firmado por una CA. Puede usar openTLS para realizar esta tarea en vCenter Server. Para obtener más información, consulte cómo reemplazar los certificados de vCenter Server en el sitio de documentos técnicos de VMware, disponible en <http://www.vmware.com/resources/techresources/>.

Este capítulo incluye los siguientes temas:

- [Determinar si este escenario se puede aplicar a su caso](#)
- [Seleccionar el tipo de certificado correcto](#)
- [Generar una solicitud de firma del certificado y obtener un certificado con la utilidad certreq de Microsoft](#)

Determinar si este escenario se puede aplicar a su caso

Los certificados de Horizon 7 se configuran al importarlos al almacén de certificados del equipo local de Windows en el host del servidor de Horizon 7.

Antes de poder importar un certificado, debe generar una solicitud de firma del certificado (CSR) y obtener un certificado válido y firmado de una CA. Si no se genera la CSR según el procedimiento de ejemplo que se describe en este escenario, el certificado resultante y su clave privada deben estar disponibles en un archivo de formato PKCS #12 (anteriormente denominado PFX).

Existen varias formas de obtener certificados TLS de una entidad de certificación. Este escenario muestra cómo usar la utilidad `certreq` de Microsoft para generar una CSR y obtener un certificado que esté disponible para un servidor Horizon 7. Puede utilizar otro método si tiene las herramientas necesarias instaladas en el servidor y está familiarizado con ellas.

Utilice este escenario para solucionar los problemas siguientes:

- No tiene los certificados TLS firmados por una CA y no sabe cómo obtenerlos
- Tiene certificados TLS válidos y firmados, pero no están en formato PKCS#12 (PFX)

Si su organización le proporciona certificados TLS firmados por una CA, podrá utilizarlos. Su organización puede usar una CA interna válida o una CA comercial de terceros. Si los certificados no están en formato PKCS #12, debe convertirlos. Consulte [Convertir un archivo de certificado al formato PKCS#12](#).

Cuando tiene un certificado firmado y en el formato correcto, puede importarlo al almacén de certificados de Windows y configurar un servidor Horizon 7 para poder usarlo. Consulte [Configurar un certificado importado para un servidor de Horizon 7](#).

Seleccionar el tipo de certificado correcto

Puede usar varios tipos de certificados TLS en Horizon 7. Es muy importante seleccionar el tipo de certificado adecuado para la implementación. Los distintos tipos de certificado tienen un costo diferente, según el número de servidores en los que se puedan utilizar.

Siga las recomendaciones de seguridad de VMware y utilice nombres de dominio plenamente cualificados (FQDN) para sus certificados, independientemente del tipo seleccionado. No utilice un simple nombre de servidor o dirección IP, ni siquiera para comunicaciones dentro de su dominio interno.

Certificado de nombre de servidor único

Es posible generar un certificado con un nombre de sujeto para un servidor específico. Por ejemplo: `dept.company.com`.

Este tipo de certificado resulta útil si, por ejemplo, solo una instancia del servidor de conexión necesita un certificado.

Al enviar una solicitud de firma de certificado a una autoridad de certificación, se proporciona el nombre del servidor que se asociará al certificado. Asegúrese de que el servidor de Horizon 7 pueda resolver el nombre de servidor que proporcione, de manera que coincida con el nombre asociado al certificado.

Nombres alternativos de sujeto

Un nombre alternativo de sujeto (SAN) es un atributo que se puede agregar a un certificado en el momento de su emisión. Este atributo se utiliza para agregar nombres de sujeto (URL) a un certificado, para que pueda validar más de un servidor.

Por ejemplo, se puede emitir un certificado para un servidor con el nombre de host `dept.company.com`. Los usuarios externos que se conecten a Horizon 7 mediante un servidor de seguridad deben utilizar el certificado. Antes de que se emita el certificado, puede agregar el SAN `dept-int.company.com` al certificado para permitir que el certificado se use en las instancias del servidor de conexión o de los servidores de seguridad que se encuentran tras un equilibrador de carga cuando el túnel está habilitado.

Certificado comodín

Un certificado comodín se genera para que se pueda utilizar en varios servicios. Por ejemplo: `*.company.com`.

Un comodín es útil si muchos servidores necesitan un certificado. Si otras aplicaciones de su entorno, además de Horizon 7, necesitan certificados TLS, también puede utilizar un certificado comodín para esos servidores. No obstante, si utiliza un certificado comodín compartido con otros servicios, la seguridad del producto VMware Horizon dependerá también de la seguridad de esos otros servicios.

Nota Solo se puede utilizar un certificado comodín en un único nivel de dominio. Por ejemplo, un certificado comodín con el Nombre del asunto `*.company.com` se puede utilizar para el subdominio `dept.company.com`, pero no para `dept.it.company.com`.

Generar una solicitud de firma del certificado y obtener un certificado con la utilidad `certreq` de Microsoft

Para que un servidor de Horizon 7 pueda acceder a un certificado, debe crear un archivo de configuración, generar una solicitud de firma del certificado (CSR) desde el archivo de configuración y enviar la solicitud firmada a una CA. Cuando la CA devuelve el certificado, debe importar el certificado firmado al almacén de certificados del equipo local Windows del host del servidor de Horizon 7, donde se une la clave privada que se generó previamente.

Se puede generar una CSR siguiendo varios procedimientos, según el modo en que se va a generar el certificado.

La utilidad `certreq` de Microsoft está disponible en Windows Server 2008 R2 y se puede usar para generar una CSR e importar un certificado firmado. Si pretende enviar una solicitud a una CA de terceros, usar `certreq` es el método más rápido y simple de obtener un certificado para Horizon 7.

Procedimiento

1 Crear un archivo de configuración CSR

La utilidad `certreq` de Microsoft usa un archivo de configuración para generar una CSR. Debe crear un archivo de configuración antes de poder generar la solicitud. Cree el archivo y genere la CSR en el equipo Windows Server que aloja el servidor de Horizon 7 que usará el certificado.

2 Generar una CSR y solicitar un certificado firmado de una CA

Con el archivo completo de configuración, puede generar una CSR ejecutando la utilidad `certreq`. Cuando envíe la solicitud a una CA de terceros, esta le devolverá un certificado firmado.

3 Verificar que la CSR y su clave privada se almacenan en el almacén de certificados de Windows

Si usa la utilidad `certreq` para generar una CSR, esta utilidad también genera una clave privada asociada. La utilidad almacena la CSR y la clave privada en el almacén de certificados del equipo local Windows del equipo en el que generó la CSR. Puede confirmar que la CSR y la clave privada se almacenan correctamente usando el complemento Certificados de Microsoft Management Console (MMC).

4 Importar un certificado firmado mediante `certreq`

Si cuenta con un certificado firmado de una CA, puede importarlo al almacén de certificados del equipo local Windows del host del servidor de Horizon 7.

5 Configurar un certificado importado para un servidor de Horizon 7

Después de importar un certificado de servidor al almacén de certificados del equipo local Windows, debe completar unos pasos adicionales para permitir que un servidor de Horizon 7 lo use.

Crear un archivo de configuración CSR

La utilidad `certreq` de Microsoft usa un archivo de configuración para generar una CSR. Debe crear un archivo de configuración antes de poder generar la solicitud. Cree el archivo y genere la CSR en el equipo Windows Server que aloja el servidor de Horizon 7 que usará el certificado.

Requisitos previos

Recopile la información que necesita para completar el archivo de configuración. Debe conocer el FQDN del servidor de Horizon 7 y la unidad organizativa, la organización, la ciudad, la región y el país para completar el Nombre del asunto.

Procedimiento

- 1 Abra un editor de texto y pegue el siguiente texto en el archivo, incluidas las etiquetas de inicio y de final.

```
;----- request.inf -----

[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "CN=FQDN_View_Server, OU=Unidad_Organizativa, O=Organización, L=Ciudad, S=Región,
C=País"
; Replace FQDN_View_Server with the FQDN of the Horizon 7 server.
; Replace the remaining Subject attributes.
KeySpec = 1
KeyLength = 2048
; KeyLength is usually chosen from 2048, 3072, or 4096. A KeyLength
; of 1024 is also supported, but it is not recommended.
HashAlgorithm = SHA256
; Algorithms earlier than SHA-2 are insufficiently secure and are not recommended.
```



```

Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

;-----

```

Si se agregan caracteres CR/LF adicionales a la línea Subject = cuando copia y pega el texto, elimínelos.

- 2 Actualice los atributos de Subject con los valores apropiados para la implementación y el servidor de Horizon 7.

Por ejemplo: CN=dept.company.com

Para cumplir las recomendaciones de seguridad de VMware, use el nombre de dominio plenamente cualificado (FQDN) que utilizan los dispositivos cliente para conectarse al host. No utilice un simple nombre de servidor o dirección IP, ni siquiera para comunicaciones dentro de su dominio interno.

Algunas CA no le permiten usar abreviaturas para el atributo del estado.

- 3 (opcional) Actualice el atributo KeyLength.

El valor predeterminado, 2048, es adecuado si no necesita un tamaño de KeyLength diferente. Muchas CA requieren el valor mínimo 2048. Las claves con un tamaño superior son más seguras pero afectan más al rendimiento.

También se admite un atributo KeyLength de 1024, aunque el Instituto Nacional de Estándares y Tecnología (NIST) no recomienda claves de este tamaño, ya que los equipos tienen cada vez más potencia y pueden descifrar cifrados más seguros.

Importante No genere un valor KeyLength inferior a 1024. Horizon Client para Windows no validará certificados de un servidor de Horizon 7 generado con un valor KeyLength inferior a 1024 y los dispositivos de Horizon Client no podrán conectarse al Horizon 7. El servidor de conexión tampoco validará los certificados, por lo que los servidores de Horizon 7 afectados se mostrarán en rojo en el panel de control de Horizon Administrator.

- 4 Guarde el archivo como request.inf.

Pasos siguientes

Genere una CSR del archivo de configuración.

Generar una CSR y solicitar un certificado firmado de una CA

Con el archivo completo de configuración, puede generar una CSR ejecutando la utilidad `certreq`. Cuando envíe la solicitud a una CA de terceros, esta le devolverá un certificado firmado.

Requisitos previos

- Verifique que completó un archivo de configuración CSR. Consulte [Crear un archivo de configuración CSR](#).
- Realice la operación de `certreq` descrita en este procedimiento en el equipo donde se encuentra el archivo de configuración CSR.

Procedimiento

- 1 Para abrir un símbolo del sistema, haga clic con el botón secundario en **Símbolo del sistema** en el menú **Inicio** y seleccione **Ejecutar como administrador**.
- 2 Acceda al directorio en el que guardó el archivo `request.inf`.
Por ejemplo: `cd c:\certificates`
- 3 Generar el archivo CSR.
Por ejemplo: `certreq -new request.inf certreq.txt`

- 4 Utilice los contenidos del archivo CSR para enviar una solicitud de certificado a la CA, según el proceso de inscripción de la CA.
 - a Al enviar la solicitud a una CA, esta le solicita que seleccione el tipo de servidor en el que instalará el certificado. Como Horizon 7 usa el complemento MMC Certificados de Microsoft para administrar los certificados, seleccione un certificado para un tipo de servidor de Microsoft, Microsoft IIS 7 o similar. La CA debe proporcionar un certificado en el formato requerido para trabajar con Horizon 7.
 - b Si solicita un certificado único de nombre de servidor, use un nombre que los dispositivos de Horizon Client puedan resolver como una dirección IP para este servidor de Horizon 7. El nombre que los equipos usan para conectarse al servidor de Horizon 7 debe coincidir con el nombre asociado al certificado.

Nota La CA puede solicitarle que copie y pegue los contenidos del archivo CSR (como `certreq.txt`) en un formulario web. Puede copiar el contenido del archivo CSR usando un editor de texto. Asegúrese de incluir las etiquetas de inicio y de fin. Por ejemplo:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBQGA1UEBhMNWV5pdGVkIFN0YXRlc2ELMAkGA1UECAwC
Q0ExEjAQBgNVBACMCVBhbG8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMDM15LmNvbXBhbnkuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQfXLIvSCea6nZiIOZYw8Dbn8dgwAqpJdzBbrwuM1TuSnx6bAK8
S52Tv0GxW58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

Después de llevar a cabo algunas comprobaciones en su empresa, la CA crea un certificado de servidor según la información de la CSR, lo firma con la clave privada y se lo envía.

La CA también le envía un certificado raíz y, si es necesario, un certificado intermedio.

- 5 Cambie el nombre del archivo de texto del certificado a `cert.cer`.
Asegúrese de que el archivo esté ubicado en el servidor de Horizon 7 en el que se generó la solicitud de certificado.
- 6 Cambie el nombre de los archivos de certificado intermedio y raíz de la CA a `intermediate.cer` y `root.cer`.

Asegúrese de que los archivos se encuentren en el servidor de Horizon 7 en el que se generó la solicitud de certificado.

Nota No es necesario que estos certificados estén en formato PKCS#12 (PFX) cuando use la utilidad `certreq` para importar los certificados en el almacén de certificados del equipo local Windows. El formato PKCS#12 (PFX) es necesario si usa el asistente Importación de certificado para importar certificados en el almacén de certificados de Windows.

Pasos siguientes

Verifique que el archivo CSR y su clave privada se almacenaron en el almacén de certificados del equipo local Windows.

Verificar que la CSR y su clave privada se almacenan en el almacén de certificados de Windows

Si usa la utilidad `certreq` para generar una CSR, esta utilidad también genera una clave privada asociada. La utilidad almacena la CSR y la clave privada en el almacén de certificados del equipo local Windows del equipo en el que generó la CSR. Puede confirmar que la CSR y la clave privada se almacenan correctamente usando el complemento Certificados de Microsoft Management Console (MMC).

La clave privada se debe unir posteriormente al certificado firmado para que este se importe correctamente y un servidor de Horizon 7 lo utilice.

Requisitos previos

- Verifique que generó una CSR usando la utilidad `certreq` y que solicitó un certificado firmado desde una CA. Consulte [Generar una CSR y solicitar un certificado firmado de una CA](#).
- Familiarícese con el procedimiento para agregar un complemento Certificados en Microsoft Management Console (MMC). Consulte "Agregar el complemento Certificado a MMC" del capítulo sobre cómo configurar los certificados TLS para los servidores de Horizon 7 que aparece en el documento *Instalación de Horizon 7*.

Procedimiento

- 1 En el equipo Windows Server, agregue el complemento Certificados a MMC.
- 2 En la ventana MMC del equipo Windows Server, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Solicitud de inscripción de certificados**.
- 3 Expanda la carpeta **Solicitud de inscripción de certificados** y seleccione la carpeta **Certificados**.
- 4 Verifique que la entrada del certificado aparezca en la carpeta **Certificados**.

Los campos **Emitido a** y **Emitido por** deben mostrar el nombre de dominio que introdujo en el campo **subject:CN** del archivo `request.inf` que se usó para generar la CSR.

- 5 Verifique que el certificado contenga una clave privada siguiendo uno de los siguientes pasos:
 - Compruebe que aparezca una clave amarilla en el icono del certificado.
 - Haga doble clic en el certificado y compruebe que aparezca la siguiente información en el cuadro de diálogo Información del certificado: Tiene una clave privada correspondiente a este certificado.

Pasos siguientes

Importe el certificado en el almacén de certificados del equipo local Windows.

Importar un certificado firmado mediante certreq

Si cuenta con un certificado firmado de una CA, puede importarlo al almacén de certificados del equipo local Windows del host del servidor de Horizon 7.

Si usa la utilidad `certreq` para generar una CSR, la clave privada del certificado es local para el servidor en el que generó la CSR. Para que funcione correctamente, el certificado debe estar combinado con la clave privada. Use el comando `certreq` que se muestra en este procedimiento para garantizar que el certificado y la clave privada se combinan y se importan correctamente al almacén de certificados de Windows.

Si utiliza otro método para obtener un certificado firmado de una CA, puede usar el asistente Importación de certificado del complemento Microsoft Management Console (MMC) para importar un certificado al almacén de certificados de Windows. Este método se describe en el apartado sobre cómo configurar certificados TLS para los servidores de Horizon 7 del documento *Instalación de Horizon 7*.

Requisitos previos

- Verifique que recibió un certificado firmado de una CA. Consulte [Generar una CSR y solicitar un certificado firmado de una CA](#).
- Realice la operación de `certreq` descrita en este procedimiento en el equipo en el que generó una CSR y almacenó el certificado firmado.

Procedimiento

- 1 Para abrir un símbolo del sistema, haga clic con el botón secundario en **Símbolo del sistema** en el menú **Inicio** y seleccione **Ejecutar como administrador**.

- 2 Desplácese al directorio en el que guardó el archivo del certificado firmado, como `cert.cer`.

Por ejemplo: `cd c:\certificates`

- 3 Importe el certificado firmado ejecutando el comando `certreq -accept`.

Por ejemplo: `certreq -accept cert.cer`

El certificado se importa al almacén de certificados del equipo local Windows.

Pasos siguientes

Configure el certificado importado que usará un servidor de Horizon 7. Consulte [Configurar un certificado importado para un servidor de Horizon 7](#).

Configurar un certificado importado para un servidor de Horizon 7

Después de importar un certificado de servidor al almacén de certificados del equipo local Windows, debe completar unos pasos adicionales para permitir que un servidor de Horizon 7 lo use.

Procedimiento

- 1 Compruebe que el certificado de servidor se importó correctamente.

2 Cambie el Nombre descriptivo a **vdm**.

vdm debe estar en minúsculas. Debe cambiar el nombre del resto de certificados que tengan el Nombre descriptivo **vdm** o eliminar el Nombre descriptivo de dichos certificados.

No es necesario que modifique el Nombre descriptivo de los certificados que utiliza View Composer.

3 Instale los certificados CA raíz e intermedios en el almacén de certificados de Windows.

4 Reinicie el servicio del servidor de conexión, el servicio del servidor de seguridad o el servicio de View Composer para permitir que el servicio empiece a usar los nuevos certificados.

5 Si utiliza HTML Access, reinicie el servicio de la puerta de enlace segura Blast de VMware View.

6 Si está configurando un certificado en un View Composer Server, es posible que deba realizar otro paso.

- Si configura el nuevo certificado después de instalar View Composer, debe ejecutar la utilidad SviConfig ReplaceCertificate para reemplazar el certificado que está enlazado al puerto que utiliza View Composer.
- Si configura el nuevo certificado antes de instalar View Composer, no es necesario que ejecute la utilidad SviConfig ReplaceCertificate. Cuando ejecuta el instalador de View Composer, puede seleccionar el nuevo certificado firmado por una CA en lugar del certificado autofirmado predeterminado.

Si desea más información, consulte "Enlazar un nuevo certificado TLS al puerto usado por View Composer" en el documento *Instalación de Horizon 7*.

Para realizar las tareas de este procedimiento, consulte los siguientes temas:

- [Modificar el Nombre descriptivo del certificado](#)
- [Importar los certificados raíz e intermedios al almacén de certificados de Windows](#)

Para obtener más información, consulte "Configurar el servidor de conexión, el servidor de seguridad o View Composer para usar un nuevo certificado TLS" en el documento de *Instalación de Horizon 7*.

Nota El tema "Importar un certificado del servidor SSL a un almacén de certificados de Windows" de *Instalación de Horizon 7* no aparece aquí porque ya importó el certificado de servidor usando la utilidad certreq. No debe usar el asistente Importación de certificado del complemento MMC para volver a importar el certificado.

Sin embargo, puede usar el asistente Importación de certificado para importar el certificado CA raíz en el almacén de certificados de Windows.

Descargar conexiones TLS a servidores intermediarios

2

Puede configurar servidores intermedios entre los servidores de Horizon 7 y los dispositivos de Horizon Client para realizar tareas, como descargar las conexiones TLS y equilibrar la carga. Los dispositivos de Horizon Client se conectan a través de HTTPS a los servidores intermedios, que envían la conexión a las instancias del servidor de conexión o a los servidores de seguridad externos.

Para descargar conexiones TLS a un servidor intermedio, debe completar algunas tareas importantes:

- Importar el certificado TLS que usó el servidor intermedio a los servidores de Horizon 7 externos.
- Establecer las URL externas en los servidores de Horizon 7 externos para que coincidan con la URL que los clientes pueden usar para conectarse al servidor intermedio.
- Permita las conexiones HTTP entre el servidor intermedio y los servidores de Horizon 7.

Este capítulo incluye los siguientes temas:

- [Importar los certificados del servidor de descarga TLS a los servidores de Horizon 7](#)
- [Configurar las URL externas del servidor de Horizon 7 para enviar los clientes a los servidores de descarga TLS](#)
- [Permitir conexiones HTTP desde servidores intermedios](#)

Importar los certificados del servidor de descarga TLS a los servidores de Horizon 7

Si descarga conexiones TLS en un servidor intermedio, debe importar el certificado del servidor intermedio a las instancias del servidor de conexión o a los servidores de seguridad que se conecten al servidor intermedio. El mismo certificado del servidor TLS debe residir en el servidor intermedio de descarga y en cada servidor de Horizon 7 descargado que se conecte al servidor intermedio.

Si implementa los servidores de seguridad, el servidor intermedio y los servidores de seguridad que se conecten a ellos deben tener el mismo certificado TLS. No es necesario instalar el mismo certificado TLS en las instancias del servidor de conexión que están emparejadas con los servidores de seguridad y que no se conectan directamente al servidor intermedio.

Si no implementa los servidores de seguridad o si tiene un entorno mixto de red con algunos servidores de seguridad e instancias del servidor de conexión externas, el servidor intermedio y las instancias del servidor de conexión que se conecten a ellos deben tener el mismo certificado TLS.

Si el certificado del servidor intermedio no está instalado en la instancia del servidor de conexión o el servidor de seguridad, los clientes no pueden validar sus conexiones a Horizon 7. En esta situación, la huella digital del certificado que envía el servidor de Horizon 7 no coincide con el certificado del servidor intermedio al que Horizon Client se conecta.

No confunda equilibrar la carga con descargar TLS. El siguiente requisito se aplica a cualquier dispositivo que esté configurado para proporcionar una descarga TLS, incluidos algunos tipos de equilibradores de carga. Sin embargo, para el equilibrio de carga puro, no es necesario copiar los certificados entre los equipos.

Importante El escenario descrito en los siguientes temas muestra un procedimiento para compartir los certificados TLS entre componentes de tercero y componentes de VMware. Este procedimiento puede no ser útil en todos los casos y no es la única manera de realizar la tarea.

Procedimiento

1 Descargar un certificado TLS del servidor intermedio

Debe descargar el certificado TLS firmado por una CA que está instalado en el servidor, de forma que se pueda importar a los servidores de Horizon 7 externos.

2 Descargar una clave privada desde el servidor intermedio

Debe descargar la clave privada asociada al certificado TLS del servidor intermedio. Se debe importar la clave privada con el certificado en los servidores de Horizon 7.

3 Convertir un archivo de certificado al formato PKCS#12

Si obtuvo un certificado y su clave privada en formato PEM u otro formato diferente, debe convertirlo a PKCS#12 (PFX) antes de poder importar el certificado a un almacén de certificados de Windows de un servidor de Horizon 7. El formato PKCS#12 (PFX) es necesario si usa el asistente Importación de certificado en el almacén de certificados de Windows.

4 Importar un certificado del servidor SSL a un almacén de certificados de Windows

Debe importar el certificado del servidor TLS al almacén de certificados del equipo local Windows en el host de Windows Server en el que están instalados la instancia del servidor de conexión o el servicio del servidor de seguridad.

5 Modificar el Nombre descriptivo del certificado

Si desea configurar un servidor de seguridad o un servidor de conexión para que reconozca y use un certificado TLS, debe cambiar el Nombre descriptivo del certificado a vdm.

6 Importar los certificados raíz e intermedios al almacén de certificados de Windows

Debe importar el certificado raíz y los intermedios de la cadena de certificados al almacén de certificados del equipo local Windows.

Descargar un certificado TLS del servidor intermedio

Debe descargar el certificado TLS firmado por una CA que está instalado en el servidor, de forma que se pueda importar a los servidores de Horizon 7 externos.

Procedimiento

- 1 Conéctese al servidor intermedio y busque los certificados TLS que se presentan a los clientes que envían solicitudes HTTPS.
- 2 Busque y descargue el certificado TLS que se utiliza para Horizon 7.

Ejemplo: Descargue un certificado TLS de un sistema BIG-IP LTM de F5

Este ejemplo usa BIG-IP Local Traffic Manager (LTM) de F5 como servidor intermedio. El ejemplo tiene el propósito de otorgarle una idea general sobre cómo puede descargarse un certificado de su propio servidor intermedio.

Importante Estos pasos son específicos de BIG-IP LTM de F5 y es posible que no se puedan aplicar a versiones más recientes o a otros productos de F5. Los pasos no se aplican a los servidores intermedios de otros proveedores.

Antes de comenzar, compruebe que el sistema BIG-IP LTM de F5 se implementa con Horizon 7. Compruebe que completó las tareas que aparecen en la guía de implementación de F5 sobre cómo *implementar el sistema BIG-IP LTM con VMware View*, que se encuentra en <http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf>.

- 1 Conectar a la utilidad de configuración de BIG-IP LTM de F5.
- 2 En la pestaña Principal del panel de navegación, expanda **Tráfico local** y haga clic en **Certificados SSL**.

La utilidad muestra una lista de certificados instalados en el sistema.

- 3 En la columna Nombre, haga clic en el nombre del certificado que se usa para Horizon 7.
- 4 En la parte inferior de la pantalla, haga clic en **Exportar**.

La utilidad muestra el certificado TLS existente en el cuadro **Texto del certificado**.

- 5 En la opción **Archivo de certificado**, haga clic en **Descargar nombre_archivo**.

El certificado TLS se descarga como un archivo CRT.

Descargar una clave privada desde el servidor intermedio

Debe descargar la clave privada asociada al certificado TLS del servidor intermedio. Se debe importar la clave privada con el certificado en los servidores de Horizon 7.

Procedimiento

- 1 Conéctese al servidor intermedio y busque los certificados TLS que se presentan a los clientes que envían solicitudes HTTPS.

- 2 Busque el certificado que se utiliza para Horizon 7 y descargue la clave privada.

Ejemplo: Descargar una clave privada de un sistema F5 BIG-IP LTM

Este ejemplo usa BIG-IP Local Traffic Manager (LTM) de F5 como servidor intermedio. El ejemplo tiene el propósito de otorgarle una idea general sobre cómo puede descargarse una clave privada de su propio servidor intermedio.

Importante Estos pasos son específicos de BIG-IP LTM de F5 y es posible que no se puedan aplicar a versiones más recientes o a otros productos de F5. Los pasos no se aplican a los servidores intermedios de otros proveedores.

Antes de comenzar, compruebe que esté conectado a la utilidad de configuración de BIG-IP LTM de F5.

- 1 En la pestaña Principal del panel de navegación, expanda **Tráfico local** y haga clic en **Certificados SSL**.

La utilidad muestra una lista de certificados instalados en el sistema.

- 2 En la columna Nombre, haga clic en el nombre del certificado que se usa para Horizon 7.
- 3 En la barra Menú, haga clic en **Clave**.
- 4 En la parte inferior de la pantalla, haga clic en **Exportar**.

La utilidad muestra la clave privada existente en el cuadro **Texto clave**.

- 5 En la opción Archivo de clave, haga clic en **Descargar nombre_archivo..**

La clave privada se descarga como un archivo KEY.

Convertir un archivo de certificado al formato PKCS#12

Si obtuvo un certificado y su clave privada en formato PEM u otro formato diferente, debe convertirlo a PKCS#12 (PFX) antes de poder importar el certificado a un almacén de certificados de Windows de un servidor de Horizon 7. El formato PKCS#12 (PFX) es necesario si usa el asistente Importación de certificado en el almacén de certificados de Windows.

Puede utilizar uno de los siguientes métodos para obtener los archivos de certificado:

- Puede obtener un archivo de almacén de claves del certificado desde una CA.
- Puede descargar un certificado y su clave privada de un servidor intermedio que esté configurado en la implementación de Horizon 7.
- La organización le proporciona los archivos de certificado.

Los archivos de certificado aparecen en varios formatos. Por ejemplo, el formato PEM se suele usar en un entorno Linux. Los archivos pueden tener un archivo de certificado, un archivo de claves y un archivo CSR con las siguientes extensiones:

```
server.crt
server.csr
server.key
```

El archivo CRT contiene el certificado SSL que devolvió la CA. El archivo CSR es el archivo de la solicitud original de firma del certificado y no es necesario. El archivo KEY contiene la clave privada.

Requisitos previos

- Verifique que OpenSSL esté instalado en el sistema. Puede descargar openssl de <http://www.openssl.org>.
- Compruebe que el certificado raíz del certificado SSL que devolvió la CA también esté disponible en el sistema.

Procedimiento

- 1 Copie los archivos KEY y CRT al directorio de instalación OpenSSL.

Por ejemplo: `cd c:\OpenSSL-Win32\bin`

- 2 Abra un símbolo del sistema de Windows y, si es necesario, acceda al directorio de instalación de OpenSSL.
- 3 Genere un archivo de almacén de claves PKCS#12 (PFX) desde el archivo del certificado y la clave privada.

Por ejemplo: `openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile CACert.crt`

En este ejemplo, CACert.crt es el nombre del certificado raíz que devolvió la entidad de certificación.

El almacén de certificados de Windows también acepta un almacén de claves que se generó con una extensión PFX. Por ejemplo: `-out server.pfx`

- 4 Escriba una contraseña de exportación para proteger el archivo PKCS #12 (PFX).

Importar un certificado del servidor SSL a un almacén de certificados de Windows

Debe importar el certificado del servidor TLS al almacén de certificados del equipo local Windows en el host de Windows Server en el que están instalados la instancia del servidor de conexión o el servicio del servidor de seguridad.

Este escenario usa un archivo de certificado en formato PKCS#12 (PFX).

Según el formato del archivo de certificado, toda la cadena de certificados que se encuentra en el archivo del almacén de claves se podría importar al almacén de certificados del equipo local Windows. Por ejemplo, se podrían importar el certificado del servidor, el certificado intermedio y el certificado raíz.

Para otros tipos de archivos de certificado, solo se importa el certificado del servidor al almacén de certificados del equipo local Windows. En este caso, debe realizar pasos independientes para importar el certificado raíz y los certificados intermedios a la cadena de certificados.

Para obtener más información sobre los certificados, consulte la ayuda en línea de Microsoft disponible con el complemento Certificado de MMC.

Requisitos previos

Verifique que el certificado del servidor TLS esté en formato PKCS#12 (PFX). Consulte [Convertir un archivo de certificado al formato PKCS#12](#).

Procedimiento

- 1 En la ventana MMC del host de Windows Server, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal**.
- 2 En el panel Acciones, diríjase a **Más acciones > Todas las tareas > Importar**.
- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenado el certificado.
- 4 Seleccione el archivo del certificado y haga clic en **Abrir**.

Para visualizar el tipo de archivo del certificado, puede seleccionar su formato en el menú desplegable **Nombre de archivo**.
- 5 Escriba la contraseña de la clave privada que se incluye en el archivo del certificado.
- 6 Seleccione **Marcar esta clave como exportable**.
- 7 Seleccione **Incluir todas las propiedades extendidas**.
- 8 Haga clic en **Siguiente** y en **Finalizar**.

El nuevo certificado aparece en la carpeta **Certificados (equipo local) > Personal > Certificados**.
- 9 Verifique que el nuevo certificado contiene una clave privada.
 - a En la carpeta **Certificados (equipo local) > Personal > Certificados**, haga doble clic en el nuevo certificado.
 - b En la pestaña General del cuadro de diálogo Información del certificado, verifique que aparece la siguiente afirmación: Tiene una clave privada correspondiente a este certificado.

Pasos siguientes

Cambie el Nombre descriptivo a **vdm**.

Modificar el Nombre descriptivo del certificado

Si desea configurar un servidor de seguridad o un servidor de conexión para que reconozca y use un certificado TLS, debe cambiar el Nombre descriptivo del certificado a **vdm**.

Requisitos previos

Verifique que el certificado del servidor se importó a la carpeta **Certificados (equipo local) > Personal > Certificados** del almacén de certificados de Windows. Consulte [Importar un certificado del servidor SSL a un almacén de certificados de Windows](#).

Procedimiento

- 1 En la ventana MMC del host de Windows Server, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal > Certificados**.
- 2 Haga clic con el botón secundario en el certificado aplicado al host del servidor de Horizon 7 y haga clic en **Propiedades**.
- 3 En la pestaña General, elimine el texto **Nombre descriptivo** y escriba **vdm**.
- 4 Haga clic en **Aplicar** y en **Aceptar**.
- 5 Verifique que ningún otro certificado del servidor de la carpeta **Personal > Certificados** tenga el Nombre descriptivo **vdm**.
 - a Busque cualquier otro certificado del servidor, haga clic en él con el botón secundario y seleccione **Propiedades**.
 - b Si su Nombre descriptivo es **vdm**, borre el nombre, haga clic en **Aplicar** y luego en **Aceptar**.

Pasos siguientes

Importe el certificado raíz y los certificados intermedios al almacén de certificados del equipo local Windows.

Una vez importados todos los certificados de la cadena, debe reiniciar el servicio del servidor de conexión o del servidor de seguridad para que se implementen los cambios.

Importar los certificados raíz e intermedios al almacén de certificados de Windows

Debe importar el certificado raíz y los intermedios de la cadena de certificados al almacén de certificados del equipo local Windows.

Si el certificado del servidor TLS que importó del servidor intermedio está firmado por una CA raíz que el host del servidor de conexión conoce y en la que confía, y no existen certificados intermedios en las cadenas de certificados, puede omitir esta tarea. Es probable que el host confíe en las entidades de certificación más usadas.

Procedimiento

- 1 En la consola MMC del host de Windows Server, expanda el nodo **Certificados (equipo local)** y diríjase a la carpeta **Entidades de certificación raíz de confianza > Certificados**.
 - Si el certificado raíz está en esta carpeta y no existen certificados intermedios en la cadena de certificados, diríjase al paso 7.
 - Si el certificado raíz está en esta carpeta y existen certificados intermedios en la cadena de certificados, diríjase al paso 6.
 - Si el certificado raíz no se encuentra en esta carpeta, comience en el paso 2.
- 2 Haga clic con el botón secundario en la carpeta **Entidades de certificación raíz de confianza > Certificados** y, a continuación, en **Todas las tareas > Importar**.

- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenada el certificado CA raíz.
- 4 Seleccione el archivo del certificado CA raíz y haga clic en **Abrir**.
- 5 Haga clic en **Siguiente**, vuelva a hacer clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
- 6 Si el certificado del servidor lo firmó una CA intermedia, importe todos los certificados intermedios de la cadena de certificados al almacén de certificados del equipo local Windows.
 - a Diríjase a la carpeta **Certificados (equipo local) > Entidades de certificación intermedias > Certificados**.
 - b Repita del paso 3 al 6 para cada certificado intermedio que se deba importar.
- 7 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.
- 8 Si utiliza HTML Access, reinicie el servicio de la puerta de enlace segura Blast de VMware View.

Configurar las URL externas del servidor de Horizon 7 para enviar los clientes a los servidores de descarga TLS

Si TLS se descarga de un servidor intermedio y los dispositivos de Horizon Client usan el túnel seguro para conectarse a Horizon 7, debe configurar la URL externa del túnel seguro como una dirección que los clientes puedan usar para acceder al servidor intermedio.

Puede configurar las opciones de la URL externa en la instancia del servidor de conexión o en el servidor de seguridad que se conecta al servidor intermedio.

Si implementa los servidores de seguridad, las URL externas son obligatorias para los servidores de seguridad, pero no para las instancias del servidor de conexión que están emparejadas con los servidores de seguridad.

Si no implementa servidores de seguridad o si tiene un entorno de red mixto con algunos servidores de seguridad e instancias del servidor de conexión externas, son necesarias las URL externas para las instancias del servidor de conexión que se conecten al servidor intermedio.

Nota No puede descargar conexiones TLS desde una puerta de enlace segura PCoIP (PSG) o una puerta de enlace segura Blast. La URL externa de PCoIP y la URL externa de la puerta de enlace segura Blast deben permitir a los clientes conectarse a los equipos que alojan la PSG y la puerta de enlace segura Blast. No restablezca la URL externa de PCoIP ni la de Blast para que se dirijan al servidor intermedio, a menos que piense establecer las conexiones TLS como obligatorias entre el servidor intermedio y el servidor de Horizon 7.

Configurar las URL externas de una instancia del servidor de conexión

Horizon Administrator permite configurar las URL externas para una instancia del servidor de conexión.

Requisitos previos

- Compruebe que las conexiones del túnel seguro estén habilitadas en la instancia del servidor de conexión.

Procedimiento

- 1 En Horizon Administrator, haga clic en **Configuración de View > Servidores**.
- 2 Seleccione la pestaña Servidores de conexión; a continuación, seleccione una instancia del servidor de conexión y haga clic en **Editar**.
- 3 Escriba la URL externa del túnel seguro en el cuadro de texto **URL externa**.

La URL debe incluir el protocolo, un nombre de host que pueda resolver el cliente y el número de puerto.

Por ejemplo: **https://myserver.example.com:443**

Nota Puede usar la dirección IP si tiene que acceder a la instancia del servidor de conexión cuando el nombre del host no se puede resolver. Sin embargo, el host con el que contacta no coincide con el certificado TLS que está configurado para la instancia del servidor de conexión, lo cual resulta en un acceso bloqueado o un acceso con seguridad reducida.

- 4 Compruebe que todas las direcciones de este cuadro de diálogo permitan a los sistemas cliente alcanzar esta instancia del servidor de conexión.
- 5 Haga clic en **Aceptar**.

Modificar las URL externas de un servidor de seguridad

Puede usar Horizon Administrator para modificar las URL externas de un servidor de seguridad.

Requisitos previos

- Verifique que las conexiones de túnel de seguridad estén habilitadas en la instancia del servidor de conexión vinculada con el servidor de seguridad.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña Servidores de seguridad, seleccione el servidor de seguridad y haga clic en **Editar**.
- 3 Escriba la URL externa del túnel seguro en el cuadro de texto **URL externa**.

La URL debe incluir el protocolo, un nombre del host del servidor de seguridad que pueda resolver el cliente y el número de puerto.

Por ejemplo: `https://myserver.example.com:443`

Nota Puede usar la dirección IP si tiene acceso al servidor de seguridad cuando el nombre del host no se puede resolver. Sin embargo, el host que contacta no coincide con el certificado TLS que se configura para el servidor de seguridad, lo que deriva en un acceso bloqueado o un acceso con seguridad reducida.

- 4 Verifique que todas las direcciones en este cuadro de diálogo permiten que los sistemas cliente alcancen este host del servidor de seguridad.
- 5 Haga clic en **Aceptar** para guardar los cambios.

Horizon Administrator envía la URL externa actualizada al servidor de seguridad. No necesita reiniciar el servidor de seguridad para que se apliquen los cambios.

Permitir conexiones HTTP desde servidores intermedios

Cuando TLS esté descargado en un servidor intermedio, puede configurar las instancias del servidor de conexión o los servidores de seguridad para permitir las conexiones HTTP desde los dispositivos intermedios y en el lado del cliente. El dispositivo intermedio debe aceptar HTTPS para las conexiones de Horizon Client.

Para permitir conexiones HTTP entre los servidores de Horizon 7 y los dispositivos intermedios, debe configurar el archivo `locked.properties` en cada instancia del servidor de conexión y el servidor de seguridad en el que las conexiones HTTP estén permitidas.

Incluso cuando se permitan las conexiones HTTP entre los servidores de Horizon 7 y los dispositivos intermedios, no puede deshabilitar TLS en Horizon 7. Los servidores de Horizon 7 siguen aceptando las conexiones HTTPS así como las conexiones HTTP.

Nota Si su Horizon Client usa la autenticación por tarjeta inteligente, el cliente debe establecer las conexiones HTTPS directamente al servidor de conexión o al servidor de seguridad. La descarga de TLS no es compatible con la autenticación por tarjeta inteligente.

Procedimiento

- 1 Cree o edite el archivo `locked.properties` en la carpeta de configuración de la puerta de enlace TLS/SSL en el host del servidor de seguridad o del servidor de conexión.

Por ejemplo: `directorio_instalación\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

- 2 Para configurar el protocolo del servidor de Horizon 7, agregue la propiedad `serverProtocol` y configúrela como `http`.

Debe escribir el valor `http` en minúsculas.

- 3 (opcional) Agregue las propiedades para configurar un puerto de escucha HTTP no predeterminado y una interfaz de red en el servidor de Horizon 7.
 - Para cambiar el puerto de escucha HTTP a uno diferente del 80, establezca `serverPortNonTLS` a otro número de puerto al que el dispositivo intermedio esté configurado para conectarse.
 - Si el servidor de Horizon 7 tiene más de una interfaz de red y pretende que el servidor escuche conexiones HTTP en una sola interfaz, establezca `serverHostNonTLS` con la dirección IP de dicha interfaz de red.
- 4 Guarde el archivo `locked.properties`.
- 5 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Ejemplo: archivo `locked.properties`

Este archivo permite las conexiones HTTP sin TLS con el servidor de Horizon 7. La dirección IP de la interfaz de red del lado cliente del servidor de Horizon 7 es 10.20.30.40. El servidor usa el puerto 80 de forma predeterminada para escuchar las conexiones HTTP. El valor `http` debe estar en minúsculas.

```
serverProtocol=http  
serverHostNonTLS=10.20.30.40
```