

Administración de Horizon Console

DICIEMBRE DE 2019
VMware Horizon 7 7.11



vmware®

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

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

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Copyright © 2018-2019 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

1	Administración de VMware Horizon Console	9
2	Usar VMware Horizon Console	10
	Características de Horizon 7 admitidas	10
	Ventajas de utilizar Horizon Console	12
	Instalar y configurar Horizon Console	12
	Iniciar sesión en Horizon Console	12
3	Configurar el servidor de conexión de Horizon en Horizon Console	15
	Configurar vCenter Server y Horizon Composer en Horizon Console	15
	Crear una cuenta de usuario para operaciones en AD de Horizon Composer	15
	Instalar la clave de licencia del producto en Horizon Console	17
	Agregar instancias de vCenter Server a Horizon 7 en Horizon Console	17
	Configurar los parámetros de Horizon Composer	20
	Configurar los dominios de Horizon Composer	21
	Agregar un administrador de dominio de clones instantáneos en Horizon Console	22
	Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados	23
	Configurar Horizon Storage Accelerator para vCenter Server	24
	Límites de operaciones simultáneas para vCenter Server y Horizon Composer	26
	Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto	27
	Aceptar la huella digital de un certificado TLS predeterminado	28
	Eliminar una instancia de vCenter Server de Horizon 7	30
	Eliminar Horizon Composer de Horizon 7	30
	ID únicos de vCenter Server en conflicto	31
	Realizar una copia de seguridad del servidor de conexión de Horizon en Horizon Console	32
	Configurar las opciones de las sesiones cliente en Horizon Console	32
	Configuración global de las sesiones cliente en Horizon Console	32
	Configuración de seguridad global para conexiones y sesiones cliente en Horizon Console	36
	Configuración global de restricciones de cliente de las sesiones cliente en Horizon Console	37
	Habilitar o deshabilitar un servidor de conexión de Horizon en Horizon Console	39
	Editar las URL externas para las instancias del servidor de conexión de Horizon	39
	Registrar puertas de enlace en Horizon Console	41
4	Configurar la autenticación de tarjeta inteligente	42
	Iniciar sesión con una tarjeta inteligente	43
	Configurar la autenticación con tarjeta inteligente en el servidor de conexión de Horizon	43
	Obtener los certificados de la autoridad de certificación	44

Obtener el certificado de CA de Windows	45
Agregar el certificado de CA a un archivo del almacén de confianza del servidor	46
Modificar las propiedades de configuración del servidor de conexión de Horizon	47
Configurar las opciones de la tarjeta inteligente en Horizon Console	47
Configurar la autenticación con tarjeta inteligente en soluciones de terceros	51
Preparar Active Directory para la autenticación con tarjeta inteligente	52
Agregar UPN para usuarios de tarjetas inteligentes	52
Agregar el certificado raíz al almacén Enterprise NTAAuth	53
Agregar el certificado raíz a las entidades de certificación raíz de confianza	53
Agregar un certificado intermedio a las entidades de certificación intermedias	55
Verificar la configuración de la autenticación con tarjeta inteligente en Horizon Console	56
Uso de la comprobación de revocación de certificados de tarjeta inteligente	57
Iniciar sesión con la comprobación de CRL	58
Iniciar sesión con la comprobación de revocación del certificado OCSP	58
Configurar comprobación de CRL	59
Configurar la comprobación de revocación del certificado OCSP	60
Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente	61

5 Configurar otros tipos de autenticación de usuario 62

Uso de la autenticación en dos fases	62
Iniciar sesión usando la autenticación en dos fases	63
Habilitar la autenticación en dos fases en Horizon Console	64
Solucionar los problemas de acceso denegado de RSA SecureID	66
Solucionar los problemas de acceso denegado de RADIUS	67
Uso de la autenticación SAML	67
Utilizar la autenticación SAML para integrar VMware Identity Manager	68
Configurar un autenticador SAML en Horizon Console	68
Configurar la compatibilidad del proxy con VMware Identity Manager	71
Cambiar el período de caducidad de los metadatos del proveedor de servicios en el servidor de conexión	71
Generar metadatos SAML para que el servidor de conexión se pueda usar como proveedor del servicio	72
Consideraciones del tiempo de respuesta para varios autenticadores SAML dinámicos	73
Configurar las directivas de acceso de Workspace ONE en Horizon Console	73
Configurar la autenticación biométrica	74

6 Autenticar usuarios y grupos 76

Restringir acceso a escritorios remotos fuera de la red	76
Configurar el acceso remoto	76
Configurar el acceso sin autenticar	77
Crear usuarios con acceso sin autenticar	77
Habilitar el acceso sin autenticar para los usuarios en Horizon Console	78

Autorizar a los usuarios sin autenticar para que accedan a las aplicaciones publicadas	79
Eliminar un usuario con acceso sin autenticar	80
Acceso sin autenticar desde Horizon Client	80
Configurar usuarios para el inicio de sesión híbrido en Horizon Console	81
Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows	83

7 Configurar la administración delegada basada en funciones en Horizon Console 85

Comprender las funciones y los privilegios	85
Uso de grupos de acceso para delegar la administración de grupos y granjas en Horizon Console	86
Administradores diferentes para grupos de acceso diferentes	87
Administradores diferentes para el mismo grupo de acceso	87
Comprender los permisos	88
Administrar administradores	89
Crear un administrador en Horizon Console	89
Eliminar un administrador en Horizon Console	90
Administrar y consultar los permisos	91
Agregar un permiso en Horizon Console	91
Eliminar un permiso en Horizon Console	92
Revisar permisos en Horizon Console	93
Administrar y consultar los grupos de acceso	93
Agregar un grupo de acceso a Horizon Console	94
Mover un grupo de escritorios o una granja a un grupo de acceso diferente en Horizon Console	94
Eliminar un grupo de acceso en Horizon Console	95
Revisar los objetos de un grupo de acceso	95
Revisar las máquinas virtuales de vCenter de un grupo de acceso	95
Administrar funciones personalizadas	96
Agregar una función personalizada en Horizon Console	96
Modificar los privilegios de una función personalizada en Horizon Console	97
Eliminar una función personalizada en Horizon Console	97
Funciones y privilegios predefinidos	98
Funciones de administrador predefinidas	98
Privilegios globales	101
Privilegios específicos de objeto	103
Privilegios internos	104
Privilegios necesarios para las tareas comunes	104
Privilegios para administrar grupos	104
Privilegios para administrar máquinas	105
Privilegios para administrar discos persistentes	106
Privilegios para administrar los usuarios y los administradores	106
Privilegios para las tareas de Horizon Help Desk Tool	107

Privilegios para los comandos y las tareas de administración general	108
Prácticas recomendadas para grupos y usuarios administradores	109
8 Establecer directivas en Horizon Console	110
Configurar las directivas globales	110
9 Mantenimiento de los componentes de Horizon 7	112
Realizar una copia de seguridad y restaurar los datos de configuración de Horizon 7	112
Realizar una copia de seguridad de los datos del servidor de conexión de Horizon y de Horizon Composer	113
Programar copias de seguridad de la configuración de Horizon 7	114
Opciones de copia de seguridad de la configuración de Horizon 7	114
Exportar los datos de configuración del servidor de conexión de Horizon	115
Restaurar los datos de configuración del servidor de conexión de Horizon y de Horizon Composer	117
Importar los datos de configuración en el servidor de conexión de Horizon	117
Restaurar una base de datos de Horizon Composer	119
Códigos de resultado de la restauración de la base de datos de Horizon Console	120
Exportar datos de la base de datos de Horizon Composer	121
Códigos de resultado de la exportación de la base de datos de Horizon Composer	122
Supervisar los componentes de Horizon 7	122
Supervisar el estado de carga del servidor de conexión de Horizon	124
Supervisar servicios en el servidor de conexión de Horizon	125
Comprender los servicios de Horizon 7	126
Detener e iniciar servicios de Horizon 7	126
Servicios de un host del servidor de conexión	126
Servicios de un servidor de seguridad	127
Cambiar la clave de licencia o los modos de licencia del producto en Horizon Console	128
Supervisar el uso del producto	129
Restablecer los datos de uso de la licencia	130
Participar en el Programa de mejora de la experiencia de cliente	131
Integración del servidor de conexión de Horizon con Skyline Collector Appliance	131
10 Primeros pasos con JMP Integrated Workflow	133
Acerca de JMP Integrated Workflow	133
Empezar a utilizar JMP Integrated Workflow	134
11 Administrar la configuración de JMP	135
Configurar las opciones de JMP por primera vez	135
Administrar la configuración de JMP	138
Editar configuración de JMP Server	138
Editar credenciales de Horizon 7	139
Editar la URL del servidor de conexión de Horizon	139

Agregar dominios de Active Directory	140
Editar la información de dominio de Active Directory	141
Eliminar la información de dominio de Active Directory	141
Agregar información de App Volumes	142
Editar la información de la instancia de App Volumes	143
Eliminar información de la instancia de App Volumes	143
Agregar información sobre el recurso compartido de configuración de Dynamic Environment Manager	144
Edita la información de recurso compartido del archivo de configuración de Dynamic Environment Manager	145
Eliminar la información de un recurso compartido de configuración de Dynamic Environment Manager	145

12 Administrar asignaciones JMP 146

Crear una asignación JMP	147
Editar una asignación JMP	148
Duplicar una asignación JMP	150
Eliminar una asignación JMP	151

13 Configurar la generación de informes de eventos en Horizon Console 152

Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7 en Horizon Console	152
Preparar una base de datos SQL Server para los informes de eventos en Horizon Console	153
Configurar la base de datos de eventos en Horizon Console	154
Configurar el registro de eventos en archivos o el servidor syslog en Horizon Console	156
Supervisar eventos en Horizon 7	158
Mensajes de eventos de Horizon 7	158

14 Usar Horizon Help Desk Tool en Horizon Console 160

Iniciar Horizon Help Desk Tool en Horizon Console	161
Solucionar los problemas de los usuarios en Horizon Help Desk Tool	161
Detalles de las sesiones para Horizon Help Desk Tool	165
Procesos de las sesiones de Horizon Help Desk Tool	170
Estado de la aplicación para Horizon Help Desk Tool	171
Solucionar problemas de las sesiones de aplicaciones o de escritorios de Horizon Help Desk Tool	172

15 Usar el comando vdmadmin 174

Uso del comando vdmadmin	176
Autenticación del comando vdmadmin	176
Formato de la salida del comando vdmadmin	177
Opciones del comando vdmadmin	177
Configurar los registros en Horizon Agent con la opción -A	178
Sobrescribir direcciones IP con la opción -A	181

Actualizar las entidades de seguridad externa con la opción -F	182
Enumerar y mostrar las supervisiones de estado con la opción -H	183
Especificar y visualizar informes sobre el funcionamiento de Horizon 7 con la opción -I	184
Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -l	185
Asignar máquinas dedicadas usando la opción -L	188
Visualizar información sobre las máquinas con la opción -M	189
Recuperar espacio de disco de las máquinas virtuales con la opción -M	190
Configurar filtros de dominios con la opción -N	192
Configurar los filtros de dominios	195
Ejemplo de filtrado para incluir dominios	196
Ejemplo de filtrado para excluir dominios	197
Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P	199
Configurar clientes en modo de pantalla completa con la opción -Q	201
Visualizar el primer usuario de un equipo con la opción -R	207
Eliminar una entrada de una instancia del servidor de conexión o del servidor de seguridad con la opción -S	208
Proporcionar credenciales secundarias para los administradores con la opción -T	209
Visualizar información sobre los usuarios con la opción -U	211
Bloquear o desbloquear las máquinas virtuales con la opción -V	211
Detectar y resolver conflictos de esquemas y entradas LDAP usando la opción -X	213

Administración de VMware Horizon Console

1

Administración de VMware Horizon Console describe cómo configurar y administrar VMware Horizon[®] 7, crear administradores, configurar la autenticación de usuario, configurar las directivas y realizar tareas de administración en Horizon Console. Este documento también describe cómo mantener y solucionar los problemas de los componentes de Horizon 7.

Para obtener más información sobre cómo utilizar Horizon Console para configurar y administrar un entorno de Arquitectura de Cloud Pod, consulte el documento *Administrar la arquitectura Cloud Pod en 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 Windows o Linux con experiencia que estén familiarizados con la tecnología de máquinas virtuales y operaciones de centros de datos.

Usar VMware Horizon Console

2

VMware Horizon Console es la versión más reciente de la interfaz web con la que puede crear y administrar aplicaciones y escritorios publicados, así como escritorios virtuales. Horizon Console también integra funciones de VMware Horizon Just-in-Time Management Platform (JMP) Integrated Workflow para administrar áreas de trabajo.

Horizon Console está disponible tras instalar y configurar el servidor de conexión de Horizon.

Para obtener más información sobre las funciones de JMP Integrated Workflow, consulte [Capítulo 10 Primeros pasos con JMP Integrated Workflow](#).

Este capítulo incluye los siguientes temas:

- [Características de Horizon 7 admitidas](#)
- [Ventajas de utilizar Horizon Console](#)
- [Instalar y configurar Horizon Console](#)
- [Iniciar sesión en Horizon Console](#)

Características de Horizon 7 admitidas

Horizon Console se basa en la tecnología HTML5 y permite administrar la implementación completa de Horizon 7. Horizon Console reemplaza la Horizon Administrator basado en Flash.

Para obtener más información sobre las funciones de Horizon 7 que se admiten con Horizon Administrator, consulte el documento *Administración de Horizon 7*.

Se admiten las siguientes funciones:

- Servidores
 - Configuración del servidor de conexión de Horizon
 - Base de datos de eventos
- Autorizaciones
 - Autorizaciones de grupos y usuarios
 - Autorizaciones de escritorios

- Autorizaciones de aplicaciones
- Autorizaciones globales
- Directivas globales
- Autenticación
 - Autenticación de acceso remoto
 - Acceso sin autenticar para las aplicaciones publicadas
 - Autenticación con tarjeta inteligente
 - Administración delegada basada en funciones
- Escritorios virtuales
 - Grupos de asignaciones dedicadas y automatizadas de máquinas virtuales completas
 - Grupos de asignaciones automatizadas flotantes y de asignaciones dedicadas de clones instantáneos
 - Grupo de escritorios automatizados de clones vinculados
 - Grupos de asignaciones flotantes y automatizadas de máquinas virtuales completas
 - Grupos de escritorios manuales
 - Discos persistentes
- Escritorios publicados
 - Granjas manuales
 - Granjas automatizadas de clones instantáneos
 - Granjas automatizadas de clones vinculados
 - grupos de escritorios RDS
- Aplicaciones publicadas
 - Grupos manuales de aplicaciones
 - Grupos de aplicaciones de aplicaciones existentes
- Máquinas virtuales
 - Máquinas virtuales disponibles en vCenter Server
 - Máquinas registradas que no están disponibles en vCenter Server
- Arquitectura de Cloud Pod

No se admiten las siguientes funciones:

- aplicaciones ThinApp
- Servidor de seguridad
- Servidor Mirage

Ventajas de utilizar Horizon Console

Entre las ventajas de utilizar Horizon Console se incluyen un proceso de implementación de aplicaciones y escritorios más sencillo, entrega de escritorios justo a tiempo y una interfaz web más segura que elimina los riesgos de seguridad.

La interfaz web de Horizon Console se actualiza para incluir los flujos de trabajo de uso sencillo de manera que se puedan implementar aplicaciones y escritorios y solucionar los problemas relacionados con ellos.

Horizon Console también incluye las funciones de JMP Integrated Workflow, que incorporan tecnologías de VMware Dynamic Environment Manager, VMware App Volumes y clon instantáneo en un flujo de trabajo integrado. Esto permite proporcionar escritorios remotos bajo demanda con rapidez de implementación y ampliación. Si desea obtener más información, consulte [Acerca de JMP Integrated Workflow](#).

Horizon Console tiene una interfaz web basada en HTML5 que es más segura y está más actualizada para eliminar muchos riesgos de seguridad y muchas vulnerabilidades.

Instalar y configurar Horizon Console

La URL de Horizon Console está disponible desde la interfaz web de Horizon Administrator tras usar el instalador del servidor de conexión de Horizon para instalar y configurar el servidor de conexión. JMP Integrated Workflow está disponible en Horizon Console después de usar el instalador de JMP Server para instalar y configurar JMP Server.

Para obtener más información sobre cómo instalar el servidor de conexión, consulte el documento *Instalación de Horizon 7*.

Para obtener más información sobre cómo instalar y configurar JMP Server consulte el documento *Guía de instalación y configuración de VMware Horizon JMP Server*.

Iniciar sesión en Horizon Console

Para realizar tareas de implementación de grupos de escritorios y aplicaciones, tareas para solucionar problemas o administrar flujos de trabajo de JMP, debe iniciar sesión en Horizon Console. Acceda a Horizon Console usando una conexión segura (TLS).

Requisitos previos

- Verifique que el servidor de conexión de Horizon esté instalado en un equipo dedicado.
- Para que un usuario inicie sesión en Horizon Console, se le debe asignar cualquier función predefinida o una combinación de funciones predefinidas. Un usuario no puede iniciar sesión en Horizon Console cuando se le asigna una función personalizada o una combinación de funciones predefinidas y personalizadas. Para obtener más información sobre cómo configurar el acceso basado en funciones, consulte [Configurar la administración delegada basada en funciones](#).

- Verifique que esté usando un navegador web que Horizon Console admita. Para obtener más información sobre los navegadores web admitidos, 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/admin

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

El acceso a Horizon Console 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.	Cuando se conecte por primera vez, el navegador web mostrará la página Bienvenidos a VMware Horizon 7 .
Se configura el certificado autofirmado y predeterminado proporcionado con el servidor de conexión.	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 Para utilizar siempre la página de inicio de sesión de Horizon Console, haga clic en **Usar siempre esta opción**.

Nota Si hace clic en **Usar siempre esta opción** y, a continuación, en **Iniciar**, la próxima vez que abra una pestaña en el navegador web e introduzca **https://servidor/admin**, accederá siempre a la página de inicio de sesión de Horizon Console. Para acceder de nuevo a la página **Bienvenidos a VMware Horizon 7**, vaya a **https://servidor/admin/#home**.

- 3 Haga clic en **Iniciar** en Horizon Console para abrir la página de inicio de sesión de Horizon Console.
- 4 Inicie sesión como un usuario con credenciales para acceder a la cuenta 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.

Pasos siguientes

Para identificar el nombre del clúster o el pod de la CPA del servidor de conexión con el que está trabajando, puede consultar el nombre en el encabezado Horizon Console y en la pestaña Navegador web.

Configurar el servidor de conexión de Horizon en Horizon Console

3

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

Este capítulo incluye los siguientes temas:

- [Configurar vCenter Server y Horizon Composer en Horizon Console](#)
- [Realizar una copia de seguridad del servidor de conexión de Horizon en Horizon Console](#)
- [Configurar las opciones de las sesiones cliente en Horizon Console](#)
- [Habilitar o deshabilitar un servidor de conexión de Horizon en Horizon Console](#)
- [Editar las URL externas para las instancias del servidor de conexión de Horizon](#)
- [Registrar puertas de enlace en Horizon Console](#)

Configurar vCenter Server y Horizon Composer en Horizon Console

Para usar las máquinas virtuales como escritorios remotos, debe configurar Horizon 7 para que se comunique con vCenter Server. Para crear y administrar grupos de escritorios de clones vinculados, debe configurar los parámetros de Horizon Composer en Horizon Console.

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 Horizon Storage Accelerator para vCenter Server.

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

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

Para garantizar la seguridad, cree una cuenta de usuario independiente que se usará con Horizon 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 Horizon 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 Console cuando configure los dominios de Horizon Composer en el asistente **Agregar vCenter Server** y cuando configure e implemente los grupos de escritorios de clones vinculados.

Instalar la clave de licencia del producto en Horizon Console

Antes de poder utilizar el servidor de conexión, debe introducir una clave de licencia.

Nota La clave de licencia del producto no es obligatoria si tiene una licencia de suscripción de Horizon 7. Para obtener más información sobre las licencias de suscripción, consulte "Habilitar Horizon 7 para las licencias de suscripción" en el documento *Instalación de Horizon 7*.

La primera vez que inicia sesión, Horizon Console muestra la página Licencia y uso del producto.

No es necesario configurar una clave de licencia cuando instala una instancia del servidor de conexión replicada o un servidor de seguridad. Las instancias replicadas y los servidores de seguridad usan la clave de licencia común almacenada en la configuración LDAP de View.

Nota El servidor de conexión necesita una clave de licencia válida. La clave de licencia del producto tiene 25 caracteres.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Licencia y uso del producto**.
- 2 En el panel **Configuración de licencias**, haga clic en **Editar licencia**.
- 3 Introduzca el número de serie de la licencia y haga clic en **Aceptar**.
- 4 Verifique la fecha de caducidad de la licencia.
- 5 Verifique que las licencias de View Composer, de escritorio y de aplicaciones remotas estén habilitadas o deshabilitadas, según la edición de VMware Horizon 7 que la licencia de producto le permita utilizar.

No todas las funciones y características de VMware Horizon 7 están disponibles en todas las ediciones. Si desea obtener más información sobre los conjuntos de funciones de cada edición, consulte <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

Agregar instancias de vCenter Server a Horizon 7 en Horizon Console

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 (TLS).

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 Horizon 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. 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 Horizon Composer.

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **vCenter Server**, 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 (opcional) Seleccione **VMware Cloud on AWS** si se implementa el vCenter Server en VMware Cloud on AWS.

Para obtener más información sobre la integración de Horizon 7 con VMware Cloud on AWS, consulte el documento *Integración de Horizon 7*.

- 9 En Configuración avanzada, establezca el límite de las operaciones simultáneas en vCenter Server y Horizon Composer.

- 10 Haga clic en **Siguiente** y siga las instrucciones del asistente.

Pasos siguientes

Configure los parámetros de Horizon Composer.

- Si la instancia de vCenter Server se configura con un certificado TLS firmado y el servidor de conexión confía en el certificado raíz, el asistente Agregar vCenter Server muestra la página Configuración de Horizon 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 los parámetros de Horizon Composer

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

Debe haber una asignación de tipo uno a uno entre cada instancia del servicio de Horizon Composer y vCenter Server. Un servicio de Horizon Composer puede funcionar con solo una instancia de vCenter Server. Cada instancia de vCenter Server puede asociarse únicamente a un servicio de Horizon Composer.

Después de la implementación inicial de Horizon 7, puede migrar el servicio de Horizon Composer a un nuevo host para admitir una implementación creciente o variable de Horizon 7. Puede editar la configuración inicial de Horizon Composer en Horizon Console, pero debe realizar pasos adicionales para asegurarse de que la migración se realizó correctamente.

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 Horizon 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 en Horizon Console](#).
- Compruebe que el servicio de Horizon Composer aún no esté configurado para conectarse a otra instancia de vCenter Server.

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **vCenter Server**, haga clic en **Agregar** y complete la información de vCenter Server information en la página **Configuración de vCenter Server Settings**. A continuación, haga clic en **Siguiente**.
- 3 En la página **Configuración de Horizon Composer**, si no está utilizando Horizon Composer, seleccione **No utilizar Horizon Composer**.

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

- 4 Si utiliza Horizon Composer, seleccione la ubicación del host de Horizon Composer.

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

- 5 Haga clic en **Siguiente** para mostrar la página **Horizon Composer Domains**.

Pasos siguientes

Configure los dominios de Horizon Composer.

- Si la instancia de Horizon Composer se configura con un certificado TLS firmado y el servidor de conexión confía en el certificado raíz, el asistente Agregar vCenter Server muestra la página Horizon Composer Domains.
- Si la instancia de Horizon Composer se configura con un certificado predeterminado, debe determinar primero si acepta la huella digital del certificado existente.

Configurar los dominios de Horizon Composer

Debe configurar un dominio de Active Directory en el que Horizon Composer implemente escritorios de clones vinculados. Puede configurar varios dominios para Horizon Composer. Después de agregar por primera vez la configuración de Horizon Composer y de vCenter Server a Horizon 7, puede agregar más dominios de Horizon Composer editando la instancia de vCenter Server en Horizon Console.

Requisitos previos

- El administrador de Active Directory debe crear un usuario de Horizon 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 Horizon Composer](#).
- En Horizon Console, compruebe que completó las páginas **Configuración de vCenter Server** y **Configuración de Horizon Composer** del asistente **Agregar vCenter Server**.

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **vCenter Server**, haga clic en **Agregar** y complete la información de vCenter Server information en la página **Configuración de vCenter Server Settings**. A continuación, haga clic en **Siguiente**.
- 3 En la página **Configuración de Horizon Composer**, si utiliza Horizon Composer, seleccione la ubicación del host de Horizon Composer y haga clic en **Siguiente**.

Para obtener más información sobre Horizon Composer, consulte [Configurar los parámetros de Horizon Composer](#).
- 4 En la página **Horizon Composer Domains**, haga clic en **Agregar** para agregar el usuario de Horizon Composer que se usará para la información de la cuenta de operaciones de AD.
- 5 Introduzca el nombre de dominio de Active Directory.

Por ejemplo: **domain.com**
- 6 Introduzca el nombre de usuario del dominio del usuario de Horizon Composer, incluido el nombre de dominio.

Por ejemplo: **domain.com\admin**
- 7 Introduzca la contraseña de la cuenta.
- 8 Haga clic en **Aceptar**.
- 9 Para agregar cuentas de usuario del dominio con privilegios en otros dominios de Active Directory en el que implementa grupos de clones vinculados, repita los pasos anteriores.
- 10 Haga clic en **Siguiente** para mostrar la página **Configuración de almacenamiento**.

Pasos siguientes

Habilite la recuperación de espacio de disco de la máquina virtual y configure Horizon Storage Accelerator para Horizon 7.

Agregar un administrador de dominio de clones instantáneos en Horizon Console

Antes de crear un grupo de escritorios de clones instantáneos, debe agregar un administrador de dominio de clones instantáneos a Horizon 7.

Requisitos previos

- Compruebe que el administrador de dominio de clones instantáneos tenga los privilegios de dominio de Active Directory necesarios. Para obtener más información, consulte "Crear una cuenta de usuario para operaciones de clones instantáneos" en el documento *Instalación de Horizon 7*.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Cuentas de dominio de Instant Clone**.

- 2 Haga clic en **Agregar**.
- 3 Seleccione el dominio para el administrador de dominio de clones instantáneos.
- 4 Introduzca el nombre de usuario y contraseña.

Pasos siguientes

En Horizon Console, puede agregar o quitar un administrador de dominio de clones instantáneos o exportar la lista de administradores de clones instantáneos a Microsoft Excel. Desplácese hasta **Configuración > Cuentas de dominio de Instant Clone** y seleccione un administrador de dominio de clones instantáneos. Haga clic en **Editar** para editar el dominio y la información de inicio de sesión del administrador. Haga clic en **Eliminar** para quitar un administrador. Haga clic en el icono de exportación para exportar la lista de administradores de clones instantáneos a un archivo de Microsoft Excel.

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. 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 versiones posteriores, 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 Console 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 Horizon Composer.
- Funciona únicamente con vSphere 5.1 o versiones posteriores 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 Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **vCenter Server**, haga clic en **Agregar** y complete las páginas del asistente **Agregar vCenter Server** que preceden a la página **Configuración de almacenamiento**.
- 3 En la página **Configuración de almacenamiento**, seleccione **Reclamar espacio de disco de la máquina virtual**.

Esta opción está seleccionada de forma predeterminada si realiza una instalación nueva de Horizon 7. Debe seleccionar **Reclamar espacio de disco de la máquina virtual** si va a actualizar a una versión posterior de Horizon 7.

Pasos siguientes

En la página **Configuración de almacenamiento**, configure Horizon Storage Accelerator.

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

Configurar Horizon Storage Accelerator para vCenter Server

vSphere permite configurar los hosts ESXi para almacenar en caché datos del disco de la máquina virtual. Esta función, denominada Horizon Storage Accelerator, usa la función de memoria caché de lectura basada en contenido (CBRC) en los hosts ESXi. Horizon Storage Accelerator 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 E/S por segundo durante los arranques masivos, Horizon Storage Accelerator 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 Horizon Storage Accelerator en el asistente **Agregar vCenter Server** en Horizon Console, como se describe en este procedimiento.

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

Horizon Storage Accelerator está habilitado para grupos de escritorios de forma predeterminada. La función puede estar deshabilitada o habilitada cuando cree o edite un grupo. Lo más recomendable es habilitar esta función cuando cree un grupo de escritorios por primera vez. Si habilita la función al editar un grupo existente, debe asegurarse de que se hayan creado una nueva réplica y sus discos resumen antes de que se aprovisionen los clones vinculados. Puede crear una nueva réplica volviendo a componer el grupo en una snapshot nueva o volviendo a equilibrar el grupo en un nuevo almacén de datos. Los archivos de resumen solo se pueden configurar en las máquinas virtuales en un grupo de escritorios cuando están desconectados.

Puede habilitar Horizon Storage Accelerator en grupos de escritorios que contengan clones vinculados y grupos que contengan máquinas virtuales completas.

No se admite la tecnología de snapshot NFS nativa (VAAI) en grupos que están habilitados para Horizon Storage Accelerator.

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

Importante Si tiene pensado usar esta función y está usando varios pods de Horizon 7 que comparten algunos hosts ESXi, debe habilitar la función Horizon Storage Accelerator en todos los pods que se encuentren en los hosts ESXi compartidos. Las configuraciones inconsistentes en varios pods puede causar inestabilidad en las máquinas virtuales de los hosts ESXi compartidos.

Requisitos previos

- Compruebe que vCenter Server y los hosts ESXi tengan la versión 5.1 o una versión posterior.

En un clúster ESXi, compruebe que todos los hosts cuenten con la versión 5.1 o posterior.

- Verifique que el usuario de vCenter Server tenga asignado el privilegio **Host > Configuración > Configuración avanzada** en vCenter Server.

Consulte los temas del documento *Instalación de Horizon 7* que describen los privilegios de Horizon 7 y de Horizon Composer necesarios para el usuario de vCenter Server.

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **vCenter Server**, haga clic en **Agregar** y complete las páginas del asistente **Agregar vCenter Server** que preceden a la página **Configuración de almacenamiento**.
- 3 En la página **Configuración de almacenamiento**, seleccione **Habilitar el acelerador de almacenamiento de Horizon**.

Esta opción está seleccionada de manera predeterminada.
- 4 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.
- 5 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**.
- 6 En la página Configuración de almacenamiento, haga clic en **Siguiente**.
- 7 Después de revisar la configuración en la página **Listo para finalizar**, haga clic en **Enviar**.

Pasos siguientes

Configure las opciones para las conexiones y sesiones cliente. Consulte "Configurar las opciones de las sesiones cliente" en el documento *Administración de Horizon 7*.

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

Límites de operaciones simultáneas para vCenter Server y Horizon 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 Horizon Composer.

Puede configurar estas opciones en el panel Configuración avanzada en la página **Configuración de vCenter Server** del asistente **Agregar vCenter Server**.

Tabla 3-1. Límites de operaciones simultáneas para vCenter Server y Horizon Composer

Configuración	Descripción
Número máximo de operaciones de aprovisionamiento de vCenter simultáneas	<p>Determina el número máximo de solicitudes simultáneas que el servidor de conexión puede realizar para aprovisionar y eliminar máquinas virtuales completas en esta instancia de vCenter Server.</p> <p>El valor predeterminado es 20.</p> <p>Esta configuración se aplica únicamente a las máquinas virtuales completas.</p>
Máximo número de operaciones de alimentación simultáneas	<p>Determina el número máximo de operaciones de alimentación simultáneas (iniciar, apagar, suspender, etc.) que pueden tener lugar en máquinas virtuales administradas por el servidor de conexión en esta instancia de vCenter Server.</p> <p>El valor predeterminado es 50.</p> <p>Para obtener más instrucciones sobre cómo calcular el valor de esta opción, consulte Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto.</p> <p>Esta configuración se aplica a las máquinas virtuales completas y a los clones vinculados.</p>
Máximo de operaciones de mantenimiento simultáneas de Horizon Composer	<p>Determina el número máximo de operaciones simultáneas de actualización, de recomposición y de reequilibrio de Horizon Composer que pueden realizarse en clones vinculados administrados por esta instancia de Horizon Composer.</p> <p>El valor predeterminado es 12.</p> <p>Es necesario que se cierren las sesiones activas de los escritorios remotos antes de que pueda comenzar una operación de mantenimiento. Si obliga a los usuarios a cerrar sesión cuando la operación de mantenimiento comienza, el número máximo de operaciones simultáneas en los escritorios remotos para las que son necesarias que se cierren las sesiones es la mitad del valor configurado. Por ejemplo, si configura esta opción en 24 y obliga a los usuarios a cerrar sesión, el número máximo de operaciones simultáneas en los escritorios para las que son necesarias que se cierren las sesiones es 12.</p> <p>Esta opción se aplica únicamente a los clones vinculados.</p>
Máximo de operaciones de aprovisionamiento simultáneas de Horizon Composer	<p>Determina el número máximo de operaciones simultáneas de creación y eliminación que pueden realizarse en clones vinculados administrados por esta instancia de Horizon Composer.</p> <p>El valor predeterminado es 8.</p> <p>Esta opción se aplica únicamente a los clones vinculados.</p>
Máximo de operaciones de aprovisionamiento simultáneas de Instant Clone Engine	<p>Determina el número máximo de operaciones simultáneas de creación y eliminación que pueden realizarse en clones instantáneos administrados por esta instancia de vCenter Server.</p> <p>Esta opción se aplica únicamente a los clones instantáneos.</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 Horizon Composer a Horizon 7, debe asegurarse de que los certificados TLS que se usan para las instancias de vCenter Server y de Horizon Composer sean válidos y que el servidor de conexión confíe en ellos. Si los certificados predeterminados instalados con vCenter Server y Horizon 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 Horizon 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 Horizon 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 "Configurar los certificados TLS de los servidores de Horizon 7", disponible en el documento *Instalación de Horizon 7*.

Primero agregue vCenter Server y Horizon Composer en Horizon Console 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 vCenter Server.

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 Horizon Composer no sea de confianza, o bien si reemplaza un certificado de confianza por uno que no lo sea.

Procedimiento

- 1 Cuando aparezca el cuadro de diálogo Se detectó un certificado no válido en Horizon Console, 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 vCenter Server o de Horizon Composer.
 - a En el host de vCenter Server o de Horizon Composer, inicie el complemento MMC y abra el almacén de certificados de Windows.
 - b Desplácese hasta el certificado de vCenter Server o de Horizon 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 Horizon 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 Horizon 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 Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **vCenter Servers**, seleccione la instancia vCenter Server.
- 3 Haga clic en **Eliminar**.

Un mensaje le advierte de 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 Horizon Composer de Horizon 7

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

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

Procedimiento

- 1 Elimine los grupos de escritorios de clones vinculados creados por Horizon Composer.
 - a En Horizon Console, seleccione **Inventario > 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. Además, se eliminan las entradas de la base de datos de Horizon Composer asociadas y las réplicas que Horizon Composer creara.
 - d Repita estos pasos para cada grupo de escritorios de clones vinculados creado por Horizon Composer.
- 2 Acceda a **Configuración > Servidores**.
- 3 En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server asociada a Horizon Composer.
- 4 Haga clic en **Editar**.
- 5 En la pestaña **Horizon Composer**, en la configuración de Horizon Composer Server, seleccione **No utilizar Horizon 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 Horizon Composer en otro host y volver a configurar Horizon 7 para conectarse al nuevo servicio de Horizon Composer, debe realizar ciertos pasos adicionales. Para obtener más información sobre cómo migrar Horizon Composer sin máquinas virtuales de clones vinculados, consulte el documento *Administración de Horizon 7*.

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 en Horizon Console

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 Horizon 7 y de Horizon Composer.

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 de los datos del servidor de conexión de Horizon y de Horizon Composer](#).

Configurar las opciones de las sesiones cliente en Horizon Console

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.

Configuración global de las sesiones cliente en Horizon Console

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 Console, si aparecen mensajes de advertencia y anteriores al inicio de sesión, y si Horizon Console trata a Windows Server como un sistema operativo que admite escritorios remotos, entre otras opciones.

En Horizon Console, puede establecer la configuración global en **Configuración > Configuración global > Configuración general**.

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 3-2. 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 Console antes de que caduque la sesión.</p> <hr/> <p>Importante Al establecer el tiempo de espera de la sesión de Horizon Console en un número elevado de minutos, aumenta el riesgo de que Horizon Console 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 Console es 30 minutos. Puede establecer el tiempo de espera de la sesión de 10 a 4320 minutos (72 horas).</p> <p>Antes de que se agote el tiempo de espera de una sesión, aparecerá un mensaje de advertencia con una cuenta atrás de 60 segundos. Si hace clic en la sesión antes de que finalice la cuenta atrás, la sesión continuará. Después de 60 segundos, aparecerá un mensaje de error informándole de que se agotó el tiempo de espera de la sesión y que debe volver a iniciarla.</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>
Habilitar actualizaciones automáticas de estado	<p>Determina si las actualizaciones de estado aparecen en el panel del estado global situado en la esquina superior izquierda de Horizon Console cada pocos minutos. La página del panel de control de Horizon Console también se actualiza cada pocos minutos.</p> <p>De forma predeterminada, esta opción no está habilitada.</p>

Tabla 3-2. 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. 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> <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> <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>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>
<p>Mostrar la advertencia antes del cierre de sesión</p>	<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> <p>Está programada una actualización importante para el escritorio y este se desconectará en 5 minutos. Guarde ahora el trabajo sin guardar.</p>

Tabla 3-2. Configuración global general de las sesiones cliente (continuación)

Configuración	Descripción
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 Console muestra todos los equipos Windows Server disponibles, incluidos los equipos en los que están instalados los componentes del servidor de Horizon 7.</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 7.0.2 y versiones posteriores.</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 versiones posteriores.</p>

Tabla 3-2. Configuración global general de las sesiones cliente (continuación)

Configuración	Descripción
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 versiones posteriores.</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> <hr/> <p>Importante Si habilita la opción 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. Esto no se aplica a Horizon Client versión 5.0 y versiones posteriores si hay un dominio de usuario único.</p> <hr/> <p>Importante Para obtener más información sobre las implicaciones de seguridad y la facilidad de uso de esta opción, consulte el documento <i>Seguridad de Horizon 7</i>.</p>
Enviar lista de dominios	<p>Seleccione esta casilla de verificación para permitir que el servidor de conexión envíe la lista de nombres de dominio al cliente antes de que el usuario se autentique.</p> <hr/> <p>Importante Para obtener más información sobre las implicaciones de seguridad y la facilidad de uso de esta opción, consulte el documento <i>Seguridad de Horizon 7</i>.</p>

Configuración de seguridad global para conexiones y sesiones cliente en Horizon Console

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 el estado de seguridad se mejoró.

En Horizon Console, puede establecer la configuración de seguridad global en **Configuración > Configuración global > Configuración de seguridad**.

TLS es necesario para todas las conexiones de Horizon Client y de Horizon Console 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.

Tabla 3-3. 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 del mensaje	<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>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

Configuración global de restricciones de cliente de las sesiones cliente en Horizon Console

La configuración global de restricciones de cliente puede restringir el inicio de escritorios virtuales, escritorios publicados y aplicaciones publicadas a clientes y versiones específicos.

En Horizon Console, puede establecer la configuración global de restricciones de cliente accediendo a **Configuración > Configuración global > Configuración de restricciones de cliente** e introduciendo la versión de Horizon Client.

Horizon Client debe tener la versión 4.5.0 o posterior, excepto Horizon Client para Chrome, que debe tener la versión 4.8.0 o posterior. Las versiones anteriores de Horizon Client no pueden conectarse a los escritorios remotos y las aplicaciones publicadas cuando esta función está configurada.

Nota La configuración de restricciones de cliente solo impide que los usuarios finales inicien aplicaciones publicadas y escritorios remotos. Esta función no impide que los usuarios finales inicien sesión en Horizon 7.

Tabla 3-4. Configuración global de restricciones de cliente de las sesiones cliente

Configuración	Descripción
Horizon Client para Windows	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Horizon Client para Linux	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Horizon Client para Mac	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Horizon Client para iOS	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Horizon Client para Android	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Horizon Client para UWP	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Horizon Client para Chrome	Para Horizon Client, introduzca la versión 4.8.0 o una versión posterior.
Horizon Client para HTML Access	Para Horizon Client, introduzca la versión 4.5.0 o una versión posterior.
Bloquear clientes adicionales	<p>Si selecciona esta opción, los demás tipos de clientes de Horizon Client, excepto los incluidos en la lista blanca, no podrán iniciar aplicaciones publicadas ni escritorios.</p> <p>Sin embargo, si desea que los usuarios finales utilicen otros tipos de clientes para iniciar aplicaciones publicadas y escritorios, debe agregar el tipo de cliente al atributo LDAP <code>pae-AdditionalClientTypes</code> para omitir la configuración de bloqueo de ese tipo de cliente.</p> <p>Puede usar la utilidad ADSI Edit para editar los atributos LDAP en el servidor de conexión.</p> <p>En la utilidad ADSI Edit, el atributo LDAP <code>pae-AdditionalClientTypes</code> está disponible en <code>CN=Common, OU=Global, OU=Properties, DC=vdi, DC=vmware, DC=int</code>.</p>
Mensaje	Introduzca el mensaje que quiere que se muestre si un usuario intenta iniciar una aplicación publicada o un escritorio desde una versión o un tipo de cliente que no estén en la lista blanca.

Habilitar o deshabilitar un servidor de conexión de Horizon en Horizon Console

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 Console, seleccione **Configuración > 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 para las instancias del servidor de conexión de Horizon

Horizon Console permite editar las URL externas para las instancias del servidor de conexión.

De forma predeterminada, únicamente los clientes de túnel que residen dentro de la misma red de un host 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.

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 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 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.

Procedimiento

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

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

Ejemplo: `https://horizon.example.com:443`

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

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

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 conexión.

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

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

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

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

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

Las URL externas se actualizan de forma inmediata. No necesita reiniciar el servidor de conexión para que se apliquen los cambios.

Registrar puertas de enlace en Horizon Console

Horizon Client se conecta a través de una puerta de enlace o de un dispositivo Unified Access Gateway que registre en Horizon Console.

Puede registrar o cancelar puertas de enlace del registro en Horizon Console. Para eliminar la puerta de enlace del registro, seleccione el dispositivo Unified Access Gateway o la puerta de enlace y haga clic en **Eliminar del registro**.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Servidores**.
- 2 En la pestaña **Puertas de enlace**, haga clic en **Registrar**.
- 3 Introduzca el FQDN del dispositivo Unified Access Gateway o de la puerta de enlace.
- 4 Haga clic en **Aceptar**.

Configurar la autenticación de tarjeta inteligente

4

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 en Horizon Console](#)
- [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 Console. 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 un dispositivo Unified Access Gateway, 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 servidor de conexión.

5 Configurar las opciones de la tarjeta inteligente en Horizon Console

Puede usar Horizon Console 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.

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.

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 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` en la carpeta de configuración de la puerta de enlace TLS/SSL en el host 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 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 `longa.key`, establece el tipo del almacén de confianza como `jks` y habilita la autenticación de certificados.

```
trustKeyfile=longa.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 Console.

Configurar las opciones de la tarjeta inteligente en Horizon Console

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

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 Console, seleccione **Configuración > 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 Horizon.

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> <p>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 autenticquen usando la autenticación SecurID y la autenticación con tarjeta inteligente.</p>

- 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 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 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 Para configurar la autenticación con tarjeta inteligente para los administradores que inicien sesión en Horizon Console, seleccione una opción de configuración del menú desplegable **Autenticación de tarjeta inteligente para los administradores** en la sección **Autenticación de Horizon 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 Console. 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 Console.

- 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 en Horizon Console](#).

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 Console.

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

Procedimiento

- 1 Crear un autenticación SAML para el equilibrador de carga o la puerta de enlace de terceros.
Consulte [Configurar un autenticador SAML en Horizon Console](#).
- 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 en Horizon Console

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 Console.

- Seleccione **Configuración > Servidores**.
- En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión y haga clic en **Editar**.
- 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**.
- 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 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 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.

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

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.

Requisitos previos

Familiarícese con las propiedades del archivo `locked.properties` para la comprobación de revocación del certificado OCSP. 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 OCSP.
 - c Establezca `ocspURL` como la URL del respondedor OCSP.
 - d Establezca `ocspSigningCert` como la ubicación del archivo que contiene el certificado firmado del respondedor OCSP.
- 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 4-1. [Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente](#) muestra las propiedades del archivo `locked.properties` para comprobar la revocación del certificado.

Tabla 4-1. 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>
<code>enableOCSP</code>	<p>Establezca esta propiedad en true para permitir la comprobación OCSP de la revocación del certificado.</p> <p>El valor predeterminado es false.</p>
<code>ocspURL</code>	Especifica la URL de un respondedor OCSP.
<code>ocspResponderCert</code>	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.
<code>ocspSendNonce</code>	<p>Cuando esta propiedad se establece en true, se envía un nonce con las solicitudes OCSP para evitar que se repitan las respuestas.</p> <p>El valor predeterminado es false.</p>
<code>ocspCRLFailover</code>	<p>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.</p> <p>El valor predeterminado es true.</p>

Configurar otros tipos de autenticación de usuario

5

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 que tenga las autenticaciones RSA SecurID o RADIUS habilitadas, aparece un cuadro de diálogo de inicio de sesión especial en Horizon Client.

- **Habilitar la autenticación en dos fases en Horizon Console**

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 Console.

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

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 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 la autenticación en dos fases en Horizon Console

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 Console.

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. Debe introducir estos valores en Horizon Console. Puede introducir valores para un autenticador RADIUS primario y secundario.

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión 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 el menú desplegable **Autenticador**, seleccione **Crear autenticador nuevo** y complete la página.

- Para permitir que las etiquetas personalizadas del nombre de usuario y el código de acceso aparezcan en el cuadro de diálogo de autenticación RADIUS para los usuarios finales, introduzca etiquetas personalizadas en los campos **Etiqueta de nombre de usuario** y **Etiqueta de código de acceso**.

- 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 SecureID

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 Console, acceda a **Configuración > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión 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 SecureID**.
- 4 Seleccione **Borrar secreto de nodo** y haga clic en **Aceptar**.
- 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 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 RADIUS no se configuró para aceptar la instancia del servidor de conexión como un cliente RADIUS. Cada instancia del servidor de conexión que use RADIUS debe configurarse como un cliente en el servidor RADIUS. Consulte la documentación de su producto de autenticación RADIUS en dos fases.
- Los valores secretos compartidos en la instancia del servidor de conexión y el servidor RADIUS no coinciden.

Uso de la autenticación SAML

El lenguaje de marcado para confirmaciones 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 inicien 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 creó los grupos de aplicaciones y de escritorios como un usuario con la función Administradores en el grupo de acceso raíz en Horizon Console. 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 Console

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 Console. 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 la documentación 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.
- Si usa Workspace ONE o VMware Identity Manager, anote la URL de la interfaz web del conector.
- Si crea un autenticador para un dispositivo 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 Console, acceda a **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 un dispositivo 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 en el dispositivo Unified Access Gateway o en un dispositivo de terceros, copiar los metadatos y, a continuación, pegarlos 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 el dispositivo Unified Access Gateway o desde un dispositivo de terceros.
Habilitado para el servidor de conexión	Seleccione 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.

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 añada los valores de las 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 cambia el período de caducidad, el servidor de conexión dejará de aceptar aserciones SAML del autenticador SAML como dispositivo Unified Access Gateway o un proveedor de identidades externo 24 horas después, 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 si desea obtener información sobre cómo utilizar la utilidad Editor ADSI en la versión que utilice del sistema operativo Windows.

Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión.
- 2 En el árbol de la consola, seleccione la opción **Conectar a**.
- 3 En el cuadro de texto para **seleccionar o escribir un nombre distinguido o el contexto de nomenclatura**, escriba el nombre distinguido **DC=vmware**, **DC=vmware**, **DC=int**.
- 4 En el panel del equipo, seleccione o escriba **localhost:389** o bien el nombre de dominio completo (FQDN) del host del servidor de conexión seguido por el puerto 389.
Por ejemplo: **localhost:389** o **miequipo.ejemplo.com:389**
- 5 Amplíe el árbol del Editor ADSI, amplíe **OU=Properties**, seleccione **OU=Global** y haga doble clic en **CN=Common** en el panel derecho.
- 6 En el cuadro de diálogo Propiedades, edite el atributo **pae-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.

Procedimiento

- 1 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.

2 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 Console para deshabilitar los autenticadores SAML dinámicos a los que no se pueda acceder. Para obtener más información sobre cómo deshabilitar un autenticador SAML, consulte [Configurar un autenticador SAML en Horizon Console](#).

Configurar las directivas de acceso de Workspace ONE en Horizon Console

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 Console.

Procedimiento

- 1 En Horizon Console, acceda a **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 BioMetricsTimeout	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 y grupos

6

Tras iniciar sesión en Horizon Console, puede configurar la autenticación de usuarios y grupos para controlar el acceso a aplicaciones y escritorios.

Puede configurar el acceso remoto para restringir el acceso de los usuarios y grupos a los escritorios desde fuera de la red. Puede establecer la configuración para que los usuarios sin autenticar accedan a las aplicaciones publicadas desde Horizon Client sin necesidad de credenciales de AD.

Este capítulo incluye los siguientes temas:

- [Restringir acceso a escritorios remotos fuera de la red](#)
- [Configurar el acceso sin autenticar](#)
- [Configurar usuarios para el inicio de sesión híbrido en Horizon Console](#)
- [Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows](#)

Restringir acceso a escritorios remotos fuera de la red

Puede permitir acceso a determinados usuarios autorizados y grupos de una red externa mientras restringe el acceso a otros. Todos los usuarios autorizados tendrán acceso a escritorios y a aplicaciones de la red interna. Si elige no restringir acceso a usuarios específicos de la red externa, todos los usuarios autorizados tendrán acceso a la red externa.

Por motivos de seguridad, es posible que los administradores necesiten restringir a usuarios y a grupos de fuera de la red el acceso a aplicaciones y a escritorios remotos dentro de la red. Cuando un usuario restringido accede al sistema desde una red externa, aparece un mensaje que indica que no está autorizado a usar el sistema. El usuario debe estar dentro de la red interna para acceder a las autorizaciones de grupos de aplicaciones y de escritorios.

Configurar el acceso remoto

Puede permitir el acceso desde fuera de la red a la instancia del servidor de conexión para algunos usuarios y algunos grupos mientras que lo restringe para otros.

Requisitos previos

- Debe implementar un servidor de seguridad, un equilibrador de carga o un dispositivo de Unified Access Gateway fuera de la red como puerta de enlace a la instancia del servidor de conexión de View al que esté autorizado el usuario. Para obtener más información sobre la implementación de un dispositivo de Unified Access Gateway, consulte el documento *Implementación y configuración de Unified Access Gateway*.
- Los usuarios que tienen acceso remoto deben autorizarse a grupos de aplicaciones o de escritorios.

Procedimiento

- 1 En Horizon Console, seleccione **Usuarios y grupos**.
- 2 Haga clic en la pestaña **Acceso remoto**.
- 3 Haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda y, a continuación, haga clic en **Buscar** para buscar grupos o usuarios que coincidan con sus criterios de búsqueda.

Nota Los usuarios con acceso sin autenticar no aparecerán en los resultados de la búsqueda.

- 4 Para proporcionar acceso remoto a un usuario o grupo o a un usuario con acceso sin autenticar, seleccione el usuario o el grupo y haga clic en **Aceptar**.
- 5 Para eliminar un usuario o un grupo del acceso remoto, seleccione el usuario o el grupo y haga clic en **Eliminar** y, a continuación en **Aceptar**.

Configurar el acceso sin autenticar

Los administradores pueden establecer la configuración para que los usuarios sin autenticar accedan a sus 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.

Nota No se admite el acceso sin autenticar para aplicaciones publicadas en un grupo de escritorios.

Para esta función, es necesario el entorno de la versión 7.1 de Horizon 7 y la versión 4.4 de Horizon Client.

Para obtener información sobre las reglas y las directrices necesarias para configurar usuarios con acceso sin autenticar, consulte el documento *Administración de Horizon 7*.

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

- Los administradores solo pueden crear un usuario para cada cuenta de Active Directory.
- 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.
- Si selecciona un usuario con autorizaciones de escritorio y lo convierte en un usuario con acceso sin autenticar, dicho usuario no tendrá acceso a los escritorios autorizados.

Procedimiento

- 1 En Horizon Console, 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.
- 4 Seleccione un usuario y haga clic en **Siguiente**.

- 5 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 **Enviar**.

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 dominio, las autorizaciones de aplicaciones y las sesiones.

Pasos siguientes

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. Consulte "Habilitar el acceso sin autenticar para los usuarios" en el documento *Administración de Horizon 7*.

Habilitar el acceso sin autenticar para los usuarios en Horizon Console

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 Console, seleccione **Configuración > 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. Para obtener más información sobre cómo crear granjas, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon Console*.
- Cree un grupo de aplicaciones para las aplicaciones publicadas que se ejecuten en una granja de hosts RDS. Para obtener más información sobre cómo crear aplicaciones publicadas, consulte *Configurar aplicaciones y escritorios publicados en Horizon Console*.

Procedimiento

- 1 En Horizon Console, seleccione **Usuarios y grupos**.
- 2 En la pestaña **Autorizaciones**, seleccione **Agregar autorización de aplicaciones** en el menú desplegable **Autorizaciones**.
- 3 Haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda, seleccione la casilla de verificación **Usuarios sin autenticar** y haga clic en **Buscar** 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 Seleccione las aplicaciones en el grupo y haga clic en **Enviar**.

Pasos siguientes

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

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. Si se elimina al usuario predeterminado, Horizon Console muestra tanto un mensaje de error interno como uno de eliminación de usuario correcta. Sin embargo, el usuario predeterminado no se elimina de Horizon Console.

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 Console, seleccione **Usuarios y grupos**.
- 2 En la pestaña **Acceso sin autenticar**, seleccione al usuario y haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar**.

Pasos siguientes

Elimine las autorizaciones de las aplicaciones del usuario.

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 usuarios para el inicio de sesión híbrido en Horizon Console

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 Console*.
- Verifique que creó un usuario con acceso sin autenticar. Consulte [Crear usuarios 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 Console, 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 **Iniciar sesión como usuario actual** en el menú **Opciones**, 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 la instancia del servidor de conexión, habilite la opción **Aceptar inicio de sesión como usuario actual** para permitir que la instancia del servidor de conexión acepte las credenciales y la identidad del usuario que se envían cuando los usuarios seleccionan **Iniciar sesión como usuario actual** en el menú **Opciones** de Horizon Client.

Importante Debe comprender los riesgos de seguridad antes de habilitar esta opción. Consulte "Opciones del servidor relacionadas con la seguridad para la autenticación de usuarios" en el documento *Seguridad de Horizon 7*.

- 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 opción **Iniciar sesión como usuario actual** del menú **Opciones** 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 **Iniciar sesión como usuario actual** en 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 **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.

Configurar la administración delegada basada en funciones en Horizon Console

7

Una tarea de administración clave en un entorno de Horizon 7 es determinar quién puede usar Horizon Console y las tareas que esos usuarios tienen autorización para realizar. Con la administración delegada basada en funciones, para asignar de forma selectiva derechos administrativos puede designar funciones de administrador a 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 en Horizon Console](#)
- [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 Console 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 Console. 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 Console.

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 Console 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. Si la función contiene privilegios específicos de objeto, es posible que deba aplicar la función a un grupo de acceso. 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 en Horizon Console

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 Console. 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 Console 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.

- **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 7-1. Administradores diferentes para grupos de acceso diferentes muestra un ejemplo de este tipo de configuración.

Tabla 7-1. 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 7-2. Administradores diferentes para el mismo grupo de acceso muestra un ejemplo de este tipo de configuración.

Tabla 7-2. 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 Console 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 Console 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 Console cuando selecciona un grupo o un usuario administrador. El usuario administrador se denomina Admin 1 y tiene dos permisos.

Tabla 7-3. 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 Console cuando selecciona el grupo de acceso MarketingDesktops.

Tabla 7-4. Permisos en la pestaña Carpetas para MarketingDesktops

Admin	Función	Heredado
horizon-domain.com\Admin1	Administradores de inventario	
horizon-domain.com\Admin1	Administradores (solo lectura)	Sí

El primer permiso es igual que el primer permiso que aparece en [Tabla 7-3. Permisos en la pestaña Administradores y grupos para Admin 1](#). El segundo permiso se hereda del que aparece en [Tabla 7-3. Permisos en la pestaña Administradores y grupos para Admin 1](#). 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 7-3. Permisos en la pestaña Administradores y grupos para Admin 1](#) aparece en Horizon Console cuando selecciona la función Administradores de inventario.

Tabla 7-5. Permisos en la pestaña Permisos de función para Administradores de inventario

Administrador	Grupo de acceso
horizon-domain.com\Admin1	/MarketingDesktops

Administrar administradores

Los usuarios con función de administradores pueden usar Horizon Console para agregar o eliminar grupos y usuarios administradores.

La función de administradores es la función con más poder en Horizon Console. 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 en Horizon Console](#)

Para crear un administrador, seleccione uno de los grupos o usuarios de Active Directory en Horizon Console y asígnele la función de administrador.

■ [Eliminar un administrador en Horizon Console](#)

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 en Horizon Console

Para crear un administrador, seleccione uno de los grupos o usuarios de Active Directory en Horizon Console y asígnele 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 en Horizon Console](#).
- 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 Console, acceda a **Configuración > 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 aplicó 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 en Horizon Console

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 Horizon Console, acceda a **Configuración > 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

Horizon Console permite agregar, eliminar y consultar los permisos de grupos y usuarios administradores concretos, las funciones y los grupos de acceso.

- [Agregar un permiso en Horizon Console](#)

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 en Horizon Console](#)

Es posible eliminar un permiso que incluya un grupo o un usuario administrador específicos, una función específica o un grupo de acceso específico.

- [Revisar permisos en Horizon Console](#)

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 en Horizon Console

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 Console, acceda a **Configuración > 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 Permisos de función, 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 en Horizon Console

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 Console, acceda a **Configuración > 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 permisos en Horizon Console

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 En Horizon Console, acceda a **Configuración > 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 Permisos de función 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

Horizon Console permite agregar y eliminar grupos de acceso, y consultar los equipos y los grupos de escritorios de un grupo de acceso particular.

- [Agregar un grupo de acceso a Horizon Console](#)
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 en Horizon Console](#)
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 en Horizon Console

Puede eliminar un grupo de acceso si no contiene ningún objeto. No puede eliminar el grupo de acceso raíz.

■ Revisar los objetos de un grupo de acceso

Puede consultar los discos persistentes, las granjas o los grupos de escritorios o de aplicaciones que se encuentran en un grupo de acceso concreto de Horizon Console.

■ Revisar las máquinas virtuales de vCenter de un grupo de acceso

Puede ver las máquinas virtuales de vCenter de un grupo de acceso concreto en Horizon Console. Una máquina virtual de vCenter hereda el grupo de acceso de su grupo.

Agregar un grupo de acceso a Horizon Console

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 Console, desplácese hasta el cuadro de diálogo Grupo de acceso.

Opción	Acción
En los escritorios	<ul style="list-style-type: none"> ■ Seleccione Inventario > Escritorios. ■ En el menú desplegable Grupo de acceso, seleccione Nuevo grupo de acceso.
En las granjas	<ul style="list-style-type: none"> ■ Seleccione Inventario > Granjas. ■ En el menú desplegable Grupos de acceso, seleccione Nuevo 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 en Horizon Console

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 Console, seleccione **Inventario > Escritorios** o **Inventario > Granjas**.
- 2 Seleccione un grupo o una granja.

- 3 Seleccione **Cambiar grupo de acceso** en el menú desplegable **Agregar grupo de acceso**.
- 4 Seleccione el grupo de acceso y haga clic en **Aceptar**.

Horizon Console mueve el grupo o granja al grupo de acceso que seleccionó.

Eliminar un grupo de acceso en Horizon Console

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 en Horizon Console](#).

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > 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 los objetos de un grupo de acceso

Puede consultar los discos persistentes, las granjas o los grupos de escritorios o de aplicaciones que se encuentran en un grupo de acceso concreto de Horizon Console.

Procedimiento

- 1 En Horizon Console, diríjase a la página principal de los objetos.

Objeto	Acción
Grupos de escritorios	Seleccione Inventario > Escritorios .
Grupos de aplicaciones	Seleccione Inventario > Aplicaciones .
Granjas	Seleccione Inventario > Granjas .
Discos persistentes	Seleccione Inventario > Discos persistentes .

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 en Horizon Console. Una máquina virtual de vCenter hereda el grupo de acceso de su grupo.

Procedimiento

- 1 En Horizon Console, acceda a **Inventario > 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

Horizon Console permite agregar, modificar y eliminar funciones personalizadas.

- [Agregar una función personalizada en Horizon Console](#)

Si las funciones de administrador predefinidas no responden a sus necesidades, puede combinar privilegios específicos para crear sus propias funciones en Horizon Console.

- [Modificar los privilegios de una función personalizada en Horizon Console](#)

Puede modificar los privilegios de una función personalizada. Sin embargo, no puede modificar las funciones de administrador predefinidas.

- [Eliminar una función personalizada en Horizon Console](#)

Puede eliminar una función personalizada si no está incluida en un permiso. No puede eliminar las funciones de administrador predefinidas.

Agregar una función personalizada en Horizon Console

Si las funciones de administrador predefinidas no responden a sus necesidades, puede combinar privilegios específicos para crear sus propias funciones en Horizon Console.

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 Console, acceda a **Configuración > Administradores**.

- 2 En la pestaña **Privilegios de función**, 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 en Horizon Console

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 Console, acceda a **Configuración > Administradores**.
- 2 En la pestaña **Privilegios de función**, seleccione la función.
- 3 Consulte los privilegios de la función y haga clic en **Editar**.
- 4 Seleccione privilegios o anule su selección.
- 5 Haga clic en **Aceptar** para guardar los cambios.

Eliminar una función personalizada en Horizon Console

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 en Horizon Console](#).

Procedimiento

- 1 En Horizon Console, acceda a **Configuración > Administradores**.
- 2 En la pestaña **Privilegios de función**, 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 Console 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 7-6. Funciones predefinidas en Horizon Console

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 Console. ■ 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 7-6. Funciones predefinidas en Horizon Console (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. ■ Poder iniciar sesión en Horizon Console. ■ 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. ■ Poder iniciar sesión en Horizon Console. 	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. ■ Administrar granjas automatizadas. <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> <p>Los administradores con esta función no pueden crear granjas manuales ni grupos manuales sin administrar, ni eliminar o agregar hosts RDS a una granja o a un grupo manual sin administrar.</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 7-6. Funciones predefinidas en Horizon Console (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 7-7. Privilegios globales

Privilegio	Características del usuario	Funciones predefinidas
Interacción de consola	<p>Inicie sesión y utilice Horizon Console.</p> <hr/> <p>Nota A partir de la versión 7.10 de Horizon 7, el privilegio Interacción de consola se agrega automáticamente a las nuevas funciones y no aparece en la lista de privilegios globales de Horizon Console.</p> <hr/>	<p>Administradores</p> <p>Administradores (solo lectura)</p> <p>Administradores de inventario</p> <p>Administradores de inventario (solo lectura)</p> <p>Configuración global y administradores de directivas</p> <p>Configuración global y administradores de directivas (solo lectura)</p> <p>Administradores del departamento de soporte técnico</p> <p>Administradores del departamento de soporte técnico (solo lectura)</p> <p>Administradores locales</p> <p>Administradores locales (solo lectura)</p>
Interacción directa	<p>Ejecute todos los comandos PowerShell y las utilidades de la línea de comandos, excepto vdmadmin y vdmimport.</p> <p>Los administradores deben tener la función Administradores en el grupo de acceso raíz para usar los comandos vdmadmin, vdmimport y lmvutil.</p> <hr/> <p>Nota A partir de la versión 7.10 de Horizon 7, el privilegio Interacción directa se agrega automáticamente a las nuevas funciones y no aparece en la lista de privilegios globales de Horizon Console.</p> <hr/>	<p>Administradores</p> <p>Administradores (solo lectura)</p>
Administrar configuración global y directivas	<p>Vea y modifique las directivas globales y las opciones de la configuración, excepto los permisos y las funciones de administrador.</p>	<p>Administradores</p> <p>Configuración global y administradores de directivas</p>
Administrar sesiones globales	<p>Administre sesiones globales en un entorno de arquitectura Cloud Pod.</p>	<p>Administradores</p>
Administrar funciones y permisos	<p>Cree, modifique y elimine los permisos y las funciones de administrador.</p>	<p>Administradores</p>

Tabla 7-7. Privilegios globales (continuación)

Privilegio	Características del usuario	Funciones predefinidas
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
Administrar configuración de vCenter (solo lectura)	Acceso de solo lectura a la configuración de vCenter Server.	Administradores Administradores (solo lectura) Administradores de inventario Administradores de inventario (solo lectura) Administradores locales Administradores locales (solo lectura)

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 7-8. 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 operaciones de mantenimiento en granjas y escritorios automatizados	Recomponer, actualizar, reequilibrar, programar inserción de imagen, programar mantenimiento y cambiar la imagen predeterminada para una granja y un grupo de escritorios.	Grupo de escritorios, granja
Administrar máquina	Ejecutar operaciones relacionadas con todas las máquinas y sesiones.	Máquina
Administrar discos persistentes	Ejecutar todas las operaciones de discos persistentes de Horizon 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

Tabla 7-8. Privilegios específicos de objeto (continuación)

Privilegio	Características del usuario	Objeto
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 7-9. 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 grupos en Horizon Console.

La siguiente tabla muestra las tareas comunes para administrar grupos, así como los privilegios necesarios para realizar cada tarea.

Tabla 7-10. 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

Tabla 7-10. Privilegios y tareas para administrar los grupos (continuación)

Tarea	Privilegios necesarios
Agregar un grupo.	Administrar granjas y grupos de aplicaciones y escritorios Nota No se puede utilizar para agregar un grupo de escritorios sin administrar. El administrador también debe tener la función Configuración global y administradores de directivas (solo lectura) para realizar esta tarea.
Modificar o eliminar un grupo.	Administrar granjas y grupos de aplicaciones y escritorios Nota No se puede utilizar para eliminar un grupo de escritorios sin administrar. El administrador también debe tener la función Configuración global y administradores de directivas (solo lectura) para realizar esta tarea.
Agregar o eliminar escritorios de un grupo.	Administrar granjas y grupos de aplicaciones y escritorios Nota No se puede utilizar para agregar o eliminar escritorios virtuales sin administrar del grupo de escritorios. El administrador también debe tener la función Configuración global y administradores de directivas (solo lectura) para realizar esta tarea.
Actualizar, recomponer, volver a equilibrar o cambiar la imagen predeterminada de Horizon Console.	Administrar la imagen de grupo de escritorios Composer y Administrar configuración de vCenter (solo lectura).
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 máquinas en Horizon Console.

La siguiente tabla muestra tareas comunes para administrar máquinas, así como los privilegios necesarios para realizar cada tarea.

Tabla 7-11. Privilegios y tareas para administrar las máquinas

Tarea	Privilegios necesarios
Eliminar una máquina virtual.	Administrar máquina o Administrar granjas y grupos de aplicaciones y escritorios Nota No se puede utilizar para eliminar escritorios no administrados o hosts RDS del grupo de escritorios o de la granja. El administrador también debe tener la función Configuración global y administradores de directivas (solo lectura) para realizar esta tarea.
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

Tabla 7-11. Privilegios y tareas para administrar las máquinas (continuación)

Tarea	Privilegios necesarios
Activar el modo de mantenimiento o salir de él.	Administrar máquina
Desconectar o cerrar sesiones.	Administrar sesiones

Privilegios para administrar discos persistentes

Los administradores deben tener ciertos privilegios para administrar discos persistentes en Horizon Console.

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 Console.

Tabla 7-12. Privilegios y tareas para administrar los discos persistentes

Tarea	Privilegios necesarios
Desconectar un disco.	<ul style="list-style-type: none"> ■ Si el disco es un disco secundario, se requiere el privilegio Administrar discos persistentes. ■ Si es un disco principal, se requieren los privilegios Administrar discos persistentes y Administrar máquina. ■ Para desconectar cualquier disco en un almacén de datos diferente, el administrador también necesitará el privilegio Administrar configuración de vCenter (solo lectura).
Conectar un disco.	Administrar discos persistentes en el disco y Administrar máquina en la máquina.
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 escritorio y aplicaciones o Administrar máquina en el último grupo de escritorios.
Importar desde vCenter.	Administrar discos persistentes en el disco y Administrar configuración de vCenter (solo lectura) .
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 en Horizon Console.

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 Console y los administradores en la página **Vista de administradores globales** de Horizon Console.

Tabla 7-13. 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 Console.

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 7-14. 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
Poder iniciar sesión en Horizon Console.	Interacción de consola Nota A partir de la versión 7.10 de Horizon 7, el privilegio Interacción de consola se agrega automáticamente a las nuevas funciones y no aparece en la lista de privilegios globales de Horizon Console.
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

Tabla 7-14. Privilegios y tareas de Horizon Help Desk Tool (continuación)

Tareas	Privilegios necesarios
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 7-15. Privilegios para los comandos y las tareas de administración general

Tarea	Privilegios necesarios
Agregar o eliminar un grupo de acceso	Debe tener la función Administradores locales o Administradores en el grupo de acceso raíz para poder eliminar un grupo de acceso. Debe tener la función Administradores de inventario, Administradores locales o Administradores 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 Nota A partir de la versión 7.10 de Horizon 7, el privilegio Interacción directa se agrega automáticamente a las nuevas funciones y no se muestra en la lista de privilegios de Horizon Console.
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.
Acceso de solo lectura a la configuración de vCenter Server.	Administrar configuración de vCenter (solo lectura)

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. Delege 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.

Establecer directivas en Horizon Console

8

Horizon Console 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.

Este capítulo incluye los siguientes temas:

- [Configurar las directivas globales](#)

Configurar las directivas globales

Puede configurar directivas globales a fin de controlar el comportamiento de todos los usuarios de sesiones cliente.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Directivas globales**.

En el panel **Directivas globales** se muestran los ajustes que afectan a todas las sesiones de cliente, usuarios o grupos de escritorios.

Tabla 8-1. 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>

2 Haga clic en **Editar directivas** para cambiar la configuración.

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

Mantenimiento de los componentes de Horizon 7

9

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](#)
- [Restaurar los datos de configuración del servidor de conexión de Horizon y de Horizon Composer](#)
- [Exportar datos de la base de datos de Horizon Composer](#)
- [Supervisar los componentes de Horizon 7](#)
- [Comprender los servicios de Horizon 7](#)
- [Cambiar la clave de licencia o los modos de licencia del producto en Horizon Console](#)
- [Supervisar el uso del producto](#)
- [Participar en el Programa de mejora de la experiencia de cliente](#)
- [Integración del servidor de conexión de Horizon con Skyline Collector Appliance](#)

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 Horizon Composer, programe o ejecute copias de seguridad automáticas en Horizon Console. 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 Horizon 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 Horizon Composer

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

Horizon 7 almacena los datos de configuración del servidor de conexión en el repositorio de LDAP de View. Horizon Composer almacena datos de configuración para los escritorios de clones vinculados en la base de datos de Horizon Composer.

Cuando utiliza Horizon Console para realizar copias de seguridad, Horizon 7 realiza una copia de seguridad de los datos de configuración de LDAP de View y de la base de datos de Horizon 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" en el documento *Administración de Horizon 7*.

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 **Crear copia de seguridad ahora** en Horizon Console.
- 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 Horizon Console.

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 Horizon Composer, Horizon 7 realiza una copia de seguridad de todas las bases de datos de Horizon 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 Console, seleccione **Configuración > 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 **Crear copia de seguridad ahora**.
- 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 de Horizon Composer y del servidor de conexión en intervalos regulares. En Horizon Console, puede establecer la frecuencia y otros aspectos de las operaciones de la copia de seguridad.

Tabla 9-1. 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>
Hora de copia de seguridad	Hora a la que se programa la realización de una copia de seguridad.
Compensación de tiempo de copia de seguridad	Compensación de tiempo de de una copia de seguridad programada.
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 Horizon 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 Horizon Composer](#).

Restaurar los datos de configuración del servidor de conexión de Horizon y de Horizon Composer

Puede restaurar de forma manual los archivos de configuración LDAP del servidor de conexión y los archivos de la base de datos de Horizon Composer de los que Horizon 7 hizo las copias de seguridad.

Ejecute de forma manual utilidades separadas para restaurar el servidor de conexión y los datos de configuración de Horizon Composer.

Antes de restaurar los datos de configuración, compruebe que realizó una copia de seguridad de los datos de configuración en Horizon Console. Consulte [Realizar una copia de seguridad de los datos del servidor de conexión de Horizon y de Horizon 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 Horizon Composer desde los archivos de la copia de seguridad `.svi` a la base de datos SQL de Horizon 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 Console 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 Horizon 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 Para detener todas las instancias de Horizon Composer, detenga el servicio de Windows de VMware Horizon Composer en los servidores donde se ejecuta Horizon Composer.
- 2 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.
- 3 Instale una instancia del servidor de conexión.
- 4 Detenga el servicio Windows del servidor de conexión VMware Horizon para detener la instancia del servidor de conexión.
- 5 Haga clic en **Iniciar > Ventana del símbolo del sistema**.
- 6 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:
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.
- 7 Importe el archivo LDIF descifrado para restaurar la configuración LDAP de View.
Especifique la opción -f con el archivo LDIF descifrado. Por ejemplo:
- 8 Desinstale el servidor de conexión.
Desinstale solo el paquete del servidor de conexión de VMware Horizon.
- 9 Vuelva a instalar el servidor de conexión.
- 10 Inicie sesión en Horizon Console y compruebe que la configuración sea correcta.
- 11 Inicie las instancias de Horizon Composer.
- 12 Vuelva a instalar las instancias del servidor de réplica.

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 Horizon Composer, si se encuentra en uso. Si es necesario, restaure la configuración de Horizon Composer a partir de la copia de seguridad. Consulte [Restaurar una base de datos de Horizon Composer](#). Tras restaurar la configuración de Horizon 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 Horizon Composer.

Restaurar una base de datos de Horizon Composer

Puede importar los archivos de copia de seguridad de la configuración de Horizon Composer en la base de datos de Horizon Composer que almacena la información de clones vinculados.

Puede usar el comando `SviConfig restoredata` para restaurar los datos de la base de datos de Horizon Composer si se produce un error en el sistema o para revertir la configuración de Horizon Composer a un estado anterior.

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

Requisitos previos

Compruebe la ubicación de los archivos de copia de seguridad de la base de datos de Horizon 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 Horizon 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 Horizon 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 Horizon 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 Composer.
- 2 En el equipo en el que esté instalado el Horizon Composer, detenga el servicio de VMware Horizon Composer.
- 3 Abra una ventana de símbolo de sistema de Windows y diríjase al archivo ejecutable SviConfig.
El archivo se encuentra con la aplicación Horizon 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 -dsname=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 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 Horizon Console](#).

Códigos de resultado de la restauración de la base de datos de Horizon Console

Al restaurar una base de datos de Horizon Console, el comando SviConfig restoredata muestra un código de resultado.

Tabla 9-2. Códigos de resultado de restoredata

Código	Descripción
0	La operación finalizó correctamente.
1	No se encuentra el DSN proporcionado.
2	Se proporcionaron credenciales de administrador de la base de datos no válidas.
3	La unidad de la base de datos no es compatible.

Tabla 9-2. Códigos de resultado de restoredata (continuación)

Código	Descripción
4	Se produjo un problema inesperado y el comando no se completó.
14	Otra aplicación está utilizando el servicio de VMware Horizon Console. 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 de la base de datos de Horizon Composer

Puede exportar los datos desde la base de datos de Horizon Composer a un archivo.

Importante Use la utilidad SviConfig solo si es un administrador de Horizon 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 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 en el que esté instalado el Horizon Composer, detenga el servicio de VMware Horizon Composer.
- 2 Abra una ventana de símbolo de sistema de Windows y diríjase al archivo ejecutable SviConfig.

El archivo se encuentra con la aplicación Horizon Composer.

Horizon-Composer-installation-directory\sviconfig.exe

3 Ejecute el comando SviConfig exportdata.

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_ (DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_Horizon_Composer_output_file
```

Por ejemplo:

```
sviconfig -operation=exportdata -dsname=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 la exportación de la base de datos de Horizon Composer](#).

Códigos de resultado de la exportación de la base de datos de Horizon Composer

Al exportar una base de datos de Horizon Composer, el comando SviConfig exportdata muestra un código de salida.

Tabla 9-3. 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 consultar rápidamente el estado de los componentes de vSphere y Horizon 7 en la implementación de Horizon 7 a través del panel de Horizon Console.

Horizon Console muestra información de supervisión relativa a: instancias del servidor de conexión, base de datos de eventos, puertas de enlace, servicios de Horizon 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 Console muestra el estado de los dominios de Kerberos como desconocido aunque un dominio esté configurado y funcione.

Procedimiento

1 En Horizon Console, vaya a **Supervisar > Panel**.

2 En el panel **Estado del sistema**, haga clic en **Ver**.

El panel Detalles muestra el nombre, la versión y otra información relacionada con cada problema.

- Una marca de verificación verde indica que el componente no tiene ningún problema.
- Un signo de exclamación rojo indica que el componente no está disponible o no funciona.
- Un signo de exclamación amarillo indica que un componente presenta un estado de advertencia.
- Cuando el estado de un componente es desconocido, aparece un signo de interrogación.

3 Seleccione un problema para ver más información sobre él.

Opción	Descripción
Componentes	<p>Muestra información sobre los componentes de servicio.</p> <p>Haga clic en las pestañas Servidores de conexión, Servidores de puerta de enlace, Base de datos de eventos, Servidores View Composer o True SSO para ver información sobre los componentes de servicio y realizar tareas de solución de problemas.</p> <p>Seleccione un componente para realizar las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Ver el estado, el nombre, la versión y otros detalles. ■ Si selecciona un servidor de conexión, haga clic en la pestaña Ver el estado de los servicios para ver información sobre los servicios de la puerta de enlace. ■ Si selecciona un servidor de conexión, haga clic en la pestaña Ver detalles de las sesiones para ver información sobre las sesiones del servidor de conexión.
Granjas de RDS	<p>Muestra información sobre las granjas. Haga clic en un identificador de granja para ver más información sobre la granja, incluidos los hosts RDS que pertenecen a ella.</p>
vSphere	<p>Muestra información sobre los componentes relacionados con vSphere.</p> <p>Haga clic en las pestañas Almacenes de datos, Hosts ESX y vCenter Server para ver información sobre cada componente.</p>

Opción	Descripción
Otros componentes	<p>Haga clic en las pestañas Dominios, SAML 2.0 y Servicio de licencias para ver más información sobre cada componente. Esta sección también se aplica a Horizon Composer.</p> <p>Nota Si un autenticador SAML 2.0 tiene una advertencia debido a un certificado que no es de confianza, puede hacer clic en el vínculo del certificado para aceptarlo y validarlo.</p>
Pods remotos	<p>Muestra información sobre los pods de Horizon 7 remotos.</p> <p>Nota Esta sección solo aparece cuando la función Arquitectura Cloud Pod está habilitada.</p>

- En el panel **Sesiones**, puede ver los gráficos de barras que muestran el número de sesiones activas, desconectadas o inactivas de escritorios virtuales, escritorios publicados y aplicaciones publicadas.

- En el panel **Sesiones**, haga clic en **Ver** para ver las sesiones.

La página Sesiones muestra información sobre las sesiones.

- En el panel **Carga de trabajo**, haga clic en **Ver** para ver los almacenes de datos.

Puede seleccionar un almacén de datos para ver detalles adicionales, como el uso actual del almacén de datos. Horizon Console muestra una advertencia si el espacio libre de un almacén de datos está por debajo del valor de un umbral. Si hay grupos de escritorios relacionados con un almacén de datos seleccionado, podrá ver la información de los grupos de escritorios cuando seleccione el almacén de datos. La columna **Otros almacenes de datos** muestra información de las granjas o los grupos de escritorios que abarcan varios almacenes de datos.

Supervisar el estado de carga del servidor de conexión de Horizon

Puede supervisar la carga de un servidor de conexión en el panel de Horizon Console. Para cada servidor de conexión, puede ver el porcentaje de CPU y memoria consumidas, el número de sesiones de protocolo de visualización, las sesiones de conexión del servidor de conexión o el número máximo de sesiones que pueden conectarse a un servidor de conexión. También puede ver el número de sesiones conectadas para un host RDS.

Procedimiento

- En Horizon Console, vaya a **Supervisar > Panel**.

- 2 En el panel **Estado del sistema**, haga clic en **Ver**.

En el panel **Componentes**, en la pestaña **Servidores de conexión**, la columna **Sesiones** muestra el porcentaje de sesiones de cada servidor de conexión. La columna **Consumo de CPU** muestra el porcentaje de CPU consumida en cada servidor de conexión. La columna **Consumo de memoria** muestra el porcentaje de memoria consumida en cada servidor de conexión.

Nota Si el servidor de conexión no está configurado con una conexión de puerta de enlace segura con el túnel seguro HTTP(s), la puerta de enlace segura PCoIP y conexiones de puerta de enlace segura Blast, Horizon Console no mostrará un porcentaje de sesiones de servidor de conexión, sino el número de sesiones de servidor de conexión.

- 3 Seleccione un servidor de conexión y haga clic en **Ver detalles de las sesiones** para ver las sesiones de servidor de conexión, el número máximo de sesiones de servidor de conexión y las sesiones de protocolo de visualización.

Nota Si el servidor de conexión no está configurado con una conexión de puerta de enlace segura con el túnel seguro HTTP(s), la puerta de enlace segura PCoIP y conexiones de puerta de enlace segura Blast, Horizon Console no mostrará el número máximo de sesiones porque no existirá un límite máximo de sesiones que se pueden conectar al servidor de conexión.

- 4 Para ver el número de sesiones en un host RDS, en el panel **Componentes**, haga clic en **Granjas RDS** y, a continuación, en el identificador de una granja.

La columna Sesiones muestra el número de sesiones en un host RDS.

Supervisar servicios en el servidor de conexión de Horizon

Puede supervisar los componentes del servicio de puerta de enlace que se ejecutan en un servidor de conexión en el panel de Horizon Console. Los componentes del servicio de puerta de enlace incluyen una conexión de puerta de enlace segura configurada con túnel seguro HTTP(s), puerta de enlace PCoIP y conexiones de puerta de enlace segura Blast.

Procedimiento

- 1 En Horizon Console, vaya a **Supervisar > Panel**.
- 2 En el panel **Estado del sistema**, haga clic en **Ver**.
- 3 Seleccione un servidor de conexión y, a continuación, seleccione **Ver el estado de los servicios**.

El cuadro de diálogo **Estado de los servicios de puerta de enlace** muestra el estado de los componentes del servicio de puerta de enlace y el servicio de puerta de enlace en uso.

Nota Los componentes del servicio que no estén habilitados aparecerán atenuados.

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 9-4. 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.
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 9-5. 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 o los modos de licencia del producto en Horizon Console

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 Console para cambiar la clave de licencia del producto. Según cómo esté implementado Horizon 7 en VMware Horizon Cloud Service, puede obtener una licencia permanente o una licencia de suscripción para Horizon 7. Puede usar Horizon Console para cambiar el modo de licencia de una licencia de suscripción a una licencia permanente y viceversa para un pod.

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 Horizon Composer y las aplicaciones publicadas, obtenga una clave de licencia del producto válida.
- Para utilizar una licencia de suscripción, compruebe que haya configurado Horizon 7 para que pueda utilizarse con una licencia de suscripción. Consulte el documento *Instalación de Horizon 7*. En el panel **Licencia** se muestra información sobre la licencia de suscripción del pod de Horizon 7.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Licencia y uso del producto**.

El primer y los últimos cinco caracteres de la clave de licencia actual aparecen en el panel **Licencia**.

- 2 Para editar la clave de licencia, haga clic en **Editar licencia**, introduzca el número de serie de la licencia y haga clic en **Aceptar**.

En el panel **Configuración de licencias** se muestra la información actualizada de la licencia.

- 3 (opcional) Para cambiar de una licencia de suscripción a una licencia permanente para un pod de Horizon 7, haga clic en **Utilizar licencia permanente** y haga clic en **Aceptar**.

En el panel **Configuración de licencias** se muestra la información actualizada de la licencia.

- 4 (opcional) Para cambiar de una licencia perpetua a una licencia de suscripción para un pod de Horizon 7, haga clic en **Utilizar licencia de suscripción** y haga clic en **Aceptar**. El administrador de VMware Horizon Cloud Service puede habilitar el pod de Horizon 7 para que admita una licencia de suscripción.

En el panel **Configuración de licencias** se muestra la información actualizada de la licencia.

- 5 Verifique la fecha de caducidad de la licencia.

- 6 Verifique que las licencias de Horizon 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>.

- 7 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 el uso del producto

En Horizon Console, puede supervisar los usuarios activos que están conectados a Horizon 7 en ese momento. El panel **Configuración de uso** 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 7 proporciona dos modelos de uso de la licencia, uno para los usuarios designados y otro para los usuarios simultáneos. Horizon 7 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 7 cuenta el número de usuarios únicos que accedieron al entorno de Horizon 7. 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** del panel **Configuración de uso** muestra el número de usuarios desde que la implementación de Horizon 7 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 7 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** del panel **Configuración de uso** muestra el número más elevado de usuarios de aplicaciones y escritorios publicados y las sesiones de escritorios simultáneos desde que la implementación de Horizon 7 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

En Horizon Console, 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 el uso del producto](#).

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > 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**.

Participar en el Programa de mejora de la experiencia de cliente

Puede configurar Horizon 7 para unirse al Programa de mejora de la experiencia de cliente de VMware (CEIP).

Para obtener información sobre el tipo de datos que VMware recopila a través del CEIP y sobre cómo utiliza VMware esos datos, consulte el centro de seguridad y confianza en <http://www.vmware.com/trustvmware/ceip.html>.

Para configurar el uso compartido de datos en Horizon Client, consulte la guía de instalación y configuración de Horizon Client correspondiente. Por ejemplo, para los clientes Windows, consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*. Para configurar el uso compartido de datos en HTML Access, consulte el documento *Guía de instalación y configuración de VMware Horizon HTML Access*.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Licencia y uso del producto**.
- 2 Seleccione la pestaña **Programa de experiencia del cliente** y haga clic en **Editar configuración**.
- 3 Para unirse al CEIP, seleccione **Participar en el Programa de mejora de la experiencia de cliente de VMware**.
Si no selecciona esta opción, no se unirá al CEIP.
- 4 (opcional) Seleccione la ubicación geográfica, el seguimiento vertical del negocio o el número de empleados de la organización.
- 5 Haga clic en **Aceptar**.

Integración del servidor de conexión de Horizon con Skyline Collector Appliance

Puede configurar el servidor de conexión de Horizon para que se integre con Skyline Collector Appliance, que utiliza el servicio de soporte técnico de VMware para diagnosticar y resolver problemas de Horizon 7.

Skyline Collector Appliance extrae los registros del servidor de conexión correspondientes al usuario administrador de Horizon 7 configurado para la recopilación de registros.

Procedimiento

- 1 En Horizon Console, cree una función personalizada denominada Administradores del recopilador de registros con el privilegio de recopilar registros de operaciones. Consulte [Agregar una función personalizada en Horizon Console](#).
- 2 Agregue una descripción para la función personalizada.
- 3 Agregue un nuevo usuario administrador y seleccione la función de administrador de inventario (solo lectura) y la función personalizada Administradores del recopilador de registros para el usuario.

Skyline Collector Appliance podrá extraer los registros del servidor de conexión de este usuario administrador para diagnosticar y resolver problemas de Horizon 7.

Primeros pasos con JMP Integrated Workflow

10

Familiarícese con los conceptos avanzados de JMP Integrated Workflow y finalice las tareas necesarias para empezar a usar las funciones de JMP Integrated Workflow.

Este capítulo incluye los siguientes temas:

- [Acerca de JMP Integrated Workflow](#)
- [Empezar a utilizar JMP Integrated Workflow](#)

Acerca de JMP Integrated Workflow

Las funciones de VMware HorizonJMP (Just-in-Time Management Platform) Integrated Workflow permiten utilizar una sola consola para definir y administrar espacios de trabajo de escritorio para usuarios o grupos de usuarios.

Para crear un espacio de trabajo de escritorio, defina una asignación JMP que incluya información sobre los grupos de escritorios de VMware Horizon, AppStacks de VMware App Volumes y la configuración de VMware Dynamic Environment Manager. Una vez enviada la asignación de JMP, el motor de automatización de JMP se comunica con los sistemas Horizon 7, App Volumes y Dynamic Environment Manager para autorizar al usuario para un escritorio.

Puede administrar las asignaciones JMP mediante la pestaña **Asignaciones (JMP)** de Horizon Console. También puede modificar la asignación de cada componente mediante la respectiva consola del componente JMP. Por ejemplo, también puede modificar los cambios realizados en los grupos de escritorio definidos en una asignación JMP si selecciona **Inventario > Escritorios** en Horizon Console.

Cuando se abre una asignación JMP en Horizon Console, el estado actual de cada componente de la asignación JMP se valida para garantizar que su estado es el correcto. Cuando se identifican diferencias, las áreas afectadas se resaltan en la consola y puede aceptar el estado actual, o bien modificar la asignación para conseguir el estado que desee y volver a autorizar al usuario.

Las funciones de JMP Integrated Workflow pasan a estar disponibles en Horizon Console después de instalar y configurar VMware HorizonJMP Server. Consulte [Empezar a utilizar JMP Integrated Workflow](#) y *Guía de instalación y configuración de VMware Horizon JMP Server* para obtener más información.

Nota Las funciones de JMP Integrated Workflow no admiten VMware Cloud[®] on AWS ya que App Volumes no admite VMware Cloud.

Empezar a utilizar JMP Integrated Workflow

Para comenzar a usar las funciones de JMP Integrated Workflow, debe instalar y configurar JMP Server, y establecer las opciones de JMP.

Requisitos previos

Revise los requisitos y los requisitos del sistema de todos los componentes tecnológicos que piensa instalar.

Procedimiento

- 1 Si es necesario, configure los grupos y usuarios administradores necesarios en Active Directory.
Consulte "Preparar Active Directory" en el documento *Instalación de Horizon 7*. Es necesaria la información de Active Directory al configurar las opciones de JMP.
- 2 Configure Microsoft SQL Server y asegúrese de que se crearon las credenciales de inicio de sesión que piensa usar durante el proceso de instalación de JMP Server. Consulte "Requisitos de base de datos para JMP Server" en el documento *Guía de instalación y configuración de VMware Horizon JMP Server* para obtener más información.
- 3 Instale y configure VMware Horizon 7 versión 7.5 o posterior.
Consulte el documento *Instalación de Horizon 7*.
- 4 (Opcional) Instale y configure VMware App Volumes 2.14 o una versión posterior, que proporciona funciones para la distribución de aplicaciones en tiempo real.
Consulte el documento *Guía de instalación de VMware App Volumes* para obtener más información.
- 5 (Opcional) Para proporcionar administración de directivas en contexto, instale y configure VMware Dynamic Environment Manager 9.2.1 o una versión posterior.
Consulte el documento *Instalar y configurar VMware Dynamic Environment Manager*.
- 6 Obtenga los certificados SSL firmados por la CA que se debe usar para que JMP Server se comunique de forma segura con otros servidores dentro de la red de su organización.
- 7 Instale JMP Server y configure los certificados SSL para que JMP Server se comunique con otros servidores necesarios para usar funciones de JMP Integrated Workflow.
Consulte *Guía de instalación y configuración de VMware Horizon JMP Server* para obtener más información.
- 8 Configure las opciones de JMP por primera vez. Consulte [Configurar las opciones de JMP por primera vez](#) para obtener más detalles.

Pasos siguientes

Tras completar correctamente las tarea anteriores, ya puede crear una asignación de JMP. Para obtener más información, consulte [Crear una asignación JMP](#).

Administrar la configuración de JMP

11

Tras instalar JMP Server, debe configurar las opciones de JMP con las credenciales necesarias para poder crear cualquier asignación JMP y comenzar a usar las funciones de JMP Integrated Workflow. Puede editar la configuración inicial de JMP y, cuando corresponda, agregar nueva información de configuración.

Este capítulo incluye los siguientes temas:

- [Configurar las opciones de JMP por primera vez](#)
- [Administrar la configuración de JMP](#)

Configurar las opciones de JMP por primera vez

Para poder crear las asignación JMP, primero debe configurar las opciones de JMP mediante Horizon Console. Debe proporcionar las credenciales del dominio de Active Directory que utilice para asignar espacios de trabajo de escritorio a los usuarios o grupos de usuarios. También puede incluir la información de credenciales para utilizar App Volumes AppStacks y el recurso compartido de configuración de Dynamic Environment Manager cuando cree asignaciones JMP.

Requisitos previos

- Compruebe que VMware Horizon JMP Server se instaló correctamente y que dispone de su dirección URL. Consulte *Guía de instalación y configuración de VMware Horizon JMP Server* para obtener más información.
- Obtenga las credenciales de cuenta de administrador para la versión 7.5 o posterior de Horizon 7 que utilizará con JMP Server.
- Obtenga las credenciales de Active Directory que se deben utilizar con JMP Server.
- Si está asignando aplicaciones a las asignación JMP, asegúrese de que cuenta con la URL y las credenciales de cuenta de administrador para la instancia de VMware App Volumes Manager que se utilizará. Si un equilibrador de carga administra las instancias de App Volumes Manager que desea utilizar, obtenga la dirección URL de dicho equilibrador de carga y utilícela cuando configure la información de App Volumes Manager.
- Si decide utilizar un recurso compartido de configuración de VMware Dynamic Environment Manager, obtenga su ruta UNC y las credenciales de cuenta de administrador necesarias para acceder a él.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.

- 2 Introduzca la información de JMP Server.

- a En la pestaña **JMP Server**, haga clic en **Agregar JMP Server**.
- b Introduzca la URL de JMP Server con el formato `https://jmp.yourcompany.com`.
- c Haga clic en **Guardar**.

La dirección URL de JMP Server está válida. Si recibió el mensaje JMP Server no está accesible, compruebe que introdujo la dirección URL correcta, que JMP Server esté configurado correctamente y que JMP Server sea accesible.

- 3 Introduzca la información de cuenta para la versión 7.5 o posterior del servidor de conexión de Horizon 7 que desea utilizar con JMP Server.

- a Haga clic en la pestaña **Horizon 7**.
- b Si no se rellena automáticamente, introduzca el valor de **URL del servidor de conexión**. Esta dirección URL es la misma que la del servidor de conexión de Horizon 7 al que Horizon Console se conectó.
- c Introduzca su nombre de usuario y contraseña de la cuenta de servicio de Horizon 7.
- d En el cuadro de texto **Dominio de la cuenta de servicio**, introduzca un nombre válido para utilizar con las asignaciones JMP que está creando y pulse **Intro**.
- e Haga clic en **Guardar**.

- 4 Introduzca la información del Active Directory que desea utilizar con las asignación JMP.

- a Haga clic en la pestaña **Active Directory**.
- b Haga clic en **Nuevo**.
- c En el cuadro de texto **Nombre de NETBIOS**, realice su selección en la lista de nombres de dominio disponibles de NetBIOS.

Los cuadros de texto Nombre de dominio DNS y Contexto se actualizan con los valores predeterminados.

- d Compruebe que el valor predeterminado que se agregó en el cuadro de texto **Nombre de dominio DNS** es el valor que se debe utilizar. También puede introducir otro nombre de dominio completo de Active Directory. Por ejemplo, `mycompany.com`.
- e En la sección **Protocolo**, seleccione el protocolo que Active Directory utiliza.
- f En los cuadros de texto **Nombre de usuario de enlace** y **Contraseña de enlace**, introduzca las credenciales de la cuenta de usuario Nombre distintivo de enlace (DN). Por ejemplo, **administrador**.

- g Modifique el valor en el cuadro de texto **Contexto** si desea utilizar un valor distinto al predeterminado.

El valor se utiliza como raíz de la búsqueda de datos de Active Directory.

- h (Opcional) Haga clic en **Propiedades avanzadas** y modifique el valor del número de puerto predeterminado.

El valor del puerto predeterminado se basa en el protocolo que seleccionó anteriormente. Puede modificar el valor del puerto o bien dejar el cuadro de texto en blanco.

- i En el cuadro de texto **Controlador de dominio**, también puede introducir uno o varios nombres de host o direcciones IP que le ayuden a administrar el tráfico de Active Directory.

Por ejemplo, `adserver.mycompany.com`, `10.111.XXX.XXX`. Si el cuadro de texto se deja en blanco, se utilizará el valor del cuadro de texto **Nombre de dominio DNS**.

- j Haga clic en **Guardar**.

5 Si desea utilizar App Volumes AppStacks para crear asignaciones JMP, configure la instancia de App Volumes Manager que va a utilizar.

- a Haga clic en la pestaña **App Volumes**.

- b Haga clic en **Nuevo**.

- c En el cuadro de texto **Nombre**, escriba un nombre para asignar a la instancia de App Volumes. Si deja el cuadro de texto en blanco, se utilizará el valor que introduzca en el cuadro de texto **URL del servidor de App Volumes**.

- d Introduzca una dirección URL válida para la instancia de App Volumes Manager que desea que el pod de JMP Server asocie.

Importante Si un equilibrador de carga administra la instancia de App Volumes Manager que desea utilizar, introduzca la URL de dicho equilibrador de carga.

- e Introduzca las credenciales de cuenta del administrador del equilibrador de carga o de App Volumes Manager que JMP Server puede utilizar para acceder a App Volumes Manager.

- f Introduzca el nombre de dominio de la cuenta de servicio de App Volumes Manager que se utilizará para las asignaciones JMP.

- g (Opcional) Si desea registrar más de una instancia de App Volumes Manager, utilice el botón de alternancia para indicar si la instancia de App Volumes Manager que está agregando es el servidor predeterminado que se utilizará al crear asignación JMP. Puede cambiar la instancia que desea utilizar en el momento en el que se está creando una asignación de JMP.

- h Haga clic en **Guardar**.

6 Si desea utilizar un recurso compartido de configuración de Dynamic Environment Manager al crear asignación JMP, agregue la información relacionada a la configuración de JMP.

- a Haga clic en la pestaña **UEM**.

- b Haga clic en **Nuevo**.

- c Introduzca un valor en el cuadro de texto **Ruta UNC del recurso compartido de archivos** con el formato `\\fileserver-name\UEM-configuration-share-pathname`. Por ejemplo, `\FileServer\UEMConfig`.

Importante No incluya General en la ruta UNC del recurso compartido de archivos que introduzca.

- d Introduzca las credenciales de cuenta de administrador de Dynamic Environment Manager que utilizará para conectarse al recurso compartido de configuración de Dynamic Environment Manager.
- e En la lista de **Active Directory**, seleccione el nombre de dominio que se usará con el recurso compartido de configuración de Dynamic Environment Manager.

Nota Un Active Directory puede asociarse únicamente con un recurso compartido de configuración de Dynamic Environment Manager.

- f Haga clic en **Guardar**.

Pasos siguientes

Tras configurar correctamente los valores iniciales de JMP, podrá crear las asignaciones JMP. Consulte [Crear una asignación JMP](#) para obtener más información.

Administrar la configuración de JMP

Puede utilizar Horizon Console para modificar, agregar o eliminar información para una opción de JMP.

- Debe contar con la información necesaria para modificar la opción específica de JMP.
- Para modificar la Configuración de JMP, asegúrese de contar con los privilegios administrativos adecuados.

Editar configuración de JMP Server

Horizon Console permite realizar cambios en la configuración de JMP Server.

Requisitos previos

- Debe contar con la información necesaria para modificar la configuración específica de JMP Server.
- Verifique que tenga los privilegios administrativos adecuados para iniciar sesión en Horizon Console y modificar la configuración de JMP Server

Procedimiento

- 1 En Horizon Console, seleccione **Configuración de JMP**.
- 2 En el panel Configuración de JMP, haga clic en la pestaña **JMP Server**.
- 3 Haga clic en **Editar**.
- 4 Introduzca una nueva **URL de JMP Server**.

5 Haga clic en **Guardar**.

La nueva URL de JMP Server se validará y, si no se consigue, aparecerá un mensaje de error.

Editar credenciales de Horizon 7

Horizon Console permite realizar cambios en las credenciales del servidor de conexión de Horizon 7.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **Horizon 7**.
- 3 Haga clic en **Editar credenciales**.
- 4 Introduzca un nuevo nombre de usuario en **Nombre de usuario de la cuenta del servicio**, si es necesario.
- 5 Introduzca una nueva contraseña en **Contraseña de la cuenta del servicio**, si es necesario.
- 6 Cambie el valor de **Dominio de la cuenta del servicio**, si es necesario.
- 7 Haga clic en **Guardar**.

Editar la URL del servidor de conexión de Horizon

Si desea asociar las asignaciones JMP a otra instancia de Horizon Connection Server, debe modificar la URL de Horizon Connection Server que está registrada con la configuración de JMP Server asociada a dichas asignaciones JMP.

No hay ninguna interfaz de usuario en Horizon Console que le permite modificar la información de Horizon Connection Server. SQL Server Management Studio permite modificar la URL del host de Horizon Connection Server en la configuración de JMP.

Requisitos previos

- Verifique que tenga los privilegios administrativos adecuados para iniciar sesión en una sesión de SQL Server Management Studio y acceder a la base de datos de SQL Server que creó para JMP Server.
- Haga una copia de seguridad de la base de datos de SQL Server antes de continuar con las modificaciones de la base de datos.

Procedimiento

- 1 Si inició sesión en Horizon Console, ciérrela.
- 2 Inicie una sesión de SQL Server Management Studio como administrador del sistema (SA) o mediante una cuenta con privilegios SA.

- 3 Compruebe que la URL del host de Horizon Connection Server de reemplazo que desea utilizar no esté ya registrada en otra instancia de JMP Server.

Por ejemplo, si la URL del host de Horizon Connection Server de reemplazo es new-horizon-host.com, la siguiente instrucción SQL permite comprobar que no esté ya registrada.

```
SELECT * from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 4 Si la instrucción SQL anterior no devolvió ningún resultado, continúe con el paso siguiente. En caso contrario, utilice la siguiente instrucción para eliminar la información del host de Horizon Connection Server existente.

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 5 Actualice la configuración de JMP Server mediante las siguientes instrucciones, donde new-horizon-server-host.com es la URL del host de Horizon Connection Server de reemplazo y old-horizon-host.com es la URL del host de Horizon Connection Server registrado.

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

- 6 Inicie sesión en Horizon Console mediante la nueva URL de Horizon Connection Server y compruebe que el nuevo host de Horizon Connection Server esté ahora asociado a las asignaciones JMP que se asociaron previamente al host anterior de Horizon Connection Server.

Agregar dominios de Active Directory

Si necesita agregar otro dominio de Active Directory después de la configuración inicial, utilice Horizon Console.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **Active Directory** y, a continuación, en **Agregar**.
- 3 En el cuadro de texto **Nombre de NETBIOS**, realice su selección en la lista de nombres de dominio disponibles de NetBIOS.

Los cuadros de texto Nombre de dominio DNS y Contexto se actualizan con los valores predeterminados.

- 4 En el campo de texto **Nombre de dominio DNS**, compruebe el valor predeterminado agregado tras actualizar el Nombre de NETBIOS. También puede introducir otro nombre de dominio completo de Active Directory. Por ejemplo, mycompany.com.
- 5 En la sección **Protocolo**, seleccione el protocolo que Active Directory utiliza.
- 6 En los campos de texto **Nombre de usuario de enlace** y **Contraseña de enlace**, introduzca las credenciales de la cuenta de usuario Nombre distintivo de enlace (DN), por ejemplo Administrador.
- 7 Modifique el valor en el campo de texto **Contexto** si desea utilizar un valor distinto al predeterminado.
- 8 (Opcional) Haga clic en **Propiedades avanzadas** y modifique el valor del número de puerto predeterminado.

El valor del puerto predeterminado se basa en el protocolo que seleccionó anteriormente. Puede modificar el valor del puerto o bien dejar el campo de texto en blanco.
- 9 En el campo de texto **Controlador de dominio**, también puede introducir uno o varios nombres de host o direcciones IP que le ayuden a gestionar el tráfico de Active Directory.
- 10 Haga clic en **Guardar**.

La información sobre el dominio de Active Directory recién agregado aparece en la tabla de Active Directory.

Editar la información de dominio de Active Directory

Si alguna información cambió desde que inicialmente configurara las opciones de JMP, Horizon Console permite modificar la información de configuración de dominio de Active Directory.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **Active Directory**.
- 3 Seleccione una de las filas en la tabla de dominios de Active Directory y haga clic en **Editar**.
- 4 Modifique la información de Active Directory que debe actualizarse.
- 5 Haga clic en **Guardar**.

Eliminar la información de dominio de Active Directory

Horizon Console permite eliminar la información existente de la configuración de dominio de Active Directory (AD).

Solo puede eliminar información sobre un dominio registrado de Active Directory de una configuración de JMP si ninguna de las asignaciones JMP está utilizando dicho dominio.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.

- 2 Haga clic en la pestaña **Active Directory**.
- 3 Seleccione la fila de la tabla del dominio de Active Directory que desea eliminar de la configuración de JMP.
- 4 En el cuadro de diálogo de confirmación de eliminación que aparece, lea el mensaje y haga clic en **Eliminar** para confirmar que desea eliminar esta información de dominio de Active Directory.

Si no hay ninguna asignación JMP que esté utilizando el dominio de Active Directory, la información se eliminará.

Si hay alguna asignación JMP que esté utilizando el dominio de Active Directory, aparecerá un cuadro de diálogo de advertencia. El mensaje de advertencia incluye la lista de asignaciones JMP que están utilizando el dominio de Active Directory. Solo puede eliminar la información de dominio si previamente la borró de las asignaciones JMP o eliminó las asignaciones JMP que la utilizan.

Agregar información de App Volumes

Horizon Console permite agregar información para las instancias adicionales de App Volumes Manager que se puede utilizar al crear asignaciones JMP.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **App Volumes** y, a continuación, en **Agregar**.
Aparecerá el cuadro de diálogo **Agregar instancia de App Volumes**.
- 3 En el cuadro de texto **Nombre**, escriba un nombre único para asignar a la instancia de App Volumes. Si deja el cuadro de texto en blanco, se utilizará el valor que introduzca en el cuadro de texto **URL del servidor de App Volumes**.
- 4 En el cuadro de texto **URL del servidor de App Volumes**, introduzca una URL válida para la instancia de App Volumes Manager que desea asociar a JMP Server. Si un equilibrador de carga administra la instancia de App Volumes Manager que desea agregar, introduzca la URL de dicho equilibrador de carga.

Nota Si las instancias de App Volumes Manager que agregó están conectadas a distintas bases de datos SQL, la información sobre la instancia de App Volumes Manager que agregue aparecerá en la pestaña App Volumes. Si las instancias de App Volumes Manager están conectadas a la misma base de datos SQL, solo se mostrará en la pestaña App Volumes la información sobre el App Volumes Manager registrado anteriormente.

- 5 Introduzca el nombre de usuario y la contraseña de administrador de App Volumes que JMP Server puede utilizar para acceder a App Volumes Manager.
- 6 Introduzca el nombre de dominio de la cuenta de servicio de App Volumes que se utiliza para las asignaciones JMP.

- 7 Para hacer que la instancia de App Volumes Manager que está agregando sea el servidor predeterminado de App Volumes Manager que se utilizará para crear asignaciones JMP, haga clic en el botón de alternancia. Puede cambiar el servidor que desee utilizar en el momento en el que se está creando una asignación JMP.

El botón de alternancia cambia a color azul con una etiqueta **Sí**.

- 8 Haga clic en **Guardar**.

Editar la información de la instancia de App Volumes

Si necesita modificar la información sobre la instancia de App Volumes que las asignaciones JMP están utilizando, Horizon Console le permitirá modificar la información.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **App Volumes** y seleccione la fila de la tabla de la instancia de App Volumes que desea modificar.
- 3 Haga clic en **Editar**.
Aparecerá el cuadro de diálogo **Agregar instancia de App Volumes**.
- 4 Modifique la información de la instancia de App Volumes que debe actualizarse.
- 5 Haga clic en **Guardar**.

Eliminar información de la instancia de App Volumes

Horizon Console permite eliminar la información de configuración existente sobre una instancia de App Volumes.

Solo puede eliminar información sobre una instancia registrada de App Volumes de una configuración de JMP si ninguna de las asignaciones JMP está utilizando dicha instancia.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **App Volumes**.
- 3 Seleccione la fila de la información de la instancia de App Volumes que desee eliminar de la configuración de JMP.
- 4 Haga clic en **Eliminar** para confirmar que desea eliminar esta información sobre la instancia de App Volumes.

Si no hay ninguna asignación JMP que utilice la instancia de App Volumes, la información se eliminará.

Si hay alguna asignación JMP que esté utilizando la instancia de App Volumes, aparecerá un cuadro de diálogo de advertencia. El mensaje de advertencia incluye la lista de asignaciones JMP que están utilizando la instancia de App Volumes. Solo puede eliminar la información de la instancia de App Volumes si previamente la borró de las asignaciones JMP o eliminó las asignaciones JMP que la utilizan.

Agregar información sobre el recurso compartido de configuración de Dynamic Environment Manager

Horizon Console permite agregar otro recurso compartido de configuración de Dynamic Environment Manager tras la configuración inicial.

Solo puede agregar un recurso compartido de configuración de Dynamic Environment Manager por dominio de AD. Por lo tanto, el recurso compartido de configuración que está a punto de agregar no puede tener la misma dirección IP ni DNS que los recursos compartidos de configuración que ya están incluidos en la configuración del servidor JMP.

Procedimiento

1 En Horizon Console, haga clic en **Configuración de JMP**.

2 Haga clic en la pestaña **UEM** y, después, en **Agregar**.

Aparecerá el cuadro de diálogo **Agregar recurso compartido de archivos de UEM**.

3 Introduzca un valor en el cuadro de texto **Ruta UNC del recurso compartido de archivos** con el formato `\\server-name\UEM-configuration-share-pathname`.

Por ejemplo, si la ubicación compartida de la configuración es `\\<dirección-IP>\uemshare\config\general\FlexRepository\..`, la ruta que debe escribir en el cuadro de texto **Ruta UNC del recurso compartido de archivos** es `\\<dirección-IP>\uemshare\config`.

4 Introduzca el nombre de usuario y la contraseña de Dynamic Environment Manager que se deben utilizar para conectarse al recurso compartido de archivo de configuración de Dynamic Environment Manager.

5 En la lista de **Active Directory**, seleccione el nombre de dominio que se deberá utilizar con el recurso compartido de archivo de configuración de Dynamic Environment Manager.

Nota Un Active Directory solo puede asociarse con un recurso compartido de archivo de configuración de Dynamic Environment Manager.

6 Haga clic en **Guardar**.

La información sobre el recurso compartido de archivo de configuración de Dynamic Environment Manager se agrega a la configuración de JMP y, así mismo, se agrega una nueva fila a la tabla en la pestaña **UEM**.

Edita la información de recurso compartido del archivo de configuración de Dynamic Environment Manager

Horizon Console permite modificar la información existente sobre el recurso compartido del archivo de configuración de Dynamic Environment Manager que las asignaciones JMP están utilizando.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **UEM** y en la tabla de información, seleccione la fila del recurso compartido de configuración de Dynamic Environment Manager que desea modificar.
- 3 Haga clic en **Editar**.
Aparecerá el cuadro de diálogo **Editar el recurso compartido de archivos de UEM**.
- 4 Modifique la información del recurso compartido del archivo de configuración de Dynamic Environment Manager que tiene que actualizarse.
- 5 Haga clic en **Guardar**.

Eliminar la información de un recurso compartido de configuración de Dynamic Environment Manager

Horizon Console permite eliminar la información de configuración existente sobre un recurso compartido de configuración de Dynamic Environment Manager.

Solo puede eliminar información sobre un recurso compartido de configuración de Dynamic Environment Manager de una configuración de JMP si ninguna de las asignaciones JMP está utilizando dicho recurso compartido de configuración.

Procedimiento

- 1 En Horizon Console, haga clic en **Configuración de JMP**.
- 2 Haga clic en la pestaña **UEM**.
- 3 Seleccione la fila de la información del recurso compartido de configuración de Dynamic Environment Manager que desee eliminar de la configuración de JMP.
- 4 Haga clic en **Eliminar** para confirmar que desea eliminar esta información del recurso compartido de configuración de Dynamic Environment Manager.

Si no hay ninguna asignación JMP que utilice el recurso compartido de configuración de Dynamic Environment Manager, la información se eliminará.

Si hay alguna asignación JMP que esté utilizando el recurso compartido de configuración de Dynamic Environment Manager, aparecerá un cuadro de diálogo de advertencia. El mensaje de advertencia incluye la lista de asignaciones JMP que están utilizando el recurso compartido de configuración de Dynamic Environment Manager. Solo puede eliminar la información del recurso compartido de configuración de Dynamic Environment Manager si previamente la borró de las asignaciones JMP o eliminó las asignaciones JMP que la utilizan.

Administrar asignaciones JMP

12

Tras instalar JMP Server y configurar los ajustes de JMP, puede empezar a utilizar las funciones de JMP Integrated Workflow para crear, modificar, duplicar o eliminar asignaciones JMP.

En primer lugar debe instalar JMP Server y configurar las opciones de JMP antes de comenzar a crear asignaciones JMP. Consulte *Guía de instalación y configuración de VMware Horizon JMP Server* y [Configurar las opciones de JMP por primera vez](#) para obtener más información.

Asegúrese de que se cumplan los siguientes requisitos antes de crear, editar, duplicar o eliminar asignaciones JMP.

- Compruebe que la instancia de Horizon 7 que está registrada con la opción JMP esté en funcionamiento.
- Asegúrese de que haya, al menos, un dominio de Active Directory registrado con la opción JMP.
- Compruebe que la instancia de App Volumes que registró con la opción JMP está en funcionamiento.
- Compruebe que el recurso compartido de la configuración Dynamic Environment Manager definido en la opción JMP está en funcionamiento.

Nota No se admiten las autorizaciones globales.

Cuando intente crear, editar, duplicar o eliminar una asignación JMP, es posible que reciba un mensaje que indica que la acción no se completó correctamente. Por ejemplo, se pueden encontrar problemas al intentar alcanzar uno de los componentes de la tecnología JMP subyacente y la validación de la asignación no pueda completarse correctamente. En la pantalla de resumen de la asignación JMP, puede intentar solucionar el problema si selecciona una de las siguientes opciones.

- Haga clic en **Editar** para corregir los problemas de forma manual.
- Haga clic en **Reparar** para que JMP Server intente solucionar los problemas que encuentre en la asignación JMP actual.
- Haga clic en **Forzar eliminación** para eliminar por completo la asignación JMP.

Este capítulo incluye los siguientes temas:

- [Crear una asignación JMP](#)
- [Editar una asignación JMP](#)
- [Duplicar una asignación JMP](#)

■ [Eliminar una asignación JMP](#)

Crear una asignación JMP

Horizon Console permite crear asignaciones JMP, que se utilizan para crear espacios de trabajo de escritorio para usuarios o grupos de usuarios.

Para definir la asignación JMP, seleccione los grupos de escritorios de Horizon, App Volumes AppStacks y la configuración de User Environment Manager.

Requisitos previos

Compruebe que se cumplieron los requisitos que aparecen en [Capítulo 12 Administrar asignaciones JMP](#).

Procedimiento

- 1 En Horizon Console, haga clic en **Asignaciones (JMP)**.
- 2 Haga clic en **Nuevo**.
- 3 En la pestaña **Usuarios** del asistente Nueva asignación, introduzca un par de caracteres junto a la lista desplegable de Active Directory y seleccione a los usuarios o al grupo de usuarios que se incluyen en la nueva asignación JMP.

Su selección se agregará a la sección Usuarios o grupos seleccionados.
- 4 Haga clic en **Siguiente**.
- 5 En la pestaña **Escritorios**, seleccione el grupo de escritorios que desea incluir en la asignación JMP y haga clic en **Siguiente**.
- 6 En la pestaña **Aplicaciones**, haga clic en la casilla de verificación situada junto al nombre de la aplicación que desee incluir en la asignación JMP. Cuando finalice su selección, haga clic en **Siguiente**.
- 7 En la pestaña **Entorno del usuario**, decida si desea configurar la asignación JMP con cualquiera de las opciones disponibles del entorno de usuario.
 - Con **¿Desea deshabilitar la configuración de UEM?** configurada como **No**, al hacer clic en **Omitir** el archivo de asignación de User Environment Manager no se guardará en el recurso compartido de configuración de User Environment Manager. Todas las opciones de User Environment Manager se aplicarán a los espacios de trabajo de escritorios virtuales creados para los usuarios mediante la asignación JMP que está creando.
 - Con **¿Desea deshabilitar la configuración de UEM?** configurada como **No**, seleccione la configuración del entorno de usuario que desee aplicar a la asignación JMP que se está creando. Si hace clic en **Siguiente** se crea el archivo de asignación de User Environment Manager con la configuración de entorno de usuario seleccionada. La configuración seleccionada se aplicará a los espacios de trabajo de escritorios virtuales creados para los usuarios mediante la asignación JMP que está creando.

- Con **¿Desea deshabilitar la configuración de UEM?** configurada como **Sí**, la lista de opciones disponibles del entorno de usuario se eliminará de la vista. Al hacer clic en **Siguiente**, se escribe un archivo de asignación vacío en el recurso compartido de configuración de User Environment Manager. Al deshabilitar las opciones de User Environment Manager, no se aplicará ninguna opción de entorno de usuario a los espacios de trabajo de escritorios virtuales creados para los usuarios mediante la asignación JMP que está creando.
- 8 En la pestaña **Definiciones**, acepte el nombre predeterminado para la asignación JMP o bien sustituya el nombre por otro y, opcionalmente, agregue una descripción.
 - 9 En la lista desplegable **Asociar AppStack**, seleccione cuándo se asociará AppStack a la asignación JMP y haga clic en **Siguiente**.
 - 10 En la pestaña **Resumen**, revise los detalles de la nueva asignación. Si todo es correcto, haga clic en **Enviar**. Si se deben realizar cambios, haga clic en **Atrás** para realizar los ajustes.

La nueva asignación JMP se pondrá en cola para el almacenamiento en la base de datos de JMP y se agregará a la lista de asignaciones en el panel Asignaciones JMP. Una vez que la asignación JMP se agregue correctamente a la base de datos JMP, el estado Pendiente cambia. Se podrá seleccionar en la lista de asignación JMP para editarla, duplicarla o eliminarla.

También puede comprobar las asignaciones o las autorizaciones que se crearon para la nueva asignación JMP mediante la siguiente información.

- Para comprobar la información sobre el grupo de escritorios de Horizon creado para la asignación JMP, utilice Horizon Console. Seleccione **Inventario > Escritorios** y busque el grupo de escritorios que JMP Server creó.
- Para ver la información de AppStacks creada por JMP Server para la nueva asignación JMP, utilice la consola de App Volumes Manager. Seleccione **Volumes > AppStacks** y busque las AppStacks que JMP Server creó.
- Para comprobar la configuración del entorno de usuario que configuró para la asignación de JMP, utilice la Consola de administración de Dynamic Environment Manager y haga clic en la pestaña **Entorno de usuario**. En el panel izquierdo, seleccione la configuración del entorno de usuario que la asignación de JMP utilizó y haga clic en la pestaña **Asignaciones** en el cuadro de diálogo resultante para ver la información de asignación de JMP sobre dicha configuración del entorno de usuario.

Editar una asignación JMP

Es posible que necesite modificar una asignación JMP debido a cambios con los componentes que se utilizaron para definirla. Horizon Console permite realizar los cambios necesarios en una asignación JMP.

Requisitos previos

- Compruebe que se cumplieron los requisitos que aparecen en [Capítulo 12 Administrar asignaciones JMP](#).
- La asignación JMP que desea editar no puede estar en un estado "Pendiente".

Procedimiento

- 1 En Horizon Console, haga clic en **Asignaciones (JMP)**.
- 2 Para seleccionar la asignación JMP que desea editar, haga clic en la casilla de verificación, o bien en el nombre de la asignación JMP en la lista.
- 3 Haga clic en **Editar**.
- 4 En el asistente Editar asignación, modifique la configuración actual.

Haga clic en **Cancelar** si desea interrumpir el proceso de edición en cualquier momento.

- a Si desea eliminar ninguno de los usuarios o grupos seleccionados, haga clic en el icono para eliminar (**X**).
- b Haga clic en **Siguiente**.
- c En la pestaña **Escritorios**, seleccione un grupo de escritorios que desee incluir en la asignación JMP. Haga clic en **Siguiente**.
- d En la pestaña **Aplicaciones**, seleccione las aplicaciones disponibles que desee agregar a la asignación JMP o anule la selección de las aplicaciones que se seleccionaron previamente. Haga clic en **Siguiente**.
- e En la pestaña **Entorno del usuario**, decida si desea configurar la asignación JMP con cualquiera de las opciones disponibles del entorno de usuario.
 - Con **¿Desea deshabilitar la configuración de UEM?** configurada como **No**, al hacer clic en **Omitir** el archivo de asignación de User Environment Manager no se guardará en el recurso compartido de configuración de User Environment Manager. Todas las opciones de User Environment Manager se aplicarán a los espacios de trabajo de escritorios virtuales creados para los usuarios mediante la asignación JMP que está editando.
 - Con **¿Desea deshabilitar la configuración de UEM?** configurada como **No**, seleccione la configuración del entorno de usuario que desee aplicar a la asignación JMP que se está creando. Si hace clic en **Siguiente** se crea el archivo de asignación de User Environment Manager con la configuración de entorno de usuario seleccionada. La configuración seleccionada se aplicará a los espacios de trabajo de escritorios virtuales creados para los usuarios mediante la asignación JMP que está editando.
 - Con **¿Desea deshabilitar la configuración de UEM?** configurada como **Sí**, la lista de opciones disponibles del entorno de usuario se eliminará de la vista. Al hacer clic en **Siguiente**, se escribe un archivo de asignación vacío en el recurso compartido de configuración de User Environment Manager. Al deshabilitar las opciones de User Environment Manager no se aplicará ninguna opción de entorno de usuario a los espacios de trabajo de escritorios virtuales creados para los usuarios mediante la asignación JMP que está editando.
- f En la pestaña **Definiciones**, si corresponde, modifique los valores de **Nombre**, **Descripción** o de cuándo se debe asociar AppStack a la asignación JMP.

- g Haga clic en **Siguiente**.
- h Revise el resumen de los cambios realizados y haga clic en **Enviar** para guardar las modificaciones.

Si es correcto, se guardarán los cambios. Si se encuentra algún problema, se proporciona información adicional y se muestra cualquier acción posible que pueda realizar.

Duplicar una asignación JMP

Puede crear asignaciones JMP con mayor rapidez si duplica asignaciones JMP existentes que son similares a las que desea crear.

Requisitos previos

- Compruebe que se cumplieron los requisitos que aparecen en [Capítulo 12 Administrar asignaciones JMP](#).
- La asignación JMP que desea duplicar no debe estar en un estado "Pendiente" ni de "Error".

Procedimiento

- 1 En Horizon Console, seleccione **Asignaciones (JMP)**.
- 2 Seleccione la asignación JMP que desee duplicar y haga clic en **Duplicar**.
- 3 En el asistente Nueva asignación, modifique la asignación JMP duplicada según sea necesario.
 - a Seleccione los nuevos usuarios o grupos o bien elimine cualquiera de los grupos o usuarios seleccionados. Haga clic en **Siguiente**.
 - b En el panel Escritorios, seleccione un nuevo grupo de escritorios o bien elimine cualquiera de los grupos de escritorios que se incluyó en la asignación JMP duplicada. Haga clic en **Siguiente**.
 - c Seleccione las aplicaciones adicionales que desee incluir en la nueva asignación JMP y desmarque las que están seleccionadas. Haga clic en **Siguiente**.
 - d En el panel Entorno de usuario, seleccione la configuración de User Environment Manager que desee aplicar a la nueva asignación JMP. Haga clic en **Siguiente**.
 - e En el nombre Definiciones, si lo desea, reemplace el nombre predeterminado que se creó. Agregue una descripción y especifique cuándo desea que AppStack se conecte a la nueva asignación JMP.
 - f Haga clic en **Siguiente** y revise el resumen de los detalles de la nueva asignación JMP.
 - g Si la información correcta, haga clic en **Enviar**. De lo contrario, haga clic en **Atrás** para realizar las correcciones necesarias.

La nueva asignación JMP se validará, lo que puede tardar algún tiempo. Una vez validada correctamente, la asignación JMP recién creada se agregará a la lista en el panel Asignaciones JMP. Si coloca el cursor encima de su nombre, verá que está en estado pendiente hasta que se guarde correctamente en la base de datos de JMP. Una vez que la asignación JMP deje de estar en estado pendiente, puede realizar cualquier acción adicional en la asignación.

Eliminar una asignación JMP

Horizon Console permite eliminar las asignaciones JMP.

Cuando una asignación JMP se elimina, también se eliminan la autorización de grupo de Horizon, la asignación de AppStack y autorización de UEM asociada a la asignación JMP. Sin embargo, si la autorización de grupo de Horizon o la asignación AppStack que la asignación JMP utiliza ya existían antes de la creación de la asignación JMP, no se eliminarán. Tras eliminar una asignación JMP, ya no se aplica a los usuarios ni a los escritorios.

Requisitos previos

- Compruebe que se cumplieron los requisitos que aparecen en [Capítulo 12 Administrar asignaciones JMP](#).
- La asignación JMP que desea eliminar no puede estar en estado "Pendiente".

Procedimiento

- 1 En Horizon Console, haga clic en **Asignaciones (JMP)**.
- 2 En el panel Asignaciones JMP, seleccione una o varias de las asignaciones JMP y haga clic en **Eliminar**.
- 3 En el cuadro de diálogo de confirmación, haga clic en **Eliminar** para confirmar que desea eliminar la asignación permanentemente.

Si la operación se realiza correctamente, la autorización de grupo de Horizon se elimina de la base de datos de JMP así como de la lista en el panel Asignaciones JMP.

Si una parte de la operación de eliminación no se realiza correctamente, la asignación JMP no se eliminará. Si hace clic en los indicadores de estado, puede obtener más información sobre por qué se produjo el error en la operación de eliminación.

Configurar la generación de informes de eventos en Horizon Console

13

Puede crear una base de datos de eventos para registrar información sobre los eventos de Horizon 7. Además, si utiliza un servidor syslog, puede configurar el servidor de conexión para que envíe eventos a un servidor syslog o crear un archivo plano de eventos en formato syslog.

Este capítulo incluye los siguientes temas:

- [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7 en Horizon Console](#)
- [Preparar una base de datos SQL Server para los informes de eventos en Horizon Console](#)
- [Configurar la base de datos de eventos en Horizon Console](#)
- [Configurar el registro de eventos en archivos o el servidor syslog en Horizon Console](#)
- [Supervisar eventos en Horizon 7](#)

Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7 en Horizon Console

Para crear una base de datos de eventos, agréguela al servidor de una base de datos existente. A continuación, puede utilizar un software de informes para analizar los eventos en la base de datos.

Implemente el servidor de base de datos para la base de datos de eventos en un servidor dedicado, de modo que el registro de eventos no afecte al aprovisionamiento u otras actividades críticas para las implementaciones de Horizon 7.

Nota No es necesario crear un origen de datos ODBC para esta base de datos.

Requisitos previos

- Compruebe que posee un servidor de base de datos de Oracle o Microsoft SQL Server compatible con el sistema al que la instancia del servidor de conexión tiene acceso.

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

- Compruebe que posea los privilegios necesarios para crear una base de datos y un usuario en el servidor de la base de datos.
- Si no está familiarizado con el procedimiento para crear bases de datos en servidores de base de datos de Microsoft SQL Server, consulte "Agregar una base de datos de View Composer a SQL Server" en el documento *Instalación de Horizon 7*.
- Si no está familiarizado con el procedimiento para crear bases de datos en servidores de base de datos de Oracle, consulte "Agregar una base de datos de View Composer a Oracle 12c o 11g" en el documento *Instalación de Horizon 7*.

Procedimiento

- 1 Agregue una base de datos al servidor y asígnele un nombre descriptivo, por ejemplo, EventosHorizon.

En el caso de bases de datos de Oracle 12c u Oracle 11g, asigne también un identificador de sistema de Oracle (SID) para configurar la base de datos de eventos en Horizon Console.

- 2 Agregue un usuario para esta base de datos con permiso para crear tablas, vistas, desencadenadores y secuencias de Oracle, además de permiso de lectura y escritura en estos objetos.

En el caso de una base de datos de Microsoft SQL Server, no utilice el modelo de seguridad de autenticación integrada de Windows. Compruebe que utiliza el método Autenticación de SQL Server.

La base de datos se creará, pero el esquema no se instalará hasta que configure la base de datos en Horizon Console.

Pasos siguientes

Siga las instrucciones de [Configurar la base de datos de eventos en Horizon Console](#).

Preparar una base de datos SQL Server para los informes de eventos en Horizon Console

Si desea utilizar Horizon Console para configurar una base de datos de eventos en Microsoft SQL Server, debe configurar las propiedades de TCP/IP adecuadas y verificar que el servidor utilice la autenticación de SQL Server.

Requisitos previos

- Crear una base de datos SQL Server para los informes de eventos. Consulte [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7 en Horizon Console](#).

- Compruebe que disponga de los privilegios de base de datos necesarios para configurar la base de datos.
- Compruebe que el servidor de la base de datos utilice el método de autenticación de SQL Server. No utilice la autenticación de Windows.

Procedimiento

- 1 Abra el administrador de configuración de SQL Server y expanda **SQL Server AAAA Configuración de red**.
- 2 Seleccione **Protocolos de nombre_servidor**.
- 3 En la lista de protocolos, haga clic con el botón secundario en **TCP/IP** y seleccione **Propiedades**.
- 4 Elija **Sí** para la propiedad **Habilitada**.
- 5 Compruebe que haya un puerto asignado o asigne uno si es necesario.

Para obtener información sobre los puertos dinámicos y estáticos y cómo asignarlos, consulte la ayuda en línea del administrador de configuración de SQL Server.
- 6 Compruebe que el puerto no esté bloqueado por un firewall.

Pasos siguientes

Utilice Horizon Console para conectar la base de datos al servidor de conexión. Siga las instrucciones de [Configurar la base de datos de eventos en Horizon Console](#).

Configurar la base de datos de eventos en Horizon Console

La base de datos de eventos almacena información sobre los eventos de Horizon 7 en forma de registros en una base de datos en lugar de hacerlo en un archivo de registro.

Configure una base de datos de eventos después de instalar una instancia del servidor de conexión. Solo es necesario configurar un host en un grupo de servidores de conexión. El resto de hosts del grupo están configurados de forma automática.

Nota La seguridad de la conexión de la base de datos entre el servidor de conexión y una base de datos externa es responsabilidad del administrador, aunque se limite el tráfico de eventos a la información sobre el estado del entorno de Horizon 7. Si desea tomar más precauciones, puede asegurar este canal a través de IPSec u otros medios, o bien puede implementar la base de datos de forma local en el equipo del servidor de conexión.

Puede usar las herramientas de informe de la base de datos de Oracle o Microsoft SQL Server para examinar los eventos de las tablas de la base de datos. Para obtener más información, consulte el documento *Integración de Horizon 7*.

También puede generar eventos de Horizon 7 en formato `syslog` para que los software de análisis de terceros puedan acceder a los datos de eventos. Puede usar el comando `vdmadmin` con la opción `-I` para registrar mensajes de eventos de Horizon 7 en formato `syslog` en archivos de registro de eventos. Consulte "Generar mensajes de registro de eventos de Horizon 7 en formato `syslog` con la opción `-I`" en el documento *Administración de Horizon 7*.

Requisitos previos

Necesita la siguiente información para configurar una base de datos de eventos:

- La dirección IP o nombre de DNS del servidor de base de datos.
- El tipo del servidor de la base de datos: Oracle o Microsoft SQL Server.
- El número de puerto que se usa para acceder al servidor de la base de datos. El predeterminado es 1521 para Oracle y 1433 para SQL Server. Para SQL Server, si el servidor de la base de datos es una instancia con nombre o si usa SQL Server Express, es posible que necesite determinar el número de puerto. Consulte el artículo de la KB de Microsoft sobre cómo conectarse a una instancia con nombre de SQL Server, disponible en <http://support.microsoft.com/kb/265808>.

- El nombre de la base de datos del evento que creó en el servidor de la base de datos. Consulte [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7 en Horizon Console](#).

En el caso de bases de datos de Oracle 12c u 11g, debe usar un identificador de sistema de Oracle (SID) como el nombre de la base de datos cuando configure la base de datos de eventos en Horizon Console.

- El nombre y la contraseña del usuario que creó para esta base de datos. Consulte [Agregar una base de datos y un usuario de base de datos para los eventos de Horizon 7 en Horizon Console](#).

Use la autenticación de SQL Server para este usuario. No use el método de autenticación del modelo de seguridad de autenticación integrada de Windows.

- Un prefijo para las tablas de la base de datos de eventos, por ejemplo, `VE_`. El prefijo habilita que se comparta la base de datos en las instalaciones de Horizon 7.

Nota Debe introducir caracteres válidos para el software de la base de datos que está utilizando. No se comprueba la sintaxis del prefijo cuando completa el cuadro de diálogo. Si introduce caracteres que no son válidos para el software de la base de datos que está utilizando, se produce un error cuando el servidor de conexión intenta conectarse al servidor de la base de datos. El archivo de registro muestra todos los errores, incluidos este y otros que devuelva el servidor de la base de datos si el nombre de la base de datos no es válido.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Configuración de eventos**.
- 2 En la sección **Base de datos de eventos**, haga clic en **Editar**, introduzca la información en los campos proporcionados y haga clic en **Aceptar**.

Para borrar la información de la base de datos de eventos, haga clic en **Borrar**.

- 3 (opcional) En la ventana Configuración de evento, haga clic en **Editar**, cambie el tiempo establecido para mostrar los eventos y el número de días para clasificar los eventos como nuevos y, a continuación, haga clic en **Aceptar**.

Estas opciones pertenecen al tiempo durante el cual los eventos aparecen en la interfaz de Horizon Console. Después, los eventos solo están disponibles en las tablas históricas de la base de datos.

- 4 Seleccione **Supervisión > Eventos** para verificar que la conexión a la base de datos del evento sea correcta.

Si la conexión no es correcta, aparece un mensaje de error. Si usa SQL Express o si usa una instancia con nombre de SQL Server, es posible que necesite determinar el número de puerto correcto, como se mencionó en los requisitos.

Configurar el registro de eventos en archivos o el servidor syslog en Horizon Console

Puede generar eventos de Horizon 7 en formato syslog para que los software de análisis puedan acceder a los datos de eventos.

Solo es necesario configurar un host en un grupo de servidores de conexión. El resto de hosts del grupo están configurados de forma automática.

Si habilita el registro de eventos basados en archivo, los eventos se acumulan en un archivo de registro local. Si especifica un recurso compartido de archivo, estos archivos de registros se mueven a ese recurso.

- El tamaño máximo del directorio local para los registros de eventos es 300 MB, incluidos los archivos de registro cerrados, antes de que se eliminen los archivos más antiguos. El destino predeterminado de la salida syslog es %PROGRAMDATA%\VMware\VDM\events\.
- Use una ruta UNC para guardar archivos de registro para registrar eventos a largo plazo, si no tiene un servidor syslog ni una base de datos de eventos, o si su servidor syslog no cumple sus necesidades.

Puede usar un comando `vdmadmin` para configurar el registro de eventos basados en archivo en formato syslog. Consulte el tema sobre la generación de mensajes de registro de eventos de Horizon 7 en formato syslog con la opción `-I` del comando `vdmadmin`, en el documento *Administración de Horizon 7*.

Importante Cuando se envían a un servidor syslog, los datos syslog se envían a través de la red sin ningún cifrado basado en software y pueden contener información confidencial, como los nombres de usuarios. VMware recomienda el uso de la seguridad de nivel de vínculo, como IPSEC, para evitar la posibilidad de que estos datos se puedan supervisar a través de la red.

Requisitos previos

Necesita la siguiente información para configurar el servidor de conexión de forma que los eventos se puedan registrar en formato syslog, que se envíen a un servidor syslog o ambas opciones:

- Si tiene pensado usar un servidor syslog para escuchar los eventos de Horizon 7 en un puerto UDP, debe tener el nombre DNS o la dirección IP del servidor syslog y el número de puerto UDP. El puerto UDP predeterminado es el 514.
- Si tiene pensado recopilar registros en formato de archivo plano, debe tener la ruta UNC al recurso compartido de archivo y la carpeta en la que se almacenan los archivos de registro. También debe tener el nombre de usuario, de dominio y la contraseña de una cuenta que tenga permiso para escribir en el recurso compartido de archivo.

Procedimiento

- 1 En Horizon Console, seleccione **Configuración > Configuración de eventos**.
- 2 (opcional) En el área **Syslog**, para configurar que los servidores de conexión envíen eventos a un servidor syslog, haga clic en **Agregar** debajo de **Enviar a servidores syslog** y proporcione el nombre del servidor o la dirección IP y el número de puerto UDP.
- 3 (opcional) En el área **Eventos del sistema de archivos**, elija si desea habilitar o no la generación y el almacenamiento de los mensajes de registro de eventos en los archivos de registro y en formato syslog.

Opción	Descripción
Always	Siempre genera y almacena los mensajes de registro de eventos en los archivos de registro y en formato syslog.
Registrar en archivo en caso de error (predeterminada)	Registra los eventos de auditoría en un archivo de registro cuando se produce un problema al escribir eventos en la base de datos de eventos o en el servidor syslog. Esta opción está habilitada de forma predeterminada.
Never	Nunca genera ni almacena los mensajes de registro de eventos en los archivos de registro en formato Syslog.

Los archivos de registro se utilizan de forma local si no especifica una ruta UNC a un recurso compartido de archivo.

- 4 (opcional) Para almacenar los mensajes de registro de eventos de Horizon 7 en un recurso compartido de archivos, haga clic en **Agregar**, situado debajo de **Copiar a ubicación** y proporcione la ruta UNC a la carpeta y al archivo de recurso compartido en el que se almacenan los archivos de registro además del nombre de usuario, el nombre de dominio y la contraseña de una cuenta que tenga permiso para escribir en el recurso compartido de archivos.

Un ejemplo de una ruta UNC es:

```
\\syslog-server\folder\file
```

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 Console, y le notifica el número de eventos del panel de control. Puede examinar todos los detalles de los eventos en la página **Eventos**.

Nota Los eventos aparecen en la interfaz de Horizon Console 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 Console.

Además de supervisar los eventos de Horizon Console, 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 [Configurar el registro de eventos en archivos o el servidor syslog en Horizon Console](#) y "Generar mensajes de registro de eventos de Horizon 7 en formato syslog con la opción -l" en el documento *Instalación de Horizon 7*.

Si configura una base de datos de eventos para varios servidores de conexión, Horizon Console muestra los eventos de todos los servidores de conexión en la página **Eventos**. Horizon Console filtra los eventos en función de las tareas que realiza y muestra estos eventos en las páginas relevantes, como los **Grupos de escritorios** o **Grupos de aplicaciones**.

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 Console, seleccione **Supervisar > Eventos**.
- 2 (opcional) En la página **Eventos** puede seleccionar el rango de tiempo de esos eventos, aplicar filtros y ordenar los que aparecen por una o varias columnas.

Pasos siguientes

En Horizon Console, desplácese hasta un grupo de aplicaciones o de escritorios, una máquina virtual, un disco persistente o un usuario o grupo y haga clic en la pestaña **Eventos** para ver eventos específicos.

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 13-1. 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.
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.

Usar Horizon Help Desk Tool en Horizon Console

14

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 el documento *Administración de Horizon 7*.
- 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 *Administración 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 el documento *Administración de Horizon 7*.
- 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}
```

Este capítulo incluye los siguientes temas:

- [Iniciar Horizon Help Desk Tool en Horizon Console](#)
- [Solucionar los problemas de los usuarios en Horizon Help Desk Tool](#)
- [Detalles de las sesiones para Horizon Help Desk Tool](#)

- [Procesos de las sesiones de Horizon Help Desk Tool](#)
- [Estado de la aplicación para Horizon Help Desk Tool](#)
- [Solucionar problemas de las sesiones de aplicaciones o de escritorios de Horizon Help Desk Tool](#)

Iniciar Horizon Help Desk Tool en Horizon Console

Horizon Help Desk Tool está integrado en Horizon Console. Puede buscar un usuario al que quiera solucionarle problemas en Horizon Help Desk Tool.

Procedimiento

- 1 Puede buscar un nombre de usuario en el cuadro de texto **Búsqueda de usuarios** o ir directamente a la herramienta Horizon Help Desk Tool.
 - En Horizon Console, introduzca un nombre de usuario en el cuadro de texto **Búsqueda de usuarios**.
 - Seleccione **Supervisor > Departamento de soporte técnico** e introduzca un nombre de usuario en el cuadro de texto **Búsqueda de usuarios**.

Horizon Console muestra una lista de usuarios en los resultados de búsqueda. La búsqueda puede devolver 100 resultados de coincidencia.

- 2 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.

También puede hacer clic en la dirección de correo electrónico para enviarle un mensaje al usuario.

También 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.

Nota No aparece la información sobre Skype Empresarial para los usuarios de escritorios de Linux.

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 14-1. 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.
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. 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. ■ La pestaña Procesos muestra la información de los procesos relacionados con la CPU y la memoria. ■ La pestaña Aplicaciones muestra los detalles acerca de las aplicaciones que están en ejecución. <hr/> <p>Nota No se puede acceder a la pestaña Aplicaciones para las sesiones de escritorio de Linux.</p> <hr/>
Protocolo	<p>Protocolo de visualización de la sesión de aplicación o de escritorio.</p>

Tabla 14-1. Pestaña Sesiones (continuación)

Opción	Descripción
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.

Escritorios

La pestaña **Escritorios** muestra información sobre los escritorios publicados y los virtuales para los que el usuario tiene autorización.

Tabla 14-2. Escritorios

Opción	Descripción
Estado	Muestra información sobre el estado de la sesión de escritorio. ■ Si la sesión está conectada, aparece en verde.
Nombre de grupo de escritorios	Nombre del grupo de escritorios de la sesión. Muestra Linux como el grupo de escritorios para una sesión de escritorios de Linux.
Tipo de escritorio	Indica si el escritorio es un escritorio publicado o de máquina virtual. Nota No muestra información sobre si la sesión se ejecuta en un pod diferente de la federación.
Tipo	Muestra información sobre el tipo de autorización de escritorio. ■ Local, para una autorización local.
vCenter	Muestra el nombre de la máquina virtual de vCenter Server. Nota No muestra información sobre si la sesión se ejecuta en un pod diferente de la federación.
Protocolo predeterminado	Protocolo de visualización predeterminado de la sesión de aplicación o de escritorio.

Aplicaciones

La pestaña **Aplicaciones** muestra información sobre las aplicaciones publicadas para las que el usuario tiene autorización.

Nota No se puede acceder a la pestaña **Aplicaciones** para las sesiones de escritorio de Linux.

Tabla 14-3. Aplicaciones

Opción	Descripción
Estado	Muestra información sobre el estado de la sesión de aplicación. ■ 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 Si existe 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. ■ Local, para una autorización local.
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 Arquitectura Cloud Pod.

Tabla 14-4. Actividades

Opción	Descripción
Time	Seleccione un intervalo de tiempo. El valor predeterminado es las últimas 12 horas. ■ 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 para Horizon Help Desk Tool

La información de las sesiones 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 14-5. 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.
Versión del SO	Versión del sistema operativo.
Servidor de conexión	El servidor de conexión al que la sesión está conectada.
Grupo	Nombre del grupo de aplicaciones o de escritorios. Muestra Linux para un grupo de escritorios de Linux.
vCenter	Dirección IP de vCenter Server.
Estado de la sesión	<p>Estado de la sesión de aplicación o de escritorio. Los estados de la sesión pueden ser inactivo, activo o desconectado. Si el usuario no está activo durante un minuto, el estado de la sesión pasa a ser inactivo. El icono de estado aparece con el contorno en verde si la sesión está inactiva, en verde si está activa y en gris si está desconectada.</p> <p>Nota Las sesiones de los escritorios de Linux no muestran el estado inactivo.</p>
Duración de la sesión	El tiempo durante el cual la sesión permaneció conectada al servidor de conexión.
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.

Tabla 14-5. Detalles de la máquina virtual (continuación)

Opción	Descripción
Nombre de proxy/puerta de enlace	Nombre del servidor de seguridad, dispositivo de Unified Access Gateway o equilibrador de carga. Esta información puede tardar entre 30 y 60 segundos en aparecer después de conectarse a la sesión.
IP de proxy/puerta de enlace	Dirección IP del servidor de seguridad, dispositivo de Unified Access Gateway o equilibrador de carga. Esta información puede tardar entre 30 y 60 segundos en aparecer después de conectarse a la sesión.
Granja	La granja de hosts RDS de la sesión de aplicación o de escritorio publicados.

Indicadores de la experiencia del usuario

Muestra información sobre el rendimiento de una sesión de escritorio publicada o virtual que usa el protocolo de visualización VMware Blast o PCoIP. Para consultar esta información sobre el rendimiento, haga clic en **Más**. Para actualizar esta información, haga clic en el icono para actualizar.

Tabla 14-6. Detalles del protocolo de visualización PCoIP

Opción	Descripción
Ancho de banda de transmisión	El ancho de banda de transmisión (en kilobits por segundo) de una sesión PCoIP.
Velocidad de fotogramas	La velocidad de fotogramas (en fotogramas por segundo) de una sesión PCoIP.
Pérdida de paquetes	Porcentaje de pérdida de paquetes de una sesión PCoIP.
Estado de Skype	<p>El estado de Skype Empresarial de una sesión PCoIP.</p> <ul style="list-style-type: none"> ■ Optimizado ■ Reserva ■ Optimizado (versión no coincidente) ■ Reserva (versión no coincidente) ■ Conectando ■ Desconectado ■ Sin definir <p>Esta opción aparece como N/D para sesiones de escritorio de Linux.</p>

Tabla 14-7. Detalles del protocolo de visualización Blast

Opción	Descripción
Velocidad de fotogramas	La velocidad de fotogramas (en fotogramas por segundo) de una sesión Blast.
Estado de Skype	<p>El estado de Skype Empresarial de una sesión Blast.</p> <ul style="list-style-type: none"> ■ Optimizado ■ Reserva ■ Optimizado (versión no coincidente) ■ Reserva (versión no coincidente) ■ Conectando ■ Desconectado ■ Sin definir <p>Esta opción aparece como N/D para sesiones de escritorio de Linux.</p>
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.

Rendimiento de disco y red, y uso de la memoria y la CPU

Muestra gráficos del uso de memoria y de CPU de las aplicaciones o los escritorios virtuales o publicados, y el rendimiento de disco o de red del protocolo de visualización Blast o PCoIP.

Nota Después de iniciar o reiniciar Horizon Agent en el escritorio, es posible que los gráficos de rendimiento no muestren la escala de tiempo inmediatamente. La escala de tiempo aparece después de algunos minutos.

Tabla 14-8. Uso de CPU

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.

Tabla 14-9. Uso de memoria

Opción	Descripción
Memoria de la sesión	Uso de memoria de la sesión actual.
Memoria del host	Uso de la memoria de la máquina virtual a la que está asignada la sesión.

Tabla 14-10. Rendimiento de la red

Opción	Descripción
Latencia	<p>Muestra un gráfico de la latencia de la sesión 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>

Tabla 14-11. Rendimiento del disco

Opción	Descripción
Lectura	El número de operaciones de entrada o salida (E/S) por segundo.
Escritura	El número de operaciones de E/S de escritura por segundo.
Latencia de disco	Muestra un gráfico con la latencia de disco. La latencia de disco es el tiempo en milisegundos de los datos de operaciones de E/S por segundo recuperados de los contadores de rendimiento de Windows.
Promedio de lectura	El número de operaciones de E/S de lectura por segundo.
Promedio de escritura	El número promedio de operaciones de E/S de escritura por segundo.
Promedio de latencia	Tiempo medio de latencia en milisegundo de los datos E/S por segundo recuperados de los contadores de rendimiento de Windows.

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 14-12. 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. ■ Conexión de protocolo. Tiempo total que tarda la conexión del protocolo PCoIP o Blast en completarse durante el proceso de inicio de sesión. ■ Script de inicio de sesión. Tiempo total que tarda un script de inicio de sesión en ejecutarse desde que se inicia hasta que se completa. ■ 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 ninguna directiva global está configurada, la hora del segmento de inicio de sesión de **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**. Aparecen 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.
- Si la sesión es una sesión de escritorio de Linux, no aparecen los segmentos **Cargar GPO** ni **Cargar perfil**.
- Los datos de inicio de sesión no estarán disponible inmediatamente cuando la sesión de escritorio se conecta. Los datos de inicio de sesión aparecen después de algunos minutos.

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**.

En las sesiones del host RDS, la pestaña **Procesos** muestra los procesos de sesiones actuales del host RDS iniciadas por el proceso del sistema actual o el usuario actual.

Tabla 14-13. 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.

Tabla 14-13. Detalles de los procesos de las sesiones (continuación)

Opción	Descripción
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	<p>Finaliza un proceso que se está ejecutando.</p> <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> <p>No puede finalizar procesos críticos, como los procesos de núcleo de Windows, que puedan aparecer en la pestaña Procesos. Si finaliza un proceso crítico, Horizon Help Desk Tool muestra un mensaje que indica que no puede finalizar el proceso del sistema.</p>

Estado de la aplicación 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**. No se puede acceder a la pestaña **Aplicaciones** con las sesiones de escritorio de Linux.

Aplicaciones

Puede consultar el estado actual y otros detalles de cada aplicación.

Puede finalizar un proceso de aplicación para el usuario final. Para hacerlo, haga clic en **Finalizar aplicación** y en **Aceptar** para confirmar el cambio.

Nota El proceso de aplicación final puede fallar si la aplicación está pendiente de una interacción del usuario, como datos no guardados u otras excepciones. Sin embargo, Horizon Help Desk Tool no muestra ningún mensaje de confirmación o error cuando finaliza una aplicación.

Tabla 14-14. 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.

Tabla 14-14. Detalles de las aplicaciones (continuación)

Opción	Descripción
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>Nota Esta función no está disponible para usuarios de escritorios de Linux.</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 el comando vdmadmin

15

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 o para realizar tareas de administración que se tengan que ejecutar automáticamente desde scripts.

- **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 `-I`**

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 `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 [#unique_9](#).

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 `vdadmin` 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 `vdadmin` 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 `vdadmin`

Algunas opciones del comando `vdadmin` le permiten especificar el formato de la información de salida.

La siguiente tabla muestra las posibilidades que algunas de las opciones del comando `vdadmin` proporcionan para dar formato al texto de salida.

Tabla 15-1. 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 `vdadmin`

Puede usar las opciones del comando `vdadmin` para especificar la operación que desee que realice.

La siguiente tabla muestra las opciones de comando que puede usar con el comando `vdadmin` para controlar y examinar la operación de Horizon 7.

Tabla 15-2. 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 #unique_186 .
-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] -getlogfilearchivo de registro-outfile archivo_local-d escritorio-mequipo
```

```
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 [-mequipo]
```

```
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 15-3. Opciones para configurar los registros en Horizon Agent

Opción	Descripción
-d <i>escritorio</i>	Especifica el grupo de escritorios.
-getDCT	Crea un paquete de herramientas de recopilación de datos (DCT) y lo guarda en un archivo local.

Tabla 15-3. Opciones para configurar los registros en Horizon Agent (continuación)

Opción	Descripción						
<code>-getlogfile</code> <i>archivo de registro</i>	Especifica el nombre del archivo de registro del que guardar una copia.						
<code>-getloglevel</code>	Muestra el nivel de registro actual de Horizon Agent.						
<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</code> <i>máquina</i>	Especifica la máquina dentro de un grupo de escritorios.						
<code>-outfile</code> <i>archivo_local</i>	Especifica el nombre del archivo local en el que se guarda un paquete DCT o una copia del archivo de registro.						
<code>-setloglevel</code> <i>nivel</i>	<p>Establece el nivel de los registros de Horizon Agent.</p> <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.

```
vdmadmin -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.

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

Sobrescribir direcciones IP con la opción -A

El comando vdmadmin con la opción -A permite sobrescribir la dirección que muestra Horizon Agent.

Sintaxis

```
vdmadmin
-A [-bargumentos_autenticación] -override-i ip_o_dns-descriptorio-mmáquina
```

```
vdmadmin
-A [-bargumentos_autenticación] -override-list-descriptorio-mmáquina
```

```
vdmadmin
-A [-bargumentos_autenticación] -override-r-descriptorio [-mmáquina]
```

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 15-4. Opciones para sobrescribir direcciones IP

Opción	Descripción
-d escritorio	Especifica el grupo de escritorios.
-i ip_o_dns	Especifica la dirección IP o nombre del dominio que se puede resolver en el DNS.
-m máquina	Especifica el nombre de la máquina en un grupo de escritorios.

Tabla 15-4. Opciones para sobrescribir direcciones IP (continuación)

Opción	Descripción
<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`.

```
vdadmin -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`.

```
vdadmin -A -override -list -d dtpool2 -m machine2
```

Elimine las direcciones IP definidas para la máquina `machine2` del grupo de escritorios `dtpool2`.

```
vdadmin -A -override -r -d dtpool2 -m machine2
```

Elimine las direcciones IP definidas para los escritorios del grupo de escritorios `dtpool3`.

```
vdadmin -A -override -r -d dtpool3
```

Actualizar las entidades de seguridad externa con la opción -F

Puede usar el comando `vdadmin` 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

```
vdadmin
-F [-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 15-5. 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 15-6. 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 `-I` para mostrar los informes disponibles sobre el funcionamiento de Horizon 7 y los resultados tras ejecutar uno de dichos informes.

Sintaxis

```
vdadmin
-I [-b argumentos_autenticación] -list [-xml] [-w | -n]
```

```
vdadmin
```



```
-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 15-7. Opciones para especificar y visualizar informes y vistas

Opción	Descripción
<code>-enddate <i>yyyy-MM-dd-HH:mm:ss</i></code>	Especifica un límite superior para la fecha de información que se visualizará.
<code>-list</code>	Enumera los informes y vistas disponibles.
<code>-report <i>report</i></code>	Especifica un informe.
<code>-startdate <i>yyyy-MM-dd-HH:mm:ss</i></code>	Especifica un límite inferior para la fecha de información que se visualizará.
<code>-view <i>view</i></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 -I

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.

Sintaxis

```
vdmadmin  
-I  
-eventSyslog  
-disable
```

```
vdmadmin  
-I  
-eventSyslog  
-enable  
-localOnly
```

```
vdmadmin  
-I  
-eventSyslog  
-enable  
-path  
ruta
```

```
vdmadmin  
-I  
-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 -I 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 -I](#).

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 15-8. Opciones para generar los mensajes del registro de eventos de Horizon 7 en formato syslog

Opción	Descripción
<code>-disable</code>	Deshabilita el registro <code>syslog</code> .
<code>-e -enable</code>	Habilita el registro <code>syslog</code> .
<code>-eventSyslog</code>	Especifica que los eventos de Horizon 7 se generan en formato <code>syslog</code> .
<code>-localOnly</code>	Almacena la salida de <code>syslog</code> únicamente en el sistema local. Cuando usa la opción <code>-localOnly</code> , el destino predeterminado de la salida de <code>Syslog</code> es <code>%PROGRAMDATA%\VMware\VDM\events\</code> .
<code>-password contraseña</code>	Especifica la contraseña del usuario que autoriza el acceso a la ruta de destino especificada para la salida de <code>syslog</code> .
<code>-path</code>	Determina la ruta UNC de destino para la salida de <code>syslog</code> .
<code>-u -user NombreDominio\nombreusuario</code>	Especifica el nombre de usuario y el dominio que pueden acceder a la ruta de destino para la salida de <code>syslog</code> .

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 `vdadmin` con la opción `-L` para asignar máquinas de un grupo dedicado a los usuarios.

Sintaxis

```
vdadmin
-L [-bargumentos_autenticación] -descriptorio -m máquina-udominio\usuario
```

```
vdadmin
-L [-bargumentos_autenticación] -descriptorio [-m máquina | -udominio\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 `vdadmin -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 `vdadmin -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 15-9. 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 15-10. 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.

```
vdmadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

Visualice información sobre la máquina machine3 en un formato de valores separados por coma.

```
vdmadmin -M -m machine3 -csv
```

Recuperar espacio de disco de las máquinas virtuales con la opción -M

El comando `vdmadmin` 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

```
vdmadmin
-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 [#unique_203](#).
- 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 15-11. 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 15-12. 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.

```
vdadmin -N -domains -list -active -xml -n
```

Elimina el dominio NEARDOM de la lista de exclusión de búsqueda para un grupo del servidor de conexión.

```
vdadmin -N -domains -exclude -domain NEARDOM -remove
```

Elimina todos los dominios de la lista de inclusión de la instancia csvr1 del servidor de conexión.

```
vdadmin -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 15-13. 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 exclusión 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 | -xsldpath ruta]]
```

```
vdmadmin  
-P [-b argumentos_autenticación] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsldpath 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 15-14. 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 15-15. Hojas de estilo XLS 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 15-15. Hojas de estilo XLS

Nombre del archivo de la hoja de estilo	Descripción
unentitled-machines.xml	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.xml	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.

```
vdadmin -O -lu -xml -n
```

Aplique su propia hoja de estilo C:\tmp\unentitled-users.xml y redireccione los resultados del archivo uu-output.html.

```
vdadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xml" > 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.

```
vdadmin -P -ld -xml -w
```

Aplique su propia hoja de estilo C:\tmp\unentitled-policies.xml y redireccione los resultados del archivo up-output.html.

```
vdadmin -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 `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.

Sintaxis

```
vdadmin
-Q
-clientauth
-add [-b argumentos_autenticación] -domain nombre_dominio-clientid id_cliente [-password
"contraseña" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-groupnombre_grupo | -nogroup]
[-description "texto_descripción"]
```

```
vdadmin
-Q
-disable [-bargumentos_autenticación] -s servidor_conexión
```

```
vdadmin
```

```
-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 15-16. 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 15-16. 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.

```
vdadmin -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.

```
vdadmin -Q -clientauth -getdefaults
```

Obtenga los valores predeterminados actuales de los clientes en formato XML.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -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 `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.

Nota El comando `vdadmin` 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

```
vdadmin
-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.

```
vdadmin -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 `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.

Sintaxis

```
vdadmin  
-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 `vdadmin` 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 `vdadmin` 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} -ownerdominio\usuario-userdominio\usuario
[-passwordcontraseña]
```

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 15-17. 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 [-bargumentos_autenticación] -e-descriptorio-mmáquina [-m máquina] ...
```

```
vdmadmin
-V [-bargumentos_autenticación] -e-vcdndn_vCenter-vmpathruta_inventario
```

```
vdmadmin
-V [-b argumentos_autenticación] -p-d escritorio -m máquina [-mmáquina] ...
```

```
vdmadmin
-V [-b argumentos_autenticación] -p-vcdndn_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 15-18. 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.
<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.

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

Bloquee la máquina virtual machine3 en el grupo de escritorios dtpool3.

```
vdmadmin -V -p -d dtpool3 -m machine3
```

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.

Sintaxis

```
vdmadmin
-X [-bargumentos_autenticación] -collisions [-resolve]
vdmadmin-X [-bargumentos_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 `vdmadmin` 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 `vdmadmin` 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 15-19. 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 15-20. 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
```