

Administración 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 © 2014–2018 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y marca comercial](#).

Contenido

Administración de Horizon 7 6

1 Usar Horizon Administrator 7

- Horizon Administrator y el servidor de conexión de Horizon 7
- Iniciar sesión en Horizon Administrator 8
- Consejos para usar la interfaz de Horizon Administrator 9
- Solucionar problemas de visualización de texto en Horizon Administrator 11

2 Configurando el servidor de conexión de Horizon 13

- Configurar vCenter Server y View Composer 13
- Realizar una copia de seguridad del servidor de conexión de Horizon 29
- Configurar las opciones de las sesiones cliente 29
- Habilitar o deshabilitar un servidor de conexión de Horizon 46
- Editar las URL externas 46
- Unirse al programa de experiencia del cliente o abandonarlo 48
- Directorio LDAP de View 49

3 Configurar la autenticación de tarjeta inteligente 51

- Iniciar sesión con una tarjeta inteligente 52
- Configurar la autenticación con tarjeta inteligente en el servidor de conexión de Horizon 53
- Configurar la autenticación con tarjeta inteligente en soluciones de terceros 60
- Preparar Active Directory para la autenticación con tarjeta inteligente 61
- Verificar la configuración de la autenticación con tarjeta inteligente 65
- Uso de la comprobación de revocación de certificados de tarjeta inteligente 66

4 Configurar otros tipos de autenticación de usuario 72

- Uso de la autenticación en dos fases 72
- Uso de la autenticación SAML 77
- Configurar la autenticación biométrica 84

5 Autenticar usuarios sin solicitar las credenciales 85

- Proporcionar acceso sin autenticar para las aplicaciones publicadas 86
- Configurar usuarios para el inicio de sesión híbrido 92
- Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows 94
- Guardar credenciales en Horizon Clients que se encuentren en equipos Mac y dispositivos móviles 95
- Configurar True SSO 96

6	Configurar la administración delegada basada en funciones	127
	Comprender las funciones y los privilegios	127
	Uso de grupos de acceso para delegar la administración de grupos y granjas	128
	Comprender los permisos	130
	Administrar administradores	131
	Administrar y consultar los permisos	133
	Administrar y consultar los grupos de acceso	135
	Administrar funciones personalizadas	138
	Funciones y privilegios predefinidos	139
	Privilegios necesarios para las tareas comunes	146
	Prácticas recomendadas para grupos y usuarios administradores	149
7	Configurar directivas en Horizon Administrator y en Active Directory	150
	Establecer directivas en Horizon Administrator	150
	Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7	153
8	Mantenimiento de los componentes de Horizon 7	161
	Realizar una copia de seguridad y restaurar los datos de configuración de Horizon 7	161
	Supervisar los componentes de Horizon 7	171
	Supervisar el estado de las máquinas	172
	Comprender los servicios de Horizon 7	173
	Cambiar la clave de licencia del producto	175
	Supervisar la licencia y el uso del producto	176
	Actualizar la información general del usuario desde Active Directory	178
	Migrar View Composer a otro equipo	179
	Actualizar los certificados en una instancia del servidor de conexión, en el servidor de seguridad o en View Composer	185
	Programa de mejora de la experiencia de cliente de VMware	187
9	Administrar las aplicaciones ThinApp en Horizon Administrator	188
	Requisitos de Horizon 7 para las aplicaciones ThinApp	188
	Capturar y almacenar paquetes de aplicaciones	189
	Asignar aplicaciones ThinApp a grupos de escritorios y máquinas	193
	Mantenimiento de las aplicaciones ThinApp en Horizon Administrator	202
	Supervisar y solucionar problemas de las aplicaciones ThinApp en Horizon Administrator	206
	Ejemplo de configuración ThinApp	210
10	Configurar clientes en modo de pantalla completa	212
	Configurar clientes en modo de pantalla completa	213

11 Solucionar problemas relacionados con Horizon 7 225

- Usar Horizon Help Desk Tool 225
- Usar VMware Logon Monitor 239
- Usar VMware Horizon Performance Tracker 244
- Supervisar el estado del sistema 249
- Supervisar eventos en Horizon 7 250
- Recopilar información de diagnóstico para Horizon 7 251
- Actualizar las solicitudes de soporte 256
- Solucionar un emparejamiento de servidor de seguridad con el servidor de conexión de Horizon que no se realizó correctamente 257
- Solucionar problemas relacionados con la comprobación de revocación de certificados de Horizon 7 Server 258
- Solucionar problemas relacionados con la comprobación de revocación de la tarjeta inteligente 259
- Más información para solucionar problemas 260

12 Usar el comando vdmadmin 261

- Uso del comando vdmadmin 263
- Configurar los registros en Horizon Agent con la opción -A 266
- Sobrescribir direcciones IP con la opción -A 268
- Actualizar las entidades de seguridad externa con la opción -F 269
- Enumerar y mostrar las supervisiones de estado con la opción -H 270
- Especificar y visualizar informes sobre el funcionamiento de Horizon 7 con la opción -I 271
- Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -I 273
- Asignar máquinas dedicadas usando la opción -L 274
- Visualizar información sobre las máquinas con la opción -M 276
- Recuperar espacio de disco de las máquinas virtuales con la opción -M 277
- Configurar filtros de dominios con la opción -N 279
- Configurar los filtros de dominios 282
- Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P 286
- Configurar clientes en modo de pantalla completa con la opción -Q 288
- Visualizar el primer usuario de un equipo con la opción -R 293
- Eliminar una entrada de una instancia del servidor de conexión o del servidor de seguridad con la opción -S 294
- Proporcionar credenciales secundarias para los administradores con la opción -T 295
- Visualizar información sobre los usuarios con la opción -U 297
- Bloquear o desbloquear las máquinas virtuales con la opción -V 298
- Detectar y resolver conflictos de esquemas y entradas LDAP usando la opción -X 299

Administración de Horizon 7

Administración de Horizon 7 describe cómo configurar y administrar VMware Horizon 7[®], incluido cómo configurar el servidor de conexión de Horizon, crear administradores, configurar la autenticación de los usuarios, configurar las directivas y administrar las aplicaciones de VMware ThinApp[®] en Horizon Administrator. Este documento también describe cómo mantener y solucionar los problemas de los componentes de Horizon 7.

Público al que se dirige

Esta información está destinada para cualquier persona que desee configurar y administrar VMware Horizon 7. La información está escrita para administradores de sistemas Linux o Windows que están familiarizados con la tecnología de máquinas virtuales y operaciones de los centros de datos.

Usar Horizon Administrator

Horizon Administrator se encuentra en la interfaz web en la que configura el servidor de conexión de Horizon y administra las aplicaciones y los escritorios remotos.

Para comparar las operaciones que puede realizar con Horizon Administrator, con los cmdlets y `vdadmin`, consulte el documento *Integración de Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Horizon Administrator y el servidor de conexión de Horizon](#)
- [Iniciar sesión en Horizon Administrator](#)
- [Consejos para usar la interfaz de Horizon Administrator](#)
- [Solucionar problemas de visualización de texto en Horizon Administrator](#)

Horizon Administrator y el servidor de conexión de Horizon

Horizon Administrator proporciona una interfaz de administración basada en Web para Horizon 7.

El servidor de conexión de Horizon puede tener varias instancias que funcionan de servidores de réplica o servidores de seguridad. En función de la implementación de Horizon 7, puede obtener una interfaz de Horizon Administrator con cada instancia de un servidor de conexión.

Utilice las siguientes prácticas recomendadas para usar Horizon Administrator con un servidor de conexión:

- Use el nombre de host y la dirección IP del servidor de conexión para iniciar sesión en Horizon Administrator. Use la interfaz de Horizon Administrator para administrar el servidor de conexión, así como cualquier servidor de seguridad asociado o servidor de réplica.
- En un entorno de pod, compruebe que todos los administradores utilicen el nombre de host y la dirección IP del mismo servidor de conexión para iniciar sesión en Horizon Administrator. No utilice el nombre de host ni la dirección IP del equilibrador de carga para acceder a la página web de Horizon Administrator.

- Para identificar el pod del servidor de conexión con el que está trabajando, puede ver el nombre del pod en el encabezado de Horizon Administrator y en la pestaña del navegador web.

Nota Si usa dispositivos de Unified Access Gateway en lugar de servidores de seguridad, debe usar la REST API de Unified Access Gateway para administrar los dispositivos de Unified Access Gateway. Las versiones anteriores de Unified Access Gateway se denominan Access Point. Si desea obtener más información, consulte *Implementación y configuración de Unified Access Gateway*.

Iniciar sesión en Horizon Administrator

Para realizar tareas iniciales de configuración, debe iniciar sesión en Horizon Administrator. Acceda a Horizon Administrator usando una conexión segura (TLS).

Requisitos previos

- Verifique que el servidor de conexión de Horizon esté instalado en un equipo dedicado.
- Verifique que esté usando un navegador web compatible con Horizon Administrator. Para obtener más información sobre los requisitos de Horizon Administrator, consulte el documento *Instalación de Horizon 7*.

Procedimiento

- 1 Abra el navegador web e introduzca la siguiente URL, donde *servidor* es el nombre del host de la instancia del servidor de conexión.

`https://servidor/administrador`

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

El acceso a Horizon Administrator depende del tipo de certificado que esté configurado en el equipo del servidor de conexión.

Si abre el navegador web en el host del servidor de conexión, use **`https://127.0.0.1`** para conectarse en lugar de **`https://localhost`**. Este método mejora la seguridad evitando ataques DNS potenciales en la resolución `localhost`.

Opción	Descripción
Configuró un certificado firmado por una CA para el servidor de conexión de View.	Cuando se conecta por primera vez, el navegador web muestra Horizon Administrator.
Se configura el certificado autofirmado y predeterminado proporcionado con el servidor de conexión de View.	Cuando se conecte por primera vez, el navegador web puede mostrar una página que advierte que ninguna entidad de certificación expidió el certificado de seguridad asociado a la dirección. Haga clic en Ignorar para continuar usando el certificado TLS actual.

2 Inicie sesión con una cuenta que tenga la función Administradores.

Debe realizar una asignación inicial a la función Administradores cuando instale una instancia del servidor de conexión independiente o la primera instancia del servidor de conexión en un grupo replicado. De forma predeterminada, se selecciona la cuenta que use para instalar el servidor de conexión, pero puede cambiar esta cuenta al grupo local de administradores o a un grupo global de dominio.

Si selecciona el grupo de administradores locales, puede usar cualquier usuario de dominio agregado a este grupo directamente o mediante la pertenencia al grupo global. No puede usar usuarios locales que estén agregados a este grupo.

Después de iniciar sesión en Horizon Administrator, puede usar **Configuración de View > Administradores** para cambiar la lista de usuarios y grupos que tengan la función Administradores.

Consejos para usar la interfaz de Horizon Administrator

Las funciones de la interfaz de usuario de Horizon Administrator permiten acceder a las páginas de Horizon, así como buscar, filtrar y ordenar objetos de Horizon.

Horizon Administrator incluye muchas funciones comunes de la interfaz de usuario. Por ejemplo, el panel de navegación situado en la parte izquierda de cada página le dirige a otras páginas de Horizon Administrator. Los filtros de búsqueda le permiten seleccionar criterios de filtros relacionados con los objetos que está buscando.

La siguiente tabla describe algunas funciones adicionales que le pueden ayudar a usar Horizon Administrator.

Tabla 1-1. Funciones de visualización y de navegación de Horizon Administrator

Función de Horizon Administrator	Descripción
Navegar hacia delante o hacia atrás en las páginas de Horizon Administrator	<p>Haga clic en el botón Atrás del navegador para volver a la página de Horizon Administrator en la que se encontraba antes. Haga clic en el botón Adelante para volver a la página actual.</p> <p>Si hace clic en el botón Atrás mientras utiliza un cuadro de diálogo o un asistente de Horizon Administrator, vuelve a la página principal de Horizon Administrator. Se pierde la información que introdujo en el asistente o en el cuadro de diálogo.</p> <p>En las versiones anteriores a la versión 5.1 de View, no era posible utilizar los botones Atrás y Adelante para navegar por Horizon Administrator. Se proporcionan botones Atrás y Adelante independientes en la ventana Horizon Administrator para la navegación. Estos botones se eliminan en la versión 5.1 de View.</p>
Marcar las páginas de Horizon Administrator	Puede marcar las páginas de Horizon Administrator en el navegador.

Tabla 1-1. Funciones de visualización y de navegación de Horizon Administrator (Continuación)

Función de Horizon Administrator	Descripción
Ordenación en varias columnas	<p>Puede ordenar objetos de Horizon de formas distintas si utiliza la ordenación en varias columnas.</p> <p>Haga clic en un encabezado de la fila superior de una tabla de Horizon Administrator para ordenar los objetos de Horizon siguiendo un orden alfabético según dicho encabezado.</p> <p>Por ejemplo, en la página Recursos > Máquinas, puede hacer clic en Grupo de escritorios para ordenar los escritorios según los grupos que los contienen.</p> <p>El número 1 aparece junto al encabezado para indicar que es la columna de ordenación primaria. Puede volver a hacer clic en el encabezado para invertir el orden, que se indica con una flecha hacia arriba o hacia abajo.</p> <p>Para ordenar los objetos de Horizon por un elemento secundario, pulse Ctrl y haga clic en otro encabezado.</p> <p>Por ejemplo, en la tabla Máquinas, puede hacer clic en Usuarios para realizar una ordenación secundaria por los usuarios a los que los escritorios están dedicados.</p> <p>El número 2 aparece junto al encabezado secundario. En este ejemplo, los escritorios están ordenados por grupo y por los usuarios dentro de cada grupo.</p> <p>Si pulsa Ctrl y hace clic, puede continuar ordenando todas las columnas de la tabla siguiendo un orden descendente de importancia.</p> <p>Pulse Ctrl+Mayús y haga clic para desmarcar un elemento de ordenación.</p> <p>Por ejemplo, es posible que quiera visualizar los escritorios de un grupo que está en un estado en concreto y se almacena en un almacén de datos concreto.</p> <p>Seleccione Recursos > Máquinas, haga clic en el encabezado Almacén de datos y, a continuación, pulse Ctrl y haga clic en el encabezado Estado.</p>
Personalizar las columnas de las tablas	<p>Puede personalizar la visualización de las columnas de las tablas de Horizon Administrator si oculta las columnas seleccionadas y bloquea la primera. Esta función le permite controlar la visualización de tablas grandes como Catálogo > Grupos de escritorios que contienen varias columnas.</p> <p>Haga clic con el botón secundario en cualquier encabezado de columna para que aparezca un menú contextual que le permita realizar las siguientes acciones:</p> <ul style="list-style-type: none"> ■ Ocultar la columna seleccionada. ■ Personalizar columnas. Un cuadro de diálogo muestra todas las columnas de una tabla. Puede seleccionar las columnas que desea mostrar u ocultar. ■ Bloquee la primera columna. Esta opción hace que la columna de la izquierda se siga mostrando al desplazarse de forma horizontal en una tabla que tiene varias columnas. Por ejemplo, en la página Catálogo > Grupos de escritorios, la ID del escritorio se sigue mostrando si se desplaza de forma horizontal para ver otras características del escritorio.

Tabla 1-1. Funciones de visualización y de navegación de Horizon Administrator (Continuación)

Función de Horizon Administrator	Descripción
Seleccionar objetos de Horizon y mostrar sus detalles	<p>En las tablas de Horizon Administrator que muestran los objetos de Horizon, puede seleccionar un objeto o mostrar sus detalles.</p> <ul style="list-style-type: none"> ■ Para seleccionar un objeto, haga clic en cualquier punto en la fila del objeto de la tabla. En la parte superior de la página, se activan los menús y los comandos que administran los objetos. ■ Para visualizar los detalles de los objetos, haga doble clic en la celda izquierda de la fila del objeto. Una nueva página muestra los detalles del objeto. <p>Por ejemplo, en la página Catálogo > Grupos de escritorios, haga clic en cualquier punto de una fila de un grupo individual para activar los comandos que afecten al grupo.</p> <p>Haga doble clic en la celda ID de la columna izquierda para mostrar una página nueva que contenga todos los detalles sobre el grupo.</p>
Ampliar los cuadros de diálogos para ver los detalles	<p>Puede ampliar los cuadros de diálogos de Horizon Administrator para ver más información en las columnas de la tabla, como nombres de escritorios y nombres de usuarios.</p> <p>Para ampliar un cuadro de diálogo, coloque el mouse sobre los puntos que aparecen en la esquina inferior derecha del cuadro de diálogo y arrastre la esquina.</p>
Mostrar los menús contextuales de los objetos de Horizon	<p>Puede hacer clic con el botón secundario en los objetos de Horizon que aparecen en las tablas de Horizon Administrator para visualizar los menús contextuales. Un menú contextual le proporciona acceso a los comandos que funcionan en el objeto de Horizon seleccionado.</p> <p>Por ejemplo, en la página Catálogo > Grupos de escritorios, puede hacer clic con el botón secundario en un grupo de escritorios para mostrar comandos tales como Agregar, Editar, Eliminar, Deshabilitar (o Habilitar) aprovisionamiento, etc.</p>

Solucionar problemas de visualización de texto en Horizon Administrator

Si el navegador web se ejecuta en un sistema operativo que no sea Windows, como Linux, UNIX o Mac OS, el texto de Horizon Administrator no aparece correctamente.

Problema

El texto de la interfaz de Horizon Administrator aparece distorsionado. Por ejemplo, aparecen espacios dentro de palabras.

Causa

Son necesarias fuentes específicas de Microsoft para Horizon Administrator.

Solución

Instale las fuentes específicas de Microsoft en su equipo.

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

Configurando el servidor de conexión de Horizon

2

Tras instalar y realizar la configuración inicial del servidor de conexión de Horizon, puede agregar instancias de vCenter Server y servicios View Composer a la implementación de Horizon 7, establecer funciones para delegar responsabilidades de administrador y programar copias de seguridad para los datos de configuración.

Este capítulo incluye los siguientes temas:

- [Configurar vCenter Server y View Composer](#)
- [Realizar una copia de seguridad del servidor de conexión de Horizon](#)
- [Configurar las opciones de las sesiones cliente](#)
- [Habilitar o deshabilitar un servidor de conexión de Horizon](#)
- [Editar las URL externas](#)
- [Unirse al programa de experiencia del cliente o abandonarlo](#)
- [Directorio LDAP de View](#)

Configurar vCenter Server y View Composer

Para usar las máquinas virtuales como escritorios remotos, debe configurar View para que se comuniquen con vCenter Server. Para crear y administrar grupos de escritorios de clones vinculados, debe configurar las opciones de View Composer en Horizon Administrator.

También puede configurar las opciones de almacenamiento para Horizon 7. Puede permitir que los hosts ESXi recuperen el espacio de disco en máquinas virtuales de clones vinculados. Para permitir que los hosts ESXi almacenen en caché los datos de las máquinas virtuales, debe habilitar el acelerador de almacenamiento de View para vCenter Server.

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

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

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

Procedimiento

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

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

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

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

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

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

Pasos siguientes

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

Agregar instancias de vCenter Server a Horizon 7

Debe configurar Horizon 7 para conectarse a las instancias de vCenter Server en la implementación de Horizon 7. vCenter Server crea y administra las máquinas virtuales que Horizon 7 utiliza en grupos de escritorios.

Si ejecuta instancias de vCenter Server en un grupo Linked Mode, debe agregar cada instancia de vCenter Server a Horizon 7 de forma independiente.

Horizon 7 se conecta a la instancia de vCenter Server mediante un canal seguro (SSL).

Requisitos previos

- Instale la clave de licencia del servidor de conexión.
- Prepare un usuario de vCenter Server con permiso para realizar las operaciones necesarias en vCenter Server para admitir Horizon 7. Para usar View Composer, otorgue al usuario privilegios adicionales.

Si desea obtener más detalles sobre la configuración de un usuario de vCenter Server para Horizon 7, consulte el documento *Instalación de Horizon 7*.

- Compruebe que el host de vCenter Server tenga instalado un certificado de servidor TLS/SSL. En entornos de producción, instale un certificado válido firmado por una autoridad de certificación (AC).

En entornos de pruebas, puede usar el certificado predeterminado instalado en vCenter Server, pero debe aceptar la huella digital del certificado cuando agregue vCenter Server a Horizon 7.

- Compruebe que todas las instancias del servidor de conexión en el grupo replicado confíen en el certificado raíz de CA para el certificado del servidor instalado en el host de vCenter Server. Asegúrese de que el certificado raíz de CA se encuentre en la carpeta **Autoridades de certificación raíz de confianza > Certificados** en el almacén de certificados local de Windows de los hosts del servidor de conexión. En caso contrario, importe el certificado raíz de AC en el almacén de certificados del equipo local de Windows.

Consulte "Importar un certificado raíz e intermedios al almacén de certificados de Windows" en el documento *Instalación de Horizon 7*.

- Compruebe que la instancia de vCenter Server contenga hosts ESXi. Si no se configuraron hosts en la instancia de vCenter Server, no podrá agregar la instancia a Horizon 7.
- Si actualiza a la versión vSphere 5.5 o una posterior, compruebe que un usuario local vCenter Server haya otorgado permisos específicos para iniciar sesión en vCenter Server a la cuenta de administrador de dominio que utiliza como usuario de dicho servicio.
- Si piensa utilizar Horizon 7 en modo FIPS, compruebe que tenga instalado vCenter Server 6.0 y hosts ESXi 6.0 o versiones posteriores.

Si desea obtener más información, consulte "Instalar Horizon 7 en modo FIPS" en el documento *Instalación de Horizon 7*.

- Familiarícese con la configuración que determina el número máximo de operaciones para vCenter Server y View Composer. Consulte [Límites de operaciones simultáneas para vCenter Server y View Composer](#) y [Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **vCenter Servers**, haga clic en **Agregar**.
- 3 En el cuadro de texto **Dirección del servidor** en la configuración de vCenter Server, escriba el nombre de dominio plenamente cualificado (fully qualified domain name, FQDN) de la instancia de vCenter Server.

El FQDN incluye el nombre de host y el de dominio. Por ejemplo: en el FQDN

myserverhost.companydomain.com, **myserverhost** es el nombre de host y **companydomain.com** es el dominio.

Nota Si ingresa en un servidor con un nombre DNS o una URL, Horizon 7 no realiza una búsqueda DNS para comprobar si el administrador añadió anteriormente este servidor a Horizon 7 con su dirección IP. Si agrega un servidor vCenter Server con su nombre DNS y dirección IP, se produce un conflicto.

- 4 Escriba el nombre del usuario vCenter Server.
Por ejemplo, **domain\user** o **user@domain.com**
- 5 Escriba la contraseña del usuario vCenter Server.
- 6 (opcional) Escriba una descripción para esta instancia de vCenter Server.
- 7 Escriba el número de puerto TCP.
El puerto predeterminado es 443.
- 8 En Configuración avanzada, establezca el límite de las operaciones simultáneas en vCenter Server y View Composer.
- 9 Haga clic en **Siguiente** para mostrar la página de Configuración de View Composer.

Pasos siguientes

Configure las opciones de View Composer.

- Si la instancia de vCenter Server se configura con un certificado SSL firmado y el servidor de conexión confía en el certificado raíz, el asistente para agregar vCenter Server muestra la página Configuración de View Composer.

- Si la instancia de vCenter Server se configura con un certificado predeterminado, primero debe determinar si acepta la huella digital del certificado existente. Consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

Si Horizon 7 utiliza varias instancias de vCenter Server, repita este procedimiento para agregar las demás instancias de vCenter Server.

Configurar las opciones de View Composer

Para usar View Composer, debe configurar las opciones que permiten a Horizon 7 conectarse al servicio VMware Horizon View Composer. View Composer se puede instalar en su propio host independiente o en el mismo host que vCenter Server.

Debe realizarse una asignación uno a uno entre el servicio VMware Horizon View Composer y la instancia de vCenter Server. Un servicio View Composer puede funcionar con solo una instancia de vCenter Server. Una instancia de vCenter Server puede asociarse con solo un servicio VMware Horizon View Composer.

Tras la implementación inicial de Horizon 7, puede migrar el servicio VMware Horizon View Composer a un nuevo host para admitir una implementación creciente o variable de Horizon 7. Puede editar la configuración inicial de View Composer en Horizon Administrator, pero debe realizar pasos adicionales para asegurarse de que la migración se realizó correctamente. Consulte [Migrar View Composer a otro equipo](#).

Requisitos previos

- Compruebe que creó un usuario en Active Directory con permiso para agregar y eliminar máquinas virtuales del dominio de Active Directory que incluye clones vinculados. Consulte [Crear una cuenta de usuario para operaciones en AD de View Composer](#).
- Compruebe que Horizon 7 esté configurado para conectarse a vCenter Server. A tal efecto, debe completar la página de Información de vCenter Server en el asistente para Agregar vCenter Server. Consulte [Agregar instancias de vCenter Server a Horizon 7](#).
- Compruebe que el servicio VMware Horizon View Composer aún no esté configurado para conectarse a otra instancia de vCenter Server.

Procedimiento

- 1 En Horizon Administrator, complete la página Información de vCenter Server en el asistente Agregar vCenter Server.
 - a Seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, haga clic en **Agregar** y configure las opciones de vCenter Server.

- 2 En la página de Configuración de View Composer, si no está utilizando dicho componente, seleccione **No utilizar View Composer**.

Si selecciona **No utilizar View Composer**, el resto de opciones de configuración de View Composer quedan inactivas. Al hacer clic en **Siguiente**, el asistente para Agregar vCenter Server muestra la página de Configuración de almacenamiento. No incluye la página de Dominios de View Composer.

- 3 Si está utilizando View Composer, seleccione la ubicación del host de View Composer.

Opción	Descripción
View Composer está instalado en el mismo host que vCenter Server.	<p>a Seleccione View Composer instalado conjuntamente con vCenter Server.</p> <p>b Asegúrese de que el número de puerto sea el mismo que se especificó cuando se instaló el servicio VMware Horizon View Composer en vCenter Server. El puerto predeterminado es el 18443.</p>
View Composer está instalado en su propio host independiente.	<p>a Seleccione Servidor View Composer independiente.</p> <p>b En el cuadro de texto de la dirección del servidor de View Composer, escriba el nombre de dominio plenamente cualificado (fully qualified domain name, FQDN) en el host de View Composer.</p> <p>c Escriba el nombre de usuario de View Composer. Por ejemplo, domain.com\user o user@domain.com</p> <p>d Escriba la contraseña de usuario de View Composer.</p> <p>e Asegúrese de que el número de puerto sea el mismo que se especificó cuando se instaló el servicio VMware Horizon View Composer. El puerto predeterminado es el 18443.</p>

- 4 Haga clic en **Siguiente** para mostrar la página de Dominios de View Composer.

Pasos siguientes

Configure los dominios de View Composer.

- Si la instancia de View Composer está configurada con un certificado TLS firmado y el servidor de conexión confía en el certificado raíz, el asistente Agregar vCenter Server muestra la página Dominios de View Composer.
- Si la instancia de View Composer está configurada con un certificado predeterminado, debe determinar primero si acepta la huella digital del certificado existente. Consulte [Aceptar la huella digital de un certificado TLS predeterminado](#).

Configurar los dominios de View Composer

Debe configurar un dominio de Active Directory en el que View Composer implemente escritorios de clonación vinculada. Puede configurar varios dominios en View Composer. Después de agregar por primera vez la configuración de View Composer y vCenter Server a View, puede agregar más dominios de View Composer editando la instancia de vCenter Server en Horizon Administrator.

Requisitos previos

- El administrador de Active Directory debe crear un usuario de View Composer para las operaciones de AD. Este usuario de dominio debe tener permiso para agregar y eliminar máquinas virtuales del dominio de Active Directory que incluya clones vinculados. Para obtener más información sobre los permisos necesarios para este usuario, consulte [Crear una cuenta de usuario para operaciones en AD de View Composer](#).
- En Horizon Administrator, compruebe que completó las páginas Información de vCenter Server y Configuración de View Composer en el asistente Agregar vCenter Server.

Procedimiento

- 1 En la página Dominios de View Composer, haga clic en **Agregar** para agregar el usuario de View Composer que se usará en las operaciones de AD de información de cuenta.
- 2 Introduzca el nombre de dominio de Active Directory.
Por ejemplo: **domain.com**
- 3 Introduzca el nombre de usuario del dominio, del usuario de View Composer incluido el nombre de dominio.
Por ejemplo: **domain.com\admin**
- 4 Introduzca la contraseña de la cuenta.
- 5 Haga clic en **Aceptar**.
- 6 Para agregar cuentas de usuario del dominio con privilegios en otros dominios de Active Directory en el que implementa grupos de clonación vinculada, repita los pasos anteriores.
- 7 Haga clic en **Siguiente** para mostrar la página de Configuración de almacenamiento.

Pasos siguientes

Habilite la reclamación de espacio de disco de la máquina virtual y configure el acelerador de almacenamiento de View para Horizon 7.

Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados

En vSphere 5.1 y versiones posteriores, puede habilitar la función de recuperación de espacio de disco de Horizon 7. A partir de vSphere 5.1, Horizon 7 crea máquinas virtuales de clones vinculados con formato de disco eficiente. Dicho formato permite que los hosts ESXi recuperen espacio de disco sin usar en los clones vinculados, con lo que se reduce el espacio de almacenamiento total necesario para los clones vinculados.

A medida que los usuarios interactúan con escritorios de clones vinculados, los discos de SO clonados crecen y pueden incluso usar tanto espacio de disco como los escritorios de clones completos. La recuperación de espacio de disco reduce el tamaño de los discos de SO sin necesidad de actualizar o recomponer los clones vinculados. Se puede recuperar el espacio mientras las máquinas virtuales están encendidas y los usuarios interactúan con sus escritorios remotos.

La recuperación de espacio de disco es especialmente útil para implementaciones que no pueden aprovechar las ventajas que ofrecen las estrategias de ahorro de almacenamiento, como actualizar al cerrar sesión. Por ejemplo, los trabajadores de conocimiento que instalan aplicaciones de usuario en escritorios remotos dedicados pueden perder sus aplicaciones personales si los escritorios remotos se actualizan o recomponen. Con la recuperación de espacio de disco, Horizon 7 puede mantener los clones vinculados casi al tamaño reducido con el que empezaron cuando se aprovisionaron por primera vez.

Esta función tiene dos componentes: formato de disco eficiente de espacio y operaciones de recuperación de espacio.

En vSphere 5.1 y entornos con una versión posterior, cuando la versión del hardware virtual de una máquina principal es 9 o posterior, Horizon 7 crea clones vinculados con discos de SO eficientes, estén o no habilitadas las operaciones de recuperación de espacio.

Debe usar Horizon Administrator para habilitar la recuperación de espacio en vCenter Server y recuperar espacio de disco de las máquinas virtuales para los grupos de escritorios individuales. La configuración de recuperación de espacio en vCenter Server presenta la opción de deshabilitar la función en todos los grupos de escritorios administrados por la instancia de vCenter Server. Al deshabilitar la función de vCenter Server, se anula la configuración a nivel de grupos de escritorios.

Las siguientes instrucciones se aplican a la función de recuperación de espacio:

- Solo funciona en discos de SO eficientes de clones vinculados.
- No afecta a los discos persistentes de View Composer.
- Funciona solo con vSphere 5.1 o una versión posterior en máquinas virtuales cuyo hardware virtual tenga la versión 9 o una posterior.
- No funciona en escritorios de clones completos.
- Funciona en máquinas virtuales con controladores SCSI. Los controladores IDE no son compatibles.

La tecnología de snapshots NFS nativas (VAAI) no es compatible con los grupos que incluyen máquinas virtuales con discos eficientes de espacio.

Requisitos previos

- Compruebe que la versión de vCenter Server y los hosts ESXi, incluidos todos los hosts ESXi de un clúster, sea 5.1 y que de la revisión de descarga ESXi 5.1 sea ESXi510-201212001 o una versión posterior.

Procedimiento

- 1 En Horizon Administrator, complete las páginas del asistente Agregar vCenter Server que preceden a la página de Configuración de almacenamiento.
 - a Seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, haga clic en **Agregar**.
 - c Complete las páginas de Información de vCenter Server, Configuración de View Composer y Dominios de View Composer.

- 2 En la página de Configuración de almacenamiento, asegúrese de que esté seleccionado **Habilitar recuperación de espacio**.

La recuperación de espacio está seleccionada de forma predeterminada si está realizando una instalación nueva de Horizon 7 5.2 o una versión posterior. Debe seleccionar **Habilitar recuperación de espacio** si está actualizando a Horizon 7 5.2 o una versión posterior desde Horizon 7 5.1 o una versión anterior.

Pasos siguientes

En la página de Configuración de almacenamiento, configure el Acelerador de almacenamiento de View.

Configure la recuperación de espacio de disco en grupos de escritorios para finalizar la configuración en Horizon 7.

Configurar el acelerador de almacenamiento de View para vCenter Server

En vSphere 5.1 y versiones posteriores, puede configurar los hosts ESXi para almacenar en caché datos del disco de la máquina virtual. Esta función, denominada Acelerador de almacenamiento de View, usa la función de almacenamiento de caché de lectura basada en el contenido (CBRC) en los hosts ESXi. El acelerador de almacenamiento de View mejora el rendimiento de Horizon 7 durante procesos de E/S masivos, que tienen lugar cuando varias máquinas virtuales se inician o realizan exámenes de antivirus a la vez. Esta función también es útil cuando los administradores o los usuarios cargan aplicaciones o datos frecuentemente. En lugar de leer todo el SO o toda la aplicación desde el sistema de almacenamiento una y otra vez, un host puede leer bloques de datos comunes desde la caché.

Al reducir el número de IOPS durante los arranques masivos, el acelerador de almacenamiento de View disminuye la demanda de la matriz de almacenamiento, que le permite usar menos ancho de banda E/S de almacenamiento para que admita la implementación de Horizon 7.

Puede habilitar el almacenamiento en caché de los hosts ESXi seleccionando la opción Acelerador de almacenamiento de View en el asistente de vCenter Server en Horizon Administrator, como se describe en este procedimiento.

Asegúrese de que el acelerador de almacenamiento de View también esté configurado en grupos de escritorios individuales. Para realizar operaciones en un grupo de escritorios, el acelerador de almacenamiento de View debe estar habilitado en vCenter Server y en el grupo de escritorios individual.

De forma predeterminada, el acelerador de almacenamiento de View está habilitado para grupos de escritorios. La función puede estar deshabilitada o habilitada cuando cree o edite un grupo. La mejor actuación es habilitar esta función cuando crea un grupo de escritorios por primera vez. Si habilita la función al editar un grupo existente, debe asegurarse que se crearon una nueva réplica y sus discos resumen antes de que se aprovisionen las clonaciones vinculadas. Puede crear una nueva réplica volviendo a componer el grupo en una snapshot nueva o volviendo a equilibrar el grupo en un nuevo almacén de datos. Los archivos de resumen solo se pueden configurar en las máquinas virtuales en un grupo de escritorios cuando están desconectados.

Puede habilitar el acelerador de almacenamiento de View en grupos de escritorios que contengan clonaciones vinculadas y grupos que contengan máquinas virtuales completas.

No se admite la tecnología de snapshot NFS nativa (VAAI) en grupos que están habilitados para el acelerador de almacenamiento de View.

El acelerador de almacenamiento de View ya está cualificado para trabajar en configuraciones que usen niveles de réplica de Horizon 7, cuyas réplicas estén almacenadas en almacenes de datos independientes de las clonaciones vinculadas. Aunque los beneficios de rendimiento del uso del acelerador de almacenamiento de View con niveles de réplica de Horizon 7 no sea significativo, algunos beneficios relacionados con la capacidad se deben realizar almacenando las réplicas en un almacén de datos independiente. Se probó esta combinación y se admite.

Importante Si tiene pensado usar esta función y está usando varios pods de View que comparten algunos hosts ESXi, debe habilitar la función el acelerador de almacenamiento de View en todos los pods que se encuentren en los hosts ESXi compartidos. Las configuraciones inconsistentes en varios pods puede causar inestabilidad en las máquinas virtuales de los hosts ESXi compartidos.

Requisitos previos

- Compruebe que vCenter Server y los hosts ESXi tengan la versión 5.1 o una versión posterior.
En un clúster ESXi, compruebe que todos los hosts cuenten con la versión 5.1 o posterior.
- Verifique que el usuario de vCenter Server tenga asignado el privilegio **Host > Configuración > Configuración avanzada** en vCenter Server.
Consulte los temas del documento *Instalación de Horizon 7* que describen los privilegios de Horizon 7 y de View Composer necesarios para el usuario de vCenter Server.

Procedimiento

- 1 En Horizon Administrator, complete las páginas del asistente Agregar vCenter Server que preceden a la página de Configuración de almacenamiento.
 - a Seleccione **Configuración de View > Servidores**.
 - b En la pestaña **vCenter Servers**, haga clic en **Agregar**.
 - c Complete las páginas de Información de vCenter Server, Configuración de View Composer y Dominios de View Composer.
- 2 En la página Configuración de almacenamiento, asegúrese de que la casilla de verificación **Habilitar el acelerador de almacenamiento de View** esté seleccionada.
Esta casilla de verificación está seleccionada de forma predeterminada.
- 3 Especifique un tamaño de la caché del host predeterminado.
El tamaño de la memoria caché predeterminado se aplica a todos los hosts ESXi administrados por esta instancia de vCenter Server.
El valor predeterminado es 1.024MB. El tamaño de la caché debe estar entre 100 MB y 2.048 MB.

- 4 Para especificar un tamaño de la caché diferente para un host ESXi individual, seleccione un host ESXi y haga clic en **Editar tamaño de caché**.
 - a En el cuadro de diálogo Tamaño de caché del host seleccione **Omitir el tamaño de caché del host predeterminado**.
 - b Introduzca un valor **Tamaño de caché del host** entre 100 MB y 2.048 MB y haga clic en **Aceptar**.
- 5 En la página Configuración de almacenamiento, haga clic en **Siguiente**.
- 6 Haga clic en **Finalizar** para agregar la configuración de almacenamiento, de vCenter Server y de View Composer a Horizon 7.

Pasos siguientes

Configure las opciones para las conexiones y sesiones cliente. Consulte [Configurar las opciones de las sesiones cliente](#).

Para completar la configuración del acelerador de almacenamiento de View en Horizon 7, configure el acelerador de almacenamiento de View en los grupos de escritorios. Consulte "Configurar el acelerador de almacenamiento de View para los grupos de escritorios" en el documento *Configurar escritorios virtuales en Horizon 7*.

Límites de operaciones simultáneas para vCenter Server y View Composer

Cuando agrega vCenter Server a Horizon 7 o edita su configuración, puede establecer el número máximo de operaciones simultáneas que realizan vCenter Server y View Composer.

Configure estas opciones en el panel Configuración avanzada en la página de información de vCenter Server.

Tabla 2-1. Límites de operaciones simultáneas para vCenter Server y View Composer

Configuración	Descripción
Número máximo de operaciones de aprovisionamiento de vCenter simultáneas	<p>Determina el número máximo de solicitudes simultáneas que el servidor de conexión puede realizar para aprovisionar y eliminar máquinas virtuales completas en esta instancia de vCenter Server.</p> <p>El valor predeterminado es 20.</p> <p>Esta configuración se aplica únicamente a las máquinas virtuales completas.</p>
Máximo número de operaciones de alimentación simultáneas	<p>Determina el número máximo de operaciones de alimentación simultáneas (iniciar, apagar, suspender, etc.) que pueden tener lugar en máquinas virtuales administradas por el servidor de conexión en esta instancia de vCenter Server.</p> <p>El valor predeterminado es 50.</p> <p>Para obtener más instrucciones sobre cómo calcular el valor de esta opción, consulte Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto.</p> <p>Esta configuración se aplica a las máquinas virtuales completas y a las clonaciones vinculadas.</p>

Tabla 2-1. Límites de operaciones simultáneas para vCenter Server y View Composer (Continuación)

Configuración	Descripción
Operaciones de mantenimiento simultáneas máximas de View Composer	<p>Determina el número máximo de operaciones simultáneas de actualización, para volver a componer y a equilibrar View Composer que pueden realizarse en clonaciones vinculadas administradas por esta instancia de View Composer.</p> <p>El valor predeterminado es 12.</p> <p>Es necesario que se cierren las sesiones activas de los escritorios remotos antes de que pueda comenzar una operación de mantenimiento. Si obliga a los usuarios a cerrar sesión cuando la operación de mantenimiento comienza, el número máximo de operaciones simultáneas en los escritorios remotos para las que son necesarias que se cierren las sesiones es la mitad del valor configurado. Por ejemplo, si configura esta opción en 24 y obliga a los usuarios a cerrar sesión, el número máximo de operaciones simultáneas en los escritorios para las que son necesarias que se cierren las sesiones es 12.</p> <p>Esta opción se aplica únicamente a las clonaciones vinculadas.</p>
Operaciones de aprovisionamiento simultáneas máximas de View Composer	<p>Determina el número máximo de operaciones simultáneas de creación y eliminación que pueden realizarse en clonaciones vinculadas administradas por esta instancia de View Composer.</p> <p>El valor predeterminado es 8.</p> <p>Esta opción se aplica únicamente a las clonaciones vinculadas.</p>

Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto

La opción **Máximo número de operaciones de alimentación simultáneas** establece el número máximo de opciones de alimentación simultáneas que se pueden producir en las máquinas virtuales del escritorio remoto en una instancia de vCenter Server. Este límite se establece en 50 de forma predeterminada. Puede cambiar este valor para que admita velocidades de encendido máximas cuando muchos usuarios inician sesión en los escritorios al mismo tiempo.

Como práctica recomendada, puede realizar una fase piloto para determinar el valor correcto de esta opción. Para obtener directrices de planificación, consulte el apartado que contiene las directrices de planificación y los elementos de diseño de arquitectura en el documento *Planificación de la arquitectura de Horizon 7*.

El número requerido de operaciones de alimentación simultáneas se basa en la velocidad máxima a la que se encienden los escritorios y en la cantidad de tiempo que tardan los escritorios en encenderse, iniciarse y estar disponibles para establecer una conexión. En general, el límite de operaciones de alimentación recomendado es el tiempo total que tardan los escritorios en iniciarse multiplicado por la velocidad máxima de encendido.

Por ejemplo, el escritorio medio tarda de dos a tres minutos en iniciarse. Por lo tanto, el límite de operaciones de alimentación simultáneas debe ser 3 veces la velocidad máxima de encendido. Se espera que la opción predeterminada de 50 admita una velocidad máxima de encendido de 16 escritorios por minuto.

El sistema espera un máximo de cinco minutos para que se inicie un escritorio. Si tarda más en iniciarse, es probable que se produzcan otros errores. Para ser conservador, puede configurar un límite de operaciones de alimentación que sea 5 veces la velocidad máxima de encendido. Con un procedimiento conservador, la opción predeterminada de 50 admite una velocidad máxima de encendido de 10 escritorios por minuto.

Los inicios de sesión y, por lo tanto, las operaciones de encendido de los escritorios, suelen suceder de forma distribuida a través de una ventana de tiempo determinada. Puede aproximar la velocidad máxima de encendido asumiendo que ocurra en la mitad de la ventana de tiempo, durante la cual cerca del 40% de las operaciones de encendido se producen en una sexta parte de la ventana de tiempo. Por ejemplo si los usuarios inician sesión entre las 8:00 y las 9:00, la ventana de tiempo es una hora y el 40% de los inicios de sesión se producen en los 10 minutos comprendidos entre las 8:25 y las 8:35. Si hay 2.000 usuarios, y el 20% tiene sus escritorios desconectados, el 40% de las 400 operaciones de encendido de los escritorios se producen en esos 10 minutos. La velocidad máxima de encendido es 16 escritorios por minuto.

Aceptar la huella digital de un certificado TLS predeterminado

Cuando agregue las instancias de vCenter Server y de View Composer a Horizon 7, debe asegurarse de que los certificados TLS que se usan para las instancias de vCenter Server y de View Composer sean válidos y que el servidor de conexión confíe en ellos. Si los certificados predeterminados instalados con vCenter Server y View Composer están aún en las instalaciones, debe determinar si desea aceptar las huellas digitales de los certificados.

Si una instancia de vCenter Server o de View Composer está configurada con un certificado firmado por una CA y el servidor de conexión confía en el certificado raíz, no es necesario que acepte la huella digital del certificado. No es necesaria ninguna acción.

Si reemplaza un certificado predeterminado por uno firmado por una CA, pero el servidor de conexión no confía en el certificado raíz, debe determinar si desea aceptar la huella digital del certificado. Una huella digital es un hash criptográfico de un certificado. La huella digital se usa para determinar rápidamente si un certificado presentado es igual a otro, como, por ejemplo, el certificado que se aceptó previamente.

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

Para obtener más información sobre 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.

Eliminar una instancia de vCenter Server de Horizon 7

Puede eliminar la conexión entre Horizon 7 y una instancia de vCenter Server. Cuando lo haga, Horizon 7 ya no administrará las máquinas virtuales que se crearon en esa instancia de vCenter Server.

Requisitos previos

Elimine todas las máquinas virtuales que están asociadas a la instancia de vCenter Server. Si desea obtener más información sobre cómo eliminar las máquinas virtuales, consulte "Eliminar un grupo de escritorios" en el documento *Configurar escritorios virtuales en Horizon 7*.

Procedimiento

- 1 En Horizon Administrator, haga clic en **Configuración de View > Servidores**.
- 2 En la pestaña **vCenter Servers**, seleccione la instancia vCenter Server.
- 3 Haga clic en **Eliminar**.

Un cuadro de diálogo le advierte que Horizon 7 ya no tendrá acceso a las máquinas virtuales que administra esta instancia de vCenter Server.

- 4 Haga clic en **Aceptar**.

Horizon 7 Ya no puede acceder a las máquinas virtuales que se crean en la instancia de vCenter Server.

Eliminar View Composer de Horizon 7

Puede eliminar la conexión entre Horizon 7 y el servicio VMware Horizon View Composer asociado con una instancia de vCenter Server.

Antes de deshabilitar la conexión a View Composer, debe eliminar de Horizon 7 todas las máquinas virtuales de clones vinculados que View Composer creó. Horizon 7 impide eliminar View Composer si aún existe algún clon vinculado asociado. Después de deshabilitar la conexión a View Composer, Horizon 7 no podrá aprovisionar o administrar clones vinculados nuevos.

Procedimiento

- 1 Elimine los grupos de escritorios de clones vinculados que View Composer creó.
 - a En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.
 - b Seleccione un grupo de escritorios de clones vinculados y haga clic en **Eliminar**.

Un cuadro de diálogo le avisa de que eliminara de forma permanente el grupo de escritorios clones vinculados de Horizon 7. Si las máquinas virtuales de clones vinculados están configuradas con discos persistentes, puede desconectar o eliminar los discos persistentes.

- c Haga clic en **Aceptar**.

Se eliminan las máquinas virtuales de vCenter Server. También se eliminan las entradas asociadas de la base de datos de View Composer y las réplicas que View Composer creó.

- d Repita estos pasos para cada grupo de escritorios de clones vinculados que View Composer creó.

2 Seleccione **Configuración de View > Servidores**.

- 3 En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server asociada a View Composer.

- 4 Haga clic en **Editar**.

- 5 En la Configuración del servidor de View Composer, haga clic en **Editar**, seleccione **No utilizar View Composer** y haga clic en **Aceptar**.

No podrá crear más grupos de escritorios de clones vinculados en dicha instancia de vCenter Server, pero podrá seguir creando y administrando grupos de escritorios de máquinas virtuales completas en la instancia de vCenter Server.

Pasos siguientes

Si planea instalar View Composer en otro host y volver a configurar Horizon 7 para conectarse al nuevo servicio VMware Horizon View Composer, debe realizar ciertos pasos adicionales. Consulte [Migrar View Composer sin máquinas virtuales de clones vinculados](#).

ID únicos de vCenter Server en conflicto

Si tiene varias instancias de vCenter Server configuradas en el entorno, se puede producir un error al intentar agregar una nueva instancia, ya que los ID únicos entran en conflicto.

Problema

Al intentar agregar una instancia de vCenter Server a Horizon 7, el ID único de la nueva instancia entra en conflicto con otra instancia ya existente.

Causa

Dos instancias de vCenter Server no pueden usar el mismo ID único. De forma predeterminada, un ID único de vCenter Server se genera de forma aleatoria, pero puede editarlo.

Solución

- 1 En vSphere Client haga clic en **Administración > Configuración de vCenter Server > Configuración en tiempo de ejecución**.
- 2 Escriba un nuevo ID único y haga clic en **Aceptar**.

Para obtener más información sobre cómo editar los valores del ID único de vCenter Server, consulte la documentación de vSphere.

Realizar una copia de seguridad del servidor de conexión de Horizon

Después de completar la configuración inicial del servidor de conexión de Horizon, debe programar copias de seguridad periódicas de los datos de la configuración de View Composer y de Horizon 7.

Para obtener más información sobre cómo hacer una copia de seguridad de la configuración de Horizon 7 y restaurarla, consulte [Realizar una copia de seguridad y restaurar los datos de configuración de Horizon 7](#).

Configurar las opciones de las sesiones cliente

Puede configurar opciones globales que afecten a las sesiones cliente y a las conexiones administradas por una instancia del servidor de conexión o un grupo replicado. Puede establecer la duración del tiempo de espera de la sesión, visualizar mensajes de advertencia y los anteriores al inicio de sesión, así como establecer las opciones de conexión cliente relacionada con la seguridad.

Configurar opciones de las conexiones y las sesiones cliente

Para determinar cómo funcionan las conexiones y las sesiones cliente, puede establecer la configuración global.

La configuración global no es específica para una instancia del servidor de conexión. Afecta a todas las sesiones cliente que se administran por una instancia independiente del servidor de conexión o un grupo de instancias replicadas.

También puede configurar las instancias del servidor de conexión para que utilicen conexiones directas y sin túnel entre Horizon Client y los escritorios remotos. Consulte [Configurar el túnel seguro y la puerta de enlace segura PCoIP](#) para obtener información sobre cómo configurar las conexiones directas.

Requisitos previos

Familiarícese con la configuración global. Consulte [Configuración global de las sesiones cliente](#) y [Configuración de seguridad global para conexiones y sesiones cliente](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración global**.
- 2 Seleccione si desea establecer la configuración general o la configuración de seguridad.

Opción	Descripción
Configuración global general	En el panel General, haga clic en Editar .
Configuración global de seguridad	En el panel Seguridad, haga clic en Editar .

- 3 Establezca la configuración global.
- 4 Haga clic en **Aceptar**.

Pasos siguientes

Puede cambiar la contraseña de recuperación de datos que proporcionó durante la instalación. Consulte [Cambiar la contraseña de Data Recovery](#).

Cambiar la contraseña de Data Recovery

Proporcione una contraseña de Data Recovery cuando instale la versión 5.1 o una versión posterior del servidor de conexión. Después de la instalación, puede cambiar esta contraseña en View Administrator. La contraseña es necesaria al restaurar la configuración LDAP de View desde una copia de seguridad.

Cuando realiza una copia de seguridad del servidor de conexión, la configuración LDAP de View se exporta como datos LDIF cifrados. Para restaurar la configuración de Horizon 7 desde la copia de seguridad cifrada, debe proporcionar la contraseña de Data Recovery.

La contraseña debe tener entre 1 y 128 caracteres. Siga las prácticas recomendadas de la organización para generar contraseñas seguras.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración global**.
- 2 En el panel Seguridad, haga clic en **Cambiar contraseña de Data Recovery**.
- 3 Escriba y vuelva a escribir la nueva contraseña.
- 4 (opcional) Escriba un recordatorio de contraseña.

Nota También puede cambiar la contraseña de Data Recovery cuando programe la copia de seguridad de los datos de configuración de Horizon 7. Consulte [Programar copias de seguridad de la configuración de Horizon 7](#).

Pasos siguientes

Cuando use la utilidad `vdmimport` para restaurar una copia de seguridad de la configuración de Horizon 7, proporcione la nueva contraseña.

Configuración global de las sesiones cliente

La configuración global general determina la duración del tiempo de espera de una sesión, los límites del tiempo de espera y la habilitación de SSO, las actualizaciones de estado en Horizon Administrator, si aparecen mensajes de advertencia y anteriores al inicio de sesión, y si Horizon Administrator trata a Windows Server como un sistema operativo que admite escritorios remotos, entre otras opciones.

Los cambios de cualquier opción de la siguiente tabla se aplican de forma inmediata. No es necesario que reinicie el servidor de conexión de Horizon 7 ni Horizon Client.

Tabla 2-2. Configuración global general de las sesiones cliente

Configuración	Descripción
Tiempo de espera de la sesión de View Administrator	<p>Determina durante cuánto tiempo sigue inactiva una sesión de Horizon Administrator antes de que la sesión caduque.</p> <hr/> <p>Importante Al establecer el tiempo de espera de la sesión de Horizon Administrator en un número elevado de minutos, aumenta el riesgo de que Horizon Administrator se use de forma no autorizada. Si desea permitir una sesión inactiva durante un tiempo prolongado, hágalo con precaución.</p> <hr/> <p>De forma predeterminada, el tiempo de espera de la sesión de Horizon Administrator es 30 minutos. Puede establecer el tiempo de espera de la sesión de 1 a 4320 minutos (72 horas).</p>
Desconectar usuarios de forma forzada	<p>Desconecta todos los escritorios y todas las aplicaciones después de que transcurra el número de minutos especificado desde que el usuario inició sesión en Horizon 7. Todos los escritorios y todas las aplicaciones se desconectarán al mismo tiempo, sin tener en cuenta cuándo el usuario los inició.</p> <p>Para los clientes que no admitan aplicaciones remotas, se aplica un valor máximo de tiempo de espera de 1200 minutos si el valor de esta opción es Nunca o superior a 1200 minutos.</p> <p>El valor predeterminado es Después de 600 minutos.</p>
Single Sign-On (SSO)	<p>Si SSO está habilitado, Horizon 7 almacena en caché las credenciales de un usuario para que este pueda iniciar aplicaciones o escritorios remotos sin tener que proporcionar credenciales para iniciar la sesión remota de Windows. El valor predeterminado es Habilitado.</p> <p>Si tiene pensado usar la función True SSO, introducida a partir de Horizon 7, se debe habilitar SSO. Con True SSO, si un usuario inicia sesión con otra forma de autenticación diferente a las credenciales de Active Directory, la función True SSO genera certificados de corta duración para usarlos, en lugar de credenciales almacenadas en la caché, después de que los usuarios inicien sesión en VMware Identity Manager.</p> <hr/> <p>Nota Si un escritorio se inicia desde Horizon Client y el escritorio está bloqueado, tanto por el usuario o por Windows según una directiva de seguridad, y si el escritorio está ejecutando Horizon 7 Agent 6.0 o una versión superior, o bien Horizon Agent 7.0 o una versión superior, el servidor de conexión de Horizon 7 descarta las credenciales SSO del usuario. El usuario debe proporcionar las credenciales de inicio de sesión para iniciar un nuevo escritorio o una nueva aplicación, o bien para volver a conectar cualquier aplicación o escritorio desconectados. Para volver a habilitar SSO, el usuario debe desconectarse del servidor de conexión de Horizon 7 o cerrar Horizon Client y volver a conectarse al servidor de conexión de Horizon 7. Sin embargo, si el escritorio se inicia desde Workspace ONE o VMware Identity Manager y el escritorio está bloqueado, las credenciales SSO no se descartan.</p>

Tabla 2-2. Configuración global general de las sesiones cliente (Continuación)

Configuración	Descripción
<p>Para clientes que admiten aplicaciones.</p> <p>Si el usuario deja de usar el teclado y el mouse, desconecte las aplicaciones y descarte las credenciales SSO:</p>	<p>Protege las sesiones de las aplicaciones donde no hay actividad de teclado ni mouse en el dispositivo cliente. Si está establecido como Después de ... minutos, Horizon 7 desconecta todas las aplicaciones y descarta las credenciales SSO después del número de minutos especificado sin actividad del usuario. No se desconectan las sesiones de escritorio. Los usuarios deben iniciar sesión de nuevo para volver a conectar todas las aplicaciones que se desconectaron o iniciar una nueva aplicación o un nuevo escritorio.</p> <p>Esta opción también se aplica a la función True SSO. Después de descartar las credenciales SSO, se solicita a los usuarios que proporcionen las credenciales de Active Directory. Si los usuarios iniciaron sesión en VMware Identity Manager sin usar las credenciales de AD y no saben las que deben introducir, pueden cerrar la sesión y volver a iniciarla para acceder a las aplicaciones y los escritorios remotos.</p> <hr/> <p>Importante Los usuarios deben saber que, cuando tienen las aplicaciones y los escritorios abiertos y se desconectan las aplicaciones debido al tiempo de espera, los escritorios siguen conectados. Los usuarios no deben confiar en este tiempo de espera para proteger los escritorios.</p> <hr/> <p>Si está establecido como Nunca, Horizon 7 no desconecta nunca las aplicaciones ni descarta las credenciales SSO debido a la inactividad de usuario.</p> <p>El valor predeterminado es Nunca.</p>
<p>Otros clientes.</p> <p>Descartar credenciales SSO:</p>	<p>Descarta las credenciales SSO después de un número de minutos especificado. Esta opción está destinada a clientes que no admiten la comunicación remota de aplicaciones. Si está establecida como Después de... minutos, los usuarios deben iniciar sesión de nuevo para conectarse a un escritorio después de que pase el número de minutos determinado desde que el usuario inició sesión en Horizon 7, sin tener en cuenta la actividad del usuario en el dispositivo cliente.</p> <p>Si está configurado como Nunca, Horizon 7 almacena las credenciales SSO hasta que el usuario cierra Horizon Client o se alcanza el tiempo de espera Desconectar usuarios de forma forzada.</p> <p>El valor predeterminado es Después de 15 minutos.</p>
<p>Habilitar actualizaciones automáticas de estado</p>	<p>Determina si las actualizaciones de estado aparecen en el panel del estado global situado en la esquina superior izquierda de Horizon Administrator cada pocos minutos. La página del panel de control de Horizon Administrator también se actualiza cada pocos minutos.</p> <p>De forma predeterminada, esta opción no está habilitada.</p>
<p>Mostrar un mensaje previo al inicio de sesión</p>	<p>Muestra una declaración de responsabilidades u otro mensaje a los usuarios de Horizon Client cuando inician sesión.</p> <p>Escriba la información o las instrucciones en el cuadro de texto del cuadro de diálogo Configuración global.</p> <p>Para no mostrar ningún mensaje, deje la casilla de verificación sin marcar.</p>

Tabla 2-2. Configuración global general de las sesiones cliente (Continuación)

Configuración	Descripción
Mostrar la advertencia antes del cierre de sesión	<p>Muestra un mensaje de advertencia cuando se obliga a los usuarios a cerrar sesión por una actualización programada o inmediata como, por ejemplo, cuando una operación de actualización de escritorio está a punto de comenzar. Esta opción también determina el tiempo de espera desde que se muestra el mensaje hasta que se cierra la sesión del usuario.</p> <p>Seleccione la casilla para mostrar un mensaje de advertencia.</p> <p>Escriba el número de minutos que se debe esperar desde que se muestra el mensaje hasta que se cierra la sesión del usuario. El valor predeterminado es 5 minutos.</p> <p>Escriba el mensaje de advertencia. Puede usar el mensaje predeterminado:</p> <div> <p>Está programada una actualización importante para el escritorio y este se desconectará en 5 minutos. Guarde ahora el trabajo sin guardar.</p> </div>
Habilitar escritorios Windows Server	<p>Determina si puede seleccionar los equipos Windows Server 2008 R2 y Windows Server 2012 R2 que estén disponibles para usarlos como escritorios. Cuando esta opción está habilitada, Horizon Administrator muestra todos los equipos Windows Server disponibles, incluidos los equipos en los que los componentes del servidor de Horizon 7 están instalados.</p> <p>Nota El software Horizon Agent no puede coexistir en la misma máquina virtual o física con cualquier otro componente de software del servidor de Horizon 7, como un servidor de seguridad, el servidor de conexión de Horizon 7 o Horizon 7 Composer.</p>
Limpiar credencial al cerrar la pestaña para HTML Access	<p>Elimina de la caché las credenciales de un usuario cuando este cierre una pestaña que establezca la conexión a una aplicación o escritorio remoto o cuando cierre una pestaña que se conecte a la página de selección de aplicaciones y escritorios, en el cliente HTML Access.</p> <p>Cuando esta opción está habilitada, Horizon 7 también elimina las credenciales de la caché en los siguientes escenarios cliente de HTML Access:</p> <ul style="list-style-type: none"> ■ Un usuario actualiza la página de selección de aplicaciones y escritorios o la página de la sesión remota. ■ El servidor presenta un certificado autofirmado, un usuario inicia una aplicación o un escritorio remotos y el usuario acepta el certificado cuando la advertencia de seguridad aparece. ■ Un usuario ejecuta un comando URI en la pestaña que contiene la sesión remota. <p>Cuando esta opción está deshabilitada, las credenciales se mantienen en la caché. Esta función está deshabilitada de forma predeterminada.</p> <p>Nota Esta función está disponible en Horizon 7 versión 7.0.2 y versiones posteriores.</p>

Tabla 2-2. Configuración global general de las sesiones cliente (Continuación)

Configuración	Descripción
Configuración del servidor Mirage	<p>Le permite especificar la URL de un servidor de Mirage, usando el formato <code>mirage://nombre-servidor:puerto</code> o <code>mirages://nombre-servidor:puerto</code>. En este caso, <i>nombre-servidor</i> es el nombre de dominio completo. Si no especifica el número de puerto, se usa el número 8000 que es el predeterminado.</p> <p>Nota Puede sobrescribir esta opción global especificando un servidor Mirage en las opciones del grupo de escritorios.</p> <p>La especificación del servidor de Mirage en Horizon Administrator es una alternativa a especificar el servidor de Mirage cuando instale el cliente Mirage. Para encontrar qué versión de Mirage admite el servidor especificado en Horizon Administrator, consulte la documentación de Mirage en https://www.vmware.com/support/pubs/mirage_pubs.html.</p>
Ocultar la información del servidor en la interfaz de usuario del cliente	<p>Habilite esta opción de seguridad para ocultar la información de la URL del servidor en Horizon Client 4.4 o una versión posterior.</p>
Ocultar la lista de dominios en la interfaz de usuario del cliente	<p>Habilite esta opción de seguridad para ocultar el menú desplegable Dominio en Horizon Client 4.4 o una versión posterior.</p> <p>Si el usuario inicia sesión en una instancia del servidor de conexión que tenga habilitada la configuración global Ocultar la lista de dominios en la interfaz de usuario del cliente, el menú desplegable Dominio permanece oculto en Horizon Client y el usuario proporciona la información de dominio en el cuadro de texto Nombre de usuario. Por ejemplo, los usuarios deben proporcionar el nombre de usuario utilizando el formato <code>domain\username</code> o <code>username@domain</code>.</p> <p>Importante Si habilita las opciones Ocultar la información del servidor en la interfaz de usuario del cliente y Ocultar la lista de dominios en la interfaz de usuario del cliente y selecciona la autenticación de dos fases (RSA SecureID o RADIUS) para la instancia del servidor de conexión, no exija que coincidan los nombres de usuarios de Windows. Exigir que coincidan los nombres de usuario de Windows evita que siempre falle el inicio de sesión si los usuarios escriben la información del dominio en el cuadro de texto de nombre de usuario. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento <i>Administración de Horizon 7</i>.</p>

Configuración de seguridad global para conexiones y sesiones cliente

La configuración de seguridad global determina si los clientes se vuelven a autenticar después de interrupciones, si el modo de seguridad de mensajes está habilitado y si IPSec se usa para las conexiones del servidor de seguridad.

TLS es necesario para todas las conexiones de Horizon Client y de Horizon Administrator con Horizon 7. Si la implementación de Horizon 7 usa equilibradores de carga u otros servidores intermedios para el cliente, puede descargar TLS en ellos y configurar conexiones TLS en instancias individuales del servidor de conexión y los servidores de seguridad. Consulte [Descargar conexiones TLS a servidores intermediarios](#).

Tabla 2-3. Configuración de seguridad global para conexiones y sesiones cliente

Configuración	Descripción
Volver a autenticar las conexiones de túnel seguro después de la interrupción en la red	<p>Determina si las credenciales del usuario deben volver a autenticarse después de una interrupción de red cuando Horizon Client usa conexiones de túnel de seguridad con los escritorios remotos.</p> <p>Cuando seleccione esta opción, si se interrumpe la conexión del túnel de seguridad, Horizon Client obliga al usuario a volver a autenticarse después de volver a conectarse. Esta opción proporciona más seguridad. Por ejemplo, si alguien roba un equipo y lo conecta a una red diferente, el usuario no puede acceder automáticamente al escritorio remoto sin introducir las credenciales.</p> <p>Si esta opción no está seleccionada, el cliente se vuelve a conectar al escritorio remoto sin solicitar al usuario que se vuelva a autenticar.</p> <p>Esta opción no se aplica cuando no se usa el túnel de seguridad.</p>
Modo de seguridad de mensajes	<p>Determina el mecanismo de seguridad usado para enviar mensajes JMS entre componentes.</p> <ul style="list-style-type: none"> ■ Cuando el modo está configurado como Habilitado, se producen la firma y la verificación de los mensajes JMS que se envían entre componentes de Horizon 7. ■ Cuando el modo está configurado como Mejorado, la seguridad se proporciona gracias a las conexiones JMS de TLS autenticadas de forma mutua al control del acceso a temas JMS. <p>Para obtener más información, consulte Modo de seguridad de mensajes para los componentes de Horizon 7.</p> <p>En las nuevas instalaciones, de forma predeterminada, se configura como Mejorada. Si actualiza una versión anterior, se mantiene la opción utilizada en la versión anterior.</p>
Estado de seguridad mejorada (solo lectura)	<p>Campos de solo lectura que aparecen cuando la opción Modo de seguridad Mensaje se cambia de Habilitado a Mejorado. Como el cambio se hace en fases, este campo muestra el progreso en las diferentes fases:</p> <ul style="list-style-type: none"> ■ La opción Esperar el reinicio del bus de mensajería es la primera fase. Este estado aparece hasta que reinicie de forma manual todas las instancias del servidor de conexión en el pod o en el servicio del componente del bus de mensajería de VMware Horizon en todos los hosts del servidor de conexión del pod. ■ La opción Mejora pendiente es el siguiente estado. Después de que se reinicien todos los servicios del componente de bus de mensajería de Horizon, el sistema comienza a cambiar el modo de seguridad de los mensajes a Mejorado de todos los escritorios y servidores de seguridad. ■ La opción Mejorado es el estado final, que indica que todos los componentes están usando el modo de seguridad de los mensajes Mejorado. <p>También puede usar la utilidad de la línea de comandos <code>vdmutil</code> para supervisar el progreso. Consulte Uso de la utilidad vdmutil para configurar el modo de seguridad de mensajes JMS.</p>
Usar IPsec para las conexiones del servidor de seguridad	<p>Determina si se debe usar el Protocolo de seguridad de Internet (IPSec) para las conexiones entre los servidores de seguridad y las instancias del servidor de conexión.</p> <p>De forma predeterminada, las conexiones seguras (con IPSec) para las conexiones de los servidores de seguridad están habilitadas.</p>

Nota Si actualiza a View 5.1 o una versión posterior desde una versión anterior de Horizon 7, la opción global **SSL obligatoria para las conexiones cliente** aparece en Horizon Administrator, pero únicamente si la opción se deshabilitó en la configuración de Horizon 7 antes de actualizar. Como TLS es obligatorio para todas las conexiones de Horizon Client y de Horizon Administrator a Horizon 7, esta opción no aparece en las instalaciones nuevas de Horizon 7 5.1 o versiones posteriores y no se muestra después de una actualización si la opción ya se habilitó en la configuración anterior de Horizon 7.

Después de una actualización, si no habilita la opción **SSL obligatoria para las conexiones cliente**, se producirá un error en las conexiones HTTPS de Horizon Client, a menos que se conecten a un dispositivo intermedio que esté configurado para establecer las siguientes conexiones con HTTP.

Consulte [Descargar conexiones TLS a servidores intermediarios](#).

Modo de seguridad de mensajes para los componentes de Horizon 7

Puede establecer el modo de seguridad de mensajes para especificar el mecanismo de seguridad usado cuando se envían mensajes JMS entre los componentes de Horizon 7.

La siguiente tabla muestra las opciones que puede seleccionar para configurar el modo de seguridad de mensajes. Para establecer una opción, selecciónela en la lista **Modo de seguridad de mensajes** en la ventana de diálogo Configuración global.

Tabla 2-4. Opciones del modo de seguridad de mensajes

Opción	Descripción
Deshabilitado	El modo de seguridad de mensajes está deshabilitado.
Mixto	<p>El modo de seguridad de mensajes está habilitado pero no se aplica.</p> <p>Puede usar este modo para detectar los componentes del entorno de Horizon 7 que sean anteriores a Horizon 7 3.0. El archivo de registro que genera el servidor de conexión contiene referencias a estos componentes. No se recomienda esta opción. Use esta opción solo para detectar los componentes que se deban actualizar.</p>
Habilitado	<p>El modo de seguridad de mensajes está habilitado, usando una combinación de cifrado y firma de mensajes. Se rechazan los mensajes JMS si no aparece la firma o esta no es válida, o bien si se modificó un mensaje después de firmarlo.</p> <p>Algunos mensajes JMS se cifran porque contienen información personal como, por ejemplo, las credenciales del usuario. Si usa la opción Habilitado, puede utilizar IPSec para cifrar todos los mensajes JMS entre instancias del servidor de conexión y entre las instancias del servidor de conexión y los servidores de seguridad.</p> <p>Nota No se permite que los componentes de Horizon 7 anteriores a la versión 3.0 se comuniquen con otros componentes de Horizon 7.</p>
Mejorado	<p>SSL se usa para todas las conexiones JMS. El control del acceso JMS también se habilita para que las instancias del servidor de conexión, los servidores de seguridad y los escritorios solo puedan enviar y recibir mensajes JMS sobre ciertos temas.</p> <p>Los componentes de Horizon 7 que sean anteriores a la versión 6.1 de Horizon 6 no se pueden comunicar con una instancia del servidor de conexión 6.1.</p> <p>Nota Para usar este modo es necesario abrir el puerto TCP 4002 entre servidores de seguridad basados en DMZ y sus instancias del servidor de conexión emparejadas.</p>

Cuando instala por primera vez Horizon 7 en un sistema, el modo del mensaje de seguridad se configura como **Mejorado**. Si actualiza Horizon 7 desde una versión anterior, la opción ya establecida del modo de seguridad de mensajes no cambia.

Importante Si tiene pensado cambiar un entorno de Horizon 7 actualizado de **Habilitado** a **Mejorado**, primero debe actualizar todas las instancias del servidor de conexión de View, los servidores de seguridad y los escritorios de Horizon 7 de Horizon 6 con la versión 6.1 o una posterior. Después de cambiar la opción a **Mejorado**, la nueva opción se aplica en etapas.

- 1 Debe reiniciar de forma manual el servicio del componente del bus de mensajería de VMware Horizon View en todos los hosts del servidor de conexión en el pod o reiniciar las instancias del servidor de conexión.
- 2 Después de que se reinicien todos los servicios, las instancias del servidor de conexión vuelven a configurar el modo de seguridad de mensajes en todos los escritorios y los servidores de seguridad, cambiando el modo a **Mejorada**.
- 3 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.

De forma alternativa, puede usar la utilidad de la línea de comandos `vdmutil` para supervisar el progreso. Consulte [Uso de la utilidad vdmutil para configurar el modo de seguridad de mensajes JMS](#).

Los componentes de Horizon 7 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.

Si tiene pensado cambiar un entorno activo de Horizon 7 de **Deshabilitado** a **Habilitado** o de **Habilitado** a **Deshabilitado**, cambie al modo **Mixto** durante un corto periodo de tiempo antes de realizar el cambio final. Por ejemplo, si el modo actual es **Deshabilitado**, cámbielo al modo **Mixto** durante un día y, a continuación, a **Habilitado**. En modo **Mixto**, las firmas se adjuntan a los mensajes pero no se verifican, lo que permite que se propague el cambio del modo de mensaje en todo el entorno.

Uso de la utilidad vdmutil para configurar el modo de seguridad de mensajes JMS

Puede usar la interfaz de línea de comandos `vdmutil` para configurar y administrar los mecanismos de seguridad usados cuando los mensajes JMS se envían entre los componentes de Horizon 7.

Sintaxis y ubicación de la utilidad

El comando `vdmutil` puede realizar las mismas operaciones que el comando `lmvutil` que se incluyó con versiones anteriores de Horizon 7. Además, el comando `vdmutil` tiene opciones para determinar el modo de seguridad de mensajes que se está usando y supervisar el progreso para cambiar todos los componentes de Horizon 7 a modo Mejorado. Use el siguiente formato del comando de `vdmutil` en una ventana de símbolo de sistema de Windows.

```
vdmutil opción_comando [argumento opción_adicional] ...
```

Las opciones adicionales que puede usar dependen de la opción del comando. Este tema se centra en las opciones del modo de seguridad de mensajes. Para otras opciones, que están relacionadas con la arquitectura de Cloud Pod, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

De forma predeterminada, la ruta del archivo ejecutable de comandos `vdmutil` es `C:\Program Files\VMware\VMware View\Server\tools\bin`. Si desea evitar introducir la ruta en la línea de comando, agréguela a la variable de entorno `PATH`.

Autenticación

Debe ejecutar el comando como un usuario con la función Administradores. Horizon Administrator permite asignar la función de administradores a un usuario. Consulte [Capítulo 6 Configurar la administración delegada basada en funciones](#).

El comando `vdmutil` incluye opciones para especificar el nombre de usuario, el dominio y la contraseña que se deben usar en la autenticación.

Tabla 2-5. Opciones de autenticación del comando `vdmutil`

Opción	Descripción
<code>--authAs</code>	Nombre de un usuario administrador de Horizon 7. No use <i>dominio\nombredeusuario</i> ni el formato de nombre principal de usuario (UPN).
<code>--authDomain</code>	Nombre de dominio completo del usuario administrador de Horizon 7 especificado en la opción <code>--authAs</code> .
<code>--authPassword</code>	Contraseña del usuario administrador de Horizon 7 especificado en la opción <code>--authAs</code> . Si introduce "*" en lugar de una contraseña, el comando <code>vdmutil</code> solicitará la contraseña y no permitirá contraseñas que distingan entre mayúsculas y minúsculas en el historial de la línea de comandos.

Debe usar las opciones de autenticación con todas las opciones del comando `vdmutil` excepto con `--help` y con `--verbose`.

Opciones específicas del modo de seguridad de mensajes JMS

La siguiente tabla enumera únicamente las opciones de la línea de comandos `vdmutil` que están relacionadas con ver, configurar o supervisar el modo de seguridad de mensajes JMS. Para obtener una lista de los argumentos que se pueden usar con una opción específica, use la opción `--help` de la línea de comandos.

El comando `vdmutil` devuelve 0 cuando una operación se realiza correctamente y un código que no es cero específico de errores cuando una operación no se realiza correctamente. El comando `vdmutil` escribe mensajes de error de los errores estándar. Cuando una operación genera una salida o cuando el registro detallado está habilitado con la opción `--verbose`, el comando `vdmutil` escribe la salida estándar en inglés de Estados Unidos.

Tabla 2-6. Opciones del comando `vdmutil`

Opción	Descripción
<code>--activatePendingConnectionServerCertificates</code>	Activa un certificado de seguridad pendiente para una instancia del servidor de conexión del pod local.
<code>--countPendingMsgSecStatus</code>	Cuenta el número de equipos que no permiten que se realice una transición desde o hacia el modo Mejorado.
<code>--createPendingConnectionServerCertificates</code>	Crea un nuevo certificado de seguridad pendiente para una instancia del servidor de conexión del pod local.
<code>--getMsgSecLevel</code>	Obtiene el estado de seguridad de mensajes mejorado para el pod local. Este estado pertenece al proceso para cambiar el modo de seguridad de mensajes JMS de Habilitado a Mejorado para todos los componentes de un entorno de Horizon 7.
<code>--getMsgSecMode</code>	Obtiene el modo de seguridad de mensajes para el pod local.
<code>--help</code>	Especifica las opciones del comando <code>vdmutil</code> . También puede usar <code>--help</code> en un comando concreto como <code>--setMsgSecMode --help</code> .
<code>--listMsgBusSecStatus</code>	Enumera el estado de seguridad del bus de mensajería para todos los servidores de conexión del pod local.
<code>--listPendingMsgSecStatus</code>	Enumera equipos que no permiten que se realice una transición desde o hacia el modo Mejorado. Se limita a 25 entradas de modo predeterminado.
<code>--setMsgSecMode</code>	Establece el modo de seguridad de mensajes para el pod local.
<code>--verbose</code>	Habilita el registro detallado. Puede agregar esta opción a cualquier otra para obtener la salida detallada del comando. El comando <code>vdmutil</code> escribe la salida estándar.

Configurar el túnel seguro y la puerta de enlace segura PCoIP

Cuando el túnel seguro está habilitado, Horizon Client establece una segunda conexión HTTPS al host del servidor de seguridad o del servidor de conexión de View cuando los usuarios se conectan a un escritorio remoto.

Cuando la puerta de enlace segura PCoIP está habilitada, Horizon Client establece una conexión más segura al host del servidor de seguridad o del servidor de conexión cuando los usuarios se conectan a un escritorio remoto con el protocolo de visualización PCoIP.

Nota Con Horizon 6 versión 6.2 y versiones posteriores, puede usar los dispositivos de Unified Access Gateway en lugar de los servidores de seguridad para permitir un acceso externo seguro a los escritorios y los servidores Horizon 6. Si usa dispositivos Unified Access Gateway, debe deshabilitar las puertas de enlace seguras en las instancias del servidor de conexión y habilitar estas puertas de enlace en los dispositivos de Unified Access Gateway. Si desea obtener más información, consulte *Implementación y configuración de Unified Access Gateway*.

Cuando el túnel seguro o la puerta de enlace segura PCoIP no estén habilitadas, se establece una sesión directamente entre el sistema cliente y la máquina virtual del escritorio remoto, omitiendo el host del servidor de seguridad o del servidor de conexión. Este tipo de conexión se denomina conexión directa.

Importante Una configuración de red típica que proporcione conexiones seguras a clientes externos incluye un servidor de seguridad. Si desea usar Horizon Administrator para habilitar o deshabilitar el túnel seguro y la puerta de enlace segura PCoIP en un servidor de seguridad, debe editar la instancia del servidor de conexión emparejada con el servidor de seguridad.

En una configuración de red en la que los clientes externos se conecten directamente a un host del servidor de conexión, puede habilitar o deshabilitar el túnel seguro y la puerta de enlace segura PCoIP si edita la instancia del servidor de conexión en Horizon Administrator.

Requisitos previos

- Si planea habilitar la puerta de enlace segura PCoIP, compruebe que la instancia del servidor de conexión y el servidor de seguridad emparejado tengan instalados Horizon 7 4.6 o una versión posterior.
- Si empareja un servidor de seguridad a una instancia del servidor de conexión en el que esté ya habilitada la puerta de enlace segura PCoIP, compruebe que el servidor de seguridad tenga instalado Horizon 7 4.6 o una versión posterior.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor de conexión y haga clic en **Editar**.
- 3 Configure el uso del túnel seguro.

Opción	Descripción
Habilitar el túnel seguro	Seleccione Usar la conexión de túnel seguro con la máquina .
Deshabilitar el túnel seguro	Anule la selección Usar la conexión de túnel seguro con la máquina .

El túnel seguro se habilita de forma predeterminada.

4 Configure el uso de la puerta de enlace segura PCoIP.

Opción	Descripción
Habilitar la puerta de enlace segura PCoIP	Seleccione Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina
Deshabilitar la puerta de enlace segura PCoIP	Anule la selección Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina

La puerta de enlace segura PCoIP está deshabilitada de forma predeterminada.

5 Haga clic en **Aceptar** para guardar los cambios.

Configurar la puerta de enlace segura Blast

En Horizon Administrator, puede configurar el uso de la puerta de enlace segura Blast para proporcionar acceso seguro a las aplicaciones y a los escritorios remotos, a través de HTML Access o a través de conexiones cliente que usan el protocolo de visualización VMware Blast.

La puerta de enlace segura de Blast incluye redes Blast Extreme Adaptive Transport (BEAT), que se ajustan dinámicamente a las condiciones de la red, como los cambios de velocidad y la pérdida de paquetes.

- La puerta de enlace segura Blast admite las redes BEAT solo cuando se ejecutan en un dispositivo de Unified Access Gateway.
- Los Horizon Clients que usen IPv4 y los Horizon Clients que usen IPv6 se pueden gestionar a la vez en el puerto TCP 8443 y en el puerto UDP 8443 (para BEAT) cuando se conecte al dispositivo Unified Access Gateway versión 3.3 o posterior.
- Los Horizon Clients que usen una condición típica de la red deben conectarse a un servidor de conexión (BSG deshabilitada), a un servidor de seguridad (BSG deshabilitada) o a versiones posteriores a la 2.8 de un dispositivo Unified Access Gateway. Si Horizon Client usa una condición típica de la red para conectarse a un servidor de conexión (BSG habilitada), a un servidor de seguridad (BSG habilitada) o a versiones anteriores a la 2.8 de un dispositivo Unified Access Gateway, el cliente detecta automáticamente la condición de la red y vuelve a la red TCP.
- Los Horizon Clients que usen una condición mala de la red deben conectarse a la versión 2.9 o a una versión posterior de un dispositivo Unified Access Gateway (con Servidor del túnel UDP habilitado). Si Horizon Client usa una condición mala de la red para conectarse al servidor de conexión (BSG habilitada), al servidor de seguridad (BSG habilitada) o a versiones anteriores a la 2.8 de un dispositivo Unified Access Gateway, el cliente detecta automáticamente la condición de la red y vuelve a la red TCP.
- Los Horizon Clients que usen una mala condición de la red para conectarse al servidor de conexión (BSG habilitada), al servidor de seguridad (BSG habilitada), a versiones posteriores a la 2.9 de un dispositivo Unified Access Gateway (sin Servidor del túnel UDP habilitado) o a la versión 2.8 del dispositivo Unified Access Gateway, el cliente detecta automáticamente la condición de la red y vuelve a la condición típica.

Para obtener más información, consulte la documentación de Horizon Client disponible en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Nota También puede usar los dispositivos de Unified Access Gateway, en lugar de los servidores de seguridad, para el acceso externo seguro a los servidores y los escritorios de Horizon 7. Si usa dispositivos Unified Access Gateway, debe deshabilitar las puertas de enlace seguras en las instancias del servidor de conexión y habilitar estas puertas de enlace en los dispositivos de Unified Access Gateway. Si desea obtener más información, consulte *Implementación y configuración de Unified Access Gateway*.

Cuando la puerta de enlace segura Blast no está habilitada, los dispositivos cliente y los navegadores web cliente usan el protocolo VMware Blast Extreme para establecer conexiones directas a aplicaciones y máquinas virtuales de escritorio remoto, omitiendo la puerta de enlace segura Blast.

Importante Una configuración de red típica que proporcione conexiones seguras a usuarios externos incluye un servidor de seguridad. Para habilitar o deshabilitar la puerta de enlace segura Blast en un servidor de seguridad, debe editar la instancia del servidor de conexión emparejada con el servidor de seguridad. Si los usuarios externos se conectan directamente a un host del servidor de conexión, habilite o deshabilite la puerta de enlace segura Blast al editar esa instancia del servidor de conexión.

Requisitos previos

Si los usuarios seleccionan los escritorios remotos usando VMware Identity Manager, verifique que VMware Identity Manager esté instalado y configurado para usar con un servidor de conexión y que ese servidor de conexión esté emparejado con un servidor de autenticación SAML 2.0.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor de conexión y haga clic en **Editar**.
- 3 Configure el uso de la puerta de enlace segura Blast.

Opción	Descripción
Habilitar la puerta de enlace segura Blast	Seleccione Usar la puerta de enlace segura Blast en las conexiones Blast de la máquina
Habilitar la puerta de enlace segura de Blast para HTML Access	Seleccione Usar la puerta de enlace segura Blast solo en las conexiones HTML Access de la máquina
Deshabilitar la puerta de enlace segura de Blast	Seleccione No usar la puerta de enlace segura de Blast

La puerta de enlace segura Blast está habilitada de forma predeterminada.

- 4 Haga clic en **Aceptar** para guardar los cambios.

Descargar conexiones TLS a servidores intermediarios

Horizon Client debe utilizar HTTPS para conectarse a Horizon 7. Si los Horizon Clients se conectan a equilibradores de carga u otros servidores intermedios que transmitan las conexiones a instancias del servidor de conexión o servidores de seguridad, podrá descargar TLS a 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.

Para obtener más información sobre la importación de certificados a los servidores de Horizon 7, consulte el apartado "Importar un certificado del servidor SSL a un almacén de certificados de Windows" que aparece en el documento *Instalación de Horizon 7*.

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.

Para obtener información sobre la configuración de URL externas, consulte "Configurar URL externas para conexiones seguras de túnel y puerta de enlace PCoIP" en el documento *Instalación de Horizon 7*.

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
```

Configurar la ubicación de la puerta de enlace para un servidor de conexión de Horizon o el host del servidor de seguridad

De forma predeterminada, las instancias del servidor de conexión de Horizon establecen la ubicación de la puerta de enlace en `Internal` mientras que los servidores de seguridad lo hacen en `External`. Configure la propiedad `gatewayLocation` en el archivo `locked.properties` para cambiar la ubicación predeterminada de la puerta de enlace.

La ubicación de la puerta de enlace determina el valor de la clave de registro `ViewClient_Broker_GatewayLocation` en un escritorio remoto. Puede utilizar este valor con las directivas inteligentes para crear una que se aplique solo cuando un usuario se conecte a un escritorio remoto desde dentro o fuera de la red corporativa. Para obtener más información, consulte "Usar directivas inteligentes" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

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 de Horizon.

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

Las propiedades del archivo `locked.properties` distinguen entre mayúsculas y minúsculas.

- 2 Agregue la siguiente línea en el archivo `locked.properties`:

```
gatewayLocation=value
```

value puede ser tanto `External` como `Internal`. `External` indica que la puerta de enlace está disponible para usuarios fuera de la red corporativa. `Internal` indica que la puerta de enlace solo está disponible para usuarios dentro de la red corporativa.

Por ejemplo, `gatewayLocation=External`

- 3 Guarde el archivo `locked.properties`.
- 4 Reinicie el servicio del servidor de conexión VMware Horizon o el servicio del servidor de seguridad VMware Horizon para que se realicen los cambios.

Habilitar o deshabilitar un servidor de conexión de Horizon

Puede deshabilitar una instancia del servidor de conexión para evitar que los usuarios inicien sesión en las aplicaciones o los escritorios virtuales o publicados. Después de deshabilitar una instancia, puede volverlo a habilitar.

Deshabilitar una instancia del servidor de conexión no afecta a los usuarios que tienen la sesión iniciada en ese momento en las aplicaciones y los escritorios.

La implementación de Horizon 7 determina de qué manera la deshabilitación de una instancia afecta a los usuarios.

- Si se trata de una instancia del servidor de conexión independiente y única, los usuarios no pueden iniciar sesión en las aplicaciones ni en los escritorios. No se pueden conectar al servidor de conexión.
- Si esta es una instancia replicada del servidor de conexión, la topología de red determina si se pueden enrutar los usuarios a otra instancia replicada. Si los usuarios pueden acceder a otra instancia, pueden iniciar sesión en las aplicaciones y los escritorios.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión.
- 3 Haga clic en **Deshabilitar**.

Para volver a habilitar la instancia, haga clic en **Habilitar**.

Editar las URL externas

Puede usar Horizon Administrator para editar las URL externas de las instancias del servidor de conexión y los servidores de seguridad.

De forma predeterminada, únicamente los clientes de túnel que residen dentro de la misma red de un host de servidor de seguridad o de servidor de conexión pueden contactar con dicho host. Los clientes en túnel que se ejecuten fuera de la red deben usar una URL que el cliente pueda resolver para conectarse a un host del servidor de conexión o a un host del servidor de seguridad.

Cuando los usuarios se conectan a escritorios remotos con el protocolo de visualización PCoIP, Horizon Client puede establecer otra conexión a la puerta de enlace segura PCoIP en el host del servidor de seguridad o el servidor de conexión. Para usar la puerta de enlace segura PCoIP, un sistema cliente debe tener acceso a una dirección IP que le permita alcanzar el host del servidor de seguridad o del servidor de conexión. Especifique esta dirección IP en la URL externa PCoIP.

Una tercera URL permite a los usuarios establecer conexiones seguras a través de la puerta de enlace segura Blast.

La URL externa del túnel de seguridad, la URL externa PCoIP y la URL externa Blast deben ser direcciones que los sistemas cliente usen para alcanzar el host.

Nota No puede editar las URL externas para un servidor de seguridad que no se actualizó al servidor de conexión 4.5 o una versión posterior.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.

Opción	Acción
Instancia del servidor de conexión de View	Seleccione la instancia del servidor de conexión en la pestaña Servidores de conexión y haga clic en Editar .
Servidor de seguridad	Seleccione el servidor de seguridad en la pestaña Servidores de seguridad y haga clic en Editar .

- 2 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://view.example.com:443`

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

- 3 Escriba la URL externa de la puerta de enlace segura PCoIP en el cuadro de texto **URL externa de PCoIP**.

Especifique la URL externa de PCoIP como una dirección IP y el número de puerto 4172. No incluya el nombre del protocolo.

Por ejemplo: `10.20.30.40:4172`

La URL debe contener la dirección IP y el número de puerto que un sistema cliente puede usar para alcanzar la instancia del servidor de seguridad o del servidor de conexión.

- 4 Escriba la URL externa de la puerta de enlace segura Blast en el cuadro de texto **URL externa de Blast**.

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

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

De forma predeterminada, la URL incluye el FQDN de la URL externa del túnel seguro y el número del puerto predeterminado, 8443. La URL debe contener el FQDN y el número de puerto que un sistema cliente puede usar para alcanzar este host.

- 5 Verifique que todas las direcciones en este cuadro de diálogo permitan que los sistemas cliente alcancen este host.
- 6 Haga clic en **Aceptar** para guardar los cambios.

Las URL externas se actualizan de forma inmediata. No es necesario que reinicie el servicio del servidor de conexión ni el servicio del servidor de seguridad para que se apliquen los cambios.

Unirse al programa de experiencia del cliente o abandonarlo

Cuando instala el servidor de conexión con una nueva configuración, puede seleccionar participar en un programa de mejora de la experiencia de cliente. Si cambia de opinión después de la instalación, puede unirse al programa o abandonarlo usando Horizon Administrator.

Si participa en el programa, VMware recopila datos anónimos sobre la implementación para mejorar la respuesta de VMware a los requisitos de los usuarios. No se recopila ningún dato que identifique a su organización.

Para ver la lista de campos de los que se obtienen los datos, incluidos los campos anónimos, consulte [GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54#GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Licencia y uso del producto**.
- 2 En el panel Programa de experiencia del cliente, haga clic en **Editar configuración**.
- 3 Decida si participar o no en el programa seleccionando o desmarcando la casilla de verificación **Enviar datos anónimos a VMware**.
- 4 (opcional) Si participa, puede seleccionar la ubicación geográfica, el tipo de empresa y el número de empleados de la organización.
- 5 Haga clic en **Aceptar**.

Directorio LDAP de View

LDAP de View es el repositorio de datos que contiene toda la información de la configuración de Horizon 7. LDAP de View es un directorio del protocolo ligero de acceso a directorios (LDAP) incrustado que se proporciona con la instalación del servidor de conexión.

LDAP de View contiene componentes del directorio de LDAP estándar que usan Horizon 7.

- Definiciones del esquema de Horizon 7
- Definiciones del árbol de información del directorio (DIT)
- Listas de control de acceso (ACL)

LDAP de View contiene las entradas del directorio que representan a los objetos de Horizon 7.

- Las entradas de los escritorios remotos que representan cada escritorio accesible. Cada entrada contiene referencias a las entradas de las Entidades de seguridad externa (FSP) de los usuarios de Windows y de los grupos en Active Directory que no tienen actualización para usar el escritorio.
- Las entradas de los grupos de escritorios remotos que representan varios escritorios que se administran juntos
- Las entradas de las máquinas virtuales que representan la máquina virtual de vCenter Server para cada escritorio remoto
- Entradas de los componentes de Horizon 7 que almacenan las opciones de configuración

LDAP de View también contiene un grupo de DLL de complementos de Horizon 7 que proporciona servicios de notificación y de automatización para otros componente de Horizon 7.

Nota Las instancias del servidor de seguridad no contienen un directorio LDAP de View.

Replicación de LDAP

Al instalar una instancia replicada del servidor de conexión, Horizon 7 copia los datos de configuración LDAP de View de la instancia existente del servidor de conexión. Los datos de configuración de LDAP de View que son idénticos se mantienen en todas las instancias del servidor de conexión del grupo replicado. Cuando se realiza un cambio en una instancia, la información actualizada se copia al resto de instancias.

Si se produce un error en una instancia replicada, el resto de instancias del grupo siguen funcionando. Cuando la instancia con el error reanuda su función, la configuración se actualiza con los cambios que se realizaron durante la interrupción. Con Horizon 7 y versiones posteriores, se realiza una comprobación del estado de la réplica cada 15 minutos para determinar si cada instancia se puede comunicar con otros servidores en el grupo replicado y si cada instancia puede recuperar las actualizaciones de LDAP de otros servidores del grupo.

Puede usar el panel de control de Horizon Administrator para comprobar el estado de replicación. Si alguna instancia del servidor de conexión tiene un icono rojo en el panel de control, haga clic en el icono para ver 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 VDMDS DSA pueden bloquear las replications
- Se produjo un problema en la red

De forma predeterminada, la comprobación de la replicación tiene lugar cada 15 minutos. Puede usar el Editor ADSI en una instancia del servidor de conexión para cambiar el intervalo. Para establecer el número de minutos, conéctese a **DC=vdi,DC=vmware,DC=int** y edite el atributo **pae-ReplicationStatusDataExpiryInMins** en el objeto **CN=Common,OU=Global,OU=Properties**.

El valor del atributo **pae-ReplicationStatusDataExpiryInMins** debe estar entre 10 minutos y 1440 minutos (un día). Si el valor del atributo es menor a 10 minutos, Horizon 7 lo trata como 10 minutos. Si el valor del atributo es superior a 1440 minutos, Horizon 7 lo trata como 1440 minutos.

Configurar la autenticación de tarjeta inteligente

3

Para una mayor seguridad, puede configurar una instancia del servidor de conexión o un servidor de seguridad para que los usuarios y los administradores se puedan autenticar a través de las tarjetas inteligentes.

Una tarjeta inteligente es una tarjeta de plástico pequeña que contiene un chip de equipo. El chip, que es como un equipo en miniatura, incluye almacenamiento seguro para los datos, entre los que encontramos los certificados de las claves públicas y las claves privadas. Un tipo de tarjeta inteligente que usa el Departamento de Defensa de los Estados Unidos se denomina Tarjeta de acceso común (CAC).

Con la autenticación de tarjeta inteligente, un usuario o administrador introduce una tarjeta inteligente en un lector conectado al equipo cliente e introduce un PIN. La autenticación de tarjeta inteligente proporciona autenticación de dos factores al verificar tanto lo que la persona tiene (la tarjeta inteligente) como lo que sabe (el PIN).

Consulte el documento *Instalación de Horizon 7* para obtener información sobre los requisitos de hardware y software para implementar la autenticación por tarjeta inteligente. El sitio web de Microsoft TechNet incluye información detallada sobre cómo planificar e implementar la autenticación con tarjetas inteligentes en sistemas Windows.

Para usar las tarjetas inteligentes, los equipos cliente deben tener un software intermedio y un lector de tarjetas inteligentes. Para instalar certificados en tarjetas inteligentes, debe configurar el equipo para que actúe como una estación de inscripción. Para obtener información sobre si un tipo concreto de Horizon Client admite tarjetas inteligentes, consulte la documentación de Horizon Client en <https://docs.vmware.com/es/VMware-Horizon-Client/index.html>.

Este capítulo incluye los siguientes temas:

- [Iniciar sesión con una tarjeta inteligente](#)
- [Configurar la autenticación con tarjeta inteligente en el servidor de conexión de Horizon](#)
- [Configurar la autenticación con tarjeta inteligente en soluciones de terceros](#)
- [Preparar Active Directory para la autenticación con tarjeta inteligente](#)
- [Verificar la configuración de la autenticación con tarjeta inteligente](#)
- [Uso de la comprobación de revocación de certificados de tarjeta inteligente](#)

Iniciar sesión con una tarjeta inteligente

Cuando un usuario o administrador inserta una tarjeta inteligente en un lector de tarjetas inteligentes, los certificados del usuario en la tarjeta inteligente se copian al almacén de certificados local en el sistema cliente si el sistema operativo es Windows. Los certificados en el almacén local están disponibles para todas las aplicaciones que se ejecuten en el equipo cliente, incluido Horizon Client.

Cuando un usuario o administrador se conecta a una instancia del servidor de conexión o al servidor de seguridad que esté configurado para la autenticación con tarjeta inteligente, dicha instancia o servidor envía una lista de entidades de certificación de confianza (AC) al sistema cliente. El sistema cliente compara la lista de las autoridades de certificación con los certificados de usuario disponibles, selecciona un certificado adecuado y pide al usuario o al administrador que introduzca el PIN de la tarjeta inteligente. Si hay varios certificados de usuario válidos, el sistema del cliente pide al usuario o al administrador que seleccione uno.

El sistema cliente envía el certificado de usuario a la instancia del servidor de conexión o al servidor de seguridad, que comprueba la confianza del certificado y su periodo de validez. Normalmente, los usuarios y administradores pueden autenticarse correctamente si el certificado de usuario es válido y está firmado. Si se configura la comprobación de revocación de certificados, los usuarios o administradores que hayan revocado certificados de usuarios no podrán autenticarse.

En ciertos entornos, un certificado de la tarjeta inteligente de un usuario se puede asignar a varias cuentas de usuario del dominio de Active Directory. Un usuario puede tener varias cuentas con privilegios de administrador, por lo que debe especificar qué cuenta desea usar en el campo Sugerencia de nombre de usuario durante el inicio de sesión de la tarjeta inteligente. Para que el campo Sugerencia de nombre de usuario aparezca en el cuadro de diálogo de inicio de sesión de Horizon Client, el administrador debe habilitar la función de sugerencias del nombre de usuario de la tarjeta inteligente en la instancia del servidor de conexión en Horizon Administrator. El usuario de tarjeta inteligente puede introducir un nombre de usuario o el nombre principal del usuario (user principal name, UPN) en el campo Sugerencia de nombre de usuario durante el inicio de sesión de la tarjeta inteligente.

Si el entorno usa un dispositivo Unified Access Gateway para conseguir un acceso externo seguro, debe configurar el dispositivo Unified Access Gateway para que admita la función de sugerencias de nombre de usuario de la tarjeta inteligente. Dicha función se admite únicamente en Unified Access Gateway 2.7.2 y versiones posteriores. Para obtener más información sobre cómo habilitar la función de sugerencias de nombre de usuario de la tarjeta inteligente en Access Point, consulte el documento *Implementación y configuración de Unified Access Gateway*.

La conmutación de protocolo de visualización no es compatible con la autenticación de tarjeta inteligente en Horizon Client. Para cambiar protocolos de visualización tras la autenticación de una tarjeta inteligente en Horizon Client, un usuario debe cerrar sesión e iniciarla de nuevo.

Configurar la autenticación con tarjeta inteligente en el servidor de conexión de Horizon

Para configurar la autenticación con tarjeta inteligente, debe obtener un certificado raíz y agregarlo a un archivo del almacén de confianza del servidor, modificar las propiedades de configuración del servidor de conexión y configurar las opciones de la autenticación con tarjeta inteligente. En función del tipo de entorno, es posible que necesite realizar pasos adicionales.

Procedimiento

1 Obtener los certificados de la autoridad de certificación

Se deben obtener todos los certificados de la autoridad de certificación (CA) correspondiente para todos los certificados de usuario de confianza en las tarjetas inteligentes presentadas por usuarios y administradores. Estos certificados incluyen certificados raíz y pueden incluir certificados intermedios si el certificado de la tarjeta inteligente del usuario fue emitida por una autoridad de certificación intermedia.

2 Obtener el certificado de CA de Windows

Si dispone de un certificado de usuario firmado por una autoridad de certificación o una tarjeta inteligente que contenga uno, y Windows confía en el certificado raíz, podrá exportar este desde Windows. Si el emisor del certificado del usuario es una autoridad de certificación intermedia, se puede exportar el certificado.

3 Agregar el certificado de CA a un archivo del almacén de confianza del servidor

Debe agregar los certificados raíces, los certificados intermedios o ambos a un archivo del almacén de confianza para todos los usuarios y los administradores en los que confíe. Las instancias del servidor de conexión y los servidores de seguridad usan esta información para autenticar a los administradores y los usuarios con tarjeta inteligente.

4 Modificar las propiedades de configuración del servidor de conexión de Horizon

Para habilitar la autenticación con tarjeta inteligente, debe modificar las propiedades de configuración de su host del servidor de seguridad o servidor de conexión.

5 Configurar las opciones de la tarjeta inteligente en Horizon Administrator

Puede usar Horizon Administrator si desea especificar opciones para tener en cuenta diferentes escenarios de autenticación con tarjeta inteligente.

Obtener los certificados de la autoridad de certificación

Se deben obtener todos los certificados de la autoridad de certificación (CA) correspondiente para todos los certificados de usuario de confianza en las tarjetas inteligentes presentadas por usuarios y administradores. Estos certificados incluyen certificados raíz y pueden incluir certificados intermedios si el certificado de la tarjeta inteligente del usuario fue emitida por una autoridad de certificación intermedia.

Si no dispone del certificado raíz o intermedio de la CA que firmó los certificados en las tarjetas inteligentes presentadas por los usuarios y administradores, puede exportar los certificados de un certificado de usuario firmado por la CA o de una tarjeta inteligente que contenga uno. Consulte [Obtener el certificado de CA de Windows](#).

Procedimiento

- ◆ Obtenga los certificados de la CA de uno de los siguientes orígenes.
 - Un servidor Microsoft IIS que ejecute Microsoft Certificate Services. Para obtener información sobre cómo instalar Microsoft IIS, emitir certificados y distribuirlos en su organización, consulte el sitio web de Microsoft TechNet.
 - El certificado raíz público de una CA de confianza. Este es el origen más habitual de los certificados raíz en entornos que ya disponen de una estructura de tarjeta inteligente y de un enfoque estándar para la distribución de tarjetas inteligentes y la autenticación.

Pasos siguientes

Agregue el certificado raíz, el certificado intermedio o ambos a un archivo del almacén de confianza del servidor.

Obtener el certificado de CA de Windows

Si dispone de un certificado de usuario firmado por una autoridad de certificación o una tarjeta inteligente que contenga uno, y Windows confía en el certificado raíz, podrá exportar este desde Windows. Si el emisor del certificado del usuario es una autoridad de certificación intermedia, se puede exportar el certificado.

Procedimiento

- 1 Si el certificado del usuario está en una tarjeta inteligente, insértela en el lector y agregue el certificado del usuario a su almacén personal.

Si el certificado del usuario no aparece en su almacén personal, utilice el software del lector para exportarlo a un archivo. Este archivo se utiliza en el Paso 4 de este procedimiento.

- 2 En Internet Explorer, seleccione **Herramientas > Opciones de Internet**.

- 3 En la pestaña **Contenido**, haga clic en **Certificados**.

- 4 En la pestaña **Personal**, seleccione el certificado que desee utilizar y haga clic en **Ver**.

Si el certificado del usuario no aparece en la lista, haga clic en **Importar** para importarlo manualmente desde un archivo. Después de importar el certificado, podrá seleccionarlo de la lista.

- 5 En la pestaña **Ruta de certificación**, seleccione el certificado que está más arriba en el árbol y haga clic en **Ver certificado**.

Si el certificado del usuario está firmado como parte de una jerarquía de confianza, el certificado de firma puede estar firmado por otro certificado de mayor nivel. Seleccione el certificado padre (el que realmente firmó el certificado del usuario) como su certificado raíz. En algunos casos, el emisor puede ser una autoridad de certificación intermedia.

- 6 En la pestaña **Detalles**, haga clic en **Copiar en archivo**.

Aparecerá el **Asistente para la exportación de certificados**.

- 7 Haga clic en **Siguiente > Siguiente** y escriba un nombre y una ubicación para el archivo que desea exportar.
- 8 Haga clic en **Siguiente** para guardar el archivo como certificado raíz en la ubicación especificada.

Pasos siguientes

Agregue el certificado de la autoridad de certificación a un archivo del almacén de confianza del servidor.

Agregar el certificado de CA a un archivo del almacén de confianza del servidor

Debe agregar los certificados raíces, los certificados intermedios o ambos a un archivo del almacén de confianza para todos los usuarios y los administradores en los que confíe. Las instancias del servidor de conexión y los servidores de seguridad usan esta información para autenticar a los administradores y los usuarios con tarjeta inteligente.

Requisitos previos

- Obtenga los certificados intermedio o raíz que se usaron para firmar los certificados en las tarjetas inteligentes que presentaron los usuarios o los administradores. Consulte [Obtener los certificados de la autoridad de certificación](#) y [Obtener el certificado de CA de Windows](#).

Importante Estos certificados pueden incluir certificados intermedios si una entidad de certificación intermedia emitió el certificado de la tarjeta inteligente del usuario.

- Verifique que la utilidad `keytool` se agregó a la ruta de acceso del sistema en el servidor de conexión o en el host del servidor de seguridad. Consulte el documento *Instalación de Horizon 7* para obtener más información.

Procedimiento

- 1 En el host del servidor de seguridad o del servidor de conexión, use la utilidad `keytool` para importar el certificado raíz, el certificado intermedio o ambos en el archivo del almacén de confianza del servidor.

Por ejemplo:

```
keytool -import -alias alias -file root_certificate -keystore truststorefile.key
```

En este comando, *alias* es un nombre único que distingue entre mayúsculas y minúsculas para una nueva entrada en el archivo del almacén de confianza del servidor; *root_certificate* es el certificado raíz o intermedio que obtuvo o exportó y *truststorefile.key* es el nombre del archivo del almacén de confianza al que agrega el certificado raíz. Si el archivo no existe, se crea en el directorio actual.

Nota La utilidad `keytool` puede solicitar que cree una contraseña para el archivo del almacén de confianza. Se le solicitará que proporcione esta contraseña en caso de que necesite agregar certificados adicionales al archivo del almacén de confianza en otro momento.

- 2 Copie el archivo del almacén de confianza en la carpeta de configuración de la puerta de enlace SSL en el host del servidor de seguridad o servidor de conexión.

Por ejemplo: `install_directory\VMware\VMware
View\Server\sslgateway\conf\truststorefile.key`

Pasos siguientes

Modifique las propiedades de configuración del servidor de conexión para habilitar la autenticación por tarjeta inteligente.

Modificar las propiedades de configuración del servidor de conexión de Horizon

Para habilitar la autenticación con tarjeta inteligente, debe modificar las propiedades de configuración de su host del servidor de seguridad o servidor de conexión.

Requisitos previos

Agregue los certificados de entidad de certificación (CA) de todos los usuarios de confianza a un archivo del almacén de confianza del servidor. Estos certificados incluyen certificados raíz y pueden incluir certificados intermedios si el certificado de la tarjeta inteligente del usuario fue emitida por una entidad de certificación intermedia.

Procedimiento

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

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

- 2 Agregue las propiedades `trustKeyfile`, `trustStoretype` y `useCertAuth` al archivo `locked.properties`.
 - a Asigne a `trustKeyfile` el nombre de su archivo del almacén de confianza.
 - b Defina `trustStoretype` como `jks`.
 - c Asigne a `useCertAuth` el valor **true** para habilitar la autenticación de certificados.
- 3 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Ejemplo: Archivo `locked.properties`

El archivo mostrado especifica que el certificado de todos los usuarios de confianza se encuentra en el archivo `lonqa.key`, establece el tipo del almacén de confianza como `jks` y habilita la autenticación de certificados.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

Pasos siguientes

Si configuró la autenticación con tarjeta inteligente de una instancia del servidor de conexión, configure sus opciones en Horizon Administrator. No necesita configurar las opciones de la autenticación con tarjeta inteligente de los servidores de seguridad. Las opciones que se configuran en una instancia del servidor de conexión de Horizon también se aplican a un servidor de seguridad emparejado.

Configurar las opciones de la tarjeta inteligente en Horizon Administrator

Puede usar Horizon Administrator si desea especificar opciones para tener en cuenta diferentes escenarios de autenticación con tarjeta inteligente.

Cuando configure estas opciones en una instancia del servidor de conexión, las opciones también se aplican a los servidores de seguridad emparejados.

Requisitos previos

- Modifique las propiedades de configuración del servidor de conexión en el host del servidor de conexión.
- Compruebe que Horizon Client establezca las conexiones HTTPS directamente al servidor de conexión o al host del servidor de seguridad. La autenticación con tarjeta inteligente no se admite si descarga TLS en un dispositivo intermedio.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión y haga clic en **Editar**.

- 3 Si desea configurar la autenticación con tarjeta inteligente para los usuarios de aplicaciones y escritorios remotos, realice estos pasos.

- a En la pestaña **Autenticación**, seleccione una opción de configuración del menú desplegable **Autenticación de tarjeta inteligente para los usuarios** en la sección Autenticación de View.

Opción	Acción
No se permite	La autenticación con tarjeta inteligente está deshabilitada en la instancia del servidor de conexión.
Opcional	Los usuarios pueden usar la autenticación con tarjeta inteligente o la autenticación con contraseña para conectarse a la instancia del servidor de conexión. Si se produce un error en la autenticación con tarjeta inteligente, el usuario debe proporcionar una contraseña.
Obligatoria	<p>Se le solicita a los usuarios usar la autenticación con tarjeta inteligente cuando se conectan a la instancia del servidor de conexión.</p> <p>Si se solicita una autenticación con tarjeta inteligente, se produce un error en la autenticación de los usuarios que seleccionaron la casilla de verificación Iniciar sesión como usuario actual cuando se conectan a la instancia del servidor de conexión. Estos usuarios se deben volver a autenticar con la tarjeta inteligente y el PIN cuando inicien sesión en el servidor de conexión.</p>

Opción	Acción
	Nota La autenticación con tarjeta inteligente solo reemplaza a la autenticación por contraseña de Windows. Si SecurID está deshabilitado, es necesario que los usuarios se autenticuen usando la autenticación SecurID y la autenticación con tarjeta inteligente.

- b Configure la directiva de extracción de la tarjeta inteligente.

No puede configurar la directiva de extracción de tarjeta inteligente si una autenticación por tarjeta inteligente está configurada como **No se permite**.

Opción	Acción
Desconectar a los usuarios del servidor de conexión de View cuando extraigan las tarjetas inteligentes.	Seleccione la casilla de verificación Desconectar las sesiones del usuario al extraer la tarjeta inteligente .
Mantener los usuarios conectados al servidor de conexión de View cuando extraigan las tarjetas inteligentes y permitirles iniciar nuevas sesiones de escritorios o aplicaciones sin una reautenticación.	Desmarque la casilla de verificación Desconectar las sesiones del usuario al extraer la tarjeta inteligente .

La directiva de extracción de tarjeta inteligente no se aplica a los usuarios que se conectan a la instancia del servidor de conexión con la casilla de verificación **Iniciar sesión como usuario actual** seleccionada, aunque inicien sesión en el sistema cliente con una tarjeta inteligente.

- c Configurar la función de sugerencias del nombre de usuario de la tarjeta inteligente.

No puede configurar la función de sugerencias del nombre de usuario de la tarjeta inteligente si una autenticación por tarjeta inteligente está configurada como **No se permite**.

Opción	Acción
Habilite que los usuarios puedan utilizar un certificado de tarjeta inteligente único para autenticar varias cuentas de usuarios.	Seleccione la casilla de verificación Permitir las sugerencias del nombre de usuario de la tarjeta inteligente .
Deshabilite que los usuarios puedan utilizar un certificado de tarjeta inteligente único para autenticar varias cuentas de usuarios.	Desmarque la casilla de verificación Permitir las sugerencias del nombre de usuario de la tarjeta inteligente .

- 4 Si desea configurar la autenticación con tarjeta inteligente para los inicios de sesión de administradores en Horizon Administrator, haga clic en la pestaña **Autenticación** y seleccione una opción de configuración desde el menú desplegable **Autenticación de tarjeta inteligente para los administradores** en la sección Autenticación de View Administrator.

Opción	Acción
No se permite	La autenticación con tarjeta inteligente está deshabilitada en la instancia del servidor de conexión.
Opcional	Los administradores pueden usar la autenticación con tarjeta inteligente o la autenticación con contraseña para iniciar sesión en Horizon Administrator. Si se produce un error en la autenticación con tarjeta inteligente, el administrador debe proporcionar una contraseña.
Obligatoria	Es necesario que los administradores usen la autenticación por tarjeta inteligente cuando inician sesión en Horizon Administrator.

- 5 Haga clic en **Aceptar**.

- 6 Reinicie el servicio del servidor de conexión.

Debe reiniciar el servicio del servidor de conexión para que los cambios en la configuración de la tarjeta inteligente se apliquen, con una excepción. Puede cambiar las opciones de autenticación con tarjeta inteligente **Opcional** y **Requerido** sin que sea necesario reiniciar el servicio del servidor de conexión.

Estos cambios de la configuración de la tarjeta inteligente no afectan a los administradores y a los usuarios con la sesión ya iniciada.

Pasos siguientes

Prepare Active Directory para la autenticación con tarjeta inteligente, si es necesario. Consulte [Preparar Active Directory para la autenticación con tarjeta inteligente](#).

Verifique la configuración de la autenticación con tarjeta inteligente. Consulte [Verificar la configuración de la autenticación con tarjeta inteligente](#).

Configurar la autenticación con tarjeta inteligente en soluciones de terceros

Las soluciones de terceros como los equilibradores de carga y las puertas de enlace pueden realizar una autenticación con tarjeta inteligente enviando una aserción SAML que contenga el PIN cifrado y el certificado X.590 de la tarjeta inteligente.

Este tema detalla las tareas para configurar que las soluciones de terceros proporcionen el certificado X.590 correspondiente al servidor de conexión después de que el dispositivo de partner valide el certificado. Como esta función usa la autenticación SAML, una de las tareas es crear un autenticador SAML en Horizon Administrator.

Para obtener más información sobre la configuración de la autenticación con tarjeta inteligente en Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Procedimiento

- 1 Crear una autenticación SAML para el equilibrador de carga o la puerta de enlace de terceros.
Consulte [Configurar un autenticador SAML en Horizon Administrator](#).
- 2 Amplíe el período de caducidad de los metadatos del servidor de conexión para que las sesiones remotas no finalicen después de solo 24 horas.
Consulte [Cambiar el período de caducidad de los metadatos del proveedor de servicios en el servidor de conexión](#).
- 3 Si es necesario, configure el dispositivo de terceros para usar los metadatos del proveedor del servicio desde el servidor de conexión.
Consulte la documentación del producto del dispositivo de terceros.
- 4 Configure las opciones de la tarjeta inteligente del dispositivo de terceros.
Consulte la documentación del producto del dispositivo de terceros.

Preparar Active Directory para la autenticación con tarjeta inteligente

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

- [Agregar UPN para usuarios de tarjetas inteligentes](#)
Como los inicios de sesión de tarjetas inteligentes se basan en los nombres principales de usuarios (UPN), las cuentas de Active Directory de usuarios y administradores que usan tarjetas inteligentes para autenticarse en Horizon 7 deben tener un UPN válido.
- [Agregar el certificado raíz al almacén Enterprise NTAAuth](#)
Si utiliza una CA para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado raíz al almacén Enterprise NTAAuth en Active Directory. No es necesario realizar este procedimiento si el controlador de dominio de Windows actúa como la CA raíz.
- [Agregar el certificado raíz a las entidades de certificación raíz de confianza](#)
Si utiliza una entidad de certificación (CA) para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado raíz a la directiva de grupo Entidades de certificación raíz de confianza en Active Directory. No es necesario realizar este procedimiento si el controlador de dominio de Windows actúa como la CA raíz.
- [Agregar un certificado intermedio a las entidades de certificación intermedias](#)
Si utiliza una entidad de certificación intermedia (CA) para expedir certificados del controlador de dominio o de inicio de sesión de tarjetas inteligentes, debe agregar el certificado intermedio a la directiva de grupo Entidades de certificación en Active Directory.

Agregar UPN para usuarios de tarjetas inteligentes

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

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

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

Requisitos previos

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

Procedimiento

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

Agregar el certificado raíz al almacén Enterprise NTAAuth

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

Procedimiento

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

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

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

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

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

Procedimiento

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

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

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

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

Pasos siguientes

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

Agregar un certificado intermedio a las entidades de certificación intermedias

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

Procedimiento

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

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

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

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

Verificar la configuración de la autenticación con tarjeta inteligente

Después de configurar la autenticación por tarjeta inteligente por primera vez o si esta autenticación no funciona correctamente, debe verificar la configuración de la autenticación con tarjeta inteligente.

Procedimiento

- Compruebe que cada sistema cliente tenga un middleware de tarjeta inteligente, una tarjeta inteligente con un certificado válido y un lector de tarjetas inteligentes. Para los usuarios finales, compruebe que tengan Horizon Client.

Consulte la documentación proporcionada por el proveedor de la tarjeta inteligente para obtener más información sobre cómo configurar el hardware y el software de la tarjeta inteligente.

- En cada sistema cliente, seleccione **Inicio > Configuración > Panel de control > Opciones de Internet > Contenido > Certificados > Personal** para verificar que los certificados estén disponibles para la autenticación con tarjeta inteligente.

Cuando un usuario o un administrador introduce una tarjeta inteligente en un lector, Windows copia los certificados de la tarjeta inteligente al equipo del usuario. Las aplicaciones en el sistema cliente, incluido Horizon Client, pueden usar estos certificados.

- En el archivo `locked.properties` que se encuentra en el host del servidor de seguridad o del servidor de conexión, compruebe que la propiedad `useCertAuth` esté configurada como **true** y esté escrita correctamente.

El archivo `locked.properties` se encuentra en `install_directory\VMware\VMware View\Server\sslgateway\conf`. La propiedad `useCertAuth` se suele escribir como `userCertAuth` de forma errónea.

- Si configuró la autenticación con tarjeta inteligente en una instancia del servidor de conexión, compruebe la opción de autenticación con tarjeta inteligente en Horizon Administrator.

a Seleccione **Configuración de View > Servidores**.

b En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión y haga clic en **Editar**.

- c Si configuró la autenticación con tarjeta inteligente para los usuarios, en la pestaña **Autenticación**, compruebe que la opción **Autenticación de tarjeta inteligente para los usuarios** esté configurada como **Opcional** o **Requerido**.
- d Si configuró la autenticación por tarjeta inteligente para los administradores, en la pestaña **Autenticación**, compruebe que la opción **Autenticación de tarjeta inteligente para los administradores** esté configurada como **Opcional** o **Requerido**.

Debe reiniciar el servicio del servidor de conexión para que se apliquen los cambios de la configuración de la tarjeta inteligente.

- Si el dominio en el que reside un usuario de tarjeta inteligente es diferente del dominio que expidió el certificado raíz, compruebe que la UPN del usuario se estableció en el SAN que se encuentra en el certificado raíz de la CA de confianza.
 - a Consulte las propiedades del certificado para buscar el SAN que se encuentra en el certificado raíz de la CA de confianza.
 - b En el servidor de Active Directory, seleccione **Inicio > Herramientas administrativas > Usuarios y equipos de Active Directory**.
 - c Haga clic con el botón secundario en la carpeta **Usuarios** y seleccione **Propiedades**. Aparece la UPN en los cuadros de texto **Nombre de inicio de sesión de usuario** en la pestaña **Cuenta**.
- Si un usuario de tarjeta inteligente selecciona el protocolo de visualización PCoIP o el protocolo de visualización VMware Blast para conectarse a escritorios de sesión única, compruebe que View Agent o el componente Horizon Agent denominado Redireccionamiento de tarjeta inteligente se encuentre instalado en los equipos de los usuarios únicos. La función de tarjeta inteligente permite a los usuarios iniciar sesión en los escritorios de sesión única con las tarjetas inteligentes. Los hosts RDS, que tienen instalada la función Servicios de Escritorio remoto, admiten la función de tarjeta inteligente automáticamente y no es necesario que la instale.
- Compruebe los archivos de registro que se encuentran en `unidad:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` en el host del servidor de seguridad o del servidor de conexión para los mensajes que afirman que la autenticación con tarjeta inteligente está habilitada.

Uso de la comprobación de revocación de certificados de tarjeta inteligente

Para impedir que los usuarios con certificados revocados se autenticuen con tarjetas inteligentes, se debe configurar la comprobación de revocación de certificados. Los certificados se revocan con frecuencia cuando un usuario abandona una organización, pierde una tarjeta inteligente o se traslada de un departamento a otro.

Horizon 7 admite la comprobación de revocación de certificados con listas de revocación de certificados (CRL) y con el protocolo de estado de certificado en línea (OCSP). Una CRL es una lista de certificados revocados publicada por la entidad de certificación que los emitió. OCSP es un protocolo de validación de certificados que se utiliza para obtener el estado de revocación de un certificado X.509.

Puede configurar la comprobación de la revocación del certificado en una instancia del servidor de conexión o en un servidor de seguridad. Cuando una instancia del servidor de conexión se empareja con un servidor de seguridad, debe configurar la comprobación de la revocación del certificado en el servidor de seguridad. Es necesario que se pueda acceder a la CA desde el host del servidor de conexión o del servidor de seguridad.

Puede configurar tanto la CRL como el OCSP en la misma instancia del servidor de conexión o en el servidor de seguridad. Al configurar ambos tipos de comprobación de revocación de certificados, Horizon 7 intenta utilizar primero OCSP y recurre a CRL si OCSP falla. Horizon 7 no utiliza OCSP si CRL falla.

- **Iniciar sesión con la comprobación de CRL**

Cuando configure la comprobación de CRL, Horizon 7 construye y lee una CRL para determinar el estado de revocación de un certificado de usuario.

- **Iniciar sesión con la comprobación de revocación del certificado OCSP**

Cuando configure la comprobación de revocación del certificado OCSP, Horizon 7 envía una solicitud a un respondedor OCSP para determinar el estado de revocación de un certificado de un usuario específico. Horizon 7 usa un certificado firmado por OCSP para verificar que las respuestas que reciba del respondedor OCSP sean originales.

- **Configurar comprobación de CRL**

Cuando configure la comprobación de CRL, Horizon 7 lee una CRL para determinar el estado de revocación del certificado de usuario de tarjeta inteligente.

- **Configurar la comprobación de revocación del certificado OCSP**

Cuando configure la comprobación de revocación del certificado OCSP, Horizon 7 envía una solicitud de verificación a un respondedor OCSP para determinar el estado de revocación del certificado de usuario de tarjeta inteligente.

- **Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente**

Establezca los valores en el archivo `locked.properties` para habilitar y configurar la comprobación de la revocación del certificado de la tarjeta inteligente.

Iniciar sesión con la comprobación de CRL

Cuando configure la comprobación de CRL, Horizon 7 construye y lee una CRL para determinar el estado de revocación de un certificado de usuario.

Si se revocó un certificado y la autenticación por tarjeta inteligente es opcional, aparece el cuadro de diálogo **Introduzca su nombre de usuario y su contraseña** y el usuario debe proporcionar una contraseña para autenticarse. Si es necesaria una autenticación por tarjeta inteligente, el usuario recibe un mensaje de error y no se le permite autenticarse. Pasará lo mismo si Horizon 7 no puede leer la CRL.

Iniciar sesión con la comprobación de revocación del certificado OSCP

Cuando configure la comprobación de revocación del certificado OSCP, Horizon 7 envía una solicitud a un respondedor OSCP para determinar el estado de revocación de un certificado de un usuario específico. Horizon 7 usa un certificado firmado por OSCP para verificar que las respuestas que reciba del respondedor OSCP sean originales.

Si se revocó el certificado de usuario y la autenticación por tarjeta inteligente es opcional, aparece el cuadro de diálogo **Introduzca su nombre de usuario y su contraseña** y el usuario debe proporcionar una contraseña para autenticarse. Si es necesaria una autenticación por tarjeta inteligente, el usuario recibe un mensaje de error y no se le permite autenticarse.

Horizon 7 recurre a la comprobación de CRL si no recibe una respuesta del respondedor OSCP o si la respuesta no es válida.

Configurar comprobación de CRL

Cuando configure la comprobación de CRL, Horizon 7 lee una CRL para determinar el estado de revocación del certificado de usuario de tarjeta inteligente.

Requisitos previos

Familiarícese con las propiedades del archivo `locked.properties` para la comprobación de CRL. Consulte [Propiedades de la comprobación de revocación del certificado de la 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_de_instalación\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 Agregue las propiedades `enableRevocationChecking` y `crlLocation` al archivo `locked.properties`.
 - a Establezca `enableRevocationChecking` como **true** para habilitar la comprobación de la revocación del certificado de tarjeta inteligente.
 - b Establezca `crlLocation` como la ubicación del CRL. El valor puede ser una URL o una ruta de archivo.
- 3 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Ejemplo: Archivo `locked.properties`

El archivo muestra la autenticación de tarjeta inteligente y la comprobación de revocación del certificado de tarjeta inteligente, configura la comprobación de CRL y especifica una URL para la ubicación de CRL.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-R00T_CA.crl
```

Configurar la comprobación de revocación del certificado OCSF

Cuando configure la comprobación de revocación del certificado OCSF, Horizon 7 envía una solicitud de verificación a un respondedor OCSF para determinar el estado de revocación del certificado de usuario de tarjeta inteligente.

Requisitos previos

Familiarícese con las propiedades del archivo `locked.properties` para la comprobación de revocación del certificado OCSF. Consulte [Propiedades de la comprobación de revocación del certificado de la 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_de_instalación\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 Agregue las propiedades `enableRevocationChecking`, `enableOCSP`, `ocspURL` y `ocspSigningCert` al archivo `locked.properties`.
 - a Establezca `enableRevocationChecking` como **true** para habilitar la comprobación de la revocación del certificado de tarjeta inteligente.
 - b Establezca `enableOCSP` como **true** para habilitar la comprobación de la revocación del certificado OCSF.
 - c Establezca `ocspURL` como la URL del respondedor OCSF.
 - d Establezca `ocspSigningCert` como la ubicación del archivo que contiene el certificado firmado del respondedor OCSF.
- 3 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Ejemplo: Archivo `locked.properties`

El archivo mostrado habilita la autenticación con tarjeta inteligente y la comprobación de la revocación del certificado con tarjeta inteligente, configura las revocaciones de los certificados OCSP y CRL, especifica la ubicación del respondedor OCSP e identifica el archivo que contiene el certificado OCSP firmado.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente

Establezca los valores en el archivo `locked.properties` para habilitar y configurar la comprobación de la revocación del certificado de la tarjeta inteligente.

[Tabla 3-1](#) muestra las propiedades del archivo `locked.properties` para comprobar la revocación del certificado.

Tabla 3-1. Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente

Propiedad	Descripción
<code>enableRevocationChecking</code>	<p>Establezca esta propiedad en true para habilitar la comprobación de la revocación del certificado.</p> <p>Cuando esta propiedad está establecida en false, la comprobación de la revocación del certificado está deshabilitada y se ignoran el resto de las propiedades de comprobación de revocación del certificado.</p> <p>El valor predeterminado es false.</p>
<code>crlLocation</code>	<p>Especifica la ubicación de la CRL, que puede ser tanto una URL como una ruta de archivo.</p> <p>Si no especifica ninguna URL o la que especifica no es válida, Horizon 7 usa la lista de las CRL del certificado de usuario si el valor de <code>allowCertCRLs</code> está establecido en true o no está especificado.</p> <p>Si Horizon 7 no puede acceder a ninguna CRL, se produce un error en la comprobación de la misma.</p>
<code>allowCertCRLs</code>	<p>Cuando esta propiedad está establecida en true, Horizon 7 extrae una lista de CRL del certificado de usuario.</p> <p>El valor predeterminado es true.</p>

Tabla 3-1. Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente (Continuación)

Propiedad	Descripción
enableOCSP	Establezca esta propiedad en true para permitir la comprobación OCSP de la revocación del certificado. El valor predeterminado es false .
ocspURL	Especifica la URL de un respondedor OCSP.
ocspResponderCert	Especifica el archivo que contiene el certificado firmado del respondedor OCSP. Horizon 7 usa este certificado para verificar que las respuestas del respondedor OCSP sean originales.
ocspSendNonce	Cuando esta propiedad se establece en true , se envía un nonce con las solicitudes OCSP para evitar que se repitan las respuestas. El valor predeterminado es false .
ocspCRLFailover	Cuando esta propiedad está establecida en true , Horizon 7 usa la comprobación CRL si se produce un error en la comprobación de la revocación del certificado OCSP. El valor predeterminado es true .

Configurar otros tipos de autenticación de usuario

4

Horizon 7 utiliza su infraestructura existente de Active Directory para la administración y la autenticación de los usuarios y los administradores. También puede integrar Horizon 7 con otras formas de autenticación además de tarjetas inteligentes, como soluciones de autenticación biométrica o de autenticación en dos fases, como por ejemplo, RSA SecurID o RADIUS, para autenticar usuarios de aplicaciones y escritorios remotos.

Este capítulo incluye los siguientes temas:

- [Uso de la autenticación en dos fases](#)
- [Uso de la autenticación SAML](#)
- [Configurar la autenticación biométrica](#)

Uso de la autenticación en dos fases

Puede configurar una instancia del servidor de conexión de Horizon para que obligue a los usuarios a utilizar una autenticación RSA SecurID o RADIUS (Servicio de autenticación remota telefónica de usuario).

- El soporte de RADIUS ofrece un amplio rango de opciones alternativas de autenticación basadas en un token de dos fases.
- Horizon 7 también proporciona una interfaz abierta de extensión estándar para permitir a los proveedores de soluciones de terceros integrar extensiones de autenticación avanzada en Horizon 7.

Como las soluciones de autenticación en dos fases, como RSA SecurID y RADIUS, funcionan con administradores de autenticación, que se encuentran instalados en servidores independientes, debe tener configurados esos servidores y que el host del servidor de conexión pueda acceder a ellos. Por ejemplo, si se utiliza RSA SecurID, el administrador de autenticación sería el Administrador de autenticación de RSA. Si se dispone de RADIUS, el administrador de autenticación sería un servidor de RADIUS.

Para utilizar la autenticación de dos factores, cada usuario debe tener un token, como un token RSA SecurID, que esté registrado con su administrador de autenticación. Un token de autenticación de dos factores es un producto de hardware o de software que genera un código de autenticación a intervalos fijos. Con frecuencia, la autenticación requiere conocer tanto un PIN como un código de autenticación.

Si tiene varias instancias del servidor de conexión, puede configurar una autenticación en dos fases en algunas instancias y un método de autenticación del usuario diferente en otras. Por ejemplo, puede configurar una autenticación en dos fases solo para los usuarios que acceden a las aplicaciones y los escritorios remotos desde fuera de la red corporativa y a través de Internet.

Horizon 7 se certifica a través del programa RSA SecurID Ready y admite el rango completo de características de SecurID, incluido el nuevo modo de PIN, el modo del siguiente código de token, RSA Authentication Manager y el equilibrio de carga.

- **Iniciar sesión usando la autenticación en dos fases**

Cuando un usuario se conecta a una instancia del servidor de conexión de View que tenga las autenticaciones RSA SecurID o RADIUS habilitadas, aparece un cuadro de diálogo de inicio de sesión especial en Horizon Client.

- **Habilitar una autenticación en dos fases en Horizon Administrator**

Habilite una instancia del servidor de conexión para la autenticación RSA SecurID o la autenticación RADIUS modificando la configuración del servidor de conexión en Horizon Administrator.

- **Solucionar los problemas de acceso denegado de RSA SecurID**

Se deniega el acceso cuando Horizon Client se conecta con una autenticación RSA SecurID en dos fases.

- **Solucionar los problemas de acceso denegado de RADIUS**

Se deniega el acceso cuando Horizon Client se conecta con una autenticación RADIUS en dos fases.

Iniciar sesión usando la autenticación en dos fases

Cuando un usuario se conecta a una instancia del servidor de conexión de View que tenga las autenticaciones RSA SecurID o RADIUS habilitadas, aparece un cuadro de diálogo de inicio de sesión especial en Horizon Client.

Los usuarios introducen el nombre de usuario y el código de acceso de las autenticaciones RADIUS o RSA SecurID en este cuadro de diálogo de inicio de sesión especial. Un código de acceso de autenticación en dos fases suele consistir en un PIN seguido de un código de token.

- Si RSA Authentication Manager necesita que los usuarios introduzcan un nuevo PIN de RSA SecurID después de introducir el nombre de usuario y el código de acceso de RSA SecurID, aparece un cuadro de diálogo de PIN. Después de configurar un nuevo PIN, se solicita a los usuarios que esperen al siguiente código de token antes de iniciar sesión. Si RSA Authentication Manager está configurado para usar los PIN generados por el sistema, aparece un cuadro de diálogo para confirmar el PIN.
- Cuando inicie sesión en Horizon 7, la autenticación RADIUS funciona de forma semejante a RSA SecurID. Si el servidor de RADIUS muestra un desafío de acceso, Horizon Client muestra un cuadro de diálogo similar a la solicitud de RSA SecurID para el siguiente código de token. La compatibilidad actual de los desafíos de RADIUS está limitada para solicitar de entrada de texto. No se muestran los textos de desafío enviado desde el servidor RADIUS. Actualmente no se admiten formas más complejas de desafíos, como varias opciones o selección de imágenes.

Después de que un usuario introduzca las credenciales en Horizon Client, el servidor de RADIUS puede enviar un mensaje de texto SMS o un correo electrónico, o bien un texto usando otro mecanismo fuera de banda, al teléfono móvil del usuario con un código. El usuario puede introducir este texto y código en Horizon Client para completar la autenticación.

- Como los proveedores de RADIUS ofrecen la capacidad de importar usuarios desde Active Directory, es posible que se solicite a los usuarios finales en primer lugar proporcionar credenciales de Active Directory antes de solicitar el nombre de usuario y el código de acceso de la autenticación RADIUS.

Habilitar una autenticación en dos fases en Horizon Administrator

Habilite una instancia del servidor de conexión para la autenticación RSA SecurID o la autenticación RADIUS modificando la configuración del servidor de conexión en Horizon Administrator.

Requisitos previos

Instale y configure el software de autenticación en dos fases, como el software RSA SecurID o el software RADIUS en un servidor de administración de autenticación.

- Para una autenticación RSA SecurID, exporte el archivo `sdconf.rec` de la instancia del servidor de conexión desde el Administrador de autenticación RSA. Consulte la documentación del Administrador de autenticación de RSA.
- Para una autenticación RADIUS, siga la documentación sobre la configuración del proveedor. Anote el nombre de host o la dirección IP del servidor de RADIUS, el número de puerto en el que está realizando la escucha de la autenticación RADIUS (generalmente el 1812), el tipo de autenticación (PAP, CHAP, MS-CHAPv1 o MS-CHAPv2) y el secreto compartido. Tendrá que introducir esos valores en Horizon Administrator. Puede introducir valores para un autenticador RADIUS primario y secundario.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione el servidor y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, acceda a la lista desplegable **Autenticación en dos fases** de la sección Autenticación avanzada y seleccione **RSA SecurID** o **RADIUS**.
- 4 Para forzar que los nombres de usuario de RSA SecurID o RADIUS coincidan con los nombres de usuario en Active Directory, seleccione **Exigir que los nombres de usuario de SecurID y Windows coincidan** u **Obligar a la autenticación en dos fases y la coincidencia de nombre de usuario de Windows**.

Si selecciona esta opción, los usuarios deben usar el mismo nombre de usuario de RSA SecurID o de RADIUS para la autenticación de Active Directory. Si no selecciona esta opción, los nombres pueden ser diferentes.

- 5 Para RSA SecurID, haga clic en **Cargar archivo**, escriba la ubicación de `sdconf.rec` o haga clic en **Examinar** para buscar el archivo.

6 Para una autenticación RADIUS, complete el resto de los campos:

- a Seleccione **Usar el mismo nombre y la misma contraseña para la autenticación RADIUS y Windows** si la autenticación RADIUS inicial usa la autenticación Windows que activa una transmisión fuera de banda de un código token y este código se utiliza como parte de una comprobación RADIUS.

Si selecciona esta casilla, no se solicitarán las credenciales de Windows a los usuarios después de una autenticación RADIUS si esta autenticación usa el nombre de usuario y la contraseña de Windows. Los usuarios no tienen que volver a introducir el nombre de usuario y la contraseña de Windows después de una autenticación RADIUS.

- b En la lista desplegable **Autenticador**, seleccione **Crear autenticador nuevo** y complete la página.

- Establezca el **Puerto de contabilidad** en **0** a menos que desee habilitar la contabilidad de RADIUS. Establezca este puerto en un número que no sea cero solo si el servidor de RADIUS admite recopilación de datos de contabilidad. Si el servidor de RADIUS no admite mensajes de contabilidad y se configura este puerto en un número que no sea cero, los mensajes se enviarán e ignorarán y, posteriormente, se volverá a intentar el envío una serie de veces que causará un retraso de autenticación.

Los datos de contabilidad permiten facturar a los usuarios en función de los datos y el tiempo de uso. Los datos de contabilidad también se pueden utilizar con propósitos estadísticos y para monitorización general de la red.

- Si especifica una cadena de prefijo de territorio, esta se colocará delante del nombre de usuario cuando se envíe al servidor de RADIUS. Por ejemplo, si el nombre de usuario introducido en Horizon Client es **jdoe** y se especifica el prefijo de territorio **DOMAIN-A**, el nombre de usuario **DOMAIN-A\jdoe** se envía al servidor de RADIUS. De forma similar, si usa el sufijo del dominio kerberos **@mycorp.com**, el nombre de usuario **jdoe@mycorp.com** se envía al servidor RADIUS.

7 Haga clic en **Aceptar** para guardar los cambios.

No es necesario reiniciar el servicio del servidor de conexión. Los archivos de configuración necesarios se distribuyen de forma automática y las opciones de configuración se aplican de forma inmediata.

Cuando los usuarios abren Horizon Client y se autentican en el servidor de conexión, se les solicita una autenticación en dos fases. Para la autenticación RADIUS, el cuadro de diálogo de inicio de sesión muestra mensajes de texto que contienen la etiqueta del token que especificó.

Los cambios de configuración de la autenticación RADIUS afectan a las sesiones de las aplicaciones y los escritorios remotos que se iniciaron después de cambiar la configuración. Estos cambios no afectan a las sesiones iniciadas en ese momento.

Pasos siguientes

Si cuenta con un grupo de instancias del servidor de conexión y desea configurar la autenticación RADIUS en ellas, puede volver a usar una configuración del autenticador RADIUS ya existente.

Solucionar los problemas de acceso denegado de RSA SecurID

Se deniega el acceso cuando Horizon Client se conecta con una autenticación RSA SecurID en dos fases.

Problema

Una conexión de Horizon Client con RSA SecurID muestra Acceso denegado y RSA Authentication Manager Log Monitor muestra el error Error al verificar el nodo.

Causa

Es necesario restablecer el secreto del nodo del host RSA Agent.

Solución

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione el servidor de conexión y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, seleccione **Borrar secreto de nodo**.
- 4 Haga clic en **Aceptar** para borrar el secreto de nodo.
- 5 En el equipo que ejecuta RSA Authentication Manager, seleccione **Inicio > Programa > RSA Security > Modo del host RSA Authentication Manager**.
- 6 Seleccione **Host agente > Editar host agente**.
- 7 Seleccione **Servidor de conexión de View** en la lista y desmarque la casilla de verificación **Secreto de nodo creado**.

La opción **Secreto de nodo creado** está seleccionada de forma predeterminada cada vez que la edita.

- 8 Haga clic en **Aceptar**.

Solucionar los problemas de acceso denegado de RADIUS

Se deniega el acceso cuando Horizon Client se conecta con una autenticación RADIUS en dos fases.

Problema

Una conexión de Horizon Client que usa una autenticación RADIUS en dos fases aparece como Acceso denegado.

Causa

RADIUS no recibe ninguna respuesta del servidor de RADIUS, lo que hace que Horizon 7 caduque.

Solución

Los siguientes errores comunes de comunicación suelen derivar en esta situación:

- El servidor de RADIUS no se configuró para aceptar la instancia del servidor de conexión de View como un cliente RADIUS. Cada instancia del servidor de conexión de View que use RADIUS debe configurarse como un cliente en el servidor de RADIUS. Consulte la documentación de su producto de autenticación RADIUS en dos fases.
- Los valores secretos compartidos en la instancia del servidor de conexión de View y el servidor de RADIUS no coinciden.

Uso de la autenticación SAML

El lenguaje de marcado para afirmaciones de seguridad (Security Assertion Markup Language, SAML) es un estándar basado en XML que se utiliza para describir e intercambiar información de autenticación y autorización entre distintos dominios de seguridad. SAML transmite información sobre los usuarios entre proveedores de identidades y de servicios en documentos XML llamados aserciones SAML.

Puede usar la autenticación SAML para integrar Horizon 7 con VMware Workspace ONE, con VMware Identity Manager o con una puerta de enlace o un equilibrador de carga de terceros completos. Cuando configure SAML para un dispositivo de terceros, consulte la documentación del proveedor si desea obtener información sobre cómo configurar Horizon 7 para que funcionen juntos. Cuando SSO está habilitado, los usuarios que inician sesión en VMware Identity Manager o en un dispositivo de terceros pueden iniciar aplicaciones y escritorios remotos sin tener que realizar un segundo proceso de inicio de sesión. También puede usar la autenticación SAML para implementar la autenticación de tarjeta inteligente en VMware Access Point o en dispositivos de terceros.

Para delegar la responsabilidad de la autenticación en Workspace ONE, VMware Identity Manager o un dispositivo de terceros, debe crear un autenticador SAML en Horizon 7. Un autenticación SAML contiene el intercambio de metadatos y la confianza entre Horizon 7 y Workspace ONE, VMware Identity Manager o el dispositivo de terceros. Se asocia un autenticador SAML con una instancia del servidor de conexión.

Utilizar la autenticación SAML para integrar VMware Identity Manager

La integración de Horizon 7 y de VMware Identity Manager (anteriormente Workspace ONE) se realiza con el estándar SAML 2.0 a fin de establecer la confianza mutua requerida para la función Single Sign-On (SSO). Al habilitar SSO, los usuarios que inician sesión en VMware Identity Manager o Workspace ONE con credenciales de Active Directory pueden iniciar escritorios remotos y aplicaciones sin tener que pasar por un segundo procedimiento de inicio de sesión.

Cuando VMware Identity Manager y Horizon 7 se integran, VMware Identity Manager genera un artefacto SAML único cada vez que un usuario inicie sesión en VMware Identity Manager y haga clic en un icono de escritorio o aplicación. VMware Identity Manager utiliza dicho artefacto SAML para crear un identificador de recursos universal (Universal Resource Identifier, URI). El URI incluye información sobre la instancia del servidor de conexión en la que se encuentra el grupo de escritorios o aplicaciones, cuál escritorio o aplicación se inicia y el artefacto SAML.

VMware Identity Manager envía el artefacto SAML a Horizon Client, que a su vez lo envía a la instancia del servidor de conexión. La instancia del servidor de conexión utiliza el artefacto para recuperar la aserción SAML de VMware Identity Manager.

Tras recibir la aserción SAML, la instancia del servidor de conexión la valida, descifra la contraseña del usuario y utiliza dicha contraseña para iniciar el escritorio o aplicación.

Configurar la integración de VMware Identity Manager y Horizon 7 supone configurar VMware Identity Manager con información de Horizon 7 y configurar Horizon 7 para que se delegue la responsabilidad de la autenticación en VMware Identity Manager.

Para delegar la responsabilidad de autenticación en VMware Identity Manager, debe crear un autenticador SAML en Horizon 7. Un autenticador de SAML incluye el intercambio de confianza y metadatos entre Horizon 7 y VMware Identity Manager. Se asocia un autenticador SAML con una instancia del servidor de conexión.

Nota Si tiene pensado proporcionar acceso a los escritorios y las aplicaciones a través de VMware Identity Manager, verifique que cree los grupos de aplicaciones y de escritorios como un usuario con la función Administradores en el grupo de acceso raíz de Horizon Administrator. Si proporciona al usuario la función Administradores en un grupo de acceso diferente al raíz, VMware Identity Manager no reconocerá el autenticador SAML que configuró en Horizon 7 y no podrá configurar el grupo en VMware Identity Manager.

Configurar un autenticador SAML en Horizon Administrator

Para iniciar aplicaciones y escritorios remotos desde VMware Identity Manager o para conectarse a estos a través de una puerta de enlace o un equilibrador de carga de terceros, debe crear un autenticador SAML en Horizon Administrator. Un autenticador SAML contiene el intercambio de metadatos y de confianza entre Horizon 7 y el dispositivo al que se conectan los clientes.

Se asocia un autenticador SAML con una instancia del servidor de conexión. Si la implementación incluye más de una instancia del servidor de conexión, el autenticador SAML se debe asociar a cada una de ellas.

Puede permitir que un autenticador estático y varios autenticadores dinámicos se publiquen a la vez. Puede configurar los autenticadores vIDM (dinámico) y Unified Access Gateway (estático) y mantenerlos en estado activo. Puede establecer conexiones a través de uno de estos autenticadores.

Puede configurar más de un autenticador SAML en un servidor de conexión y todos los autenticadores pueden estar activos de forma simultánea. Sin embargo, el ID de entidad de cada uno de estos autenticadores SAML configurados en el servidor de conexión deben ser diferentes.

El estado del autenticador SAML en el panel de control siempre es verde ya que este metadato es predefinido y estático. La alternancia verde y rojo solo se aplica para autenticadores dinámicos.

Para obtener más información sobre cómo configurar un autenticador SAML en dispositivos de VMware Unified Access Gateway, consulte *Implementación y configuración de Unified Access Gateway*.

Requisitos previos

- Compruebe que Workspace ONE, VMware Identity Manager, un equilibrador de carga o una puerta de enlace de terceros estén instalados y configurados. Consulte la documentación de instalación de ese producto.
- Verifique que el certificado raíz de la autoridad de certificación que firma el certificado del servidor SAML esté instalado en el host del servidor de conexión. VMware no recomienda configurar los autenticadores SAML para utilizar certificados autofirmados. Para obtener información sobre la autenticación de certificados, consulte el documento *Instalación de Horizon 7*.
- Anote el FQDN o la dirección IP de los servidores de Workspace ONE, de VMware Identity Manager o el equilibrador de carga externo.
- (opcional) Si usa Workspace ONE o VMware Identity Manager, anote la URL de la interfaz web del conector.
- Si crea un autenticador para Unified Access Gateway o un dispositivo de terceros que necesite que genere metadatos SAML y que cree un autenticador estático, realice el procedimiento en el dispositivo para generar los metadatos SAML y, a continuación, cópielos.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor para asociarla al autenticador SAML y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, seleccione un valor del menú desplegable **Delegación de la autenticación a VMware Horizon (autenticador SAML 2.0)** para habilitar o deshabilitar el autenticador SAML.

Opción	Descripción
Deshabilitada	La autenticación SAML está deshabilitada. Solo se pueden iniciar aplicaciones y escritorios remotos desde Horizon Client.
Permitida	La autenticación SAML está habilitada. Puede iniciar aplicaciones y escritorios remotos para Horizon Client y VMware Identity Manager o el dispositivo de terceros.
Obligatoria	La autenticación SAML está habilitada. Puede iniciar aplicaciones y escritorios remotos solo desde el VMware Identity Manager o el dispositivo de terceros. No puede iniciar aplicaciones o escritorios desde Horizon Client de forma manual.

Cada una de las instancias del servidor de conexión de la implementación se puede configurar con distintos valores de autenticación SAML, de acuerdo a las necesidades.

- 4 Haga clic en **Administrar autenticadores SAML** y en **Agregar**.

5 Configure el autenticador SAML en el cuadro de diálogo Agregar autenticador SAML 2.0.

Opción	Descripción
Tipo	Para Unified Access Gateway o un dispositivo de terceros, seleccione Estático . Para VMware Identity Manager, seleccione Dinámico . Para los autenticadores dinámicos, puede especificar una URL de metadatos y una URL de administración. Para los autenticadores estáticos, debe generar en primer lugar los metadatos de Unified Access Gateway o de un dispositivo de terceros, copie los metadatos y, a continuación, péguelos en el cuadro de texto Metadatos SAML .
Etiqueta	Nombre único que identifica al autenticador SAML.
Descripción	Breve descripción del autenticador SAML. Este valor es opcional.
URL de metadatos	(Para los autenticadores dinámicos) URL para recuperar toda la información necesaria para intercambiar la información SAML entre el proveedor de identidad SAML y la instancia del servidor de conexión. En la URL <code>https://<NOMBRE DEL HORIZON SERVER>/SAAS/API/1.0/GET/metadata/idp.xml</code> , haga clic en <NOMBRE DEL HORIZON SERVER> y reemplace el FQDN o la dirección IP del servidor de VMware Identity Manager o el equilibrador de carga externo (dispositivo de terceros).
URL de administración	(Para autenticadores dinámicos) URL para acceder a la consola de administración del proveedor de identidades SAML. Para VMware Identity Manager, esta URL debe dirigir a la interfaz web del conector de VMware Identity Manager. Este valor es opcional.
Metadatos SAML	(Para autenticadores estáticos) Texto de metadatos que generó y copió desde Unified Access Gateway o de un dispositivo de terceros.
Habilitado para el servidor de conexión	Selecione esta casilla para habilitar el autenticador. Se pueden habilitar varios autenticadores. La lista solo incluye los autenticadores habilitados.

6 Haga clic en **Aceptar** para guardar la configuración del autenticador SAML.

Si se proporcionó información válida, se debe aceptar el certificado autofirmado (no se recomienda) o utilizar un certificado de confianza para Horizon 7 y VMware Identity Manager o el dispositivo de terceros.

El cuadro de diálogo Administrar autenticadores SAML muestra el nuevo autenticador creado.

7 En la sección Estado del sistema del panel de información de Horizon Administrator, seleccione **Otros componentes > Autenticadores SAML 2.0**, seleccione el autenticador SAML agregado y verifique los detalles.

Si la configuración es correcta, el estado del autenticador se mostrará en verde. El estado del autenticador puede estar en rojo si no se confía en el certificado, si VMware Identity Manager no está disponible o si la URL de metadatos no es válida. Si no se confía en el certificado, es posible que se pueda hacer clic en **Verificar** para validar y aceptar el certificado.

Pasos siguientes

Amplíe el período de caducidad de los metadatos del servidor de conexión para que las sesiones remotas no finalicen después de solo 24 horas. Consulte [Cambiar el período de caducidad de los metadatos del proveedor de servicios en el servidor de conexión](#).

Configurar la compatibilidad del proxy con VMware Identity Manager

Horizon 7 hace que el proxy sea compatible con el servidor de VMware Identity Manager (vIDM). Los detalles del proxy, como el número de puerto y el nombre de host, pueden configurarse en la base de datos ADAM, y las solicitudes HTTP se enrutan a través del proxy.

Esta función es compatible con la implementación híbrida, donde la implementación de Horizon 7 en las instalaciones puede comunicarse con un servidor vIDM que se aloja en la nube.

Requisitos previos

Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión.
- 2 Expanda el árbol ADAM ADSI que aparece en la ruta de acceso del objeto:
`cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes.`
- 3 Seleccione **Acción > Propiedades** y, en el atributo **pae-NameValuePair**, agregue las nuevas entradas **pae-SAMLProxyName** y **pae-SAMLProxyPort**.

Cambiar el período de caducidad de los metadatos del proveedor de servicios en el servidor de conexión

Si no lo hace, el servidor de conexión dejará de aceptar aserciones SAML del autenticador SAML 24 horas después, por ejemplo, Unified Access Gateway o un proveedor de identidades externo, y el intercambio de metadatos se deberá repetir.

Utilice este procedimiento para especificar el número de días que pueden transcurrir para que el servidor de conexión deje de aceptar aserciones SAML del proveedor de identidades. Este número es el que se utiliza cuando finaliza el período de caducidad actual. Por ejemplo, si el período de caducidad actual es de 1 día y especifica 90 días, cuando transcurra 1 día, el servidor de conexión generará metadatos con un período de caducidad de 90 días.

Requisitos previos

Visite el sitio web de Microsoft TechNet Web si desea obtener información sobre cómo utilizar la utilidad Editor ADSI en la versión que utilice del sistema operativo de 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**.

- 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**

- Amplíe el árbol del Editor ADSI, amplíe **OU=Properties**, seleccione **OU=Global** y haga doble clic en **CN=Common** en el panel derecho.
- En el cuadro de diálogo Propiedades, edite el atributo **pae-NameValuePair** para agregar los valores siguientes

```
cs-samlencryptionkeyvaliditydays=número_de_días
cs-samlsigningkeyvaliditydays=número_de_días
```

En este ejemplo, *número_de_días* es el número de días que pueden transcurrir para que un servidor de conexión remoto deje de aceptar aserciones SAML. Tras este período de tiempo se debe repetir el proceso de intercambio de metadatos SMLS.

Generar metadatos SAML para que el servidor de conexión se pueda usar como proveedor del servicio

Después de crear y habilitar un autenticador SAML para el proveedor de identidades que desee utilizar, es posible que necesite generar los metadatos del servidor de conexión. Use estos metadatos para crear un proveedor del servicio en el dispositivo de Unified Access Gateway o un equilibrador de carga de terceros para que sean el proveedor de identidades.

Requisitos previos

Verifique que creó un autenticador SAML para el proveedor de identidades: Unified Access Gateway o una puerta de enlace o un equilibrador de carga de terceros. En la sección Estado del sistema del panel de información de Horizon Administrator, puede seleccionar **Otros componentes > Autenticadores SAML 2.0**; a continuación puede seleccionar el autenticador SAML que agregó y verificar los detalles.

Procedimiento

- Abra una nueva pestaña del navegador e introduzca la URL para obtener los metadatos SAML del servidor de conexión.

`https://connection-server.example.com/SAML/metadata/sp.xml`

En este ejemplo, *connection-server.example.com* es el nombre de dominio completo del host del servidor de conexión.

Esta página muestra los metadatos SAML del servidor de conexión.

- Use un comando **Guardar como** para guardar la página web en un archivo XML.

Por ejemplo, puede guardar la página en un archivo denominado `connection-server-metadata.xml`. El contenido de este archivo comienza con el texto siguiente:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

Pasos siguientes

Use el procedimiento apropiado en el proveedor de identidades para copiar los metadatos SAML del servidor de conexión. Consulte la documentación de Unified Access Gateway o de una puerta de enlace o un equilibrador de carga de terceros.

Consideraciones del tiempo de respuesta para varios autenticadores SAML dinámicos

Si configura la autenticación SAML 2.0 como opcional u obligatoria en una instancia del servidor de conexión y asocia varios autenticadores SAML dinámicos a la instancia del servidor de conexión, si no se puede acceder a alguno de ellos, aumenta el tiempo de respuesta para iniciar escritorios remotos desde otros autenticadores SAML dinámicos.

Puede disminuir el tiempo de respuesta del inicio de los escritorios remotos en el resto de autenticadores SAML dinámicos usando Horizon Administrator para deshabilitar los autenticadores SAML dinámicos a los que no se puedan acceder. Para obtener más información sobre cómo deshabilitar un autenticador SAML, consulte [Configurar un autenticador SAML en Horizon Administrator](#).

Configurar directivas de acceso de Workspace ONE en Horizon Administrator

Los administradores de Workspace ONE o VMware Identity Manager (vIDM) pueden configurar las directivas de acceso para limitar el acceso a los escritorios y aplicaciones autorizados en Horizon 7. Para aplicar las directivas creadas en vIDM, Horizon Client debe estar configurado en el modo Workspace ONE para que pueda insertar al usuario en el cliente de Workspace ONE para iniciar las autorizaciones. Cuando inicie sesión Horizon Client, la directiva de acceso le dirige para iniciar sesión a través de Workspace ONE para acceder a sus aplicaciones y escritorios publicados.

Requisitos previos

- Configure las directivas de acceso para aplicaciones en Workspace ONE. Para obtener más información sobre la configuración de directivas de acceso, consulte *Guía de administración de VMware Identity Manager*.
- Autorice a los usuarios a aplicaciones y escritorios publicados en Horizon Administrator.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor que esté asociada con un autenticador SAML y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, establezca la opción **Delegación de la autenticación a VMware Horizon (autenticador SAML 2.0)** en **Requerida**.

La opción Requerida habilita la autenticación SAML. El usuario final solo puede conectarse a Horizon Server con un token SAML proporcionado por un proveedor de identidades externo o de vIDM. No puede iniciar aplicaciones o escritorios desde Horizon Client de forma manual.

- 4 Seleccione **Habilitar el modo Workspace ONE**.
- 5 En el cuadro de texto **Nombre del host del servidor de Workspace ONE**, introduzca el valor FQDN del nombre de host de Workspace ONE.
- 6 (opcional) Seleccione **Bloquear las conexiones desde clientes que no admitan el modo Workspace ONE** para restringir los Horizon Client que sean compatibles con el modo Workspace ONE de las aplicaciones de acceso.

Las versiones de Horizon Client anteriores a 4.5 no admiten la función del modo Workspace ONE. Si selecciona esta opción, las versiones de Horizon Client anteriores a 4.5 no pueden acceder a las aplicaciones de Workspace ONE. La función del modo Workspace ONE no está habilitada para versiones posteriores a la versión 7.2 de Horizon 7, si la versión de Workspace ONE es anterior a la versión 2.9.1.

Configurar la autenticación biométrica

Puede configurar una autenticación biométrica al editar el atributo `pae-ClientConfig` en la base de datos LDAP.

Requisitos previos

Visite el sitio web de Microsoft TechNet si desea obtener información sobre cómo utilizar la utilidad Editor ADSI en su servidor de Windows.

Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión.
- 2 En el cuadro de diálogo Configuración de conexión, seleccione o conéctese a **DC=vdi,DC=vmware,DC=int**.
- 3 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.midominio.com:389**
- 4 En el objeto **CN=Common, OU=Global, OU=Properties**, edite el atributo **pae-ClientConfig** y agregue el valor **BioMetricsTimeout=<integer>**.

Los siguientes valores de `BioMetricsTimeout` son válidos:

Valor <code>BioMetricsTimeout</code>	Descripción
0	La autenticación biométrica no es compatible. Este es el valor predeterminado.
-1	La autenticación biométrica es compatible sin ningún límite de tiempo.
Cualquier entero positivo	La autenticación biométrica es compatible y se puede usar durante el número especificado de minutos.

La nueva configuración se aplica inmediatamente. No es necesario reiniciar el servicio del servidor de conexión ni el dispositivo cliente.

Autenticar usuarios sin solicitar las credenciales

5

Después de que los usuarios inicien sesión en un dispositivo cliente o en VMware Identity Manager, pueden conectarse a una aplicación o a un escritorio publicados sin que se les soliciten las credenciales de Active Directory.

Los administradores pueden seleccionar establecer la configuración según los requisitos de los usuarios.

- Proporcione a los usuarios acceso sin autenticar a las aplicaciones publicadas. Los administradores pueden establecer la configuración de forma que no sea necesario que los usuarios inicien sesión en Horizon Client con las credenciales de Active Directory (AD).
- Use Iniciar sesión como usuario actual para los clientes basados en Windows. En los clientes basados en Windows, los administradores pueden establecer la configuración de forma que los usuarios no necesiten proporcionar credenciales adicionales para iniciar sesión en Horizon Server después de iniciar sesión en un cliente basado en Windows con credenciales de AD.
- Guarde las credenciales en clientes Mac y en dispositivos móviles. Para clientes Mac y móviles, los administradores pueden configurar el servidor de Horizon para guardar las credenciales. Con esta función, no es necesario que los usuarios recuerden las credenciales de AD para SSO (Single Sign-On) después de proporcionarlas una vez en un cliente Mac o móvil.
- Configure True SSO para VMware Identity Manager. En VMware Identity Manager, los administradores pueden configurar True SSO, de forma que los usuarios que se autentican con otro método diferente a las credenciales de AD también puedan iniciar sesión en una aplicación o escritorio publicados sin que se soliciten las credenciales de AD.

Este capítulo incluye los siguientes temas:

- [Proporcionar acceso sin autenticar para las aplicaciones publicadas](#)
- [Configurar usuarios para el inicio de sesión híbrido](#)
- [Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows](#)
- [Guardar credenciales en Horizon Clients que se encuentren en equipos Mac y dispositivos móviles](#)
- [Configurar True SSO](#)

Proporcionar acceso sin autenticar para las aplicaciones publicadas

Los administradores pueden establecer la configuración para que los usuarios sin autenticar accedan a las aplicaciones publicadas desde Horizon Client sin que se les soliciten las credenciales de AD.

Considere configurar el acceso sin autenticar si los usuarios necesitan acceder a una aplicación de conexión directa que tenga su propia seguridad y su propia administración del usuario.

Cuando un usuario inicia una aplicación publicada que está configurada para el acceso sin autenticar, el host RDS crea una sesión de usuario local en las instalaciones y asigna la sesión al usuario.

Para usar esta función se necesita Horizon Client 4.4 o versiones posteriores. Para el cliente HTML Access, esta función requiere la versión 4.5 o posterior.

Flujo de trabajo para configurar usuarios sin autenticar

- 1 Cree usuarios con acceso sin autenticar. Consulte [Crear usuarios con acceso sin autenticar](#).
- 2 Habilite el acceso sin autenticar para los usuarios y establezca un usuario sin autenticar predeterminado. Consulte [Habilitar el acceso sin autenticar para los usuarios](#).
- 3 Autorice a los usuarios sin autenticar para que accedan a las aplicaciones publicadas. Consulte [Autorizar a los usuarios sin autenticar para que accedan a las aplicaciones publicadas](#).
- 4 Habilite el acceso sin autenticar desde Horizon Client. Consulte [Acceso sin autenticar desde Horizon Client](#).

Reglas y directrices para configurar usuarios sin autenticar

- No se admiten la autenticación en dos fases, como RSA y RADIUS, ni la autenticación de tarjeta inteligente para el acceso sin autenticar.
- La autenticación de tarjeta inteligente y el acceso sin autenticar son mutuamente exclusivos. Cuando la autenticación de tarjeta inteligente está configurada como **Requerido** en el servidor de conexión, el acceso sin autenticar está deshabilitado aunque se establezca previamente.
- El acceso sin autenticar no admite VMware Identity Manager ni VMware App Volumes.
- Los protocolos de visualización PCoIP y VMware Blast son compatibles con esta función.
- La función del acceso sin autenticar no verifica la información de la licencia de los hosts RDS. El administrador debe configurar y usar las licencias de los dispositivos.
- La función de acceso sin autenticar no almacena ninguna información específica del usuario. El usuario puede verificar los requisitos de almacenamiento de datos para la aplicación.
- No puede volver a conectarse a las sesiones sin autenticar de aplicaciones. Cuando un usuario se desconecta del cliente, el host RDS cierra la sesión del usuario local de forma automática.
- El acceso sin autenticar solo se admite con las aplicaciones publicadas.

- El acceso sin autenticar no es compatible con un servidor de seguridad ni con un dispositivo Unified Access Gateway.
- Las preferencias de usuario no se guardan en el caso de los usuarios sin autenticar.
- Los escritorios virtuales no admiten usuarios sin autenticar.
- Horizon Administrator muestra un estado de color rojo para el servidor de conexión si este está configurado con un certificado firmado por una CA y habilitado para el acceso sin autenticar, pero no está configurado ningún usuario sin autenticar.
- La función de acceso sin autenticar no funcionará si está deshabilitada la opción de la directiva de grupo AllowSingleSignon del Horizon Agent instalado en un host RDS. Los administradores también pueden controlar si desean habilitar o deshabilitar el acceso sin autenticar con la opción de directiva de grupo UnAuthenticatedAccessEnabled de Horizon Agent. La configuración de directiva de grupo de Horizon Agent se incluye en el archivo de plantilla vdm_agent.admx. Debe reiniciar el host RDS para que se aplique esta directiva.

Crear usuarios con acceso sin autenticar

Los administradores pueden crear usuarios con acceso sin autenticar a las aplicaciones publicadas. Después de que un administrador configure un usuario para que pueda acceder sin autenticar, el usuario puede iniciar sesión en la instancia del servidor de conexión desde Horizon Client únicamente con acceso sin autenticar.

Requisitos previos

- Verifique que el usuario de Active Directory (AD) para el que quiere configurar el acceso sin autenticar tenga un UPN válido. Solo se puede configurar un usuario de AD como un usuario con acceso sin autenticar.

Nota Los administradores solo pueden crear un usuario para cada cuenta de AD. Los administradores no pueden crear grupos de usuarios sin autenticar. Si crea un usuario con acceso sin autenticar y existe una sesión cliente para ese usuario de AD, debe reiniciar la sesión cliente para aplicar estos cambios.

Procedimiento

- 1 En Horizon Administrator, seleccione **Usuarios y grupos**.
- 2 En la pestaña **Acceso sin autenticar**, haga clic en **Agregar**.
- 3 En el asistente **Agregar usuario sin autenticar**, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para encontrar usuarios que cumplan dichos criterios.

El usuario debe tener un UPN válido.
- 4 Seleccione un usuario y haga clic en **Siguiente**.

Repita este paso para agregar varios usuarios.

- 5 (opcional) Introduzca el alias del usuario.

El alias predeterminada del usuario es el nombre de usuario que se configuró para la cuenta de AD. Los usuarios finales pueden usar el alias de usuario para iniciar sesión en la instancia del servidor de conexión desde Horizon Client.

- 6 (opcional) Revise los detalles del usuario y agregue comentarios.

- 7 Haga clic en **Finalizar**.

El servidor de conexión crea al usuario con acceso sin autenticar y muestra los detalles del usuario, entre los que se incluyen el alias, el nombre de usuario, el nombre y el apellido, el nombre de pods de origen, las autorizaciones de aplicaciones y las sesiones. Puede hacer clic en el número de la columna Pods de origen para mostrar la información de los pods.

Pasos siguientes

Habilite el acceso sin autenticar para los usuarios en el servidor de conexión. Consulte [Habilitar el acceso sin autenticar para los usuarios](#).

Habilitar el acceso sin autenticar para los usuarios

Después de crear usuarios con acceso sin autenticar, debe habilitar el acceso sin autenticar en el servidor de conexión para permitir que los usuarios se conecten y accedan a las aplicaciones publicadas.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.

- 2 Haga clic en la pestaña **Servidores de conexión**.

- 3 Seleccione la instancia del servidor de conexión y haga clic en **Editar**.

- 4 Haga clic en la pestaña **Autenticación**.

- 5 Cambie **Acceso sin autenticar** a **Habilitado**.

- 6 En el menú desplegable **Usuario con acceso sin autenticar predeterminado**, seleccione un usuario como el predeterminado.

El usuario predeterminado debe estar presente en el pod local de un entorno de Arquitectura de Cloud Pod. Si selecciona un usuario predeterminado desde un pod diferente, el servidor de conexión crea el usuario en el pod local antes de establecerlo como predeterminado.

- 7 (opcional) Especifique el tiempo de espera predeterminado de la sesión del usuario.

El tiempo de espera predeterminado de la sesión es 10 minutos desde que empieza a estar inactiva.

- 8 Haga clic en **Aceptar**.

Pasos siguientes

Autorice a los usuarios sin autenticar para que accedan a las aplicaciones publicadas. Consulte [Autorizar a los usuarios sin autenticar para que accedan a las aplicaciones publicadas](#).

Autorizar a los usuarios sin autenticar para que accedan a las aplicaciones publicadas

Después de crear un usuario con acceso sin autenticar, debe autorizar al usuario para que acceda a las aplicaciones publicadas.

Requisitos previos

- Cree una granja basada en un grupo de hosts RDS. Consulte "Crear granjas" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Cree un grupo de aplicaciones para las aplicaciones publicadas que se ejecuten en una granja de hosts RDS. Consulte la sección "Crear grupos de aplicaciones" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de aplicaciones** y haga clic en el nombre del grupo de aplicaciones.
- 2 Seleccione **Agregar autorización** en el menú desplegable **Autorizaciones**.
- 3 Haga clic en **Agregar**, seleccione uno o varios criterios, haga clic en **Buscar** y seleccione la casilla **Usuarios sin autenticar** para buscar usuarios con acceso sin autenticar según sus criterios de búsqueda.
- 4 Seleccione los usuarios a los que desea autorizar para acceder a las aplicaciones en el grupo y haga clic en **Aceptar**.
- 5 Haga clic en **Aceptar** para guardar los cambios.

Un icono de acceso sin autenticar aparece junto al usuario con acceso sin autenticar después de que el proceso de autorización se complete.

Pasos siguientes

Use un usuario con acceso sin autenticar para iniciar sesión en Horizon Client. Consulte [Acceso sin autenticar desde Horizon Client](#).

Buscar sesiones con acceso sin autenticar

Utilice Horizon Administrator para enumerar o buscar las sesiones de aplicaciones a las que estén conectados los usuarios con acceso sin autenticar. El icono de usuario con acceso sin autenticar aparece junto a las sesiones que tengan este tipo de usuarios conectados.

Procedimiento

- 1 En Horizon Administrator, seleccione **Supervisión > Sesiones**.
- 2 Haga clic en **Aplicaciones** para buscar sesiones de aplicaciones.

3 Seleccione los criterios e inicie la búsqueda.

Los resultados de la búsqueda incluyen el usuario, el tipo de la sesión (escritorio o aplicación), equipo, grupo o granja, nombre DNS, ID de cliente y la puerta de enlace de seguridad. La hora de inicio de sesión, la duración, el estado y última sesión también aparecen en los resultados.

Eliminar un usuario con acceso sin autenticar

Cuando elimina un usuario con acceso sin autenticar, también debe eliminar las autorizaciones del grupo de aplicaciones del usuario. No puede eliminar el usuario con acceso sin autenticar predeterminado.

Nota Si elimina un usuario con acceso sin autenticar y existe una sesión cliente para ese usuario de AD, debe reiniciar la sesión cliente para aplicar estos cambios.

Procedimiento

- 1 En Horizon Administrator, seleccione **Usuarios y grupos**.
- 2 En la pestaña **Acceso sin autenticar**, haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar**.

Pasos siguientes

Elimine las autorizaciones de las aplicaciones del usuario. Consulte "Eliminar autorizaciones de un grupo de aplicaciones o de escritorios" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Acceso sin autenticar desde Horizon Client

Inicie sesión en Horizon Client con acceso sin autenticar e inicie la aplicación publicada.

Para garantizar una mayor seguridad, el usuario de acceso sin autenticar tiene un alias de usuario que puede utilizar para iniciar sesión en Horizon Client. Cuando selecciona un alias de usuario, no necesita proporcionar las credenciales de AD o el UPN del usuario. Después de iniciar sesión en Horizon Client, puede hacer clic en sus aplicaciones publicadas para iniciar las aplicaciones. Para obtener más información sobre la instalación y configuración de Horizon Clients, consulte la documentación de Horizon Client en la página web [Documentación de VMware Horizon Client](#).

Requisitos previos

- Compruebe que el servidor de conexión de la versión 7.1 de Horizon 7 está configurado para acceso sin autenticar.
- Compruebe que se crearon usuarios de acceso sin autenticar en Horizon Administrator. Si el usuario sin autenticar predeterminado es el único usuario de acceso sin autenticar, Horizon Client se conecta a la instancia del servidor de conexión con el usuario predeterminado.

Procedimiento

- 1 Inicie Horizon Client.

- 2 En Horizon Client, seleccione **Iniciar sesión de forma anónima con Acceso sin autenticar**.
- 3 Conéctese a la instancia del servidor de conexión.
- 4 Seleccione un alias de usuario desde el menú desplegable y haga clic en **Inicio de sesión**.
El usuario predeterminado tiene el sufijo "predeterminado".
- 5 Haga doble clic en una aplicación publicada para iniciar la aplicación.

Configurar la ralentización del inicio de sesión del acceso no autenticado a las aplicaciones publicadas

Como los usuarios no introducen las credenciales cuando usan el acceso sin autenticar, es posible que los hosts RDS se saturen con las solicitudes de aplicaciones publicadas. La ralentización del inicio de sesión calma esta situación. Puede ajustar el nivel de ralentización. También puede bloquear a los clientes que no admitan la ralentización.

Requisitos previos

- Compruebe que tenga habilitado el acceso sin autenticar para los usuarios.
- Verifique que cuente con Horizon Client versión 4.9 o una versión posterior. Si utiliza Horizon Client versión 4.8, se pueden producir errores ocasionales cuando los usuarios inician sesión de forma anónima con el acceso sin autenticar en Horizon 7 versión 7.6, que puede requerir varios reintentos para iniciar sesión.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 Haga clic en la pestaña **Servidores de conexión**.
- 3 Haga clic en la pestaña **Autenticación**.
- 4 En el menú desplegable **Nivel de ralentización de inicio de sesión**, seleccione un nivel de ralentización para los inicios de sesión con acceso sin autenticar.

Opción	Descripción
Bajo	Establece un nivel de ralentización bajo para los inicios de sesión con acceso sin autenticar. Para los navegadores web, como Microsoft Internet Explorer y Microsoft Edge, la recomendación es establecer el nivel bajo de ralentización.
Medio	Establece un nivel de ralentización medio para los inicios de sesión con acceso sin autenticar. Se establece de forma predeterminada. No cambie esta opción si usa Horizon Client versión 4.8.
Alta	Establece un nivel de ralentización alto para los inicios de sesión con acceso sin autenticar. Al establecer un nivel alto de ralentización, esto puede aumentar el tiempo de registro y afectar a la experiencia del usuario final.

- 5 (opcional) Para evitar que los clientes que no admitan la ralentización de inicio de sesión se conecten a Horizon 7 con acceso sin identificar, seleccione **Bloquear clientes no conformes**.

Los Horizon Client anteriores a la versión 4.8 no son compatibles.

6 Haga clic en **Aceptar**.

Pasos siguientes

Inicie sesión en Horizon Client con acceso sin autenticar e inicie la aplicación publicada. Consulte [Acceso sin autenticar desde Horizon Client](#).

Configurar usuarios para el inicio de sesión híbrido

Después de crear un usuario con acceso sin autenticar, puede habilitar el inicio de sesión híbrido para el usuario. Si habilita el inicio de sesión híbrido, los usuarios con acceso sin autenticar pueden acceder a los dominios para obtener recursos de red, como recursos compartidos de archivos o impresoras de red, sin tener que introducir las credenciales.

Nota La función de inicio de sesión híbrido usa el mismo usuario de dominio de todos los usuarios que iniciaron sesión para un usuario con acceso sin autenticar en concreto que está configurado para el inicio de sesión híbrido.

Nota Si utiliza la pestaña del perfil de usuario para establecer el directorio principal como una ruta de red desde la máquina del host RDS, de forma predeterminada, la interfaz administrativa de usuario de Windows elimina todos los permisos existentes del directorio principal y agrega permisos para el administrador y el usuario local con control total. Utilice la cuenta de administrador para eliminar de la lista de permisos el usuario local y, a continuación, agregue el usuario de dominio con los permisos que necesita establecer para el usuario.

Requisitos previos

- Verifique que seleccionó la opción personalizada Inicio de sesión híbrido cuando instaló Horizon Agent en el host RDS. Para obtener más información sobre las opciones de configuración personalizadas de Horizon Agent para un host RDS, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Verifique que creó un usuario con acceso sin autenticar.
- Verifique que el cifrado DES de Kerberos no está habilitado para la cuenta de usuario del dominio. No se admite el cifrado DES de Kerberos para la función de inicio de sesión híbrido.

Procedimiento

- 1 En Horizon Administrator, seleccione **Usuarios y grupos**.
- 2 En la pestaña **Acceso sin autenticar**, haga clic en **Agregar**.
- 3 En el asistente **Agregar usuario sin autenticar**, seleccione un criterio de búsqueda o varios, y haga clic en **Buscar** para encontrar un usuario con acceso sin autenticar que cumpla dichos criterios.
El usuario debe tener un UPN válido.
- 4 Seleccione un usuario con acceso sin autenticar y haga clic en **Siguiente**.
Repita este paso para agregar varios usuarios.

5 (opcional) Introduzca el alias del usuario.

El alias predeterminada del usuario es el nombre de usuario que se configuró para la cuenta de AD. Los usuarios finales pueden usar el alias de usuario para iniciar sesión en la instancia del servidor de conexión desde Horizon Client.

6 (opcional) Revise los detalles del usuario y agregue comentarios.**7** Seleccione **Habilitar inicio de sesión híbrido**.

La opción **Habilitar True SSO** está seleccionada de forma predeterminada. Debe tener True SSO habilitado para el entorno de Horizon 7. A continuación, los usuarios con acceso sin autenticar habilitados para el inicio de sesión híbrido usan True SSO para iniciar sesión en la instancia del servidor de conexión desde Horizon Client.

Nota Si el pod del servidor de conexión no está configurado para True SSO, el usuario puede iniciar una aplicación autorizada con acceso sin autenticar. Sin embargo, el usuario no tiene acceso a la red porque True SSO no está habilitado en el pod.

8 (opcional) Para habilitar que el usuario inicie sesión en la instancia del servidor de conexión desde Horizon Client, seleccione **Habilitar inicio de sesión con contraseña** e introduzca la contraseña del usuario.

Utilice esta opción si no tiene True SSO configurado para el entorno Horizon 7.

En un entorno CPA, la función de inicio de sesión híbrido solo funciona en el pod del servidor de conexión en el que el usuario con inicio de sesión híbrido se configuró con la opción **Habilitar inicio de sesión con contraseña** y se autorizó para utilizar aplicaciones publicadas.

Por ejemplo, en un entorno CPA con un Pod A y un Pod B, el usuario de inicio de sesión híbrido configurado con la opción **Habilitar inicio de sesión híbrido** está autorizado para usar una aplicación en el Pod A. El usuario puede ver e iniciar la aplicación desde un cliente que se conecta a un Pod A o a un Pod B. Sin embargo, si otra aplicación está autorizada al mismo usuario en el Pod B, el usuario no puede ver ni iniciar la aplicación desde un cliente que se conecte al Pod B. Para que la función de inicio de sesión híbrido funcione en el Pod B, debe crear otro usuario con inicio de sesión híbrido configurado con la opción **Habilitar inicio de sesión con contraseña** y autorizar aplicaciones a dicho usuario. Para obtener más información sobre cómo configurar un entorno CPA, consulte el documento *Administrar la arquitectura Cloud Pod en Horizon 7*.

9 Haga clic en **Finalizar**.**Pasos siguientes**

Autorice al usuario para utilizar aplicaciones publicadas. Consulte [Autorizar a los usuarios sin autenticar para que accedan a las aplicaciones publicadas](#).

Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows

Con Horizon Client para Windows, cuando los usuarios seleccionan la casilla **Iniciar sesión como usuario actual**, las credenciales que se proporcionaron al iniciar sesión en el sistema cliente se usan para autenticarse en la instancia del servidor de conexión de Horizon y en el escritorio remoto. No es necesaria otra autenticación del usuario.

Para dar soporte a esta función, las credenciales del usuario se almacenan en la instancia del servidor de conexión y en el sistema cliente.

- En la instancia del servidor de conexión, las credenciales del usuario están cifradas y se almacenan en la sesión del usuario junto al nombre de usuario, dominio y el UPN opcional. Las credenciales se agregan cuando se produce una autenticación y se eliminan cuando el objeto de sesión se destruye. El objeto de sesión se elimina cuando el usuario cierra sesión, se acaba el tiempo de espera de la sesión o se produce un error en la autenticación. El objeto de sesión reside en la memoria volátil y no se almacena en LDAP de Horizon ni en el archivo de disco.
- En el sistema cliente, las credenciales del usuario se cifran y se almacenan en una tabla del paquete de autenticación, que es un componente de Horizon Client. Las credenciales se agregan a la tabla cuando el usuario inicia sesión y se eliminan de la tabla cuando cierra sesión. La tabla se encuentra en una memoria volátil.

Los administradores pueden usar la configuración de la directiva de grupo de Horizon Client para controlar la disponibilidad de la casilla de verificación **Iniciar sesión como usuario actual** y para especificar su valor predeterminado. Los administradores también pueden usar la directiva de grupo para especificar las instancias del servidor de conexión que aceptan la información de la credencial y de la identidad de usuario que se transmite cuando los usuarios seleccionan la casilla **Iniciar sesión como usuario actual** de Horizon Client.

Se habilita la función Desbloqueo recursivo después de que un usuario inicie sesión en el servidor de conexión con la función Iniciar sesión como usuario actual. La función Desbloqueo recursivo desbloquea todas las sesiones remotas después de que lo hiciera el equipo cliente. Los administradores pueden controlar la función Desbloqueo recursivo con la opción de directiva global **Desbloquear sesiones remotas cuando la máquina cliente está desbloqueada** de Horizon Client. Para obtener más información sobre la configuración de directiva global de Horizon Client, consulte la documentación de Horizon Client en la página web [Documentación de VMware Horizon Client](#).

La función Iniciar sesión como usuario actual tiene las siguientes limitaciones y requisitos:

- Cuando la autenticación con tarjeta inteligente se establece como Requerida en una instancia del servidor de conexión, se produce un error en la autenticación de los usuarios que seleccionaron la casilla **Iniciar sesión como usuario actual** cuando se conectan a la instancia del servidor de conexión. Estos usuarios se deben volver a autenticar con la tarjeta inteligente y el PIN cuando inicien sesión en el servidor de conexión.
- La hora del sistema en el que el cliente inicia sesión y la hora del host del servidor de conexión deben estar sincronizadas.

- Si las asignaciones de los derechos del usuario **Tener acceso a este equipo desde la red** se modifican en el sistema cliente, deben modificarse como se describe en el artículo 1025691 de la base de conocimientos de VMware.
- El equipo cliente debe poder comunicarse con el servidor Active Directory corporativo y no debe usar las credenciales almacenadas en caché para la autenticación. Por ejemplo, si los usuarios inician sesión en los equipos cliente desde fuera de la red corporativa, las credenciales almacenadas en caché se utilizan para la autenticación. Si el usuario intenta conectarse a un servidor de seguridad o a una instancia del servidor de conexión sin establecer en primer lugar una conexión VPN, se le solicitan las credenciales y la función Iniciar sesión como usuario actual no funciona.

Guardar credenciales en Horizon Clients que se encuentren en equipos Mac y dispositivos móviles

Los administradores pueden configurar el servidor de conexión para habilitar que los Horizon Clients instalados en equipos Mac y dispositivos móviles recuerden el nombre de usuario, la contraseña y la información del dominio de un usuario.

En Horizon Client para dispositivos móviles, esta función provoca que la casilla de verificación **Guardar contraseña** aparezca en los cuadros de diálogo de inicio de sesión. En Horizon Client para Mac, esta función provoca que la casilla de verificación **Recordar esta contraseña** aparezca en el cuadro de diálogo de inicio de sesión.

Si los usuarios deciden guardar las credenciales, estas se agregan a los campos de inicio de sesión de Horizon Client en las siguientes conexiones.

Para habilitar esta función, debe establecer un valor en el LDAP de View para indicar durante cuánto tiempo desea guardar la información de las credenciales en el cliente. En Horizon Client para Mac, esta función solo se admite en la versión 4.1 o en versiones posteriores.

Nota En Horizon Clients basados en Windows, gracias a la función para iniciar sesión como el usuario actual, los usuarios no tienen que proporcionar las credenciales varias veces.

Configurar un límite de tiempo de espera para guardar las credenciales de Horizon Client

Puede configurar un límite de tiempo de espera que indique durante cuánto tiempo se guardará la información de las credenciales de Horizon Client en sistemas cliente Mac y en dispositivos móviles al configurar un valor en LDAP de View. El límite del tiempo de espera se establece en minutos. Cuando cambia el LDAP de View en una instancia del servidor de conexión, el cambio se propaga a todas las instancias replicadas del servidor de conexión.

Requisitos previos

Visite el sitio web de Microsoft TechNet Web si desea obtener información sobre cómo utilizar la utilidad Editor ADSI en la versión que utilice del sistema operativo de Windows.

Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión.
- 2 En el cuadro de diálogo Configuración de conexión, seleccione o conéctese a **DC=vdi,DC=vmware,DC=int**.
- 3 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.midominio.com:389**
- 4 En el objeto **CN=Common, OU=Global, OU=Properties**, edite el valor del atributo **clientCredentialCacheTimeout**.

Cuando **clientCredentialCacheTimeout** no está establecido o está establecido en **0**, la función está deshabilitada. Para habilitar esta función, puede establecer el número de minutos para guardar la información de las credenciales, o bien establecer un valor **-1**, lo que supone que no existe tiempo de espera.

En el servidor de conexión, la nueva opción se aplicará inmediatamente. No es necesario reiniciar el servicio del servidor de conexión ni el equipo cliente.

Configurar True SSO

Con la función True SSO (Single Sign-On), una vez que los usuarios inicien sesión en VMware Identity Manager con una tarjeta inteligente o con las autenticaciones RADIUS o RSA SecurID, no es necesario que también introduzcan las credenciales de Active Directory para utilizar un escritorio virtual una aplicación o un escritorio publicados.

Si un usuario se autentica con credenciales de Active Directory, la función True SSO no es necesaria, pero puede configurar True SSO para que se utilice incluso en este caso, de forma que las credenciales de AD que el usuario proporcione se ignoren y el usuario True SSO no se utilice.

Cuando se conectan a una aplicación o un escritorio publicados, los usuarios pueden elegir HTML Access o el Horizon Client nativo.

Esta función tiene las siguientes limitaciones:

- No funciona con escritorios virtuales que se proporcionan con el complemento View Agent Direct-Connection.
- Solo se admite en entornos IPv4.

A continuación, aparece una lista de tareas que debe realizar si desea configurar el entorno para True SSO:

- 1 [Determinar una arquitectura para True SSO](#)
- 2 [Configurar una entidad de certificación empresarial](#)
- 3 [Crear plantillas de certificado para usarlas con True SSO](#)
- 4 [Instalar y configurar un servidor de inscripción](#)

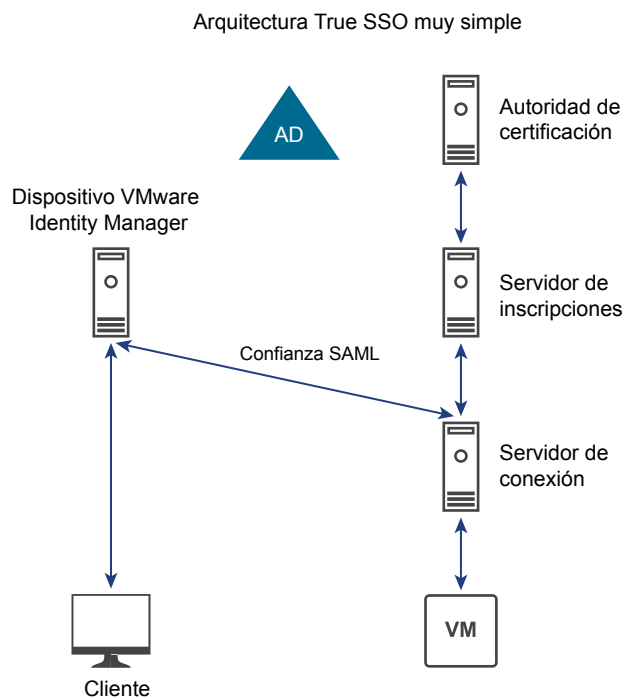
- 5 [Exportar el certificado cliente del servicio de inscripciones](#)
- 6 [Configurar la autenticación SAML para que funcione con True SSO](#)
- 7 [Configurar el servidor de conexión de Horizon para True SSO](#)

Determinar una arquitectura para True SSO

Para usar True SSO, debe tener o agregar una entidad de certificación y crear un servidor de inscripción. Estos dos servidores se comunican para crear el certificado virtual de corta duración de Horizon que habilita un inicio de sesión sin contraseña en Windows. Puede usar True SSO en un dominio único, en un bosque único con varios dominios y en un bosque múltiple, con una configuración de varios dominios.

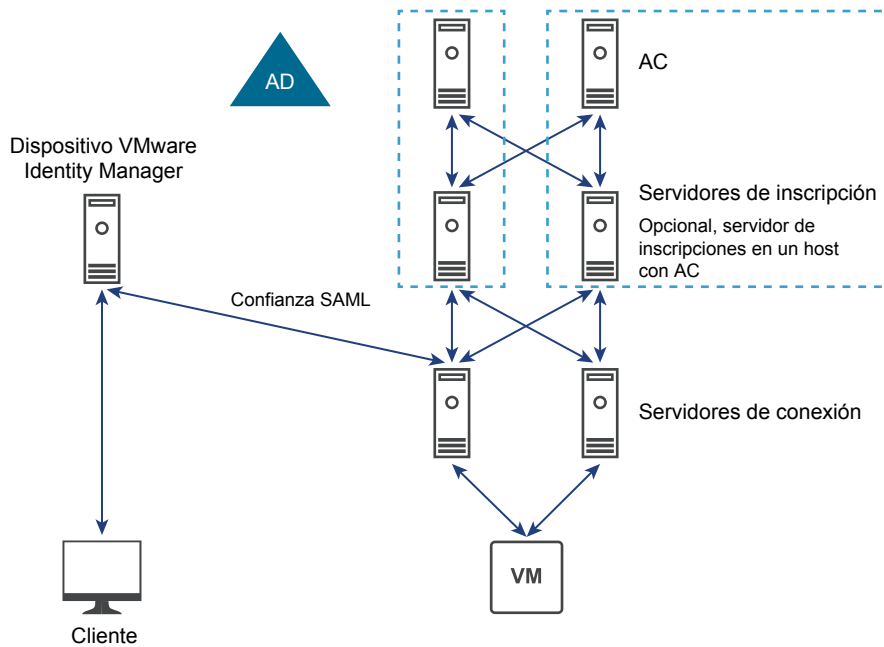
VMware le recomienda tener dos CA y dos servidores de inscripción implementados para usar True SSO. Los siguientes ejemplos muestran True SSO en diferentes arquitecturas.

La siguiente ilustración muestra una arquitectura simple de True SSO.



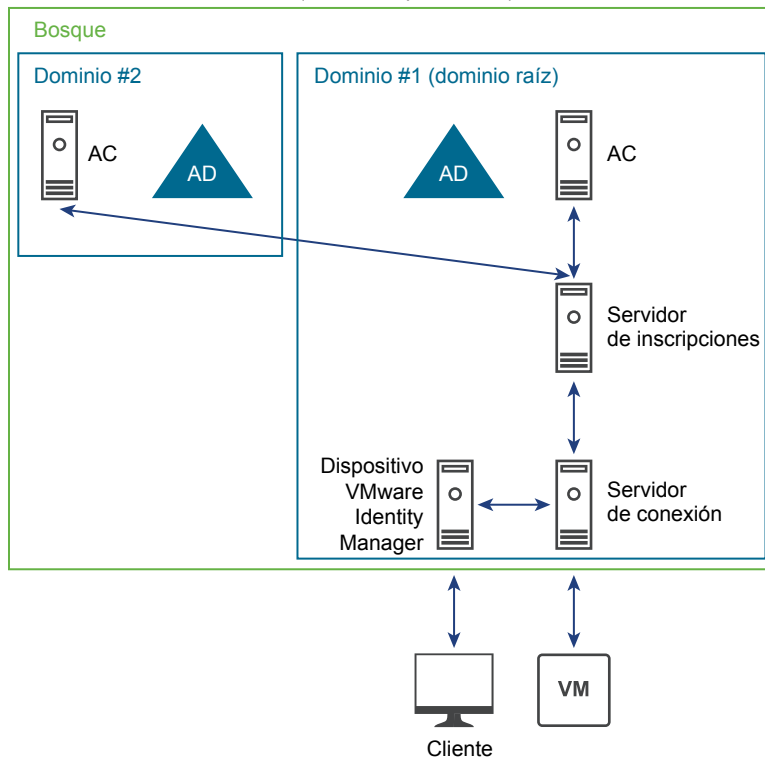
La siguiente ilustración muestra True SSO en una arquitectura de dominio única.

Arquitectura típica de alta disponibilidad True SSO (un solo dominio)

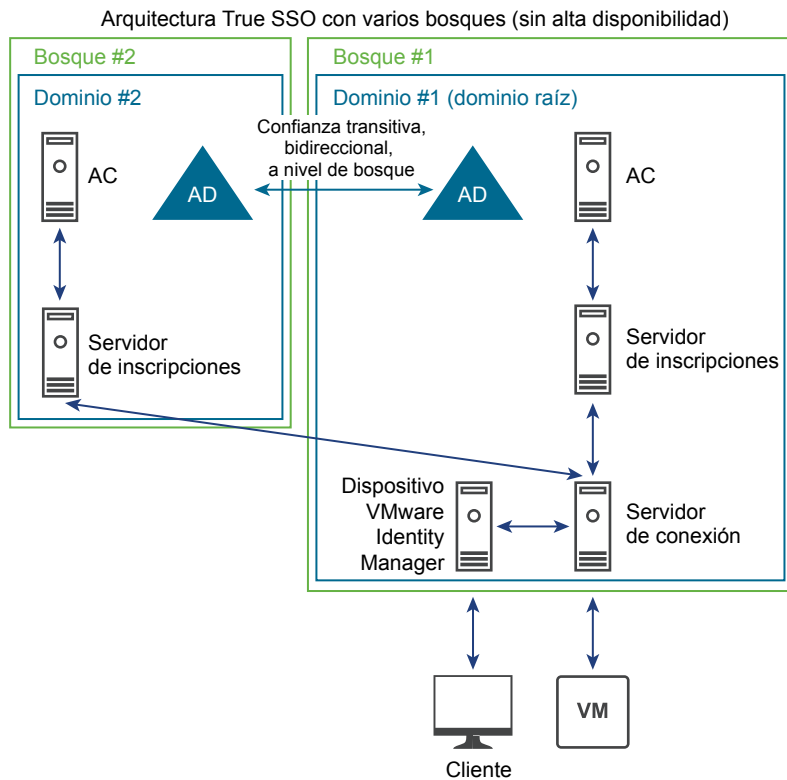


La siguiente ilustración muestra True SSO en una arquitectura de bosque único con varios dominios.

Arquitectura True SSO con un solo bosque y varios dominios (sin alta disponibilidad)



La siguiente ilustración muestra True SSO en una arquitectura de bosques múltiples.



Configurar una entidad de certificación empresarial

Si aún no tiene una entidad de certificación configurada, debe agregar la función Servicios de certificados de Active Directory (AD CS) a un servidor Windows y configurar el servidor para que sea una CA empresarial.

Si ya tiene una CA empresarial establecida, compruebe que esté utilizando la configuración descrita en este procedimiento.

Debe tener al menos una CA empresarial y VMware recomienda que tenga dos para el equilibrio de carga y para los errores por conmutación. El servidor de inscripciones que cree para True SSO se comunica con la CA empresarial. Si configura el servidor de inscripciones para que utilice varias CA empresariales, el servidor de inscripciones se alternará entre las CA que estén disponibles. Si instala el servidor de inscripciones en el mismo equipo que aloja la CA empresarial, puede configurar el servidor de inscripciones para que prefiera usar la CA local. Se recomienda utilizar esta configuración para obtener un mejor rendimiento.

Parte de este procedimiento incluye habilitar el proceso del certificado no persistente. De forma predeterminada, el proceso del certificado incluye el almacenamiento de un registro de cada solicitud del certificado y expide un certificado en la base de datos de CA. Un volumen elevado y constante de solicitudes aumenta la tasa del crecimiento de la base de datos de CA y puede consumir todo el espacio de disco disponible si no se supervisan. Habilitar el proceso del certificado no persistente puede ayudar a reducir la velocidad de crecimiento de la base de datos y la frecuencia de las tareas de administración de la misma.

Requisitos previos

- Cree una máquina virtual Windows Server 2008 R2 o Windows Server 2012 R2.
- Compruebe que la máquina virtual sea parte del dominio de Active Directory para la implementación de Horizon 7.
- Compruebe que esté utilizando un entorno IPv4. En este momento, esta función no se admite en un entorno IPv6.
- Compruebe que el sistema tenga una dirección IP estática.

Procedimiento

- 1 Inicie sesión en el sistema operativo de la máquina virtual como administrador e inicie Server Manager.
- 2 Seleccione la configuración para agregar funciones.

Sistema operativo	Selecciones
Windows Server 2012 R2	<ol style="list-style-type: none"> a Seleccione Agregar roles y características. b En la página Seleccionar tipo de instalación, seleccione Instalación basada en características o en roles. c En la página Seleccionar servidor de destino, seleccione un servidor.
Windows Server 2008 R2	<ol style="list-style-type: none"> a Seleccione Funciones en el árbol de navegación. b Haga clic en Agregar funciones para iniciar el asistente Agregar función.

- 3 En la página Seleccionar funciones de servidor, seleccione **Servicios de certificados de Active Directory**.
- 4 En el asistente Agregar roles y características, haga clic en **Agregar funciones** y deje la casilla **Incluir herramientas de administración** seleccionada.
- 5 En la página Seleccionar características, acepte los valores predeterminados.
- 6 En la página Seleccionar servicios de función, seleccione **Entidad de certificación**.
- 7 Siga los pasos que se le indican y finalice la instalación.
- 8 Cuando se complete la instalación, en la página Progreso de la instalación, haga clic en el vínculo **Configurar Servicios de certificados de Active Directory en el servidor de destino** para abrir el asistente Configuración de AD CS.

- 9 En la página Credenciales, haga clic en **Siguiente** y complete las páginas del asistente Configuración AD CS como se describe en la siguiente tabla.

Opción	Acción
Servicios de función	Seleccione Entidad de certificación y haga clic en Siguiente (en lugar de Configurar).
Tipo de instalación	Seleccione CA empresarial .
Tipo de CA	Seleccione CA raíz o CA subordinada . Algunas empresas prefieren una implementación PKI de dos niveles. Si desea obtener más información, consulte el documento http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx .
Clave privada	Seleccione Crear una nueva clave privada .
Criptografía de CA	Para un algoritmo hash, puede seleccionar SHA1 , SHA256 , SHA384 o SHA512 . Para la longitud de la clave, puede seleccionar 1024 , 2048 , 3072 o 4096 . VMware recomienda un mínimo de SHA256 y una clave 2048.
Nombre de CA	Acepte el nombre predeterminado o cámbielo.
Periodo de validez	Acepte el valor predeterminado de 5 años.
Base de datos del certificado	Acepte los valores predeterminados.

- 10 En la página Confirmación, haga clic en **Configurar** y cuando el asistente informe sobre una configuración correcta, ciérrelo.
- 11 Abra una ventana de símbolo de sistema e introduzca el siguiente comando para configurar la CA del proceso del certificado no persistente:

```
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

- 12 Introduzca el siguiente comando para ignorar los errores de la CRL (lista de revocación de certificados) sin conexión de la CA:

```
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

Esta marca es obligatoria ya que el certificado raíz que True SSO utiliza suele estar sin conexión y, por lo tanto, se producirá un error en la comprobación de la revocación, comportamiento que es el esperado.

- 13 Introduzca los siguientes comandos para reiniciar el servicio:

```
sc stop certsvc
sc start certsvc
```

Pasos siguientes

Cree una plantilla de certificado. Consulte [Crear plantillas de certificado para usarlas con True SSO](#).

Crear plantillas de certificado para usarlas con True SSO

Debe crear una plantilla de certificado que se pueda usar para expedir certificados de corta duración y debe especificar los equipos del dominio que pueden solicitar este tipo de certificado.

Se puede crear más de una plantilla de certificado. Solo puede configurar una plantilla por dominio, pero puede compartir la plantilla en varios. Por ejemplo, si tiene un bosque de Active Directory con tres dominios y quiere usar True SSO en esos tres dominios, puede seleccionar si desea configurar una, dos o tres plantillas. Todos los dominios pueden compartir la misma plantilla, o bien puede tener diferentes plantillas para cada dominio.

Requisitos previos

- Compruebe que tenga una CA empresarial para crear la plantilla descrita en este procedimiento. Consulte [Configurar una entidad de certificación empresarial](#).
- Compruebe que preparara Active Directory para la autenticación de tarjeta inteligente. Para obtener más información, consulte el documento *Instalación de Horizon 7*.
- Cree un grupo de seguridad en el dominio y en el bosque para los servidores de inscripción y agregue a ese grupo las cuentas de los equipos de los servidores de inscripción.

Procedimiento

- 1 Para configurar True SSO, en el equipo que está utilizando para la entidad de certificación, inicie sesión en el sistema operativo como un administrador y diríjase a **Herramientas administrativas > Entidad de certificación**.
 - a Expanda el árbol que se encuentra en el panel de la izquierda, haga clic con el botón secundario en **Plantillas de certificado** y seleccione **Administrar**.
 - b Haga clic con el botón secundario en la plantilla **Inicio de sesión de tarjeta inteligente** y seleccione **Duplicar**.

c Realice los siguientes cambios en estas pestañas:

Pestaña	Acción
Pestaña Compatibilidad	<ul style="list-style-type: none"> ■ En Entidad de certificación, seleccione Windows Server 2008 R2. ■ En Destinatario del certificado, seleccione Windows 7/Windows Server 2008 R2.
Pestaña General	<ul style="list-style-type: none"> ■ Cambie el nombre para mostrar de la plantilla a True SS0. ■ Cambie el periodo de validez a un periodo que sea tan amplio como una jornada laboral; es decir, tan amplio como el periodo durante el cual es probable que el usuario tenga la sesión iniciada en el sistema. <p>Para que el usuario no pierda el acceso a los recursos de la red mientras tiene la sesión iniciada, el periodo de validez debe ser superior al tiempo de renovación TGT de Kerberos en el dominio de los usuarios.</p> <p>(La duración máxima predeterminada del ticket es 10 horas. Para encontrar la directiva predeterminada del dominio, puede dirigirse a Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas de cuenta > Directiva Kerberos: Vigencia máxima del vale de usuario.)</p> <ul style="list-style-type: none"> ■ Cambie el periodo de renovación del 50 % al 75 % del periodo de validez.
Pestaña Tratamiento de la solicitud	<ul style="list-style-type: none"> ■ En Propósito, seleccione Firma e inicio de sesión mediante tarjeta inteligente. ■ Seleccione Para renovar automáticamente las tarjetas inteligentes, ...
Pestaña Criptografía	<ul style="list-style-type: none"> ■ En Categoría del proveedor, seleccione Proveedor de almacenamiento de claves. ■ En Nombre de algoritmo, seleccione RSA.
Pestaña Servidor	<p>Seleccione No almacenar certificados y solicitudes en la base de datos de CA.</p> <p>Importante Asegúrese de que la opción No incluir información de revocación en los certificados emitidos no esté seleccionada. (Este cuadro se selecciona cuando selecciona el primero y tiene que desmarcarlo).</p>
Pestaña Requisitos de emisión	<ul style="list-style-type: none"> ■ Seleccione Este nombre de firmas autorizadas y escriba 1 en el cuadro. ■ En Tipo de directiva, seleccione Directiva de aplicación y establezca la directiva en Agente de solicitud de certificados. ■ En Requiere lo siguiente para volver a hacer la inscripción, seleccione Certificado existente válido.
Pestaña Seguridad	<p>En el grupo de seguridad que creó para las cuentas del equipo del servidor de inscripción, como se describe en los requisitos, proporcione los siguientes permisos: Lectura, Inscripción</p> <ol style="list-style-type: none"> 1 Haga clic en Agregar. 2 Especifique qué equipos desea permitir que inscriban certificados. 3 Para estos equipos, seleccione las casillas de verificación apropiadas para proporcionar a los equipos los siguientes permisos: Lectura, Inscripción.

d Haga clic en **Aceptar** en el cuadro de diálogo Propiedades de plantilla nueva.

e Cierre la ventana Consola de plantillas de certificado.

- f Haga clic con el botón secundario en **Plantillas de certificado** y seleccione **Nuevo > Plantilla de certificado que se va a emitir**.

Nota Este paso es obligatorio para todas las entidades de certificación que expiden certificados basados en esta plantilla.

- g En la ventana Habilitar plantillas de certificados, seleccione la plantilla que acaba de crear (por ejemplo, **Plantilla True SSO**) y haga clic en **Aceptar**.
- 2** Para configurar Agente de inscripción (equipo), en el equipo que está utilizando para la entidad de certificación, inicie sesión en el sistema operativo como administrador y diríjase a **Herramientas administrativas > Entidad de certificación**.
- a Expanda el árbol que se encuentra en el panel de la izquierda, haga clic con el botón secundario en **Plantillas de certificado** y seleccione **Administrar**.
 - b Busque y abra la plantilla Agente de inscripción (equipo) y, a continuación, realice el siguiente cambio en la pestaña **Seguridad**:

En el grupo de seguridad que creó para las cuentas del equipo del servidor de inscripción, como se describe en los requisitos, proporcione los siguientes permisos: Lectura, Inscripción
 - 1 Haga clic en **Agregar**.
 - 2 Especifique qué equipos desea permitir que inscriban certificados.
 - 3 Para estos equipos, seleccione las casillas de verificación apropiadas para proporcionar a los equipos los siguientes permisos: Lectura, Inscripción.
 - c Haga clic con el botón secundario en **Plantillas de certificado** y seleccione **Nuevo > Plantilla de certificado que se va a emitir**.

Nota Este paso es obligatorio para todas las entidades de certificación que expiden certificados basados en esta plantilla.

- d En la ventana Habilitar plantillas de certificados, seleccione **Agente de inscripción (equipo)** y haga clic en **Aceptar**.

Pasos siguientes

Cree un servicio de inscripción. Consulte [Instalar y configurar un servidor de inscripción](#).

Instalar y configurar un servidor de inscripción

Ejecute el instalador del servidor de conexión y seleccione la opción Servidor de inscripciones de Horizon 7 para instalar un servidor de inscripciones. El servidor de inscripciones solicita certificados de corta duración en nombre de los usuarios que especifique. Estos certificados de corta duración son el mecanismo que True SSO usa para la autenticación, evitando solicitar a los usuarios credenciales de Active Directory.

Debe instalar y configurar al menos un servidor de inscripciones y este servidor no puede estar instalado en el mismo host que el servidor de conexión de View. VMware recomienda que tenga dos servidores de inscripciones para la conmutación por error y el equilibrio de carga. Si tiene dos servidores de inscripciones, de forma predeterminada, uno es el preferido y el otro se usa para la conmutación por error. Sin embargo, puede cambiar este valor para que el servidor de conexión envíe de forma alterna las solicitudes de certificado a ambos servidores de inscripciones.

Si instala el servidor de inscripciones en el mismo equipo que aloja la CA empresarial, puede configurar el servidor de inscripciones para que prefiera usar la CA local. Para obtener un rendimiento óptimo, VMware recomienda combinar la configuración para preferir usar la CA local con la configuración para equilibrar la carga de los servidores de inscripciones. Como resultado, cuando llegan solicitudes de certificado, el servidor de conexión usará servidores de inscripciones y cada servidor atenderá a las solicitudes con la CA local. Para obtener más información sobre las opciones de configuración, consulte [Opciones de configuración del servidor de inscripción](#) y [Opciones de configuración del servidor de conexión](#).

Requisitos previos

- Cree una máquina virtual Windows Server 2008 R2, Windows Server 2012 R2 o Windows Server 2016 con, al menos, 4 GB de memoria, o bien use la máquina virtual que aloja la CA empresarial. No use una máquina que sea un controlador de dominio.
- Verifique que ningún otro componente de View, incluidos el servidor de conexión de View, View Composer, el servidor de seguridad, Horizon Client o bien View Agent u Horizon Agent estén instalados en la máquina virtual.
- Compruebe que la máquina virtual sea parte del dominio de Active Directory para la implementación de Horizon 7.
- Compruebe que esté utilizando un entorno IPv4. En este momento esta función no se admite en un entorno IPv6.
- VMware recomienda que el sistema tenga una dirección IP estática.
- Verifique que pueda iniciar sesión en el sistema operativo como un usuario de dominio con privilegios Administrador. Debe iniciar sesión como un administrador para ejecutar el instalador.

Procedimiento

- 1 En el equipo en el que piense usar el servidor de inscripciones, agregue el complemento Certificados a MMC:
 - a Abra la consola MMC y seleccione **Archivo > Agregar o quitar complemento**
 - b En **Complementos disponibles**, seleccione **Certificados** y haga clic en **Agregar**.
 - c En la ventana Complemento Certificados, seleccione **Cuenta de equipo**, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
 - d En la ventana Agregar o quitar complementos, haga clic en **Aceptar**.

2 Expedir un certificado agente de inscripciones:

- En la consola de certificados, expanda el árbol raíz de la consola, haga clic con el botón secundario en la carpeta **Personal** y seleccione **Todas las tareas > Solicitar un nuevo certificado**.
- En el asistente Inscripción de certificados, acepte los valores predeterminados hasta llegar a la página Solicitar certificados.
- En la página Solicitar certificados, seleccione la casilla de verificación **Agente de inscripción (PC)** y haga clic en **Inscribir**.
- Acepte los valores predeterminados en las otras páginas del asistente y haga clic en **Finalizar** en la última página.

En la consola de MMC, si expande la carpeta **Personal** y selecciona **Certificados** en el panel de la izquierda, verá un nuevo certificado en el panel de la derecha.

3 Instale el servidor de inscripciones:

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

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

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.

- Haga doble clic en el archivo instalador para iniciar el asistente y siga las instrucciones hasta llegar a la página Opciones de instalación.
- En la página Opciones de instalación, seleccione **Servidor de inscripciones de Horizon 7**, elija un modo de autenticación para la instancia del servidor de inscripción y haga clic en **Siguiente**.

Opción	Descripción
Horizon 7	Configura el modo de autenticación para un entorno Horizon 7.
Horizon Cloud	Configura el modo de autenticación para un entorno Horizon Cloud.

- Siga los pasos que se le indican para finalizar la instalación.

Debe habilitar las conexiones entrantes en el Puerto 32111 (TCP) para que funcionen el servidor de inscripciones. El instalador abre el puerto de forma predeterminada durante la instalación.

Pasos siguientes

- Si instaló el servidor de inscripciones en el mismo equipo que aloja una CA empresarial, configure el servidor de inscripciones para que prefiera usar la CA local. Consulte [Opciones de configuración del servidor de inscripción](#). De forma opcional, si instala y configura más de un servidor de inscripciones, puede configurar los servidores de conexión para habilitar el equilibrio de carga entre los servidores de inscripciones. Consulte [Opciones de configuración del servidor de conexión](#).

- Empareje los servidores de conexión con los servidores de inscripciones. Consulte [Exportar el certificado cliente del servicio de inscripciones](#).

Exportar el certificado cliente del servicio de inscripciones

Para cumplir el emparejamiento, puede usar el complemento Certificados de MMC para exportar el certificado cliente del servicio de inscripciones autofirmado y generado automáticamente desde un servidor de conexión del clúster. Este certificado se denomina certificado cliente porque el servidor de conexión es un cliente del servicio de inscripciones proporcionado por el servidor de inscripciones.

El servicio de inscripciones debe confiar en el servidor de conexión de VMware Horizon cuando solicite que los servidores de inscripción expidan los certificados de corta duración para los usuarios Active Directory. Por ello, los pods o los clústeres del servidor de conexión de VMware Horizon deben emparejarse con los servidores de inscripciones.

El certificado cliente del servicio de inscripciones se crea automáticamente cuando un servidor de conexión de Horizon 7 o una versión posterior se instala y se inicia el servicio del servidor de conexión de VMware Horizon. El certificado se distribuye a través de LDAP de View a otros servidores de conexión de Horizon 7 que se agregarán posteriormente al clúster. El certificado se almacena entonces en un contenedor personalizado (VMware Horizon View Certificates\Certificates) en el almacén de certificados de Windows del equipo.

Requisitos previos

Verifique que tenga instalado Horizon 7 o un servidor de conexión posterior. Para obtener instrucciones de instalación, consulte *Instalación de Horizon 7*. Para obtener instrucciones de actualización, consulte *Actualizaciones de Horizon 7*.

Importante Los clientes pueden usar sus propios certificados para el emparejamiento, en lugar de usar el certificado autogenerado creado por el servidor de conexión. Para ello, coloque el certificado preferido (y la clave privada asociada) en el contenedor personalizado (VMware Horizon View Certificates\Certificates) en el almacén de certificados de Windows de la máquina del servidor de conexión. A continuación, tiene que establecer el nombre descriptivo del certificado en **vdm.ec.new** y volver a iniciar el servidor. Los otros servidores del clúster recuperarán dicho certificado del LDAP. Puede entonces realizar los pasos de este procedimiento.

Procedimiento

- 1 En uno de los equipos del servidor de conexión del clúster, agregue el complemento Certificados en MMC:
 - a Abra la consola MMC y seleccione **Archivo > Agregar o quitar complemento**
 - b En **Complementos disponibles**, seleccione **Certificados** y haga clic en **Agregar**.
 - c En la ventana Complemento Certificados, seleccione **Cuenta de equipo**, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
 - d En la ventana Agregar o quitar complementos, haga clic en **Aceptar**.

- 2 En la consola MMC, en el panel izquierdo, amplíe la carpeta **Certificados de VMware Horizon View** y seleccione la carpeta **Certificados**.
- 3 En el panel derecho, haga clic con el botón secundario en el archivo del certificado con el nombre descriptivo **vdm.ec** y seleccione **Todas las tareas > Exportar**.
- 4 En el asistente de exportación del certificado, acepte los valores predeterminados, que incluye dejar el botón de radio **No exportar la clave privada** seleccionado.
- 5 Cuando se le solicite asignar un nombre al archivo, escriba un nombre como **EnrollClient** para el certificado cliente del servicio de inscripciones y siga las ventanas para finalizar la exportación del certificado.

Pasos siguientes

Importe el certificado en el servidor de inscripción. Consulte [Importar el certificado cliente del servicio de inscripciones en el servidor de inscripciones](#).

Importar el certificado cliente del servicio de inscripciones en el servidor de inscripciones

Para completar el proceso de emparejamiento, utilice el Complemento Certificados de MMC para importar el certificado cliente del servicio de inscripciones en el servidor de inscripciones. Tiene que realizar este procedimiento en cada servidor de inscripciones.

Requisitos previos

- Compruebe que el servidor de inscripciones tenga instalado Horizon 7 o una versión posterior. Consulte [Instalar y configurar un servidor de inscripción](#).
- Compruebe que el certificado que desea importar sea el correcto. Puede utilizar su propio certificado o el certificado cliente del servicio de inscripciones autofirmado que se genere de forma automática desde un servidor de conexión en el clúster, como se describe en [Exportar el certificado cliente del servicio de inscripciones](#).

Importante Si quiere utilizar sus propios certificados para el emparejamiento, coloque el certificado preferido (y la clave privada asociada) en el contenedor personalizado (VMware Horizon View Certificates\Certificates) en el almacén de certificados de Windows de la máquina del servidor de conexión. A continuación, tiene que establecer el nombre descriptivo del certificado en **vdm.ec.new** y volver a iniciar el servidor. Los otros servidores del clúster recuperarán dicho certificado del LDAP. Puede entonces realizar los pasos de este procedimiento.

Si tiene su propio certificado cliente, el certificado que debe copiar al servidor de inscripciones es el certificado raíz que se utilizó para generar el certificado cliente.

Procedimiento

- 1 Copie el archivo del certificado adecuado para la máquina del servidor de inscripciones.
Para utilizar el certificado generado de forma automática, copie el certificado cliente del servicio de inscripciones del servidor de conexión. Para utilizar su propio certificado, copie el certificado raíz que se utilizó para generar el certificado cliente.
- 2 En el servidor de inscripciones, agregue el Complemento Certificados a MMC.
 - a Abra la consola MMC y seleccione **Archivo > Agregar o quitar complemento**
 - b En **Complementos disponibles**, seleccione **Certificados** y haga clic en **Agregar**.
 - c En la ventana Complemento Certificados, seleccione **Cuenta de equipo**, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
 - d En la ventana Agregar o quitar complementos, haga clic en **Aceptar**.
- 3 En la consola MMC, en el panel izquierdo, haga clic con el botón secundario en la carpeta **Raíces de confianza del servidor de inscripciones de VMware Horizon View** y seleccione **Todas las tareas > Importar**.
- 4 En el asistente para Importar el certificado, siga los pasos que se le indican para explorar y abrir el archivo del certificado **InscribirCliente**.
- 5 Siga los pasos que se le indican y acepte los valores predeterminados para completar la importación del certificado.
- 6 Haga clic con el botón secundario en el certificado importado y agregue un nombre descriptivo como por ejemplo **vdm.ec** (para el certificado cliente de inscripción).

VMware recomienda que utilice un nombre descriptivo que identifique el clúster de Horizon 7, pero también puede utilizar cualquier otro nombre que le ayude a identificar el certificado cliente con facilidad.

Pasos siguientes

Configure el autenticador SAML que se utilizó para delegar la autenticación en VMware Identity Manager. Consulte [Configurar la autenticación SAML para que funcione con True SSO](#).

Configurar la autenticación SAML para que funcione con True SSO

Gracias a la función True SSO que se introdujo en Horizon 7, los usuarios pueden iniciar sesión en VMware Identity Manager 2.6 y en versiones posteriores con la autenticación RSA SecurID, RADIUS y con tarjeta inteligente, y no se les solicitará las credenciales de Active Directory, aunque inicien una aplicación o un escritorio remoto por primera vez.

Con versiones anteriores, SSO (Single Sign-On) funcionaba solicitando a los usuarios las credenciales de Active Directory la primera vez que iniciaban un escritorio remoto o una aplicación publicada si no se autenticaron previamente con las credenciales de Active Directory. Las credenciales se almacenaron en caché, por lo que no es necesario que los usuarios vuelvan a introducir sus credenciales en los inicios posteriores. Con True SSO, se crean certificados de corta duración y se usan en lugar de las credenciales de AD.

Aunque el proceso para configurar la autenticación SAML para VMware Identity Manager no cambió, se agregó un paso adicional para True SSO. Debe configurar VMware Identity Manager para que se eliminen las ventanas emergentes de contraseña.

Nota Si la implementación incluye más de una instancia del servidor de conexión, el autenticador SAML se debe asociar a cada una de ellas.

Requisitos previos

- Verifique que Single Sign-On está habilitado en la configuración global. En Horizon Administrator, seleccione **Configuración > Configuración global** y compruebe que **Configurar Single Sign-On (SSO)** esté establecido como **Habilitado**.
- Compruebe que VMware Identity Manager esté instalado y configurado. Consulte la documentación de VMware Identity Manager, disponible en <https://docs.vmware.com/es/VMware-Identity-Manager/index.html>
- Verifique que el certificado raíz de la autoridad de certificación que firma el certificado del servidor SAML esté instalado en el host del servidor de conexión. VMware no recomienda configurar los autenticadores SAML para utilizar certificados autofirmados. Consulte el tema "Importar un certificado raíz e intermedios al almacén de certificados de Windows" en el capítulo "Configurar certificados SSL de los servidores de Horizon 7" del documento *Instalación de Horizon 7*.
- Anote el FQDN de la instancia del servidor de VMware Identity Manager.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor para asociarla al autenticador SAML y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, del menú desplegable **Delegación de la autenticación a VMware Horizon (autenticador SAML 2.0)**, seleccione **Permitido** o **Requerido**.

Cada una de las instancias del servidor de conexión de la implementación se puede configurar con distintos valores de autenticación SAML, de acuerdo a las necesidades.

- 4 Haga clic en **Administrar autenticadores SAML** y en **Agregar**.

5 Configure el autenticador SAML en el cuadro de diálogo Agregar autenticador SAML 2.0.

Opción	Descripción
Etiqueta	Puede usar el FQDN de la instancia del servidor de VMware Identity Manager.
Descripción	(Opcional) Puede usar el FQDN de la instancia del servidor de VMware Identity Manager.
URL de metadatos	URL para recuperar toda la información necesaria para intercambiar la información SAML entre el proveedor de identidad SAML y la instancia del servidor de conexión de Horizon. En la URL <code>https://<NOMBRE DEL HORIZON SERVER>/SAAS/API/1.0/GET/metadata/idp.xml</code> , haga clic en <NOMBRE DEL SERVIDOR HORIZON> y reemplace el FQDN de la instancia del servidor de VMware Identity Manager.
URL de administración	URL para acceder a la consola de administración del proveedor de identidades SAML (instancia de VMware Identity Manager). Esta URL tiene el formato <code>https://<Identity-Manager-FQDN>:8443</code> .

6 Haga clic en **Aceptar** para guardar la configuración del autenticador SAML.

Si se proporcionó información válida, se debe aceptar el certificado autofirmado (no se recomienda) o utilizar un certificado de confianza para Horizon 7 y VMware Identity Manager.

El menú desplegable **Autenticadores SAML 2.0** muestra el autenticador creado recientemente, configurado como el seleccionado.

7 En la sección Estado del sistema del panel de información de Horizon Administrator, seleccione **Otros componentes > Autenticadores SAML 2.0**, seleccione el autenticador SAML agregado y verifique los detalles.

Si la configuración es correcta, el estado del autenticador se mostrará en verde. El estado del autenticador puede estar en rojo si no se confía en el certificado, si el servicio de VMware Identity Manager no está disponible o si la URL de metadatos no es válida. Si no se confía en el certificado, es posible que se pueda hacer clic en **Verificar** para validar y aceptar el certificado.

8 Inicie sesión en la consola de administración de VMware Identity Manager, diríjase a la página Grupos de View y seleccione la casilla de verificación **Suprimir el elemento emergente de contraseña**.

Pasos siguientes

- Amplíe el período de caducidad de los metadatos del servidor de conexión para que las sesiones remotas no finalicen después de solo 24 horas. Consulte [Cambiar el período de caducidad de los metadatos del proveedor de servicios en el servidor de conexión](#).
- Use la interfaz de línea de comandos `vdmutil` para configurar True SSO en un servidor de conexión. Consulte [Configurar el servidor de conexión de Horizon para True SSO](#).

Para obtener más información sobre cómo funciona la autenticación SAML, consulte [Uso de la autenticación SAML](#).

Configurar el servidor de conexión de Horizon para True SSO

Puede usar la interfaz de línea de comandos de `vdmutil` para configurar y habilitar o deshabilitar True SSO.

Es necesario realizar este procedimiento en un solo servidor de conexión del clúster.

Importante Este procedimiento usa únicamente los comandos necesarios para habilitar True SSO. Para obtener una lista de todas las opciones de configuración disponibles para administrar las opciones de True SSO y una descripción de cada opción, consulte [Referencia de la línea de comandos para configurar True SSO](#).

Requisitos previos

- Verifique que puede ejecutar el comando como un usuario con la función Administradores. Horizon Administrator permite asignar la función de administradores a un usuario. Consulte [Capítulo 6 Configurar la administración delegada basada en funciones](#).
- Verifique que tiene el nombre de dominio completo (FQDN) de los siguientes servidores:
 - Servidor de conexión
 - Servidor de inscripciones

Si desea obtener más información, consulte [Instalar y configurar un servidor de inscripción](#).
 - Entidad de certificación empresarial

Si desea obtener más información, consulte [Configurar una entidad de certificación empresarial](#).
- Compruebe que cuenta con el nombre Netbios o el FQDN del dominio.
- Compruebe que creó una plantilla de certificado. Consulte [Crear plantillas de certificado para usarlas con True SSO](#).
- Compruebe que creó un autenticador SAML para delegar la autenticación a VMware Identity Manager. Consulte [Configurar la autenticación SAML para que funcione con True SSO](#).

Procedimiento

- 1 En un servidor de conexión del clúster, abra una ventana de símbolo de sistema e introduzca el comando para agregar un servidor de inscripciones.

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-dominio --authPassword
contraseña-usuario-administrador --trueoso --environment --add --enrollmentServer fqdn-servidor-
inscripción
```

El servidor de inscripción se agrega a la lista global.

- 2 Introduzca el comando para que aparezca la información de ese servidor de inscripción.

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-dominio --authPassword contraseña-usuario-administrador --truessso --environment --list --enrollmentServer fqdn-servidor-inscripción --domain fqdn-dominio
```

El resultado muestra el nombre del bosque, si el certificado del servidor de inscripción es válido, el nombre y los detalles de la plantilla del certificado que puede usar y el nombre común de la entidad de certificación. Para configurar los dominios a los que el servidor de inscripción puede conectarse, puede usar una opción de Registro de Windows en el servidor de inscripción. El valor predeterminado es conectarse a todos los dominios de confianza.

Importante Se le solicitará que especifique el nombre común de la entidad de certificación en el siguiente paso.

- 3 Introduzca un comando para crear un conector True SSO, que contendrá la información de la configuración y habilite el conector.

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-dominio --authPassword contraseña-usuario-administrador --truessso --create --connector --domain fqdn-dominio --template nombre-plantilla-TrueSSO --primaryEnrollmentServer fqdn-servidor-inscripción --certificateServer nombre-común-ca --mode enabled
```

En este comando, *nombre-plantilla-TrueSSO* es el nombre de la plantilla que aparece en el resultado del paso anterior y *nombre-común-ca* es el nombre común de la entidad de certificación empresarial que aparece en ese resultado.

El conector True SSO está habilitado en un grupo o clúster del dominio especificado. Para deshabilitar True SSO en el nivel de grupos, ejecute `vdmUtil --certsso --edit --connector <domain> --mode disabled`. Para deshabilitar True SSO en una máquina virtual individual, puede usar GPO (`vdm_agent.adm`).

- 4 Introduzca el comando para ver los autenticadores SAML disponibles.

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-dominio --authPassword contraseña-usuario-administrador --truessso --list --authenticator
```

Los autenticadores se crean cuando configura la autenticación SAML entre VMware Identity Manager y un servidor de conexión, usando Horizon Administrator.

Los resultados muestran el nombre del autenticador y también si True SSO está habilitado.

Importante Se le solicitará que especifique el nombre del autenticador en el siguiente paso.

- 5 Introduzca el comando para habilitar el uso del autenticador en modo True SSO.

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-dominio --authPassword contraseña-usuario-administrador --truessso --authenticator --edit --name fqdn-autenticador --truesssoMode {ENABLED|ALWAYS}
```

Para `--trueSSOMode`, use `ENABLED` si desea que se use True SSO únicamente si no se proporcionó ninguna contraseña cuando el usuario inició sesión en VMware Identity Manager. En este caso, si una contraseña se usó y se almacenó en caché, el sistema usará la contraseña. Configure `--trueSSOMode` como `ALWAYS` si desea que se use True SSO aunque no se proporcionara ninguna contraseña cuando el usuario inició sesión en VMware Identity Manager.

Pasos siguientes

En Horizon Administrator, verifique el estado de la configuración True SSO. Si desea obtener más información, consulte [Uso del panel de control del estado del sistema para solucionar problemas relacionados con True SSO](#).

Para configurar las opciones avanzadas, use la configuración avanzada de Windows en el sistema apropiado. Consulte [Opciones de configuración avanzadas para True SSO](#).

Referencia de la línea de comandos para configurar True SSO

Puede usar la interfaz de línea de comandos `vdmutil` para configurar y administrar la función True SSO.

Ubicación de la utilidad

De forma predeterminada, la ruta del archivo ejecutable de comandos `vdmutil` es `C:\Program Files\VMware\VMware View\Server\tools\bin`. Si desea evitar introducir la ruta en la línea de comando, agréguela a la variable de entorno `PATH`.

Sintaxis y autenticación

Use el siguiente formato del comando de `vdmutil` en una ventana de símbolo de sistema de Windows.

```
vdmutil opciones de autenticación --trueSSO argumentos y opciones adicionales
```

Las opciones adicionales que puede usar dependen de la opción del comando. Este tema se centra en las opciones para configurar True SSO (`--trueSSO`). A continuación, aparece un ejemplo de un comando para enumerar conectores que se configuraron para True SSO:

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-dominio --authPassword contraseña-usuario-administrador --trueSSO --list --connector
```

El comando `vdmutil` incluye opciones de autenticación para especificar el nombre de usuario, el dominio y la contraseña que se deben usar en la autenticación.

Tabla 5-1. Opciones de autenticación del comando vdmutil

Opción	Descripción
<code>--authAs</code>	Nombre de un usuario administrador de Horizon 7. No use <i>dominio\nombredeusuario</i> ni el formato de nombre principal de usuario (UPN).
<code>--authDomain</code>	Nombre de dominio completo o nombre Netbios del dominio del usuario administrador de Horizon 7 especificado en la opción <code>--authAs</code> .
<code>--authPassword</code>	Contraseña del usuario administrador de Horizon 7 especificado en la opción <code>--authAs</code> . Si introduce "*" en lugar de una contraseña, el comando <code>vdmutil</code> solicitará la contraseña y no permitirá contraseñas que distingan entre mayúsculas y minúsculas en el historial de la línea de comandos.

Debe usar las opciones de autenticación con todas las opciones del comando `vdmutil` excepto con `--help` y con `--verbose`.

Salida de comando

El comando `vdmutil` devuelve 0 cuando una operación se realiza correctamente y un código que no es cero específico de errores cuando una operación no se realiza correctamente. El comando `vdmutil` escribe mensajes de error de los errores estándar. Cuando una operación genera una salida o cuando el registro detallado está habilitado con la opción `--verbose`, el comando `vdmutil` escribe la salida estándar en inglés de Estados Unidos.

Comandos para administrar los servidores de registro

Debe agregar un servidor de inscripción en cada dominio. También puede agregar un servidor de inscripción secundario y designar posteriormente dicho servidor para que se utilice como copia de seguridad.

Para que se puedan leer con facilidad, las opciones que aparecen en la siguiente tabla no representan el comando completo que tiene que introducir. Solo se incluyen las opciones específicas de la tarea en concreto. Por ejemplo, una fila muestra las opciones `--environment` `--list` `--enrollmentServers`, pero el comando `vdmUtil` que introdujo también contiene opciones para la autenticación y para especificar que está configurando True SSO:

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-netbios --authPassword contraseña-usuario-administrador --trueSSO --environment --list --enrollmentServers
```

Para obtener más información sobre las opciones de autenticación, consulte [Referencia de la línea de comandos para configurar True SSO](#).

Tabla 5-2. Opciones del comando vdmutil truesso para administrar los servidores de inscripción

Comandos y opciones	Descripción
<code>--environment --add --enrollmentServer fqdn-servidor-inscripción</code>	Agrega el servidor de inscripción especificado al entorno, donde <i>fqdn-servidor-inscripción</i> es el FQDN del servidor de inscripción. Si ya se agregó el servidor de inscripción, no ocurre nada al ejecutar este comando.
<code>--environment --remove --enrollmentServer fqdn-servidor-inscripción</code>	Elimina el servidor de inscripción especificado del entorno, donde <i>fqdn-servidor-inscripción</i> es el FQDN del servidor de inscripción. Si ya se eliminó el servidor de inscripción, no ocurre nada al ejecutar este comando.
<code>--environment --list --enrollmentServers</code>	Muestra los FQDN de todos los servidores de inscripción del entorno.
<code>--environment --list --enrollmentServer fqdn-servidor-inscripción</code>	<p>Muestra los FQDN de los dominios y sus bosques de confianza, así como los bosques a los que el servidor de inscripción pertenece y el estado del certificado de inscripción, que puede ser VÁLIDO o NO VÁLIDO. VÁLIDO supone que el servidor de registro tiene instalado un certificado Enrollment Agent. El estado puede ser NO VÁLIDO por varias razones:</p> <ul style="list-style-type: none"> ■ No se instaló el certificado. ■ El certificado ya no es válido o caducó. ■ El certificado no proviene de una CA empresarial de confianza. ■ La clave privada no está disponible. ■ El certificado está dañado. <p>El archivo de registro del servidor de inscripción puede proporcionar la razón del estado NO VÁLIDO.</p>
<code>--environment --list --enrollmentServer fqdn-servidor-inscripción --domain fqdn-dominio</code>	Para el servidor de inscripción en el dominio especificado, muestra los CN (nombres comunes) de las entidades de certificación disponibles y proporciona la siguiente información sobre cada plantilla de certificado que se puede usar para True SSO: nombre, longitud mínima de la clave y algoritmo hash.

Comandos para administrar conectores

Debe crear un conector para cada dominio. El conector define los parámetros que se usan para True SSO.

Para que se puedan leer con facilidad, las opciones que aparecen en la siguiente tabla no representan el comando completo que tiene que introducir. Solo se incluyen las opciones específicas de la tarea en concreto. Por ejemplo, una fila muestra las opciones `--list --connector`, pero el comando `vdmUtil` que introdujo también contiene opciones para la autenticación y para especificar que está configurando True SSO:

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-netbios --authPassword contraseña-usuario-administrador --truesso --list --connector
```

Para obtener más información sobre las opciones de autenticación, consulte [Referencia de la línea de comandos para configurar True SSO](#).

Tabla 5-3. Opciones del comando vdmutil truesso para administrar los conectores

Opciones	Descripción
<pre>--create --connector --domain fqdn-dominio --template nombre-plantilla --primaryEnrollmentServer fqdn-servidor1- inscripción [--secondaryEnrollmentServer fqdn-servidor2-inscripción] --certificateServer nombre-común-CA --mode {enabled disabled}</pre>	<p>Crea un conector para el dominio especificado y configura el conector para que use las siguientes opciones:</p> <ul style="list-style-type: none"> ■ <i>nombre-plantilla</i> es el nombre de la plantilla del certificado que debe usar. ■ <i>fqdn-servidor1-inscripción</i> es el FQDN del servidor de inscripción primario que debe usar. ■ <i>fqdn-servidor2-inscripción</i> es el FQDN del servidor de inscripción secundario que debe usar. Esta configuración es opcional. ■ <i>nombre-común-CA</i> es el nombre común de la entidad de certificación que debe usar. Esta puede ser una lista de CA separadas por comas. <p>Para determinar qué plantilla de certificado y qué entidad de certificación están disponibles para un servidor de inscripción en concreto, puede ejecutar el comando vdmutil con las opciones</p> <pre>--truesso --environment --list --enrollmentServer fqdn- servidor-registro --domain fqdn-dominio.</pre>
<pre>--list --connector</pre>	Enumera los FQDN de los dominios que ya tienen un conector creado.
<pre>--list --connector --verbose</pre>	<p>Enumera todos los dominios que tienen conectores y proporciona la siguiente información de cada conector:</p> <ul style="list-style-type: none"> ■ Servidor de inscripción primario ■ Servidor de inscripción secundario, si existe ■ Nombre de plantilla de certificado ■ Si el conector está habilitado o deshabilitado ■ Nombre común del servidor o de los servidores de la entidad de certificación, si existe más de uno
<pre>--edit --connector fqdn-dominio [--template nombre-plantilla] [--mode {enabled disabled} [--primaryEnrollmentServer fqdn-servidor1- inscripción] [--secondaryEnrollmentServer fqdn-servidor2-inscripción] [--certificateServer nombre-común-CA]</pre>	<p>En el conector creado para el dominio especificado en <i>domain-fqdn</i> le permite cambiar cualquiera de las siguientes opciones:</p> <ul style="list-style-type: none"> ■ <i>nombre-plantilla</i> es el nombre de la plantilla del certificado que debe usar. ■ El modo puede ser <i>enabled</i> o <i>disabled</i>. ■ <i>fqdn-servidor1-inscripción</i> es el FQDN del servidor de inscripción primario que debe usar. ■ <i>fqdn-servidor2-inscripción</i> es el FQDN del servidor de inscripción secundario que debe usar. Esta configuración es opcional. ■ <i>nombre-común-CA</i> es el nombre común de la entidad de certificación que debe usar. Esta puede ser una lista de CA separadas por comas.
<pre>--delete --connector fqdn-dominio</pre>	Elimina el conector que se creó para el dominio especificado por <i>fqdn-dominio</i> .

Comandos para administrar autenticadores

Los autenticadores se crean cuando configura la autenticación SAML entre VMware Identity Manager, Horizon 7 y un servidor de conexión. La única tarea de administración es habilitar o deshabilitar True SSO para el autenticador.

Para que se puedan leer con facilidad, las opciones que aparecen en la siguiente tabla no representan el comando completo que tiene que introducir. Solo se incluyen las opciones específicas de la tarea en concreto. Por ejemplo, una fila muestra las opciones `--list --authenticator`, pero el comando `vdmUtil` que introdujo también contiene opciones para la autenticación y para especificar que está configurando True SSO:

```
vdmUtil --authAs usuario-función-administrador --authDomain nombre-netbios --authPassword contraseña-usuario-administrador --truesso --list --authenticator
```

Para obtener más información sobre las opciones de autenticación, consulte [Referencia de la línea de comandos para configurar True SSO](#).

Tabla 5-4. Opciones del comando `vdmutil truesso` para administrar los autenticadores

Comandos y opciones	Descripción
<code>--list --authenticator [--verbose]</code>	Realiza una lista de los nombres de dominios completos (FQDN) de todos los autenticadores SAML que se encuentran en el dominio. En cada uno, especifique si True SSO está habilitado. Si usa la opción <code>--verbose</code> , los FQDN de los servidores de conexión asociados también aparecen en la lista.
<code>--list --authenticator --name etiqueta</code>	Para el autenticador especificado, muestra si True SSO está habilitado y también los FQDN de los servidores de conexión asociados. Para <i>etiqueta</i> , use uno de los nombres que aparecen en la lista cuando utiliza la opción <code>--authenticator</code> sin la opción <code>--name</code> .
<code>--edit --authenticator --name etiqueta</code> <code>--truessoMode valor-modo</code>	<p>Para el autenticador especificado, configure el modo True SSO con el valor que especificó, donde <i>valor-modo</i> puede corresponder a uno de los siguientes valores:</p> <ul style="list-style-type: none"> ■ ENABLED. True SSO se usa únicamente cuando las credenciales de Active Directory del usuario no están disponibles. ■ ALWAYS. True SSO se usa siempre aunque vDM tenga las credenciales de AD del usuario. ■ DISABLED. True SSO está deshabilitado. <p>Para <i>etiqueta</i>, use uno de los nombres que aparecen en la lista cuando utiliza la opción <code>--authenticator</code> sin la opción <code>--name</code>.</p>

Opciones de configuración avanzadas para True SSO

Puede administrar la configuración avanzada de True SSO usando la plantilla de GPO en el equipo de Horizon Agent, la configuración de registro en el servidor de registro y las entradas LDAP en el servidor de conexión. Estas opciones incluyen un tiempo de espera predeterminado, configurar el equilibrador de carga y especificar los dominios que se deben incluir, entre otros.

Opciones de configuración de Horizon Agent

Puede usar la plantilla de GPO en el SO agente para desactivar True SSO en el nivel de grupos o para cambiar los valores predeterminados de la configuración del certificado como el recuento y el tamaño de clave, así como las opciones de los intentos de reconexión.

Nota La siguiente tabla muestra las opciones que se deben usar para configurar el agente en máquinas virtuales individuales, pero puede usar de forma alternativa los archivos de plantilla de configuración de Horizon Agent. El archivo de plantilla ADMX se denomina (`vdm_agent.admx`). Use estos archivos de plantilla para aplicar esta configuración de directivas en todas las máquinas virtuales de un grupo de aplicaciones o de escritorios. Si una directiva está configurada, esta tiene preferencia sobre la opción de registro.

Los archivos ADMX están disponibles en `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, que puede descargarse desde el sitio de descargas de VMware:

<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.

Tabla 5-5. Claves para configurar True SSO en Horizon Agent

Clave	Mín. y máx.	Descripción
Disable True SSO	No disponible	Establezca esta clave como true para deshabilitar la función en el agente. Use esta opción en la directiva de grupo para deshabilitar True SSO en el nivel de grupo. El valor predeterminado es false .
Certificate wait timeout	10 -120	Especifica el periodo de tiempo de espera de los certificados para llegar al agente, en segundos. El valor predeterminado es 40 .
Minimum key size	1024 - 8192	Tamaño mínimo permitido para una clave. El valor predeterminado es 1024 , lo que supone que, de forma predeterminada, sin el tamaño de la clave es inferior a 1024, esta no se puede utilizar.
All key sizes	No disponible	Lista separada por comas de los tamaños de clave que se pueden usar. Se pueden especificar hasta 5 tamaños, por ejemplo: 1024,2048,3072,4096 . El valor predeterminado es 2048 .
Number of keys to pre-create	1-100	Número de claves que se crean previamente en servidores RDS que proporcionan escritorios remotos y aplicaciones alojadas en Windows. El valor predeterminado es 5 .
Minimum validity period required for a certificate	No disponible	Periodo de validez mínimo, en minutos, que necesita un certificado cuando se vuelve a usar para reconectar un usuario. El valor predeterminado es 5 .

Opciones de configuración del servidor de inscripción

Puede usar la configuración del Registro de Windows en el SO del servidor de inscripción para configurar los dominios a los que conectarse, varios periodos de tiempo de espera, periodos de sondeo, reintentos y si prefiere usar la entidad de certificación que está instalada en el mismo servidor local (recomendado).

Para cambiar las opciones de configuración avanzada, puede abrir el Editor del Registro de Windows (regedit.exe) en el equipo del servidor de inscripción y dirigirse a la siguiente clave de registro:

HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service

Tabla 5-6. Claves de registro para configurar TrueSSO en el servidor de registro

Clave del registro	Min. y máx.	Tipo	Descripción
ConnectToDomains	No disponible	REG_MULTI_SZ	<p>Lista de dominios a los que el servidor de inscripción intenta conectarse automáticamente. Para este tipo de registro de varias cadenas, el nombre de dominio completo DNS (FQDN) de cada dominio aparece en su propia línea.</p> <p>El comportamiento predeterminado es confiar en todos los dominios.</p>
ExcludeDomains	No disponible	REG_MULTI_SZ	<p>Lista de dominios a los que el servidor de inscripción no se conecta automáticamente. Si el servidor de conexión proporciona un conjunto de configuraciones con cualquier dominio, el servidor de inscripción intentará conectarse a ese dominio o esos dominios. Para este tipo de registro de varias cadenas, el FQDN DNS de cada dominio aparece en su propia línea.</p> <p>El comportamiento predeterminado es no excluir a ningún dominio.</p>
ConnectToDomainsInForest	No disponible	REG_SZ	<p>Especifica si se conecta a todos los dominios y los usa en el bosque del que el servidor de inscripción es miembro. El valor predeterminado es TRUE.</p> <p>Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> 0 significa false, no se conecta a los dominios del bosque que se está utilizando. !=0 significa true.
ConnectToTrustingDomains	No disponible	REG_SZ	<p>Especifica si se conecta a dominios entrantes o de confianza explícitamente. El valor predeterminado es TRUE.</p> <p>Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> 0 significa false, no se conecta a los dominios entrantes o de confianza explícitamente. !=0 significa true.
PreferLocalCa	No disponible	REG_SZ	<p>Especifica si prefiere la CA que se encuentra en las instalaciones, en caso de que esté disponible, para obtener beneficios en el rendimiento. Si está establecido como TRUE, el servidor de inscripción enviará solicitudes a la CA local. Si se produce un error en la conexión a la CA, el servidor de inscripción intentará enviar solicitudes de certificados a CA alternativas. El valor predeterminado es FALSE (falso).</p> <p>Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> 0 significa false. !=0 significa true.

Tabla 5-6. Claves de registro para configurar TrueSSO en el servidor de registro (Continuación)

Clave del registro	Min. y máx.	Tipo	Descripción
MaxSubmitRetryTime	9500- 59000	DWORD	Cantidad de tiempo que se debe esperar antes de volver a intentar enviar una solicitud de firma del certificado, en milisegundos. El valor predeterminado es 25000 .
SubmitLatencyWarningTime	500 - 5000	DWORD	<p>Envía el tiempo de advertencia de latencia cuando la interfaz está marcada como "Degradada" (en milisegundos). El valor predeterminado es 1500.</p> <p>El servidor de inscripción usa esta opción para determinar si se debe considerar que una CA esté en estado degradado. Si las últimas tres solicitudes de certificado tardaron en completarse más milisegundos de los especificados por esta opción, la CA se considera degradada y este estado aparece en el panel de control de estado de Horizon Administrator.</p> <p>Una CA suele expedir un certificado en 20 ms, pero si la CA estuvo inactiva durante algunas horas, cualquier solicitud inicial puede tardar más tiempo en completarse. Esta opción permite a un administrador descubrir que una CA es lenta, sin necesidad de tenerla marcada como tal. Use esta opción para configurar el umbral que marca la CA como lenta.</p>
WarnForLonglivedCert	No disponible	REG_SZ	<p>Deshabilita la advertencia del certificado de True SSO permanente (plantillas). El valor predeterminado es True.</p> <p>El servidor de inscripción muestra un estado de advertencia en el panel de control de estado de Horizon Administrator notificando que las plantillas True SSO están degradadas o no tienen un estado óptimo si el certificado tiene una vigencia de más de 14 días. El servidor de inscripción usa esta opción para deshabilitar la advertencia.</p> <p>Se debe reiniciar el servidor de inscripción para que esta opción se aplique.</p>

Opciones de configuración del servidor de conexión

Puede editar el LDAP de View en el servidor de conexión si desea configurar un tiempo de espera para generar los certificados y si desea habilitar las solicitudes del certificado de equilibrio de carga entre los servidores de inscripción (recomendado).

Para cambiar las opciones de configuración avanzada, debe usar el Editor ADSI en el host del servidor de conexión. Puede conectarse escribiendo el nombre distintivo **DC=vdi**, **DC=vmware**, **DC=int** como el punto de conexión e introduciendo **localhost:389** en el puerto y el nombre del servidor. Amplíe **OU=Properties**, seleccione **OU=Global** y haga doble clic en **OU=Common** en el panel derecho.

Puede editar el atributo **pae-NameValuePair** para agregar uno o varios de los valores que aparecen en la siguiente tabla. Debe usar la sintaxis **nombre=valor** al agregar los valores.

Tabla 5-7. Configuración avanzada de True SSO para los servidores de conexión

Clave del registro	Descripción
cs-view-certssso-enable-es-loadbalance=[true false]	<p>Especifica si habilitar las solicitudes CSR de equilibrio de carga entre dos servidores de inscripción. El valor predeterminado es false (falso).</p> <p>Por ejemplo, agregue cs-view-certssso-enable-es-loadbalance=true para habilitar el equilibrio de carga de forma que, si llegan las solicitudes del certificado, el servidor de conexión usará servidores de inscripción alternativos. Cada servidor de inscripción puede atender a las solicitudes usando la CA local, en caso de tener el servidor de inscripción y la CA en el mismo host.</p>
cs-view-certssso-certgen-timeout-sec=número	Cantidad de tiempo, en segundos, que se debe esperar para generar un certificado después de recibir un CSR. El valor predeterminado es 35.

Identificar un usuario de AD que no tenga un UPN de AD

Puede configurar filtros en la URL de LDAP para que el servidor de conexión identifique a un usuario de AD que no tenga un UPN de AD.

Debe usar el Editor ADSI de ADAM en un host del servidor de conexión. Es posible conectarse introduciendo un nombre distintivo **DC=vdi**, **DC=vmware**, **DC=int**. Expanda **OU=Properties** y seleccione **OU=Authenticator**.

A continuación, puede editar el atributo **pae-LDAPURLList** si desea agregar un filtro para la URL de LDAP.

Por ejemplo, agregue el siguiente filtro:

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(telephoneNumber=$NAMEID)
```

De forma predeterminada, el servidor de conexión usa los siguientes filtros para la URL de LDAP:

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???
(&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???
(&(objectCategory=group)(objectclass=group)(sAMAccountName=$NAMEID))
```

```
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///???
(&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???
(&(objectCategory=group)(objectclass=group)(sAMAccountName=$NAMEID))
```

Si configura un filtro para la URL de LDAP, el servidor de conexión usa este filtro y no el predeterminado para identificar al usuario.

Ejemplos de identificadores que puede usar en una autenticación SAML para un usuario de AD que no tenga un UPN de AD:

- "cn"
- "mail"
- "description"
- "givenName"

- "sn"
- "canonicalName"
- "sAMAccountName"
- "member"
- "memberOf"
- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

Uso del panel de control del estado del sistema para solucionar problemas relacionados con True SSO

Puede usar el panel de control del estado del sistema en Horizon Administrator para identificar rápidamente los problemas que puedan afectar la operación de la función True SSO.

Para los usuarios finales, si True SSO deja de funcionar, cuando el sistema intenta iniciar la sesión del usuario en la aplicación o el escritorio remotos, el usuario ve el siguiente mensaje: "El nombre de usuario o la contraseña es incorrecto." Después de que el usuario haga clic en **Aceptar**, aparece la pantalla de inicio de sesión. En la pantalla de inicio de sesión de Windows, el usuario ve un icono adicional denominado **Usuario SSO de VMware**. Si el usuario tiene las credenciales de Active Directory de un usuario con autorización, puede iniciar sesión con las credenciales de AD.

El panel de control del estado del sistema situado en la parte superior izquierda de la ventana de Horizon Administrator muestra varios elementos que pertenecen a True SSO.

Nota La función True SSO proporciona información al panel de control una vez por minuto. Haga clic en el icono de actualización situado en la esquina superior derecha para actualizar la información inmediatamente.

- Puede hacer clic para expandir **Componentes de View > True SSO** para ver una lista de los dominios que usan True SSO.

Puede hacer clic en un nombre de dominio para ver la siguiente información: una lista de servidores de inscripciones configurados para dicho dominio, una lista de entidades de certificación empresarial, el nombre de la plantilla del certificado que se está utilizando y el estado. Si hay algún problema, el campo Estado explica cuál es.

Para cambiar las opciones de configuración que aparecen en el cuadro de diálogo Detalles del dominio True SSO, use la interfaz de línea de comandos `vdmutil` para editar el conector True SSO. Si desea obtener más información, consulte [Comandos para administrar conectores](#).

- Puede hacer clic para expandir **Otros componentes > Autenticadores SAML 2.0** para ver una lista de autenticadores SAML que se crearon para delegar la autenticación a las instancias de VMware Identity Manager. Puede hacer clic en el nombre del autenticador para examinar los detalles y el estado.

Nota Para usar True SSO, se debe habilitar la opción global para SSO. En Horizon Administrator, seleccione **Configuración > Configuración global** y compruebe que **Configurar Single Sign-On (SSO)** esté establecido como **Habilitado**.

Tabla 5-8. Estado de conexión del servidor de conexión con el servidor de inscripción

Texto del estado	Descripción
No se pudo recuperar la información de estado de True SSO.	El panel de control no puede recuperar la información del estado desde la instancia del servidor de conexión.
El servicio de configuración True SSO no puede contactar con el servidor de inscripción <FQDN>.	En un pod, una de las instancias del servidor de conexión se selecciona para enviar la información de configuración a todos los servidores de inscripciones que usa el pod. Esta instancia del servidor de conexión actualizará la configuración del servidor de inscripciones una vez por minuto. Este mensaje aparece si la tarea de configuración no pudo actualizar el servidor de inscripciones. Para obtener más información, consulte la tabla Conectividad del servidor de inscripciones.
No se puede contactar con el servidor de inscripción <FQDN> para administrar las sesiones en este servidor de conexión.	La instancia actual del servidor de conexión no puede conectarse al servidor de inscripciones. Este estado solo aparece para la instancia del servidor de conexión al que el navegador se dirige. Si existen varias instancias del servidor de conexión en el pod, es necesario que cambie el navegador para que se dirija a otras instancias del servidor de conexión para comprobar sus estados. Para obtener más información, consulte la tabla Conectividad del servidor de inscripciones.

Tabla 5-9. Conectividad del servidor de inscripciones

Texto del estado	Descripción
Este dominio <Nombre dominio> no existe en el servidor de inscripciones <FQDN>.	El conector True SSO se configuró para usar este servidor de inscripciones en este dominio, pero aún no se configuró este servidor para que se conecte al dominio. Si el estado se mantiene durante más de un minuto, es necesario que compruebe el estado del servidor de conexión responsable de actualizar la configuración de las inscripciones.
La conexión del servidor de inscripción de <FQDN> al dominio <Nombre dominio> aún se está estableciendo.	El servidor de inscripciones no se pudo conectar a un controlador de este dominio. Si este estado se mantiene durante más de un minuto, tiene que verificar que la resolución del nombre del servidor de inscripciones al dominio sea correcta y que exista una conectividad de red entre el servidor de inscripciones y el dominio.
La conexión del servidor de inscripción de <FQDN> al dominio <Nombre dominio> se está deteniendo o está en un estado problemático.	El servidor de inscripciones se conectó a un controlador de dominio, pero no puede leer la información PKI de este controlador. Si esto sucede, es posible que haya un problema con el controlador del dominio actual. Este problema también puede suceder si DNS no está configurado correctamente. Revise el archivo de registro del servidor de inscripciones para ver el controlador de dominio que el servidor de inscripciones está intentando usar y compruebe que el controlador de dominio esté totalmente operativo.
El servidor de inscripción <FQDN> no leyó aún las propiedades de inscripción de ningún controlador de dominio.	Este es un estado de transición y solo se muestra durante el inicio del servidor de inscripciones o cuando se agrega un nuevo dominio al entorno. Este estado suele durar menos de un minuto. Si dura más, puede ser que la red sea muy lenta o que exista un problema que no permita acceder correctamente al controlador del dominio.

Tabla 5-9. Conectividad del servidor de inscripciones (Continuación)

Texto del estado	Descripción
El servidor de inscripción <FQDN> leyó las propiedades de inscripción al menos una vez, pero no pudo acceder a un controlador de dominio durante un tiempo.	Mientras el servidor de inscripciones lea la configuración PKI desde un controlador de dominio, se mantiene sondeando los cambios cada dos minutos. Este estado se establecerá si no se puede acceder al controlador de dominio (DC) durante un breve periodo de tiempo. Normalmente, esta situación supone que el servidor de inscripciones no puede detectar ningún cambio en la configuración PKI. Mientras los servidores de certificados puedan acceder a un controlador de dominio, los certificados se pueden seguir expidiendo.
El servidor de inscripción <FQDN> leyó las propiedades de inscripción al menos una vez, pero no pudo acceder a un controlador de dominio durante un largo período de tiempo o existe otro problema.	Si el servidor de inscripciones no puede acceder al controlador de dominio durante un tiempo prolongado, aparece este estado. El servidor de inscripciones intentará encontrar un controlador de dominio alternativo para este dominio. Si un servidor de certificados puede seguir accediendo a un controlador de dominio, los certificados pueden seguir expidiéndose, pero si este estado se mantiene durante más de un minuto, esto significa que el servidor de inscripciones perdió el acceso a todos los controladores del dominio y es posible que no se puedan seguir expidiendo los certificados.

Tabla 5-10. Estado del certificado de inscripción

Texto del estado	Descripción
No hay instalado un certificado de inscripción válido para este bosque <nombre dominio> del dominio en el servidor de inscripción <FQDN> o puede que caducara.	No se instaló ningún certificado de inscripción para este dominio o el certificado no es válido o caducó. Una CA empresarial debe expedir el certificado de inscripción y esta debe ser de confianza para el bosque al que este dominio pertenece. Compruebe que completó los pasos del documento <i>Administración de Horizon 7</i> , que describe cómo instalar el certificado de inscripción en el servidor de inscripciones. También puede abrir el MMC, el complemento de administración de certificados, abriendo el almacén del equipo local. Abra el contenedor de certificados personales y compruebe que el certificado esté instalado y que sea válido. También puede abrir el archivo de registros del servidor de inscripciones. Los servidores de inscripciones registrarán información adicional sobre el estado de cualquier certificado que esté ubicado.

Tabla 5-11. Estado de plantilla del certificado

Texto del estado	Descripción
La plantilla <nombre> no existe en el dominio del servidor de inscripción <FQDN>.	Compruebe que especificó el nombre de plantilla correcto.
Los certificados generados por esta plantilla NO se pueden usar para iniciar sesión en Windows.	Esta plantilla no tiene habilitados el uso de la tarjeta inteligente ni la firma de datos. Compruebe que especificó el nombre de plantilla correcto. Compruebe que completó los pasos descritos en Crear plantillas de certificado para usarlas con True SSO .
La plantilla <nombre> está habilitada para iniciar sesión con una tarjeta inteligente, pero no se puede utilizar.	Esta plantilla está habilitada para iniciar sesión con una tarjeta inteligente, pero no puede usarse con True SSO. Compruebe que especificara el nombre de la plantilla correcto y compruebe que completó los pasos descritos en Crear plantillas de certificado para usarlas con True SSO . También puede revisar el archivo de registro del servidor de inscripciones, ya que tiene registrada la opción de la plantilla que hace que no se pueda usar con True SSO.

Tabla 5-12. Estado de configuración del servidor de certificados

Texto del estado	Descripción
El servidor de certificado <CN de CA> no existe en el dominio.	Compruebe que especificó el nombre correcto de la CA. Debe especificar el Nombre común (CN).
El certificado no está en el almacén NTAAuth (Enterprise).	Esta CA no es empresarial o su certificado no se agregó al almacén NTAUTH. Si esta CA no es miembro del bosque, debe agregar el certificado de la CA manualmente al almacén NTAUTH de este bosque.

Tabla 5-13. Estado de conexión del servidor de certificados

Texto del estado	Descripción
El servidor de inscripción <FQDN> no está conectado al servidor de certificados <CN de CA>.	El servidor de inscripción no está conectado al servidor de certificados. Este estado puede ser de transición si el servidor de inscripciones se acaba de iniciar o si la CA se agregó recientemente a un conector True SSO. Si este estado se mantiene durante más de un minuto, esto significa que el servidor de inscripciones no se pudo conectar a la CA. Valide que la resolución del nombre esté funcionando correctamente, que tenga conectividad de red a la CA y que la cuenta del sistema para el servidor de inscripciones tenga permiso para acceder a la CA.
El servidor de inscripción <FQDN> se conectó al servidor de certificados <CN of CA>, pero este está en estado degradado.	<p>Este estado se muestra si la CA expide certificados a un ritmo lento. Si la CA se mantiene en este estado, compruebe su carga o los controladores de dominio que usan la CA.</p> <p>Nota Si la CA se marcó como lenta, mantendrá este estado hasta que se complete al menos una solicitud de certificado correctamente y se expida dentro de un intervalo de tiempo normal.</p>
El servidor de inscripción <FQDN> se puede conectar al servidor de certificados <CN de CA>, pero el servicio no está disponible.	Este estado se expide si el servidor de inscripciones tiene una conexión activa a la CA pero no puede expedir certificados. Este suele ser un estado de transición. Si la CA no vuelve a estar disponible rápidamente, el estado cambiará a desconectado.

Configurar la administración delegada basada en funciones

6

Una tarea de administración clave en un entorno de Horizon 7 es determinar quién puede usar Horizon Administrator y las tareas que esos usuarios tienen autorización para realizar. Con la administración delegada basada en funciones, puede asignar de forma selectiva los derechos administrativos al designar funciones de administrador para grupos y usuarios específicos de Active Directory.

Este capítulo incluye los siguientes temas:

- [Comprender las funciones y los privilegios](#)
- [Uso de grupos de acceso para delegar la administración de grupos y granjas](#)
- [Comprender los permisos](#)
- [Administrar administradores](#)
- [Administrar y consultar los permisos](#)
- [Administrar y consultar los grupos de acceso](#)
- [Administrar funciones personalizadas](#)
- [Funciones y privilegios predefinidos](#)
- [Privilegios necesarios para las tareas comunes](#)
- [Prácticas recomendadas para grupos y usuarios administradores](#)

Comprender las funciones y los privilegios

La capacidad para realizar tareas en Horizon Administrator se rige por un sistema de control de acceso que consta de privilegios y funciones de administrador. Este sistema es similar al sistema de control de acceso de vCenter Server.

Una función de administrador es una recopilación de privilegios. Los privilegios otorgan la capacidad de realizar acciones específicas, como proporcionar autorización a un usuario para utilizar un grupo de escritorios. Los privilegios también controlan qué puede ver un administrador en Horizon Administrator. Por ejemplo, si un administrador no tiene privilegios para ver o modificar directivas, la opción **Directivas globales** no aparece visible en el panel de navegación cuando el administrador inicia sesión en Horizon Administrator.

Los privilegios de administrador pueden ser globales o específicos de objeto. Los privilegios globales controlan las operaciones de todo el sistema, como ver y cambiar la configuración global. Los privilegios específicos de objeto controlan las operaciones de determinados tipos de objetos.

Las funciones de administrador suelen combinar todos los privilegios individuales necesarios para realizar una tarea de administración de nivel superior. Horizon Administrator incluye funciones predefinidas que contienen los privilegios necesarios para realizar tareas de administración comunes. Puede asignar estas funciones predefinidas a los grupos y a los usuarios administradores, o bien puede crear sus propias funciones combinando los privilegios seleccionados. Estas funciones no se pueden modificar.

Para crear administradores, seleccione los grupos y los usuarios de los que tiene en Active Directory y asigne funciones de administrador. Los administradores obtienen privilegios gracias a las asignaciones de funciones. No puede asignar los privilegios directamente a los administradores. Un administrador que tenga varias asignaciones de funciones adquiere la suma de todos los privilegios contenidos en esas funciones.

Uso de grupos de acceso para delegar la administración de grupos y granjas

De forma predeterminada, los grupos de escritorios automáticos, los grupos de escritorios manuales y las granjas se crean en el grupo de acceso raíz, que aparece como / o Raíz(/) en Horizon Administrator. Los grupos de aplicaciones y los grupos de escritorios publicados heredan los grupos de acceso de la granja. Puede volver a crear grupos de acceso bajo el grupo de acceso raíz para delegar la administración de granjas o grupos específicos a administradores diferentes.

Nota No puede cambiar el grupo de acceso de un grupo de aplicaciones o un grupo de escritorios publicados directamente. Debe cambiar el grupo de acceso de la granja a la que pertenecen el grupo de aplicaciones o el grupo de escritorios publicados.

Un equipo físico o una máquina virtual hereda el grupo de acceso desde el grupo de escritorios. Un disco persistente conectado hereda el grupo de acceso de este equipo. Puede tener un máximo de 100 grupos de acceso, incluido el grupo de acceso raíz.

Configure el acceso administrador a los recursos en un grupo de acceso asignando una función a un administrador de ese grupo de acceso. Los administradores pueden acceder a los recursos que se encuentran únicamente en los grupos de acceso para los que asignaron funciones. La función que tiene un administrador en un grupo de acceso determina el nivel de acceso que tiene este administrador a los recursos en ese grupo.

Como las funciones se heredan del grupo de acceso raíz, un administrador que tenga una función en el grupo de acceso tiene esa función en todos los grupos de acceso. Los administradores que tengan la función Administradores en el grupo de acceso raíz son superadministradores porque tienen acceso completo a todos los objetos del sistema.

Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso. Las funciones que incluyen privilegios específicos de objeto no se pueden aplicar a grupos de acceso.

Puede usar Horizon Administrator para crear grupos de acceso y para mover los grupos de escritorios existentes a los grupos de acceso. Cuando cree un grupo de escritorios automático, un grupo manual o una granja, puede aceptar el grupo de acceso raíz predeterminado o seleccionar un grupo de acceso diferente.

Nota Si tiene pensado proporcionar acceso a los escritorios y las aplicaciones a través de VMware Identity Manager, verifique que cree los grupos de aplicaciones y de escritorios como un usuario con la función Administradores en el grupo de acceso raíz de Horizon Administrator. Si proporciona al usuario la función Administradores en un grupo de acceso diferente al raíz, VMware Identity Manager no reconocerá el autenticador SAML que configuró en Horizon 7 y no podrá configurar el grupo en VMware Identity Manager.

- **Administradores diferentes para grupos de acceso diferentes**

Puede crear un administrador diferente para administrar cada grupo de acceso en la configuración.

- **Administradores diferentes para el mismo grupo de acceso**

Puede crear diferentes administradores para gestionar el mismo grupo de acceso.

Administradores diferentes para grupos de acceso diferentes

Puede crear un administrador diferente para administrar cada grupo de acceso en la configuración.

Por ejemplo, si los grupos de escritorios empresariales están en un grupo de acceso y los grupos de escritorio de los desarrolladores de software están en otro grupo de acceso, puede crear administradores diferentes para gestionar los recursos en cada grupo de acceso.

Tabla 6-1 muestra un ejemplo de este tipo de configuración.

Tabla 6-1. Administradores diferentes para grupos de acceso diferentes

Administrador	Función	Grupo de acceso
view-domain.com\Admin1	Administradores de inventario	/CorporateDesktops
view-domain.com\Admin2	Administradores de inventario	/DeveloperDesktops

En este ejemplo, el administrador denominado Admin1 tiene la función Administradores de inventario en el grupo de acceso denominado CorporateDesktops y el administrador denominado Admin2 tiene la función Administradores de inventario en el grupo de acceso denominado DeveloperDesktops.

Administradores diferentes para el mismo grupo de acceso

Puede crear diferentes administradores para gestionar el mismo grupo de acceso.

Por ejemplo, si los grupos de escritorios empresariales están en un grupo de acceso, puede crear un administrador que pueda ver y modificar estos grupos y otro administrador que solo pueda verlos.

Tabla 6-2 muestra un ejemplo de este tipo de configuración.

Tabla 6-2. Administradores diferentes para el mismo grupo de acceso

Administrador	Función	Grupo de acceso
view-domain.com\Admin1	Administradores de inventario	/CorporateDesktops
view-domain.com\Admin2	Administradores de inventario (solo lectura)	/CorporateDesktops

En este ejemplo, el administrador denominado Admin1 tiene la función Administradores de inventario en el grupo de acceso denominado CorporateDesktops y el administrador denominado Admin2 tiene la función Administradores de inventario (solo lectura) en el mismo grupo de acceso.

Comprender los permisos

Horizon Administrator presenta la combinación de una función, un grupo o usuario administrador y un grupo de acceso como permiso. La función define las acciones que se pueden realizar, el usuario o el grupo indican quién puede realizar la acción y el grupo de acceso contiene los objetos sobre los que se realiza la acción.

Los permisos aparecen de forma diferente en Horizon Administrator según si selecciona un grupo o un usuario administrador, un grupo de acceso o una función.

La siguiente tabla muestra cómo aparecen los permisos en Horizon Administrator cuando selecciona un grupo o un usuario administrador. El usuario administrador se denomina Admin 1 y tiene dos permisos.

Tabla 6-3. Permisos en la pestaña Administradores y grupos para Admin 1

Función	Grupo de acceso
Administradores de inventario	MarketingDesktops
Administradores (solo lectura)	/

El primer permiso muestra que Admin 1 tiene la función Administradores de inventario en el grupo de acceso denominado MarketingDesktops. El segundo permiso muestra que Admin 1 tiene la función Administradores (solo lectura) en el grupo de acceso raíz.

La siguiente tabla muestra cómo aparecen los mismos permisos en Horizon Administrator cuando selecciona el grupo de acceso MarketingDesktops.

Tabla 6-4. Permisos en la pestaña Carpetas para MarketingDesktops

Admin	Función	Heredado
view-domain.com\Admin1	Administradores de inventario	
view-domain.com\Admin1	Administradores (solo lectura)	Sí

El primer permiso es igual que el primer permiso que aparece en [Tabla 6-3](#). El segundo permiso se hereda del que aparece en [Tabla 6-3](#). Como los grupos de acceso heredan los permisos del grupo de acceso raíz, Admin1 tiene la función Administradores (solo lectura) en el grupo de acceso MarketingDesktops. Cuando se hereda un permiso, Sí aparece en la columna Heredado.

La siguiente tabla muestra cómo el primer permiso de [Tabla 6-3](#) aparece en Horizon Administrator cuando selecciona la función Administradores de inventario.

Tabla 6-5. Permisos en la pestaña Función para Administradores de inventario

Administrador	Grupo de acceso
view-domain.com\Admin1	/MarketingDesktops

Administrar administradores

Los usuarios con función de administradores pueden usar Horizon Administrator para agregar o eliminar grupos y usuarios administradores.

La función de administradores es la función con más poder en Horizon Administrator. Los miembros de la cuenta Administradores poseen inicialmente la función de administradores. La cuenta Administradores se especifica al instalar el servidor de conexión. La cuenta Administradores puede ser el grupo de administradores locales (BUILTIN\Administrators) del equipo del servidor de conexión o una cuenta de usuario o grupo del dominio.

Nota De forma predeterminada, el grupo de administradores del dominio es miembro del grupo local de administradores. Si especificó la cuenta Administradores a modo de grupo de administradores local y no desea que los administradores del dominio tengan acceso completo a los objetos del inventario y las opciones de configuración de Horizon 7, elimine el grupo de administradores del dominio del grupo local de administradores.

■ [Crear un administrador](#)

Para crear un administrador, seleccione uno de los grupos y usuarios de Active Directory en Horizon Administrator y asigne la función de administrador.

■ [Eliminar un administrador](#)

Puede eliminar un grupo o un usuario administradores. No puede eliminar el último superadministrador del sistema. Un superadministrador es un administrador que tiene la función Administradores en el grupo de acceso raíz.

Crear un administrador

Para crear un administrador, seleccione uno de los grupos y usuarios de Active Directory en Horizon Administrator y asigne la función de administrador.

Requisitos previos

- Familiarícese con las funciones de administrador predefinidas. Consulte [Funciones y privilegios predefinidos](#).
- Familiarícese con las prácticas recomendadas para crear grupos e usuarios administradores. Consulte [Prácticas recomendadas para grupos y usuarios administradores](#).
- Para asignar una función personalizada al administrador, cree la función. Consulte [Agregar una función personalizada](#).

- Para crear un administrador que pueda gestionar grupos de escritorios específicos, cree un grupo de acceso y mueva los grupos de escritorios a ese grupo de acceso. Consulte [Administrar y consultar los grupos de acceso](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Administradores y grupos**, haga clic en **Agregar usuarios al grupo**.
- 3 Haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los grupos o los usuarios de Active Directory según sus criterios de búsqueda.
- 4 Seleccione el grupo o el usuario de Active Directory que desea que sea el usuario o grupo administrador, haga clic en **Aceptar** y, a continuación, en **Siguiente**.

Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios.

- 5 Seleccione la función que desee asignar al grupo o usuario administrador.

La columna Se aplica a un grupo de acceso indica si una función se aplica a los grupos de acceso. Solo las funciones que incluyen privilegios específicos de objeto se aplican a los grupos de acceso. Las funciones que incluyen privilegios específicos de objeto pueden aplicarse a grupos de acceso.

Opción	Acción
La función que seleccionó se aplica a los grupos de acceso	Seleccione uno o varios grupos de acceso y haga clic en Siguiente .
Desea que la función se aplique a todos los grupos de acceso	Seleccione el grupo de acceso raíz y haga clic en Siguiente .

- 6 Haga clic en **Finalizar** para crear el grupo o usuario administrador.

El nuevo grupo o usuario administrador aparece en el panel izquierdo y la función y el grupo de acceso que seleccionó aparecen en el panel derecho de la pestaña **Administradores y grupos**.

Eliminar un administrador

Puede eliminar un grupo o un usuario administradores. No puede eliminar el último superadministrador del sistema. Un superadministrador es un administrador que tiene la función Administradores en el grupo de acceso raíz.

Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Administradores y grupos** seleccione el grupo o el usuario administradores, haga clic en **Eliminar usuario o grupo** y haga clic en **Aceptar**.

El grupo o el usuario administradores ya no aparecen en la pestaña **Administradores y grupos**.

Administrar y consultar los permisos

Puede usar Horizon Administrator para agregar, eliminar y consultar los permisos de los grupos y usuarios administradores específicos, de las funciones específicas y de los grupos de acceso específicos.

- [Agregar un permiso](#)

Es posible agregar un permiso que incluya un grupo o un usuario administrador específicos, una función específica o un grupo de acceso específico.

- [Eliminar un permiso](#)

Es posible eliminar un permiso que incluya un grupo o un usuario administrador específicos, una función específica o un grupo de acceso específico.

- [Revisar los permisos](#)

Es posible revisar los permisos que incluyan a un grupo o un administrador específicos, una función específica o un grupo de acceso específico.

Agregar un permiso

Es posible agregar un permiso que incluya un grupo o un usuario administrador específicos, una función específica o un grupo de acceso específico.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.

2 Cree el permiso.

Opción	Acción
Crear un permiso que incluya un grupo o un usuario administrador específico	<ul style="list-style-type: none"> a En la pestaña Administradores y grupos, seleccione el administrador o el grupo y haga clic en Agregar permiso. b Seleccione una función. c Si la función no se aplica a los grupos de acceso, haga clic en Finalizar. d Si la función se aplica a los grupos de acceso, haga clic en Siguiente, seleccione uno o varios grupos de acceso y haga clic en Finalizar. Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso.
Crear un permiso que incluya una función específica	<ul style="list-style-type: none"> a En la pestaña Funciones, seleccione la función, haga clic en Permisos y, a continuación, haga clic en Agregar permiso. b Haga clic en Agregar, seleccione uno o varios criterios de búsqueda y, a continuación, haga clic en Buscar para buscar los grupos o los usuarios administradores que coincidan con sus criterios de búsqueda. c Seleccione un usuario administrador o un grupo para incluir en el permiso y haga clic en Aceptar. Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios. d Si la función no se aplica a los grupos de acceso, haga clic en Finalizar. e Si la función se aplica a los grupos de acceso, haga clic en Siguiente, seleccione uno o varios grupos de acceso y haga clic en Finalizar. Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso.
Crear un permiso que incluya un grupo de acceso específico	<ul style="list-style-type: none"> a En la pestaña Grupos de acceso, seleccione el grupo de acceso y haga clic en Agregar permiso. b Haga clic en Agregar, seleccione uno o varios criterios de búsqueda y, a continuación, haga clic en Buscar para buscar los grupos o los usuarios administradores que coincidan con sus criterios de búsqueda. c Seleccione un usuario administrador o un grupo para incluir en el permiso y haga clic en Aceptar. Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios. d Haga clic en Siguiente, seleccione una función y, a continuación, haga clic en Finalizar. Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso.

Eliminar un permiso

Es posible eliminar un permiso que incluya un grupo o un usuario administrador específicos, una función específica o un grupo de acceso específico.

Si elimina el último permiso de un grupo o de un usuario administrador, estos últimos también se eliminan. Dado que al menos un administrador debe tener la función Administradores en el grupo de acceso raíz, no puede eliminar un permiso que elimine al administrador. No puede eliminar un permiso heredado.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.

- 2 Seleccione el permiso que va a eliminar.

Opción	Acción
Eliminar un permiso que se aplica a un grupo o administrador específicos	Seleccione el grupo o el administrador en la pestaña Administradores y grupos .
Eliminar un permiso que se aplica a una función	Seleccione la función en la pestaña Funciones .
Eliminar un permiso que se aplica a un grupo de acceso específico	Seleccione la carpeta en la pestaña Grupos de acceso .

- 3 Seleccione el permiso y haga clic en **Eliminar permiso**.

Revisar los permisos

Es posible revisar los permisos que incluyan a un grupo o un administrador específicos, una función específica o un grupo de acceso específico.

Procedimiento

- 1 Seleccione **Configuración de View > Administradores**.
- 2 Revise los permisos.

Opción	Acción
Revisar los permisos que incluyan un grupo o un usuario administrador específico	Seleccione el grupo o el administrador en la pestaña Administradores y grupos .
Revisar los permisos que incluyan una función específica	Seleccione la función en la pestaña Funciones y haga clic en Permisos .
Revisar los permisos que incluyan un grupo de acceso específico	Seleccione la carpeta en la pestaña Grupos de acceso .

Administrar y consultar los grupos de acceso

Puede usar Horizon Administrator para agregar y eliminar grupos de acceso y para consultar los equipos y los grupos de escritorios de un grupo de acceso particular.

■ [Agregar un grupo de acceso](#)

Cree grupos de acceso para delegar la administración de determinadas máquinas, grupos de escritorios o granjas en otros administradores. De forma predeterminada, las granjas y los grupos de escritorios o de aplicaciones se encuentran en el grupo de acceso root.

■ [Mover un grupo de escritorios o una granja a un grupo de acceso diferente](#)

Después de crear un grupo de acceso, puede mover los grupos de escritorios automáticos, los grupos manuales o las granjas al nuevo grupo de acceso.

■ [Eliminar un grupo de acceso](#)

Puede eliminar un grupo de acceso si no contiene ningún objeto. No puede eliminar el grupo de acceso raíz.

- [Revisar las granjas o los grupos de escritorios o de aplicaciones de un grupo de acceso](#)

Puede consultar las granjas o los grupos de escritorios o de aplicaciones que se encuentran en un grupo de acceso concreto de Horizon Administrator.

- [Revisar las máquinas virtuales de vCenter de un grupo de acceso](#)

Puede ver las máquinas virtuales de vCenter de un grupo de acceso concreto de Horizon Administrator. Una máquina virtual de vCenter hereda el grupo de acceso de su grupo.

Agregar un grupo de acceso

Cree grupos de acceso para delegar la administración de determinadas máquinas, grupos de escritorios o granjas en otros administradores. De forma predeterminada, las granjas y los grupos de escritorios o de aplicaciones se encuentran en el grupo de acceso root.

Puede tener un máximo de 100 grupos de acceso, incluido el grupo de acceso raíz.

Procedimiento

- 1 En Horizon Administrator, diríjase al cuadro de diálogo Agregar grupo de acceso.

Opción	Acción
En Catálogo	<ul style="list-style-type: none"> ■ Seleccione Catálogo > Grupos de escritorios. ■ En el menú desplegable Grupo de acceso situado en el panel de ventana superior, seleccione Nuevo grupo de acceso.
En Recursos	<ul style="list-style-type: none"> ■ Seleccione Recursos > Granjas. ■ En el menú desplegable Grupo de acceso situado en el panel de ventana superior, seleccione Nuevo grupo de acceso.
En Configuración de View	<ul style="list-style-type: none"> ■ Seleccione Configuración de View > Administradores. ■ En la pestaña Grupos de acceso, seleccione Agregar grupo de acceso.

- 2 Introduzca un nombre y una descripción para el grupo de acceso y haga clic en **Aceptar**.

La descripción es opcional.

Pasos siguientes

Desplace uno o más objetos al grupo de acceso.

Mover un grupo de escritorios o una granja a un grupo de acceso diferente

Después de crear un grupo de acceso, puede mover los grupos de escritorios automáticos, los grupos manuales o las granjas al nuevo grupo de acceso.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios** o **Recursos > Granjas**.
- 2 Seleccione un grupo o una granja.

- 3 Seleccione **Cambiar grupo de acceso** en el menú desplegable **Grupo de acceso** que aparece en el panel de ventana superior.
- 4 Seleccione el grupo de acceso y haga clic en **Aceptar**.

Horizon Administrator mueve el grupo al grupo de acceso que seleccionó.

Eliminar un grupo de acceso

Puede eliminar un grupo de acceso si no contiene ningún objeto. No puede eliminar el grupo de acceso raíz.

Requisitos previos

Si el grupo de acceso contiene objetos, mueva esos objetos a otro grupo de acceso o al grupo de acceso raíz. Consulte [Mover un grupo de escritorios o una granja a un grupo de acceso diferente](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Grupos de acceso**, seleccione el grupo de acceso y haga clic en **Eliminar grupo de acceso**.
- 3 Haga clic en **Aceptar** para eliminar el grupo de acceso.

Revisar las granjas o los grupos de escritorios o de aplicaciones de un grupo de acceso

Puede consultar las granjas o los grupos de escritorios o de aplicaciones que se encuentran en un grupo de acceso concreto de Horizon Administrator.

Procedimiento

- 1 En Horizon Administrator, diríjase a la página principal de los objetos.

Objeto	Acción
Grupos de escritorios	Seleccione Catálogo > Grupos de escritorios .
Grupos de aplicaciones	Seleccione Catálogo > Grupos de aplicaciones .
Granjas	Seleccione Recursos > Granjas .

De forma predeterminada, se muestran los objetos de todos los grupos de acceso.

- 2 Seleccione un grupo de acceso del menú desplegable **Grupo de acceso** que aparece en el panel de ventana principal.

Aparecen los objetos del grupo de acceso que seleccionó.

Revisar las máquinas virtuales de vCenter de un grupo de acceso

Puede ver las máquinas virtuales de vCenter de un grupo de acceso concreto de Horizon Administrator. Una máquina virtual de vCenter hereda el grupo de acceso de su grupo.

Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Máquinas**.

- 2 Seleccione la pestaña **Máquinas virtuales de vCenter**.

De forma predeterminada, se muestran las máquinas virtuales de vCenter de todos los grupos de acceso.

- 3 Seleccione un grupo de acceso en el menú desplegable **Agregar grupo de acceso**.

Aparecerán las máquinas virtuales de vCenter del grupo de acceso que seleccionó.

Administrar funciones personalizadas

Debe tener una licencia para usar la función de administración ThinApp en Horizon Administrator.

- [Agregar una función personalizada](#)

Si las funciones de administrador predefinidas no responden a sus necesidades, puede combinar privilegios específicos para crear sus propias funciones en Horizon Administrator.

- [Modificar los privilegios de una función personalizada](#)

Puede modificar los privilegios de una función personalizada. Sin embargo, no puede modificar las funciones de administrador predefinidas.

- [Eliminar una función personalizada](#)

Puede eliminar una función personalizada si no está incluida en un permiso. No puede eliminar las funciones de administrador predefinidas.

Agregar una función personalizada

Si las funciones de administrador predefinidas no responden a sus necesidades, puede combinar privilegios específicos para crear sus propias funciones en Horizon Administrator.

Requisitos previos

Familiarícese con los privilegios de administrador disponibles para crear funciones personalizadas. Consulte [Funciones y privilegios predefinidos](#).

Nota Cuando cree una función de administrador personalizada, los permisos globales no estarán disponibles para el administrador personalizado. Solo las funciones de administrador predefinidas tendrán permisos globales, lo que habilitará la gestión de autorizaciones globales en un entorno de Arquitectura de Cloud Pod.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.

- 2 En la pestaña **Funciones**, haga clic en **Agregar función**.

- 3 Escriba un nombre y una descripción para la función nueva, seleccione uno o más privilegios y haga clic en **Aceptar**.

La función nueva aparece en el panel izquierdo.

Modificar los privilegios de una función personalizada

Puede modificar los privilegios de una función personalizada. Sin embargo, no puede modificar las funciones de administrador predefinidas.

Requisitos previos

Familiarícese con los privilegios de administrador disponibles para crear funciones personalizadas. Consulte [Funciones y privilegios predefinidos](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Funciones**, seleccione la función.
- 3 Haga clic en **Privilegios** para mostrar los privilegios de la función y seleccione **Editar**.
- 4 Seleccione privilegios o anule su selección.
- 5 Haga clic en **Aceptar** para guardar los cambios.

Eliminar una función personalizada

Puede eliminar una función personalizada si no está incluida en un permiso. No puede eliminar las funciones de administrador predefinidas.

Requisitos previos

Si la función está incluida en un permiso, elimine el permiso. Consulte [Eliminar un permiso](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Funciones**, seleccione la función y haga clic en **Eliminar función**.

El botón **Eliminar función** no está disponible para las funciones predefinidas o para las funciones personalizadas que se incluyen en un permiso.

- 3 Haga clic en **Aceptar** para eliminar la función.

Funciones y privilegios predefinidos

Horizon Administrator incluye funciones predefinidas que puede asignar a sus grupos y usuarios administradores. También puede combinar privilegios seleccionados para crear sus propias funciones de administrador.

- **Funciones de administrador predefinidas**

Las funciones de administrador predefinidas combinan todos los privilegios individuales necesarios para realizar las tareas de administración habituales. Estas funciones no se pueden modificar.

- **Privilegios globales**

Los privilegios globales controlan las operaciones de todo el sistema, como ver y cambiar la configuración global. Las funciones que incluyen privilegios específicos de objeto no se pueden aplicar a grupos de acceso.

- **Privilegios específicos de objeto**

Los privilegios específicos de objeto controlan las operaciones de determinados tipos de objetos del inventario. Las funciones que incluyen privilegios específicos de objeto pueden aplicarse a grupos de acceso.

- **Privilegios internos**

Algunas de las funciones de administrador predefinidas contienen privilegios internos. No puede seleccionar los privilegios internos cuando crea funciones personalizadas.

Funciones de administrador predefinidas

Las funciones de administrador predefinidas combinan todos los privilegios individuales necesarios para realizar las tareas de administración habituales. Estas funciones no se pueden modificar.

Nota Asignar a los usuarios una combinación de funciones personalizadas o predefinidas puede proporcionarles acceso a operaciones que no se pueden llevar a cabo con funciones personalizadas o predefinidas individuales.

La siguiente tabla describe las funciones predefinidas e indica si se pueden aplicar a un grupo de acceso.

Tabla 6-6. Funciones predefinidas de Horizon Administrator

Función	Características del usuario	Se aplica a un grupo de acceso
Administradores	<p>Realizar todas las operaciones de administrador, que incluyen la creación de más grupos y usuarios administradores. En un entorno de arquitectura de Cloud Pod, los administradores que tengan esta función pueden configurar y gestionar una federación de pods, así como administrar sesiones de pods remotos.</p> <p>Los administradores que tengan la función Administradores en el grupo de acceso raíz son superusuarios porque tienen acceso completo a todos los objetos del inventario del sistema. Dado que esta función reúne todos los privilegios, debe asignarla a un número limitado de usuarios. Inicialmente, se asigna esta función a los miembros del grupo local de administradores del host del servidor de conexión en el grupo de acceso raíz.</p> <p>Importante Los administradores deben tener la función Administradores en el grupo de acceso raíz para realizar las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Agregar y eliminar grupos de acceso. ■ Administrar aplicaciones ThinApp y sus opciones de configuración en Horizon Administrator. ■ Usar los comandos vdmadmin, vdmimport y lmvutil. 	Sí
Administradores (solo lectura)	<ul style="list-style-type: none"> ■ Ver, pero no modificar, la configuración global y los objetos del inventario. ■ Ver, pero no modificar, las aplicaciones ThinApp y su configuración. ■ Ejecutar todos los comandos PowerShell y las utilidades de la línea de comandos, incluido vdmexport, pero no vdmadmin, vdmimport ni lmvutil. <p>En un entorno de arquitectura de Cloud Pod, los administradores que tienen esta función pueden ver los objetos del inventario y la configuración de la capa de datos global.</p> <p>Cuando los administradores tienen esta función en un grupo de acceso, solo pueden ver los objetos del inventario del mismo.</p>	Sí
Administradores de registro de agente	Registrar máquinas sin administrar, como sistemas físicos, máquinas virtuales independientes y hosts RDS.	No
Configuración global y administradores de directivas	Ver y modificar las directivas globales y las opciones de configuración, excepto los permisos y las funciones de administrador, las aplicaciones ThinApp y su configuración.	No
Configuración global y administradores de directivas (solo lectura)	Ver, pero no modificar, las directivas globales y las opciones de la configuración, excepto los permisos y las funciones de administrador, y las aplicaciones ThinApp junto con su configuración.	No

Tabla 6-6. Funciones predefinidas de Horizon Administrator (Continuación)

Función	Características del usuario	Se aplica a un grupo de acceso
Administradores del departamento de soporte técnico	<p>Realizar acciones de escritorios y de aplicaciones, como apagar, restablecer y reiniciar, y acciones de asistencia remota, como terminar procesos de escritorio o de aplicación de un usuario. Un administrador debe tener permisos en el grupo de acceso raíz para acceder a Horizon Help Desk Tool.</p> <ul style="list-style-type: none"> ■ Acceso de solo lectura a Horizon Help Desk Tool. ■ Administrar sesiones globales. ■ Se puede iniciar sesión en Horizon Administrator. ■ Ejecutar comandos relacionados con todas las máquinas y sesiones. ■ Administrar aplicaciones y procesos remotos. ■ Asistir de forma remota el escritorio virtual o el escritorio publicado. 	No
Administradores del departamento de soporte técnico (solo lectura)	<p>Ver la información de los usuarios y las sesiones, y poder conocer mejor los detalles de la sesión. Un administrador debe tener permisos en el grupo de acceso raíz para acceder a Horizon Help Desk Tool.</p> <ul style="list-style-type: none"> ■ Acceso de solo lectura a Horizon Help Desk Tool. ■ Se puede iniciar sesión en Horizon Administrator. 	No
Administradores de inventario	<ul style="list-style-type: none"> ■ Ejecutar todas las operaciones relacionadas con los grupos, las sesiones y las máquinas. ■ Administrar discos persistentes. ■ Resincronizar, actualizar y volver a equilibrar grupos de clones vinculados y cambiar la imagen de grupo predeterminada. <p>Cuando los administradores tienen esta función en un grupo de acceso, solo pueden realizar estas operaciones en los objetos del inventario del mismo.</p>	Sí
Administradores de inventario (solo lectura)	<p>Ver, pero no modificar, los objetos del inventario.</p> <p>Cuando los administradores tienen esta función en un grupo de acceso, solo pueden ver los objetos del inventario del mismo.</p>	Sí

Tabla 6-6. Funciones predefinidas de Horizon Administrator (Continuación)

Función	Características del usuario	Se aplica a un grupo de acceso
Administradores locales	<p>Realizar todas las operaciones de administrador local, excepto crear más grupos y usuarios administradores. En un entorno de arquitectura de Cloud Pod, los administradores que tienen esta función no pueden realizar operaciones en la capa de datos global ni administrar sesiones en pods remotos.</p> <p>Nota Los administradores con la función Administradores locales no pueden acceder a Horizon Help Desk Tool. Los administradores de un entorno que no sea CPA no pueden tener el privilegio Administrar sesiones globales, necesario para realizar tareas en Horizon Help Desk Tool.</p>	Sí
Administradores locales (solo lectura)	<p>Es igual que la función Administradores (solo lectura), pero no pueden ver los objetos del inventario ni la configuración en la capa de datos global. Los administradores que tienen esta función tienen derechos de solo lectura únicamente en el pod local.</p> <p>Nota Los administradores con la función Administradores locales (solo lectura) no pueden acceder a Horizon Help Desk Tool. Los administradores de un entorno que no sea CPA no pueden tener el privilegio Administrar sesiones globales, necesario para realizar tareas en Horizon Help Desk Tool.</p>	Sí

Privilegios globales

Los privilegios globales controlan las operaciones de todo el sistema, como ver y cambiar la configuración global. Las funciones que incluyen privilegios específicos de objeto no se pueden aplicar a grupos de acceso.

La siguiente tabla describe los privilegios globales y enumera las funciones predefinidas que contiene cada privilegio.

Tabla 6-7. Privilegios globales

Privilegio	Características del usuario	Funciones predefinidas
Interacción de consola	Inicie sesión y use Horizon Administrator.	Administradores Administradores (solo lectura) Administradores de inventario Administradores de inventario (solo lectura) Configuración global y administradores de directivas Configuración global y administradores de directivas (solo lectura) Administradores del departamento de soporte técnico Administradores del departamento de soporte técnico (solo lectura) Administradores locales Administradores locales (solo lectura)
Interacción directa	Ejecute todos los comandos PowerShell y las utilidades de la línea de comandos, excepto vdmadmin y vdmimport. Los administradores deben tener la función Administradores en el grupo de acceso raíz para usar los comandos vdmadmin, vdmimport y lmvutil.	Administradores Administradores (solo lectura)
Administrar configuración global y directivas	Vea y modifique las directivas globales y las opciones de la configuración, excepto los permisos y las funciones de administrador.	Administradores Configuración global y administradores de directivas
Administrar sesiones globales	Administre sesiones globales en un entorno de arquitectura Cloud Pod.	Administradores
Administrar funciones y permisos	Cree, modifique y elimine los permisos y las funciones de administrador.	Administradores
Registrar agente	Instale Horizon Agent en máquinas sin administrar, como sistemas físicos, máquinas virtuales independientes y hosts RDS. Durante la instalación de Horizon Agent, debe proporcionar las credenciales de inicio de sesión del administrador para registrar la máquina sin administrar con la instancia del servidor de conexión.	Administradores Administradores de registro de agente

Privilegios específicos de objeto

Los privilegios específicos de objeto controlan las operaciones de determinados tipos de objetos del inventario. Las funciones que incluyen privilegios específicos de objeto pueden aplicarse a grupos de acceso.

La siguiente tabla describe los privilegios específicos de objeto. Las funciones predeterminadas de Administradores y Administradores de inventario incluyen todos estos privilegios.

Tabla 6-8. Privilegios específicos de objeto

Privilegio	Características del usuario	Objeto
Habilitar granjas y grupos de aplicaciones y escritorios	Habilitar y deshabilitar grupos de escritorios.	Grupo de escritorios, granja
Autorizar grupos de escritorios y aplicaciones	Agregar y eliminar autorizaciones de usuario.	Grupo de escritorios, grupo de aplicación
Administrar la imagen de grupo de escritorios Composer	Resincronizar, actualizar y volver a equilibrar grupos de clones vinculados y cambiar la imagen de grupo predeterminada.	Grupo de escritorios
Administrar máquina	Ejecutar operaciones relacionadas con todas las máquinas y sesiones.	Máquina
Administrar discos persistentes	Ejecutar todas las operaciones de discos persistentes de View Composer, como conectar, desconectar e importar discos persistentes.	Disco persistente
Administrar granjas y grupos de aplicaciones y escritorios	Agregar, modificar y eliminar granjas. Agregar, eliminar y autorizar grupos de aplicaciones y escritorios. Agregar y eliminar máquinas.	Grupo de escritorios, grupo de aplicaciones, granja
Administrar sesiones	Desconectar y cerrar sesiones y enviar mensajes a usuarios.	Sesión
Administrar operación de reinicio	Restablecer las máquinas virtuales o reiniciar los escritorios virtuales.	Máquina

Privilegios internos

Algunas de las funciones de administrador predefinidas contienen privilegios internos. No puede seleccionar los privilegios internos cuando crea funciones personalizadas.

La siguiente tabla describe los privilegios internos y enumera las funciones predefinidas que contiene cada privilegio.

Tabla 6-9. Privilegios internos

Privilegio	Descripción	Funciones predefinidas
Completo (solo lectura)	Otorga acceso de solo lectura a toda la configuración.	Administradores (solo lectura)
Administrar inventario (solo lectura)	Otorga acceso de solo lectura a los objetos del inventario.	Administradores de inventario (solo lectura)
Administrar configuración global y directivas (solo lectura)	Otorga acceso de solo lectura a las opciones de configuración y las directivas globales excepto para las funciones y los administradores.	Configuración global y administradores de directivas (solo lectura)

Privilegios necesarios para las tareas comunes

Muchas tareas comunes de administración necesitan un conjunto coordinado de privilegios. Además, algunas operaciones necesitan permiso en el grupo de acceso raíz para acceder al objeto con el que se está trabajando.

Privilegios para administrar grupos

Los administradores deben tener ciertos privilegios para administrar los grupos de Horizon Administrator.

La siguiente tabla muestra las tareas comunes para administrar grupos, así como los privilegios necesarios para realizar cada tarea.

Tabla 6-10. Privilegios y tareas para administrar los grupos

Tarea	Privilegios necesarios
Habilitar o deshabilitar un grupo de escritorios	Habilitar granjas y grupos de aplicaciones y escritorios
Autorizar o eliminar una autorización de usuarios a un grupo	Autorizar grupos de escritorios y aplicaciones
Agregar un grupo	Administrar granjas y grupos de aplicaciones y escritorios
Modificar o eliminar un grupo	Administrar granjas y grupos de aplicaciones y escritorios
Agregar o eliminar escritorios de un grupo	Administrar granjas y grupos de aplicaciones y escritorios
Actualizar, recomponer, volver a equilibrar o cambiar la imagen de View Composer predeterminada	Administrar la imagen de grupo de escritorios Composer
Cambiar grupos de acceso	Administrar granjas y grupos de aplicaciones y escritorios en los grupos de acceso de origen y de destino.

Privilegios para administrar máquinas

Los administradores deben tener ciertos privilegios para administrar las máquinas de Horizon Administrator.

La siguiente tabla muestra tareas comunes para administrar máquinas, así como los privilegios necesarios para realizar cada tarea.

Tabla 6-11. Privilegios y tareas para administrar las máquinas

Tarea	Privilegios necesarios
Eliminar una máquina virtual	Administrar máquina
Restablecer una máquina virtual	Administrar operación de reinicio
Reiniciar un escritorio virtual	Administrar operación de reinicio
Asignar o eliminar la propiedad del usuario	Administrar máquina
Activar el modo de mantenimiento o salir de él	Administrar máquina
Desconectar o cerrar las sesiones	Administrar sesiones

Privilegios para administrar discos persistentes

Los administradores deben tener ciertos privilegios para administrar los discos persistentes de Horizon Administrator.

La siguiente tabla muestra las tareas comunes para administrar discos persistentes, así como los privilegios necesarios para realizar cada tarea. Realice estas tareas en la página Discos persistentes de Horizon Administrator.

Tabla 6-12. Privilegios y tareas para administrar los discos persistentes

Tarea	Privilegios necesarios
Desconectar un disco	Administrar discos persistentes en el disco y Administrar granjas y grupos de aplicaciones y escritorios en el grupo.
Conectar un disco	Administrar discos persistentes en el disco y Administrar granjas y grupos de aplicaciones y escritorios en el equipo.
Editar un disco	Administrar discos persistentes en el disco y Administrar granjas y grupos de aplicaciones y escritorios en el grupo seleccionado.
Cambiar grupos de acceso	Administrar discos persistentes en los grupos de acceso de origen y de destino.
Volver a crear un escritorio	Administrar discos persistentes en el disco y Administrar granjas y grupos de aplicaciones y escritorios en el último grupo.
Importar desde vCenter	Administrar discos persistentes en la carpeta y Administrar grupo en el grupo.
Eliminar un disco	Administrar discos persistentes en el disco.

Privilegios para administrar los usuarios y los administradores

Los administradores deben tener ciertos privilegios para administrar usuarios y administradores de Horizon Administrator.

La siguiente tabla muestra las tareas comunes para administrar los usuarios y los administradores, así como los privilegios necesarios para realizar cada tarea. Debe administrar los usuarios en la página Usuarios y grupos de Horizon Administrator y los administradores en la página View de administradores globales de Horizon Administrator.

Tabla 6-13. Privilegios y tareas para administrar usuarios y administradores

Tarea	Privilegios necesarios
Actualizar la información general del usuario	Administrar configuración global y directivas
Enviar mensajes a los usuarios	Administrar sesiones remotas en la máquina.
Agregar un grupo o un usuario administrador	Administrar funciones y permisos
Agregar, modificar o eliminar un permiso de administrador	Administrar funciones y permisos
Agregar, modificar o eliminar una función de administrador	Administrar funciones y permisos

Privilegios para las tareas de Horizon Help Desk Tool

Los administradores de Horizon Help Desk Tool deben tener ciertos privilegios para realizar tareas de solución de problemas en Horizon Administrator.

La siguiente tabla muestra las tareas comunes que el administrador de Horizon Help Desk Tool puede realizar, así como los privilegios necesarios para realizar cada tarea.

Tabla 6-14. Privilegios y tareas de Horizon Help Desk Tool

Tareas	Privilegios necesarios
Acceso de solo lectura a Horizon Help Desk Tool.	Administrar el departamento de soporte técnico (solo lectura)
Administrar sesiones globales.	Administrar sesiones globales
Se puede iniciar sesión en Horizon Administrator.	Interacción de consola
Ejecutar comandos relacionados con todas las máquinas y sesiones.	Administrar máquina
Restablecer o reiniciar las máquinas.	Administrar operación de reinicio
Desconectar y cerrar las sesiones.	Administrar sesiones
Administrar aplicaciones y procesos remotos.	Administrar aplicaciones y procesos remotos
Asistir de forma remota el escritorio virtual o el escritorio publicado.	Asistencia remota
Operaciones para desconectar, cerrar sesión, restablecer y reiniciar las sesiones globales.	Administrar el departamento de soporte técnico (solo lectura) y Administrar sesiones globales
Operaciones para restablecer y reiniciar sesiones locales.	Administrar el departamento de soporte técnico (solo lectura) y Administrar operación de reinicio
Operaciones de asistencia remota.	Administrar el departamento de soporte técnico (solo lectura) y Asistencia remota
Cierra aplicaciones y finaliza procesos remotos.	Administrar el departamento de soporte técnico (solo lectura) y Administrar aplicaciones y procesos remotos
Realice todas las tareas en Horizon Help Desk Tool.	Administrar el departamento de soporte técnico (solo lectura), Administrar sesiones globales, Administrar operación de reinicio, Asistencia remotay Administrar aplicaciones y procesos remotos
Se realizan operaciones de asistencia remota, se cierran las aplicaciones y se finalizan los procesos.	Administrar el departamento de soporte técnico (solo lectura), Asistencia remotay Administrar aplicaciones y procesos remotos
Operaciones para desconectar y cerrar sesión sesiones locales.	Administrar el departamento de soporte técnico (solo lectura) y Administrar sesiones

Privilegios para los comandos y las tareas de administración general

Los administradores deben tener algunos privilegios para realizar tareas de administración general y ejecutar las utilidades de la línea de comandos.

La siguiente tabla muestra los privilegios necesarios para realizar tareas de administración general y ejecutar las utilidades de la línea de comandos.

Tabla 6-15. Privilegios para los comandos y las tareas de administración general

Tarea	Privilegios necesarios
Agregar o eliminar un grupo de acceso	Debe tener la función Administrador en el grupo de acceso raíz.
Administrar las aplicaciones ThinApp y su configuración en Horizon Administrator	Debe tener la función Administrador en el grupo de acceso raíz.
Instalar Horizon Agent en una máquina sin administrar, como un sistema físico, una máquina virtual independiente o un host RDS	Registrar agente
Ver o modificar las opciones de configuración (excepto para los administradores) en Horizon Administrator	Administrar configuración global y directivas
Ejecute todos los comandos PowerShell y las utilidades de la línea de comandos excepto vdmadmin y vdmimport.	Interacción directa
Usar los comandos vdmadmin y vdmimport	Debe tener la función Administrador en el grupo de acceso raíz.
Usar el comando vdmexport	Debe tener la función Administradores o la función Administradores (solo lectura) en el grupo de acceso raíz.

Prácticas recomendadas para grupos y usuarios administradores

Para aumentar la seguridad y la facilidad de administración de su entorno de Horizon 7, debe seguir las prácticas recomendadas para administrar grupos y usuarios administradores.

- Cree nuevos grupos de usuarios en Active Directory y asígneles funciones administrativas. Evite usar grupos integrados de Windows u otros grupos existentes que puedan incluir usuarios que no necesiten o no debieran tener privilegios de Horizon 7.
- Mantenga al mínimo el número de usuarios con privilegios administrativos de Horizon 7.
- Puesto que la función de administradores posee todos los privilegios, no debe utilizarse para una administración corriente.
- Evite usar el nombre Administrador al crear grupos y usuarios administradores, ya que es muy visible y se adivina con facilidad.
- Cree grupos de acceso para segregar escritorios y granjas sensibles. Delegue la administración de dichos grupos de acceso a un número limitado de usuarios.
- Cree administradores independientes que puedan modificar las directivas globales y la configuración de Horizon 7.

Configurar directivas en Horizon Administrator y en Active Directory

7

Puede usar Horizon Administrator si desea configurar directivas para las sesiones cliente. Puede configurar las opciones de la directiva de grupo de Active Directory para controlar el comportamiento del servidor de conexión de View, el protocolo de visualización PCoIP, el registro de Horizon 7 y las alarmas de rendimiento.

También puede configurar las opciones de la directiva de grupo de Active Directory para controlar el comportamiento de Horizon Agent, de Horizon Client para Windows, de Horizon Persona Management y de algunas funciones. Para obtener más información sobre la configuración de estas directivas, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Establecer directivas en Horizon Administrator](#)
- [Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7](#)

Establecer directivas en Horizon Administrator

Horizon Administrator permite configurar directivas para las sesiones de cliente.

Puede establecer estas directivas para que afecten a usuarios específicos, a grupos de escritorios específicos o a todos los usuarios de las sesiones de cliente. Las directivas que afectan a grupos de escritorios y usuarios específicos se denominan directivas de nivel de usuario y directivas de nivel de grupo. Las directivas que afectan a todas las sesiones y usuarios se denominan directivas globales.

Las directivas de nivel de usuario heredan la configuración de las directivas de nivel de grupo. De forma similar, las directivas de nivel de grupo de escritorio heredan la configuración de las directivas globales equivalentes. La configuración de la directiva de nivel de escritorio tiene preferencia sobre la configuración de la directiva global equivalente. La configuración de la directiva de nivel de usuario tiene preferencia sobre la configuración de la directiva global equivalente y la directiva de nivel de grupo de escritorios.

La configuración de la directiva de nivel inferior puede ser más o menos restrictiva que la configuración de nivel superior equivalente. Por ejemplo, puede establecer una directiva global en **Denegar** y la directiva equivalente de nivel del grupo de escritorios en **Permitir** o viceversa.

Nota Solo las directivas globales están disponibles para los grupos de aplicaciones y los escritorios publicados. No puede establecer directivas de nivel de usuario ni de nivel de grupo para los grupos de aplicaciones y los escritorios publicados.

- [Configurar las opciones de la directiva global](#)

Puede configurar directivas globales a fin de controlar el comportamiento de todos los usuarios de sesiones cliente.

- [Configurar directivas para los grupos de escritorios](#)

Puede configurar directivas en el nivel de escritorios para que afecten a grupos de escritorios específicos. La configuración de las directivas en el nivel de escritorios tiene preferencia sobre la configuración de directivas global equivalente.

- [Configurar directivas para los usuarios](#)

Puede configurar directivas en el nivel de usuarios para que afecten a usuarios específicos. La configuración de la directiva a nivel de usuario siempre tiene preferencia ante la configuración de directivas global equivalente y las directivas en el nivel de grupo de escritorios.

- [Directivas de Horizon 7](#)

Puede configurar las directivas de Horizon 7 para que afecten a todas las sesiones de cliente, o bien puede aplicarlas para que afecten a usuarios o grupos de escritorios específicos.

Configurar las opciones de la directiva global

Puede configurar directivas globales a fin de controlar el comportamiento de todos los usuarios de sesiones cliente.

Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Directivas > Directivas globales**.
- 2 Haga clic en **Editar directivas** en el panel **Directivas de View**.
- 3 Haga clic en **Aceptar** para guardar los cambios.

Configurar directivas para los grupos de escritorios

Puede configurar directivas en el nivel de escritorios para que afecten a grupos de escritorios específicos. La configuración de las directivas en el nivel de escritorios tiene preferencia sobre la configuración de directivas global equivalente.

Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.

- 2 Haga doble clic en el ID del grupo de escritorios y haga clic en la pestaña **Directivas**.

La pestaña **Directivas** muestra la configuración de directivas actual. Cuando se hereda una opción de la directiva global equivalente, **Heredada** aparece en la columna **Directiva del grupo de escritorios**.

- 3 Haga clic en **Editar directivas** en el panel **Directivas de View**.
- 4 Haga clic en **Aceptar** para guardar los cambios.

Configurar directivas para los usuarios

Puede configurar directivas en el nivel de usuarios para que afecten a usuarios específicos. La configuración de la directiva a nivel de usuario siempre tiene preferencia ante la configuración de directivas global equivalente y las directivas en el nivel de grupo de escritorios.

Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo de escritorios y haga clic en la pestaña **Directivas**.
La pestaña **Directivas** muestra la configuración de directivas actual. Cuando se hereda una opción de la directiva global equivalente, **Heredada** aparece en la columna **Directiva del grupo de escritorios**.
- 3 Haga clic en **Reemplazos del usuario** y, a continuación, en **Agregar usuario**.
- 4 Para buscar un usuario, haga clic en **Agregar**, escriba el nombre o la descripción del usuario y, a continuación, haga clic en **Buscar**.
- 5 Seleccione uno o varios usuarios de la lista, haga clic en **Aceptar** y, a continuación, en **Siguiente**.
Aparece el cuadro de diálogo Agregar directiva individual.
- 6 Configure las directivas de Horizon y haga clic en **Finalizar** para guardar los cambios.

Directivas de Horizon 7

Puede configurar las directivas de Horizon 7 para que afecten a todas las sesiones de cliente, o bien puede aplicarlas para que afecten a usuarios o grupos de escritorios específicos.

La siguiente tabla describe cada opción de configuración de la directiva de Horizon 7.

Tabla 7-1. Directivas de Horizon

Directiva	Descripción
Redireccionamiento multimedia (MMR)	<p>Determina si MMR está habilitado para los sistemas cliente.</p> <p>MMR es un filtro de Windows Media Foundation que reenvía datos multimedia desde códecs específicos que se encuentran en escritorios remotos directamente a través de un socket TCP al sistema cliente. Los datos se descodifican directamente en el sistema cliente, donde se reproducen.</p> <p>El valor predeterminado es Denegar.</p> <p>Si los sistemas cliente no tienen recursos suficientes para administrar la descodificación multimedia local, mantenga la opción como Denegar.</p> <p>Los datos del redireccionamiento multimedia (MMR) se envían a través de la red sin cifrado basado en las aplicaciones y pueden contener datos confidenciales, dependiendo del contenido que se redirija. Para asegurarse de que esta información no se supervise en la red, use MMR únicamente en una red segura.</p>
Acceso USB	<p>Determina si los escritorios remotos pueden usar los dispositivos USB conectados al sistema cliente.</p> <p>El valor predeterminado es Permitir. Para evitar el uso de dispositivos externos por seguridad, cambie la opción a Denegar.</p>
Aceleración de hardware PCoIP	<p>Determina si desea habilitar la aceleración del hardware del protocolo de visualización PCoIP y especifica la prioridad de aceleración que está asignada a la sesión del usuario de PCoIP.</p> <p>Esta opción solo tiene efecto si el dispositivo de aceleración del hardware PCoIP se encuentra en el equipo físico que aloja el escritorio remoto.</p> <p>El valor predeterminado es Permitir con la prioridad Media.</p>

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.

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.

Archivos de plantilla ADMX de Horizon 7

Los archivos de plantilla ADMX de Horizon 7 proporcionan una configuración de directiva de grupo que le permite controlar y optimizar los componentes de Horizon 7.

Los archivos ADMX están disponibles en VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip, que puede descargarse desde el sitio de descargas de VMware:

<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.

Tabla 7-2. Archivos de plantilla ADMX de Horizon

Nombre de plantilla	Archivo de plantilla	Descripción
Configuración de VMware View Agent	vdm_agent.admx	<p>Contiene la configuración de las directivas relacionada con los componentes de entorno y de autenticación de Horizon Agent.</p> <p>Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>
Configuración de VMware Horizon Client	vdm_client.admx	<p>Contiene la configuración de las directivas relacionada con Horizon Client para Windows.</p> <p>Los clientes que se conectan desde fuera del dominio del host del servidor de conexión no se ven afectados por las directivas que se aplican a Horizon Client.</p> <p>Consulte el documento <i>Guía de instalación y configuración de VMware Horizon Client para Windows</i>.</p>
Redireccionamiento URL de VMware Horizon	urlRedirection.admx	<p>Contiene la configuración de las directivas relacionada con la función de redireccionamiento de contenido URL. Si agrega esta plantilla a un GPO para un grupo de aplicaciones o de escritorios remotos, algunos vínculos URL a los que se hacen clic dentro de las aplicaciones o los escritorios remotos se pueden redireccionar a un cliente basado en Windows y se pueden abrir en un navegador del cliente.</p> <p>Si agrega esta plantilla en una GPO del cliente, cuando un usuario hace clic en ciertos vínculos URL en un sistema cliente basado en Windows, la URL se puede abrir en una aplicación o un escritorio remotos.</p> <p>Consulte los documentos <i>Configurar funciones de escritorios remotos en Horizon 7</i> y <i>Guía de instalación y configuración de VMware Horizon Client para Windows</i>.</p>

Tabla 7-2. Archivos de plantilla ADMX de Horizon (Continuación)

Nombre de plantilla	Archivo de plantilla	Descripción
Configuración común de VMware View Server	vdm_server.admx	Contiene la configuración de las directivas relacionadas con el servidor de conexión.
Configuración común de VMware View Agent	vdm_common.admx	Contiene la configuración de las directivas que son comunes a todos los componentes de Horizon.
Variables de las sesiones PCoIP	pcoip.admx	Contiene la configuración de directivas relacionada con el protocolo de visualización PCoIP. Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
Variables de las sesiones del cliente PCoIP	pcoip.client.admx	Contiene la configuración de las directivas relacionada con el protocolo de visualización PCoIP que afecta a Horizon Client para Windows. Consulte el documento <i>Guía de instalación y configuración de VMware Horizon Client para Windows</i> .
Administración de identidades	ViewPM.admx	Contiene la configuración de directivas relacionadas con Horizon Persona Management. Consulte el documento <i>Configurar escritorios virtuales en Horizon 7</i> .
Redireccionamiento de impresión virtual de VMware	printerRedirection.admx	Contiene la configuración de directivas para deshabilitar la impresión basada en ubicación, deshabilitar la persistencia de la configuración de impresión y seleccionar el controlador de una impresora cliente redireccionada.
Impresión basada en ubicación	LBP.xml	Plantilla para definir las reglas de traducción para cada impresora basada en ubicación para la impresión virtual de VMware.
Servicios de Escritorio remoto	vmware_rdsh_server.admx	Contiene la configuración de las directivas relacionadas con los Servicios de Escritorio remoto. Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
Configuración de audio/vídeo en tiempo real de View	vdm_agent_rtav.admx	Contiene la configuración de las directivas relacionada con las cámaras web que se usan con la función Audio/vídeo en tiempo real. Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
Redireccionamiento de escáner	vdm_agent_scanner.admx	Contiene la configuración de las directivas relacionadas con dispositivos de escáner que se redireccionan para usarlos en aplicaciones y dispositivos publicados. Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .

Tabla 7-2. Archivos de plantilla ADMX de Horizon (Continuación)

Nombre de plantilla	Archivo de plantilla	Descripción
COM serie	vdm_agent_serialport.admx	Contiene la configuración de las directivas relacionadas con los puertos (COM) serie que se redireccionan para usarlos en escritorios virtuales. Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
Redireccionamiento de impresora de VMware Horizon	vdm_agent_printing.admx	Contiene la configuración de directiva relacionada con el filtrado de impresoras redireccionadas. Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
View Agent Direct-Connection	view_agent_direct_connection.admx	Contiene la configuración de directiva relativa al complemento View Agent Direct-Connection. Consulte el documento <i>Administración del complemento View Agent Direct-Connection</i> .
VMware Horizon Performance Tracker	perf_tracker.admx	Contiene la configuración de la directiva relativa a la función VMware Horizon Performance Tracker. Consulte Usar VMware Horizon Performance Tracker .

Opciones de las plantillas ADMX de configuración del servidor de conexión de Horizon

Los archivos de plantillas ADMX de configuración de View Server (vdm_server.admx) incluyen la configuración de la directiva relacionada con todos los servidores de conexión de Horizon.

La siguiente tabla describe cada opción de las directivas del archivo de plantilla ADMX de configuración del servidor de conexión. La plantilla contiene únicamente las opciones de Configuración del equipo.

Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración del servidor de VMware View** en el Editor de administración de directivas de grupo.

Tabla 7-3. Opciones de la plantilla de configuración de Horizon Server

Configuración	Propiedades
Enumerate Forest Trust Child Domains	<p>Determina si se enumeran todos los dominios de confianza del dominio en el que se encuentra el servidor. Para establecer una cadena completa de confianza, los dominios en los que confían cada dominio de confianza también se enumeran y el proceso continúa recursivamente hasta que se detectan todos los dominios de confianza. Esta información se envía al servidor de conexión para garantizar que todos los dominios de confianza estén disponibles cuando el cliente inicia sesión.</p> <p>Esta propiedad está habilitada de forma predeterminada. Cuando está deshabilitada, solo se enumeran los dominios de confianza directamente y no se establece la conexión a los controladores de dominios remotos.</p> <p>Nota En entornos con relaciones de dominio complejas, como las que usan varias estructuras de bosques con dominios de confianza entre dominios, el proceso puede durar varios minutos en completarse.</p>
Recursive Enumeration of Trusted Domains	<p>Determina si se enumeran todos los dominios de confianza del dominio en el que se encuentra el servidor. Para establecer una cadena completa de confianza, los dominios en los que confían cada dominio de confianza también se enumeran y el proceso continúa recursivamente hasta que se detectan todos los dominios de confianza. Esta información se envía al servidor de conexión de View para que todos los dominios de confianza estén disponibles cuando el cliente inicia sesión.</p> <p>Esta configuración está habilitada de forma predeterminada. Cuando está deshabilitada, solo se enumeran los dominios de confianza directamente y no se establece la conexión a los controladores de dominios remotos.</p> <p>En entornos con relaciones de dominio complejas, como las que usan varias estructuras de bosques con dominios de confianza entre dominios, este proceso puede durar varios minutos en completarse.</p>
Windows Password Authentication Mode	<p>Seleccione el modo de autenticación de contraseñas para Windows.</p> <ul style="list-style-type: none"> ■ KerberosOnly. Autenticar con Kerberos. ■ KerberosWithFallbackToNTLM. Autenticar con Kerberos pero, en caso de fallo, utilizar NTLM. ■ Legacy. Autenticar con NTLM pero, en caso de fallo, utilizar Kerberos. Se utiliza para dar soporte a controladores de dominio NT heredados. <p>El valor predeterminado es KerberosOnly.</p>

Opciones de la plantilla ADMX de configuración común de Horizon 7

Los archivos de las plantillas ADMX de configuración común (vdm_common.admx) de Horizon 7 incluyen la configuración de la directiva común para todos los componentes de Horizon. Estas plantillas contienen únicamente las opciones de Configuración del equipo.

Opciones de configuración del registro

La siguiente tabla describe la opción de las directivas de configuración del registro de los archivos de plantilla ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View > Configuración de registro** del Editor de administración de directivas de grupo.

Tabla 7-4. Plantilla de configuración común de View: opciones de configuración de registro

Configuración	Propiedades
Number of days to keep production logs	Especifica el número de días durante los cuales los archivos de registro se mantienen en el sistema. Si no se establece ningún valor, se aplica el valor predeterminado y los archivos de registro se mantienen durante siete días.
Maximum number of debug logs	Especifica el número máximo de archivos de registro de depuración que se mantienen en el sistema. Cuando un archivo de registro alcanza su tamaño máximo, no se agregan más entradas y se crea un nuevo archivo de registro. Cuando el número de archivos de registro previos alcanza este valor, se elimina el archivo más antiguo.
Maximum debug log size in Megabytes	Especifica el tamaño máximo en megabytes que un registro de depuración puede alcanzar después de que se cierre el archivo de registro y se cree uno nuevo.
Log Directory	Especifica la ruta completa al directorio de los archivos de registro. Si no se puede escribir en la ubicación, se usa la predeterminada. Para los archivos de registro cliente, se crea un directorio adicional con el nombre del cliente.
Send logs to a Syslog server	<p>Permite que se envíen los registros de View Server a un servidor syslog como VMware vCenter Log Insight. Los registros se envían desde todos los View Servers de la OU o del dominio en el que está configurado este GPO. Puede enviar los registros de Horizon Agent a un servidor syslog si habilita esta opción en una GPO que esté vinculada a una OU que contenga el escritorio.</p> <p>Para enviar los datos de registro a un servidor syslog, habilite esta opción y especifique el nivel de registro y el nombre de dominio completo (FQDN) del servidor o la dirección IP. Puede especificar un puerto alternativo si no desea usar el puerto 514 predeterminado. Separe cada elemento de la especificación con una barra vertical (). Utilice la siguiente sintaxis:</p> <p>Nivel de registro FQDN o IP del servidor [Número de puerto(514 predeterminado)]</p> <p>Por ejemplo: Depuración 192.0.2.2</p> <p>Importante Los datos de syslog se envían a través de la red sin el cifrado basado en software. Como los registros de View Server pueden contener datos personales, evite enviar datos syslog en una red que no sea segura. Si es posible, use la seguridad de nivel de vínculo como IPsec para evitar la posibilidad de que se supervisen estos datos en la red.</p>

Configuración de las alarmas de rendimiento

Tabla 7-5 describe la configuración de las alarmas de rendimiento de los archivos de plantilla ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View > Alarmas de rendimiento** del Editor de administración de directivas de grupo.

Tabla 7-5. Plantilla de configuración común de View: configuración de las alarmas de rendimiento

Configuración	Propiedades
CPU and Memory Sampling Interval in Seconds	Especifica la CPU y la CPU del intervalo de sondeo de la memoria. Un bajo intervalo de muestreo puede provocar un nivel elevado de salida del registro.
Overall CPU usage percentage to issue log info	Especifica el umbral al que se registra el uso de la CPU general del sistema. Cuando están disponibles varios procesadores, este porcentaje representa el uso combinado.
Overall memory usage percentage to issue log info	Especifica el umbral al que se registra el uso general de la memoria del sistema asignada. La memoria asignada del sistema es la memoria que se asignó a través de procesos y a la que el sistema operativo asignó memoria física o una ranura de página en el archivo de paginación.
Process CPU usage percentage to issue log info	Especifica el umbral al que se registra el uso de CPU de cualquier proceso individual.
Process memory usage percentage to issue log info	Especifica el umbral al que se registra el uso de la memoria de cualquier proceso individual.
Process to check, comma separated name list allowing wild cards and exclusion	<p>Especifica una lista de consultas separada por comas que corresponde al nombre de uno o más procesos que se deben examinar. Puede filtrar la lista usando caracteres comodines dentro de cada consulta.</p> <ul style="list-style-type: none"> ■ Un asterisco (*) coincide con cero o más caracteres. ■ Un signo de interrogación (?) coincide exactamente con un carácter. ■ Un signo de exclamación (!) al comienzo de una consulta excluye todos los resultados de dicha consulta. <p>Por ejemplo, la siguiente consulta selecciona todos los procesos que comienzan por ws y excluye todos los procesos que acaban con sys:</p> <pre>'!*sys,ws*'</pre>

Nota La configuración de la alarma de rendimiento se aplica únicamente a los sistemas Horizon Agent y al servidor de conexión de Horizon. No se aplican a los sistemas Horizon Client.

Configuración de seguridad

Tabla 7-6 describe la configuración de seguridad de los archivos de plantilla ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View > Configuración de seguridad** del Editor de administración de directivas de grupo.

Tabla 7-6. Plantilla de configuración común de View: configuración de seguridad

Configuración	Propiedades
Only use cached revocation URLs	<p>La comprobación de revocación de certificados accederá únicamente a las URL en caché.</p> <p>El valor predeterminado, si no está configurado, es false.</p>
Revocation URL check timeout milliseconds	<p>El tiempo de espera acumulado en todas las recuperaciones de filtrado de URL de revocación en milisegundos.</p> <p>Si el valor no está configurado o está establecido en 0, esto significa que se utiliza la manipulación predeterminada de Microsoft.</p>
Type of certificate revocation check	<p>Seleccione el tipo de comprobación de revocación de certificados que se va a realizar:</p> <ul style="list-style-type: none"> ■ Ninguna ■ EndCertificateOnly ■ WholeChain ■ WholeChain <p>El valor predeterminado es WholeChainButRoot.</p>

Configuración general

[Tabla 7-7](#) describe la configuración general de los archivos de plantilla ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View** en el Editor de administración de directivas de grupo.

Tabla 7-7. Plantilla de configuración común de View: configuración general

Configuración	Propiedades
Disk threshold for log and events in Megabytes	<p>Especifica el umbral mínimo de espacio de disco restante para los registros y los eventos. Si no se especifica ningún valor, el predeterminado es 200.</p> <p>Cuando se alcanza el valor especificado, se detiene el registro de eventos.</p>
Enable extended logging	<p>Determina si los eventos de depuración y de seguimiento se incluyen en los archivos de registro.</p>
Override the default View Windows event generation	<p>Se admiten los siguientes valores:</p> <ul style="list-style-type: none"> ■ 0 = solo se generan entradas del registro de eventos para los eventos de View (no se generan entradas del registro de eventos para los mensajes de registro) ■ 1 = se generan entradas del registro de eventos en el modo de compatibilidad 4.5 (y versiones anteriores). No se generan entradas del registro de eventos para los eventos de View estándar. Las entradas del registro de eventos se basan exclusivamente en el texto del archivo de registro. ■ 2 = se generan entradas del registro de eventos en el modo de compatibilidad 4.5 (y versiones anteriores) con eventos de View incluidos.

Mantenimiento de los componentes de Horizon 7

8

Para mantener los componentes de Horizon 7 disponibles y en ejecución, puede realizar varias tareas de mantenimiento.

Este capítulo incluye los siguientes temas:

- [Realizar una copia de seguridad y restaurar los datos de configuración de Horizon 7](#)
- [Supervisar los componentes de Horizon 7](#)
- [Supervisar el estado de las máquinas](#)
- [Comprender los servicios de Horizon 7](#)
- [Cambiar la clave de licencia del producto](#)
- [Supervisar la licencia y el uso del producto](#)
- [Actualizar la información general del usuario desde Active Directory](#)
- [Migrar View Composer a otro equipo](#)
- [Actualizar los certificados en una instancia del servidor de conexión, en el servidor de seguridad o en View Composer](#)
- [Programa de mejora de la experiencia de cliente de VMware](#)

Realizar una copia de seguridad y restaurar los datos de configuración de Horizon 7

Para hacer una copia de seguridad de los datos de configuración de Horizon 7 y de View Composer, programe o ejecute copias de seguridad automáticas en Horizon Administrator. Para restaurar la configuración de Horizon 7, importe de forma manual los archivos de la copia de seguridad de LDAP de View y los archivos de la base de datos de View Composer.

Puede usar las funciones de restauración y de copia de seguridad para conservar y migrar los datos de configuración de Horizon 7.

Realizar una copia de seguridad de los datos del servidor de conexión de Horizon y de View Composer

Después de completar la configuración inicial del servidor de conexión, debe programar copias de seguridad periódicas de los datos de la configuración de View Composer y de Horizon 7. Puede conservar los datos de View Composer y de Horizon 7 usando Horizon Administrator.

Horizon 7 almacena los datos de configuración del servidor de conexión en el repositorio de LDAP de View. View Composer almacena datos de configuración para los escritorios de clones vinculados en la base de datos de View Composer.

Cuando utiliza Horizon Administrator para realizar copias de seguridad, Horizon 7 realiza una copia de seguridad de los datos de configuración de LDAP de View y la base de datos de View Composer. Ambos conjuntos de archivos de copias de seguridad se almacenan en la misma ubicación. Los datos de LDAP de View se exportan en formato de intercambio de datos LDAP (LDIF) cifrado. Para obtener una descripción de LDAP de View, consulte [Directorio LDAP de View](#).

Puede realizar copias de seguridad siguiendo varios procedimientos.

- Programe copias de seguridad automáticas usando la función de copia de seguridad de la configuración de Horizon 7.
- Inicie una copia de seguridad en el momento usando la función **Hacer copia de seguridad ahora** de Horizon Administrator.
- Exporte de forma manual los datos LDAP de View usando la utilidad `vdmexport`. Esta utilidad se proporciona con cada instancia del servidor de conexión.

La utilidad `vdmexport` puede exportar los datos LDAP de View como datos LDIF cifrados, texto sin formato o texto sin formato con contraseñas y otra información confidencial eliminada.

Nota La herramienta `vdmexport` solo realiza la copia de seguridad de los datos LDAP de View. Esta herramienta no hace copias de seguridad de la información de la base de datos de View Composer.

Para obtener más información sobre `vdmexport`, consulte [Exportar los datos de configuración del servidor de conexión de Horizon](#).

Las siguientes instrucciones se aplican a las copias de seguridad de los datos de configuración de Horizon 7:

- Horizon 7 puede exportar los datos de configuración desde cualquier instancia del servidor de conexión.
- Si cuenta con varias instancias del servidor de conexión en un grupo replicado, solo es necesario que exporte la información desde una instancia. Todas las instancias replicadas contienen los mismos datos de configuración.

- No utilice las instancias replicadas del servidor de conexión como mecanismo de copia de seguridad. Cuando Horizon 7 sincroniza los datos en instancias replicadas del servidor de conexión, los datos que se pierdan en una instancia se pueden perder en todos los miembros del grupo.
- Si el servidor de conexión usa varias instancias de vCenter Server con varios servicios de Composer, Horizon 7 realiza una copia de seguridad de todas las bases de datos de View Composer asociadas a las instancias de vCenter Server.

Programar copias de seguridad de la configuración de Horizon 7

Puede programar que se realicen copias de seguridad de los datos de la configuración de Horizon 7 a intervalos regulares. Horizon 7 realiza copias de seguridad de los contenidos de los repositorios LDAP de View en los que las instancias del servidor de conexión almacenan los datos de configuración.

Puede realizar una copia de seguridad de la configuración inmediatamente si selecciona la instancia del servidor de conexión y hace clic en **Hacer copia de seguridad ahora**.

Requisitos previos

Familiarícese con la configuración de copia de seguridad. Consulte [Opciones de copia de seguridad de la configuración de Horizon 7](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión de la que desee hacer la copia de seguridad y haga clic en **Editar**.
- 3 En la pestaña **Copia de seguridad**, especifique las opciones de la copia de seguridad de la configuración de Horizon 7 para establecer la frecuencia de las copias de seguridad, el número máximo y la ubicación de la carpeta de los archivos de la copia de seguridad.
- 4 (opcional) Cambie la contraseña de recuperación de datos.
 - a Haga clic en **Cambiar contraseña de Data Recovery**.
 - b Escriba y vuelva a escribir la nueva contraseña.
 - c (opcional) Escriba un recordatorio de contraseña.
 - d Haga clic en **Aceptar**.
- 5 Haga clic en **Aceptar**.

Opciones de copia de seguridad de la configuración de Horizon 7

Horizon 7 puede realizar una copia de seguridad de los datos de configuración del servidor de conexión y de View Composer en intervalos regulares. En Horizon Administrator, puede establecer la frecuencia y otros aspectos de las operaciones de la copia de seguridad.

Tabla 8-1. Opciones de copia de seguridad de la configuración de Horizon 7

Configuración	Descripción
Frecuencia de copia de seguridad automática	<p>Cada hora. Se realiza una copia de seguridad cada hora en punto.</p> <p>Cada 6 horas. Las copias de seguridad se realizan a medianoche, a las 6:00, al mediodía y a las 18:00.</p> <p>Cada 12 horas. Las copias de seguridad se realizan a medianoche y al mediodía.</p> <p>Cada día. Las copias de seguridad se realizan cada día a medianoche.</p> <p>Cada 2 días. Las copias de seguridad se realizan a medianoche los sábados, los lunes, los miércoles y los viernes.</p> <p>Cada semana. Las copias de seguridad se realizan semanalmente el sábado a medianoche.</p> <p>Cada 2 semanas. Las copias de seguridad se realizan una de cada dos semanas el sábado a medianoche.</p> <p>Nunca. Las copias de seguridad no se realizan automáticamente.</p>
Número máximo de copias de seguridad	<p>Número de archivos de copia de seguridad que se pueden almacenar en la instancia del servidor de conexión. El número debe ser un entero superior a 0.</p> <p>Cuando se alcanza el número máximo, Horizon 7 elimina los archivos de copia de seguridad más antiguos.</p> <p>Esta opción también se aplica a los archivos de copia de seguridad que se crean cuando usa Hacer copia de seguridad ahora.</p>
Ubicación de la carpeta	<p>La ubicación predeterminada de los archivos de copia de seguridad donde se ejecuta el servidor de conexión: C:\Programdata\VMWare\VDM\backups.</p> <p>Cuando usa Hacer copia de seguridad ahora, Horizon 7 también almacena los archivos de copia de seguridad en esta ubicación.</p>

Exportar los datos de configuración del servidor de conexión de Horizon

Puede hacer una copia de seguridad de los datos de configuración de una instancia del servidor de conexión de Horizon exportando los contenidos de su repositorio LDAP de View.

Use el comando `vdmexport` para exportar los datos de configuración LDAP de View a un archivo LDIF cifrado. También puede usar la opción `vdmexport -v` (textual) para exportar los datos a un archivo LDIF de texto sin formato, o bien la opción `vdmexport -c` (limpio) para exportar los datos como texto sin formato sin incluir las contraseñas y otros datos personales.

Puede ejecutar el comando `vdmexport` en cualquier instancia del servidor de conexión. Si cuenta con varias instancias del servidor de conexión en un grupo replicado, solo es necesario que exporte la información desde una instancia. Todas las instancias replicadas contienen los mismos datos de configuración.

Nota El comando `vdmexport.exe` solo realiza la copia de seguridad de los datos LDAP de View. Este comando no hace copias de seguridad de la información de la base de datos de View Composer.

Requisitos previos

- Ubique el archivo ejecutable del comando `vdmexport.exe` con el servidor de conexión en la ruta predeterminada.

C:\Program Files\VMware\VMware View\Server\tools\bin

- Inicie sesión en la instancia del servidor de conexión como un usuario con la función Administradores o Administradores (solo lectura).

Procedimiento

- 1 Seleccione **Iniciar > Ventana del símbolo del sistema**.
- 2 En la ventana del símbolo del sistema, escriba el comando `vdmexport` y redireccione la salida a un archivo. Por ejemplo:

```
vdmexport > Myexport.LDF
```

De forma predeterminada, los datos exportados están cifrados.

Puede especificar el nombre del archivo de salida como un argumento de la opción `-f`. Por ejemplo:

```
vdmexport -f Myexport.LDF
```

Puede exportar los datos en un archivo de texto sin formato (textual) con la opción `-v`. Por ejemplo:

```
vdmexport -f Myexport.LDF -v
```

Puede exportar los datos en texto sin formato sin incluir las contraseñas y los datos confidenciales (limpio) con la opción `-c`. Por ejemplo:

```
vdmexport -f Myexport.LDF -c
```

Nota No utilice los datos de la copia de seguridad limpia para restaurar una configuración LDAP de View. Los datos de esta configuración no contienen contraseñas ni otro tipo de información importante.

Para obtener más información sobre el comando `vdmexport`, consulte el documento *Integración de Horizon 7*.

Pasos siguientes

Puede restaurar o transferir la información de la configuración del servidor de conexión usando el comando `vdmimport`.

Para obtener más información sobre la importación del archivo LDIF, consulte [Restaurar los datos de configuración del servidor de conexión de Horizon y de View Composer](#).

Restaurar los datos de configuración del servidor de conexión de Horizon y de View Composer

Puede restaurar de forma manual los archivos de configuración LDAP del servidor de conexión y los archivos de la base de datos de View Composer de los que Horizon 7 hizo las copias de seguridad.

Puede ejecutar distintas utilidades para restaurar el servidor de conexión y los datos de configuración de View Composer.

Antes de restaurar los datos de configuración, compruebe que realizó una copia de seguridad de los datos de configuración en Horizon Administrator. Consulte [Realizar una copia de seguridad de los datos del servidor de conexión de Horizon y de View Composer](#).

La utilidad `vdmimport` permite importar los datos del servidor de conexión desde los archivos de copia de seguridad LDIF al repositorio LDAP de View en la instancia del servidor de conexión.

La utilidad `SviConfig` le permitirá importar los datos de View Composer desde los archivos de la copia de seguridad `.svi` a la base de datos SQL de View Composer.

Nota En determinadas situaciones, es posible que deba instalar la versión actual de una instancia del servidor de conexión y restaurar la configuración existente de Horizon 7 si importa los archivos de configuración de LDAP del servidor de conexión. Es posible que necesite que este proceso forme parte de un plan de continuidad empresarial y de recuperación ante desastres (BCDR), como un paso de la configuración de un segundo centro de datos que incluya la configuración de Horizon 7 existente o por otras razones. Para obtener más información, consulte el documento *Instalación de Horizon 7*.

Importar los datos de configuración en el servidor de conexión de Horizon

Puede restaurar los datos de configuración de una instancia del servidor de conexión si importa una copia de seguridad de los datos almacenados en un archivo LDIF.

Utilice el comando `vdmimport` para importar los datos desde el archivo LDIF al repositorio LDAP de View en la instancia del servidor de conexión.

Si realizó una copia de seguridad de la configuración LDAP de View con Horizon Administrator o el comando `vdmexport` predeterminado, el archivo LDIF exportado estará cifrado. Debe descifrar el archivo LDIF antes de importarlo.

Si el archivo LDIF exportado posee un texto sin formato, no debe descifrarlo.

Nota No importe un archivo LDIF en formato limpio, es decir, en texto sin formato, contraseñas ni información confidencial. En caso de hacerlo, la información de configuración crítica no estará presente en el repositorio LDAP de View.

Para obtener más información sobre cómo realizar una copia de seguridad del repositorio LDAP de View, consulte [Realizar una copia de seguridad de los datos del servidor de conexión de Horizon y de View Composer](#).

Requisitos previos

- Ubique el archivo ejecutable del comando `vdmimport` con el servidor de conexión en la ruta predeterminada.

C:\Program Files\VMware\VMware View\Server\tools\bin
- Inicie sesión en la instancia del servidor de conexión como usuario con la función Administradores.

- Compruebe que conoce la contraseña de Data Recovery. Si se configuró un recordatorio de contraseña, puede mostrar el recordatorio al ejecutar el comando `vdmimport` sin la opción de contraseña.

Procedimiento

- 1 Detenga el servicio Windows de VMware Horizon View Composer en los servidores donde se ejecuta View Composer para detener todas las instancias de dicho servicio.
- 2 Detenga el servicio Windows del servidor de seguridad VMware Horizon en todos los servidores de seguridad para detener todas las instancias de dichos servidores.
- 3 Desinstale todas las instancias del servidor de conexión de Horizon.

Desinstale los servidores de conexión de VMware Horizon y la instancia de AD LDS VMwareVDMDS.
- 4 Instale una instancia del servidor de conexión.
- 5 Detenga el servicio Windows del servidor de conexión VMware Horizon para detener la instancia del servidor de conexión.
- 6 Haga clic en **Iniciar > Ventana del símbolo del sistema**.
- 7 Descifre el archivo LDIF cifrado.

En la ventana del símbolo del sistema, escriba el comando `vdmimport`. Especifique la opción `-d`, la opción `-p` con la contraseña de Data Recovery y la opción `-f` con un archivo LDIF cifrado existente seguido de un nombre para el archivo LDIF descifrado. Por ejemplo:

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

Si no recuerda la contraseña de Data Recovery, escriba el comando sin la opción `-p`. La utilidad muestra el recordatorio de contraseña y pide al usuario que introduzca la contraseña.

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

Especifique la opción `-f` con el archivo LDIF descifrado. Por ejemplo:

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

- 9 Desinstale el servidor de conexión.

Desinstale solo el paquete del servidor de conexión de VMware Horizon.
- 10 Vuelva a instalar el servidor de conexión.
- 11 Inicie sesión en Horizon Administrator y compruebe que la configuración sea correcta.
- 12 Inicie las instancias de View Composer.
- 13 Vuelva a instalar las instancias del servidor de réplica.
- 14 Inicie las instancias del servidor de seguridad.

Si existe riesgo de que la configuración de los servidores de seguridad sea incoherente, deben desinstalarse también en lugar de detenerlos y volver a instalarlos al final del proceso.

El comando `vdmimport` actualiza el repositorio LDAP de View en el servidor de conexión con los datos de configuración del archivo LDIF. Para obtener más información sobre el comando `vdmimport`, consulte el documento *Instalación de Horizon 7*.

Nota Asegúrese de que la configuración restaurada coincida con las máquinas virtuales que conozcan vCenter Server y View Composer, si se encuentra en uso. Si es necesario, restaure la configuración de View Composer a partir de la copia de seguridad. Consulte [Restaurar una base de datos de View Composer](#). Tras restaurar la configuración de View Composer, puede que tenga que resolver de forma manual las incoherencias si las máquinas virtuales en vCenter Server cambiaron desde que se realizó la copia de seguridad de la configuración de View Composer.

Restaurar una base de datos de View Composer

Puede importar los archivos de copia de seguridad de la configuración de View Composer en la base de datos de View Composer que almacena la información de clones vinculados.

Puede usar el comando `SviConfig restoredata` para restaurar los datos de la base de datos de View Composer si se produce un error en el sistema o para revertir la configuración de View Composer a un estado anterior.

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

Compruebe la ubicación de los archivos de copia de seguridad de la base de datos de View Composer. De forma predeterminada, Horizon 7 almacena los archivos de copia de seguridad en la unidad C: del equipo del servidor de conexión en `C:\Programdata\VMware\VDM\backups`.

Los archivos de copia de seguridad de View Composer usan una convención de nomenclatura con la fecha y el sufijo `.svi`.

`Backup-AñoMesDíaNúmero-Nombre de dominio_Nombre vCenter Server.svi`

Por ejemplo: `Backup-20090304000010-foobar_test_org.svi`

Familiarícese con los parámetros de `SviConfig restoredata`:

- **DsnName:** el DSN que se usa para conectarse a la base de datos. El parámetro `DsnName` es obligatorio y no puede estar vacío.
- **Username:** el nombre de usuario que se usa para conectarse a la base de datos. Si este parámetro no se especificó, se usa la autenticación de Windows.
- **Password:** la contraseña del usuario que se conecta a la base de datos. Si este parámetro no se especifica y no se usa la autenticación de Windows, se le pedirá que introduzca la contraseña más adelante.

- BackupFilePath: la ruta del archivo de la copia de seguridad de View Composer.

Los parámetros DsnName y BackupFilePath son obligatorios y no pueden estar vacíos. Los parámetros Username y Password son opcionales.

Procedimiento

- 1 Copie los archivos de copia de seguridad de View Composer del equipo del servidor de conexión en una ubicación a la que pueda acceder el equipo donde está instalado el servicio de VMware Horizon View Composer.
- 2 En el equipo donde View Composer está instalado, detenga el servicio de VMware Horizon View Composer.
- 3 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.
- 4 Ejecute el comando SviConfig restoredata.

```
sviconfig -operation=restoredata
          -DsnName=nombre_recurso_base_de_datos_destino_(DSN)
          -Username=nombre_usuario_administrador_base_de_datos
          -Password=contraseña_administrador_base_de_datos
          -BackupFilePath=ruta_al_archivo_de_copia_de_seguridad_de_View_Composer
```

Por ejemplo:

```
sviconfig -operation=restoredata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
          Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 Inicie el servicio de VMware Horizon View Composer.

Pasos siguientes

Para los códigos de resultado de salida del comando SviConfig restoredata, consulte [Códigos de resultado de la restauración de la base de datos de View Composer](#).

Códigos de resultado de la restauración de la base de datos de View Composer

Al restaurar una base de datos de View Composer, el comando SviConfig restoredata muestra un código de resultado.

Tabla 8-2. Códigos de resultado de restoredata

Código	Descripción
0	La operación finalizó correctamente.
1	No se encuentra el DSN proporcionado.

Tabla 8-2. Códigos de resultado de restoredata (Continuación)

Código	Descripción
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 VMware Horizon 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.

Exportar datos en la base de datos de View Composer

Puede exportar los datos desde la base de datos de View Composer a un archivo.

Importante Use la utilidad SviConfig solo si es un administrador de View Composer con experiencia.

Requisitos previos

De forma predeterminada, Horizon 7 almacena los archivos de copia de seguridad en la unidad C: del equipo del servidor de conexión de View en C:\Programdata\VMWare\VDM\backups.

Familiarícese con los parámetros de SviConfig exportdata:

- DsnName: el DSN que se usa para conectarse a la base de datos. Si no está especificado, el nombre de DNS, el nombre de usuario y la contraseña se recuperarán del archivo de configuración del servidor.
- Username: el nombre de usuario que se usa para conectarse a la base de datos. Si este parámetro no se especificó, se usa la autenticación de Windows.
- Password: la contraseña del usuario que se conecta a la base de datos. Si este parámetro no se especifica y no se usa la autenticación de Windows, se le pedirá que introduzca la contraseña más adelante.
- OutputFilePath: la ruta del archivo de salida.

Procedimiento

- 1 En el equipo donde View Composer está instalado, detenga el servicio de VMware Horizon View Composer.
- 2 Abra una ventana de símbolo de sistema de Windows y diríjase al archivo ejecutable SviConfig.

El archivo se encuentra con la aplicación View Composer.

View-Composer-installation-directory\sviconfig.exe

3 Ejecute el comando `SviConfig exportdata`.

```
sviconfig -operation=exportdata
          -DsnName=nombre_recurso_base_de_datos_destino_(DSN)
          -Username=nombre_usuario_administrador_base_de_datos
          -Password=contraseña_administrador_base_de_datos
          -OutputFilePath=ruta_al_archivo_de_salida_de_View_Composer
```

Por ejemplo:

```
sviconfig -operation=exportdata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
          Composer\Export-20090304000010-foobar_test_org.SVI"
```

Pasos siguientes

Para los códigos de resultado de exportación del comando `SviConfig exportdata`, consulte [Códigos de resultado de exportar la base de datos de View Composer](#).

Códigos de resultado de exportar la base de datos de View Composer

Al exportar una base de datos de View Composer, el comando `SviConfig exportdata` muestra un código de salida.

Tabla 8-3. Códigos Exportdata ExitStatus

Código	Descripción
0	Los datos se exportan correctamente.
1	No se encuentra el nombre DSN proporcionado.
2	Las credenciales no son válidas.
3	El controlador no es compatible con la base de datos proporcionada.
4	Se produjo un problema inesperado.
18	No se puede conectar con el servidor de la base de datos.
24	No se puede abrir el archivo de salida.

Supervisar los componentes de Horizon 7

Puede utilizar el panel de control de Horizon Administrator para consultar el estado de los componentes de vSphere y de Horizon 7 en la implementación de Horizon 7.

Horizon Administrator muestra información de supervisión relativa a: instancias del servidor de conexión, base de datos de eventos, puertas de enlace, servidores de seguridad, servicios de View Composer, almacenes de datos, instancias de vCenter Server y dominios.

Nota Horizon 7 no puede determinar los datos sobre el estado de los dominios de Kerberos. Horizon Administrator muestra el estado de los dominios de Kerberos como desconocido aunque un dominio esté configurado y funcione.

Procedimiento

- 1 En Horizon Administrator, haga clic en **Panel**.
- 2 En el panel Estado del sistema, expanda **Componentes de View**, **Componentes de vSphere** u **Otros componentes**.
 - Si aparece una flecha hacia arriba de color verde, significa que el componente no tiene ningún problema.
 - La flecha hacia abajo de color rojo indica que el componente no está disponible o no funciona.
 - Si se muestra una flecha doble amarilla, el componente presenta un estado de advertencia.
 - Cuando el estado de un componente es desconocido, aparece un signo de interrogación.
- 3 Haga clic en el nombre de un componente.

Se mostrará un cuadro de diálogo con el nombre, la versión, el estado y otra información sobre el componente.

Pasos siguientes

Use vCenter Server para supervisar los clústeres de vSAN y los discos que participan en un almacén de datos vSAN. Para obtener más información sobre cómo supervisar vSAN en vSphere 5.5 Update 1, consulte el documento *Almacenamiento de vSphere* y la documentación *Supervisión y rendimiento de vSphere*. Para obtener más información sobre cómo supervisar vSAN en vSphere 6 o versiones posteriores, consulte el documento *Administrar VMware vSAN*.

Supervisar el estado de las máquinas

Puede supervisar el estado de las máquinas de la implementación de Horizon 7 usando el panel de control de Horizon Administrator. Por ejemplo, puede mostrar todas las máquinas desconectadas o las máquinas que estén en modo mantenimiento.

Requisitos previos

Familiarícese con los valores de estado de las máquinas virtuales. Si desea obtener más información sobre el estado de las máquinas virtuales, consulte "Estado de las máquinas virtuales de vCenter Server" en el documento *Configurar escritorios virtuales en Horizon 7*.

Procedimiento

- 1 En Horizon Administrator, haga clic en **Panel**.

- En el panel Estado de la máquina, expanda una carpeta de estado.

Opción	Descripción
Preparando	Muestra los estados mientras la máquina se aprovisiona, se elimina o está en modo mantenimiento.
Máquinas con problemas	Muestra los estados de error.
Preparado para su uso	Muestra los estados cuando la máquina está lista para su uso.

- Ubique el estado de la máquina y haga clic en el número hipervinculado que aparece junto a ella.

La página **Máquinas** muestra todas las máquinas con el estado seleccionado.

Pasos siguientes

Puede hacer clic en el nombre de una máquina para ver los detalles sobre la máquina o en la flecha de retroceso de Horizon Administrator para volver a la página Panel.

Comprender los servicios de Horizon 7

La operación de las instancias del servidor de conexión y de los servidores de seguridad depende de varios servicios que se ejecutan en el sistema. Estos sistemas se inician y se detienen automáticamente, pero a veces es posible que necesite configurar la operación de estos servicios de forma manual.

Use la herramienta Microsoft Windows Services para detener o iniciar los servicios de Horizon 7. Si detiene los servicios de Horizon 7 en un host del servidor de conexión o un servidor de seguridad, los usuarios finales no pueden conectarse a las aplicaciones ni a los escritorios remotos hasta que reinicie los servicios. Es posible que necesite reiniciar un servicio si dejó de ejecutarse o si la funcionalidad Horizon 7 que controla no responde.

Detener e iniciar servicios de Horizon 7

La operación de las instancias del servidor de conexión y de los servidores de seguridad depende de varios servicios que se ejecutan en el sistema. En algunas ocasiones, resulta necesario detener e iniciar estos servicios de forma manual para solucionar problemas con la operación de Horizon 7.

Al detener los servicios de Horizon 7, los usuarios finales no pueden conectarse a los escritorios remotos y aplicaciones. Debe programar dicha acción como parte del mantenimiento del sistema o advertir a los usuarios de que los escritorios remotos y las aplicaciones no estarán disponibles temporalmente.

Nota Detenga solo el servicio del servidor de conexión de VMware Horizon View en un host del servidor de conexión o el servicio de seguridad de VMware Horizon View en un servidor de seguridad. No detenga ningún otro servicio de componente.

Requisitos previos

Familiarícese con los servicios que se ejecutan en los hosts del servidor de seguridad y los servidores de seguridad, como se describe en [Servicios de un host del servidor de conexión](#) y [Servicios de un servidor de seguridad](#).

Procedimiento

- 1 Introduzca **services.msc** en la ventana del símbolo del sistema para iniciar la herramienta de Windows Service.
- 2 Seleccione el servicio del servidor de conexión VMware Horizon View en el host del servidor de conexión o el servicio del servidor de seguridad VMware Horizon View en el servidor de seguridad y haga clic en **Detener**, **Reiniciar** o **Iniciar**, según corresponda.
- 3 Compruebe que el estado del servicio determinado cambie según lo esperado.

Servicios de un host del servidor de conexión

La operación de Horizon 7 depende de varios dispositivos que se ejecutan en el host del servidor de conexión.

Tabla 8-4. Servicios de los hosts del servidor de conexión de Horizon

Nombre del servicio	Tipo de inicio	Descripción
Puerta de enlace segura de Blast VMware Horizon View	Automático	Proporciona servicios HTML Access y Blast Extreme seguros. Este servicio debe ejecutarse si los clientes se conectan al servidor de conexión a través de la puerta de enlace segura de Blast.
Servidor de conexión de VMware Horizon View	Automático	Proporciona los servicios del agente de conexión. Este servicio siempre debe estar en ejecución. Al iniciar o detener este servicio, también se inician o se detienen los servicios web, de la puerta de enlace de seguridad, del bus de mensajería y del marco de trabajo. Este servicio no inicia ni detiene el servicio VMwareVDMDS ni el servicio del host de script de VMware Horizon View.
Componente del marco de VMware Horizon View	Manual	Proporciona servicios de registro de eventos, seguridad y marco de trabajo COM+. Este servicio siempre debe estar en ejecución.
Componente de bus de mensajería VMware Horizon View	Manual	Proporciona servicios de mensajería entre los componentes de Horizon 7. Este servicio siempre debe estar en ejecución.
Puerta de enlace segura PCoIP de VMware Horizon View	Manual	Proporciona servicios de la puerta de enlace segura de PCoIP. Este servicio debe estar ejecutándose si los clientes se conectan al servidor de conexión a través de la puerta de enlace segura de PCoIP.
VMware Horizon View Script Host	Deshabilitado	Proporciona compatibilidad para que los scripts de terceros se ejecuten cuando elimina máquinas virtuales. Este servicio está deshabilitado de forma predeterminada. Debe habilitar este servicio si desea ejecutar los scripts.
Componente de puerta de enlace de seguridad de VMware Horizon View	Manual	Proporciona servicios de puerta de enlace común. Este servicio siempre debe estar en ejecución.

Tabla 8-4. Servicios de los hosts del servidor de conexión de Horizon (Continuación)

Nombre del servicio	Tipo de inicio	Descripción
Componente Web de VMware Horizon View	Manual	Proporciona servicios web. Este servicio siempre debe estar en ejecución.
VMwareVDMDS	Automático	Proporciona servicios del directorio LDAP. Este servicio siempre debe estar en ejecución. Durante las actualizaciones de Horizon 7, este servicio asegura que los datos existentes se migren correctamente.

Servicios de un servidor de seguridad

La operación de Horizon 7 depende de varios dispositivos que se ejecutan en el servidor de seguridad.

Tabla 8-5. Servicios del servidor de seguridad

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

Cambiar la clave de licencia del producto

Si caduca la licencia actual de un sistema o si desea acceder a funciones de Horizon 7 que no tienen licencia en ese momento, puede usar Horizon Administrator para cambiar la clave de licencia del producto.

Puede agregar una licencia a Horizon 7 mientras Horizon 7 se está ejecutando. No es necesario que reinicie el sistema y tampoco se interrumpirá el acceso a los escritorios y las aplicaciones.

Requisitos previos

Para la correcta operación de Horizon 7 y de funciones de los complementos, como View Composer y las aplicaciones publicadas, obtenga una clave de licencia del producto válida.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Licencia y uso del producto**.

El primer y los últimos cinco caracteres de la clave de licencia actual aparecen en el panel **Licencia**.

- 2 Haga clic en **Editar licencia**.

- 3 Introduzca el número de serie de la licencia y haga clic en **Aceptar**.

La ventana **Licencia de producto** muestra la información actualizada de la licencia.

- 4 Verifique la fecha de caducidad de la licencia.

- 5 Verifique que las licencias de View Composer, de escritorio y de aplicaciones remotas estén habilitadas o deshabilitadas, según la edición de VMware Horizon 7 que la licencia de producto le permita utilizar.

No todas las funciones y características de VMware Horizon 7 están disponibles en todas las ediciones. Si desea obtener más información sobre los conjuntos de funciones de cada edición, consulte

<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

- 6 Verifique que el modelo de uso de la licencia coincida con el modelo que se usa en la licencia de producto.

El uso se contabiliza según el número de usuarios con nombre o de usuarios simultáneos, dependiendo de la edición y el acuerdo de uso de la licencia de producto.

Supervisar la licencia y el uso del producto

En Horizon 7 Administrator, puede supervisar los usuarios activos que están conectados a Horizon en ese momento. La página **Licencia y uso del producto** muestra los números de uso histórico actuales y más elevados. Puede usar estos números para realizar un seguimiento del uso de la licencia del producto. También puede restablecer los datos históricos de uso y volver a comenzar con los datos actuales.

Horizon proporciona dos modelos de uso de la licencia, uno para los usuarios designados y otro para los usuarios simultáneos. Horizon cuenta los usuarios designados y los simultáneos del entorno, sin tener en cuenta la edición de la licencia del producto o el acuerdo de modelo de uso.

Para los usuarios designados, Horizon cuenta el número de usuarios únicos que accedieron al entorno de Horizon. Si un usuario designado ejecuta varios escritorios de usuario único, aplicaciones y escritorios publicados, este usuario solo se cuenta una vez.

Para los usuarios designados, la columna **Actual** de la página **Licencia y uso del producto** muestra el número de usuarios desde que la implementación de Horizon se configuró por primera vez o desde la última vez que restableció el **recuento de usuarios designados**. La columna **El más alto** no se aplica a los usuarios designados.

Para los usuarios simultáneos, Horizon cuenta las conexiones al escritorio de usuario único por sesión. Si un usuario simultáneo ejecuta varios escritorios de usuario único, cada sesión de escritorio conectada se cuenta de forma independiente.

Para los usuarios simultáneos, las conexiones de las aplicaciones y los escritorios publicados se cuentan por usuario. Si un usuario simultáneo ejecuta varias aplicaciones y sesiones de escritorios publicados, este usuario solo se cuenta una vez, aunque se alojen aplicaciones o escritorios publicados diferentes en hosts RDS diferentes. Si un usuario simultáneo ejecuta un escritorio de usuario único y aplicaciones y escritorios publicados adicionales, el usuario solo se cuenta una vez.

Para los usuarios simultáneos, la columna **El más alto** de la página **Licencia y uso del producto** muestra el número más elevado de usuarios de aplicaciones y escritorios publicados y las sesiones de escritorios simultáneos desde que la implementación de Horizon se configuró por primera vez o desde la última vez que restableció el **recuento máximo**.

Puede supervisar el número de sesiones de colaborativas y colaboradores de sesiones que estén conectados a una sesión.

- **Activo: sesiones de colaboración:** el número de sesiones en el que el propietario de una sesión invitó a uno o varios usuarios a unirse a una sesión. Ejemplo: Juan invitó a dos personas a unirse a su sesión y María invitó a una persona a unirse a su sesión. El valor de esta fila es 2, independientemente de que alguno de los invitados se uniera a la sesión.
- **Activo: colaboradores totales:** el número total de usuarios que están conectados a una sesión colaborativa, incluidos el propietario de la sesión y los colaboradores. Ejemplo: Juan invitó a dos personas y solo una persona se unió a la sesión. María invitó a una persona que no se unió a la sesión. El valor de esta fila es 3: la sesión colaborativa de Juan tiene uno principal y otro secundario, mientras que la sesión colaborativa de María tiene uno principal y cero secundarios. Como también se cuenta el propietario de la sesión, se garantiza que el número total de colaboradores siempre sea mayor que el número total de sesiones colaborativas o igual a este número.

Restablecer los datos de uso de la licencia del producto

En Horizon Administrator, puede restablecer los datos históricos de uso del producto y volver a comenzar con los datos actuales.

Un administrador con el privilegio **Administrar configuración global y directivas** puede seleccionar las opciones **Restablecer el recuento máximo** y **Restablecer el recuento de usuarios designados**. Para restringir el acceso a esas opciones, otorgue este privilegio únicamente a administradores designados.

Requisitos previos

Familiarícese con el uso de la licencia del producto. Consulte [Supervisar la licencia y el uso del producto](#).

Procedimiento

1 En Horizon Administrator, seleccione **Configuración de View > Licencia y uso del producto**.

2 (opcional) En el panel **Uso**, seleccione **Restablecer el recuento máximo**.

El número histórico máximo de conexiones simultáneas se restablece al número actual.

3 (opcional) En el panel **Uso**, seleccione **Restablecer el recuento de usuarios designados**.

El número histórico máximo de usuarios designados se restablece a 0.

Nota Al seleccionar **Actualizar la información general del usuario** en la página **Usuarios y grupos** también restablece a 0 el número máximo de usuarios designados.

Actualizar la información general del usuario desde Active Directory

Puede actualizar Horizon 7 con la información de usuario actual que se almacena en Active Directory. Esta función actualiza el nombre, el teléfono, el correo electrónico, el nombre de usuario y el dominio de Windows predeterminado de los usuarios de Horizon 7. También se actualizan los dominios externos de confianza.

Use esta función si modifica la lista de dominios externos de confianza en Active Directory, sobre todo si las relaciones de confianza modificadas entre los dominios afectan a los permisos de usuario en Horizon 7.

Esta función examina Active Directory para encontrar la información de usuario más reciente y actualiza la configuración de Horizon 7.

Al actualizar la información de usuario general, también se restablece el número de usuarios designados a 0. Este número aparece en la página **Licencia y uso del producto** de Horizon Administrator. Consulte [Restablecer los datos de uso de la licencia del producto](#).

También puede usar el comando `vdadmin` para actualizar la información de dominio y de usuario. Consulte [Actualizar las entidades de seguridad externa con la opción -F](#).

Requisitos previos

Compruebe que pueda iniciar sesión en Horizon Administrator como administrador con el privilegio **Administrar configuración global y directivas**.

Procedimiento

1 En Horizon Administrator, haga clic en **Usuarios y grupos**.

- 2 Seleccione si desea actualizar la información de todos los usuarios o de uno individual.

Opción	Acción
Para todos los usuarios	Haga clic en Actualizar la información general del usuario . Si actualiza todos los usuarios y los grupos, esta acción puede tardar un tiempo prolongado.
Para un usuario individual	a Haga clic en el nombre del usuario que desea actualizar. b Haga clic en Actualizar la información general del usuario .

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.

- [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 [Configurar las opciones de View Composer](#) y [Configurar los dominios de View Composer](#).
- 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 [Eliminar View Composer de Horizon 7](#).

Antes de eliminar View Composer, verifique que ya no administre ningún escritorio de clones vinculados. Si aparece alguno, debe eliminarlo.

- Familiarícese con la configuración de View Composer en Horizon Administrator. Consulte [Configurar las opciones de View Composer](#) y [Configurar los dominios de View Composer](#).

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 los certificados en una instancia del servidor de conexión, en el servidor de seguridad o en View Composer

Cuando recibe certificados intermedios o certificados TLS de servidor actualizados, importe los certificados en el almacén de certificados del equipo local Windows de cada host de View Composer, del servidor de seguridad o del servidor de conexión.

Normalmente, los certificados del servidor caducan después de 12 meses. Los certificados raíz e intermediarios caducan después de 5 o 10 años.

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

Requisitos previos

- Obtenga los certificados intermedios y los servidores actualizados desde la CA antes de que caduquen los certificados que son válidos en ese momento.
- Compruebe que el complemento Certificado se agregó a MMC en el Windows Server en el que se instaló la instancia del servidor de conexión, el servidor de seguridad o el servicio de VMware Horizon View Composer.

Procedimiento

- 1 Importe el certificado de servidor TLS firmado en el almacén de certificados del equipo local Windows del host de Windows Server.
 - a En el complemento Certificado, importe el certificado del servidor en la carpeta **Certificados (equipo local) > Personal > Certificados**.
 - b Seleccione **Marcar esta clave como exportable**.
 - c Haga clic en **Siguiente** y en **Finalizar**.
- 2 En el servidor de conexión o el servidor de seguridad, elimine el certificado Nombre descriptivo, **vdm**, del certificado antiguo que se expidió para Horizon 7 Server.
 - a Haga clic con el botón secundario en el certificado antiguo y, a continuación, en **Propiedades**.
 - b En la pestaña General, elimine el texto de Nombre descriptivo, **vdm**.
- 3 En el servidor de conexión o en el servidor de seguridad, agregue el certificado Nombre descriptivo, **vdm**, al nuevo certificado que reemplaza al certificado anterior.
 - a Haga clic con el botón secundario en el nuevo certificado y, a continuación, en **Propiedades**.
 - b En la pestaña General, en el campo Nombre descriptivo, escriba **vdm**.
 - c Haga clic en **Aplicar** y en **Aceptar**.
- 4 En un certificado de servidor que se expidió para View Composer, ejecute la utilidad SviConfig ReplaceCertificate para enlazar el nuevo certificado al puerto que usa View Composer.
Esta utilidad reemplaza el enlace con el antiguo certificado por el enlace con el nuevo.
 - a Detenga el servicio de VMware Horizon View Composer.
 - b 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.

- c Escriba el comando SviConfig ReplaceCertificate. Por ejemplo:

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

La utilidad muestra una lista numerada de certificados TLS que están disponibles en el almacén de certificados del equipo local Windows.

- d Para seleccionar un certificado, escriba su número y pulse Intro.
- 5 Si se expiden certificados intermedios para un host de View Composer, del servidor de seguridad o del servidor de conexión, importe la actualización más reciente del certificado intermedio en la carpeta **Certificados (equipo local) > Entidades de certificación intermedias > Certificados** en el almacén de certificados de Windows.
 - 6 Reinicie el servicio del servidor de conexión VMware Horizon View, del servidor de seguridad VMware Horizon View o de VMware Horizon View Composer para que se realicen los cambios.

Programa de mejora de la experiencia de cliente de VMware

Este producto forma parte del programa de mejora de la experiencia de cliente (CEIP) de VMware. Si lo desea, puede unirse o dejar el CEIP de este producto.

La información relacionada con los datos recopilados a través del CEIP y los propósitos para los que VMware los utiliza están establecidos en el centro de seguridad y confianza:

<http://www.vmware.com/trustvmware/ceip.html>.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Licencia y uso del producto**.
- 2 En el panel **Programa de experiencia del cliente**, haga clic en **Editar configuración**.
- 3 Seleccione **Participar en el Programa de mejora de la experiencia de cliente de VMware** para unirse al CEIP.

Si no selecciona esta opción, no se unirá al CEIP.

- 4 Haga clic en **Aceptar**.

Administrar las aplicaciones ThinApp en Horizon Administrator

9

Puede usar Horizon Administrator para distribuir y administrar las aplicaciones empaquetadas con VMware ThinApp. La administración de aplicaciones ThinApp en Horizon Administrator implica realizar tareas como capturar y almacenar paquetes de aplicaciones, agregar aplicaciones ThinApp a Horizon Administrator y asignar aplicaciones ThinApp a grupos de escritorios y equipos.

Debe tener una licencia para usar la función de administración ThinApp en Horizon Administrator.

Importante Si, en lugar de distribuir las ThinApps asignándolas a grupos de escritorios y a equipos, prefiere asignar las ThinApps a los usuarios y grupos de Active Directory, puede usar VMware Identity Manager.

Este capítulo incluye los siguientes temas:

- [Requisitos de Horizon 7 para las aplicaciones ThinApp](#)
- [Capturar y almacenar paquetes de aplicaciones](#)
- [Asignar aplicaciones ThinApp a grupos de escritorios y máquinas](#)
- [Mantenimiento de las aplicaciones ThinApp en Horizon Administrator](#)
- [Supervisar y solucionar problemas de las aplicaciones ThinApp en Horizon Administrator](#)
- [Ejemplo de configuración ThinApp](#)

Requisitos de Horizon 7 para las aplicaciones ThinApp

Cuando se capturen y se almacenen las aplicaciones ThinApp que se transmitirán a los escritorios remotos en Horizon Administrator, debe cumplir ciertos requisitos.

- Debe empaquetar las aplicaciones en paquetes de Microsoft Installation (MSI).
- Debe usar la versión 4.6 de ThinApp o una versión posterior para crear o volver a empaquetar los paquetes MSI.
- Debe almacenar los paquetes MSI en un recurso compartido de red Windows que se encuentre en un dominio de Active Directory al que pueda acceder el host del servidor de conexión y los escritorios remotos. El servidor del archivo debe admitir los permisos de archivo y de autenticación que se basan en cuentas de equipos.

- Debe configurar el archivo y los permisos de uso compartido en el recurso compartido de red que aloja los paquetes MSI para proporcionarle Acceso de lectura en el grupo integrado Equipos del dominio de Active Directory. Si tiene pensado distribuir las aplicaciones ThinApp a los controladores de dominio, también debe proporcionarle Acceso de lectura al grupo integrado Controladores de dominio de Active Directory.
- Para permitir que los usuarios accedan a las transmisiones de paquetes de aplicaciones ThinApp, debe establecer el permiso NTFS en el recurso compartido de red que aloja los paquetes ThinApp como Lectura y ejecución para los usuarios.
- Asegúrese de que un espacio de nombres independiente no evite que los equipos que pertenecen al dominio accedan al recurso compartido de red que aloja los paquetes MSI. Un espacio de nombres independiente se produce cuando un nombre de dominio de Active Directory es diferente al espacio de nombres DNS que usan los equipos en dicho dominio. Consulte el artículo 1023309 de la base de conocimientos (KB) de VMware para obtener más información.
- Para ejecutar aplicaciones ThinApp transmitidas en los escritorios remotos, los usuarios deben tener acceso al recurso compartido de red que aloja los paquetes MSI.

Capturar y almacenar paquetes de aplicaciones

ThinApp ofrece virtualización de aplicaciones mediante el desacoplamiento de una aplicación desde el sistema operativo subyacente y sus bibliotecas y entorno, y el agrupamiento de la aplicación en un único archivo ejecutable denominado paquete de la aplicación.

Para administrar las aplicaciones ThinApp en Horizon Administrator, debe usar el asistente **Configurar la captura** de ThinApp a fin de capturar y empaquetar sus aplicaciones en formato MSI y almacenar los paquetes MSI en un repositorio de aplicaciones.

El repositorio de una aplicación es un recurso compartido en red de Windows. Use Horizon Administrator para registrar el recurso compartido como un repositorio de la aplicación. Puede registrar varios repositorios de aplicaciones.

Nota Si posee varios repositorios de aplicaciones, puede usar soluciones de terceros para administrar el equilibrio de carga y la disponibilidad. Horizon 7 no incluye el equilibrio de carga ni las soluciones de disponibilidad.

Consulte la *Introducción a VMware ThinApp* y la *Guía de usuario de ThinApp* para obtener información completa de las funciones ThinApp y sobre cómo utilizar el asistente para **Configurar la captura** de ThinApp.

1 Empaquetar aplicaciones

El asistente de ThinApp **Configurar la captura** permite capturar y empaquetar aplicaciones.

2 Crear un recurso compartido de red de Windows

Debe crear un recurso compartido en red de Windows para alojar los paquetes MSI distribuidos a los grupos y los escritorios remotos de Horizon Administrator.

3 Registrar un repositorio de aplicaciones

Debe registrar un recurso compartido de red de Windows que aloje los paquetes MSI como un repositorio de aplicaciones en Horizon Administrator.

4 Agregar aplicaciones ThinApp a Horizon Administrator

Para agregar aplicaciones ThinApp a Horizon Administrator, examine el repositorio de aplicaciones y seleccione las aplicaciones ThinApp. Después de agregar una aplicación ThinApp a Horizon Administrator, puede asignarla a los equipos o a los grupos de escritorios.

5 Crear una plantilla ThinApp

Puede crear una plantilla en Horizon Administrator para especificar un grupo de aplicaciones ThinApp. Puede usar plantillas para agrupar aplicaciones por función, proveedor o cualquier otra agrupación lógica que sea efectiva para su organización.

Empaquetar aplicaciones

El asistente de ThinApp **Configurar la captura** permite capturar y empaquetar aplicaciones.

Requisitos previos

- Descargue el software de ThinApp en <http://www.vmware.com/products/thinapp> e instálelo en un equipo limpio. View es compatible con ThinApp 4.6 y versiones posteriores.
- Familiarícese con los requisitos del software de ThinApp y las instrucciones para empaquetar aplicaciones de la *Guía de usuario de ThinApp*.

Procedimiento

- 1 Inicie el asistente de ThinApp **Configurar la captura** y siga las instrucciones que se indican.
- 2 Cuando el asistente de ThinApp **Configurar la captura** le solicite una ubicación de proyecto, seleccione **Compilar paquete MSI**.
- 3 Si quiere enviar la aplicación a escritorios remotos, asigne el valor 1 a la propiedad MSISstreaming en el archivo package.ini.

```
MSISstreaming=1
```

El asistente de ThinApp **Configurar la captura** encapsula la aplicación y todos los componentes necesarios para ejecutarla en un paquete MSI.

Pasos siguientes

Cree un recurso compartido de red de Windows para almacenar los paquetes MSI.

Crear un recurso compartido de red de Windows

Debe crear un recurso compartido en red de Windows para alojar los paquetes MSI distribuidos a los grupos y los escritorios remotos de Horizon Administrator.

Requisitos previos

- Use el asistente de ThinApp **Configurar la captura** para empaquetar las aplicaciones.
- Compruebe que el recurso compartido de red cumpla los requisitos de Horizon 7 para almacenar las aplicaciones ThinApp. Consulte [Requisitos de Horizon 7 para las aplicaciones ThinApp](#) para obtener más información.

Procedimiento

- 1 Cree una carpeta compartida en un equipo de un dominio de Active Directory a la que pueda acceder desde el host del servidor de conexión y los escritorios remotos.
- 2 Configure el archivo y los permisos de uso compartido de la carpeta compartida para proporcionar Acceso de lectura al grupo de Active Directory integrado Equipos del dominio.
- 3 Si tiene pensado asignar aplicaciones ThinApp a controladores de dominio, proporcione Acceso de lectura en el grupo de Active Directory integrado Equipo de dominio.
- 4 Si tiene pensado usar paquetes de aplicaciones ThinApp secuenciales, configure el permiso NTF en el recurso compartido de red que aloja los paquetes ThinApp como Leer y ejecutar para los usuarios.
- 5 Copie los paquetes MSI en la carpeta compartida.

Pasos siguientes

Registre el recurso compartido de red de Windows como un repositorio de aplicaciones en Horizon Administrator.

Registrar un repositorio de aplicaciones

Debe registrar un recurso compartido de red de Windows que aloje los paquetes MSI como un repositorio de aplicaciones en Horizon Administrator.

Puede registrar varios repositorios de aplicaciones.

Requisitos previos

Cree un recurso compartido de red de Windows.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración de ThinApp** y haga clic en **Agregar repositorio**.
- 2 Escriba un nombre para mostrar del repositorio de aplicaciones en el cuadro de texto **Nombre para mostrar**.

- 3 Escriba la ruta al recurso compartido de red de Windows que aloja los paquetes de aplicaciones en el cuadro de texto **Ruta del recurso compartido**.

La ruta del recurso compartido de red debe tener el formato `\\ServerComputerName\ShareName`, donde *ServerComputerName* es el nombre DNS del equipo del servidor. No especifique ninguna dirección IP.

Por ejemplo: `\\server.domain.com\MSIPackages`

- 4 Haga clic en **Guardar** para registrar el repositorio de aplicaciones con Horizon Administrator.

Agregar aplicaciones ThinApp a Horizon Administrator

Para agregar aplicaciones ThinApp a Horizon Administrator, examine el repositorio de aplicaciones y seleccione las aplicaciones ThinApp. Después de agregar una aplicación ThinApp a Horizon Administrator, puede asignarla a los equipos o a los grupos de escritorios.

Requisitos previos

Registre un repositorio de aplicaciones con Horizon Administrator.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps**.
- 2 En la pestaña **Resumen**, haga clic en **Examinar ThinApps nuevas**.
- 3 Seleccione el repositorio de aplicaciones y la carpeta que desee examinar y haga clic en **Siguiente**.
Si el repositorio de aplicaciones contiene subcarpetas, puede expandir la carpeta raíz y seleccionar una.
- 4 Seleccione las aplicaciones ThinApp que desee agregar a Horizon Administrator.
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias aplicaciones ThinApp.
- 5 Haga clic en **Examinar** para comenzar a examinar los paquetes MSI que seleccionó.
Puede hacer clic en **Detener exploración** si necesita detenerla.
Horizon Administrator informa sobre el estado de cada operación de exploración y el número de aplicaciones ThinApp que se agregaron a Horizon Administrator. Si selecciona una aplicación que ya está en Horizon Administrator, esta no se vuelve a agregar.
- 6 Haga clic en **Finalizar**.
Las nuevas aplicaciones ThinApp aparecen en la tabla **Resumen**.

Pasos siguientes

(Opcional) Cree plantillas ThinApp.

Crear una plantilla ThinApp

Puede crear una plantilla en Horizon Administrator para especificar un grupo de aplicaciones ThinApp. Puede usar plantillas para agrupar aplicaciones por función, proveedor o cualquier otra agrupación lógica que sea efectiva para su organización.

Con las plantillas ThinApp, puede simplificar la distribución de varias aplicaciones. Cuando asigne una plantilla ThinApp a un grupo de escritorios o máquinas, Horizon Administrator instala todas las aplicaciones que se encuentran en ese momento en la plantilla.

La creación de plantillas ThinApp es opcional.

Nota Si agrega una aplicación a una plantilla ThinApp después de asignar la plantilla a un equipo o un grupo de escritorios, Horizon Administrator no asigna automáticamente la nueva aplicación al grupo de escritorio o al equipo. Si elimina una aplicación de una plantilla ThinApp que se asignó previamente a un grupo de escritorios o a un equipo, la aplicación sigue asignada a esos elementos.

Requisitos previos

Agregue las aplicaciones ThinApp seleccionadas a Horizon Administrator.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApp** y haga clic en **Nueva plantilla**.
- 2 Escriba un nombre para la plantilla y haga clic en **Agregar**.
Todas las aplicaciones ThinApp aparecen en la tabla.
- 3 Para buscar una aplicación ThinApp en concreto, escriba el nombre de la aplicación en el cuadro de texto **Buscar** y haga clic en **Buscar**.
- 4 Seleccione las aplicaciones ThinApp que desee incluir en la plantilla y haga clic en **Agregar**.
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias aplicaciones.
- 5 Haga clic en **Aceptar** para guardar la plantilla.

Asignar aplicaciones ThinApp a grupos de escritorios y máquinas

Para instalar una aplicación ThinApp en un escritorio remoto, use Horizon Administrator para asignar esta aplicación a una máquina o un grupo de escritorios.

Cuando asigne una aplicación ThinApp a una máquina, Horizon Administrator comienza a instalar la aplicación en la máquina virtual unos minutos después. Cuando asigne una aplicación ThinApp a un grupo de escritorios, Horizon Administrator comienza a instalar la aplicación la primera vez que un usuario inicia sesión en un escritorio remoto del grupo.

Secuencial	Horizon Administrator instala un acceso directo a la aplicación ThinApp en el escritorio remoto. El acceso directo lleva a la aplicación ThinApp en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar las aplicaciones ThinApp transmitidas.
Completa	Horizon Administrator instala la aplicación ThinApp completa en el sistema de archivos local.

La cantidad de tiempo que tarda en instalar una aplicación ThinApp depende del tamaño de la aplicación.

Importante Puede asignar aplicaciones ThinApp a escritorios basados en máquinas virtuales y grupos de escritorios automáticos o grupos manuales que contienen máquinas virtuales de vCenter Server. No puede asignar aplicaciones ThinApp a escritorios publicados ni a equipos tradicionales.

- [Prácticas recomendadas para asignar aplicaciones ThinApp](#)
Siga las prácticas recomendadas cuando asigne aplicaciones ThinApps a grupos de escritorios y máquinas.
- [Asignar una aplicación ThinApp a varias máquinas](#)
Puede asignar una ThinApp en particular a una o varias máquinas.
- [Asignar varias aplicaciones ThinApps a una máquina](#)
Puede asignar una o varias aplicaciones ThinApps a una máquina.
- [Asignar una aplicación ThinApp a varios grupos de escritorios](#)
Puede asignar una aplicación ThinApp determinada a uno o más grupos de escritorios.
- [Asignar varias aplicaciones ThinApps a un grupo de escritorios](#)
Puede asignar una o varias aplicaciones ThinApps a un grupo de escritorios en particular.
- [Asignar una plantilla ThinApp a una máquina o grupo de escritorios](#)
Puede simplificar la distribución de varias aplicaciones ThinApp al asignar una plantilla ThinApp a una máquina o un grupo de escritorios.
- [Revisar las asignaciones de las aplicaciones ThinApp](#)
Puede revisar todas las máquinas y los grupos de escritorios a los que una aplicación ThinApp está asignada en ese momento. También puede revisar todas las aplicaciones ThinApp que están asignadas a un grupo de escritorios o a una máquina en concreto.
- [Visualizar información del paquete MSI](#)
Después de agregar una aplicación ThinApp a Horizon Administrator, puede visualizar información sobre su paquete MSI.

Prácticas recomendadas para asignar aplicaciones ThinApp

Siga las prácticas recomendadas cuando asigne aplicaciones ThinApps a grupos de escritorios y máquinas.

- Para instalar una aplicación ThinApp en un escritorio remoto en concreto, asigne la aplicación a la máquina virtual que aloja el escritorio. Si usa una convención de nomenclatura común para sus máquinas, puede usar las asignaciones de máquinas para distribuir rápidamente las aplicaciones a todas las máquinas que usen dicha convención.
- Para instalar una aplicación ThinApp en todas las máquinas de un grupo de escritorios, asigne la aplicación al grupo de escritorios. Si organiza los grupos de escritorios por tipo de usuario o departamento, puede usar las asignaciones de los grupos de escritorios para distribuir rápidamente las aplicaciones a usuarios o departamentos específicos. Por ejemplo, si tiene un grupo de escritorios para los usuarios del departamento de contabilidad, puede distribuir la misma aplicación a todos los usuarios de este departamento asignando la aplicación al grupo de contabilidad.
- Para perfeccionar la distribución de varias aplicaciones ThinApp, incluya las aplicaciones en una plantilla ThinApp. Cuando asigne una plantilla ThinApp a una máquina o un grupo de escritorios, Horizon Administrator instala todas las aplicaciones que se encuentran en ese momento en la plantilla.
- No asigne una plantilla ThinApp a una máquina o un grupo de escritorios si la plantilla contiene una aplicación ThinApp que ya está asignada a esa máquina o grupo de escritorios. Tampoco asigne una plantilla ThinApp a la misma máquina o grupo de escritorios más de una vez con un tipo de instalación diferente. Horizon Administrator devolverá errores de asignación de ThinApp en ambas situaciones.

Asignar una aplicación ThinApp a varias máquinas

Puede asignar una ThinApp en particular a una o varias máquinas.

Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a Horizon Administrator. Consulte [Agregar aplicaciones ThinApp a Horizon Administrator](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps** y seleccione la aplicación ThinApp.

- 2 Seleccione **Asignar máquinas** en el menú desplegable **Agregar asignación**.

Las máquinas que aún no tengan asignadas la aplicación ThinApp aparecen en la tabla.

Opción	Acción
Buscar una máquina específica	Escriba el nombre de la máquina en el cuadro de texto Buscar y haga clic en Buscar .
Buscar todas las máquinas que sigan la misma convención de nomenclatura	Escriba parte de un nombre de una máquina en el cuadro de texto Buscar y haga clic en Buscar .

- 3 Seleccione las máquinas que desee asignar a la aplicación ThinApp y haga clic en **Agregar**.
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias máquinas.
- 4 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
Secuencial	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
Completa	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

Horizon Administrator comienza a instalar la aplicación ThinApp unos minutos después. Tras finalizar la instalación, la aplicación está disponible para todos los usuarios de los escritorios alojados en las máquinas virtuales.

Asignar varias aplicaciones ThinApps a una máquina

Puede asignar una o varias aplicaciones ThinApps a una máquina.

Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a Horizon Administrator. Consulte [Agregar aplicaciones ThinApp a Horizon Administrator](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Máquinas** y haga doble clic en el nombre de la máquina que aparece en la columna Máquina.
- 2 En la tabla **Resumen**, haga clic en **Agregar asignación** en el panel ThinApps.
Las aplicaciones ThinApp que no aún no están asignadas a la máquina aparecen en la tabla.
- 3 Para buscar una aplicación en concreto, escriba el nombre de la aplicación en el cuadro de texto **Buscar** y haga clic en **Buscar**.

- 4 Seleccione la aplicación ThinApp que desee asignar a la máquina y haga clic en **Agregar**.
Repita este paso para agregar varias aplicaciones.
- 5 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
Secuencial	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
Completa	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

Horizon Administrator comienza a instalar las aplicaciones ThinApp unos minutos después. Tras finalizar la instalación, las aplicaciones están disponibles para todos los usuarios del escritorio que están alojados en la máquina virtual.

Asignar una aplicación ThinApp a varios grupos de escritorios

Puede asignar una aplicación ThinApp determinada a uno o más grupos de escritorios.

Si asigna una aplicación ThinApp a un grupo de clones vinculados y, posteriormente, actualiza, recompone o vuelve a equilibrar el grupo, Horizon Administrator vuelve a instalar la aplicación. No es necesario que vuelva a instalar la aplicación de forma manual.

Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a Horizon Administrator. Consulte [Agregar aplicaciones ThinApp a Horizon Administrator](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps** y seleccione la aplicación ThinApp.
- 2 Seleccione **Asignar grupos de escritorios** del menú desplegable **Agregar asignación**.

Los grupos de escritorios que todavía no asignó la aplicación ThinApp aparecerán en la tabla.

Opción	Acción
Buscar un grupo de escritorio determinado	Escriba el nombre del grupo de escritorios en el cuadro de texto Buscar y haga clic en Buscar .
Buscar todos los grupos de escritorios que sigan la misma convención de nomenclatura	Escriba parte del nombre de un grupo de escritorios en el cuadro de texto Buscar y haga clic en Buscar .

- 3 Seleccione los grupos de escritorios que desea asignar a la aplicación ThinApp y haga clic en **Agregar**.

Haga clic mientras mantiene pulsada la tecla Ctrl o Mayús para seleccionar varios grupos de escritorios.

- 4 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
Secuencial	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
Completa	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

Horizon Administrator comienza a instalar la aplicación ThinApp la primera vez que un usuario inicia sesión en un escritorio del grupo. Al finalizar la instalación, la aplicación estará disponible para todos los usuarios del grupo de escritorios.

Asignar varias aplicaciones ThinApps a un grupo de escritorios

Puede asignar una o varias aplicaciones ThinApps a un grupo de escritorios en particular.

Si asigna una aplicación ThinApp a un grupo de clones vinculados y, posteriormente, actualiza, recompone o vuelve a equilibrar el grupo, Horizon Administrator vuelve a instalar la aplicación. No es necesario que vuelva a instalar la aplicación de forma manual.

Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a Horizon Administrator. Consulte [Agregar aplicaciones ThinApp a Horizon Administrator](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios** y haga doble clic en el ID del grupo.
- 2 En la pestaña **Inventario**, haga clic en **ThinApps** y, a continuación, en **Agregar asignación**.
Las aplicaciones ThinApp que no aún no están asignadas al grupo aparecen en la tabla.
- 3 Para buscar una aplicación en concreto, escriba el nombre de la aplicación ThinApp en el cuadro de texto **Buscar** y haga clic en **Buscar**.
- 4 Seleccione la aplicación ThinApp que desee asignar al grupo y haga clic en **Agregar**.
Repita este paso para seleccionar varias aplicaciones.

5 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
Secuencial	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
Completa	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

Horizon Administrator comienza a instalar las aplicaciones ThinApp la primera vez que un usuario inicia sesión en un escritorio del grupo. Tras finalizar la instalación, las aplicaciones están disponibles para todos los usuarios del grupo de escritorios.

Asignar una plantilla ThinApp a una máquina o grupo de escritorios

Puede simplificar la distribución de varias aplicaciones ThinApp al asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

Si asigna una plantilla ThinApp a un grupo de escritorios o máquinas, Horizon Administrator instala las aplicaciones ThinApp que estén presentes en ese momento en la plantilla.

Requisitos previos

Cree una plantilla ThinApp. Consulte [Crear una plantilla ThinApp](#).

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps**.
- 2 Seleccione la plantilla ThinApp.
- 3 Seleccione **Asignar máquinas** o **Asignar grupos de escritorios** del menú desplegable **Agregar asignación**.

Todos los grupos de escritorios y máquinas aparecerán en la tabla.

Opción	Acción
Buscar una máquina o un grupo de escritorios determinado	Escriba el nombre de la máquina o del grupo de escritorios en el cuadro de texto Buscar y haga clic en Buscar .
Buscar todos los grupos de escritorios y máquinas que sigan la misma convención de nomenclatura	Escriba parte del nombre de la máquina o del grupo de escritorios en el cuadro de texto Buscar y haga clic en Buscar .

- 4 Seleccione las máquinas y grupos de escritorios a los que desea asignar la plantilla ThinApp y haga clic en **Agregar**.

Repita el mismo paso para seleccionar varias máquinas y grupos de escritorios.

5 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
Secuencial	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
Completa	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

Al asignar una plantilla de ThinApp a una máquina, Horizon Administrator comienza la instalación de aplicaciones en la plantilla unos minutos después. Al asignar una plantilla de ThinApp a un grupo de escritorios, Horizon Administrator comienza la instalación de las aplicaciones en la plantilla cuando un usuario inicia sesión en un escritorio del grupo por primera vez. Al finalizar la instalación, la aplicación está disponible para todos los usuarios de la máquina o del grupo de escritorio.

Horizon Administrator devuelve un mensaje de error si una plantilla ThinApp incluye una aplicación que ya esté asignada a la máquina o al grupo de escritorios.

Revisar las asignaciones de las aplicaciones ThinApp

Puede revisar todas las máquinas y los grupos de escritorios a los que una aplicación ThinApp está asignada en ese momento. También puede revisar todas las aplicaciones ThinApp que están asignadas a un grupo de escritorios o a una máquina en concreto.

Requisitos previos

Familiarícese con los valores de estado de la instalación ThinApp en [Valores del estado de instalación de la aplicación ThinApp](#).

Procedimiento

- ◆ Seleccione las asignaciones de aplicaciones ThinApp que desee revisar.

Opción	Acción
Revisar todas las máquinas y los grupos de escritorios a los que una aplicación ThinApp está asignada	<p>Seleccione Catálogo > ThinApp y haga doble clic en el nombre de la aplicación ThinApp.</p> <p>La pestaña Asignaciones muestra las máquinas y los grupos de escritorios a los que la aplicación está asignada en el momento e incluye el tipo de instalación.</p> <p>La pestaña Máquinas muestra las máquinas que están asociadas en el momento a la aplicación e incluye la información del estado de instalación.</p> <p>Nota Cuando asigne una aplicación ThinApp a un grupo, las máquinas del grupo aparecen en la pestaña Máquinas únicamente después de que se instale la aplicación.</p>
Revisar todas las aplicaciones ThinApp que están asignadas a un equipo en concreto	<p>Seleccione Recursos > Máquinas y haga doble clic en el nombre de la máquina que aparece en la columna Máquina.</p> <p>El panel ThinApp de la pestaña Resumen muestra todas las aplicaciones que están asignadas en el momento a la máquina e incluye el estado de instalación.</p>
Revisar todas las aplicaciones ThinApp que están asignadas a un grupo de escritorios en concreto	<p>Seleccione Catálogo > Grupos de escritorios, haga doble clic en el ID del grupo, seleccione la pestaña Inventario y haga clic a continuación en ThinApp.</p> <p>El panel Asignaciones de ThinApp muestra todas las aplicaciones que están asignadas en el momento al grupo de escritorios.</p>

Valores del estado de instalación de la aplicación ThinApp

Después de asignar una aplicación ThinApp a una máquina o a un grupo, Horizon Administrator indica el estado de la instalación.

La siguiente tabla describe cada valor del estado.

Tabla 9-1. Estado de instalación de la aplicación ThinApp

Estado	Descripción
Asignado	La aplicación ThinApp está asignada a la máquina.
Error en la instalación	Se produjo un error cuando Horizon Administrator intentó instalar la aplicación ThinApp.
Error al desinstalar	Se produjo un error cuando Horizon Administrator intentó desinstalar la aplicación ThinApp.
Instalado	La aplicación ThinApp está instalada.
Instalación pendiente	<p>Horizon Administrator está intentando instalar la aplicación ThinApp.</p> <p>No puede anular la asignación de una aplicación con este estado.</p> <p>Nota Este valor no aparece para las máquinas de los grupos de escritorios.</p>
Desinstalación pendiente	Horizon Administrator está intentando desinstalar la aplicación ThinApp.

Visualizar información del paquete MSI

Después de agregar una aplicación ThinApp a Horizon Administrator, puede visualizar información sobre su paquete MSI.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps**.

La pestaña **Resumen** muestra las aplicaciones que se encuentran disponibles y el número de asignaciones completas y secuenciales.

- 2 Haga doble clic en el nombre de la aplicación en la columna ThinApp.
- 3 Seleccione la pestaña **Resumen** para ver la información general sobre el paquete MSI.
- 4 Haga clic en **Información del paquete** para ver información detallada sobre el paquete MSI.

Mantenimiento de las aplicaciones ThinApp en Horizon Administrator

El mantenimiento de las aplicaciones ThinApp en Horizon Administrator, implica tareas como eliminar asignaciones de aplicaciones ThinApp, eliminar los repositorios de aplicaciones y las aplicaciones ThinApp, así como modificar y eliminar las plantillas ThinApp.

Nota Para actualizar una aplicación ThinApp, debe anular la asignación, eliminar la versión antigua de la aplicación y agregar y asignar la versión más actual.

- **Eliminar una asignación de aplicaciones ThinApp de varias máquinas**
Puede eliminar una asignación de aplicaciones ThinApp determinada de una o varias máquinas.
- **Eliminar varias asignaciones de aplicaciones ThinApp de una máquina**
Puede eliminar las asignaciones a una o varias aplicaciones ThinApps de una máquina particular.
- **Eliminar una asignación de aplicaciones ThinApp de varios grupos de escritorios**
Puede eliminar una asignación de aplicaciones ThinApp determinada de uno o varios grupos de escritorios.
- **Eliminar varias asignaciones de aplicaciones ThinApp de un grupo de escritorios**
Puede eliminar una o varias asignaciones de aplicaciones ThinApp de un grupo de escritorios en particular.
- **Eliminar una aplicación ThinApp de Horizon Administrator**
Cuando elimine una aplicación ThinApp de Horizon Administrator, ya no podrá asignarla a las máquinas ni a los grupos de escritorios.
- **Modificar o eliminar una plantilla ThinApp**
Puede agregar o eliminar aplicaciones de una plantilla ThinApp. También es posible eliminar la plantilla.
- **Eliminar el repositorio de una aplicación**
Puede eliminar el repositorio de una aplicación de Horizon Administrator.

Eliminar una asignación de aplicaciones ThinApp de varias máquinas

Puede eliminar una asignación de aplicaciones ThinApp determinada de una o varias máquinas.

Requisitos previos

Notifique a los usuarios de los escritorios remotos que se alojan en las máquinas de que pretende eliminar la aplicación.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApp** y haga doble clic en el nombre de la aplicación ThinApp.
- 2 En la pestaña **Asignaciones**, seleccione una máquina y haga clic en **Eliminar asignación**.

Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias máquinas.

Horizon Administrator desinstala la aplicación ThinApp unos minutos después.

Importante Si un usuario final usa la aplicación ThinApp al mismo tiempo que Horizon Administrator intenta desinstalar la aplicación, se produce un error y el estado de la aplicación cambia a Error al desinstalar. Cuando se produce este error, en primer lugar debe desinstalar de forma manual los archivos de la aplicación ThinApp de la máquina y luego hacer clic en **Eliminar estado de la aplicación para el escritorio** en Horizon Administrator.

Eliminar varias asignaciones de aplicaciones ThinApp de una máquina

Puede eliminar las asignaciones a una o varias aplicaciones ThinApps de una máquina particular.

Requisitos previos

Notifique a los usuarios del escritorio remoto que aloja la máquina que pretende eliminar las aplicaciones.

Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Máquinas** y haga doble clic en el nombre de la máquina que aparece en la columna Máquina.
- 2 En la pestaña **Resumen**, seleccione la aplicación ThinApp y haga clic en **Eliminar asignación** que aparece en el panel ThinApps.

Repita este paso para eliminar otra asignación de aplicaciones.

Horizon Administrator desinstala la aplicación ThinApp unos minutos después.

Importante Si un usuario final usa la aplicación ThinApp al mismo tiempo que Horizon Administrator intenta desinstalar la aplicación, se produce un error y el estado de la aplicación cambia a Error al desinstalar. Cuando se produce este error, en primer lugar debe desinstalar de forma manual los archivos de la aplicación ThinApp de la máquina y luego hacer clic en **Eliminar estado de la aplicación para el escritorio** en Horizon Administrator.

Eliminar una asignación de aplicaciones ThinApp de varios grupos de escritorios

Puede eliminar una asignación de aplicaciones ThinApp determinada de uno o varios grupos de escritorios.

Requisitos previos

Notifique a los usuarios de los escritorios remotos de los grupos de que pretende eliminar la aplicación.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApp** y haga doble clic en el nombre de la aplicación ThinApp.
- 2 En la pestaña **Asignaciones**, seleccione un grupo de escritorios y haga clic en **Eliminar asignación**.

Haga clic mientras mantiene pulsada la tecla Ctrl o Mayús para seleccionar varios grupos de escritorios.

Horizon Administrator desinstala la aplicación ThinApp la primera vez que un usuario inicia sesión en un escritorio remoto del grupo.

Eliminar varias asignaciones de aplicaciones ThinApp de un grupo de escritorios

Puede eliminar una o varias asignaciones de aplicaciones ThinApp de un grupo de escritorios en particular.

Requisitos previos

Notifique a los usuarios de los escritorios remotos del grupo de que pretende eliminar las aplicaciones.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios** y haga doble clic en el ID del grupo.
- 2 En la pestaña **Inventario**, haga clic en **ThinApps**, seleccione la aplicación ThinApp y haga clic en **Eliminar asignación**.

Repita este paso para eliminar varias aplicaciones.

Horizon Administrator desinstala las aplicaciones ThinApp la primera vez que un usuario inicia sesión en un escritorio remoto del grupo.

Eliminar una aplicación ThinApp de Horizon Administrator

Cuando elimine una aplicación ThinApp de Horizon Administrator, ya no podrá asignarla a las máquinas ni a los grupos de escritorios.

Es posible que necesite eliminar una aplicación ThinApp si su organización decide reemplazarla por una aplicación diferente del proveedor.

Nota No puede eliminar una aplicación ThinApp si ya está asignada a una máquina o a un grupo de escritorios o si está en estado Desinstalación pendiente.

Requisitos previos

Si una aplicación ThinApp ya está asignada a un grupo de escritorios o a un equipo, elimine la asignación del grupo de escritorios o de la máquina.

Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps** y seleccione la aplicación ThinApp.
- 2 Haga clic en **Eliminar ThinApp**.
- 3 Haga clic en **Aceptar**.

Modificar o eliminar una plantilla ThinApp

Puede agregar o eliminar aplicaciones de una plantilla ThinApp. También es posible eliminar la plantilla.

Si agrega una aplicación a una plantilla ThinApp después de asignar la plantilla a un equipo o un grupo de escritorios, Horizon Administrator no asigna automáticamente la nueva aplicación al equipo o al grupo de escritorios. Si elimina una aplicación de una plantilla ThinApp que se asignó previamente a un grupo de escritorios o a un equipo, la aplicación sigue asignada a esos elementos.

Procedimiento

- ◆ En Horizon Administrator, seleccione **Catálogo > ThinApps** y seleccione la plantilla ThinApp.

Opción	Acción
Agregar aplicaciones ThinApp a una plantilla o eliminarlas	Haga clic en Editar plantilla .
Eliminar la plantilla	Haga clic en Eliminar plantilla .

Eliminar el repositorio de una aplicación

Puede eliminar el repositorio de una aplicación de Horizon Administrator.

Es posible que necesite eliminar el repositorio de una aplicación si ya no necesita los paquetes MSI incluidos o si necesita mover dichos paquetes a otro recurso compartido en red. No se puede editar la ruta del recurso compartido del repositorio de una aplicación en Horizon Administrator.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración de ThinApp** y seleccione el repositorio de la aplicación.
- 2 Haga clic en **Eliminar repositorio**.

Supervisar y solucionar problemas de las aplicaciones ThinApp en Horizon Administrator

Horizon Administrator registra los eventos relacionados con la administración de las aplicaciones ThinApp en la base de datos de eventos e informes. Puede ver esos eventos en la página **Eventos** de Horizon Administrator.

Un evento puede aparecer en la página **Eventos** cuando se producen las siguientes situaciones.

- Se asignó una aplicación ThinApp o se eliminó una asignación de aplicación
- Se instaló o se desinstaló una aplicación ThinApp en un equipo
- No se puede instalar ni desinstalar una aplicación ThinApp
- Se registró, se modificó o se eliminó un repositorio de aplicaciones ThinApp de Horizon Administrator
- Se agregó una aplicación ThinApp a Horizon Administrator

Existen consejos para solucionar problemas comunes relacionados con la administración de aplicaciones ThinApp.

No se puede registrar un repositorio de aplicaciones

No puede registrar un repositorio de aplicaciones en Horizon Administrator.

Problema

Recibe un mensaje de error al intentar registrar un repositorio de aplicaciones en Horizon Administrator.

Causa

El host del servidor de conexión no puede acceder al recurso compartido de red que aloja el repositorio de aplicaciones. La ruta del recurso compartido de red que introdujo en el cuadro de diálogo **Ruta del recurso compartido** puede no ser correcta, el recurso compartido de red que aloja el repositorio de aplicaciones está en un dominio al que no se puede acceder desde el host del servidor de conexión o los permisos del recurso compartido de red no se configuraron correctamente.

Solución

- Si la ruta del recurso compartido de red es incorrecta, escriba la correcta. No se admiten las rutas de recursos compartidos de red que contienen direcciones IP.

- Si el recurso compartido de red no es un dominio al que se pueda acceder, copie los paquetes de aplicaciones a un recurso compartido de red en un dominio al que se pueda acceder desde el host del servidor de conexión.
- Compruebe que el archivo y los permisos de uso compartido de la carpeta compartida proporcione Acceso de lectura al grupo de Active Directory integrado Equipos del dominio. Si piensa asignar aplicaciones ThinApps a controladores de dominio, compruebe que el archivo y los permisos de uso compartido también proporcionen Acceso de solo lectura al grupo de Active Directory integrado Controladores de dominio. Tras establecer o cambiar los permisos, es posible que transcurran 20 minutos hasta que se pueda acceder al recurso compartido de red.

No se puede agregar aplicaciones ThinApp a Horizon Administrator

Horizon Administrator no puede agregar aplicaciones ThinApp a Horizon Administrator.

Problema

Ningún paquete MSI está disponible cuando hace clic en **Examinar ThinApps nuevas** en Horizon Administrator.

Causa

Ni los paquetes de aplicaciones que no están en formato MSI ni el host del servidor de conexión pueden acceder a los directorios en el recurso compartido de red.

Solución

- Compruebe que los paquetes de aplicaciones del repositorio estén en formato MSI.
- Compruebe que el recurso compartido de red cumpla los requisitos de Horizon 7 para almacenar las aplicaciones ThinApp. Consulte [Requisitos de Horizon 7 para las aplicaciones ThinApp](#) para obtener más información.
- Compruebe que los directorios del recurso compartido de red tengan los permisos correspondientes. Consulte [No se puede registrar un repositorio de aplicaciones](#) para obtener más información.

Aparecen mensajes en el archivo de registro de depuración del servidor de conexión cuando se examina un repositorio de aplicaciones. Los archivos de registro del servidor de conexión se encuentran en el host de dicho servidor en el directorio *unidad:\Documents and Settings\All Users\Application Data\VMware\VDM\Logs*.

No se puede asignar una plantilla ThinApp

No puede asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

Problema

Horizon Administrator devuelve un error de asignación cuando intenta asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

Causa

La plantilla ThinApp contiene una aplicación que ya está asignada a la máquina o al grupo de escritorios, o bien la plantilla ThinApp se asignó previamente a la máquina o al grupo de escritorios con un tipo de instalación diferente.

Solución

Si la plantilla contiene una aplicación ThinApp que ya está asignada a la máquina o al grupo de escritorios, cree una nueva plantilla que no contenga la aplicación o edite la plantilla existente y elimine la aplicación. Asigne la plantilla nueva o modificada a la máquina o al grupo de escritorios.

Para cambiar el tipo de instalación de una aplicación ThinApp, debe eliminar la asignación de la aplicación existente de la máquina o del grupo de escritorios. Después de desinstalar la aplicación ThinApp, puede asignarla a la máquina o al grupo de escritorios con un tipo de instalación diferente.

La aplicación ThinApp no está instalada

Horizon Administrator no puede instalar una aplicación ThinApp.

Problema

El estado de la instalación de la aplicación ThinApp es Instalación pendiente o Error en la instalación.

Causa

Entre las causas comunes de este problema se encuentran las siguientes:

- No hay espacio de disco suficiente en el equipo para instalar la aplicación ThinApp.
- Se perdió la conectividad de red entre el host del servidor de conexión y el equipo o entre el host del servidor de conexión y el repositorio de la aplicación.
- No se puede acceder a la aplicación ThinApp en el recurso compartido de red.
- La aplicación ThinApp se instaló previamente, o bien el directorio o el archivo ya existe en el equipo.

Puede consultar los archivos de registro de Horizon Agent y del servidor de conexión para obtener más información sobre la causa del problema.

Los archivos de registro de Horizon Agent se encuentran la ruta *unidad:\ProgramData\VMware\VDM\logs* del equipo.

Los archivos de registro del servidor de conexión se encuentran en el host de dicho servidor en el directorio *unidad:\Documents and Settings\All Users\Application Data\VMware\VDM\logs*.

Solución

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps**.
- 2 Haga clic en el nombre de la aplicación ThinApp.
- 3 En la pestaña **Máquinas**, seleccione el equipo y haga clic en **Volver a intentar la instalación** para volver a instalar la aplicación ThinApp.

La aplicación ThinApp no está desinstalada

Horizon Administrator no puede desinstalar una aplicación ThinApp.

Problema

El estado de la instalación de la aplicación ThinApp muestra Error al desinstalar.

Causa

Entre las causas comunes de este error se encuentran las siguientes:

- La aplicación ThinApp estaba ocupada cuando Horizon Administrator intentó desinstalarla.
- Se perdió la conectividad a la red entre el host del servidor de conexión y el equipo.

Puede consultar los archivos de registro de Horizon Agent y del servidor de conexión para obtener más información sobre la causa del problema.

Los archivos de registro Horizon Agent se encuentran en la ruta *unidad:\Documents and Settings\All Users\Application Data\VMware\VDM\logs* en los sistemas Windows XP y en *unidad:\ProgramData\VMware\VDM\logs* en los sistemas Windows 7.

Los archivos de registro del servidor de conexión se encuentran en el host de dicho servidor en el directorio *unidad:\Documents and Settings\All Users\Application Data\VMware\VDM\logs*.

Solución

- 1 En Horizon Administrator, seleccione **Catálogo > ThinApps**.
- 2 Haga clic en el nombre de la aplicación ThinApp.
- 3 Haga clic en la pestaña **Máquinas**, seleccione el equipo y haga clic en **Volver a intentar la desinstalación** para volver a intentar realizar la operación de desinstalación.
- 4 Si aún se produce algún error en la operación de desinstalación, elimine de forma manual la aplicación ThinApp del equipo y vuelva a hacer clic en **Eliminar estado de la aplicación para el escritorio**.

Este comando borra la asignación de la aplicación ThinApp en Horizon Administrator. No elimina ningún archivo ni configuración del equipo.

Importante Use este comando únicamente después de eliminar manualmente la aplicación ThinApp del equipo.

El paquete MSI no es válido

Horizon Administrator notifica que un paquete MSI de un repositorio de aplicaciones no es válido.

Problema

Horizon Administrator notifica que un paquete MSI no es válido durante una operación de análisis.

Causa

Entre las causas comunes de este problema se encuentran las siguientes:

- El archivo MSI está dañado.
- El archivo MSI no se creó con ThinApp.
- El archivo MSI se creó o se volvió a empaquetar con una versión de ThinApp que no es compatible. Debe usar la versión 4.6 de ThinApp o una versión posterior.

Solución

Consulte la *Guía de usuario de ThinApp* para obtener más información sobre cómo solucionar los problemas de los paquetes MSI.

Ejemplo de configuración ThinApp

El ejemplo de configuración ThinApp lo guía paso a paso a través de una configuración ThinApp típica, desde la captura y el empaquetado de las aplicaciones hasta la comprobación del estado de una instalación.

Requisitos previos

Consulte estos temas para obtener una información completa sobre cómo realizar estos pasos en este ejemplo.

- [Capturar y almacenar paquetes de aplicaciones](#)
- [Asignar aplicaciones ThinApp a grupos de escritorios y máquinas](#)

Procedimiento

- 1 Descargue el software de ThinApp en <http://www.vmware.com/products/thinapp> e instálelo en un equipo limpio.

Horizon 7 se admite con ThinApp 4.6 y versiones posteriores.
- 2 Use el asistente de ThinApp **Configurar la captura** para capturar y empaquetar las aplicaciones en formato MSI.
- 3 Cree una carpeta compartida en un equipo de un dominio de Active Directory a la que se pueda acceder desde el host del servidor de conexión y desde los escritorios remotos y, a continuación, configure el archivo y los permisos de uso compartido en la carpeta compartida para proporcionar Acceso de lectura al grupo de Active Directory integrado Equipos del dominio.

Si tiene pensado asignar aplicaciones ThinApp a controladores de dominio, proporcione también Acceso de lectura en el grupo de Active Directory integrado Controladores de dominio.
- 4 Copie los paquetes MSI en la carpeta compartida.
- 5 Registre la carpeta compartida como un repositorio de aplicaciones en Horizon Administrator.
- 6 En Horizon Administrator, examine los paquetes MSI del repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas en Horizon Administrator.

- 7 Decida si desea asignar las aplicaciones ThinApp a grupos de escritorios o a máquinas.

Si usa una convención de nomenclatura común para sus máquinas, puede usar las asignaciones de máquinas para distribuir rápidamente las aplicaciones a todas las máquinas que usen dicha convención. Si organiza los grupos de escritorios por tipo de usuario o departamento, puede usar las asignaciones de los grupos de escritorios para distribuir rápidamente las aplicaciones a usuarios o departamentos específicos.

- 8 En Horizon Administrator, seleccione las aplicaciones ThinApp que desea asignar a las máquinas o a los grupos de escritorios y especifique el método de instalación.

Opción	Acción
Secuencial	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
Completa	Instale la aplicación completa en el sistema de archivos local de la máquina.

- 9 En Horizon Administrator, compruebe el estado de instalación de las aplicaciones ThinApp.

Configurar clientes en modo de pantalla completa

10

Puede establecer que los clientes desatendidos puedan obtener acceso a los escritorios desde Horizon 7.

Un cliente en modo de pantalla completa es un cliente ligero o un equipo bloqueado que ejecuta Horizon Client para conectarse a la instancia del servidor de conexión y ejecutar una sesión. No es necesario que los usuarios finales inicien sesión para acceder al dispositivo cliente, aunque el escritorio publicado pueda solicitarles que proporcionen información de autenticación para algunas aplicaciones. Entre las aplicaciones de ejemplo se incluyen estaciones de trabajo en las que se introducen datos médicos, estaciones de facturación de líneas aéreas, puntos de autoservicio para los clientes y terminales de información para el acceso público.

Debe comprobar que la aplicación del escritorio implemente los mecanismos de autenticación para realizar transacciones seguras, que la red física sea segura ante ataques snooping y manipulaciones y que todos los dispositivos conectados a la red sean de confianza.

Los clientes en modo de pantalla completa admiten las funciones estándar en el acceso remoto como, por ejemplo, el redireccionamiento automático de dispositivos USB a las sesiones remotas y la impresión según ubicación.

Horizon 7 usa la función Autenticación flexible en Horizon 7 4.5 y en versiones posteriores para autenticar un dispositivo cliente en modo de pantalla completa en lugar del usuario final. Puede configurar una instancia del servidor de conexión para autenticar clientes que se identifiquen por la dirección MAC, por nombre de usuario que comience por los caracteres "custom-" o por una cadena de prefijos alternativo que definió en ADAM. Si configura que un cliente que tenga una contraseña generada automáticamente, puede ejecutar Horizon Client en el dispositivo sin especificar una contraseña. Si configura una contraseña explícita, debe especificarla en Horizon Client. Al ejecutar normalmente Horizon Client desde un script y aparecer la contraseña como texto no cifrado, debería tomar precauciones para hacer que el script sea ilegible por los usuarios sin privilegios.

Solamente las instancias del servidor de conexión que habilite para autenticar clientes en modo de pantalla completa pueden aceptar conexiones desde cuentas que comiencen por los caracteres "cm-" seguidos por una dirección MAC, por los caracteres "custom-" o por la cadena alternativa que definió. Horizon Client en Horizon 7 4.5 y versiones posteriores no permite que se introduzcan de forma manual los nombres de usuario que utilicen estas formas.

Como práctica recomendada, use las instancias del servidor de conexión dedicadas para administrar clientes en modo de pantalla completa y para crear grupos y unidades organizativas dedicadas en Active Directory para las cuentas de dichos clientes. Esta práctica no solo realiza particiones en estos sistemas ante intrusiones no deseadas, sino que también facilita la configuración y la administración de los clientes.

Configurar clientes en modo de pantalla completa

Para configurar Active Directory y Horizon 7 de forma que admitan clientes en modo de pantalla completa, debe realizar varias tareas en secuencia.

Requisitos previos

Compruebe que tenga los privilegios necesarios para realizar las tareas de configuración.

- Las credenciales **Admins. del dominio** u **Oper. de cuentas** en Active Directory para realizar cambios en las cuentas de usuarios y grupos de un dominio.
- Las funciones **Administradores**, **Administradores de inventario** o una equivalente para usar Horizon Administrator para autorizar el uso de escritorios remotos por parte de usuarios o grupos.
- La función **Administradores** o una equivalente para ejecutar el comando `vdadmin`.

Procedimiento

1 Preparar Active Directory y Horizon 7 para clientes en modo de pantalla completa

Debe configurar Active Directory para que acepte las cuentas que cree para autenticar dispositivos cliente. Cuando cree un grupo, también debe autorizarlo para acceder al grupo de escritorios al que tiene acceso un cliente. También puede preparar el grupo de escritorios que los clientes utilizan.

2 Establecer valores predeterminados para clientes en modo de pantalla completa

Puede utilizar el comando `vdadmin` para establecer los valores predeterminados sobre la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de Active Directory de los clientes en modo de pantalla completa.

3 Visualizar las direcciones MAC de dispositivos cliente

Si desea crear una cuenta para un cliente que se basa en su dirección MAC, puede usar Horizon Client para ver la dirección MAC del dispositivo cliente.

4 Agregar cuentas de clientes en modo de pantalla completa

Puede usar el comando `vdadmin` para agregar cuentas de clientes a la configuración de un grupo de servidores de conexión. Después de agregar un cliente, este se encuentra disponible para su uso con una instancia del servidor de conexión en la que habilitó la autenticación de los clientes. También puede actualizar la configuración de los clientes o eliminar las cuentas del sistema.

5 Habilitar la autenticación de clientes en modo de pantalla completa

Puede utilizar el comando `vdadmin` para habilitar la autenticación de clientes que intenten conectarse a sus escritorios remotos a través de una instancia del servidor de conexión.

6 Verificar la configuración de los clientes en modo de pantalla completa

Puede usar el comando `vdmadmin` para mostrar información sobre los clientes en modo de pantalla completa y las instancias del servidor de conexión que se configuraron para autenticar dichos clientes.

7 Conectarse a escritorios remotos desde clientes en modo de pantalla completa

Puede ejecutar el cliente desde una línea de comandos o usar un script para conectar un cliente a una sesión remota.

Preparar Active Directory y Horizon 7 para clientes en modo de pantalla completa

Debe configurar Active Directory para que acepte las cuentas que cree para autenticar dispositivos cliente. Cuando cree un grupo, también debe autorizarlo para acceder al grupo de escritorios al que tiene acceso un cliente. También puede preparar el grupo de escritorios que los clientes utilizan.

La práctica recomendada es crear una unidad organizativa independiente y un grupo para reducir el trabajo a la hora de administrar clientes en modo de pantalla completa. Puede agregar cuentas independientes de clientes que no pertenecen a ningún grupo, pero así genera gastos de administración elevados si configura más de un pequeño número de clientes.

Procedimiento

- 1 En Active Directory, cree un grupo y una unidad organizativa independientes para utilizarlos con los clientes en modo de pantalla completa.

Debe asignarle al grupo un nombre anterior a Windows 2000. Utilice este nombre para identificar al grupo con el comando `vdmadmin`.

- 2 Cree la imagen o plantilla de la máquina virtual invitada.

Puede utilizar una máquina virtual administrada por vCenter Server como plantilla para un grupo automático, como principal de un grupo de clones vinculados o como máquina virtual en un grupo de escritorios manual. También puede instalar y configurar aplicaciones en el sistema operativo invitado.

- 3 Configure el sistema operativo invitado para que los clientes no se bloqueen cuando no estén atendidos.

Horizon 7 elimina el mensaje previo al inicio de sesión para los clientes que se conectan en modo de pantalla completa. Si requiere un evento para desbloquear la pantalla y mostrar un mensaje, puede configurar una aplicación adecuada en el sistema operativo invitado.

- 4 En Horizon Administrator, cree un grupo de escritorios para que los clientes lo utilicen y autorícelo a acceder al grupo.

Por ejemplo, puede elegir crear un grupo de escritorios de clones vinculados y asignaciones flotantes como la opción más adecuada para los requisitos de la aplicación cliente. También puede asociar una o varias aplicaciones ThinApp al grupo de escritorios.

Importante No autorice a un cliente ni a un grupo a acceder a más de un grupo de escritorios. Si lo hace, Horizon 7 asigna al cliente un escritorio remoto al azar entre los grupos para los que el cliente está autorizado y genera un evento de advertencia.

- 5 Si desea habilitar la impresión según ubicación para los clientes, configure la opción AutoConnect Location-based Printing for VMware View de la directiva de grupo de Active Directory, que se encuentra en el Editor de objetos de directiva de grupo de Microsoft. Para acceder a ella, seleccione Configuración del equipo y abra la carpeta Configuración de software.

- 6 Configure otras directivas que necesite optimizar y asegure los escritorios remotos de los clientes.

Por ejemplo, puede anular las directivas que conectan los dispositivos USB locales al escritorio remoto cuando este se inicia o al conectar los dispositivos. De forma predeterminada, Horizon Client para Windows habilita estas directivas para los clientes en modo de pantalla completa.

Ejemplo: Preparar Active Directory para clientes en modo de pantalla completa

La intranet tiene un dominio MYORG y su unidad organizativa tiene el nombre distintivo OU=myorg-ou,DC=myorg,DC=com. En Active Directory, cree la unidad organizativa kiosk-ou con el nombre distintivo OU=kiosk-ou,DC=myorg,DC=com y el grupo kc-grp para utilizarlo con los clientes en modo de pantalla completa.

Pasos siguientes

Defina los valores predeterminados de los clientes.

Establecer valores predeterminados para clientes en modo de pantalla completa

Puede utilizar el comando `vdadmin` para establecer los valores predeterminados sobre la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de Active Directory de los clientes en modo de pantalla completa.

Debe ejecutar el comando `vdadmin` en una de las instancias del servidor de conexión del grupo que contiene la instancia que los clientes usarán para conectarse a sus escritorios publicados.

Al configurar los valores predeterminados sobre la caducidad de la contraseña y pertenencia a grupos de Active Directory, estas opciones se comparten con todas las instancias del servidor de conexión en un grupo.

Procedimiento

- ◆ Establezca los valores predeterminados para clientes.

```
vdmadmin -Q -clientauth -setdefaults [-b argumentos_autenticación] [-ou DN] [ -expirepassword | -noexpirepassword ] [-group nombre_grupo | -nogroup]
```

Opción	Descripción
-expirepassword	Especifica el mismo periodo de caducidad para las contraseñas de las cuentas cliente que el del grupo del servidor de conexión. Si no se definió un periodo de caducidad para el grupo, las contraseñas nunca expirarán.
-group nombre_grupo	Especifica el nombre del grupo predeterminado al que se agregan las cuentas cliente. El nombre del grupo debe especificarse como el nombre del grupo de Active Directory anterior a Windows 2000.
-noexpirepassword	Especifica que las contraseñas de las cuentas cliente no expiran.
-nogroup	Borra la configuración para el grupo predeterminado.
-ou DN	Especifica el nombre distintivo de la unidad organizativa predeterminada a la que se agregan las cuentas cliente. Por ejemplo: OU=kiosk-ou,DC=myorg,DC=com Nota No puede utilizar el comando para cambiar la configuración de una unidad organizativa.

El comando actualiza los valores predeterminados para los clientes en el grupo del servidor de conexión.

Ejemplo: Establecer valores predeterminados para clientes en modo de pantalla completa

Establezca los valores predeterminados de la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de clientes.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Pasos siguientes

Encuentre las direcciones MAC de los dispositivos cliente que utilicen dichas direcciones para autenticarse.

Visualizar las direcciones MAC de dispositivos cliente

Si desea crear una cuenta para un cliente que se basa en su dirección MAC, puede usar Horizon Client para ver la dirección MAC del dispositivo cliente.

Requisitos previos

Inicie sesión en la consola del cliente.

Procedimiento

- ◆ Para ver la dirección MAC, escriba el comando apropiado según la plataforma.

Opción	Acción
Windows	<p>Introduzca</p> <pre>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo.</pre> <p>El cliente usa la instancia del servidor de conexión de Horizon predeterminada que configuró para ella. Si no configuró un valor predeterminado, el cliente le solicitará el valor.</p> <p>El comando muestra la dirección IP, la dirección MAC y el nombre del equipo del dispositivo cliente.</p>
Linux	<p>Introduzca <code>vmware-view --printEnvironmentInfo -s connection_server</code>.</p> <p>Debe especificar la dirección IP o el FQDN de la instancia del servidor de conexión que el cliente usará para conectarse al escritorio.</p> <p>El comando muestra la dirección IP, la dirección MAC, el nombre de la máquina, el dominio, el nombre y el dominio de cualquier usuario con la sesión iniciada y la zona horaria del dispositivo cliente.</p>

Pasos siguientes

Agregue las cuentas de los clientes.

Agregar cuentas de clientes en modo de pantalla completa

Puede usar el comando `vdadmin` para agregar cuentas de clientes a la configuración de un grupo de servidores de conexión. Después de agregar un cliente, este se encuentra disponible para su uso con una instancia del servidor de conexión en la que habilitó la autenticación de los clientes. También puede actualizar la configuración de los clientes o eliminar las cuentas del sistema.

Debe ejecutar el comando `vdadmin` en una de las instancias del servidor de conexión del grupo que contiene la instancia que los clientes usarán para conectarse a sus escritorios publicados.

Cuando agrega un cliente en modo de pantalla completa, Horizon 7 crea una cuenta de usuario para el cliente en Active Directory. Si especifica un nombre para el cliente, este nombre debe comenzar por una cadena de prefijo reconocida, como "custom-", o bien con una cadena de prefijo alternativa que definió en ADAM y que no puede ser superior a 20 caracteres. Si no especifica un nombre para un cliente, Horizon 7 genera un nombre para la dirección MAC que especificó para el dispositivo cliente. Por ejemplo, si la dirección MAC es 00:10:db:ee:76:80, el nombre de la cuenta correspondiente es cm-00_10_db_ee_76_80. Solo puede usar estas cuentas con las instancias del servidor de conexión que habilitó para autenticar clientes.

Importante No use un nombre especificado con más de un dispositivo cliente. Es posible que las próximas versiones no admitan esta configuración.

Procedimiento

- ◆ Ejecute el comando `vdmadmin` con las opciones `-domain` y `-clientid` para especificar el dominio y el nombre o la dirección MAC del cliente.

```
vdmadmin -Q -clientauth -add [-b argumentos_autenticación] -domain nombre_dominio -clientid id_cliente [-password "contraseña" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group nombre_grupo | -nogroup] [-description "texto_descripción"]
```

Opción	Descripción
<code>-clientid id_cliente</code>	Especifica el nombre o la dirección MAC del cliente.
<code>-description "texto_descripción"</code>	Crea una descripción de la cuenta del dispositivo cliente en Active Directory.
<code>-domain nombre_dominio</code>	Especifica el dominio del cliente.
<code>-expirepassword</code>	Especifica que el tiempo de caducidad de la contraseña de la cuenta es el mismo que el del grupo del servidor de conexión. Si no se definió el tiempo de caducidad, la contraseña no caduca.
<code>-genpassword</code>	Genera una contraseña para la cuenta del cliente. Este es el comportamiento predeterminado si no especifica <code>-password</code> ni <code>-genpassword</code> . Una contraseña generada tiene 16 caracteres, contiene al menos una letra en mayúscula, una en minúscula, un símbolo y un número. Además, puede contener caracteres repetidos. Si necesita una contraseña más segura, use la opción <code>-password</code> para especificar la contraseña.
<code>-group nombre_grupo</code>	Especifica el nombre del grupo al que se agregó la cuenta del cliente. El nombre del grupo debe especificarse como el nombre del grupo de Active Directory anterior a Windows 2000. Si estableció previamente un grupo predeterminado, la cuenta del cliente se agrega a este grupo.
<code>-noexpirepassword</code>	Especifica que la contraseña de la cuenta del cliente no caduca.
<code>-nogroup</code>	Especifica que la cuenta del cliente no se agrega al grupo predeterminado.
<code>-ou DN</code>	Especifica el nombre distintivo de la unidad organizativa a la que se agregó la cuenta del cliente. Por ejemplo: OU=kiosk-ou,DC=myorg,DC=com
<code>-password "contraseña"</code>	Especifica una contraseña explícita para la cuenta del cliente.

El comando crea una cuenta de usuario en Active Directory para el cliente en el dominio y grupo especificados (si existe alguno).

Ejemplo: Agregar cuentas para los clientes

Agregue una cuenta para un cliente especificado por la dirección MAC al dominio MYORG, usando la configuración predeterminada del grupo kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Agregue una cuenta para un cliente especificado por su dirección MAC al dominio MYORG, usando una contraseña generada automáticamente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

Agregue una cuenta para un cliente con nombre y especifique la contraseña que se usará con el cliente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Agregue una cuenta para un cliente con nombre, usando una contraseña generada automáticamente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

Pasos siguientes

Habilite la autenticación de los clientes.

Habilitar la autenticación de clientes en modo de pantalla completa

Puede utilizar el comando `vdmadmin` para habilitar la autenticación de clientes que intenten conectarse a sus escritorios remotos a través de una instancia del servidor de conexión.

Debe ejecutar el comando `vdmadmin` en una de las instancias del servidor de conexión del grupo que contiene la instancia que utilizarán los clientes para conectarse a sus escritorios remotos.

Aunque habilite la autenticación para una instancia independiente del servidor de conexión, todas sus instancias del grupo comparten el resto de opciones de configuración para la autenticación cliente. Solo es necesario agregar una vez una cuenta para un cliente. En un grupo del servidor de conexión, cualquier instancia habilitada de dicho servidor puede autenticar el cliente.

Si planea utilizar la pantalla completa con un escritorio basado en sesiones de un host RDS, debe agregar también la cuenta de usuario al grupo Usuarios de escritorio remoto.

Procedimiento

- 1 Habilite la autenticación de clientes en una instancia del servidor de conexión.

```
vdmadmin -Q -enable [-b argumentos_autenticación] -s servidor_conexión [-requirepassword]
```

Opción	Descripción
<code>-requirepassword</code>	Especifique que los clientes deben facilitar contraseñas. Importante Si especifica esta opción, la instancia del servidor de conexión no puede autenticar clientes que generaron contraseñas de forma automática. Si cambia la configuración de una instancia del servidor de conexión para especificar esta opción, dichos clientes no podrán autenticarse ellos mismos y obtendrán el mensaje de error Nombre de usuario desconocido o contraseña incorrecta.
<code>-s servidor_conexión</code>	Especifique el nombre NetBIOS de la instancia del servidor de conexión donde se habilitará la autenticación de clientes.

El comando habilita la instancia especificada del servidor de conexión para autenticar clientes.

- 2 Si un host RDS de Microsoft proporciona el escritorio publicado, inicie sesión en el host RDS y agregue la cuenta de usuario al grupo Usuarios de escritorio remoto.

Por ejemplo, supongamos que, en Horizon 7 Server, permite a la cuenta de usuario custom-11 utilizar un escritorio de View basado en sesiones de un host RDS. Debe iniciar sesión después en el host RDS y agregar el usuario custom-11 al grupo Usuarios de escritorio remoto desde el **Panel de control > Sistema y seguridad > Sistema > Configuración remota > Seleccionar usuarios > Agregar**.

Ejemplo: Habilitar la autenticación de clientes en modo de pantalla completa

Habilite la autenticación de clientes en la instancia csvr-2 del servidor de conexión. Los clientes con contraseñas generadas de forma automática pueden autenticarse por sí solos sin facilitar una contraseña.

```
vdmadmin -Q -enable -s csvr-2
```

Habilite la autenticación de clientes en la instancia csvr-3 del servidor de conexión y solicite a los clientes que especifiquen sus contraseñas en Horizon Client. Los clientes con contraseñas generadas de forma automática no pueden autenticarse por sí solos.

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

Pasos siguientes

Compruebe la configuración de las instancias del servidor de conexión y los clientes.

Verificar la configuración de los clientes en modo de pantalla completa

Puede usar el comando `vdmadmin` para mostrar información sobre los clientes en modo de pantalla completa y las instancias del servidor de conexión que se configuraron para autenticar dichos clientes.

Debe ejecutar el comando `vdmadmin` en una de las instancias del servidor de conexión del grupo que contiene la instancia que utilizarán los clientes para conectarse a sus escritorios remotos.

Procedimiento

- ◆ Visualice la información sobre los clientes en modo de pantalla completa y la autenticación de los clientes.

```
vdmadmin -Q -clientauth -list [-b argumentos_autenticación] [-xml]
```

El comando muestra información sobre los clientes en modo de pantalla completa y las instancias del servidor de conexión en la que habilitó la autenticación del cliente.

Ejemplo: Mostrar la información de los clientes en modo de pantalla completa

Muestra la información sobre los clientes en formato de texto. El cliente cm-00_0c_29_0d_a3_e6 tiene una contraseña generada de forma automática y no requiere un script de una aplicación o un usuario final para especificar esta contraseña a Horizon Client. El cliente cm-00_22_19_12_6d_cf tiene una contraseña especificada explícitamente y requiere que el usuario final la proporcione. La instancia del servidor de conexión CONSVR2 acepta las solicitudes de autenticación de clientes con contraseñas generadas de forma automática. CONSVR1 no acepta solicitudes de autenticación desde clientes en modo de pantalla completa.

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
Domain              : myorg.com
Password Generated: true

GUID                : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID            : cm-00_22_19_12_6d_cf
Domain              : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name          : CONSVR1
Client Authentication Enabled : false
Password Required     : false

Common Name          : CONSVR2
Client Authentication Enabled : true
Password Required     : false
```

Pasos siguientes

Compruebe que los clientes se puedan conectar a los escritorios remotos.

Conectarse a escritorios remotos desde clientes en modo de pantalla completa

Puede ejecutar el cliente desde una línea de comandos o usar un script para conectar un cliente a una sesión remota.

Lo habitual es usar un script de comandos para ejecutar Horizon Client en un dispositivo cliente implementado.

Nota En un cliente Mac o Windows, los dispositivos USB no se reenvían automáticamente de forma predeterminada si otra aplicación u otro servicio los están utilizando cuando se inicia la sesión del escritorio remoto. En todos los clientes, los dispositivos de interfaz de usuario (HID) y los lectores de tarjetas inteligentes no se reenvían de forma predeterminada.

Procedimiento

- ◆ Para conectarse a una sesión remota, introduzca el comando apropiado según la plataforma que utilice.

Opción	Descripción
Windows	<p>Introduzca</p> <pre>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL <i>servidor_conexión</i>] [-userName <i>nombre_usuario</i>] [-password <i>contraseña</i>]</pre> <p>-password<i>contraseña</i> Especifica la contraseña para la cuenta del cliente. Si definió una contraseña para la cuenta, debe especificarla.</p> <p>-serverURL <i>servidor_conexión</i> Especifica la dirección IP o el FQDN de la instancia del servidor de conexión que Horizon Client usará para conectarse al escritorio. Si no especifica la dirección IP o el FQDN de la instancia del servidor de conexión que el cliente usará para conectarse al escritorio remoto, el cliente usa la instancia predeterminada del servidor de conexión que configuró para ello.</p> <p>-userName <i>nombre_usuario</i> Especifica el nombre de la cuenta del cliente. Si desea que un cliente se autentique con un nombre de cuenta que comienza con una cadena de prefijo reconocida, como "custom-", en lugar de usar la dirección MAC, debe especificar este nombre.</p>
Linux	<p>Introduzca</p> <pre>vmware-view --unattended -s <i>servidor_conexión</i> [--once] [-u <i>nombre_usuario</i>] [-p <i>contraseña</i>]</pre> <p>--once Especifica que no desea que Horizon Client vuelva a intentar conectarse si se produce un error.</p> <hr/> <p>Importante Normalmente, es necesario que especifique esta opción y que use el código de salida para solucionar el error. De lo contrario, será difícil terminar el proceso <code>vmware-view</code> de forma remota.</p> <hr/> <p>-p<i>contraseña</i> Especifica la contraseña para la cuenta del cliente. Si definió una contraseña para la cuenta, debe especificarla.</p> <p>-s <i>servidor_conexión</i> Especifica la dirección IP o el FQDN de la instancia del servidor de conexión que el cliente usará para conectarse al escritorio.</p> <p>-u <i>nombre_usuario</i> Especifica el nombre de la cuenta del cliente. Si desea que un cliente se autentique con un nombre de cuenta que comienza con una cadena de prefijo reconocida, como "custom-", en lugar de usar la dirección MAC, debe especificar este nombre.</p>

Si el servidor autentica el cliente en modo de pantalla completa y un escritorio remoto está disponible, el comando inicia la sesión remota.

Ejemplo: Ejecutar Horizon Client en clientes en modo de pantalla completa

Ejecute Horizon Client en un cliente Windows cuyo nombre de cuenta esté basado en su dirección MAC y que tenga una contraseña generada automáticamente.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL  
consrv2.myorg.com
```

Ejecute Horizon Client en un cliente Linux utilizando una contraseña y un nombre asignados.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```


Solucionar problemas relacionados con Horizon 7

11

Existen varios procedimientos para diagnosticar y arreglar los problemas que pueda encontrar cuando utilice Horizon 7. Puede utilizar Horizon Help Desk Tool para solucionar problemas, usar otros procedimientos para investigarlos y solucionarlos, u obtener asistencia del equipo de soporte técnico de VMware.

Para obtener información sobre la solución de problemas relacionados con los escritorios y grupos de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Usar Horizon Help Desk Tool](#)
- [Usar VMware Logon Monitor](#)
- [Usar VMware Horizon Performance Tracker](#)
- [Supervisar el estado del sistema](#)
- [Supervisar eventos en Horizon 7](#)
- [Recopilar información de diagnóstico para Horizon 7](#)
- [Actualizar las solicitudes de soporte](#)
- [Solucionar un emparejamiento de servidor de seguridad con el servidor de conexión de Horizon que no se realizó correctamente](#)
- [Solucionar problemas relacionados con la comprobación de revocación de certificados de Horizon 7 Server](#)
- [Solucionar problemas relacionados con la comprobación de revocación de la tarjeta inteligente](#)
- [Más información para solucionar problemas](#)

Usar Horizon Help Desk Tool

Horizon Help Desk Tool es una aplicación web que puede utilizar para obtener el estado de las sesiones de usuario de Horizon 7 y para realizar operaciones de mantenimiento y de solución de problemas.

En Horizon Help Desk Tool, puede buscar sesiones de usuarios para solucionar problemas y realizar operaciones de mantenimiento de escritorios, como reiniciarlos y restablecerlos.

Para configurar Horizon Help Desk Tool, debe cumplir los siguientes requisitos:

- Licencia de la edición Horizon Enterprise o de la edición Horizon Apps Advanced para Horizon 7. Para comprobar que tiene la licencia correcta, consulte [Comprobar la licencia de Horizon Help Desk Tool](#).
- Una base de datos de eventos para almacenar información acerca de los componentes de Horizon 7. Para obtener más información sobre cómo configurar una base de datos de eventos, consulte el documento *Instalación de Horizon 7*.
- Las funciones Administrador del departamento de soporte técnico o Administrador del departamento de soporte técnico (solo lectura) para iniciar sesión en Horizon Help Desk Tool. Para obtener más información sobre estas funciones, consulte [Configurar el acceso basado en funciones para Horizon Help Desk Tool](#).
- Habilite el generador de perfiles en cada instancia del servidor de conexión para ver los segmentos de inicio de sesión.

Utilice el siguiente comando `vdadmin` para habilitar el generador de perfiles de intervalos en cada instancia del servidor de conexión:

```
vdadmin -I -timingProfiler -enable
```

Utilice el siguiente comando `vdadmin` para habilitar el generador de perfiles de intervalos en una instancia del servidor de conexión que use un puerto de administración:

```
vdadmin -I -timingProfiler -enable -server {ip/server}
```

Comprobar la licencia de Horizon Help Desk Tool

No puede iniciar sesión en Horizon Help Desk Tool si no tiene una clave de licencia del producto que sea válida. Puede comprobar la clave de licencia del producto en Horizon Administrator y aplicar una licencia válida.

Requisitos previos

- Obtenga una clave de licencia de producto válida para las licencias de la edición Horizon Enterprise o la edición Horizon Apps Advanced.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Licencia y uso del producto**.

El primer y los últimos cinco caracteres de la clave de licencia actual aparecen en el panel **Licencia**.

- Compruebe el estado de la licencia en el campo **Licencia del departamento de soporte técnico**.

Opción	Descripción
Deshabilitado	La clave de licencia de producto no es válida. No se puede iniciar sesión en Horizon Help Desk Tool.
Habilitado	La clave de licencia de producto es válida. Puede iniciar sesión en Horizon Help Desk Tool.

- (opcional) Si la clave de licencia de producto no es válida, haga clic en **Editar licencia**, introduzca el número de serie válido de la licencia, haga clic en **Aceptar** y actualice la URL de Horizon Administrator.

La ventana **Licencia de producto** muestra la información actualizada de la licencia.

Pasos siguientes

Inicie sesión en Horizon Help Desk Tool.

Configurar el acceso basado en funciones para Horizon Help Desk Tool

Puede asignar las funciones predefinidas de los administradores de Horizon Help Desk Tool para delegar las tareas de solución de problemas de un usuario administrador a otro. También puede crear funciones personalizadas y agregar privilegios según las funciones predefinidas de los administradores.

Puede asignar las siguientes funciones predefinidas a los administradores de Horizon Help Desk Tool:

- Administrador del departamento de soporte técnico
- Administrador del departamento de soporte técnico (solo lectura)

Si crea una función personalizada para un administrador de Horizon Help Desk Tool, debe asignar el privilegio Administrar el departamento de soporte técnico (solo lectura) junto con otros privilegios basados en las funciones Administrador del departamento de soporte técnico o Administradores del departamento de soporte técnico (solo lectura).

Requisitos previos

Familiarícese con los privilegios de administrador disponibles para crear funciones personalizadas. Consulte [Funciones y privilegios predefinidos](#).

Procedimiento

- En Horizon Administrator, seleccione **Configuración de View > Administradores** y haga clic en la pestaña **Funciones**.

- 2 En la pestaña **Funciones**, haga clic en **Agregar función** y seleccione la función Administrador del departamento de soporte técnico o Administrador del departamento de soporte técnico (solo lectura) y haga clic en **Aceptar**.
 - a (opcional) Para agregar una función personalizada, en la pestaña **Funciones**, haga clic en **Agregar función** y seleccione el privilegio Administrar el departamento de soporte técnico (solo lectura), seleccione los privilegios basados en la función Administrador del departamento de soporte técnico o Administrador del departamento de soporte técnico (solo lectura) y haga clic en **Aceptar**.

Iniciar sesión en Horizon Help Desk Tool

Horizon Help Desk Tool está integrado en Horizon Console. A partir de la versión 7.5 de Horizon 7, no podrá seguir utilizando la URL de Horizon Help Desk Tool para iniciar sesión en Horizon Help Desk Tool.

Procedimiento

- 1 Para iniciar sesión en Horizon Help Desk Tool desde Horizon Administrator, haga clic en **Horizon Console**, que aparece en el panel superior derecho. Este es un inicio de sesión Single Sign-On en la interfaz web de Horizon Console.
- 2 En Horizon Console, introduzca un nombre de usuario en el campo Búsqueda de usuarios.
Horizon Console muestra una lista de usuarios en los resultados de búsqueda. La búsqueda puede devolver 100 resultados de coincidencia.
- 3 Seleccione un nombre de usuario.
La información del usuario aparece en una ficha de usuario.

Pasos siguientes

Para solucionar problemas, haga clic en las pestañas pertinentes de la ficha de usuario.

Solucionar los problemas de los usuarios en Horizon Help Desk Tool

En Horizon Help Desk Tool, puede consultar la información básica del usuario gracias a una ficha de usuario. Puede hacer clic en las pestañas de la ficha de usuario para obtener más información sobre los componentes específicos.

En ocasiones, los detalles de los usuarios pueden aparecer en tablas. Puede ordenar estos detalles en columnas.

- Para ordenar una columna en orden ascendente, haga clic una vez en la columna.
- Para ordenar una columna en orden descendente, haga clic dos veces en la columna.
- Para no ordenar la columna, haga clic en la columna tres veces.

Información básica del usuario

Muestra la información básica del usuario, como el nombre, el número de teléfono y la dirección de correo electrónico, así como si está conectado o desconectado. Si el usuario tiene una sesión de aplicación o de escritorio, el estado es conectado. Si el usuario no tiene ninguna sesión de aplicación ni de escritorio, el estado es desconectado.

Puede hacer clic en el número de teléfono para iniciar una sesión de Skype Empresarial para comunicarse con el usuario y colaborar con él en la solución de los problemas.

También puede hacer clic en el correo electrónico para enviarle un mensaje al usuario.

Sesiones

La pestaña **Sesiones** muestra la información sobre las sesiones de aplicaciones o de escritorios a las que el usuario está conectado.

Puede utilizar el cuadro de texto **Filtrar** para filtrar las sesiones de aplicaciones o de escritorios.

Nota La pestaña **Sesiones** no muestra la información de las sesiones que usan el protocolo de visualización Microsoft RDP o las que acceden a las máquinas virtuales desde vSphere Client o ESXi.

La pestaña **Sesiones** incluye la siguiente información:

Tabla 11-1. Pestaña Sesiones

Opción	Descripción
Estado	<p>Muestra información sobre el estado de la sesión de la aplicación o del escritorio.</p> <ul style="list-style-type: none"> ■ Si la sesión está conectada, aparece en verde. ■ L, si la sesión es local o si una sesión se ejecuta en el pod local. ■ G, si la sesión se ejecuta en un pod diferente de la federación.
Nombre del equipo	<p>Nombre de la sesión de aplicación o del escritorio. Haga clic en el nombre para abrir la información de la sesión en una ficha.</p> <p>Puede hacer clic en las pestañas de la ficha de sesión para ver información adicional:</p> <ul style="list-style-type: none"> ■ La pestaña Detalles muestra la información del usuario, como la información de la máquina virtual, la CPU o el uso de memoria. Consulte Detalles de las sesiones de Horizon Help Desk Tool. ■ La pestaña Procesos muestra la información de los procesos relacionados con la CPU y la memoria. Consulte Procesos de las sesiones de Horizon Help Desk Tool. ■ La pestaña Aplicaciones muestra los detalles acerca de las aplicaciones que están en ejecución. Consulte Estados de las aplicaciones para Horizon Help Desk Tool.

Tabla 11-1. Pestaña Sesiones (Continuación)

Opción	Descripción
Protocolo	Protocolo de visualización de la sesión de aplicación o de escritorio.
Tipo	Muestra si el escritorio es un escritorio publicado, un escritorio de máquina virtual o una aplicación.
Hora de conexión	La hora a la que se conectó la sesión al servidor de conexión.
Duración de la sesión	El tiempo durante el cual la sesión permaneció conectada al servidor de conexión.

Autorizaciones de escritorios

La pestaña **Autorizaciones de escritorios** muestra información sobre los escritorios publicados y los virtuales para los que el usuario tiene autorización.

Tabla 11-2. Autorizaciones de escritorios

Opción	Descripción
Estado	Muestra información sobre el estado de la sesión de escritorio. <ul style="list-style-type: none"> ■ Si la sesión está conectada, aparece en verde.
Nombre de grupo de escritorios	Nombre del grupo de escritorios de la sesión.
Tipo de escritorio	Indica si el escritorio es un escritorio publicado o de máquina virtual. <p>Nota No muestra información sobre si la sesión se ejecuta en un pod diferente de la federación.</p>
Tipo	Muestra información sobre el tipo de autorización de escritorio. <ul style="list-style-type: none"> ■ Local, para una autorización local. ■ Global, para una autorización global.
vCenter	Muestra el nombre de la máquina virtual de vCenter Server. <p>Nota No muestra información sobre si la sesión se ejecuta en un pod diferente de la federación.</p>
Protocolo predeterminado	Protocolo de visualización predeterminado de la sesión de aplicación o de escritorio.

Autorizaciones de aplicaciones

La pestaña **Autorizaciones de aplicaciones** muestra información sobre las aplicaciones publicadas para las que el usuario tiene autorización.

Tabla 11-3. Autorizaciones de aplicaciones

Opción	Descripción
Estado	Muestra información sobre el estado de la sesión de aplicación. <ul style="list-style-type: none"> ■ Si la sesión está conectada, aparece en verde.
Aplicaciones	Muestra los nombres de las aplicaciones publicadas del grupo de aplicaciones.
Granja	Nombre de la granja que contiene el host RDS al que la sesión está conectada. Nota En el caso de una autorización de aplicación global, esta columna muestra el número de granjas de la autorización global.
Tipo	Muestra información sobre el tipo de autorización de aplicación. <ul style="list-style-type: none"> ■ Local, para una autorización local. ■ Global, para una autorización global.
Editor	Nombre del fabricante de software de la aplicación publicada.

Actividades

La pestaña **Actividades** muestra la información de los registros de eventos referentes a las actividades de los usuarios. Puede filtrar las actividades por un intervalo de tiempo, como por las últimas 12 horas, los últimos 30 días o por nombre de administrador. Haga clic en **Solo eventos del departamento de soporte técnico** para filtrar únicamente por actividades de Horizon Help Desk Tool. Haga clic en el icono de actualización para actualizar el registro de eventos. Haga clic en el icono de exportación para exportar el registro de eventos a un archivo.

Nota No se muestra la información del registro de eventos para los usuarios en un entorno CPA.

Tabla 11-4. Actividades

Opción	Descripción
Time	Seleccione un intervalo de tiempo. El valor predeterminado es las últimas 12 horas. <ul style="list-style-type: none"> ■ Últimas 12 horas ■ Últimas 24 horas ■ Últimos 7 días ■ Últimos 30 días ■ Todo
Administradores	Nombre del usuario administrador.
Mensaje	Muestra los mensajes de un usuario o administrador que sean específicos a las actividades que el usuario o administrador realizó.
Nombre del recurso	Muestra información sobre el nombre de la máquina virtual o del grupo de escritorios en el que se realizó la actividad.

Detalles de las sesiones de Horizon Help Desk Tool

La información de los usuarios de la sesión aparece en la pestaña **Detalles** cuando hace clic en el nombre de un usuario en la opción **Nombre del equipo** que aparece en la pestaña **Sesiones**. Puede consultar información sobre Horizon Client y sobre la CPU y la memoria, así como el escritorio virtual o publicado.

Horizon Client

La información que muestra depende del tipo de Horizon Client e incluye detalles como el nombre de usuario, la versión de Horizon Client, la dirección IP del equipo cliente y el sistema operativo del equipo cliente.

Nota Si actualizó Horizon Agent, debe actualizar también Horizon Client a la versión más reciente. En caso contrario, no se muestra ninguna versión de Horizon Client. Para obtener más información sobre cómo actualizar Horizon Client, consulte el documento *Actualizaciones de Horizon 7*.

MV

Muestra información acerca de los escritorios virtuales o publicados.

Tabla 11-5. Detalles de la máquina virtual

Opción	Descripción
Nombre del equipo	Nombre de la sesión de aplicación o del escritorio.
Versión del agente	Versión de Horizon Agent.
Estado de la sesión	Estado de la sesión de aplicación o de escritorio.
Duración del estado	El tiempo durante el cual la sesión se mantuvo en el mismo estado.
Hora de inicio de sesión	La hora en la que el usuario inició la sesión.
Duración de inicio de sesión	El tiempo durante el cual el usuario tuvo la sesión iniciada.
Duración de la sesión	El tiempo durante el cual la sesión permaneció conectada al servidor de conexión.
Servidor de conexión	El servidor de conexión al que la sesión está conectada.
Nombre de Unified Access Gateway	Nombre del dispositivo Unified Access Gateway. Esta información puede tardar entre 30 y 60 segundos en aparecer después de conectarse a la sesión.
IP de Unified Access Gateway	Dirección IP del dispositivo Unified Access Gateway. Esta información puede tardar entre 30 y 60 segundos en aparecer después de conectarse a la sesión.
Grupo	Nombre del grupo de aplicaciones o de escritorios.
Granja	La granja de hosts RDS de la sesión de aplicación o de escritorio publicados.
vCenter	Dirección IP de vCenter Server.

Mostrar métricas de BLAST

Muestra información sobre el rendimiento de una sesión de escritorio publicada o virtual que usa el protocolo de visualización VMware Blast. Para ver esa información, haga clic en **Mostrar métricas de BLAST**.

Tabla 11-6. Detalles del protocolo de visualización Blast

Opción	Descripción
Contadores de sesiones de BLAST	<ul style="list-style-type: none"> ■ Ancho de banda estimado (enlace ascendente). Ancho de banda estimado de la señal del enlace ascendente. ■ Pérdida de paquetes (enlace ascendente). Porcentaje de pérdida de paquetes de la señal del enlace ascendente.
Contadores de imágenes de BLAST	<ul style="list-style-type: none"> ■ Bytes transmitidos. Número total de bytes de datos de imágenes transmitidos durante una sesión Blast. ■ Bytes recibidos. Número total de bytes de datos de imágenes recibidos durante una sesión Blast.
Contadores de audio de BLAST	<ul style="list-style-type: none"> ■ Bytes transmitidos. Número total de bytes de datos de audio transmitidos durante una sesión Blast. ■ Bytes recibidos. Número total de bytes de datos de audio recibidos durante una sesión Blast.
Contadores de CDR de BLAST	<ul style="list-style-type: none"> ■ Bytes transmitidos. Número total de bytes de datos del redireccionamiento de la unidad cliente transmitidos durante una sesión Blast. ■ Bytes recibidos. Número total de bytes de datos del redireccionamiento de la unidad cliente recibidos durante una sesión Blast.

CPU, memoria y latencia

Muestra gráficos del uso de memoria y de CPU de las aplicaciones o los escritorios virtuales o publicados, y la latencia del protocolo de visualización Blast.

Tabla 11-7. Detalles de CPU, memoria y latencia

Opción	Descripción
CPU de la sesión	Uso de CPU de la sesión actual.
CPU del host	Uso de CPU de la máquina virtual a la que está asignada la sesión.
Memoria de la sesión	Uso de memoria de la sesión actual.

Tabla 11-7. Detalles de CPU, memoria y latencia (Continuación)

Opción	Descripción
Memoria del host	Uso de la memoria de la máquina virtual a la que está asignada la sesión.
Latencia de la sesión	<p>Muestra un gráfico de la latencia del protocolo de visualización Blast o PCoIP.</p> <p>Para el protocolo de visualización Blast, el tiempo de latencia es el tiempo de ida y vuelta en milisegundos. El contador de rendimiento que realiza un seguimiento de este tiempo de latencia es Contadores de VMware Blast Session > RTT.</p> <p>Para el protocolo de visualización PCoIP, el tiempo de latencia es el tiempo de latencia de ida y vuelta en milisegundos. El contador de rendimiento que realiza un seguimiento de este tiempo de latencia es Estadísticas de red de sesiones PCoIP > Latencia de ida y vuelta.</p>

Segmentos de inicio de sesión

Muestra los segmentos de uso y de duración del inicio de sesión que se crean durante el proceso de inicio de sesión.

Tabla 11-8. Segmentos de inicio de sesión

Opción	Descripción
Duración de inicio de sesión	Tiempo calculado desde la hora en la que el usuario hace clic en el grupo de aplicaciones o de escritorios hasta la hora en la que el Explorador de Windows se inicia.
Hora de inicio de la sesión	El tiempo durante el cual el usuario tuvo la sesión iniciada.
Segmentos de inicio de sesión	<p>Muestra los segmentos que se crean durante el inicio de sesión.</p> <ul style="list-style-type: none"> ■ Brokering. Tiempo total que tarda el servidor de conexión en procesar una conexión de sesión o en volver a conectarse. Se calcula desde que el usuario hace clic en el grupo de escritorios hasta la hora en la que se configura la conexión del túnel. Incluye los tiempos para tareas del servidor de conexión, como la autenticación del usuario, la selección del equipo y la preparación del equipo para configurar la conexión del túnel. ■ Cargar GPO. Tiempo total del procesamiento de la directiva de grupo de Windows. Si no hay ninguna directiva global configurada, aparece 0. ■ Cargar perfil. Tiempo total del procesamiento del perfil de usuario de Windows. ■ Interactivo. Tiempo total que tarda Horizon Agent en procesar una conexión de sesión o en volver a conectarse. Se calcula desde la hora en la que PCoIP o Blast Extreme usan la conexión del túnel hasta la hora en la que se inicia el Explorador de Windows. ■ Autenticación. Tiempo total que tarda el servidor de conexión en autenticar la sesión. ■ Inicio de máquina virtual. Tiempo total que tarda una máquina virtual en iniciarse. Este tiempo incluye el tiempo que tarda en arrancar el sistema operativo, en reanudar una máquina en suspensión y el tiempo que tarda Horizon Agent en notificar que está preparado para establecer una conexión.

Siga las siguientes directrices cuando use la información de los segmentos de inicio de sesión para solucionar problemas:

- Si la sesión es una nueva sesión de escritorio virtual, aparecen todos los segmentos de inicio de sesión. Si no se configuró ninguna directiva global, el tiempo del segmento de inicio de sesión **Cargar GPO** es 0.
- Si la sesión de escritorio virtual es una sesión que se volvió a conectar desde una sesión desconectada, aparecen los segmentos de inicio de sesión **Duración de inicio de sesión**, **Interactivo** y **Brokering**.
- Si la sesión es una sesión de escritorio publicado, aparecen los segmentos de inicio de sesión **Duración de inicio de sesión**, **Cargar GPO** o **Cargar perfil**. Deben aparecer los segmentos de inicio de sesión **Cargar GPO** y **Cargar perfil** para las nuevas sesiones. Si estos segmentos de inicio de sesión no aparecen para las nuevas sesiones, debe reiniciar el host RDS.

Procesos de las sesiones de Horizon Help Desk Tool

Los procesos de las sesiones aparecen en la pestaña **Procesos** cuando hace clic en el nombre de un usuario en la opción **Nombre del equipo** que aparece en la pestaña **Sesiones**.

Procesos

Puede consultar información adicional sobre los procesos de CPU y memoria de cada sesión. Por ejemplo, si advierte que el uso de memoria y de CPU de una sesión es demasiado elevado, puede consultar información del proceso en la pestaña **Procesos**.

Tabla 11-9. Detalles de los procesos de las sesiones

Opción	Descripción
Nombre del proceso	Nombre del proceso de la sesión. Por ejemplo, chrome.exe.
CPU	Porcentaje del uso de CPU del proceso.
Memoria	KB del uso de memoria del proceso.
Disco	E/S por segundo del disco de memoria. Se calcula con la siguiente fórmula: (Bytes de E/S totales en este momento) - (Bytes de E/S totales un segundo después). Este cálculo puede resultar en un valor de 0 KB por segundo si el Administrador de tareas muestra un valor positivo.
Nombre de usuario	Nombre del usuario propietario del proceso.
CPU del host	Uso de CPU de la máquina virtual a la que está asignada la sesión.
Memoria del host	Uso de la memoria de la máquina virtual a la que está asignada la sesión.
Procesos	Recuento de procesos de la máquina virtual
Actualizar	El icono de actualización actualiza la lista de procesos.
Finalizar proceso	Finaliza un proceso que se está ejecutando.
<p>Nota Debe tener la función Administrador del departamento de soporte técnico.</p> <p>Para finalizar un proceso, selecciónelo y haga clic en el botón Finalizar proceso.</p>	

Estados de las aplicaciones para Horizon Help Desk Tool

Puede consultar el estado y la información de una aplicación en la pestaña **Aplicaciones**, si hace clic en un nombre de usuario en la opción **Nombre del equipo** que aparece en la pestaña **Sesiones**.

Aplicaciones

Puede consultar el estado actual y otros detalles de cada aplicación.

Tabla 11-10. Detalles de las aplicaciones

Opción	Descripción
Aplicación	Nombre de la aplicación.
Descripción	Descripción de la aplicación.
Estado	Estado de la aplicación. Indica si la aplicación se está ejecutando.
CPU del host	Uso de CPU de la máquina virtual a la que está asignada la sesión.
Memoria del host	Uso de la memoria de la máquina virtual a la que está asignada la sesión.
Aplicaciones	Lista de las aplicaciones que se están ejecutando.
Actualizar	El icono de actualización actualiza la lista de aplicaciones.

Solucionar problemas de las sesiones de aplicaciones o de escritorios de Horizon Help Desk Tool

En Horizon Help Desk Tool, puede solucionar los problemas de las sesiones de aplicaciones de escritorios según el estado de conexión del usuario.

Requisitos previos

- Inicie Horizon Help Desk Tool.

Procedimiento

- 1 En la ficha de usuario, haga clic en la pestaña **Sesiones**.

Aparece una ficha de rendimiento que muestra el uso de la memoria y la CPU, e incluye la información sobre Horizon Client y el escritorio virtual o publicado.

2 Seleccione una opción para solucionar el problema.

Opción	Acción
Enviar mensaje	<p>Envía un mensaje al usuario del escritorio virtual o publicado. Puede seleccionar que la gravedad del mensaje incluya Advertencia, Información o Error.</p> <p>Haga clic en Enviar mensaje, escriba el tipo de gravedad y los detalles del mensaje y, a continuación, haga clic en Enviar.</p>
Asistencia remota	<p>Puede generar tickets de asistencia remota para las sesiones conectadas de aplicaciones o de escritorios. Los administradores pueden usar el ticket de asistencia remota para controlar el escritorio del usuario y solucionar los problemas.</p> <p>Haga clic en Asistencia remota y descargue el archivo de ticket del soporte técnico. Abra el ticket y espere que el usuario la acepte en el escritorio remoto. Solo puede abrir el ticket en un escritorio Windows. Después de que el usuario acepte el ticket, puede comunicarse con él y solicitarle permiso para controlar su escritorio.</p> <p>Nota La función de asistencia remota del soporte técnico se basa en la Asistencia remota de Microsoft. Debe instalar la Asistencia remota de Microsoft y habilitar la función Asistencia remota en el escritorio publicado. Es posible que la asistencia remota del soporte técnico no se inicie si la Asistencia remota de Microsoft tiene problemas de conexión o de actualización. Para obtener más información, consulte la documentación sobre la Asistencia remota de Microsoft en el sitio web.</p>
Reiniciar	<p>Inicia el proceso de reinicio de Windows en el escritorio virtual. Esta función no está disponible para una sesión de aplicación o de escritorio publicados.</p> <p>Haga clic en Reiniciar VDI.</p>
Desconectar	<p>Desconectar la sesión de aplicación o de escritorio.</p> <p>Haga clic en Más > Desconectar.</p>
Cerrar sesión	<p>Inicia el cierre de sesión de un escritorio virtual o publicado, o bien cierra sesión del proceso de una sesión de aplicación.</p> <p>Haga clic en Más > Cerrar sesión.</p>
Restablecer	<p>Inicia el restablecimiento de la máquina virtual. Esta función no está disponible para una sesión de aplicación o de escritorio publicados.</p> <p>Haga clic en Más > Restablecer máquina virtual.</p> <p>Nota El usuario puede perder el trabajo no guardado.</p>

Usar VMware Logon Monitor

VMware Logon Monitor supervisa los inicios de sesión de los usuarios de Windows e informa sobre las métricas de rendimiento para ayudar a los administradores, al personal y a los desarrolladores a resolver los problemas de rendimiento lento al iniciar sesión.

Las métricas incluyen el tiempo de inicio de sesión, el tiempo del script de inicio de sesión, el uso de la CPU y la memoria, y la velocidad de la conexión de red. Logon Monitor también puede recibir métricas de otros productos de VMware para proporcionar más información sobre el proceso de inicio de sesión.

Plataformas admitidas

Logon Monitor admite las mismas plataformas de Windows que Horizon Agent.

Funciones principales

Logon Monitor proporciona las siguientes funciones:

- Se instala como parte de Horizon Agent y se habilita de forma predeterminada.
- Se integra con el generador de perfiles de intervalos de Horizon Help Desk Tool. Las métricas relacionadas con el inicio de sesión se agregan y se envían a la base de datos de eventos de Horizon Agent.
- Permite a los clientes cargar registros a un servidor de archivos para que el acceso sea más sencillo.
- Se integra con otros productos de VMware, como Horizon Persona Management, App Volumes, UEM y el Horizon Agent que envía eventos a Logon Monitor relacionados con los inicios de sesión. Logon Monitor registra los eventos conforme aparecen para mostrar los eventos en el flujo de inicio de sesión y cuánto tiempo duran.
- Supervisa los inicios de sesión simultáneos en la misma máquina.

Registros

Logon Monitor escribe los archivos de registro para los mensajes de estado del servicio y para una sesión de usuario. De forma predeterminada, los archivos de registro se escriben en `C:\ProgramData\VMware\VMware Logon Monitor\Logs`.

- Registro principal: el archivo de registro principal, `vm1m.txt`, contiene todos los mensajes de estado para el servicio `vm1m` y los eventos de sesión que aparecen antes y después de supervisar el inicio de sesión. Compruebe este registro para determinar si Logon Monitor se está ejecutando correctamente.

- Registro de sesión: el registro de sesión contiene todos los eventos relacionados con el inicio de sesión de un usuario. Los eventos empiezan en este registro cuando el inicio de sesión comienza y solo se aplica a una única sesión de usuario. Un resumen al final del registro proporciona una descripción general de las métricas más importantes. Compruebe este registro para solucionar los problemas de inicios de sesión lentos. Cuando se completa el inicio de sesión, no se escriben más eventos en el registro de sesión.

Métricas de Logon Monitor

Logon Monitor procesa métricas relacionadas con el inicio de sesión, la directiva de grupo, el perfil del usuario y el rendimiento. Estas métricas proporcionan a los administradores una vista detallada de los sistemas de los usuarios finales durante el tiempo de inicio de sesión para ayudar a determinar la causa principal de que aparezcan cuellos de botella de rendimiento.

Tabla 11-11. Métricas de Logon Monitor

Métrica	Parámetros	Descripción
Tiempo para iniciar sesión	<ul style="list-style-type: none"> ■ Iniciar ■ Fin ■ Tiempo total 	Las métricas incluyen la hora de inicio de sesión en el invitado, de la finalización del inicio de sesión, la hora en la que se carga el perfil y el tiempo en el que el escritorio está visible, así como el tiempo total empleado para procesar el inicio de sesión en el invitado. Excluye el tiempo que se pasa fuera del invitado.
Tiempo para comenzar a iniciar sesión	Tiempo total	Tiempo desde que Windows crea una sesión de usuario hasta que comienza el inicio de sesión.
Tiempo para sincronizar el perfil	Tiempo total	Tiempo que tarda Windows en conciliar el perfil de usuario durante el inicio de sesión.
Carga de shell	<ul style="list-style-type: none"> ■ Iniciar ■ Fin ■ Tiempo total 	Windows proporciona a la hora de inicio de la carga de shell del usuario. La hora de finalización corresponde al momento de creación de la ventana del explorador.
Tiempo de inicio de sesión para cargar claves	Tiempo total	Las métricas proporcionan el tiempo total desde que el inicio de sesión comenzó hasta que se carga la clave del registro de usuario.

Tabla 11-11. Métricas de Logon Monitor (Continuación)

Métrica	Parámetros	Descripción
Redireccionamiento de carpetas de Windows	<ul style="list-style-type: none"> ■ Iniciar ■ Fin ■ Tiempo total 	Métricas relacionadas con la hora en la que el redireccionamiento de las carpetas de Windows comienza y se aplica completamente, así como el tiempo total necesario para habilitar el redireccionamiento de las carpetas de Windows. Este tiempo puede ser elevado la primera vez que se aplica el redireccionamiento de carpetas o si se cargan nuevos archivos al recurso compartido redireccionado.
Tiempo para aplicar las directivas de grupos	<ul style="list-style-type: none"> ■ Tiempo de aplicación de la directiva de grupo del usuario ■ Tiempo de aplicación de la directiva de grupo de la máquina 	Las métricas relacionadas con la aplicación de directiva de grupo al invitado incluyen el tiempo que tarda en aplicar la directiva de grupo del usuario y la directiva de grupo de la máquina.
Métricas de perfiles	<ul style="list-style-type: none"> ■ Tipo de perfil: local, móvil y temporal ■ Tamaño de perfil: número de archivos, de carpetas y megabytes totales 	Las métricas relacionadas con el perfil de usuario indican el tipo de perfil de usuario y si se almacena en la máquina local, en un almacén central de perfiles o si se eliminan después de cerrar sesión. El tamaño del perfil incluye las métricas del número de archivos, el número total de carpetas y el tamaño total en MB del perfil del usuario.
Distribución del tamaño de los perfiles	<ul style="list-style-type: none"> ■ Número de archivos entre 0 y 1 MB ■ Número de archivos entre 1 MB y 10 MB ■ Número de archivos entre 10 MB y 100 MB ■ Número de archivos entre 100 MB y 1 GB ■ Número de archivos entre 1 GB y 10 GB 	Un recuento del número de archivos en varios rangos de tamaños del perfil de usuario.
Procesos iniciados durante el inicio de sesión	<ul style="list-style-type: none"> ■ Nombre ■ ID de proceso ■ ID de proceso principal ■ ID de sesión 	Estos valores se registran para cada proceso que se inicia desde la hora en la que la sesión se inicia hasta el momento en el que esta se completa.
Tiempo para el script de inicio de sesión de la directiva de grupo	Tiempo total	Las métricas relacionadas con la ejecución de los scripts de inicio de sesión de la directiva de grupo informan sobre el tiempo total empleado para ejecutar dichos scripts.
Tiempo para el script PowerShell de la directiva de grupo	Tiempo total	Las métricas relacionadas con la ejecución de los scripts de PowerShell de la directiva de grupo indican el tiempo empleado para ejecutar dichos scripts.

Tabla 11-11. Métricas de Logon Monitor (Continuación)

Métrica	Parámetros	Descripción
Uso de memoria	<ul style="list-style-type: none"> ■ Bytes disponibles: mín., máx., media ■ Bytes asignados: mín., máx., media ■ Bloque paginado: mín., máx., media 	Métricas de WMI relacionadas con el uso de la memoria durante el inicio de sesión. Se recopilan muestras hasta que se completa el inicio de sesión. Deshabilitado de forma predeterminada.
Uso de CPU	<ul style="list-style-type: none"> ■ CPU inactiva: mín., máx., media ■ CPU de usuario: mín., máx., media ■ CPU de kernel: mín., máx., media 	Métricas de WMI relacionadas con el uso de CPU durante el inicio de sesión. Se recopilan muestras hasta que se completa el inicio de sesión. Deshabilitado de forma predeterminada.
¿Los scripts de inicio de sesión son sincrónicos?		Informa si los scripts de inicio de sesión de la directiva de grupo se ejecutan de forma sincrónica o asincrónica con respecto al inicio de sesión.
Estado de la conexión de red	<ul style="list-style-type: none"> ■ Interrumpida ■ Restaurada 	Informa si la conexión de red está activa o desconectada.
Instalación del software de la directiva de grupo	<ul style="list-style-type: none"> ■ Asincrónico: true/false ■ Código de error ■ Tiempo total 	Las métricas relacionadas con la instalación del software de directiva de grupo indican si las instalaciones son sincrónicas o asincrónicas con respecto al inicio de sesión, si las instalaciones se realizaron correctamente o si se produjo un error y el tiempo total empleado para instalar el software con la directiva de grupo.
Uso de disco para el volumen de perfiles	<ul style="list-style-type: none"> ■ Espacio de disco disponible para el usuario ■ Espacio de disco libre ■ Espacio de disco total 	Métricas relacionadas con el uso de disco en el volumen en el que el perfil de usuario se almacena.
Detección de controladores de dominio	<ul style="list-style-type: none"> ■ Código de error ■ Tiempo total 	Métricas relacionadas con el controlador de dominio. El código de error indica si existe algún error al acceder al controlador de dominio.
Ancho de banda de red estimado	Ancho de banda	Valor recopilado del evento con ID 5327.
Detalles de la conexión de red	<ul style="list-style-type: none"> ■ Ancho de banda ■ Umbral del vínculo lento ■ Vínculo lento detectado: true/false 	Valores recopilados del evento con ID 5314.

Tabla 11-11. Métricas de Logon Monitor (Continuación)

Métrica	Parámetros	Descripción
Opciones que pueden afectar al tiempo de inicio de sesión	<ul style="list-style-type: none"> ■ Equipo\Plantillas administrativas\Inicio de sesión\Esperar siempre la detección de red al inicio del equipo y de sesión ■ Equipo\Plantillas administrativas\Inicio de sesión\Ejecutar estos programas cuando el usuario inicie la sesión ■ Equipo\Plantillas administrativas\Perfiles de usuario\Esperar al perfil móvil de usuario ■ Equipo\Plantillas administrativas\Perfiles de usuario\Establecer el tiempo de espera máximo para la red si un usuario tiene un perfil móvil o un directorio principal remoto ■ Equipo\Plantillas administrativas\Directiva de grupo\Configurar retraso de script de inicio de sesión ■ Usuario\Plantillas administrativas\Sistema\Inicio de sesión\Ejecutar estos programas cuando el usuario inicie la sesión ■ Usuario\Plantillas administrativas\Sistema\Perfiles de usuario\Especificar directorios de red que se sincronizarán solo al iniciar y cerrar sesión 	
Métricas de Horizon Agent, Persona Management y de App Volumes		Productos de VMware que interactúan con las métricas de personalización de informes de Logon Monitor de los registros de Logon Monitor. Estas métricas pueden ayudar a determinar si alguno de estos productos pueden contribuir de forma negativa al tiempo de inicio de sesión.

Opciones de configuración de Logon Monitor

Puede configurar las opciones de Logon Monitor con los valores del Registro de Windows.

Configuración del Registro

Para cambiar las opciones de configuración, acceda a la clave del registro HKLM\Software\VMware, Inc.\VMware Logon Monitor.

Tabla 11-12. Valores de configuración de Logon Monitor

Clave del registro	Tipo	Descripción
RemoteLogPath	REG_SZ	<p>Ruta de acceso al recurso compartido remoto para cargar registros. Cuando los registros se copian al recurso compartido de registros remoto, se colocan en las carpetas especificadas por la clave de registro RemoteLogPath.</p> <p>Ejemplo: \\server\share\username%.%userdomain%. Logon Monitor crea las carpetas según sea necesario. Deshabilitado de forma predeterminada.</p> <ul style="list-style-type: none"> ■ Ruta de acceso UNC a la carpeta de registros remota ■ Opcional. Si no está configurada, no se cargará el registro. ■ Variables de entorno local opcionales admitidas.
Flags	REG_DWORD	<p>Este valor es una máscara de bits que influye en el comportamiento de Logon Monitor.</p> <ul style="list-style-type: none"> ■ El valor que puede asignar o quitar para habilitar o deshabilitar las métricas de CPU y memoria es 0x4. Deshabilitado de forma predeterminada. ■ El valor que puede asignar o eliminar para habilitar los eventos de proceso y las métricas de script de inicio de sesión es 0x8. Deshabilitado de forma predeterminada. ■ El valor que puede asignar o eliminar para habilitar o deshabilitar la integración con Horizon 7 es 0x2. Habilitado de forma predeterminada. ■ El valor que puede asignar para deshabilitar los volcados de memoria es 0x1. Los volcados de memoria se escriben en C:\ProgramData\VMware\VMware Logon Monitor\Data. Deshabilitado de forma predeterminada. ■ El valor que se configura para crear carpetas por usuario en la ruta remota es 0x10. Deshabilitado de forma predeterminada.
LogMaxSizeMB	REG_DWORD	Tamaño máximo del registro principal en MB. El tamaño predeterminado es 100 MB.
LogKeepDays	REG_DWORD	Número máximo de días que se mantiene el registro principal antes de implementarlo. El valor predeterminado es 7 días.

Configuración del generador de perfiles de intervalos

Logon Monitor se integra con el generador de perfiles de intervalos de Horizon Help Desk. El generador de perfiles está desactivado de forma predeterminada.

- Si quiere que Logon Monitor utilice el generador de perfiles de intervalos para escribir los eventos de la base de datos de eventos, ejecute `vdadmin -I -timingProfiler -enable`.
- Si quiere que Logon Monitor no utilice el generador de perfiles, ejecute `vdadmin -I -timingProfiler -disable`.

Usar VMware Horizon Performance Tracker

VMware Horizon Performance Tracker es una utilidad que se ejecuta en un escritorio remoto y supervisa el rendimiento del protocolo de visualización y el uso de los recursos del sistema. También se puede crear un grupo de aplicaciones y ejecutar Horizon Performance Tracker como aplicación publicada.

Configurar VMware Horizon Performance Tracker

Puede ejecutar Horizon Performance Tracker en un escritorio remoto. También puede ejecutar Horizon Performance Tracker como una aplicación publicada.

Funciones de Horizon Performance Tracker

Horizon Performance Tracker muestra información importante de las siguientes funciones:

Tabla 11-13. Funciones de Horizon Performance Tracker

Supervisión del rendimiento	Detalles
Datos específicos del protocolo	<ul style="list-style-type: none"> ■ Nombre del codificador: el nombre del codificador utilizado en el protocolo de visualización. ■ Ancho de banda usado: media del ancho de banda entrante y saliente del periodo de muestreo para el protocolo de visualización PCoIP o Blast. ■ Velocidad de fotogramas por segundo: número de fotogramas de imágenes que se codificaron durante un periodo de muestreo de un segundo. ■ Audio activado: indica si la función Audio está activada. ■ Audio iniciado: indica si la función Audio se inició. ■ Uso de CPU: <ul style="list-style-type: none"> ■ CPU del codificador: uso de CPU del codificador del protocolo de visualización en la sesión actual del usuario. ■ CPU del sistema: uso de CPU total del sistema.
Tipo de transporte	<ul style="list-style-type: none"> ■ Cliente a sesión remota: paquete de transporte del protocolo UDP o TCP utilizado del cliente al elemento remoto del mismo nivel. ■ Sesión remota a cliente: paquete de transporte del protocolo UDP o TCP utilizado del elemento remoto del mismo nivel al cliente. ■ Horizon Connection Server: paquete de transporte del protocolo UDP o TCP utilizado para conectarse a una instancia del servidor de conexión.
Estado de mantenimiento del sistema	<ul style="list-style-type: none"> ■ Ancho de banda estimado: estimación general del ancho de banda disponible entre Horizon Client y Horizon Agent. ■ Ida y vuelta: latencia de ida y vuelta en milisegundos entre el Horizon Agent y el Horizon Client.

Tabla 11-13. Funciones de Horizon Performance Tracker (Continuación)

Supervisión del rendimiento	Detalles
Contexto de la sesión	<ul style="list-style-type: none"> ■ Detalles del servidor, como el nombre DNS, nombre de dominio, si se envía por túnel o no, la URL o la dirección IP remota. ■ Detalles de la máquina cliente, como el número de pantalla, la dirección IP, la distribución de teclado y ratón, el idioma o la zona horaria.
Cambio de protocolo en tiempo real	

Nota Horizon Performance Tracker solo recopila y muestra los datos cuando Horizon Agent se está ejecutando en una sesión de escritorio virtual.

Requisitos del sistema para Horizon Performance Tracker

Horizon Performance Tracker admite las siguientes configuraciones.

Tabla 11-14. Requisitos del sistema para Horizon Performance Tracker

Sistema	Requisitos
Sistemas operativos de escritorios virtuales	Todos los sistemas operativos que admiten Horizon Agent
Sistemas operativos de máquinas cliente	Se admiten todas las versiones de Horizon Client, excepto Horizon Client para Linux y Horizon Client para Windows 10 UWP, ya que las aplicaciones publicadas no son compatibles.
Protocolos de visualización	VMware Blast y PCoIP

Instalar Horizon Performance Tracker

Horizon Performance Tracker es una opción de configuración personalizada del instalador de Horizon Agent. Debe seleccionar la opción, ya que no está seleccionada de forma predeterminada. Horizon Performance Tracker está disponible para IPv4 e IPv6.

Puede instalar Horizon Performance Tracker en un escritorio virtual o en un host RDS. Si lo instala en un host RDS, podrá publicarlo como aplicación publicada y ejecutarla desde Horizon Client. Consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

La instalación crea un acceso directo en el escritorio.

Configurar opciones de la directiva de grupo Horizon Performance Tracker

Puede configurar las opciones de la directiva de grupo para cambiar la configuración predeterminada. Consulte [Configurar las opciones de la directiva de grupo Horizon Performance Tracker](#).

Configurar las opciones de la directiva de grupo Horizon Performance Tracker

Para configurar Horizon Performance Tracker, instale el archivo de plantilla ADMX de Horizon Performance Tracker (`perf_tracker.admx`) en la máquina agente y use el Editor de directivas de grupo local para establecer la configuración de las directivas.

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-yyyyyyy.zip`, donde `x.x.x` es la versión e `yyyyyyy` es el número de compilación. Puede descargar el archivo desde el sitio de descargas de VMware en <https://my.vmware.com/web/vmware/downloads>. En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el archivo ZIP.

Procedimiento

- 1 Extraiga el archivo `perf_tracker.admx` del archivo `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` y cópielo en la carpeta `%systemroot%\PolicyDefinitions` de la máquina agente.
- 2 Extraiga el archivo `perf_tracker.adml` del archivo `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` y cópielo en la subcarpeta de idioma apropiada de la carpeta `%systemroot%\PolicyDefinitions` de la máquina agente.

Por ejemplo, copie la versión en_us del archivo `perf_tracker.adml` de la subcarpeta `%systemroot%\PolicyDefinitions\en_us`.

- 3 Inicie el Editor de directivas de grupo local (`gpedit.msc`) y acceda a **Configuración del equipo > Plantillas administrativas > VMware Horizon Performance Tracker**.
- 4 Edite la configuración de directiva de grupo.

Configuración	Descripción
Opción básica de Horizon Performance Tracker	Cuando está habilitada, puede establecer la frecuencia en segundos a la que Horizon Performance Tracker recopila los datos.
Habilite el inicio automático de Horizon Performance Tracker en la conexión de escritorio remoto.	Cuando se habilita, Horizon Performance Tracker se inicia automáticamente cuando un usuario inicia sesión en una conexión de escritorio remoto. Para borrar esta preferencia de opción de GPO, seleccione Deshabilitar .
Habilitar el inicio automático de Horizon Performance Tracker en la conexión de aplicación remota	Si se habilita, Horizon Performance Tracker se inicia automáticamente cuando un usuario inicia sesión en una conexión de aplicación remota. Para borrar esta preferencia de opción de GPO, seleccione Deshabilitar .

- 5 Para que se apliquen los cambios, reinicie Horizon Performance Tracker en la máquina agente.

Ejecutar Horizon Performance Tracker

Puede utilizar Horizon Client para ejecutar Horizon Performance Tracker en un escritorio remoto o como una aplicación publicada.

Si la plataforma de Horizon Client que usa admite varias sesiones, puede ejecutar varias aplicaciones publicadas Horizon Performance Tracker desde granjas diferentes. En clientes Windows y Mac que admitan varias sesiones, el nombre de la máquina en la ventana de información general identifica la granja desde la que se origina la aplicación publicada. En clientes iOS y Android, así como en HTML Access, solo se admite una sesión abierta. Si abre una segunda sesión desde otra granja, la primera se cierra.

Requisitos previos

- Instale y configure Horizon Performance Tracker. Consulte [Configurar VMware Horizon Performance Tracker](#).
- Configure las opciones de la directiva de grupo Horizon Performance Tracker. Consulte [Configurar las opciones de la directiva de grupo Horizon Performance Tracker](#).

Procedimiento

- Para ejecutar Horizon Performance Tracker en un escritorio remoto, use Horizon Client o HTML Access para conectarse al servidor e iniciar el escritorio remoto.

Si Horizon Performance Tracker no se inicia automáticamente cuando el escritorio remoto se abre, puede hacer doble clic en el acceso directo **VMware Horizon Performance Tracker** del escritorio Windows o iniciar Horizon Performance Tracker de la misma forma que inicia cualquier aplicación de Windows.

Para seleccionar las opciones para mostrar la ventana de información general o la barra flotante y salir de la aplicación, haga clic en el icono VMware Horizon Performance Tracker en la bandeja del sistema del escritorio remoto.

- Para ejecutar Horizon Performance Tracker como una aplicación publicada, use Horizon Client o HTML Access para conectarse al servidor e iniciar la aplicación publicada Horizon Performance Tracker.

La forma en la que use la aplicación publicada Horizon Performance Tracker depende del tipo de cliente que use. No puede usar Horizon Client para Linux ni Horizon Client para Windows 10 UWP para ejecutar Horizon Performance Tracker como una aplicación publicada.

- Con Horizon Client para Windows, el icono VMware Horizon Performance Tracker aparece en la bandeja de sistema en el sistema cliente Windows. Puede hacer doble clic en este icono para abrir Horizon Performance Tracker en el cliente Windows. Puede hacer clic con el botón secundario en este icono para mostrar la ventana de información general o la barra flotante, y cerrar la aplicación.
- Con Horizon Client para Mac, el icono VMware Horizon Performance Tracker aparece en la barra de menú del sistema cliente Mac. Puede hacer doble clic en este icono para abrir Horizon Performance Tracker en el cliente Mac. También puede hacer clic con el botón secundario en este icono para mostrar la ventana de información general o la barra flotante, y salir de la aplicación.

- Con Horizon Client para Android o Horizon Client para iOS, aparece el icono VMware Horizon Performance Tracker en la barra lateral Unity Touch de Horizon Client. Puede tocar y mantener pulsado este icono y mostrar la ventana de información general, la barra flotante y salir de la aplicación.
- Con HTML Access, aparece el icono VMware Horizon Performance Tracker en la barra lateral de HTML Access. Puede hacer clic con el botón secundario en este icono y mostrar la ventana de información general o la barra flotante, y salir de la aplicación.

Pasos siguientes

Para obtener más información sobre los datos que aparecen en Horizon Performance Tracker, consulte [Configurar VMware Horizon Performance Tracker](#).

Supervisar el estado del sistema

Puede usar el panel de control del estado del sistema en Horizon Administrator para ver rápidamente los problemas que puedan afectar al funcionamiento de Horizon 7 o el acceso de los usuarios finales a los escritorios remotos.

El panel de control del estado del sistema que aparece en la parte superior izquierda de la pantalla de Horizon Administrator proporciona un número de vínculos que puede usar para ver informes sobre el funcionamiento de Horizon 7:

Sesiones	Proporciona un vínculo a la pantalla Sesiones, donde aparece información sobre el estado de las sesiones de las aplicaciones y los escritorios remotos.
Máquinas virtuales de vCenter con problemas	Proporciona un vínculo a la pantalla Máquinas, donde aparece información sobre las máquinas virtuales de vCenter, los hosts RDS y otras máquinas que Horizon 7 marcó con problemas.
Host RDS con problemas	Proporciona un vínculo a la pestaña Host RDS en la pantalla Máquinas, donde aparece información sobre los hosts RDS que Horizon 7 marcó con problemas.
Eventos	Proporciona vínculos a la pantalla Eventos filtrada por los eventos de error y los eventos de advertencia.
Estado del sistema	Proporciona vínculos a la pantalla Panel, que muestra resúmenes sobre el estado de los componentes de Horizon 7, detalles de Unified Access Gateway registrados para la versión 3.4 o posterior, uso del almacén de datos, escritorios, dominios y componentes de vSphere.

El panel de control del estado del sistema muestra un vínculo numerado con cada elemento. Este valor indica el número de elementos sobre los que el informe vinculado proporciona información.

Supervisar eventos en Horizon 7

La base de datos de eventos almacena información sobre los eventos que tienen lugar en el grupo o el host del servidor de conexión, en Horizon Agent y en Horizon Administrator, y le notifica el número de eventos del panel de control. Puede examinar todos los detalles de los eventos en la pantalla Eventos.

Nota Los eventos aparecen en la interfaz de Horizon Administrator durante un periodo de tiempo limitado. Después, los eventos solo están disponibles en las tablas históricas de la base de datos. Puede usar las herramientas de informe de la base de datos de Oracle o Microsoft SQL Server para examinar los eventos de las tablas de la base de datos. Para obtener más información, consulte el documento *Integración de Horizon 7*.

Nota Si la base de datos de eventos no está disponible, Horizon 7 conserva el historial para auditorías de los eventos que tuvieron lugar en ese periodo y los guarda en la base de datos de eventos cuando vuelve a estar disponible. Debe reiniciar la base de datos de eventos y el servidor de conexión para que dichos eventos aparezcan en la interfaz de Horizon Administrator.

Además de supervisar los eventos de Horizon Administrator, puede generar los eventos de Horizon 7 en formato syslog para que los software de análisis puedan acceder a la información de los eventos. Consulte [Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -l](#) y "Configurar el registro de eventos para servidores Syslog" en el documento *Instalación de Horizon 7*.

Requisitos previos

Cree y configure la base de datos de eventos como aparece descrito en el documento *Instalación de Horizon 7*.

Procedimiento

- 1 En Horizon Administrator, seleccione **Supervisar > Eventos**.
- 2 (opcional) En la ventana Eventos puede seleccionar el rango de tiempo de esos eventos, aplicar filtros y ordenar los que aparecen por una o varias columnas.

Mensajes de eventos de Horizon 7

Horizon 7 informa sobre los eventos cuando cambia el estado del sistema o existe algún problema. Puede usar la información de los mensajes de eventos para realizar la acción apropiada.

La siguiente tabla muestra los tipos de eventos que notifica Horizon 7.

Tabla 11-15. Tipos de eventos notificados por Horizon 7

Tipo de evento	Descripción
Error de auditoría o Auditoría correcta	Informa sobre si se realizó correctamente o no un cambio que un administrador o un usuario realiza en la operación o en la configuración de Horizon 7.
Error	Notifica que Horizon 7 no realizó una operación correctamente.

Tabla 11-15. Tipos de eventos notificados por Horizon 7 (Continuación)

Tipo de evento	Descripción
Información	Notifica las operaciones normales de Horizon 7.
Advertencia	Notifica problemas menores con las opciones de configuración o de operación que pueden derivar a problemas más graves con el tiempo.

Es posible que sea necesario realizar alguna acción si aparecen mensajes relacionados con Error de auditoría, Error o Eventos de advertencia. No es necesario que realice ninguna acción cuando aparecen eventos de Información o de Auditoría correcta.

Recopilar información de diagnóstico para Horizon 7

Puede recopilar información de diagnóstico para ayudar al equipo de soporte técnico de VMware a diagnosticar y resolver problemas con Horizon 7.

Puede recopilar información de diagnóstico para varios componentes de Horizon 7. La forma de recopilar dicha información varía en función del componente de Horizon 7.

- [Crear un paquete de herramientas de recopilación de datos para Horizon Agent](#)

Para ayudar al equipo de soporte técnico de VMware a solucionar los problemas de Horizon Agent, es posible que necesite usar el comando `vdmadmin` para crear un paquete de herramientas de recopilación de datos (DCT). También puede obtener el paquete DCT de forma manual sin usar `vdmadmin`.

- [Guardar información de diagnóstico de Horizon Client](#)

Si al utilizar Horizon Client encuentra problemas que no puede solucionar con las técnicas generales, puede guardar una copia de los archivos de registro y la información de la configuración.

- [Recopilar información de diagnóstico de View Composer con el script de soporte](#)

Puede usar el script de soporte de View Composer para recopilar datos de configuración y generar archivos de registro de View Composer. Esta información ayuda al equipo de asistencia al cliente de VMware a diagnosticar cualquier problema que se produzca con View Composer.

- [Recopilar información de diagnóstico del servidor de conexión de Horizon](#)

Puede usar la herramienta de soporte para establecer niveles de registro y generar archivos de registro del servidor de conexión de Horizon.

- [Recopilar información de diagnóstico de Horizon Agent, de Horizon Client o del servidor de conexión de Horizon desde la consola](#)

Si cuenta con acceso directo a la consola, puede usar los scripts de soporte para generar archivos de registro del servidor de conexión, de Horizon Client o de los escritorios remotos que ejecutan Horizon Agent. Esta información ayuda al equipo de asistencia técnica de VMware a diagnosticar cualquier problema que se produzca con estos componentes.

Crear un paquete de herramientas de recopilación de datos para Horizon Agent

Para ayudar al equipo de soporte técnico de VMware a solucionar los problemas de Horizon Agent, es posible que necesite usar el comando `vdadmin` para crear un paquete de herramientas de recopilación de datos (DCT). También puede obtener el paquete DCT de forma manual sin usar `vdadmin`.

Para su comodidad, puede usar el comando `vdadmin` en una instancia del servidor de conexión para solicitar un paquete DCT desde un escritorio remoto. El paquete se devuelve al servidor de conexión.

Puede iniciar sesión de forma alternativa en un escritorio remoto específico y ejecutar un comando `support` que cree el paquete DCT en ese escritorio. Si Control de cuentas de usuario (UAC) está activado, debe obtener el paquete DCT de esta manera.

Procedimiento

- 1 Inicie sesión como un usuario con los privilegios necesarios.

Opción	Acción
En el servidor de conexión de View, con <code>vdadmin</code>	Inicie sesión en el servidor de conexión estándar o réplica como un usuario con la función Administradores .
En el escritorio remoto	Inicie sesión en el escritorio remoto como un usuario con privilegios administrativos.

- 2 Abra una ventana de símbolo de sistema y ejecute el comando para generar el paquete DCT.

Opción	Acción
En el servidor de conexión de View, con <code>vdadmin</code>	Para especificar los nombres en el archivo del paquete de salida, el grupo de escritorios y el equipo, use las opciones <code>-outfile</code> , <code>-d</code> y <code>-m</code> con el comando <code>vdadmin</code> . <pre>vdadmin -A [-b argumentos_autenticación] -getDCT -outfile archivo_local -d escritorio -m equipo</pre>
En el escritorio remoto	Cambie los directorios a <code>c:\Program Files\VMware\VMware View\Agent\DCT</code> y ejecute el siguiente comando: <pre>support</pre>

El comando registra el paquete en el archivo de salida especificado.

Ejemplo: Usar `vdadmin` para crear un archivo de paquete para Horizon Agent

Cree el paquete DCT para la máquina `machine1` en el grupo de escritorios `dtpool2` y regístrelo en el archivo zip `C:\myfile.zip`.

```
vdadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

Pasos siguientes

Si tiene una solicitud de soporte ya existente, puede actualizarla adjuntando el archivo del paquete DCT.

Guardar información de diagnóstico de Horizon Client

Si al utilizar Horizon Client encuentra problemas que no puede solucionar con las técnicas generales, puede guardar una copia de los archivos de registro y la información de la configuración.

Puede intentar solucionar los problemas de conexión de Horizon Client antes de guardar la información de diagnóstico y contactar con el equipo de soporte técnico de VMware. Para obtener más información, consulte "Problemas de conexión entre Horizon Client y el servidor de conexión de Horizon" en el documento *Configurar escritorios virtuales en Horizon 7*.

Procedimiento

- 1 En Horizon Client, haga clic en **Información de soporte técnico** o bien seleccione **Opciones > Información de soporte técnico** en el menú del escritorio remoto.
- 2 En la ventana **Información de soporte**, haga clic en **Recopilar datos del soporte técnico** y haga clic en **Sí** cuando se le solicite.

El progreso de recopilación de información se mostrará en una ventana de comandos. Este proceso puede tardar varios minutos.

- 3 En la ventana de comandos, para responder a las solicitudes, introduzca las URL de las instancias del servidor de conexión de Horizon en las que quiere probar la configuración de Horizon Client y, si es necesario, seleccione la opción para generar los volcados del diagnóstico de los procesos de Horizon 7.

La información se escribe en un archivo zip dentro de una carpeta del escritorio del equipo cliente.

- 4 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte el archivo zip de salida.

Recopilar información de diagnóstico de View Composer con el script de soporte

Puede usar el script de soporte de View Composer para recopilar datos de configuración y generar archivos de registro de View Composer. Esta información ayuda al equipo de asistencia al cliente de VMware a diagnosticar cualquier problema que se produzca con View Composer.

Requisitos previos

Inicie sesión en el equipo en el que View Composer está instalado.

Como debe utilizar la utilidad Windows Script Host (cscript) para ejecutar el script de soporte, familiarícese con ella usando cscript. Consulte <http://technet.microsoft.com/library/bb490887.aspx>.

Procedimiento

- 1 Abra una ventana de símbolo del sistema y cambie el directorio C:\Program Files\VMware\VMware View Composer.

Si no instaló el software en los directorios predeterminados, sustituya la ruta y la letra de la unidad que correspondan.

- 2 Escriba el comando para ejecutar el script svi-support.

```
cscript ".\svi-support.wsf" /zip
```

Puede usar la opción /? para visualizar información sobre otras opciones de comandos que están disponibles con el script.

Cuando el script finalice, le informa del nombre y la ubicación del archivo de salida.

- 3 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte el archivo de salida.

Recopilar información de diagnóstico del servidor de conexión de Horizon

Puede usar la herramienta de soporte para establecer niveles de registro y generar archivos de registro del servidor de conexión de Horizon.

La herramienta de soporte recopila datos de registro del servidor de conexión. Esta información ayuda al equipo de asistencia técnica de VMware a diagnosticar cualquier problema que se produzca con el servidor de conexión. La herramienta de soporte no está destinada a recopilar información de Horizon Client o de Horizon Agent. En su lugar debe usar el script de soporte. Consulte [Recopilar información de diagnóstico de Horizon Agent, de Horizon Client o del servidor de conexión de Horizon desde la consola](#).

Requisitos previos

Inicie sesión en la instancia del servidor de conexión estándar o réplica como un usuario con la función **Administradores**.

Procedimiento

- 1 Seleccione **Inicio > Todos los programas > VMware > Establecer los niveles del servidor de conexión de View**.
- 2 En el cuadro de texto **Elección**, escriba un valor numérico para establecer el nivel de registro y pulse Intro.

Opción	Descripción
0	Restablece el nivel de registro al valor predeterminado.
1	Selecciona un nivel normal de registro.

Opción	Descripción
2	Selecciona un nivel de depuración de registro (predeterminada).
3	Selecciona un registro completo.

El sistema comienza a recopilar información de registro con el nivel de detalle que seleccionó.

- 3 Cuando recopile información suficiente sobre el comportamiento del servidor de conexión, seleccione **Inicio > Todos los programas > VMware > Generar paquete de registro del servidor de conexión de View**.

La herramienta de soporte crea los archivos de registro en una carpeta denominada vdm-sdct en el escritorio de la instancia del servidor de conexión.

- 4 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte los archivos de salida.

Recopilar información de diagnóstico de Horizon Agent , de Horizon Client o del servidor de conexión de Horizon desde la consola

Si cuenta con acceso directo a la consola, puede usar los scripts de soporte para generar archivos de registro del servidor de conexión, de Horizon Client o de los escritorios remotos que ejecutan Horizon Agent. Esta información ayuda al equipo de asistencia técnica de VMware a diagnosticar cualquier problema que se produzca con estos componentes.

Requisitos previos

Inicie sesión en el sistema en el que quiere recopilar información. Debe iniciar sesión como un usuario con privilegios de administrador.

- Para Horizon Agent, inicie sesión en la máquina virtual que tenga Horizon Agent instalado.
- Para Horizon Client, inicie sesión en el sistema con Horizon Client instalado.
- Para el servidor de conexión, inicie sesión en el host del servidor de conexión.

Procedimiento

- 1 Abra una ventana de símbolo del sistema y cambie al directorio apropiado de los componentes de Horizon 7 de los que desee recopilar información de diagnóstico.

Opción	Descripción
Horizon Agent	Cambiar al directorio C:\Program Files\VMware View\Agent\DCT.
Horizon Client	Cambiar al directorio C:\Program Files\VMware View\Client\DCT.
Servidor de conexión de View	Cambiar al directorio C:\Program Files\VMware View\Server\DCT.

Si no instaló el software en los directorios predeterminados, sustituya la ruta y la letra de la unidad que correspondan.

2 Escriba el comando para ejecutar el script de soporte.

```
.\support.bat [loglevels]
```

Si desea habilitar el inicio de sesión avanzado, especifique la opción `loglevels` e introduzca el valor numérico del nivel de registro cuando se solicite.

Opción	Descripción
0	Restablece el nivel de registro al valor predeterminado.
1	Selecciona un nivel normal de registro.
2	Selecciona un nivel de depuración de registro (predeterminada).
3	Selecciona un registro completo.
4	Selecciona el registro informativo de PColP (únicamente Horizon Agent y Horizon Client).
5	Selecciona el registro de depuración de PColP (únicamente Horizon Agent y Horizon Client).
6	Selecciona el registro informativo de los canales virtuales (únicamente Horizon Agent y Horizon Client).
7	Selecciona el registro de depuración de los canales virtuales (únicamente Horizon Agent y Horizon Client).
8	Selecciona el registro de seguimiento de los canales virtuales (únicamente Horizon Agent y Horizon Client).

El script crea los archivos de registros comprimidos en la carpeta `vdm-sdct` del escritorio.

- 3 Puede encontrar los registros del agente invitado de View Composer en el directorio `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support`.
- 4 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte el archivo de salida.

Actualizar las solicitudes de soporte

Puede actualizar la solicitud de soporte existente en el sitio web Soporte.

Después de registrar una solicitud de soporte, es posible que reciba una solicitud por correo electrónico del equipo de soporte técnico de VMware en la que le pidan el archivo de salida de los scripts `support` o `svi-support`. Cuando ejecuta los scripts, obtiene información sobre el nombre y la ubicación del archivo de salida. Responda al mensaje y adjunte a la respuesta el archivo de salida.

Si el archivo de salida es demasiado grande para incluirlo como archivo adjunto (10 MB o más), póngase en contacto con el equipo de soporte técnico de VMware, dígalos el número de la solicitud de soporte y solicite instrucciones para cargarlo por FTP. De forma alternativa, puede adjuntar el archivo a la solicitud de soporte existente a través del sitio web de Soporte.

Procedimiento

- 1 Visite la página Soporte en el sitio web de VMware e inicie sesión.

- 2 Haga clic en **Historial de solicitudes de soporte** y busque el número de solicitud de soporte aplicable.
- 3 Actualice la solicitud de soporte y adjunte el archivo saliente que obtuvo al ejecutar los scripts support o svi-support.

Solucionar un emparejamiento de servidor de seguridad con el servidor de conexión de Horizon que no se realizó correctamente

Es posible que un servidor de seguridad no funcione si no se emparejó correctamente con una instancia del servidor de conexión de Horizon.

Problema

Si un servidor de seguridad no se empareja correctamente con el servidor de conexión, pueden producirse los siguientes problemas en el servidor de seguridad:

- Cuando intenta instalar el servidor de seguridad por segunda vez, este no puede conectarse al servidor de conexión.
- Horizon Client no puede conectarse a Horizon 7. Aparece el siguiente mensaje de error: Se produjo un error en la autenticación del servidor de conexión de View. Ninguna puerta de enlace está disponible para proporcionar una conexión segura a un escritorio. Póngase en contacto con su administrador de red.
- El servidor de seguridad aparece en el panel de control de Horizon Administrator como Fuera de servicio.

Causa

Este problema se puede producir si comenzó a instalar un servidor de seguridad y se canceló o se anuló el proceso después de introducir una contraseña de emparejado del servidor de seguridad.

Solución

Si tiene pensado mantener el servidor de seguridad en el entorno de Horizon 7, siga estos pasos:

- 1 En Horizon Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de seguridad**, seleccione un servidor de seguridad; a continuación, seleccione **Preparar para la actualización o para la reinstalación** en el menú desplegable **Más comandos** y haga clic en **Aceptar**.
- 3 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión que desee emparejar con el servidor de seguridad. A continuación, seleccione **Especificar contraseña para emparejar al servidor de seguridad** en el menú desplegable **Más comandos**, escriba una contraseña y haga clic en **Aceptar**.
- 4 Vuelva a instalar el servidor de seguridad.

Si pretende eliminar la entrada del servidor de seguridad del entorno de Horizon 7, ejecute el comando `vdmadmin -S`.

Por ejemplo: `vdmadmin -S -r -s nombre_servidor_seguridad`

Solucionar problemas relacionados con la comprobación de revocación de certificados de Horizon 7 Server

Un servidor de seguridad o una instancia del servidor de conexión que se utilice para conexiones de Horizon Client seguras aparecerá en rojo en View Administrator si la comprobación de revocación de certificados no se puede realizar en el certificado TLS del servidor.

Problema

El icono del servidor de seguridad o del servidor de conexión aparece en color rojo en el panel de control de Horizon Administrator. El estado del servidor de Horizon 7 muestra el siguiente mensaje: El certificado del servidor no se puede comprobar.

Causa

La comprobación de revocación de certificados puede fallar si la organización utiliza un servidor proxy para acceder a Internet o si la instancia del servidor de conexión no puede alcanzar los servidores que ofrecen la comprobación de revocación debido al firewall u otros controles.

Una instancia del servidor de conexión comprueba la revocación de certificados en su propio certificado y en los servidores de seguridad emparejados. De forma predeterminada, el servicio del servidor de conexión de VMware Horizon View se inicia con la cuenta LocalSystem. Al ejecutarse con LocalSystem, la instancia del servidor de conexión no puede utilizar la configuración del proxy de Internet Explorer para acceder a la URL de puntos de distribución de listas de revocación de certificados o al respondedor OCSP para determinar el estado de revocación del certificado.

Puede utilizar el comando Netshell de Microsoft para importar la configuración del proxy a la instancia del servidor de conexión y que así el servidor pueda acceder a los sitios de comprobación de revocación de certificados en Internet.

Solución

- 1 En el equipo del servidor de conexión, abra una ventana de línea de comando con la opción **Ejecutar como administrador**.

Por ejemplo: haga clic en **Iniciar**, escriba **cmd**, haga clic con el botón secundario en el icono **cmd.exe** y seleccione **Ejecutar como administrador**.

- 2 Escriba **netsh** y pulse Intro.
- 3 Escriba **winhttp** y pulse Intro.
- 4 Escriba **show proxy** y pulse Intro.

Netshell muestra que la conexión del proxy se configuró como DIRECT. Con esta opción, el equipo del servidor de conexión no puede conectarse a Internet si la organización está usando el proxy.

5 Configure las opciones del proxy.

Por ejemplo: en la solicitud `netsh winhttp>`, escriba **`import proxy source=ie`**.

La configuración del proxy se importa al equipo del servidor de conexión.

6 Escriba **`show proxy`** para comprobar la configuración del proxy.**7** Reinicie el servicio del servidor de conexión VMware Horizon View.**8** En el panel de control de Horizon Administrator, compruebe que el icono del servidor de conexión o del servidor de seguridad aparezca en verde.

Solucionar problemas relacionados con la comprobación de revocación de la tarjeta inteligente

La instancia del servidor de conexión o el servidor de seguridad que tengan la tarjeta inteligente conectada no pueden realizar comprobaciones de revocación del certificado TLS a menos que configurara la comprobación de revocación del certificado de la tarjeta inteligente.

Problema

Se puede producir un error en la comprobación de revocación de certificados si la organización utiliza un servidor proxy para acceder a Internet, o bien si una instancia del servidor de conexión o el servidor de seguridad no pueden acceder a los servidores que ofrecen la comprobación de revocación debido al firewall u otros controles.

Importante Asegúrese de que el archivo CRL esté actualizado.

Causa

Horizon 7 admite la comprobación de revocación de certificados con listas de revocación de certificados (CRL) y con el protocolo de estado de certificado en línea (OCSP). Una CRL es una lista de certificados revocados publicada por la autoridad de certificación (CA) que los emitió. OCSP es un protocolo de validación de certificados que se utiliza para obtener el estado de revocación de un certificado X.509. Es necesario que se pueda acceder a la CA desde el host del servidor de conexión o del servidor de seguridad. Este problema puede ocurrir si configuró la comprobación de revocación de los certificados de tarjetas inteligentes. Consulte [Uso de la comprobación de revocación de certificados de tarjeta inteligente](#).

Solución

- 1 Cree su propio procedimiento (manual) para descargar y actualizar la CRL en una ruta de Horizon 7 Server desde el sitio web de la CA que utiliza.
- 2 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_de_instalación\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

- 3 Agregue las propiedades `enableRevocationChecking` y `crlLocation` en el archivo `locked.properties` de la ruta local donde la CRL está almacenada.
- 4 Reinicie el servicio del servidor de conexión o el servicio del servidor de seguridad para que se apliquen los cambios.

Más información para solucionar problemas

Puede encontrar más información para solucionar problemas en los artículos de la base de conocimientos de VMware.

La base de conocimientos de VMware (KB) se actualiza de forma continua con nueva información para solucionar los problemas de los productos de VMware.

Para obtener más información sobre cómo solucionar los problemas de Horizon 7, consulte los artículos de la KB que están disponibles en el sitio web de la KB de VMware:

<http://kb.vmware.com/selfservice/microsites/microsite.do>

Usar el comando vdmadmin

Puede usar la interfaz de línea de comandos `vdmadmin` para realizar varias tareas de administración en una instancia del servidor de conexión.

Puede usar `vdmadmin` para realizar tareas de administración que no se puedan hacer desde la interfaz de usuario de Horizon Administrator o para realizar tareas de administración que se tengan que ejecutar automáticamente desde scripts.

Para obtener una comparación de las operaciones que se pueden realizar con Horizon Administrator, con cmdlets de Horizon 7 y con `vdmadmin`, consulte el documento *Integración de Horizon 7*.

- **Uso del comando vdmadmin**

La sintaxis de los comandos de `vdmadmin` controla su funcionamiento.

- **Configurar los registros en Horizon Agent con la opción -A**

Puede usar el comando `vdmadmin` con la opción `-A` para configurar los registros de Horizon Agent.

- **Sobrescribir direcciones IP con la opción -A**

El comando `vdmadmin` con la opción `-A` permite sobrescribir la dirección que muestra Horizon Agent.

- **Actualizar las entidades de seguridad externa con la opción -F**

Puede usar el comando `vdmadmin` con la opción `-F` para actualizar las entidades de seguridad externa (FSP) de los usuarios de Windows en Active Directory con autorización para usar un escritorio.

- **Enumerar y mostrar las supervisiones de estado con la opción -H**

Puede usar el comando `vdmadmin -H` para enumerar las supervisiones de estado existentes, para supervisar las instancias de los componentes de Horizon 7 y para mostrar los detalles de una instancia específica de supervisión o de supervisión de estado.

- **Especificar y visualizar informes sobre el funcionamiento de Horizon 7 con la opción -I**

Puede usar el comando `vdmadmin` con la opción `-I` para mostrar los informes disponibles sobre el funcionamiento de Horizon 7 y los resultados tras ejecutar uno de dichos informes.

- **Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -l**

Puede usar el comando `vdmadmin` con la opción `-I` para registrar mensajes de eventos de Horizon 7 en formato `syslog` en archivos de registro de eventos. Muchos productos de análisis de terceros requieren datos `syslog` en archivo plano de entrada para las operación de análisis.

- **Asignar máquinas dedicadas usando la opción -L**

Puede usar el comando `vdadmin` con la opción `-L` para asignar máquinas de un grupo dedicado a los usuarios.

- **Visualizar información sobre las máquinas con la opción -M**

Puede usar el comando `vdadmin` con la opción `-M` para ver la información sobre la configuración de máquinas virtuales o equipos físicos.

- **Recuperar espacio de disco de las máquinas virtuales con la opción -M**

El comando `vdadmin` con la opción `-M` permite seleccionar una máquina virtual de clones vinculados en la que realizar una operación de recuperación de espacio de disco. Horizon 7 dirige el host ESXi para recuperar espacio de disco del SO de clones vinculados sin esperar a que el espacio sin utilizar del disco del SO alcance el umbral mínimo que se especifica en Horizon Administrator.

- **Configurar filtros de dominios con la opción -N**

Puede usar el comando `vdadmin` con la opción `-N` para los dominios que Horizon 7 tiene disponibles para los usuarios finales.

- **Configurar los filtros de dominios**

Puede configurar los filtros de dominio para limitar los dominios que una instancia del servidor de conexión o un servidor de seguridad tienen disponibles para los usuarios finales.

- **Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P**

Puede usar el comando `vdadmin` con las opciones `-O` y `-P` para mostrar las directivas y las máquinas virtuales que están asignadas a usuarios que ya no tienen autorización para usar el sistema.

- **Configurar clientes en modo de pantalla completa con la opción -Q**

Puede usar el comando `vdadmin` con la opción `-Q` para establecer valores predeterminados y crear cuentas de clientes en modo de pantalla completa, para habilitar la autenticación de dichos clientes y para mostrar la información de su configuración.

- **Visualizar el primer usuario de un equipo con la opción -R**

Puede usar el comando `vdadmin` con la opción `-R` para encontrar la asignación inicial de una máquina virtual administrada. Por ejemplo, en el caso de perder datos LDAP, es posible que necesite esta información para poder volver a asignar las máquinas virtuales a los usuarios.

- **Eliminar una entrada de una instancia del servidor de conexión o del servidor de seguridad con la opción -S**

Puede usar el comando `vdadmin` con la opción `-S` para eliminar la entrada de la instancia del servidor de conexión o del servidor de seguridad de la configuración de Horizon 7.

- **Proporcionar credenciales secundarias para los administradores con la opción -T**

Puede usar el comando `vdadmin` con la opción `-T` para proporcionar credenciales secundarias de Active Directory a los usuarios administradores.

- [Visualizar información sobre los usuarios con la opción -U](#)

Puede usar el comando `vdmadmin` con la opción `-U` para mostrar información detallada sobre los usuarios.

- [Bloquear o desbloquear las máquinas virtuales con la opción -V](#)

Puede usar el comando `vdmadmin` con la opción `-V` para bloquear o desbloquear las máquinas virtuales en el centro de datos.

- [Detectar y resolver conflictos de esquemas y entradas LDAP usando la opción -X](#)

Puede usar el comando `vdmadmin` con la opción `-X` para detectar y resolver conflictos de las entradas LDAP y los esquemas LDAP en las instancias del servidor de conexión replicadas en un grupo. También puede utilizar esta opción para detectar y resolver conflictos de esquemas y entradas LDAP en un entorno de Arquitectura de Cloud Pod.

Uso del comando `vdmadmin`

La sintaxis de los comandos de `vdmadmin` controla su funcionamiento.

Use el siguiente formato del comando de `vdmadmin` en una ventana de símbolo de sistema de Windows.

```
vdmadmin opción_comando [opción_adicional argumento] ...
```

Las opciones adicionales que puede usar dependen de la opción del comando.

De forma predeterminada, la ruta del archivo ejecutable de comandos `vdmadmin` es `C:\Program Files\VMware\VMware View\Server\tools\bin`. Para no tener que introducir la ruta en la línea de comandos, agregue la ruta a la variable del entorno `PATH`.

- [Autenticación del comando `vdmadmin`](#)

Debe ejecutar el comando `vdmadmin` como un usuario que tenga la función **Administradores** para que se realice correctamente una acción específica.

- [Formato de la salida del comando `vdmadmin`](#)

Algunas opciones del comando `vdmadmin` le permiten especificar el formato de la información de salida.

- [Opciones del comando `vdmadmin`](#)

Puede usar las opciones del comando `vdmadmin` para especificar la operación que desee que realice.

Autenticación del comando `vdmadmin`

Debe ejecutar el comando `vdmadmin` como un usuario que tenga la función **Administradores** para que se realice correctamente una acción específica.

Horizon Administrator permite asignar la función **Administradores** a un usuario. Consulte [Capítulo 6 Configurar la administración delegada basada en funciones](#).

Si inició sesión como un usuario con privilegios insuficientes, puede usar la opción `-b` para ejecutar el comando como un usuario al que se le asignara la función **Administradores**, si conoce la contraseña del usuario. Puede especificar la opción `-b` para ejecutar el comando `vdmadmin` como el usuario especificado del dominio especificado. Las siguientes formas de uso de la opción `-b` son equivalentes.

```
-b nombredeusuario dominio [contraseña | *]
```

```
-b nombredeusuario@dominio [contraseña | *]
```

```
-b dominio\nombredeusuario [contraseña | *]
```

Si especifica un asterisco (*) en lugar de una contraseña, se le solicitará introducir la contraseña y el comando `vdmadmin` no guardará contraseñas confidenciales en el historial de comandos de la línea de comandos.

Puede usar la opción `-b` con todas las opciones de comandos, excepto las opciones `-R` y `-T`.

Formato de la salida del comando `vdmadmin`

Algunas opciones del comando `vdmadmin` le permiten especificar el formato de la información de salida.

La siguiente tabla muestra las posibilidades que algunas de las opciones del comando `vdmadmin` proporcionan para dar formato al texto de salida.

Tabla 12-1. Opciones para seleccionar el formato de salida

Opción	Descripción
<code>-csv</code>	Otorga un formato a la salida de valores separados por coma.
<code>-n</code>	Visualice la salida utilizando caracteres ASCII (UTF-8). Este es el grupo de caracteres predeterminado para los valores separados por coma y la salida de texto.
<code>-w</code>	Visualice la salida utilizando caracteres Unicode (UTF-16). Este es el grupo de caracteres predeterminados para la salida XML.
<code>-xml</code>	Otorga el formato XML a la salida.

Opciones del comando `vdmadmin`

Puede usar las opciones del comando `vdmadmin` para especificar la operación que desee que realice.

La siguiente tabla muestra las opciones de comando que puede usar con el comando `vdmadmin` para controlar y examinar la operación de Horizon 7.

Tabla 12-2. Opciones del comando vdmadmin

Opción	Descripción
-A	Administra la información que Horizon Agent incluye en los archivos de registro. Consulte Configurar los registros en Horizon Agent con la opción -A . Sobrescribe la dirección IP que envía Horizon Agent. Consulte Sobrescribir direcciones IP con la opción -A .
-C	Establece el nombre de un grupo del servidor de conexión. Consulte GUID-3AD7B00C-43C4-417E-A06B-7251805657D6#GUID-3AD7B00C-43C4-417E-A06B-7251805657D6 .
-F	Actualiza las Entidades de seguridad externa (FSP) en Active Directory para todos los usuarios o para los usuarios especificados. Consulte Actualizar las entidades de seguridad externa con la opción -F .
-H	Muestra información del estado de los servicios de Horizon 7. Consulte Enumerar y mostrar las supervisiones de estado con la opción -H .
-I	Genera los informes de la operación de Horizon 7. Consulte Especificar y visualizar informes sobre el funcionamiento de Horizon 7 con la opción -I .
-L	Asigna un escritorio dedicado a un usuario o elimina una asignación. Consulte Asignar máquinas dedicadas usando la opción -L .
-M	Muestra información sobre una máquina virtual o un equipo físico. Consulte Visualizar información sobre las máquinas con la opción -M .
-N	Configura los dominios que un grupo o una instancia del servidor de conexión disponen para Horizon Client. Consulte Configurar filtros de dominios con la opción -N .
-O	Muestra los escritorios remotos que están asignados a los usuarios que ya no tienen autorización para usarlos. Consulte Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P .
-P	Muestra las directivas de usuario que están asociadas con los escritorios remotos de los usuarios sin autorización. Consulte Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P .
-Q	Configura la cuenta de Active Directory y la configuración de Horizon 7 de un dispositivo cliente en modo de pantalla completa. Consulte Configurar clientes en modo de pantalla completa con la opción -Q .
-R	Informa sobre el primer usuario que accedió a un escritorio remoto. Consulte Visualizar el primer usuario de un equipo con la opción -R .
-S	Elimina una entrada de la configuración para una instancia del servidor de conexión desde la configuración de Horizon 7. Consulte Eliminar una entrada de una instancia del servidor de conexión o del servidor de seguridad con la opción -S .
-T	Proporciona credenciales secundarias de Active Directory para los usuarios administradores. Consulte Proporcionar credenciales secundarias para los administradores con la opción -T .
-U	Muestra información sobre un usuario, incluidas las autorizaciones de escritorio remoto y las asignaciones ThinApp, así como las funciones de Administrador. Consulte Visualizar información sobre los usuarios con la opción -U .
-V	Bloquea o desbloquea las máquinas virtuales. Consulte Bloquear o desbloquear las máquinas virtuales con la opción -V .
-X	Detecta y resuelve las entradas de LDAP duplicadas en las instancias del servidor de conexión replicadas. Consulte Detectar y resolver conflictos de esquemas y entradas LDAP usando la opción -X .

Configurar los registros en Horizon Agent con la opción -A

Puede usar el comando `vdmadmin` con la opción `-A` para configurar los registros de Horizon Agent.

Sintaxis

```
vdmadmin -A [-b argumentos_autenticación] -getDCT-outfile archivo_local -d escritorio -m equipo
```

```
vdmadmin -A [-b argumentos_autenticación] -getlogfile archivo de registro -outfile archivo_local -d escritorio -m equipo
```

```
vdmadmin -A [-b argumentos_autenticación] -getloglevel [-xml] -d escritorio [-m equipo]
```

```
vdmadmin -A [-b argumentos_autenticación] -getstatus [-xml] -d escritorio [-m equipo]
```

```
vdmadmin -A [-b argumentos_autenticación] -getversion [-xml] -d escritorio [-m equipo]
```

```
vdmadmin -A [-b argumentos_autenticación] -list [-xml] [-w | -n] -d escritorio -m equipo
```

```
vdmadmin -A [-b argumentos_autenticación] -setloglevel nivel -d escritorio [-m equipo]
```

Notas de uso

Para ayudar al equipo de soporte técnico de VMware a solucionar los problemas de Horizon Agent, puede crear un paquete de herramientas de recopilación de datos (DCT). También puede cambiar el nivel de registro, visualizar la versión y el estado de Horizon Agent y guardar los archivos de registros individuales en el disco local.

Opciones

La siguiente tabla muestra las opciones que puede especificar para configurar el registro Horizon Agent.

Tabla 12-3. Opciones para configurar los registros en Horizon Agent

Opción	Descripción
<code>-d escritorio</code>	Especifica el grupo de escritorios.
<code>-getDCT</code>	Crea un paquete de herramientas de recopilación de datos (DCT) y lo guarda en un archivo local.
<code>-getlogfile <i>archivo de registro</i></code>	Especifica el nombre del archivo de registro del que guardar una copia.
<code>-getloglevel</code>	Muestra el nivel de registro actual de Horizon Agent.

Tabla 12-3. Opciones para configurar los registros en Horizon Agent (Continuación)

Opción	Descripción						
<code>-getstatus</code>	Muestra el estado de Horizon Agent.						
<code>-getversion</code>	Muestra la versión de Horizon Agent.						
<code>-list</code>	Muestra los archivos de registro de Horizon Agent.						
<code>-m máquina</code>	Especifica la máquina dentro de un grupo de escritorios.						
<code>-outfile archivo_local</code>	Especifica el nombre del archivo local en el que se guarda un paquete DCT o una copia del archivo de registro.						
<code>-setloglevel nivel</code>	Establece el nivel de los registros de Horizon Agent.						
	<table> <tr> <td>debug</td><td>Registra los eventos de errores, de advertencias y de depuración.</td></tr> <tr> <td>normal</td><td>Registra los eventos de errores y de advertencias.</td></tr> <tr> <td>trace</td><td>Registra los eventos informativos, de errores, de advertencias y de depuración.</td></tr> </table>	debug	Registra los eventos de errores, de advertencias y de depuración.	normal	Registra los eventos de errores y de advertencias.	trace	Registra los eventos informativos, de errores, de advertencias y de depuración.
debug	Registra los eventos de errores, de advertencias y de depuración.						
normal	Registra los eventos de errores y de advertencias.						
trace	Registra los eventos informativos, de errores, de advertencias y de depuración.						

Ejemplos

Visualice el nivel de registro de Horizon Agent de la máquina machine1 del grupo de escritorios dtpool2.

```
vdmadmin -A -d dtpool2 -m machine1 -getloglevel
```

Establezca el nivel de registro de Horizon Agent de la máquina machine1 del grupo de escritorios dtpool2 para la depuración.

```
vdmadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

Visualice la lista de los archivos de registro de Horizon Agent de la máquina machine1 del grupo de escritorios dtpool2.

```
vdmadmin -A -d dtpool2 -m machine1 -list
```

Guarde una copia del archivo de registro de Horizon Agent log-2009-01-02.txt para la máquina machine1 en el grupo de escritorios dtpool2 como C:\mycopiedlog.txt.

```
vdmadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

Visualice la versión de Horizon Agent de la máquina machine1 del grupo de escritorios dtpool2.

```
vdmadmin -A -d dtpool2 -m machine1 -getversion
```

Visualice el estado de Horizon Agent de la máquina machine1 del grupo de escritorios dtpool2.

```
vdadmin -A -d dtpool2 -m machine1 -getstatus
```

Cree el paquete DCT para la máquina machine1 en el grupo de escritorios dtpool2 y regístrelo en el archivo zip C:\myfile.zip.

```
vdadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

Sobrescribir direcciones IP con la opción -A

El comando `vdadmin` con la opción `-A` permite sobrescribir la dirección que muestra Horizon Agent.

Sintaxis

```
vdadmin -A [-b argumentos_autenticación] -override -i ip_o_dns -d escritorio -m máquina
```

```
vdadmin -A [-b argumentos_autenticación] -override -list -d escritorio -m máquina
```

```
vdadmin -A [-b argumentos_autenticación] -override -r -d escritorio [-m máquina]
```

Notas de uso

Horizon Agent muestra la dirección IP descubierta de la máquina en la que se está ejecutando a la instancia del servidor de conexión. En las configuraciones seguras en las que la instancia del servidor de conexión no puede confiar en el valor que Horizon Agent muestra, puede sobrescribir el valor que le proporciona Horizon Agent y especificar la dirección IP que debe utilizar la máquina administrada. Si la dirección de una máquina que proporciona Horizon Agent no coincide con la dirección definida, no puede usar Horizon Client para acceder a la máquina.

Opciones

La siguiente tabla muestra las opciones que puede especificar para sobrescribir direcciones IP.

Tabla 12-4. Opciones para sobrescribir direcciones IP

Opción	Descripción
<code>-d escritorio</code>	Especifica el grupo de escritorios.
<code>-i ip_o_dns</code>	Especifica la dirección IP o nombre del dominio que se puede resolver en el DNS.
<code>-m máquina</code>	Especifica el nombre de la máquina en un grupo de escritorios.
<code>-override</code>	Especifica una operación para sobrescribir direcciones IP.
<code>-r</code>	Elimina una dirección IP sobrescrita.

Ejemplos

Sobrescriba la dirección IP de la máquina machine2 del grupo de escritorios dtpool2.

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

Muestre las direcciones IP definidas para la máquina machine2 del grupo de escritorios dtpool2.

```
vdmadmin -A -override -list -d dtpool2 -m machine2
```

Elimine las direcciones IP definidas para la máquina machine2 del grupo de escritorios dtpool2.

```
vdmadmin -A -override -r -d dtpool2 -m machine2
```

Elimine las direcciones IP definidas para los escritorios del grupo de escritorios dtpool3.

```
vdmadmin -A -override -r -d dtpool3
```

Actualizar las entidades de seguridad externa con la opción -F

Puede usar el comando vdmadmin con la opción -F para actualizar las entidades de seguridad externa (FSP) de los usuarios de Windows en Active Directory con autorización para usar un escritorio.

Sintaxis

```
vdmadmin -F [-b argumentos_autenticación] [-u dominio\usuario]
```

Notas de uso

Si confía en dominios que se encuentran fuera de sus dominios locales, debe permitir que las entidades de seguridad de los dominios externos accedan a los recursos de los dominios locales. Active Directory usa FSP para representar entidades de seguridad en dominios externos de confianza. Es posible que quiera actualizar las FSP de los usuarios si modifica la lista de dominios externos de confianza.

Opciones

La opción -u especifica el nombre y el dominio del usuario cuya FSP desee actualizar. Si no especifica esta opción, el comando actualiza las FSP de todos los usuarios en Active Directory.

Ejemplos

Actualice la FSP del usuario Jim en el dominio EXTERNAL.

```
vdadmin -F -u EXTERNAL\Jim
```

Actualice las FSP de todos los usuarios en Active Directory.

```
vdadmin -F
```

Enumerar y mostrar las supervisiones de estado con la opción -H

Puede usar el comando `vdadmin -H` para enumerar las supervisiones de estado existentes, para supervisar las instancias de los componentes de Horizon 7 y para mostrar los detalles de una instancia específica de supervisión o de supervisión de estado.

Sintaxis

```
vdadmin -H [-b argumentos_autenticación] -list -xml [-w | -n]
```

```
vdadmin -H [-b argumentos_autenticación] -list -monitorid id_supervisión -xml [-w | -n]
```

```
vdadmin -H [-b argumentos_autenticación] -monitorid id_supervisión -instanceid id_instancia -xml [-w | -n]
```

Notas de uso

La siguiente tabla muestra las supervisiones de estado que usa Horizon 7 para supervisar el estado de sus componentes.

Tabla 12-5. Supervisiones de estado

Supervisar	Descripción
CBMonitor	Supervisa el estado de las instancias del servidor de conexión.
DBMonitor	Supervisa el estado de la base de datos de eventos.
DomainMonitor	Supervisa el estado del dominio local del host del servidor de conexión y todos los dominios de confianza.
SGMonitor	Supervisa el estado de los servicios de la puerta de enlace de seguridad y los servidores de seguridad.
VCMonitor	Supervisa el estado de los servidores de vCenter.

Si un componente tiene varias instancias, Horizon 7 crea una instancia de supervisión independiente para supervisar cada instancia del componente.

El comando muestra toda la información sobre las supervisiones de estado y las instancias de supervisión en formato XML.

Opciones

La siguiente tabla muestra las opciones que puede especificar para enumerar y ver las supervisiones de estado.

Tabla 12-6. Opciones para enumerar y mostrar las supervisiones de estado

Opción	Descripción
<code>-instanceid <i>id_instancia</i></code>	Especifica una instancia de supervisión de estado.
<code>-list</code>	Muestra las supervisiones de estado existentes si no se especificó ningún ID de supervisión de estado.
<code>-list -monitorid <i>id_supervisión</i></code>	Muestra las instancias de supervisión para el ID de supervisión de estado.
<code>-monitorid <i>id_supervisión</i></code>	Especifica un ID de supervisión de estado.

Ejemplos

Muestra todas las supervisiones de estado en XML, usando caracteres Unicode.

```
vdadmin -H -list -xml
```

Muestra todas las instancias de la supervisión de vCenter (VCMonitor) en XML, usando caracteres ASCII.

```
vdadmin -H -list -monitorid VCMonitor -xml -n
```

Muestra el estado de una instancia de supervisión vCenter específica.

```
vdadmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

Especificar y visualizar informes sobre el funcionamiento de Horizon 7 con la opción -l

Puede usar el comando `vdadmin` con la opción `-l` para mostrar los informes disponibles sobre el funcionamiento de Horizon 7 y los resultados tras ejecutar uno de dichos informes.

Sintaxis

```
vdmadmin -I [-b argumentos_autenticación] -list [-xml] [-w | -n]
```

```
vdmadmin -I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

Notas de uso

Puede utilizar el comando para visualizar los informes y vistas disponibles, además de la información que Horizon 7 almacenó para un informe y vista determinados.

También puede utilizar el comando `vdmadmin` con la opción `-I` para generar los mensajes de registro de Horizon 7 en formato `syslog`. Consulte [Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -I](#).

Opciones

La siguiente tabla muestra las opciones que puede especificar para enumerar y ver los informes y vistas.

Tabla 12-7. Opciones para especificar y visualizar informes y vistas

Opción	Descripción
<code>-enddate yyyy-MM-dd-HH:mm:ss</code>	Especifica un límite superior para la fecha de información que se visualizará.
<code>-list</code>	Enumera los informes y vistas disponibles.
<code>-report report</code>	Especifica un informe.
<code>-startdate yyyy-MM-dd-HH:mm:ss</code>	Especifica un límite inferior para la fecha de información que se visualizará.
<code>-view view</code>	Especifica una vista.

Ejemplos

Enumera los informes y vistas disponibles en XML con caracteres Unicode.

```
vdmadmin -I -list -xml -w
```

Muestra una lista de eventos de usuario que ocurrieron desde el 1 de agosto de 2010 como valores separados por comas con caracteres ASCII.

```
vdmadmin -I -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```


Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -l

Puede usar el comando `vdmadmin` con la opción `-l` para registrar mensajes de eventos de Horizon 7 en formato syslog en archivos de registro de eventos. Muchos productos de análisis de terceros requieren datos syslog en archivo plano de entrada para las operación de análisis.

Sintaxis

```
vdmadmin -l -eventSyslog -disable
```

```
vdmadmin -l -eventSyslog -enable -localOnly
```

```
vdmadmin -l -eventSyslog -enable -path ruta
```

```
vdmadmin -l -eventSyslog -enable -path ruta  
-user NombreDominio\nombreusuario -password contraseña
```

Notas de uso

Puede usar el comando para generar mensajes de registro de eventos de Horizon 7 en formato syslog. En un archivo syslog, los mensajes del registro de eventos de Horizon 7 aparecen en valores clave-valor, lo que provoca que los datos del registro sean accesible para los software de análisis.

También puede usar el comando `vdmadmin` con la opción `-l` para mostrar los informes y las vistas disponibles, así como para visualizar los contenidos de un informe específico. Consulte [Especificar y visualizar informes sobre el funcionamiento de Horizon 7 con la opción -l](#).

Opciones

Puede habilitar o deshabilitar la opción `eventSyslog`. Puede dirigir la salida de syslog al sistema local únicamente o a otra ubicación. Dirija la conexión UDP a un servidor syslog compatible con Horizon 7 5.2 o una versión posterior Consulte "Configurar el registro de eventos para servidores Syslog" en el documento *Instalación de Horizon 7*.

Tabla 12-8. Opciones para generar los mensajes del registro de eventos de Horizon 7 en formato syslog

Opción	Descripción
<code>-disable</code>	Deshabilita el registro syslog.
<code>-e -enable</code>	Habilita el registro syslog.
<code>-eventSyslog</code>	Especifica que los eventos de Horizon 7 se generan en formato syslog.

Tabla 12-8. Opciones para generar los mensajes del registro de eventos de Horizon 7 en formato syslog (Continuación)

Opción	Descripción
<code>-localOnly</code>	Almacena la salida de syslog únicamente en el sistema local. Cuando usa la opción <code>-localOnly</code> , el destino predeterminado de la salida de Syslog es <code>%PROGRAMDATA%\VMware\VDM\events\</code> .
<code>-passwordcontraseña</code>	Especifica la contraseña del usuario que autoriza el acceso a la ruta de destino especificada para la salida de syslog.
<code>-path</code>	Determina la ruta UNC de destino para la salida de syslog.
<code>-u</code> <code>-user NombreDominio\nombreusuario</code>	Especifica el nombre de usuario y el dominio que pueden acceder a la ruta de destino para la salida de syslog.

Ejemplos

Deshabilite la generación de eventos de Horizon 7 en formato syslog.

```
vdmadmin -I -eventSyslog -disable
```

Dirija la salida de syslog de los eventos de Horizon 7 únicamente al sistema local.

```
vdmadmin -I -eventSyslog -enable -localOnly
```

Dirija la salida de syslog de los eventos de Horizon 7 a una ruta especificada.

```
vdmadmin -I -eventSyslog -enable -path ruta
```

Dirija la salida de syslog de los eventos de Horizon 7 a una ruta especificada que requiera el acceso por parte de un usuario de dominio autorizado.

```
vdmadmin -I -eventSyslog -enable -path \\logserver\share\ViewEvents -user midominio\miusuario  
-password micontraseña
```

Asignar máquinas dedicadas usando la opción -L

Puede usar el comando `vdmadmin` con la opción `-L` para asignar máquinas de un grupo dedicado a los usuarios.

Sintaxis

```
vdmadmin -L [-b argumentos_autenticación] -d escritorio -m máquina -u dominio\usuario
```

```
vdmadmin -L [-b argumentos_autenticación] -d escritorio [-m máquina | -u dominio\usuario] -r
```

Notas de uso

Horizon 7 asigna máquinas a usuarios cuando se conectan por primera vez a un grupo de escritorios dedicado. En algunas circunstancias, es posible que desee preasignar máquinas a usuarios. Por ejemplo, es posible que desee preparar los entornos del sistema antes de establecer la conexión inicial. Después de que un usuario se conecte a un escritorio remoto que Horizon 7 asigna desde un grupo dedicado, la máquina virtual que aloja el escritorio sigue asignada al usuario durante la sesión de la máquina virtual. Puede asignar un usuario a una única máquina en un grupo dedicado.

Puede asignar una máquina a cualquier usuario autorizado. Es posible que desee realizar esta acción al recuperarse de la pérdida de datos LDAP de View en una instancia del servidor de conexión, o bien cuando desee cambiar la propiedad de una máquina en concreto.

Después de que un usuario se conecte a un escritorio remoto que Horizon 7 asigna desde un grupo dedicado, ese escritorio remoto sigue asignado al usuario durante la sesión de la máquina virtual que aloja el escritorio. Es posible que desee eliminar la asignación de una máquina a un usuario que dejó la organización, que ya no necesite acceso al escritorio o que usará un escritorio en un grupo de escritorios diferente. También puede eliminar las asignaciones de todos los usuarios que tienen acceso a un grupo de escritorios.

Nota El comando `vdmadmin -L` no asigna la propiedad de los discos persistentes de View Composer. Para asignar escritorios de clones vinculados con discos persistentes a los usuarios, utilice la opción del menú **Asignar usuario** en Horizon Administrator.

Si utiliza `vdmadmin -L` para asignar a un usuario un escritorio de clones vinculados con un disco persistente, se pueden producir resultados inesperados en algunas situaciones. Por ejemplo, si desconecta un disco persistente y lo usa para volver a crear un escritorio, este escritorio no se asigna al propietario del original.

Opciones

La siguiente tabla muestra las opciones que puede especificar para asignar un escritorio a un usuario o para eliminar una asignación.

Tabla 12-9. Opciones para asignar escritorios dedicados

Opción	Descripción
<code>-d escritorio</code>	Especifica el nombre del grupo de escritorios.
<code>-m máquina</code>	Especifica el nombre de la máquina virtual que aloja el escritorio remoto.
<code>-r</code>	Elimina una asignación de un usuario especificado o todas las asignaciones de una máquina específica.
<code>-u dominio\usuario</code>	Especifica el nombre de inicio de sesión y el dominio del usuario.

Ejemplos

Asigne la máquina machine2 del grupo de escritorios dtpool1 al usuario Jo del dominio CORP.

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

Elimine las asignaciones del usuario Jo del dominio CORP a los escritorios del grupo dtpool1.

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

Elimine todas las asignaciones de usuario a la máquina machine1 del grupo de escritorios dtpool3.

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

Visualizar información sobre las máquinas con la opción -M

Puede usar el comando `vdmadmin` con la opción `-M` para ver la información sobre la configuración de máquinas virtuales o equipos físicos.

Sintaxis

```
vdmadmin -M [-b argumentos_autenticación] [-m máquina | [-u dominio\usuario][-d escritorio]] [-xml | -csv] [-w | -n]
```

Notas de uso

El comando muestra información sobre un equipo físico o una máquina virtual subyacente del escritorio remoto.

- Nombre para mostrar de la máquina.
- Nombre del grupo de escritorios.
- Estado de la máquina.

El estado de la máquina puede tener uno de los siguientes valores: UNDEFINED, PRE_PROVISIONED, CLONING, CLONINGERROR, CUSTOMIZING, READY, DELETING, MAINTENANCE, ERROR, LOGOUT.

El comando no muestra todos los estados de las máquinas dinámicas, como Conectado o Desconectado, que aparecen en Horizon Administrator.

- SID del usuario asignado.
- Nombre de cuenta del usuario asignado.
- Nombre de dominio del usuario asignado.

- Ruta de inventario de la máquina virtual (si es necesaria).
- Fecha en la que se creó la máquina.
- Ruta de la plantilla de la máquina (si es necesaria).
- URL de vCenter Server (si es necesaria).

Opciones

La siguiente tabla muestra las opciones que puede usar para especificar la máquina cuyos detalles desea visualizar.

Tabla 12-10. Opciones para visualizar la información sobre las máquinas

Opción	Descripción
<code>-d escritorio</code>	Especifica el nombre del grupo de escritorios.
<code>-m máquina</code>	Especifica el nombre de la máquina virtual.
<code>-u dominio\usuario</code>	Especifica el nombre de inicio de sesión y el dominio del usuario.

Ejemplos

Visualice la información sobre la máquina subyacente del escritorio remoto en el grupo dtpool2 que está asignado al usuario Jo en el dominio CORP y que el formato del archivo salida es XML con caracteres ASCII.

```
vdadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

Visualice información sobre la máquina machine3 en un formato de valores separados por coma.

```
vdadmin -M -m machine3 -csv
```

Recuperar espacio de disco de las máquinas virtuales con la opción -M

El comando `vdadmin` con la opción `-M` permite seleccionar una máquina virtual de clones vinculados en la que realizar una operación de recuperación de espacio de disco. Horizon 7 dirige el host ESXi para recuperar espacio de disco del SO de clones vinculados sin esperar a que el espacio sin utilizar del disco del SO alcance el umbral mínimo que se especifica en Horizon Administrator.

Sintaxis

```
vdadmin -M [-b argumentos_autenticación] -d escritorio -m equipo -markForSpaceReclamation
```

Notas de uso

Con esta opción, puede iniciar la recuperación del espacio de disco en una máquina virtual en concreto para solucionar problemas o para realizar demostraciones.

La recuperación del espacio no se realiza si ejecuta este comando durante un periodo sin disponibilidad.

Para poder recuperar el espacio de disco mediante el comando `vdmadmin` con la opción `-M`, se deben cumplir los siguientes requisitos previos:

- Compruebe que Horizon 7 esté usando vCenter Server y ESXi con la versión 5.1 o con una versión posterior.
- Compruebe que la instancia de VMware Tools que se proporciona con vSphere versión 5.1 o posterior está instalada en la máquina virtual.
- Compruebe que la máquina virtual tenga la versión 9 del hardware virtual o una versión posterior.
- En Horizon Administrator, compruebe que la opción **Habilitar recuperación de espacio** esté seleccionada para vCenter Server. Consulte [Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados](#).
- En Horizon Administrator, compruebe que la opción **Reclamar espacio de disco de la máquina virtual** esté seleccionada para el grupo de escritorios. Consulte la sección sobre cómo recuperar el espacio de disco en los clones vinculados de View Composer en el documento *Configurar escritorios virtuales en Horizon 7*.
- Compruebe que la máquina virtual esté encendida antes de iniciar la operación de recuperación de espacio.
- Compruebe que no se esté aplicando ningún periodo sin disponibilidad. Consulte la sección sobre cómo establecer el acelerador de almacenamiento y las horas sin disponibilidad de recuperación de espacio para los clones vinculados de View Composer en el documento *Configurar escritorios virtuales en Horizon 7*.

Opciones

Tabla 12-11. Opciones para recuperar el espacio de disco en máquinas virtuales

Opción	Descripción
<code>-d escritorio</code>	Especifica el nombre del grupo de escritorios.
<code>-m máquina</code>	Especifica el nombre de la máquina virtual.
<code>-MarkForSpaceReclamation</code>	Selecciona la máquina virtual para recuperar el espacio de disco.

Ejemplo

Selecciona la máquina virtual `machine3` en el grupo de escritorios `pool1` para recuperar el espacio de disco.

```
vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

Configurar filtros de dominios con la opción -N

Puede usar el comando `vdmadmin` con la opción `-N` para los dominios que Horizon 7 tiene disponibles para los usuarios finales.

Sintaxis

```
vdmadmin -N [-b argumento_autenticación] -domains {-exclude | -include | -search} -domain dominio -add [-s connsvr]
```

```
vdmadmin -N [-b argumentos_autenticación] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b argumentos_autenticación] -domains -list -active [-w | -n] [-xml]
```

```
vdmadmin -N [-b argumento_autenticación] -domains {-exclude | -include | -search} -domain dominio -remove [-s connsvr]
```

```
vdmadmin -N [-b argumentos_autenticación] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

Notas de uso

Especifique una de las opciones `-exclude`, `-include` o `-search` para aplicar una operación a la lista de exclusión, de inclusión o la lista de exclusión de búsqueda, respectivamente.

Si agrega un dominio a la lista de exclusión de búsqueda, el dominio se excluye de una búsqueda de dominio automática.

Si agrega un dominio a una lista de inclusión, el dominio se incluye en los resultados de la búsqueda.

Si agrega un dominio a una lista de exclusión, el dominio se excluye de los resultados de la búsqueda.

Opciones

La siguiente tabla muestra las opciones que puede especificar para configurar los filtros de dominios.

Tabla 12-12. Opciones para configurar los filtros de dominios

Opción	Descripción
<code>-add</code>	Agrega un dominio a una lista.
<code>-domain <i>dominio</i></code>	Especifica el dominio que se filtrará. Debe especificar los dominios por sus nombres NetBIOS y no por sus nombres DNS.
<code>-domains</code>	Especifica una operación de filtro de dominios.
<code>-exclude</code>	Especifica una operación en una lista de exclusión.
<code>-include</code>	Especifica una operación en una lista de inclusión.
<code>-list</code>	Muestra los dominios que se configuran en la lista de exclusión de búsqueda, la lista de exclusión y la lista de inclusión en cada instancia del servidor de conexión y para el grupo del servidor de conexión.
<code>-list -active</code>	Muestra los dominios disponibles para la instancia del servidor de conexión en la que ejecuta el comando.
<code>-remove</code>	Elimina un dominio de una lista.
<code>-removeall</code>	Elimina todos los dominios de una lista.
<code>-s <i>connsvr</i></code>	Especifica que la operación se aplica a los filtros de dominios de una instancia del servidor de conexión. Puede especificar la instancia del servidor de conexión por su nombre o su dirección IP. Si no especifica esta opción, cualquier cambio que realice en la configuración de búsqueda se aplica a todas las instancias del servidor de conexión del grupo.
<code>-search</code>	Especifica una operación en una lista de exclusión de búsqueda.

Ejemplos

Agrega el dominio FARDOM a la lista de exclusión de búsqueda para la instancia csvr1 del servidor de conexión.

```
vdmadmin -N -domains -search -domain FARDOM -add -s csvr1
```

Agrega el dominio NEARDOM a la lista de exclusión de búsqueda para un grupo del servidor de conexión.

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```


Muestra la configuración de la búsqueda de dominio en el grupo y en ambas instancias del servidor de conexión del grupo.

```
C:\ vdmadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
```

```
Include:
```

```
Exclude:
```

```
Search :
```

Horizon 7 limita la búsqueda de dominios en cada host del servidor de conexión del grupo para excluir los dominios FARDOM y DEPTX. Los caracteres (*) junto a la lista de exclusión para CONSVR-1 indican que Horizon 7 excluye el dominio YOURDOM de los resultados de la búsqueda de dominios en CONSVR-1.

Muestra los filtros de dominios en XML usando caracteres ASCII.

```
vdmadmin -N -domains -list -xml -n
```

Muestra los dominios que están disponibles para Horizon 7 en la instancia del servidor de conexión.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS:fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Muestra los dominios disponibles en XML usando caracteres ASCII.

```
vdmadmin -N -domains -list -active -xml -n
```

Elimina el dominio NEARDOM de la lista de exclusión de búsqueda para un grupo del servidor de conexión.

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

Elimina todos los dominios de la lista de inclusión de la instancia csvr1 del servidor de conexión.

```
vdmadmin -N -domains -include -removeall -s csvr1
```

Configurar los filtros de dominios

Puede configurar los filtros de dominio para limitar los dominios que una instancia del servidor de conexión o un servidor de seguridad tienen disponibles para los usuarios finales.

Horizon 7 determina los dominios que son accesibles a través de las relaciones de confianza, comenzando por el dominio en el que se encuentra una instancia del servidor de conexión o el servidor de seguridad. En un conjunto de dominios reducido y conectados correctamente, Horizon 7 puede determinar rápidamente una lista completa de dominios, pero la duración de esta operación aumenta si también lo hace el número de dominios o si disminuye la conectividad entre los dominios. Horizon 7 también puede incluir dominios en los resultados de búsqueda que prefiera no ofrecer a los usuarios cuando inician sesión en los escritorios remotos.

Si configuró previamente el valor de la clave del Registro de Windows que controla la enumeración recursiva de dominios como false (HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum), la búsqueda recursiva de dominios está deshabilitada y la instancia del servidor de conexión usa únicamente el dominio primario. Para usar la función de filtrado de dominios, elimine la clave de registro o establezca su valor como true y reinicie el sistema. Debe hacer esto en cada instancia del servidor de conexión en la que tenga configurada esta clave.

La siguiente tabla muestra los tipos de listas de dominio que puede especificar para configurar los filtros de dominios.

Tabla 12-13. Tipos de lista de dominios

Tipo de lista de dominios	Descripción
Listas de exclusión de búsqueda	Especifica los dominios por los que Horizon 7 puede pasar durante una búsqueda automática. La búsqueda ignora los dominios que están incluidos en la lista de exclusión de búsquedas y no intenta encontrar los dominios en los que confíe el excluido. No puede excluir el dominio primario de la búsqueda.
Lista de exclusión	Especifica los dominios que Horizon 7 excluye de los resultados de una búsqueda de dominios. No puede excluir el dominio primario.
Lista de inclusión	Especifica los dominios que Horizon 7 no excluye de los resultados de una búsqueda de dominios. Todos los dominios se eliminan del dominio primario.

La búsqueda automática de dominios recupera una lista de dominios, de los que excluye los dominios que especificó en la lista de exclusión de búsqueda y los dominios en los que confían estos dominios excluidos. Horizon 7 selecciona la primera lista de inclusión o de exclusión que no está vacía en este orden.

- 1 Lista de exclusión configurada para la instancia del servidor de conexión.
- 2 Lista de exclusión configurada para el grupo de servidores de conexión.
- 3 Lista de inclusión configurada para la instancia del servidor de conexión.
- 4 Lista de inclusión configurada para el grupo de servidores de conexión.

Horizon 7 aplica únicamente la primera lista que seleccionó de los resultados de búsqueda.

Si especifica un dominio para su inclusión y no se puede acceder al controlador de dominio en ese momento, Horizon 7 no incluye ese dominio en la lista de dominios activos.

No puede excluir el dominio primario al que pertenecen el servidor de conexión o el servidor de seguridad.

Ejemplo de filtrado para incluir dominios

Puede utilizar una lista de inclusión para especificar los dominios que Horizon 7 no excluirá de los resultados de la búsqueda de dominios. Se elimina el resto de dominios, excepto el dominio principal.

Una instancia del servidor de conexión se conecta al dominio MYDOM principal y tiene una relación de confianza con el dominio YOURDOM. El dominio YOURDOM tiene una relación de confianza con el dominio DEPTX.

Visualice los dominios activos en ese momento para una instancia del servidor de conexión.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS:fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Los dominios DEPTY y DEPTZ aparecen en la lista porque son dominios de confianza del DEPTX.

Especifique que la instancia del servidor de conexión debe establecer como disponible los dominios YOURDOM y DEPTX, además del dominio MYDOM principal.

```
vdmadmin -N -domains -include -domain YOURDOM -add
vdmadmin -N -domains -include -domain DEPTX -add
```

Visualice los dominios activos en ese momento después de incluir los dominios YOURDOM y DEPTX.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 aplica la lista de inclusión a los resultados de una búsqueda de dominios. Si la jerarquía de dominio es muy compleja o la conectividad de red a algunos dominios es de baja intensidad, la búsqueda de dominios puede ser lenta. En esos casos, use la exclusión de búsqueda en su lugar.

Ejemplo de filtrado para excluir dominios

Puede utilizar una lista de inclusión para especificar los dominios que Horizon 7 excluirá de los resultados de la búsqueda de dominios.

Un grupo de dos instancias del servidor de conexión, CONSVR-1 y CONSVR-2, se conecta al dominio MYDOM principal y tiene una relación de confianza con el dominio YOURDOM. El dominio YOURDOM tiene una relación de confianza con los dominios DEPTX y FARDOM.

El dominio FARDOM se encuentra en una ubicación geográfica remota y la conectividad remota a dicho dominio se produce a través de un vínculo lento con una alta latencia. No hay requisitos para usuarios en el dominio FARDOM para que puedan acceder al grupo del servidor de conexión en el dominio MYDOM.

Mostrar los dominios activos en ese momento para un miembro del grupo del servidor de conexión.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS: fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Los dominios DEPTY y DEPTZ son dominios de confianza del dominio DEPTX.

Para mejorar el rendimiento de la conexión en Horizon Client, excluya el dominio FARDOM de la búsqueda realizada por el grupo del servidor de conexión.

```
vdmadmin -N -domains -search -domain FARDOM -add
```

El comando muestra los dominios activos en ese momento tras excluir el dominio FARDOM de la búsqueda.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Ampliar la lista de exclusión para excluir el dominio DEPTX y todos sus dominios de confianza de la búsqueda en todas las instancias del servidor de conexión de un grupo. Evitar también que el dominio YOURDOM esté disponible en CONSVR-1.

```
vdmadmin -N -domains -search -domain DEPTX -add
```

```
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

Mostrar la nueva configuración de búsqueda de dominios.

```
C:\ vdmadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
```

```
Include:
```

```
Exclude:
```

```
Search :
```

Horizon 7 limita la búsqueda de dominios en cada host del servidor de conexión del grupo para excluir los dominios FARDOM y DEPTX. Los caracteres (*) junto a la lista de exclusión para CONSVR-1 indican que Horizon 7 excluye el dominio YOURDOM de los resultados de la búsqueda de dominios en CONSVR-1.

Muestra los dominios activos en ese momento en CONSVR-1.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

Muestra los dominios activos en ese momento en CONSVR-2.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P

Puede usar el comando `vdmadmin` con las opciones `-O` y `-P` para mostrar las directivas y las máquinas virtuales que están asignadas a usuarios que ya no tienen autorización para usar el sistema.

Sintaxis

```
vdmadmin -O [-b argumentos_autenticación] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath ruta]]
```

```
vdmadmin -P [-b argumentos_autenticación] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath ruta]]
```

Notas de uso

Si revoca una autorización de usuario a una máquina virtual persistente o a un sistema físico, la asignación del escritorio remoto asociado no se revoca automáticamente. Esta condición se puede aceptar si suspendió de forma temporal una cuenta de usuario o si el usuario está ausente durante una larga temporada. Cuando vuelva a habilitar la autorización, el usuario puede continuar con la misma máquina virtual como hacía antes. Si un usuario dejó la organización, los otros usuarios no pueden acceder a la máquina virtual y se considera huérfana. También es posible que desee examinar las directivas que se asignaron a usuarios sin autorización.

Opciones

La siguiente tabla muestra las opciones que puede especificar para visualizar las máquinas virtuales y las directivas de usuarios sin autorización.

Tabla 12-14. Opciones para visualizar las máquinas y las directivas de usuarios sin autorización

Opción	Descripción
-ld	Ordena las entradas de los resultados por máquina.
-lu	Ordena las entradas de los resultados por usuario.
-noxslt	Especifica que las hojas de estilo predeterminadas no se deben aplicar a la salida XML.
-xsltpath <i>ruta</i>	Especifica la ruta a la hoja de estilo que se usa para transformar la salida XML.

Tabla 12-15 muestra las hojas de estilo que puede aplicar a la salida XML para transformarla en HTML. Las hojas de estilo se encuentran en el directorio C:\Program Files\VMware\VMware View\server\etc.

Tabla 12-15. Hojas de estilo XLS

Nombre del archivo de la hoja de estilo	Descripción
unentitled-machines.xsl	Transforma los informes que contienen una lista de máquinas virtuales sin autorización, agrupadas por usuario o sistema, y que están asignadas a un usuario en ese momento. Esta hoja de estilo es la predeterminada.
unentitled-policies.xsl	Transforma los informes que contienen una lista de máquinas virtuales con directivas en el nivel de usuarios que se aplican a usuarios sin autorización.

Ejemplos

Visualice las máquinas virtuales que se asignaron a los usuarios sin autorización, agrupadas por máquinas virtuales en formato de texto.

```
vdmadmin -O -ld
```

Visualice las máquinas virtuales que están asignadas a usuarios sin autorización, agrupadas por usuario, en formato XML con caracteres ASCII.

```
vdmadmin -O -lu -xml -n
```

Aplique su propia hoja de estilo C:\tmp\unentitled-users.xsl y redireccione los resultados del archivo uu-output.html.

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

Visualice las directivas de usuario que están asociadas con las máquinas virtuales de los usuarios, agrupadas por escritorio en formato XML con caracteres Unicode.

```
vdmadmin -P -ld -xml -w
```

Aplice su propia hoja de estilo `C:\tmp\unentitled-policies.xml` y redireccione los resultados del archivo `up-output.html`.

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xml" > up-output.html
```

Configurar clientes en modo de pantalla completa con la opción -Q

Puede usar el comando `vdmadmin` con la opción `-Q` para establecer valores predeterminados y crear cuentas de clientes en modo de pantalla completa, para habilitar la autenticación de dichos clientes y para mostrar la información de su configuración.

Sintaxis

```
vdmadmin -Q -clientauth -add [-b argumentos_autenticación] -domain nombre_dominio-clientid id_cliente  
[-password "contraseña" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group  
nombre_grupo | -nogroup] [-description "texto_descripción"]
```

```
vdmadmin -Q -disable [-b argumentos_autenticación] -s servidor_conexión
```

```
vdmadmin -Q -enable [-b argumentos_autenticación] -s servidor_conexión [-requirepassword]
```

```
vdmadmin -Q -clientauth -getdefaults [-b argumentos_autenticación] [-xml]
```

```
vdmadmin -Q -clientauth -list [-b argumentos_autenticación] [-xml]
```

```
vdmadmin -Q -clientauth -remove [-b argumentos_autenticación] -domain nombre_dominio-clientid  
id_cliente
```

```
vdmadmin -Q -clientauth -removeall [-b argumentos_autenticación] [-force]
```

```
vdmadmin -Q -clientauth -setdefaults [-b argumentos_autenticación] [-ouDN] [ -expirepassword |  
-noexpirepassword ] [-groupnombre_grupo | -nogroup]
```

```
vdmadmin -Q -clientauth -update [-b argumentos_autenticación] -domain nombre_dominio-clientid  
id_cliente [-password "contraseña " | -genpassword] [-description "texto_descripción"]
```

Notas de uso

Debe ejecutar el comando `vdmadmin` en una de las instancias del servidor de conexión del grupo que contiene la instancia que utilizan los clientes para conectarse a sus escritorios remotos.

Al configurar los valores predeterminados sobre la caducidad de la contraseña y pertenencia a grupos de Active Directory, estas opciones se comparten con todas las instancias del servidor de conexión en un grupo.

Cuando agrega un cliente en modo de pantalla completa, Horizon 7 crea una cuenta de usuario para el cliente en Active Directory. Si especifica un nombre para el cliente, este nombre debe comenzar por los caracteres "custom-", o bien por una de las cadenas alternativas que definió en ADAM y que no puede ser superior a 20 caracteres. Use un nombre especificado con un solo dispositivo cliente.

Puede definir los prefijos alternativos como "custom-" en el atributo con varios valores pae-ClientAuthPrefix en cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int en ADAM de una instancia del servidor de conexión. Evite usar estos prefijos con cuentas normales de usuarios.

Si no especifica un nombre para un cliente, Horizon 7 genera un nombre para la dirección MAC que especificó para el dispositivo cliente. Por ejemplo, si la dirección MAC es 00:10:db:ee:76:80, el nombre de la cuenta correspondiente es cm-00_10_db_ee_76_80. Solo puede usar estas cuentas con las instancias del servidor de conexión que habilitó para autenticar clientes.

Algunos clientes ligeros solo permiten nombres de usuarios que comienzan con los caracteres "custom-" o "com-" para usarlos en modo de pantalla completa.

Una contraseña generada automáticamente tiene 16 caracteres, contiene al menos una letra en mayúscula, una en minúscula, un símbolo y un número. Además, puede contener caracteres repetidos. Si necesita una contraseña más segura, debe usar la opción `-password` para especificar la contraseña.

Si usa la opción `-group` para especificar un grupo o estableció un grupo predeterminado previamente, Horizon 7 agrega la cuenta cliente a este grupo. Puede especificar la opción `-nogroup` para evitar que la cuenta se agregue a ningún grupo.

Si habilita una instancia del servidor de conexión para autenticar clientes en modo de pantalla completa, puede especificar de forma opcional que los clientes introduzcan una contraseña. Si deshabilita la autenticación, los clientes no podrán conectarse a sus escritorios remotos.

Aunque habilite o deshabilite la autenticación para una instancia independiente del servidor de conexión, todas sus instancias del grupo comparten el resto de opciones de configuración para la autenticación cliente. Solo necesita agregar un cliente una vez en todas las instancias del servidor de conexión de un grupo para que pueda aceptar las solicitudes desde el cliente.

Si especifica la opción `-requirepassword` al habilitar la autenticación, la instancia del servidor de conexión no puede autenticar clientes que generaron contraseñas de forma automática. Si cambia la configuración de una instancia del servidor de conexión para especificar esta opción, dichos clientes no podrán autenticarse ellos mismos y obtendrán el mensaje de error Nombre de usuario desconocido o contraseña incorrecta.

Opciones

La siguiente tabla muestra las opciones que puede especificar para configurar los clientes en modo de pantalla completa.

Tabla 12-16. Opciones para configurar clientes en pantalla completa

Opción	Descripción
<code>-add</code>	Agrega una cuenta de clientes en modo de pantalla completa.
<code>-clientauth</code>	Especifica una operación que configure la autenticación de un cliente en modo de pantalla completa.
<code>-clientid <i>id_cliente</i></code>	Especifica el nombre o la dirección MAC del cliente.
<code>-description "<i>texto_descripción</i>"</code>	Crea una descripción de la cuenta del dispositivo cliente en Active Directory.
<code>-disable</code>	Deshabilita la autenticación de los clientes en modo de pantalla completa en una instancia del servidor de conexión especificada.
<code>-domain <i>nombre_dominio</i></code>	Especifica el dominio de las cuentas del dispositivo cliente.
<code>-enable</code>	Habilita la autenticación de los clientes en modo de pantalla completa en una instancia del servidor de conexión especificada.
<code>-expirepassword</code>	Especifica que el tiempo de caducidad de la contraseña de las cuentas cliente sea el mismo que el del grupo del servidor de conexión. Si no se definió un periodo de caducidad para el grupo, las contraseñas nunca expirarán.
<code>-force</code>	Deshabilita la solicitud de confirmación cuando se elimina la cuenta de un cliente en modo de pantalla completa.
<code>-genpassword</code>	Genera una contraseña para la cuenta del cliente. Este es el comportamiento predeterminado si no especifica <code>-password</code> ni <code>-genpassword</code> .
<code>-getdefaults</code>	Obtiene los valores predeterminados que se usan para agregar cuentas cliente.
<code>-group <i>nombre_grupo</i></code>	Especifica el nombre del grupo predeterminado al que se agregan las cuentas cliente. El nombre del grupo debe especificarse como el nombre del grupo de Active Directory anterior a Windows 2000.
<code>-list</code>	Muestra información sobre los clientes en modo de pantalla completa y sobre las instancias del servidor de conexión para las que tiene la autenticación habilitada de los clientes en modo de pantalla completa.
<code>-noexpirepassword</code>	Especifica que la contraseña de una cuenta del cliente no caduca.
<code>-nogroup</code>	Al agregar una cuenta para un cliente, especifica que esta cuenta no se agrega al grupo predeterminado. Al establecer los valores predeterminados para los clientes, borra la configuración del grupo predeterminado.
<code>-ou <i>DN</i></code>	Especifica el nombre distintivo de la unidad organizativa a la que se agregan las cuentas cliente. Por ejemplo: OU=kiosk-ou,DC=myorg,DC=com
Nota No puede utilizar la opción <code>-setdefaults</code> para cambiar la configuración de una unidad organizativa.	

Tabla 12-16. Opciones para configurar clientes en pantalla completa (Continuación)

Opción	Descripción
<code>-password "contraseña"</code>	Especifica una contraseña explícita para la cuenta del cliente.
<code>-remove</code>	Elimina la cuenta de un cliente en modo de pantalla completa.
<code>-removeall</code>	Elimina las cuentas de todos los clientes en modo de pantalla completa.
<code>-requirepassword</code>	Especifica que los clientes en modo de pantalla completa deben introducir la contraseña. Horizon 7 no aceptará contraseñas generadas para las nuevas conexiones.
<code>-s servidor_conexión</code>	Especifica el nombre NetBIOS de la instancia del servidor de conexión donde se habilitará o se deshabilitará la autenticación de clientes en modo de pantalla completa.
<code>-setdefaults</code>	Establece los valores predeterminados que se usan para agregar cuentas cliente.
<code>-update</code>	Actualiza una cuenta de clientes en modo de pantalla completa.

Ejemplos

Establezca los valores predeterminados de la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de clientes.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Obtenga los valores predeterminados actuales de los clientes en texto sin formato.

```
vdmadmin -Q -clientauth -getdefaults
```

Obtenga los valores predeterminados actuales de los clientes en formato XML.

```
vdmadmin -Q -clientauth -getdefaults -xml
```

Agregue una cuenta para un cliente especificado por la dirección MAC al dominio MYORG y use la configuración predeterminada del grupo kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Agregue una cuenta para un cliente especificado por su dirección MAC al dominio MYORG y use una contraseña generada automáticamente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -group kc-grp
```

Agregue una cuenta para un cliente con nombre y especifique la contraseña que se usará con el cliente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Actualice una cuenta para un cliente especificando una nueva contraseña y un texto descriptivo.

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -description "Foyer Entry Workstation"
```

Elimine la cuenta de un cliente en modo de pantalla completa especificado por su dirección MAC desde el dominio MYORG.

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

Elimine las cuentas de todos los clientes sin solicitar la confirmación de esta acción.

```
vdmadmin -Q -clientauth -removeall -force
```

Habilite la autenticación de clientes en la instancia csvr-2 del servidor de conexión. Los clientes con contraseñas generadas de forma automática pueden autenticarse por sí solos sin facilitar una contraseña.

```
vdmadmin -Q -enable -s csvr-2
```

Habilite la autenticación de clientes en la instancia csvr-3 del servidor de conexión y solicite a los clientes que especifiquen sus contraseñas en Horizon Client. Los clientes con contraseñas generadas de forma automática no pueden autenticarse por sí solos.

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

Deshabilite la autenticación de clientes en la instancia csvr-1 del servidor de conexión.

```
vdmadmin -Q -disable -s csvr-1
```

Muestra la información sobre los clientes en formato de texto. El cliente cm-00_0c_29_0d_a3_e6 tiene una contraseña generada de forma automática y no requiere un script de una aplicación o un usuario final para especificar esta contraseña a Horizon Client. El cliente cm-00_22_19_12_6d_cf tiene una contraseña especificada de forma explícita y obliga al usuario final a proporcionarla. La instancia del servidor de conexión CONSVR2 acepta las solicitudes de autenticación de clientes con contraseñas generadas de forma automática. CONSVR1 no acepta solicitudes de autenticación desde clientes en modo de pantalla completa.

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
```

```

Domain           : myorg.com
Password Generated: true

GUID             : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID         : cm-00_22_19_12_6d_cf
Domain           : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name      : CONSVR1
Client Authentication Enabled : false
Password Required      : false

Common Name      : CONSVR2
Client Authentication Enabled : true
Password Required      : false

```

Visualizar el primer usuario de un equipo con la opción -R

Puede usar el comando `vdmadmin` con la opción `-R` para encontrar la asignación inicial de una máquina virtual administrada. Por ejemplo, en el caso de perder datos LDAP, es posible que necesite esta información para poder volver a asignar las máquinas virtuales a los usuarios.

Nota El comando `vdmadmin` con la opción `-R` funciona únicamente en máquinas virtuales que tienen una versión anterior a View Agent 5.1. En máquinas virtuales que ejecutan View Agent 5.1 y versiones posteriores, así como Horizon Agent 7.0 y versiones posteriores, esta opción no funciona. Para ubicar el primer usuario de una máquina virtual, use la base de datos de eventos para determinar los usuarios que iniciaron sesión en la máquina.

Sintaxis

```
vdmadmin -R -i dirección_red
```

Notas de uso

No puede usar la opción `-b` para ejecutar este comando como un usuario con privilegios. Debe iniciar sesión como un usuario con la función **Administrador**.

Opciones

La opción `-i` especifica la dirección IP de la máquina virtual.

Ejemplos

Vea el primer usuario que accedió a la máquina virtual en la dirección IP 10.20.34.120.

```
vdmadmin -R -i 10.20.34.120
```

Eliminar una entrada de una instancia del servidor de conexión o del servidor de seguridad con la opción -S

Puede usar el comando `vdmadmin` con la opción `-S` para eliminar la entrada de la instancia del servidor de conexión o del servidor de seguridad de la configuración de Horizon 7.

Sintaxis

```
vdmadmin -S [-b argumentos_autenticación] -r -s servidor
```

Notas de uso

Para proporcionar una alta disponibilidad, Horizon 7 le permite configurar una o varias instancias de réplica del servidor de conexión en un grupo de servidores de conexión. Si deshabilita una instancia del servidor de conexión en un grupo, la entrada del servidor se mantiene en la configuración de Horizon 7.

También puede usar el comando `vdmadmin` con la opción `-S` para eliminar un servidor de seguridad del entorno de Horizon 7. No es necesario que utilice esta opción si pretende actualizar o volver a instalar un servidor de seguridad sin eliminarlo de forma permanente.

Para eliminarlo de forma permanente, realice estas tareas:

- 1 Desinstale la instancia del servidor de conexión o el servidor de seguridad del equipo Windows Server al ejecutar el instalador del servidor de conexión.
- 2 Elimine el programa Adam Instance VMwareVDMDS del equipo Windows Server ejecutando la herramienta Agregar o quitar programas.
- 3 En otra instancia del servidor de conexión, use el comando `vdmadmin` para eliminar la entrada de la instancia del servidor de conexión desinstalada o el servidor de seguridad de la configuración.

Si desea volver a instalar Horizon 7 en los sistemas eliminados sin replicar la configuración Horizon 7 del grupo original, reinicie todos los hosts del servidor de conexión en el grupo original antes de reinstalar. Esto evita que las instancias del servidor de conexión reciban actualizaciones de la configuración desde el grupo original.

Opciones

La opción `-s` especifica el nombre NetBIOS de la instancia del servidor de conexión o el servidor de seguridad que se eliminarán.

Ejemplos

Elimine la entrada de la instancia del servidor de conexión connsvr3.

```
vdadmin -S -r -s connsvr3
```

Proporcionar credenciales secundarias para los administradores con la opción -T

Puede usar el comando `vdadmin` con la opción `-T` para proporcionar credenciales secundarias de Active Directory a los usuarios administradores.

Sintaxis

```
vdadmin -T [-b argumentos_autenticación] -domainauth  
{-add | -update | -remove | -removeall | -list} -owner dominio\usuario -user dominio\usuario  
[-password contraseña]
```

Notas de uso

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

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

El comando `vdadmin` permite configurar credenciales secundarias por usuario. No puede configurar las credenciales secundarias especificadas de forma global.

En una confianza de bosque, normalmente solo puede configurar credenciales secundarias para el dominio raíz del bosque. A continuación, el servidor de conexión podrá enumerar dominios secundarios en la confianza de bosque.

Las comprobaciones de las horas de inicio de sesión, la deshabilitación y el bloqueo de las cuentas de Active Directory se pueden realizar solo cuando un usuario de un dominio de confianza unidireccional inicia sesión por primera vez.

La administración PowerShell y la autenticación por tarjeta inteligente de los usuarios no son compatibles con los dominios de confianza unidireccional. No se admite la autenticación SAML de los usuarios en dominios de confianza unidireccional.

Las cuentas de credenciales secundarias necesitan los siguientes permisos. Una cuenta de usuario estándar debe tener estos permisos de forma predeterminada.

- Mostrar contenido
- Leer todas las propiedades
- Permisos de lectura
- Leer tokenGroupsGlobalAndUniversal (implícito en Leer todas las propiedades)

Limitaciones

- No se admite la administración PowerShell ni la autenticación de tarjeta inteligente de los usuarios en dominios de confianza unidireccional.
- No se admite la autenticación SAML de los usuarios en dominios de confianza unidireccional.

Opciones

Tabla 12-17. Opciones para proporcionar credenciales secundarias

Opción	Descripción
<code>-add</code>	Agrega una credencial secundaria para la cuenta propietaria. Se realiza un inicio de sesión en Windows para comprobar que las credenciales especificadas sean válidas. Se crea una entidad de seguridad externa (FSP) para el usuario de LDAP de View.
<code>-update</code>	Actualiza una credencial secundaria para la cuenta propietaria. Se realiza un inicio de sesión en Windows para comprobar que las credenciales actualizadas sean válidas.
<code>-list</code>	Muestra las credenciales de seguridad para la cuenta propietaria. No se muestran las contraseñas.
<code>-remove</code>	Elimina una credencial de seguridad de la cuenta propietaria.
<code>-removeall</code>	Elimina todas las credenciales de seguridad de la cuenta propietaria.

Ejemplos

Agregue una credencial secundaria para la cuenta propietaria especificada. Se realiza un inicio de sesión en Windows para comprobar que las credenciales especificadas sean válidas.

```
vdmadmin -T -domainauth -add -owner dominio\usuario -user dominio\usuario -password contraseña
```

Actualice una credencial secundaria para la cuenta propietaria especificada. Se realiza un inicio de sesión en Windows para comprobar que las credenciales actualizadas sean válidas.

```
vdmadmin -T -domainauth -update -owner dominio\usuario -user dominio\usuario -password contraseña
```


Elimine una credencial secundaria para la cuenta propietaria especificada.

```
vdmadmin -T -domainauth -remove -owner dominio\usuario -user dominio\usuario
```

Elimine todas las credenciales secundarias para la cuenta propietaria especificada.

```
vdmadmin -T -domainauth -removeall -owner dominio\usuario
```

Visualice todas las credenciales secundarias para la cuenta propietaria especificada. No se muestran las contraseñas.

```
vdmadmin -T -domainauth -list -owner dominio\usuario
```

Visualizar información sobre los usuarios con la opción -U

Puede usar el comando vdmadmin con la opción -U para mostrar información detallada sobre los usuarios.

Sintaxis

```
vdmadmin -U [-b argumentos_autenticación] -u dominio\usuario [-w | -n] [-xml]
```

Notas de uso

El comando muestra información sobre un usuario, que se obtiene de Active Directory y Horizon 7.

- Detalles de Active Directory sobre la cuenta de usuario.
- Pertenencia a grupos de Active Directory.
- Autorizaciones de equipo, incluido el ID del equipo, el nombre para mostrar, la descripción, la carpeta y si un equipo se deshabilitó.
- Asignaciones de ThinApp.
- Las funciones de administrador, incluido los derechos administrativos de un usuario y las carpetas para las que tienen dichos derechos.

Opciones

La opción -u especifica el nombre y el dominio del usuario.

Ejemplos

Visualice la información sobre el usuario Jo en el dominio CORP en XML con caracteres ASCII.

```
vdmadmin -U -u CORP\Jo -n -xml
```

Bloquear o desbloquear las máquinas virtuales con la opción -V

Puede usar el comando `vdmadmin` con la opción `-V` para bloquear o desbloquear las máquinas virtuales en el centro de datos.

Sintaxis

```
vdmadmin -V [-b argumentos_autenticación] -e -d escritorio -m máquina [-m máquina] ...
```

```
vdmadmin -V [-b argumentos_autenticación] -e -vcdn dn_vCenter -vmpathruta_inventario
```

```
vdmadmin -V [-b argumentos_autenticación] -p -d escritorio -m máquina [-m máquina] ...
```

```
vdmadmin -V [-b argumentos_autenticación] -p -vcdn dn_vCenter -vmpathruta_inventario
```

Notas de uso

Solo debe usar el comando `vdmadmin` para bloquear o desbloquear una máquina virtual si se encuentra con un problema que dejara al escritorio remoto en un estado incorrecto. No use el comando para administrar escritorios remotos que funcionan correctamente.

Si un escritorio remoto está bloqueado y la entrada de sus máquinas virtuales ya no existe en ADAM, use las opciones `-vmpath` y `-vcdn` para especificar la ruta del inventario de la máquina virtual y de vCenter Server. Puede usar vCenter Client para encontrar la ruta del inventario de una máquina virtual de un escritorio remoto en `Home/Inventory/VMs and Templates`. Puede usar el Editor ADSI de ADAM para encontrar el nombre distintivo de vCenter Server que se encuentra bajo el encabezado `OU=Properties`.

Opciones

La siguiente tabla muestra las opciones que puede especificar para bloquear o desbloquear las máquinas virtuales.

Tabla 12-18. Opciones para bloquear o desbloquear las máquinas virtuales

Opción	Descripción
<code>-d escritorio</code>	Especifica el grupo de escritorios.
<code>-e</code>	Desbloquea una máquina virtual.
<code>-m máquina</code>	Especifica el nombre de la máquina virtual.
<code>-p</code>	Bloquea una máquina virtual.

Tabla 12-18. Opciones para bloquear o desbloquear las máquinas virtuales (Continuación)

Opción	Descripción
<code>-vcdn dn_vCenter</code>	Especifica el nombre distintivo de vCenter Server.
<code>-vmpath ruta_inventario</code>	Especifica la ruta de inventario de la máquina virtual.

Ejemplos

Desbloquee las máquinas virtuales `machine1` y `machine2` en el grupo de escritorios `dtpool3`.

```
vdadmin -V -e -d dtpool3 -m machine1 -m machine2
```

Bloquee la máquina virtual `machine3` en el grupo de escritorios `dtpool3`.

```
vdadmin -V -p -d dtpool3 -m machine3
```

Detectar y resolver conflictos de esquemas y entradas LDAP usando la opción -X

Puede usar el comando `vdadmin` con la opción `-X` para detectar y resolver conflictos de las entradas LDAP y los esquemas LDAP en las instancias del servidor de conexión replicadas en un grupo. También puede utilizar esta opción para detectar y resolver conflictos de esquemas y entradas LDAP en un entorno de Arquitectura de Cloud Pod.

Sintaxis

```
vdadmin -X [-b argumentos_autenticación] -collisions [-resolve]
vdadmin -X [-b argumentos_autenticación] -schemacollisions [-resolve] [-global]
```

Notas de uso

Las entradas LDAP duplicadas en dos o más instancias del servidor de conexión pueden causar problemas con la integridad de los datos LDAP en Horizon 7. Esta condición se puede producir durante una actualización mientras la replicación LDAP no está operativa. Aunque Horizon 7 busque esta condición de error a intervalos regulares, puede ejecutar el comando `vdadmin` en una de las instancias del servidor de conexión del grupo para detectar y resolver conflictos de entradas LDAP de forma manual.

Los conflictos de esquemas LDAP también se pueden producir durante una actualización mientras la replicación LDAP no está operativa. Debido a que Horizon 7 no busca esta condición de error, debe ejecutar el comando `vdadmin` para detectar y resolver los conflictos de esquemas LDAP de forma manual.

Opciones

En la siguiente tabla se muestran las opciones que puede especificar para detectar y resolver conflictos de entradas LDAP.

Tabla 12-19. Opciones para detectar y resolver entradas LDAP en conflicto

Opción	Descripción
<code>-collisions</code>	Especifica una operación para detectar conflictos de entradas LDAP en un grupo de servidores de conexión.
<code>-resolve</code>	Resuelve todos los conflictos LDAP en la instancia LDAP. Si no especifica esta opción, el comando solo muestra los problemas que encuentra.

En la siguiente tabla se muestran las opciones que puede especificar para detectar y resolver conflictos de esquemas LDAP.

Tabla 12-20. Opciones para detectar y resolver conflictos de esquemas LDAP

Opción	Descripción
<code>-schemacollisions</code>	Especifica una operación para detectar conflictos de esquemas LDAP en un grupo de servidores de conexión o en un entorno de Arquitectura de Cloud Pod.
<code>-resolve</code>	Resuelve todos los conflictos de esquemas LDAP en la instancia LDAP. Si no especifica esta opción, el comando solo muestra los problemas que encuentra.
<code>-global</code>	Realiza comprobaciones y aplica las correcciones necesarias a la instancia LDAP en un entorno de Arquitectura de Cloud Pod. Si no especifica esta opción, las comprobaciones se ejecutarán en la instancia LDAP local.

Ejemplos

Detectar los conflictos de entradas LDAP en un grupo de servidores de conexión.

```
vdmadmin -X -collisions
```

Detectar y resolver conflictos de entradas LDAP en la instancia LDAP local.

```
vdmadmin -X -collisions -resolve
```

Detectar y resolver conflictos de esquemas LDAP en la instancia LDAP global.

```
vdmadmin -X -schemacollisions -resolve -global
```