

# Administración de View

VMware Horizon 7 7.1



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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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

Copyright © 2014-2017 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

# Contenido

## Administración de View 12

### 1 Uso de View Administrator 13

- View Administrator y el servidor de conexión de View 13
- Iniciar sesión en View Administrator 14
- Consejos para usar la interfaz de View Administrator 15
- Solucionar problemas de visualización de texto en View Administrator 17

### 2 Configurar el servidor de conexión de View 18

- Configurar vCenter Server y View Composer 18
  - Crear una cuenta de usuario para operaciones en AD de View Composer 18
  - Agregar instancias de vCenter Server a View 20
  - Configurar las opciones de View Composer 22
  - Configurar los dominios de View Composer 23
  - Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados 24
  - Configurar el acelerador de almacenamiento de View para vCenter Server 26
  - Límites de operaciones simultáneas para vCenter Server y View Composer 28
  - Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto 29
  - Aceptar la huella digital de un certificado SSL predeterminado 30
  - Eliminar una instancia de vCenter Server de View 32
  - Eliminar View Composer de View 32
  - ID únicos de vCenter Server en conflicto 33
- Realizar una copia de seguridad del servidor de conexión de View 33
- Configurar las opciones de las sesiones cliente 34
  - Configurar opciones de las conexiones y las sesiones cliente 34
  - Cambiar la contraseña de Data Recovery 34
  - Configuración global de las sesiones cliente 35
  - Configuración de seguridad global para conexiones y sesiones cliente 39
  - Modo de seguridad del mensaje para los componentes de View 41
  - Configurar el túnel seguro y la puerta de enlace segura PCoIP 44
  - Configurar la puerta de enlace segura Blast 46
  - Descargar conexiones SSL a servidores intermedios 47
  - Configurar la ubicación de la puerta de enlace para un servidor de conexión de Horizon o el host del servidor de seguridad 50
- Habilitar o deshabilitar un servidor de conexión de View 51
- Editar las URL externas 51
- Unirse al programa de experiencia del cliente o abandonarlo 53

Directorio LDAP de View 53

### 3 Configurar la autenticación de tarjeta inteligente 56

- Iniciar sesión con una tarjeta inteligente 57
- Configurar la autenticación con tarjeta inteligente en el servidor de conexión de View 57
  - Obtener los certificados de la autoridad de certificación 58
  - Obtener el certificado de CA de Windows 59
  - Agregar el certificado de CA a un archivo del almacén de confianza del servidor 60
  - Modificar las propiedades de configuración del servidor de conexión de View 61
  - Configurar las opciones de la tarjeta inteligente en View Administrator 62
- Configurar la autenticación con tarjeta inteligente en soluciones de terceros 65
- Preparar Active Directory para la autenticación con tarjeta inteligente 66
  - Agregar UPN para usuarios de tarjetas inteligentes 66
  - Agregar el certificado raíz al almacén Enterprise NTAAuth 67
  - Agregar el certificado raíz a las entidades de certificación raíz de confianza 67
  - Agregar un certificado intermedio a las entidades de certificación intermedias 68
- Verificar la configuración de la autenticación con tarjeta inteligente 69
- Uso de la comprobación de revocación de certificados de tarjeta inteligente 71
  - Iniciar sesión con la comprobación de CRL 72
  - Iniciar sesión con la comprobación de revocación del certificado OCSP 72
  - Configurar comprobación de CRL 72
  - Configurar la comprobación de revocación del certificado OCSP 73
  - Propiedades de la comprobación de revocación del certificado de la tarjeta inteligente 74

### 4 Configurar otros tipos de autenticación de usuario 76

- Uso de la autenticación en dos fases 76
  - Iniciar sesión usando la autenticación en dos fases 77
  - Habilitar una autenticación en dos fases en View Administrator 78
  - Solucionar los problemas de acceso denegado de RSA SecurID 80
  - Solucionar los problemas de acceso denegado de RADIUS 81
- Uso de la autenticación SAML 81
  - Utilizar la autenticación SAML para integrar VMware Identity Manager 81
  - Configurar un autenticador SAML en View Administrator 82
  - Cambiar el período de caducidad de los metadatos del proveedor de servicios en el servidor de conexión de View 85
  - Generar metadatos SAML para que el servidor de conexión de View se pueda usar como proveedor del servicio 86
  - Consideraciones del tiempo de respuesta para varios autenticadores SAML dinámicos 86
- Configurar la autenticación biométrica 87

### 5 Autenticar usuarios sin solicitar las credenciales 88

- Proporcionar acceso sin autenticar para las aplicaciones publicadas 89

Crear usuarios con acceso sin autenticar	90
Habilitar el acceso sin autenticar para los usuarios	91
Autorizar a los usuarios sin autenticar para que accedan a las aplicaciones publicadas	92
Buscar sesiones con acceso sin autenticar	92
Eliminar un usuario con acceso sin autenticar	93
Acceso sin autenticar desde Horizon Client	93
Uso de la función Iniciar sesión como usuario actual disponible con Horizon Client basado en Windows	94
Guardar credenciales en Horizon Clients que se encuentren en equipos Mac y dispositivos móviles	95
Configurar un límite de tiempo de espera para guardar las credenciales de Horizon Client	95
Configurar True SSO	96
Determinar una arquitectura para True SSO	97
Configurar una entidad de certificación empresarial	99
Crear plantillas de certificado para usarlas con True SSO	101
Instalar y configurar un servidor de inscripción	103
Exportar el certificado cliente del servicio de inscripciones	106
Importar el certificado cliente del servicio de inscripciones en el servidor de inscripciones	107
Configurar la autenticación SAML para que funcione con True SSO	108
Configurar el servidor de conexión de View para True SSO	110
Referencia de la línea de comandos para configurar True SSO	113
Opciones de configuración avanzadas para True SSO	117
Uso del panel de control del estado del sistema para solucionar problemas relacionados con True SSO	121

## 6 Configurar la administración delegada basada en funciones 125

Comprender las funciones y los privilegios	125
Uso de grupos de acceso para delegar la administración de grupos y granjas	126
Administradores diferentes para grupos de acceso diferentes	127
Administradores diferentes para el mismo grupo de acceso	127
Comprender los permisos	128
Administrar administradores	129
Crear un administrador	129
Eliminar un administrador	130
Administrar y consultar los permisos	131
Agregar un permiso	131
Eliminar un permiso	132
Revisar los permisos	133
Administrar y consultar los grupos de acceso	133
Agregar un grupo de acceso	134
Mover un grupo de escritorios o una granja a un grupo de acceso diferente	134
Eliminar un grupo de acceso	135

Revisar las granjas o los grupos de escritorios o de aplicaciones de un grupo de acceso	135
Revisar las máquinas virtuales de vCenter de un grupo de acceso	136
Administrar funciones personalizadas	136
Agregar una función personalizada	136
Modificar los privilegios de una función personalizada	137
Eliminar una función personalizada	137
Funciones y privilegios predefinidos	138
Funciones de administrador predefinidas	138
Privilegios globales	140
Privilegios específicos de objeto	141
Privilegios internos	142
Privilegios necesarios para las tareas comunes	143
Privilegios para administrar grupos	143
Privilegios para administrar máquinas	143
Privilegios para administrar discos persistentes	144
Privilegios para administrar los usuarios y los administradores	144
Privilegios para los comandos y las tareas de administración general	145
Prácticas recomendadas para grupos y usuarios administradores	145
<b>7 Configurar directivas en Horizon Administrator y en Active Directory</b>	<b>147</b>
Establecer directivas en View Administrator	147
Configurar las opciones de la directiva global	148
Configurar directivas para los grupos de escritorios	148
Configurar directivas para los usuarios	149
Directivas de View	149
Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7	150
Archivos de plantilla ADM y ADMX de Horizon 7	151
Configuración de las plantillas ADM o ADMX de configuración del servidor de conexión de Horizon	153
Configuración de las plantillas ADM y ADMX de configuración común de Horizon 7	154
<b>8 Mantener los componentes de View</b>	<b>158</b>
Realizar una copia de seguridad y restaurar los datos de configuración de View	158
Realizar una copia de seguridad de los datos del servidor de conexión de View y de View Composer	159
Restaurar los datos de configuración del servidor de conexión de View y de View Composer	162
Exportar datos en la base de datos de View Composer	167
Supervisar los componentes de View	168
Supervisar el estado de las máquinas	169
Comprender los servicios de View	170
Detener e iniciar servicios de View	170
Servicios en un host del servidor de conexión de View	171

Servicios de un servidor de seguridad	172
Cambiar la clave de licencia del producto	172
Supervisar la licencia y el uso del producto	173
Restablecer los datos de uso de la licencia del producto	174
Actualizar la información general del usuario desde Active Directory	175
Migrar View Composer a otro equipo	175
Directrices para migrar View Composer	176
Migrar View Composer con una base de datos existente	177
Migrar View Composer sin máquinas virtuales de clones vinculados	179
Preparar Microsoft .NET Framework para migrar las claves RSA	180
Migrar el contenedor de claves RSA al nuevo servicio de View Composer	181
Actualizar los certificados en una instancia del servidor de conexión de View, en el servidor de seguridad o en View Composer	182
Información recopilada por el programa de mejora de la experiencia de cliente	183
Cómo VMware asegura su privacidad	184
Previsualizar los datos recopilados para el programa de mejora de la experiencia de cliente	185
Información adicional sobre el Programa de mejora de la experiencia de cliente	185
Datos de View globales recopilados por VMware	186
Datos del servidor de conexión de View recopilados por VMware	188
Datos del servidor de seguridad recopilados por VMware	190
Información del grupo de escritorios recopilada por VMware	191
Datos de las máquinas recopilados por VMware	194
Datos de vCenter Server recopilados por VMware	196
Datos de ThinApp recopilados por VMware	197
Información de Arquitectura de Cloud Pod recopilada por VMware	198
Datos de Horizon Client recopilados por VMware	199
Datos recopilados por VMware	201

## 9 Administrar máquinas virtuales de escritorios de clones vinculados de View Composer 203

Reducir el tamaño de clones vinculados con una actualización de máquinas	203
Operaciones de actualización de la máquina	204
Actualizar los escritorios de clones vinculados	206
Preparar una máquina virtual principal para recomponer clones vinculados	206
Recomponer máquinas virtuales de clones vinculados	207
Actualizar clones vinculados mediante una recomposición	209
Corregir una recomposición que no se realizó correctamente	210
Volver a equilibrar máquinas virtuales de clones vinculados	211
Volver a equilibrar clones vinculados entre unidades lógicas	212
Migrar las máquinas virtuales de clones vinculados a otro almacén de datos	213
Nombres de archivos de discos de clones vinculados después de una operación para volver a equilibrar	214

Administrar los discos persistentes de View Composer	215
Discos persistentes de View Composer	215
Desconectar un disco persistente de View Composer	216
Conectar un disco persistente de View Composer a otro clon vinculado	216
Editar un usuario o un grupo de discos persistentes de View Composer	217
Volver a crear un clon vinculado con un disco persistente desconectado	218
Restaurar un clon vinculado importando un disco persistente desde vSphere	219
Eliminar un disco persistente desconectado de View Composer	220

## 10 Administrar grupos de escritorios, equipos y sesiones 221

Administrar grupos de escritorios de clones instantáneos	221
Cambiar la imagen de un grupo de escritorios de clones instantáneos	221
Supervisar una operación de inserción de imagen	222
Volver a programar o cancelar una operación de inserción de imagen	222
Administrar grupos de escritorios	223
Editar un grupo de escritorios	223
Modificar la configuración de un grupo de escritorios existente	223
Opciones mantenidas en un grupo de escritorios existente	226
Cambiar el tamaño de un grupo automático aprovisionado por un patrón de nomenclatura	226
Agregar máquinas a un grupo automatizado aprovisionado con una lista de nombres	227
Deshabilitar o habilitar un grupo de escritorios	229
Habilitar o deshabilitar el aprovisionamiento en un grupo de escritorios automático	229
Configurar los límites y la calidad de Adobe Flash	230
Límites y calidad de Adobe Flash	230
Eliminar un grupo de escritorios	231
Configurar View para no permitir la eliminación de un grupo que contiene equipos de escritorio	232
Administrar escritorios basados en máquinas virtuales	233
Asignar una máquina a un usuario	233
Eliminar la asignación de un usuario de una máquina dedicada	234
Personalizar los equipos existentes en modo de mantenimiento	234
Supervisar el estado del escritorio de la máquina virtual	235
Estado de las máquinas virtuales de vCenter Server	236
Eliminar escritorios de máquina virtual	238
Recuperar los escritorios de clones instantáneos	239
Gestionar equipos no administrados	239
Agregar un equipo no administrado a un grupo manual	240
Eliminar un equipo no administrado de un grupo de escritorios manual	240
Eliminar las máquinas registradas de View	241
Estado de las máquinas no administradas	241
Administrar sesiones de aplicaciones y escritorios publicados	243
Exportar información de View a archivos externos	243



## 11 Administrar hosts RDS, granjas y grupos de aplicaciones 245

- Administrar grupos de aplicaciones 245
  - Editar un grupo de aplicaciones 245
  - Eliminar un grupo de aplicaciones 246
- Administrar granjas 246
  - Editar una granja 246
  - Eliminar una granja 247
  - Habilitar o deshabilitar una granja 247
  - Recomponer una granja automática de clones vinculados 247
  - Programar el mantenimiento para una granja automática de clones instantáneos 249
- Administrar los hosts RDS 252
  - Editar un host RDS 252
  - Agregar un host RDS a una granja manual 253
  - Eliminar un host RDS de una granja 253
  - Eliminar un host RDS de Horizon 7 254
  - Deshabilitar o habilitar un host RDS 254
  - Supervisar los hosts RDS 254
  - Estado de los hosts RDS 255
  - Configurar el límite de Adobe Flash con Internet Explorer en escritorios RDS 256
- Configurar el equilibrio de carga de los hosts RDS 257
  - Preferencias de carga asignada y valores de carga 257
  - Límites de la función de equilibrio de carga 258
  - Escribir un script de equilibrio de carga para un host RDS 258
  - Habilitar el servicio de VMware Horizon View Script Host en un host RDS 259
  - Configurar un script de equilibrio de carga en un host RDS 260
  - Verificar un script de equilibrio de carga 261
  - Ejemplos de ubicación de sesiones de equilibrio de carga 262
- Configurar una regla anti-compatibilidad para un grupo de aplicaciones 264
  - Restricciones de la función Anticompatibilidad 265

## 12 Administrar las aplicaciones ThinApp en View Administrator 266

- Requisitos de View para las aplicaciones ThinApp 266
- Capturar y almacenar paquetes de aplicaciones 267
  - Empaquetar aplicaciones 268
  - Crear un recurso compartido de red de Windows 269
  - Registrar un repositorio de aplicaciones 269
  - Agregar aplicaciones ThinApp a View Administrator 270
  - Crear una plantilla ThinApp 271
- Asignar aplicaciones ThinApp a grupos de escritorios y máquinas 271
  - Prácticas recomendadas para asignar aplicaciones ThinApp 273
  - Asignar una aplicación ThinApp a varias máquinas 273

Asignar varias aplicaciones ThinApps a una máquina	274
Asignar una aplicación ThinApp a varios grupos de escritorios	275
Asignar varias aplicaciones ThinApps a un grupo de escritorios	276
Asignar una plantilla ThinApp a una máquina o grupo de escritorios	277
Revisar las asignaciones de las aplicaciones ThinApp	278
Visualizar información del paquete MSI	279
Mantener las aplicaciones ThinApp en View Administrator	279
Eliminar una asignación de aplicaciones ThinApp de varias máquinas	280
Eliminar varias asignaciones de aplicaciones ThinApp de una máquina	280
Eliminar una asignación de aplicaciones ThinApp de varios grupos de escritorios	281
Eliminar varias asignaciones de aplicaciones ThinApp de un grupo de escritorios	281
Eliminar una aplicación ThinApp de View Administrator	282
Modificar o eliminar una plantilla ThinApp	282
Eliminar el repositorio de una aplicación	283
Supervisar y solucionar problemas de las aplicaciones ThinApp en View Administrator	283
No se puede registrar un repositorio de aplicaciones	283
No se puede agregar aplicaciones ThinApp a View Administrator	284
No se puede asignar una plantilla ThinApp	285
La aplicación ThinApp no está instalada	285
La aplicación ThinApp no está desinstalada	286
El paquete MSI no es válido	287
Ejemplo de configuración ThinApp	287

## **13 Configurar clientes en modo de pantalla completa 289**

Configurar clientes en modo de pantalla completa	290
Preparar Active Directory y View para clientes en modo de pantalla completa	291
Establecer valores predeterminados para clientes en modo de pantalla completa	292
Visualizar las direcciones MAC de dispositivos cliente	293
Agregar cuentas de clientes en modo de pantalla completa	294
Habilitar la autenticación de clientes en modo de pantalla completa	296
Verificar la configuración de los clientes en modo de pantalla completa	298
Conectarse a escritorios remotos desde clientes en modo de pantalla completa	299

## **14 Solucionar problemas relacionados con View 302**

Supervisar el estado del sistema	302
Supervisar eventos en View	303
Mensajes de eventos de View	304
Recopilar información de diagnóstico para View	304
Crear un paquete de herramientas de recopilación de datos para Horizon Agent	305
Guardar información de diagnóstico de Horizon Client	306
Recopilar información de diagnóstico de View Composer con el script de soporte	307

Recopilar información de diagnóstico del servidor de conexión de Horizon	307
Recopilar información de diagnóstico de Horizon Agent, de Horizon Client o del servidor de conexión de Horizon desde la consola	308
Actualizar las solicitudes de soporte	310
Solucionar un emparejamiento de servidor de seguridad con el servidor de conexión de View que no se realizó correctamente	310
Solucionar problemas relacionados con la comprobación de revocación de certificados de View Server	311
Solucionar problemas relacionados con la comprobación de revocación de la tarjeta inteligente	312
Más información para solucionar problemas	313

## 15 Usar el comando vdmadmin 314

Uso del comando vdmadmin	316
Autenticación del comando vdmadmin	316
Formato de la salida del comando vdmadmin	317
Opciones del comando vdmadmin	317
Configurar los registros en Horizon Agent con la opción -A	319
Sobrescribir direcciones IP con la opción -A	321
Establecer el nombre del grupo del servidor de conexión de View con la opción -C	322
Actualizar las entidades de seguridad externa con la opción -F	323
Enumerar y mostrar las supervisiones de estado con la opción -H	324
Especificar y visualizar informes sobre el funcionamiento de View con la opción -I	325
Generar mensajes de registro de eventos de View en formato syslog con la opción -I	327
Asignar máquinas dedicadas usando la opción -L	329
Visualizar información sobre las máquinas con la opción -M	331
Recuperar espacio de disco de las máquinas virtuales con la opción -M	332
Configurar filtros de dominios con la opción -N	333
Configurar los filtros de dominios	336
Ejemplo de filtrado para incluir dominios	338
Ejemplo de filtrado para excluir dominios	338
Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P	341
Configurar clientes en modo de pantalla completa con la opción -Q	342
Visualizar el primer usuario de un equipo con la opción -R	348
Eliminar una entrada de una instancia del servidor de conexión de View o del servidor de seguridad con la opción -S	349
Proporcionar credenciales secundarias para los administradores con la opción -T	350
Visualizar información sobre los usuarios con la opción -U	352
Bloquear o desbloquear las máquinas virtuales con la opción -V	353
Detectar y resolver colisiones de entradas LDAP usando la opción -X	354

# Administración de View

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

## Público al que se dirige

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

# Uso de View Administrator

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

Para comparar las operaciones que puede realizar con View Administrator, con los cmdlets de View y con vdmadmin, consulte el documento *Integración de View*.

---

**Nota** En Horizon 7, View Administrator recibe el nombre de Horizon Administrator. En este documento se refiere a Horizon Administrator como View Administrator.

---

Este capítulo incluye los siguientes temas:

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

## View Administrator y el servidor de conexión de View

View Administrator proporciona una interfaz de administración basada en Web para View.

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

Use las siguientes prácticas recomendadas para usar View Administrator con un servidor de conexión de View:

- Use el nombre de host y la dirección IP del servidor de conexión de View para iniciar sesión en View Administrator. Use la interfaz de View Administrator para administrar el servidor de conexión de View, así como cualquier servidor de seguridad asociado o servidor de réplica.

- En un entorno de pod, compruebe que todos los administradores utilicen el nombre de host y la dirección IP del mismo servidor de conexión de View para iniciar sesión en View Administrator. No utilice el nombre de host y la dirección IP del equilibrador de carga para acceder a la página web de View Administrator.

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

## Iniciar sesión en View Administrator

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

### Requisitos previos

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

### 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 de View.

**`https://servidor/administrador`**

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

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

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

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

## 2 Inicie sesión como un usuario con credenciales para acceder a la cuenta de View Administrator.

Debe especificar la cuenta de View Administrator cuando instale una instancia del servidor de conexión de View independiente o la primera instancia del servidor de conexión de View en un grupo replicado. La cuenta de View Administrator puede ser el grupo de administradores local (BUILTIN\Administrators) en el equipo del servidor de conexión de View o una cuenta de usuario o grupo del dominio.

Después de iniciar sesión en View Administrator, puede usar **Configuración de View >**

**Administradores** para cambiar la lista de usuarios y grupos que tengan la función View Administrator.

## Consejos para usar la interfaz de View Administrator

Las funciones de la interfaz de usuario de View Administrator permiten dirigirse a las páginas de View y buscar, filtrar y ordenar objetos de View.

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

[Tabla 1-1. Funciones de visualización y de navegación de View Administrator](#) describe algunas funciones adicionales que le pueden ayudar a usar View Administrator.

**Tabla 1-1. Funciones de visualización y de navegación de View Administrator**

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

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



Función de View Administrator	Descripción
Ampliar los cuadros de diálogos para ver los detalles	<p>Puede ampliar los cuadros de diálogos de View Administrator para ver detalles tales como nombres de escritorios y nombres de usuarios en las columnas de la tabla.</p> <p>Para ampliar un cuadro de diálogo, coloque el mouse sobre los puntos que aparecen en la esquina inferior derecha del cuadro de diálogo y arrastre la esquina.</p>
Mostrar los menús contextuales de los objetos de View	<p>Si hace clic con el botón secundario en las tablas de View Administrator, mostrará los menús contextuales. Un menú contextual le proporciona acceso a los comandos que funcionan en el objeto de View seleccionado.</p> <p>Por ejemplo, en la página <b>Catálogo &gt; Grupos de escritorios</b>, puede hacer clic con el botón secundario en un grupo de escritorios para mostrar comandos tales como <b>Agregar</b>, <b>Editar</b>, <b>Eliminar</b>, <b>Deshabilitar (o Habilitar) aprovisionamiento</b>, etc.</p>

## Solucionar problemas de visualización de texto en View Administrator

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

### Problema

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

### Causa

Son necesarias fuentes específicas de Microsoft para View Administrator.

Instale las fuentes específicas de Microsoft en su equipo.

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

# Configurar el servidor de conexión de View

## 2

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

Este capítulo incluye los siguientes temas:

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

## Configurar vCenter Server y View Composer

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

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

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

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

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

### Procedimiento

- 1 En Active Directory, cree una cuenta de usuario en el mismo dominio que el host del servidor de conexión de View 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 View Administrator cuando configure los dominios de View Composer en el asistente Agregar vCenter Server y cuando configure e implemente los grupos de escritorios de clones vinculados.

## Agregar instancias de vCenter Server a View

Debe configurar View para conectar las instancias de vCenter Server en la implementación de View. vCenter Server crea y administra las máquinas virtuales que View utiliza en grupos de escritorios.

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

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

### Requisitos previos

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

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

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

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

- Compruebe que todas las instancias del servidor de conexión de View en el grupo replicado confíen en el certificado raíz de AC para el certificado del servidor instalado en el host de vCenter Server. Asegúrese de que el certificado raíz de AC 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 de View. 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 View*.

- 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 View.
- 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 View 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 View en modo FIPS" en el documento *Instalación de View*.

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

### Procedimiento

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

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

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

---

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

---

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

### Pasos siguientes

Configure las opciones de View Composer.

- Si la instancia de vCenter Server se configura con un certificado SSL firmado y el servidor de conexión de View confía en el certificado raíz, el asistente para agregar vCenter Server muestra la página de Configuración de View Composer.
- Si la instancia de vCenter Server se configura con un certificado predeterminado, primero debe determinar si acepta la huella digital del certificado existente. Consulte [Aceptar la huella digital de un certificado SSL predeterminado](#).

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

## Configurar las opciones de View Composer

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

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

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

### Requisitos previos

- Compruebe que creó un usuario en Active Directory con permiso para agregar y eliminar máquinas virtuales del dominio de Active Directory que incluye clones vinculados. Consulte [Crear una cuenta de usuario para operaciones en AD de View Composer](#).
- Compruebe que View 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 View](#).
- Compruebe que el servicio VMware Horizon View Composer aún no esté configurado para conectarse a otra instancia de vCenter Server.

### Procedimiento

- 1 En View Administrator, complete la página de Información de vCenter Server en el asistente para Agregar vCenter Server.
  - a Seleccione **Configuración de View > Servidores**.
  - b En la pestaña **vCenter Servers**, haga clic en **Agregar** y configure las opciones de vCenter Server.
- 2 En la página de Configuración de View Composer, si no está utilizando dicho componente, seleccione **No utilizar View Composer**.

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

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

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

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

#### Pasos siguientes

Configure los dominios de View Composer.

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

## Configurar los dominios de View Composer

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

#### Requisitos previos

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

## Procedimiento

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

## Pasos siguientes

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

## 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 View. A partir de vSphere 5.1, View 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 el clon.

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, View puede mantener los clones vinculados casi al tamaño reducido con el que empezaron cuando se aprovisionaron por primera vez.

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



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

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

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

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

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

#### Requisitos previos

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

#### Procedimiento

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

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

#### Pasos siguientes

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

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

## Configurar el acelerador de almacenamiento de View para vCenter Server

En vSphere 5.0 y versiones posteriores, puede configurar los hosts ESXi para almacenar en caché datos del disco de la máquina virtual. Esta función, denominada Acelerador de almacenamiento de View, usa la función de almacenamiento de caché de lectura basada en el contenido (CBRC) en los hosts ESXi. El acelerador de almacenamiento de View mejora el rendimiento de Horizon 7 durante procesos de E/S masivos, que tienen lugar cuando varias máquinas virtuales se inician o realizan exámenes de antivirus a la vez. Esta función también es útil cuando los administradores o los usuarios cargan aplicaciones o datos frecuentemente. En lugar de leer todo el SO o toda la aplicación desde el sistema de almacenamiento una y otra vez, un host puede leer bloques de datos comunes desde la caché.

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

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

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

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

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

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

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

---

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

---

### Requisitos previos

- Compruebe que vCenter Server y los hosts ESXi tengan la versión 5.0 o una versión posterior.

En un clúster ESXi, compruebe que todos los hosts cuenten con la versión 5.0 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 View* que describen los privilegios de Horizon 7 y de View Composer necesarios para el usuario de vCenter Server.

### Procedimiento

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

- 2 En la página Configuración de almacenamiento, asegúrese de que la casilla de verificación **Habilitar el acelerador de almacenamiento de View** esté seleccionada.

Esta casilla de verificación está seleccionada de forma predeterminada.

- 3 Especifique un tamaño de la caché del host predeterminado.

El tamaño de la memoria caché predeterminado se aplica a todos los hosts ESXi administrados por esta instancia de vCenter Server.

El valor predeterminado es 1.024MB. El tamaño de la caché debe estar entre 100 MB y 2.048 MB.

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

### Pasos siguientes

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

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

## Límites de operaciones simultáneas para vCenter Server y View Composer

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

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

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

Configuración	Descripción
<b>Número máximo de operaciones de aprovisionamiento de vCenter simultáneas</b>	<p>Determina el número máximo de las solicitudes simultáneas que el servidor de conexión de View 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>
<b>Máximo número de operaciones de alimentación simultáneas</b>	<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 de View 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 <a href="#">Configurar la velocidad de las operaciones de alimentación simultáneas para admitir inicios de sesión masivos en el escritorio remoto</a>.</p> <p>Esta configuración se aplica a las máquinas virtuales completas y a los clones vinculados.</p>

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

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

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

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

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 SSL predeterminado

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

Si una instancia de vCenter Server o de View Composer está configurada con un certificado firmado por una CA y el servidor de conexión de View 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 de View no confía en el certificado raíz, debe determinar si desea aceptar la huella digital del certificado. Una huella digital es un hash criptográfico de un certificado. La huella digital se usa para determinar rápidamente si un certificado presentado es igual a otro, como, por ejemplo, el certificado que se aceptó previamente.

---

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

---

Para obtener más información sobre la configuración de los certificados SSL, consulte "Configurar certificados SSL en View Server", disponible en el documento *Instalación de View*.

Primero agregue vCenter Server y View Composer en View Administrator usando el asistente Agregar vCenter Server. Si un certificado no es de confianza y no acepta la huella digital, no puede agregar vCenter Server ni View Composer.

Después de agregar estos servidores, puede volver a configurarlos en el cuadro de diálogo Editar vCenter Server.

**Nota** También debe aceptar una huella digital de certificado cuando actualice una versión anterior y un certificado de vCenter Server o de View Composer no sea de confianza, o bien si reemplaza un certificado de confianza por uno que no lo sea.

En el panel de control de View Administrator, el icono de vCenter Server o de View Composer se vuelve rojo y aparece el cuadro de diálogo Se detectó un certificado no válido. Debe hacer clic en **Verificar** y seguir el procedimiento que aparece a continuación.

De forma similar, en View Administrator puede configurar un autenticador SAML para que la use una instancia del servidor de conexión de View. Si el servidor de conexión de View no confía en el certificado del servidor SAML, debe determinar si desea aceptar la huella digital del certificado. Si no acepta la huella digital, no puede configurar el autenticador SAML en View. Después de configurar un autenticador SAML, puede volver a configurarlo en el cuadro de diálogo Editar servidor de conexión de View.

### Procedimiento

- 1 Cuando aparece el cuadro de diálogo Se detectó un certificado no válido en View Administrator, haga clic en **Ver certificado**.
- 2 Examine la huella digital del certificado en la ventana Información del certificado.
- 3 Examine la huella digital del certificado que se configuró para la instancia de View Composer o vCenter Server.
  - a En el host de View Composer o de vCenter Server, inicie el complemento MMC y abra el almacén de certificados de Windows.
  - b Diríjase al certificado de vCenter Server o de View Composer.
  - c Haga clic en la pestaña Información del certificado para mostrar la huella digital del certificado.

De forma similar, examine la huella digital del certificado de un autenticador SAML. Si es necesario, lleve a cabo los pasos anteriores en el host del autenticador SAML.
- 4 Compruebe que la huella digital de la ventana Información del certificado coincida con la huella digital de la instancia de vCenter Server o de View Composer.
 

De forma similar, compruebe que las huellas digitales coincidan con un autenticador SAML.
- 5 Determine si desea aceptar la huella digital del certificado.

Opción	Descripción
La huella digital coincide.	Haga clic en <b>Aceptar</b> para usar el certificado predeterminado.
Las huellas digitales no coinciden.	Haga clic en <b>Rechazar</b> . Solucione los problemas con los certificados que no coinciden. Por ejemplo, es posible que haya proporcionado una dirección IP incorrecta para vCenter Server o View Composer.

## Eliminar una instancia de vCenter Server de View

Puede eliminar la conexión entre View y una instancia de vCenter Server. Cuando lo haga, View 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. Consulte [Eliminar un grupo de escritorios](#).

### Procedimiento

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

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

- 4 Haga clic en **Aceptar**.

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

## Eliminar View Composer de View

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

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

### Procedimiento

- 1 Elimine los grupos de escritorios de clones vinculados que View Composer creó.

- a En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- b Seleccione un grupo de escritorios de clones vinculados y haga clic en **Eliminar**.

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

- c Haga clic en **Aceptar**.

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

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

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



- 3 En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server asociada a View Composer.
- 4 Haga clic en **Editar**.
- 5 En la Configuración del servidor de View Composer, haga clic en **Editar**, seleccione **No utilizar View Composer** y haga clic en **Aceptar**.

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

#### Pasos siguientes

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

## ID únicos de vCenter Server en conflicto

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

#### Problema

Al intentar agregar una instancia de vCenter Server a View, 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 View

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

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

## Configurar las opciones de las sesiones cliente

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

## Configurar opciones de las conexiones y las sesiones cliente

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

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

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

### Requisitos previos

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

### Procedimiento

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

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

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

### Pasos siguientes

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

## Cambiar la contraseña de Data Recovery

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

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

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

#### Procedimiento

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

---

**Nota** Puede cambiar la contraseña de Data Recovery cuando programe la copia de seguridad de los datos de configuración de View. Consulte [Programar copias de seguridad de la configuración de View](#).

---

#### Pasos siguientes

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

## Configuración global de las sesiones cliente

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

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

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

Configuración	Descripción
<b>Tiempo de espera de la sesión de View Administrator</b>	<p>Determina durante cuánto tiempo continua una sesión inactiva de View Administrator antes de que la sesión caduque.</p> <p><b>Importante</b> Al establecer el tiempo de espera de la sesión de View Administrator a un número elevado de minutos, aumenta el riesgo de que View Administrator se use de forma no autorizada. Si desea permitir una sesión inactiva durante un tiempo prolongado, hágalo con precaución.</p> <p>De forma predeterminada, el tiempo de espera de la sesión de View Administrator es 30 minutos. Puede establecer el tiempo de espera de la sesión de 1 a 4320 minutos (72 horas).</p>
<b>Desconectar usuarios de forma forzada</b>	<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 View. 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 <b>Nunca</b> o superior a 1200 minutos.</p> <p>El valor predeterminado es <b>Después de 600 minutos</b>.</p>
<b>Single Sign-On (SSO)</b>	<p>Si SSO está habilitado, View 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 <b>Habilitado</b>.</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> <p><b>Nota</b> 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 View Agent 6.0 o una versión superior, o bien Horizon Agent 7.0 o una versión superior, el servidor de conexión de View 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 View o cerrar Horizon Client y volver a conectarse al servidor de conexión de View. Sin embargo, si el escritorio se inicia desde Workspace Portal o VMware Identity Manager y el escritorio está bloqueado, las credenciales SSO no se descartan.</p>

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

Configuración	Descripción
<b>Mostrar la advertencia antes del cierre de sesión</b>	<p>Muestra un mensaje de advertencia cuando se obliga a los usuarios a cerrar sesión por una actualización programada o inmediata como, por ejemplo, cuando una operación de actualización de escritorio está a punto de comenzar. Esta opción también determina el tiempo de espera desde que se muestra el mensaje hasta que se cierra la sesión del usuario.</p> <p>Seleccione la casilla para mostrar un mensaje de advertencia.</p> <p>Escriba el número de minutos que se debe esperar desde que se muestra el mensaje hasta que se cierra la sesión del usuario. El valor predeterminado es 5 minutos.</p> <p>Escriba el mensaje de advertencia. Puede usar el mensaje predeterminado:</p> <div> <p>Está programada una actualización importante para el escritorio y este se desconectará en 5 minutos. Guarde ahora el trabajo sin guardar.</p> </div>
<b>Habilitar escritorios Windows Server</b>	<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, View Administrator muestra todos los equipos Windows Server disponibles, incluidos los equipos en los que los componentes del servidor de View están instalados.</p> <p><b>Nota</b> El software Horizon Agent no puede coexistir en la misma máquina virtual o física con cualquier otro componente de software del servidor de View, como un servidor de seguridad, el servidor de conexión de View o View Composer.</p>
<b>Limpiar credencial al cerrar la pestaña para HTML Access</b>	<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, View también elimina las credenciales de la caché en los siguientes escenarios cliente de HTML Access:</p> <ul style="list-style-type: none"> <li>■ Un usuario actualiza la página de selección de aplicaciones y escritorios o la página de la sesión remota.</li> <li>■ 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.</li> <li>■ Un usuario ejecuta un comando URI en la pestaña que contiene la sesión remota.</li> </ul> <p>Cuando esta opción está deshabilitada, las credenciales se mantienen en la caché. Esta función está deshabilitada de forma predeterminada.</p> <p><b>Nota</b> Esta función está disponible en Horizon 7 versión 7.0.2 y versiones posteriores.</p>
<b>Configuración del servidor Mirage</b>	<p>Le permite especificar la URL de un servidor de Mirage, usando el formato <b>mirage://nombre-servidor:puerto</b> o <b>mirages://nombre-servidor:puerto</b>. En este caso, <i>nombre-servidor</i> es el nombre de dominio completo. Si no especifica el número de puerto, se usa el número 8000 que es el predeterminado.</p> <p><b>Nota</b> Puede sobrescribir esta opción global especificando un servidor Mirage en las opciones del grupo de escritorios.</p> <p>La especificación del servidor de Mirage en View Administrator es una alternativa a especificar el servidor de Mirage cuando instale el cliente Mirage. Para encontrar qué versión de compatibilidad de Mirage tiene el servidor especificado en View Administrator, consulte la documentación de Mirage en <a href="https://www.vmware.com/support/pubs/mirage_pubs.html">https://www.vmware.com/support/pubs/mirage_pubs.html</a>.</p>

Configuración	Descripción
<b>Ocultar la información del servidor en la interfaz de usuario del cliente</b>	Habilite esta opción de seguridad para ocultar la información de la URL del servidor en Horizon Client 4.4 o una versión posterior.
<b>Ocultar la lista de dominios en la interfaz de usuario del cliente</b>	<p>Habilite esta opción de seguridad para ocultar el menú desplegable Dominio en Horizon Client 4.4 o una versión posterior.</p> <p>Si el usuario inicia sesión en una instancia del servidor de conexión que tenga habilitada la configuración global <b>Ocultar la lista de dominios en la interfaz de usuario del cliente</b>, el menú desplegable Dominio permanece oculto en Horizon Client y el usuario proporciona la información de dominio en el cuadro de texto <b>Nombre de usuario</b>. Por ejemplo, los usuarios deben proporcionar el nombre de usuario utilizando el formato <code>domain\username</code> o <code>username@domain</code>.</p> <p><b>Importante</b> Si habilita las opciones <b>Ocultar la información del servidor en la interfaz de usuario del cliente</b> y <b>Ocultar la lista de dominios en la interfaz de usuario del cliente</b> 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. Si exige que coincidan los nombres de usuarios de Windows, se impide a los usuarios que introduzcan información de dominio en el cuadro de texto del nombre de usuario y siempre se producirá un error al iniciar sesión. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento <i>Administración de View</i>.</p>

## Configuración de seguridad global para conexiones y sesiones cliente

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

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

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

Configuración	Descripción
<b>Volver a autenticar las conexiones de túnel seguro después de la interrupción en la red</b>	<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>
<b>Modo de seguridad del mensaje</b>	<p>Determina el mecanismo de seguridad usado para enviar mensajes JMS entre componentes.</p> <ul style="list-style-type: none"> <li>■ Cuando el modo está configurado como <b>Habilitado</b>, se producen la firma y la verificación de los mensajes JMS que se envían entre componentes de View.</li> <li>■ Cuando el modo está configurado como <b>Mejorada</b>, la seguridad se proporciona gracias a las conexiones JMS de SSL autenticadas de forma mutua y al control del acceso a temas JMS</li> </ul> <p>Para obtener más información, consulte <a href="#">Modo de seguridad del mensaje para los componentes de View</a>.</p> <p>En las nuevas instalaciones, de forma predeterminada, se configura como <b>Mejorada</b>. Si actualiza una versión anterior, se mantiene la opción utilizada en la versión anterior.</p>
<b>Estado de seguridad mejorada (solo lectura)</b>	<p>Campos de solo lectura que aparecen cuando la opción <b>Modo de seguridad Mensaje</b> se cambia de <b>Habilitado</b> a <b>Mejorado</b>. Como el cambio se hace en fases, este campo muestra el progreso en las diferentes fases:</p> <ul style="list-style-type: none"> <li>■ La opción <b>Esperar el reinicio del bus de mensajería</b> 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 View en todos los hosts del servidor de conexión del pod.</li> <li>■ La opción <b>Mejora pendiente</b> es el siguiente estado. Después de que se reinicien todos los servicios del componente de bus de mensajería de View, el sistema comienza a cambiar el modo de seguridad de los mensajes a <b>Mejorado</b> de todos los escritorios y servidores de seguridad.</li> <li>■ La opción <b>Mejorado</b> es el estado final, que indica que todos los componentes están usando el modo de seguridad de los mensajes <b>Mejorado</b></li> </ul> <p>También puede usar la utilidad de la línea de comandos <code>vdmutil</code> para supervisar el progreso. Consulte <a href="#">Uso de la utilidad vdmutil para configurar el modo de seguridad del mensaje JMS</a>.</p>
<b>Usar IPsec para las conexiones del servidor de seguridad</b>	<p>Determina si se debe usar el Protocolo de seguridad de Internet (IPSec) para las conexiones entre los servidores de seguridad y las instancias del servidor de conexión de View.</p> <p>De forma predeterminada, las conexiones seguras (con IPSec) para las conexiones de los servidores de seguridad están habilitadas.</p>



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

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

## Modo de seguridad del mensaje para los componentes de View

Puede establecer el modo de seguridad del mensaje para especificar el mecanismo de seguridad usado cuando se envían mensajes JMS entre los componentes de View.

[Tabla 2-4. Opciones del modo de seguridad del mensaje](#) muestra las opciones que puede seleccionar para configurar el modo de seguridad del mensaje. Para establecer una opción, selecciónela en la lista **Modo de seguridad del mensaje** en la ventana de diálogo Configuración global.

**Tabla 2-4. Opciones del modo de seguridad del mensaje**

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

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

---

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

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

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

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

Los componentes de View que sean anteriores a la versión 6.1 de Horizon 6 no se pueden comunicar con una instancia del servidor de conexión de View 6.1 que usan el modo Mejorada.

---

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

## Uso de la utilidad vdmutil para configurar el modo de seguridad del mensaje JMS

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

### Sintaxis y ubicación de la utilidad

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

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

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

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

## Autenticación

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

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

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

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

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

## Opciones específicas del modo de seguridad del mensaje JMS

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

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

Tabla 2-6. Opciones del comando vdmutil

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

## Configurar el túnel seguro y la puerta de enlace segura PCoIP

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

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

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

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

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

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

### Requisitos previos

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

### Procedimiento

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

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

El túnel seguro se habilita de forma predeterminada.

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

Opción	Descripción
Habilitar la puerta de enlace segura PCoIP	Seleccione <b>Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina</b> .
Deshabilitar la puerta de enlace segura PCoIP	Anule la selección <b>Usar la puerta de enlace segura PCoIP para las conexiones PCoIP de la máquina</b> .

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

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

## Configurar la puerta de enlace segura Blast

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

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

- Los Horizon Clients pueden usar la red BEAT con una condición excelente de la red mientras se conecta al servidor de conexión, al servidor de seguridad o al dispositivo Access Point.
- Los Horizon Clients que usen una condición típica de la red deben conectarse a un servidor de conexión (BSG deshabilitada), a un servidor de seguridad (BSG deshabilitada) o a versiones posteriores a la 2.8 de un dispositivo Access Point. Si Horizon Client usa una condición típica de la red para conectarse a un servidor de conexión (BSG habilitada), a un servidor de seguridad (BSG habilitada) o a versiones anteriores a la 2.8 de un dispositivo Access Point, el cliente detecta automáticamente la condición de la red y vuelve a la red TCP.
- Los Horizon Clients que usen una condición mala de la red deben conectarse a la versión 2.9 o a una versión posterior de un dispositivo Access Point (con Servidor del túnel UDP habilitado). Si Horizon Client usa una condición mala de la red para conectarse al servidor de conexión (BSG habilitada), al servidor de seguridad (BSG habilitada) o a versiones anteriores a la 2.8 de un dispositivo Access Point, el cliente detecta automáticamente la condición de la red y vuelve a la red TCP.
- Los Horizon Clients que usen una mala condición de la red para conectarse al servidor de conexión (BSG habilitada), al servidor de seguridad (BSG habilitada), a versiones posteriores a la 2.9 de un dispositivo Access Point (sin Servidor del túnel UDP habilitado) o a la versión 2.8 del dispositivo Access Point, el cliente detecta automáticamente la condición de la red y vuelve a la condición típica.

Para obtener más información, consulte la documentación de Horizon Client disponible en [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html).

---

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

---

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

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

### Requisitos previos

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

### Procedimiento

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

Opción	Descripción
Habilitar la puerta de enlace segura Blast	Seleccione <b>Usar la puerta de enlace segura Blast en las conexiones Blast de la máquina</b>
Deshabilitar la puerta de enlace segura Blast	Desmarque <b>Usar la puerta de enlace segura Blast en las conexiones Blast de la máquina</b>

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

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

## Descargar conexiones SSL a servidores intermedios

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

### Importar certificados de servidores de descarga SSL a los servidores de View

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

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

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

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

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

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

## Configurar las URL externas de View Server para enviar los clientes a los servidores de descarga SSL

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

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

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

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

---

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

---



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

## Permitir conexiones HTTP desde servidores intermedios

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

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

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

---

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

---

### Procedimiento

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

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

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

Debe escribir el valor `http` en minúsculas.

- 3 (opcional) Agregue las propiedades para configurar un puerto de escucha HTTP no predeterminado y una interfaz de red en el servidor de View.

- Para cambiar el puerto de escucha HTTP a uno diferente del 80, establezca `serverPortNonSSL` a otro número de puerto al que el dispositivo intermedio esté configurado para conectarse.
- Si el servidor de View tiene más de una interfaz de red y pretende que el servidor escuche conexiones HTTP en una sola interfaz, establezca `serverHostNonSSL` con la dirección IP de dicha interfaz de red.

- 4 Guarde el archivo `locked.properties`.
- 5 Reinicie el servicio del servidor de conexión de View o el servicio del servidor de seguridad para que se apliquen los cambios.

**Ejemplo: archivo locked.properties**

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

```
serverProtocol=http
serverHostNonSSL=10.20.30.40
```

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

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

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

**Procedimiento**

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

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

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

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

```
gatewayLocation=value
```

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

Por ejemplo, `gatewayLocation=External`

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

## Habilitar o deshabilitar un servidor de conexión de View

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

Cuando deshabilite una instancia del servidor de conexión de View, esto no afecta a los usuarios que tienen la sesión iniciada en ese momento en las aplicaciones y los escritorios remotos.

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

- Si se trata de una instancia del servidor de conexión de View independiente y única, los usuarios no pueden iniciar sesión en las aplicaciones ni en los escritorios remotos. No se pueden conectar al servidor de conexión de View.
- Si esta es una instancia replicada del servidor de conexión de View, 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 remotos.

### Procedimiento

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

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

## Editar las URL externas

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

De forma predeterminada, un host del servidor de seguridad o del servidor de conexión de View se pueden contactar únicamente a través de clientes de túnel que residen dentro de la misma red. 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 de View o a un host del servidor de seguridad.

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

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

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

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

## Procedimiento

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

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

- 2 Escriba la URL externa del túnel seguro en el cuadro de texto **URL externa**.

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

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

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

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

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

Por ejemplo: `10.20.30.40:4172`

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

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

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

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

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

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

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

## Unirse al programa de experiencia del cliente o abandonarlo

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

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

Para ver la lista de campos de los que se obtienen los datos, incluidos los campos anónimos, consulte [Información recopilada por el programa de mejora de la experiencia de cliente](#).

### Procedimiento

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

## Directorio LDAP de View

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

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

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

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

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

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

---

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

---

## Replicación de LDAP

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

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

Puede usar el panel de control de View Administrator para comprobar el estado de replicación. Si alguna instancia del servidor de conexión de View tiene un icono rojo en el panel de control, haga clic en el icono para ver el estado de replicación. Es posible que la replicación se vea afectada por las siguientes razones:

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

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

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

# Configurar la autenticación de tarjeta inteligente

## 3

Para una mayor seguridad, puede configurar una instancia del servidor de conexión de View 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 debe introducir 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 de *instalación de View* 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://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.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 View](#)
- [Configurar la autenticación con tarjeta inteligente en soluciones de terceros](#)
- [Preparar Active Directory para la autenticación con tarjeta inteligente](#)
- [Verificar la configuración de la autenticación con tarjeta inteligente](#)
- [Uso de la comprobación de revocación de certificados de tarjeta inteligente](#)



## Iniciar sesión con una tarjeta inteligente

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

Cuando un usuario o administrador se conecta a una instancia del servidor de conexión de View o al servidor de seguridad que esté configurado para la autenticación con tarjeta inteligente, dicha instancia o servidor envía una lista de autoridades 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 de View 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 View Administrator. El usuario de tarjeta inteligente puede introducir un nombre de usuario o el nombre principal del usuario (user principal name, UPN) en el campo Sugerencia de nombre de usuario durante el inicio de sesión de la tarjeta inteligente.

Si el entorno utiliza un dispositivo de Access Point para garantizar un acceso externo seguro, debe configurar el dispositivo para que sea compatible con la función de sugerencias de nombre de usuario de la tarjeta inteligente. Dicha función es compatible únicamente con Access Point 2.7.2 y versiones posteriores. Para obtener más información sobre cómo habilitar la función de sugerencias de nombre de usuario de la tarjeta inteligente en Access Point, consulte el documento *Implementación y configuración de Access Point*.

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 View

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 de View 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 de View 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 View

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

### 5 Configurar las opciones de la tarjeta inteligente en View Administrator

Puede usar View Administrator si especifica opciones para tener en cuenta diferentes escenarios de autenticación con tarjeta inteligente.

## Obtener los certificados de la autoridad de certificación

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

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

## Procedimiento

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

## Pasos siguientes

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

## Obtener el certificado de CA de Windows

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

## Procedimiento

- 1 Si el certificado del usuario está en una tarjeta inteligente, insértela en el lector y agregue el certificado del usuario a su almacén personal.  
  
Si el certificado del usuario no aparece en su almacén personal, utilice el software del lector para exportarlo a un archivo. Este archivo se utiliza en el Paso 4 de este procedimiento.
- 2 En Internet Explorer, seleccione **Herramientas > Opciones de Internet**.
- 3 En la pestaña **Contenido**, haga clic en **Certificados**.
- 4 En la pestaña **Personal**, seleccione el certificado que desee utilizar y haga clic en **Ver**.  
  
Si el certificado del usuario no aparece en la lista, haga clic en **Importar** para importarlo manualmente desde un archivo. Después de importar el certificado, podrá seleccionarlo de la lista.
- 5 En la pestaña **Ruta de certificación**, seleccione el certificado que está más arriba en el árbol y haga clic en **Ver certificado**.  
  
Si el certificado del usuario está firmado como parte de una jerarquía de confianza, el certificado de firma puede estar firmado por otro certificado de mayor nivel. Seleccione el certificado padre (el que realmente firmó el certificado del usuario) como su certificado raíz. En algunos casos, el emisor puede ser una autoridad de certificación intermedia.
- 6 En la pestaña **Detalles**, haga clic en **Copiar en archivo**.  
  
Aparecerá el **Asistente para la exportación de certificados**.

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

### Pasos siguientes

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

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

Debe agregar los certificados raíces, los certificados intermedios o ambos a un archivo del almacén de confianza para todos los usuarios y los administradores en los que confíe. Las instancias del servidor de conexión de View 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 de View o en el host del servidor de seguridad. Consulte el documento *Instalación de View* para obtener más información.

### Procedimiento

- 1 En el host del servidor de seguridad o del servidor de conexión de View, 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 de View.

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

### Pasos siguientes

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

## Modificar las propiedades de configuración del servidor de conexión de View

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

### 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 de SSL en el host del servidor de seguridad o el servidor de conexión de View.

Por ejemplo: `install_directory\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 de View o el servicio del servidor de seguridad para que se apliquen los cambios.

### Ejemplo: Archivo `locked.properties`

El archivo mostrado especifica que el certificado de todos los usuarios de confianza se encuentra en el archivo `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 de View, configure sus opciones en View Administrator. No necesita configurar las opciones de la autenticación con tarjeta inteligente de los servidores de seguridad. Las opciones que se configuran en una instancia del servidor de conexión de View también se aplican al servidor de seguridad vinculado.

## Configurar las opciones de la tarjeta inteligente en View Administrator

Puede usar View Administrator si especifica opciones para tener en cuenta diferentes escenarios de autenticación con tarjeta inteligente.

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

### Requisitos previos

- Modifique las propiedades de configuración del servidor de conexión de View en el host del servidor de conexión de View.
- Compruebe que Horizon Client establezca las conexiones directamente al servidor de conexión de View o al host del servidor de seguridad. La autenticación con tarjeta inteligente no es compatible si descarga SSL a un dispositivo intermedio.

### Procedimiento

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

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

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

Opción	Acción
<b>No se permite</b>	La autenticación con tarjeta inteligente está deshabilitada en la instancia del servidor de conexión de View.
<b>Opcional</b>	Los usuarios pueden usar la autenticación con tarjeta inteligente o la autenticación con contraseña para conectarse a la instancia del servidor de conexión de View. Si se produce un error en la autenticación con tarjeta inteligente, el usuario debe proporcionar una contraseña.
<b>Obligatoria</b>	<p>Se le solicita a los usuarios usar la autenticación con tarjeta inteligente cuando se conectan a la instancia del servidor de conexión de View.</p> <p>Cuando se solicita una autenticación con tarjeta inteligente, se produce un error en la autenticación de los usuarios que seleccionaron la casilla de verificación <b>Iniciar sesión como usuario actual</b> cuando se conectan a la instancia del servidor de conexión de View. Estos usuarios se deben volver a autenticar con la tarjeta inteligente y el PIN cuando inicien sesión en el servidor de conexión de View.</p> <p><b>Nota</b> 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
<b>Desconectar a los usuarios del servidor de conexión de View cuando extraigan las tarjetas inteligentes.</b>	Seleccione la casilla de verificación <b>Desconectar las sesiones del usuario al extraer la tarjeta inteligente</b> .
<b>Mantener los usuarios conectados al servidor de conexión de View cuando extraigan las tarjetas inteligentes y permitirles iniciar nuevas sesiones de escritorios o aplicaciones sin una reautenticación.</b>	Desmarque la casilla de verificación <b>Desconectar las sesiones del usuario al extraer la tarjeta inteligente</b> .

La directiva de extracción de tarjeta inteligente no se aplica a los usuarios que se conectan a la instancia del servidor de conexión de View 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 <b>Permitir las sugerencias del nombre de usuario de la tarjeta inteligente</b> .
Deshabilite que los usuarios puedan utilizar un certificado de tarjeta inteligente único para autenticar varias cuentas de usuarios.	Desmarque la casilla de verificación <b>Permitir las sugerencias del nombre de usuario de la tarjeta inteligente</b> .

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

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

- 5 Haga clic en **Aceptar**.

- 6 Reinicie el servicio del servidor de conexión de View.

Debe reiniciar el servicio del servidor de conexión de View 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 de View.

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



## Pasos siguientes

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

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

## Configurar la autenticación con tarjeta inteligente en soluciones de terceros

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

Este tema detalla las tareas para configurar que las soluciones de terceros proporcionen el certificado X.590 correspondiente al servidor de conexión de View 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 View Administrator.

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

### Procedimiento

- 1 Crear un autenticación SAML para el equilibrador de carga o la puerta de enlace de terceros.  
Consulte [Configurar un autenticador SAML en View Administrator](#).
- 2 Amplíe el período de caducidad de los metadatos del servidor de conexión de View 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 de View](#).
- 3 Si es necesario, configure el dispositivo de terceros para usar los metadatos del proveedor del servicio desde el servidor de conexión de View.  
  
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 el nombre principal de usuario (UPN), las cuentas de Active Directory de usuarios y administradores que usan tarjetas inteligentes para autenticarse en View 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 el nombre principal de usuario (UPN), las cuentas de Active Directory de usuarios y administradores que usan tarjetas inteligentes para autenticarse en View 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"> <li>a Seleccione <b>Inicio &gt; Todos los programas &gt; Herramientas administrativas &gt; Usuarios y equipos de Active Directory</b>.</li> <li>b Haga clic con el botón secundario en el dominio y, a continuación, en <b>Propiedades</b>.</li> <li>c En la pestaña <b>Directiva de grupo</b>, haga clic en <b>Abrir</b> para abrir el complemento Administración de directivas de grupo.</li> <li>d Haga clic con el botón secundario en <b>Directiva predeterminada de dominio</b> y seleccione <b>Editar</b>.</li> </ol>
Windows 2008	<ol style="list-style-type: none"> <li>a Seleccione <b>Inicio &gt; Herramientas administrativas &gt; Administración de directivas de grupo</b>.</li> <li>b Expanda el dominio, haga clic con el botón secundario en <b>Directiva predeterminada de dominio</b> y, a continuación, en <b>Editar</b>.</li> </ol>

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

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

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

## Verificar la configuración de la autenticación con tarjeta inteligente

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

### Procedimiento

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

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

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

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

- ◆ En el archivo `locked.properties` que se encuentra en el host del servidor de seguridad o del servidor de conexión de View, 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 de View, compruebe la opción de autenticación con tarjeta inteligente en View Administrator.

- a Seleccione **Configuración de View > Servidores**.
- b En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión de View y haga clic en **Editar**.
- c Si configuró la autenticación con tarjeta inteligente para los usuarios, en la pestaña **Autenticación**, compruebe que la opción **Autenticación de tarjeta inteligente para los usuarios** esté configurada como **Opcional** o **Requerido**.
- d Si configuró la autenticación por tarjeta inteligente para los administradores, en la pestaña **Autenticación**, compruebe que la opción **Autenticación de tarjeta inteligente para los administradores** esté configurada como **Opcional** o **Requerido**.

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

- ◆ Si el dominio en el que reside un usuario de tarjeta inteligente es diferente del dominio que expidió el certificado raíz, compruebe que la UPN del usuario se estableció en el SAN que se encuentra en el certificado raíz de la CA de confianza.
  - a Consulte las propiedades del certificado para buscar el SAN que se encuentra en el certificado raíz de la CA de confianza.
  - b En el servidor de Active Directory, seleccione **Inicio > Herramientas administrativas > Usuarios y equipos de Active Directory**.
  - c Haga clic con el botón secundario en la carpeta **Usuarios** y seleccione **Propiedades**.

Aparece la UPN en los cuadros de texto **Nombre de inicio de sesión de usuario** en la pestaña **Cuenta**.

- ◆ Si un usuario de tarjeta inteligente selecciona el protocolo de visualización PCoIP o el protocolo de visualización VMware Blast para conectarse a escritorios de sesión única, compruebe que View Agent o el componente Horizon Agent denominado Redireccionamiento de tarjeta inteligente se encuentre instalado en los equipos de los usuarios únicos. La función de tarjeta inteligente permite a los usuarios iniciar sesión en los escritorios de sesión única con las tarjetas inteligentes. Los hosts RDS, que tienen instalada la función Servicios de Escritorio remoto, admiten la función de tarjeta inteligente automáticamente y no es necesario que la instale.
- ◆ Compruebe los archivos de registro que se encuentran en *unidad:* \Documents and Settings\All Users\Application Data\VMware\VDM\logs en el host del servidor de seguridad o del servidor de conexión de View 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.

View admite la comprobación de revocación de certificados con listas de revocación de certificados (CRL) y con el protocolo de estado de certificado en línea (OCSP). Una CRL es una lista de certificados revocados publicada por la autoridad de certificación 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 de View o en un servidor de seguridad. Cuando una instancia del servidor de conexión de View 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 de View o del servidor de seguridad.

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

### ■ [Iniciar sesión con la comprobación de CRL](#)

Cuando configure la comprobación de CRL, View construye y lee un 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, View envía una solicitud a un respondedor OCSP para determinar el estado de revocación de un certificado de un usuario específico. View usa un certificado firmado por OCSP para verificar que las respuestas que reciba del respondedor OCSP son originales.

- [Configurar comprobación de CRL](#)

Cuando configure la comprobación de CRL, View lee un 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, View 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, View construye y lee un 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. Los mismos eventos suceden si View no puede leer CRL.

## Iniciar sesión con la comprobación de revocación del certificado OCSP

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

View 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, View lee un 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 SSL en el host del servidor de seguridad o el servidor de conexión de View.

Por ejemplo: `install_directory\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 de View 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, View 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 SSL en el host del servidor de seguridad o el servidor de conexión de View.

Por ejemplo: `install_directory\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 de View 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=longa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.longa.int/ocsp
```

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

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

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

Propiedad	Descripción
<code>enableRevocationChecking</code>	<p>Establezca esta propiedad en <b>true</b> para habilitar la comprobación de la revocación del certificado.</p> <p>Cuando esta propiedad está establecida en <b>false</b>, 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 <b>false</b>.</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, View usa la lista de CRL del certificado de usuario si el valor de <code>allowCertCRLs</code> está establecido en <b>true</b> o no está especificado.</p> <p>Si View 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 <b>true</b>, View extrae una lista de CRL del certificado de usuario.</p> <p>El valor predeterminado es <b>true</b>.</p>
<code>enableOCSP</code>	<p>Establezca esta propiedad en <b>true</b> para permitir la comprobación OCSP de la revocación del certificado.</p> <p>El valor predeterminado es <b>false</b>.</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. View usa este certificado para verificar que las respuestas del respondedor OCSP sean originales.
<code>ocspSendNonce</code>	<p>Cuando esta propiedad se establece en <b>true</b>, se envía un nonce con las solicitudes OCSP para evitar que se repitan las respuestas.</p> <p>El valor predeterminado es <b>false</b>.</p>
<code>ocspCRLFailover</code>	<p>Cuando esta propiedad está establecida en <b>true</b>, View usa la comprobación CRL si se produce un error en la comprobación de la revocación del certificado OCSP.</p> <p>El valor predeterminado es <b>true</b>.</p>

# Configurar otros tipos de autenticación de usuario

# 4

View utiliza su infraestructura existente de Active Directory para la administración y la autenticación de los usuarios y los administradores. También puede integrar View 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 View para que obligue a los usuarios a utilizar una autenticación RSA SecurID o una autenticación 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.
- View también proporciona una interfaz abierta de extensión estándar para permitir a los proveedores de soluciones de terceros integrar extensiones de autenticación avanzada en View.

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 estén accesibles para el host del servidor de conexión de View. 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 de View, 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.

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

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

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

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

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

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

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

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

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

## Iniciar sesión usando la autenticación en dos fases

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

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

- Si RSA Authentication Manager necesita que los usuarios introduzcan un nuevo PIN de RSA SecurID después de introducir el nombre de usuario y el código de acceso de RSA SecurID, aparece un cuadro de diálogo de PIN. Después de configurar un nuevo PIN, se solicita a los usuarios que esperen al siguiente código de token antes de iniciar sesión. Si RSA Authentication Manager está configurado para usar los PIN generados por el sistema, aparece un cuadro de diálogo para confirmar el PIN.
- Cuando inicie sesión en View, la autenticación RADIUS funciona de forma semejante a RSA SecurID. Si el servidor de RADIUS muestra un desafío de acceso, Horizon Client muestra un cuadro

de diálogo similar a la solicitud de RSA SecurID para el siguiente código de token. La compatibilidad actual de los desafíos de RADIUS está limitada para solicitar de entrada de texto. No se muestran los textos de desafío enviado desde el servidor RADIUS. Actualmente no se admiten formas más complejas de desafíos, como varias opciones o selección de imágenes.

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

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

## Habilitar una autenticación en dos fases en View Administrator

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

### Requisitos previos

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

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

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione el servidor y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, acceda a la lista desplegable **Autenticación en dos fases** de la sección Autenticación avanzada y seleccione **RSA SecurID** o **RADIUS**.

- 4 Para forzar que los nombres de usuario de RSA SecurID o RADIUS coincidan con los nombres de usuario en Active Directory, seleccione **Exigir que los nombres de usuario de SecurID y Windows coincidan** u **Obligar a la autenticación en dos fases y la coincidencia de nombre de usuario de Windows**.

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

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

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

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

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

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

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

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

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

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

No es necesario reiniciar el servicio del servidor de conexión de View. 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 de View, 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 de View y desea configurar la autenticación RADIUS en ellas, puede volver a usar una configuración del autenticador RADIUS ya existente.

## Solucionar los problemas de acceso denegado de RSA SecurID

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

### Problema

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

### Causa

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

### Solución

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

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

- 8 Haga clic en **Aceptar**.



## Solucionar los problemas de acceso denegado de RADIUS

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

### Problema

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

### Causa

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

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

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

## Uso de la autenticación SAML

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

Puede usar la autenticación SAML para integrar View con VMware Workspace Portal, con VMware Identity Manager o con una puerta de enlace o un equilibrador de carga de terceros. 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 Portal, VMware Identity Manager o un dispositivo de terceros, debe crear un autenticador SAML en View. Un autenticación SAML contiene el intercambio de metadatos y la confianza entre View y Workspace Portal, VMware Identity Manager o el dispositivo de terceros. Se asocia un autenticador SAML con una instancia del servidor de conexión de View.

## Utilizar la autenticación SAML para integrar VMware Identity Manager

La integración entre View y VMware Identity Manager (anteriormente Workspace Portal) se realiza con el estándar SAML 2.0 a fin de establecer la confianza mutua requerida para la función de inicio de sesión único (Single Sign-On, SSO). Al habilitar SSO, los usuarios que inician sesión en VMware Identity

Manager o Workspace Portal 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 View 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 de View 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 de View. La instancia del servidor de conexión de View utiliza el artefacto para recuperar la aserción SAML de VMware Identity Manager.

Tras recibir la aserción SAML, la instancia del servidor de conexión de View 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 View supone configurar VMware Identity Manager con información de View y configurar View 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 View. Un autenticador de SAML incluye el intercambio de confianza y metadatos entre View y VMware Identity Manager. Se asocia un autenticador SAML con una instancia del servidor de conexión de View.

---

**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 View Administrator. Si proporciona al usuario la función Administradores en un grupo de acceso diferente al raíz, VMware Identity Manager no reconocerá el autenticador SAML que configuró en View y no podrá configurar el grupo en VMware Identity Manager.

---

## Configurar un autenticador SAML en View Administrator

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

Se asocia un autenticador SAML con una instancia del servidor de conexión de View. Si la implementación incluye más de una instancia del servidor de conexión de View, 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 Access Point (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 de View 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 de View 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 Access Point, consulte *Implementación y configuración de Access Point*.

### Requisitos previos

- Compruebe que Workspace Portal, 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 *ViewInstalación*.
- Anote el FQDN o la dirección IP de los servidores de Workspace Portal, de VMware Identity Manager o el equilibrador de carga externo.
- Si usa Workspace Portal o VMware Identity Manager, anote la URL de la interfaz web del conector.
- Si crea un autenticador para Access Point 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 View Administrator, seleccione **Configuración > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione una instancia del servidor para asociarla al autenticador SAML y haga clic en **Editar**.
- 3 En la pestaña **Autenticación**, seleccione un valor del menú desplegable **Delegación de la autenticación a VMware Horizon (autenticador SAML 2.0)** para habilitar o deshabilitar el autenticador SAML.

Opción	Descripción
<b>Deshabilitada</b>	La autenticación SAML está deshabilitada. Solo se pueden iniciar aplicaciones y escritorios remotos desde Horizon Client.
<b>Permitida</b>	La autenticación SAML está habilitada. Puede iniciar aplicaciones y escritorios remotos para Horizon Client y VMware Identity Manager o el dispositivo de terceros.
<b>Obligatoria</b>	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 View 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
<b>Tipo</b>	Para Access Point o un dispositivo de terceros, seleccione <b>Estático</b> . Para VMware Identity Manager, seleccione <b>Dinámico</b> . Para los autenticadores dinámicos, puede especificar una URL de metadatos y una URL de administración. Para los autenticadores estáticos, debe generar en primer lugar los metadatos de Access Point o de un dispositivo de terceros, copie los metadatos y, a continuación, péguelos en el cuadro de texto <b>Metadatos SAML</b> .
<b>Etiqueta</b>	Nombre único que identifica al autenticador SAML.
<b>Descripción</b>	Breve descripción del autenticador SAML. Este valor es opcional.
<b>URL de metadatos</b>	(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 de View. En la URL <code>https://&lt;NOMBRE DEL HORIZON SERVER&gt;/SAAS/API/1.0/GET/metadata/idp.xml</code> , haga clic en <b>&lt;NOMBRE DEL HORIZON SERVER&gt;</b> y reemplace el FQDN o la dirección IP del servidor de VMware Identity Manager o el equilibrador de carga externo (dispositivo de terceros).
<b>URL de administración</b>	(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.
<b>Metadatos SAML</b>	(Para autenticadores estáticos) Texto de metadatos que generó y copió desde Access Point o de un dispositivo de terceros.
<b>Habilitado para el servidor de conexión</b>	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 View y VMware Identity Manager o el dispositivo de terceros.

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

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

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

## Pasos siguientes

Amplíe el período de caducidad de los metadatos del servidor de conexión de View 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 de View](#).

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

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

Utilice este procedimiento para especificar el número de días que pueden transcurrir para que el servidor de conexión de View 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 de View generará metadatos con un período de caducidad de 90 días.

### Requisitos previos

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

### Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión de View.
- 2 En el árbol de la consola, seleccione la opción **Conectar a**.
- 3 En el cuadro de texto para **seleccionar o escribir un nombre distinguido o el contexto de nomenclatura**, escriba el nombre distinguido **DC=vdi**, **DC=vmware**, **DC=int**.
- 4 En el panel del equipo, seleccione o escriba **localhost:389** o bien el nombre de dominio plenamente cualificado (FQDN) del host del servidor de conexión de View 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=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

En este ejemplo, *number-of-days* es el número de días que pueden transcurrir para que un servidor de conexión de View 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 de View 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 de View. Use estos metadatos para crear un proveedor del servicio en el dispositivo de Access Point 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: Access Point o una puerta de enlace o un equilibrador de carga de terceros. En la sección Estado del sistema del panel de información de View Administrator, puede seleccionar **Otros componentes > Autenticadores SAML 2.0**, seleccionar a continuación el autenticador SAML agregado y verificar los detalles.

### Procedimiento

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

**`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 de View.

Esta página muestra los metadatos SAML del servidor de conexión de View.

- 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 de View. Consulte la documentación de Access Point 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 de View y asocia varios autenticadores SAML dinámicos a la instancia del servidor de conexión de View, si alguno de los autenticadores SAML dinámicos se vuelve no accesible, 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 View Administrator para deshabilitar los autenticadores SAML dinámicos que no sean accesibles. Para obtener más información sobre cómo deshabilitar un autenticador SAML, consulte [Configurar un autenticador SAML en View Administrator](#).

## 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 de View.
- 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 plenamente cualificado (FQDN) del host del servidor de conexión de View seguido por el puerto 389.  
Por ejemplo: **localhost:389** o **miequipo.midominio.com:389**
- 4 En el objeto **CN=Common, OU=Global, OU=Properties**, edite el atributo **pae-ClientConfig** y agregue el valor **BioMetricsTimeout=<integer>**.

Los siguientes valores de `BioMetricsTimeout` son válidos:

Valor <code>BioMetricsTimeout</code>	Descripción
<b>0</b>	La autenticación biométrica no es compatible. Este es el valor predeterminado.
<b>-1</b>	La autenticación biométrica es compatible sin ningún límite de tiempo.
<b>Cualquier entero positivo</b>	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 de View ni el dispositivo cliente.

# Autenticar usuarios sin solicitar las credenciales

## 5

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

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

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

Este capítulo incluye los siguientes temas:

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



## Proporcionar acceso sin autenticar para las aplicaciones publicadas

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

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

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

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

### Flujo de trabajo para configurar usuarios sin autenticar

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

### Reglas y directrices para configurar usuarios sin autenticar

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

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

## Crear usuarios con acceso sin autenticar

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

### Requisitos previos

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

---

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

---

### Procedimiento

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

## 5 (opcional) Introduzca el alias del usuario.

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

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

## 7 Haga clic en **Finalizar**.

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

### Pasos siguientes

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

## Habilitar el acceso sin autenticar para los usuarios

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

### Procedimiento

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

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

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

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

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

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

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

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

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

#### 8 Haga clic en **Aceptar**.

### Pasos siguientes

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

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

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

### Requisitos previos

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

### Procedimiento

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

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

### Pasos siguientes

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

## Buscar sesiones con acceso sin autenticar

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

### Procedimiento

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

### 3 Seleccione los criterios e inicie la búsqueda.

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

## Eliminar un usuario con acceso sin autenticar

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

---

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

---

### Procedimiento

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

### Pasos siguientes

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

## Acceso sin autenticar desde Horizon Client

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

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

### Requisitos previos

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

### Procedimiento

- 1 Inicie Horizon Client.
- 2 En Horizon Client, seleccione **Iniciar sesión de forma anónima con Acceso sin autenticar**.

- 3 Conéctese a la instancia del servidor de conexión.
- 4 Seleccione un alias de usuario desde el menú desplegable y haga clic en **Inicio de sesión**.  
El usuario predeterminado tiene el sufijo "predeterminado".
- 5 Haga doble clic en una aplicación publicada para iniciar la aplicación.

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

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

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

- En la instancia del servidor de conexión de View, las credenciales del usuario están cifradas y se almacenan en la sesión del usuario junto al nombre de usuario, dominio y la 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 View ni en el archivo de disco.
- En el sistema cliente, las credenciales del usuario se cifran y se almacenan en una tabla del paquete de autenticación, que es un componente de Horizon Client. Las credenciales se agregan a la tabla cuando el usuario inicia sesión y se eliminan de la tabla cuando cierra sesión. La tabla se encuentra en una memoria volátil.

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

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

- Cuando una autenticación con tarjeta inteligente se establece como obligatoria en una instancia del servidor de conexión de View, 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 de View. Estos usuarios se deben volver a autenticar con la tarjeta inteligente y el PIN cuando inicien sesión en el servidor de conexión de View.
- La hora del sistema en el que el cliente inicia sesión y la hora en el host del servidor de conexión de View 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 de View sin establecer en primer lugar una conexión VPN, se le solicitan las credenciales y la función Iniciar sesión como usuario actual no funciona.

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

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

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

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

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

---

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

---

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

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

### Requisitos previos

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

## Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión de View.
- 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 plenamente cualificado (FQDN) del host del servidor de conexión de View seguido por el puerto 389.  
Por ejemplo: **localhost:389** o **miequipo.midominio.com:389**
- 4 En el objeto **CN=Common, OU=Global, OU=Properties**, edite el valor del atributo **clientCredentialCacheTimeout**.

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

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

## Configurar True SSO

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

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

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

Esta función tiene las siguientes limitaciones:

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

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

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



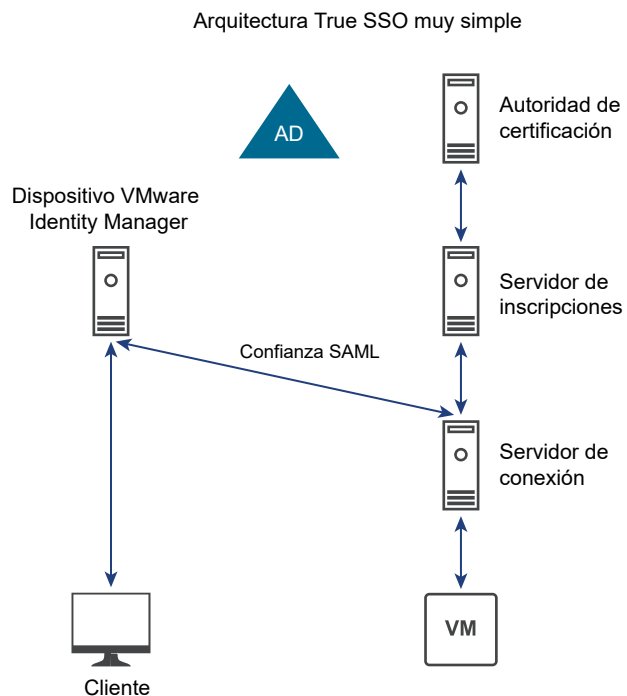
- 5 [Exportar el certificado cliente del servicio de inscripciones](#)
- 6 [Configurar la autenticación SAML para que funcione con True SSO](#)
- 7 [Configurar el servidor de conexión de View para True SSO](#)

## Determinar una arquitectura para True SSO

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

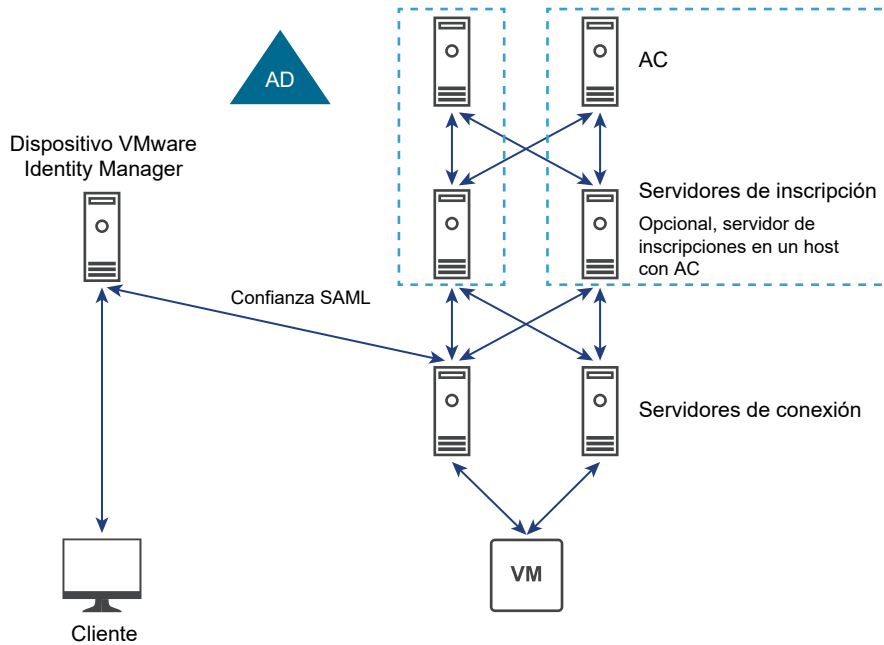
VMware le recomienda tener dos CA y dos servidores de inscripción implementados para usar True SSO. Los siguientes ejemplos muestran True SSO en diferentes arquitecturas.

La siguiente ilustración muestra una arquitectura simple de True SSO.



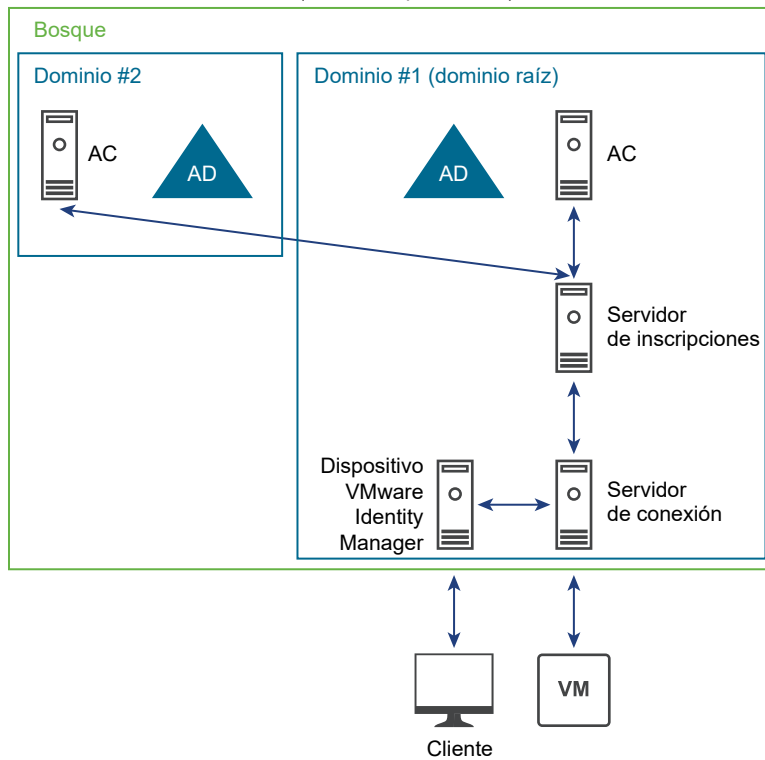
La siguiente ilustración muestra True SSO en una arquitectura de dominio única.

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

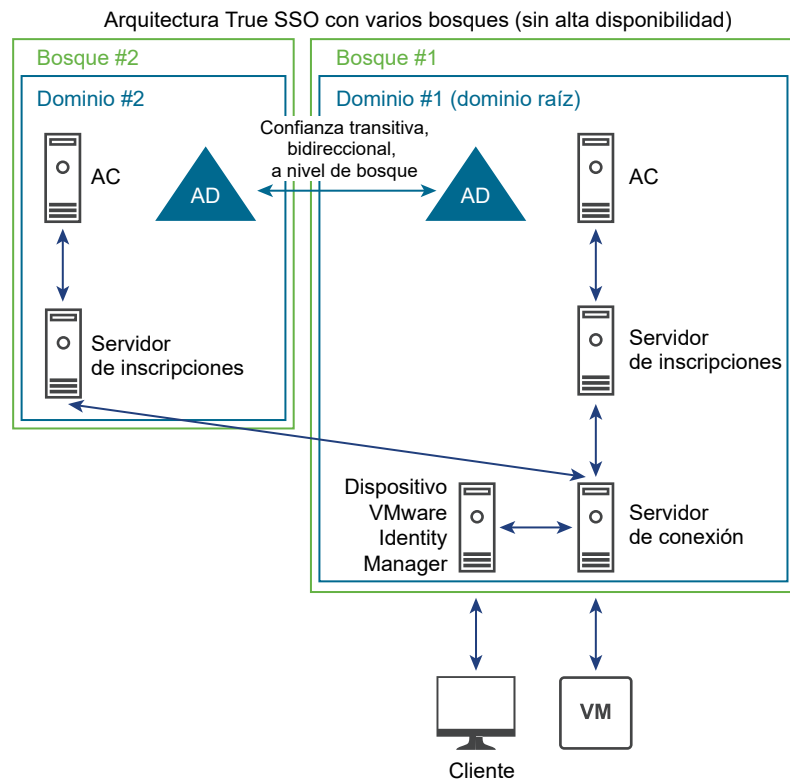


La siguiente ilustración muestra True SSO en una arquitectura de bosque único con varios dominios.

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



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



## Configurar una entidad de certificación empresarial

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

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

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

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

## Requisitos previos

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

## Procedimiento

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

Sistema operativo	Selecciones
Windows Server 2012 R2	a Seleccione <b>Agregar roles y características</b> . b En la página Seleccionar tipo de instalación, seleccione <b>Instalación basada en características o en roles</b> . c En la página Seleccionar servidor de destino, seleccione un servidor.
Windows Server 2008 R2	a Seleccione <b>Funciones</b> en el árbol de navegación. b Haga clic en <b>Agregar funciones</b> para iniciar el asistente <b>Agregar función</b> .

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

Opción	Acción
Servicios de función	Seleccione <b>Entidad de certificación</b> y haga clic en <b>Siguiente</b> (en lugar de <b>Configurar</b> ).
Tipo de instalación	Seleccione <b>CA empresarial</b> .

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

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

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

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

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

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

- 13 Introduzca los siguientes comandos para reiniciar el servicio:

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

### Pasos siguientes

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

## Crear plantillas de certificado para usarlas con True SSO

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

Puede crear más de una plantilla de certificado, pero solo puede configurar que se use una plantilla cada vez.

## Requisitos previos

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

## Procedimiento

- 1 En el equipo que está utilizando para la entidad de certificación, inicie sesión en el sistema operativo como un administrador y diríjase a **Herramientas administrativas > Entidad de certificación**.
- 2 Expanda el árbol que se encuentra en el panel de la izquierda, haga clic con el botón secundario en **Plantillas de certificado** y seleccione **Administrar**.
- 3 Haga clic con el botón secundario en la plantilla **Inicio de sesión de tarjeta inteligente** y seleccione **Duplicar**.
- 4 Realice los siguientes cambios en estas pestañas:

Pestaña	Acción
<b>Pestaña Compatibilidad</b>	<ul style="list-style-type: none"> <li>■ En <b>Entidad de certificación</b>, seleccione <b>Windows Server 2008 R2</b>.</li> <li>■ En <b>Destinatario del certificado</b>, seleccione <b>Windows 7/Windows Server 2008 R2</b>.</li> </ul>
<b>Pestaña General</b>	<ul style="list-style-type: none"> <li>■ Cambie el nombre para mostrar de la plantilla a <b>True SS0</b>.</li> <li>■ Cambie el periodo de validez a un periodo que sea tan amplio como una jornada laboral; es decir, tan amplio como el periodo durante el cual es probable que el usuario tenga la sesión iniciada en el sistema.  Para que el usuario no pierda el acceso a los recursos de la red mientras tiene la sesión iniciada, el periodo de validez debe ser superior al tiempo de renovación TGT de Kerberos en el dominio de los usuarios.  (La duración máxima predeterminada del ticket es 10 horas. Para encontrar la directiva predeterminada del dominio, puede dirigirse a <b>Configuración del equipo &gt; Directivas &gt; Configuración de Windows &gt; Configuración de seguridad &gt; Directivas de cuenta &gt; Directiva Kerberos: Vigencia máxima del vale de usuario</b>.)</li> <li>■ Cambie el periodo de renovación a 1 día.</li> </ul>
<b>Pestaña Tratamiento de la solicitud</b>	<ul style="list-style-type: none"> <li>■ En <b>Propósito</b>, seleccione <b>Firma e inicio de sesión mediante tarjeta inteligente</b>.</li> <li>■ Seleccione <b>Para renovar automáticamente las tarjetas inteligentes, ...</b></li> </ul>
<b>Pestaña Criptografía</b>	<ul style="list-style-type: none"> <li>■ En <b>Categoría del proveedor</b>, seleccione <b>Proveedor de almacenamiento de claves</b>.</li> <li>■ En <b>Nombre de algoritmo</b>, seleccione <b>RSA</b>.</li> </ul>

Pestaña	Acción
Pestaña Servidor	<p>Seleccione <b>No almacenar certificados y solicitudes en la base de datos de CA</b>.</p> <p><b>Importante</b> Asegúrese de que la opción <b>No incluir información de revocación en los certificados emitidos</b> no esté seleccionada. (Este cuadro se selecciona cuando selecciona el primero y tiene que desmarcarlo).</p>
Pestaña Requisitos de emisión	<ul style="list-style-type: none"> <li>■ Seleccione <b>Este nombre de firmas autorizadas</b> y escriba <b>1</b> en el cuadro.</li> <li>■ En <b>Tipo de directiva</b>, seleccione <b>Directiva de aplicación</b> y establezca la directiva en <b>Agente de solicitud de certificados</b>.</li> <li>■ En <b>Requiere lo siguiente para volver a hacer la inscripción</b>, seleccione <b>Certificado existente válido</b>.</li> </ul>
Pestaña Seguridad	<p>En el grupo de seguridad que creó para las cuentas del equipo del servidor de inscripción, como se describe en los requisitos, proporcione los siguientes permisos: Lectura, Inscripción</p> <ul style="list-style-type: none"> <li>a Haga clic en <b>Agregar</b>.</li> <li>b Especifique qué equipos desea permitir que inscriban certificados.</li> <li>c Para estos equipos, seleccione las casillas de verificación apropiadas para proporcionar a los equipos los siguientes permisos: Lectura, Inscripción.</li> </ul>

- 5 Haga clic en **Aceptar** en el cuadro de diálogo Propiedades de plantilla nueva.
- 6 Cierre la ventana Consola de plantillas de certificado.
- 7 Haga clic con el botón secundario en **Plantillas de certificado** y seleccione **Nuevo > Plantilla de certificado que se va a emitir**.

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

- 8 En la ventana Habilitar plantillas de certificados, seleccione la plantilla que acaba de crear (por ejemplo, **Plantilla True SSO**) y haga clic en **Aceptar**.
- 9 En la ventana Habilitar plantillas de certificados, seleccione **Agente de inscripción (equipo)** y haga clic en **Aceptar**.

#### Pasos siguientes

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

## Instalar y configurar un servidor de inscripción

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

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

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

### Requisitos previos

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

### Procedimiento

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



## 2 Expedir un certificado agente de inscripciones:

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

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

## 3 Instale el servidor de inscripciones:

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

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

El nombre del archivo instalador es VMware-viewconnectionserver-x86\_64-y.y.y-xxxxxx.exe, donde xxxxxx es el número de compilación y y.y.y es el número de la versión.

- b Haga doble clic en el archivo instalador para iniciar el asistente y siga las instrucciones hasta llegar a la página Opciones de instalación.
- c En la página Opciones de instalación, seleccione **Servidor de inscripciones de Horizon 7** y haga clic en **Siguiente**.
- d Siga los pasos que se le indican para finalizar la instalación.

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

### Pasos siguientes

- Si instaló el servidor de inscripciones en el mismo equipo que aloja una CA empresarial, configure el servidor de inscripciones para que prefiera usar la CA local. Consulte [Opciones de configuración del servidor de inscripción](#).
- Si instala y configura más de un servidor de inscripciones, configure los servidores de conexión para habilitar el equilibrio de carga entre los servidores de inscripciones. Consulte [Opciones de configuración del servidor de conexión](#).
- Empareje los servidores de conexión con los servidores de inscripciones. Consulte [Exportar el certificado cliente del servicio de inscripciones](#).

## Exportar el certificado cliente del servicio de inscripciones

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

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

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

### Requisitos previos

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

---

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

---

### Procedimiento

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

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

### Pasos siguientes

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

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

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

### Requisitos previos

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

---

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

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

---

### Procedimiento

- 1 Copie el archivo del certificado adecuado para la máquina del servidor de inscripciones.  
  
Para utilizar el certificado generado de forma automática, copie el certificado cliente del servicio de inscripciones del servidor de conexión. Para utilizar su propio certificado, copie el certificado raíz que se utilizó para generar el certificado cliente.

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

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

#### Pasos siguientes

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

## Configurar la autenticación SAML para que funcione con True SSO

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

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

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

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

### Requisitos previos

- Verifique que Single Sign-On está habilitado en la configuración global. En View Administrator, seleccione **Configuración > Configuración global** y compruebe que **Configurar Single Sign-On (SSO)** esté establecido como **Habilitado**.
- Compruebe que VMware Identity Manager esté instalado y configurado. Consulte la documentación de VMware Identity Manager, disponible en [https://www.vmware.com/support/pubs/vidm\\_pubs.html](https://www.vmware.com/support/pubs/vidm_pubs.html)
- Verifique que el certificado raíz de la autoridad de certificación que firma el certificado del servidor SAML esté instalado en el host del servidor de conexión. VMware no recomienda configurar los autenticadores SAML para utilizar certificados autofirmados. Consulte el tema sobre cómo importar un certificado raíz y certificados intermedios en el almacén de certificados de Windows, en el capítulo "Configurar certificados SSL en View Server" del documento *Instalación de View*.
- Anote el FQDN de la instancia del servidor de VMware Identity Manager.

### Procedimiento

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

Cada una de las instancias del servidor de conexión de View 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
<b>Etiqueta</b>	Puede usar el FQDN de la instancia del servidor de VMware Identity Manager.
<b>Descripción</b>	(Opcional) Puede usar el FQDN de la instancia del servidor de VMware Identity Manager.

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

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

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

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

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

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

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

#### Pasos siguientes

- Amplíe el período de caducidad de los metadatos del servidor de conexión de View 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 de View](#).
- Use la interfaz de línea de comandos `vdmutil` para configurar True SSO en un servidor de conexión. Consulte [Configurar el servidor de conexión de View para True SSO](#).

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

## Configurar el servidor de conexión de View para True SSO

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

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

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

### Requisitos previos

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

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

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

### Procedimiento

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

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

El servidor de inscripción se agrega a la lista global.

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

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

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

---

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

---

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

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

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

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

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

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

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

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

---

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

---

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

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

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



## Pasos siguientes

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

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

## Referencia de la línea de comandos para configurar True SSO

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

### Ubicación de la utilidad

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

### Sintaxis y autenticación

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

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

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

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

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

**Tabla 5-1. Opciones de autenticación del comando vdmutil**

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

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

## Salida de comando

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

## Comandos para administrar los servidores de registro

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

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

```
vdmutil --authAs usuario-función-administrador --authDomain nombre-netbios --authPassword contraseña-usuario-administrador --trueoso --environment --list --enrollmentServers
```

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

**Tabla 5-2. Opciones del comando `vdmutil trueoso` para administrar los servidores de inscripción**

Comandos y opciones	Descripción
<code>--environment --add --enrollmentServer <i>fqdn-servidor-inscripción</i></code>	Agrega el servidor de inscripción especificado al entorno, donde <i>fqdn-servidor-inscripción</i> es el FQDN del servidor de inscripción. Si ya se agregó el servidor de inscripción, no ocurre nada al ejecutar este comando.
<code>--environment --remove --enrollmentServer <i>fqdn-servidor-inscripción</i></code>	Elimina el servidor de inscripción especificado del entorno, donde <i>fqdn-servidor-inscripción</i> es el FQDN del servidor de inscripción. Si ya se eliminó el servidor de inscripción, no ocurre nada al ejecutar este comando.
<code>--environment --list --enrollmentServers</code>	Muestra los FQDN de todos los servidores de inscripción del entorno.

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

## Comandos para administrar conectores

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

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

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

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

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

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

## Comandos para administrar autenticadores

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

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

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

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

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

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

## Opciones de configuración avanzadas para True SSO

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

## Opciones de configuración de Horizon Agent

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

**Nota** La siguiente tabla muestra las opciones que se deben usar para configurar el agente en máquinas virtuales individuales, pero puede usar de forma alternativa los archivos de plantilla de configuración de Horizon Agent. El archivo de plantilla ADMX se denomina (`vdm_agent.admx`). El archivo de plantilla ADM se denomina (`vdm_agent.adm`). Use estos archivos de plantilla para aplicar esta configuración de directivas en todas las máquinas virtuales de un grupo de aplicaciones o de escritorios. Si una directiva está configurada, esta tiene preferencia sobre la opción de registro. En la versión 7.1 de Horizon 7, los archivos de plantilla ADM quedan obsoletos y se agregan los archivos de plantilla ADMX.

Los archivos ADMX están disponibles en un archivo de paquete .zip con el nombre VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip, que puede descargar desde el sitio de descargas de VMware en <https://my.vmware.com/web/vmware/downloads>. En el apartado de escritorios y equipos de usuarios finales, seleccione la descarga de VMware Horizon 7, que incluye el archivo de paquete .zip.

**Tabla 5-5. Claves para configurar True SSO en Horizon Agent**

Clave	Mín. y máx.	Descripción
Disable True SSO	No disponible	Establezca esta clave como <b>true</b> para deshabilitar la función en el agente. Use esta opción en la directiva de grupo para deshabilitar True SSO en el nivel de grupo. El valor predeterminado es <b>false</b> .
Certificate wait timeout	10 -120	Especifica el periodo de tiempo de espera de los certificados para llegar al agente, en segundos. El valor predeterminado es <b>40</b> .
Minimum key size	1024 - 8192	Tamaño mínimo permitido para una clave. El valor predeterminado es <b>1024</b> , lo que supone que, de forma predeterminada, sin el tamaño de la clave es inferior a 1024, esta no se puede utilizar.
All key sizes	No disponible	Lista separada por comas de los tamaños de clave que se pueden usar. Se pueden especificar hasta 5 tamaños, por ejemplo: <b>1024,2048,3072,4096</b> . El valor predeterminado es <b>2048</b> .
Number of keys to pre-create	1-100	Número de claves que se crean previamente en servidores RDS que proporcionan escritorios remotos y aplicaciones alojadas en Windows. El valor predeterminado es <b>5</b> .
Minimum validity period required for a certificate	No disponible	Periodo de validez mínimo, en minutos, que necesita un certificado cuando se vuelve a usar para reconectar un usuario. El valor predeterminado es <b>5</b> .

## Opciones de configuración del servidor de inscripción

Puede usar la configuración del Registro de Windows en el SO del servidor de inscripción para configurar los dominios a los que conectarse, varios periodos de tiempo de espera, periodos de sondeo, reintentos y si prefiere usar la entidad de certificación que está instalada en el mismo servidor local (recomendado).

Para cambiar las opciones de configuración avanzada, puede abrir el Editor del Registro de Windows (regedit.exe) en el equipo del servidor de inscripción y dirigirse a la siguiente clave de registro:

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

**Tabla 5-6. Claves de registro para configurar TrueSSO en el servidor de registro**

Clave del registro	Mín. y máx.	Tipo	Descripción
ConnectToDomains	No disponible	REG_MULTI_SZ	<p>Lista de dominios a los que el servidor de inscripción intenta conectarse automáticamente. Para este tipo de registro de varias cadenas, el nombre de dominio completo DNS (FQDN) de cada dominio aparece en su propia línea.</p> <p>El comportamiento predeterminado es confiar en todos los dominios.</p>
ExcludeDomains	No disponible	REG_MULTI_SZ	<p>Lista de dominios a los que el servidor de inscripción no se conecta automáticamente. Si el servidor de conexión proporciona un conjunto de configuraciones con cualquier dominio, el servidor de inscripción intentará conectarse a ese dominio o esos dominios. Para este tipo de registro de varias cadenas, el FQDN DNS de cada dominio aparece en su propia línea.</p> <p>El comportamiento predeterminado es no excluir a ningún dominio.</p>
ConnectToDomainsInForest	No disponible	REG_SZ	<p>Especifica si se conecta a todos los dominios y los usa en el bosque del que el servidor de inscripción es miembro. El valor predeterminado es TRUE.</p> <p>Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ 0 significa false, no se conecta a los dominios del bosque que se está utilizando.</li> <li>■ !=0 significa true.</li> </ul>
ConnectToTrustingDomains	No disponible	REG_SZ	<p>Especifica si se conecta a dominios entrantes o de confianza explícitamente. El valor predeterminado es TRUE.</p> <p>Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ 0 significa false, no se conecta a los dominios entrantes o de confianza explícitamente.</li> <li>■ !=0 significa true.</li> </ul>
PreferLocalCa	No disponible	REG_SZ	<p>Especifica si prefiere la CA que se encuentra en las instalaciones, en caso de que esté disponible, para obtener beneficios en el rendimiento. Si está establecido como TRUE, el servidor de inscripción enviará solicitudes a la CA local. Si se produce un error en la conexión a la CA, el servidor de inscripción intentará enviar solicitudes de certificados a CA alternativas. El valor predeterminado es FALSE (falso).</p> <p>Utilice uno de los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ 0 significa false.</li> <li>■ !=0 significa true.</li> </ul>

Clave del registro	Mín. y máx.	Tipo	Descripción
MaxSubmitRetryTime	9500-59000	DWORD	Cantidad de tiempo que se debe esperar antes de volver a intentar enviar una solicitud de firma del certificado, en milisegundos. El valor predeterminado es <b>25000</b> .
SubmitLatencyWarningTime	500 - 5000	DWORD	Envía el tiempo de advertencia de latencia cuando la interfaz está marcada como "Degradada" (en milisegundos). El valor predeterminado es <b>1500</b> .  El servidor de inscripción usa esta opción para determinar si se debe considerar que una CA esté en estado degradado. Si las últimas tres solicitudes de certificado tardaron en completarse más milisegundos de los especificados por esta opción, la CA se considera degradada y este estado aparece en el panel de control de estado de View Administrator.  Una CA suele expedir un certificado en 20 ms, pero si la CA estuvo inactiva durante algunas horas, cualquier solicitud inicial puede tardar más tiempo en completarse. Esta opción permite a un administrador descubrir que una CA es lenta, sin necesidad de tenerla marcada como tal. Use esta opción para configurar el umbral que marca la CA como lenta.

## Opciones de configuración del servidor de conexión

Puede editar el LDAP de View en el servidor de conexión de View si desea configurar un tiempo de espera para generar los certificados y si desea habilitar las solicitudes del certificado de equilibrio de carga entre los servidores de inscripción (recomendado).

Para cambiar las opciones de configuración avanzada, debe usar el Editor ADSI en el host del servidor de conexión de View. Puede conectarse escribiendo el nombre distintivo **DC=vdi**, **DC=vmware**, **DC=int** como el punto de conexión e introduciendo **localhost:389** en el puerto y el nombre del servidor. Amplíe **OU=Properties**, seleccione **OU=Global** y haga doble clic en **OU=Common** en el panel derecho.

Puede editar el atributo **pae-NameValuePair** para agregar uno o varios de los valores que aparecen en la siguiente tabla. Debe usar la sintaxis **nombre=valor** al agregar los valores.

**Tabla 5-7. Configuración avanzada de True SSO para los servidores de conexión**

Clave del registro	Descripción
cs-view-certsso-enable-es-loadbalance=[true false]	Especifica si habilitar las solicitudes CSR de equilibrio de carga entre dos servidores de inscripción. El valor predeterminado es false (falso).  Por ejemplo, agregue <b>cs-view-certsso-enable-es-loadbalance=true</b> para habilitar el equilibrio de carga de forma que, si llegan las solicitudes del certificado, el servidor de conexión usará servidores de inscripción alternativos. Cada servidor de inscripción puede atender a las solicitudes usando la CA local, en caso de tener el servidor de inscripción y la CA en el mismo host.
cs-view-certsso-certgen-timeout-sec=número	Cantidad de tiempo, en segundos, que se debe esperar para generar un certificado después de recibir un CSR. El valor predeterminado es <b>35</b> .



## Uso del panel de control del estado del sistema para solucionar problemas relacionados con True SSO

Puede usar el panel de control del estado del sistema en View Administrator para identificar rápidamente los problemas que puedan afectar la operación de la función True SSO.

Para los usuarios finales, si True SSO deja de funcionar, cuando el sistema intenta iniciar la sesión del usuario en la aplicación o el escritorio remotos, el usuario ve el siguiente mensaje: "El nombre de usuario o la contraseña es incorrecto." Después de que el usuario haga clic en **Aceptar**, aparece la pantalla de inicio de sesión. En la pantalla de inicio de sesión de Windows, el usuario ve un icono adicional denominado **Usuario SSO de VMware**. Si el usuario tiene las credenciales de Active Directory de un usuario con autorización, puede iniciar sesión con las credenciales de AD.

El panel de control del estado del sistema situado en la parte superior izquierda de la ventana de View Administrator muestra varios elementos que pertenecen a True SSO.

---

**Nota** La función True SSO proporciona información al panel de control una vez por minuto. Haga clic en el icono de actualización situado en la esquina superior derecha para actualizar la información inmediatamente.

---

- Puede hacer clic para expandir **Componentes de View > True SSO** para ver una lista de los dominios que usan True SSO.

Puede hacer clic en un nombre de dominio para ver la siguiente información: una lista de servidores de inscripciones configurados para dicho dominio, una lista de entidades de certificación empresarial, el nombre de la plantilla del certificado que se está utilizando y el estado. Si hay algún problema, el campo Estado explica cuál es.

Para cambiar las opciones de configuración que aparecen en el cuadro de diálogo Detalles del dominio True SSO, use la interfaz de línea de comandos `vdmtutil` para editar el conector True SSO. Si desea obtener más información, consulte [Comandos para administrar conectores](#).

- Puede hacer clic para expandir **Otros componentes > Autenticadores SAML 2.0** para ver una lista de autenticadores SAML que se crearan para delegar la autenticación a las instancias de VMware Identity Manager. Puede hacer clic en el nombre del autenticador para examinar los detalles y el estado.

---

**Nota** Para usar True SSO, se debe habilitar la opción global para SSO. En View Administrator, seleccione **Configuración > Configuración global** y compruebe que **Configurar Single Sign-On (SSO)** esté establecido como **Habilitado**.

---

**Tabla 5-8. Agente del estado de conexión del servidor de inscripciones**

Texto del estado	Descripción
No se pudo recuperar la información de estado de True SSO.	El panel de control no puede recuperar la información del estado desde el agente.
El servicio de configuración True SSO no puede contactar con el servidor de inscripción <FQDN>.	En un POD, uno de los agentes se selecciona para enviar la información de configuración a todos los servidores de inscripciones que usa el POD. Este agente actualizará la configuración del servidor de inscripciones una vez por minuto. Este mensaje aparece si la tarea de configuración no pudo actualizar el servidor de inscripciones. Para obtener más información, consulte la tabla Conectividad del servidor de inscripciones.
No se puede contactar con el servidor de inscripción <FQDN> para administrar las sesiones en este servidor de conexión.	El agente actual no puede conectarse al servidor de inscripciones. Este estado solo aparece para el agente al que el navegador se dirige. Si existen varios agentes en el pod, es necesario que cambie el navegador para que se dirija a otros agentes para comprobar sus estados. Para obtener más información, consulte la tabla Conectividad del servidor de inscripciones.

**Tabla 5-9. Conectividad del servidor de inscripciones**

Texto del estado	Descripción
Este dominio <Nombre dominio> no existe en el servidor de inscripciones <FQDN>.	El conector True SSO se configuró para usar este servidor de inscripciones en este dominio, pero aún no se configuró este servidor para que se conecte al dominio. Si el estado se mantiene durante más de un minuto, es necesario que compruebe el estado del agente responsable de actualizar la configuración de las inscripciones.
La conexión del servidor de inscripción de <FQDN> al dominio <Nombre dominio> aún se está estableciendo.	El servidor de inscripciones no se pudo conectar a un controlador de este dominio. Si este estado se mantiene durante más de un minuto, tiene que verificar que la resolución del nombre del servidor de inscripciones al dominio sea correcta y que exista una conectividad de red entre el servidor de inscripciones y el dominio.
La conexión del servidor de inscripción de <FQDN> al dominio <Nombre dominio> se está deteniendo o está en un estado problemático.	El servidor de inscripciones se conectó a un controlador de dominio, pero no puede leer la información PKI de este controlador. Si esto sucede, es posible que haya un problema con el controlador del dominio actual. Este problema también puede suceder si DNS no está configurado correctamente. Revise el archivo de registro del servidor de inscripciones para ver el controlador de dominio que el servidor de inscripciones está intentando usar y compruebe que el controlador de dominio esté totalmente operativo.
El servidor de inscripción <FQDN> no leyó aún las propiedades de inscripción de ningún controlador de dominio.	Este es un estado de transición y solo se muestra durante el inicio del servidor de inscripciones o cuando se agrega un nuevo dominio al entorno. Este estado suele durar menos de un minuto. Si dura más, puede ser que la red sea muy lenta o que exista un problema que no permita acceder correctamente al controlador del dominio.

Texto del estado	Descripción
El servidor de inscripción <FQDN> leyó las propiedades de inscripción al menos una vez, pero no pudo acceder a un controlador de dominio durante un tiempo.	Mientras el servidor de inscripciones lea la configuración PKI desde un controlador de dominio, se mantiene sondeando los cambios cada dos minutos. Este estado se establecerá si no se puede acceder al controlador de dominio (DC) durante un breve periodo de tiempo. Normalmente, esta situación supone que el servidor de inscripciones no puede detectar ningún cambio en la configuración PKI. Mientras los servidores de certificados puedan acceder a un controlador de dominio, los certificados se pueden seguir expidiendo.
El servidor de inscripción <FQDN> leyó las propiedades de inscripción al menos una vez, pero no pudo acceder a un controlador de dominio durante un largo período de tiempo o existe otro problema.	Si el servidor de inscripciones no puede acceder al controlador de dominio durante un tiempo prolongado, aparece este estado. El servidor de inscripciones intentará encontrar un controlador de dominio alternativo para este dominio. Si un servidor de certificados puede seguir accediendo a un controlador de dominio, los certificados pueden seguir expidiéndose, pero si este estado se mantiene durante más de un minuto, esto significa que el servidor de inscripciones perdió el acceso a todos los controladores del dominio y es posible que no se puedan seguir expidiendo los certificados.

Tabla 5-10. Estado del certificado de inscripción

Texto del estado	Descripción
No hay instalado un certificado de inscripción válido para este bosque <nombre dominio> del dominio en el servidor de inscripción <FQDN> o puede que caducara.	No se instaló ningún certificado de inscripción para este dominio o el certificado no es válido o caducó. Una CA empresarial debe expedir el certificado de inscripción y esta debe ser de confianza para el bosque al que este dominio pertenece. Compruebe que completó los pasos del documento <i>Administración de View</i> , que describe cómo instalar el certificado de inscripción en el servidor de inscripciones. También puede abrir el MMC, el complemento de administración de certificados, abriendo el almacén del equipo local. Abra el contenedor de certificados personales y compruebe que el certificado esté instalado y que sea válido. También puede abrir el archivo de registros del servidor de inscripciones. Los servidores de inscripciones registrarán información adicional sobre el estado de cualquier certificado que esté ubicado.

Tabla 5-11. Estado de plantilla del certificado

Texto del estado	Descripción
La plantilla <nombre> no existe en el dominio del servidor de inscripción <FQDN>.	Compruebe que especificó el nombre de plantilla correcto.
Los certificados generados por esta plantilla NO se pueden usar para iniciar sesión en Windows.	Esta plantilla no tiene habilitados el uso de la tarjeta inteligente ni la firma de datos. Compruebe que especificó el nombre de plantilla correcto. Compruebe que completó los pasos descritos en <a href="#">Crear plantillas de certificado para usarlas con True SSO</a> .
La plantilla <nombre> está habilitada para iniciar sesión con una tarjeta inteligente, pero no se puede utilizar.	Esta plantilla está habilitada para iniciar sesión con una tarjeta inteligente, pero no puede usarse con True SSO. Compruebe que especificara el nombre de la plantilla correcto y compruebe que completó los pasos descritos en <a href="#">Crear plantillas de certificado para usarlas con True SSO</a> . También puede revisar el archivo de registro del servidor de inscripciones, ya que tiene registrada la opción de la plantilla que hace que no se pueda usar con True SSO.

**Tabla 5-12. Estado de configuración del servidor de certificados**

Texto del estado	Descripción
El servidor de certificado <CN de CA> no existe en el dominio.	Compruebe que especificó el nombre correcto de la CA. Debe especificar el Nombre común (CN).
El certificado no está en el almacén NTAUTH (Enterprise).	Esta CA no es empresarial o su certificado no se agregó al almacén NTAUTH. Si esta CA no es miembro del bosque, debe agregar el certificado de la CA manualmente al almacén NTAUTH de este bosque.

**Tabla 5-13. Estado de conexión del servidor de certificados**

Texto del estado	Descripción
El servidor de inscripción <FQDN> no está conectado al servidor de certificados <CN de CA>.	El servidor de inscripción no está conectado al servidor de certificados. Este estado puede ser de transición si el servidor de inscripciones se acaba de iniciar o si la CA se agregó recientemente a un conector True SSO. Si este estado se mantiene durante más de un minuto, esto significa que el servidor de inscripciones no se pudo conectar a la CA. Valide que la resolución del nombre esté funcionando correctamente, que tenga conectividad de red a la CA y que la cuenta del sistema para el servidor de inscripciones tenga permiso para acceder a la CA.
El servidor de inscripción <FQDN> se conectó al servidor de certificados <CN of CA>, pero este está en estado degradado.	<p>Este estado se muestra si la CA expide certificados a un ritmo lento. Si la CA se mantiene en este estado, compruebe su carga o los controladores de dominio que usan la CA.</p> <p><b>Nota</b> Si la CA se marcó como lenta, mantendrá este estado hasta que se complete al menos una solicitud de certificado correctamente y se expida dentro de un intervalo de tiempo normal.</p>
El servidor de inscripción <FQDN> se puede conectar al servidor de certificados <CN de CA>, pero el servicio no está disponible.	Este estado se expide si el servidor de inscripciones tiene una conexión activa a la CA pero no puede expedir certificados. Este suele ser un estado de transición. Si la CA no vuelve a estar disponible rápidamente, el estado cambiará a desconectado.

# Configurar la administración delegada basada en funciones

# 6

Una tarea de administración clave en un entorno de View es determinar quién puede usar View Administrator y las tareas para las que esos usuarios tienen autorización. Con la administrador delegada basada en funciones, puede asignar de forma selectiva los derechos administrativos al designar funciones de administrador para grupos y usuarios específicos de Active Directory.

Este capítulo incluye los siguientes temas:

- [Comprender las funciones y los privilegios](#)
- [Uso de grupos de acceso para delegar la administración de grupos y granjas](#)
- [Comprender los permisos](#)
- [Administrar administradores](#)
- [Administrar y consultar los permisos](#)
- [Administrar y consultar los grupos de acceso](#)
- [Administrar funciones personalizadas](#)
- [Funciones y privilegios predefinidos](#)
- [Privilegios necesarios para las tareas comunes](#)
- [Prácticas recomendadas para grupos y usuarios administradores](#)

## Comprender las funciones y los privilegios

La capacidad para realizar tareas en View Administrator se rige por un sistema de control de acceso que consta de los 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 View Administrator. Por ejemplo, si un administrador no tiene privilegios para ver o modificar directivas, la opción **Directivas globales** no aparece visible en el panel de navegación cuando el administrador inicia sesión en View Administrator.

Los privilegios de administrador pueden ser globales o específicos de objeto. Los privilegios globales controlan las operaciones de todo el sistema, como ver y cambiar la configuración global. Los privilegios específicos de objeto controlan las operaciones de determinados tipos de objetos.

Las funciones de administrador suelen combinar todos los privilegios individuales necesarios para realizar una tarea de administración de nivel superior. View Administrator incluye funciones predefinidas que contienen los privilegios necesarios para realizar tareas de administración comunes. Puede asignar estas funciones predefinidas a los grupos y a los usuarios administradores, o bien puede crear sus propias funciones combinando los privilegios seleccionados. Estas funciones no se pueden modificar.

Para crear administradores, seleccione los grupos y los usuarios de los que tiene en Active Directory y asigne funciones de administrador. Los administradores obtienen privilegios gracias a las asignaciones de funciones. No puede asignar los privilegios directamente a los administradores. Un administrador que tenga varias asignaciones de funciones adquiere la suma de todos los privilegios contenidos en esas funciones.

## Uso de grupos de acceso para delegar la administración de grupos y granjas

De forma predeterminada, los grupos de escritorios automáticos, los grupos de escritorios manuales y las granjas se crean en el grupo de acceso raíz, que aparece como / o Raíz(/) en View Administrator. Los grupos de aplicaciones y los grupos de escritorios RDS 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 escritorios RDS o un grupo de aplicaciones directamente. Debe cambiar el grupo de acceso de la granja a la que pertenecen el grupo de escritorios RDS o el grupo de aplicaciones.

---

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 View Administrator para crear grupos de acceso y para mover los grupos de escritorios existentes a los grupos de acceso. Cuando cree un grupo de escritorios automático, un grupo manual o una granja, puede aceptar el grupo de acceso raíz predeterminado o seleccionar un grupo de acceso diferente.

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

- **Administradores diferentes para grupos de acceso diferentes**

Puede crear un administrador diferente para administrar cada grupo de acceso en la configuración.

- **Administradores diferentes para el mismo grupo de acceso**

Puede crear diferentes administradores para gestionar el mismo grupo de acceso.

## Administradores diferentes para grupos de acceso diferentes

Puede crear un administrador diferente para administrar cada grupo de acceso en la configuración.

Por ejemplo, si los grupos de escritorios empresariales están en un grupo de acceso y los grupos de escritorio de los desarrolladores de software están en otro grupo de acceso, puede crear administradores diferentes para gestionar los recursos en cada grupo de acceso.

**Tabla 6-1. Administradores diferentes para grupos de acceso diferentes** muestra un ejemplo de este tipo de configuración.

**Tabla 6-1. Administradores diferentes para grupos de acceso diferentes**

Administrador	Función	Grupo de acceso
view-domain.com\Admin1	Administradores de inventario	/CorporateDesktops
view-domain.com\Admin2	Administradores de inventario	/DeveloperDesktops

En este ejemplo, el administrador denominado Admin1 tiene la función Administradores de inventario en el grupo de acceso denominado CorporateDesktops y el administrador denominado Admin2 tiene la función Administradores de inventario en el grupo de acceso denominado DeveloperDesktops.

## Administradores diferentes para el mismo grupo de acceso

Puede crear diferentes administradores para gestionar el mismo grupo de acceso.

Por ejemplo, si los grupos de escritorios empresariales están en un grupo de acceso, puede crear un administrador que pueda ver y modificar estos grupos y otro administrador que solo pueda verlos.

**Tabla 6-2. Administradores diferentes para el mismo grupo de acceso** muestra un ejemplo de este tipo de configuración.

**Tabla 6-2. Administradores diferentes para el mismo grupo de acceso**

Administrador	Función	Grupo de acceso
view-domain.com\Admin1	Administradores de inventario	/CorporateDesktops
view-domain.com\Admin2	Administradores de inventario (solo lectura)	/CorporateDesktops

En este ejemplo, el administrador denominado Admin1 tiene la función Administradores de inventario en el grupo de acceso denominado CorporateDesktops y el administrador denominado Admin2 tiene la función Administradores de inventario (solo lectura) en el mismo grupo de acceso.

## Comprender los permisos

View Administrator presenta la combinación de una función, un grupo o usuario administrador y un grupo de acceso como un 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 View Administrator en función de que se seleccione un grupo o un usuario administrador, un grupo de acceso o una función.

[Tabla 6-3. Permisos en la pestaña Administradores y grupos para Admin 1](#) muestra cómo aparecen los permisos en View Administrator cuando selecciona un grupo o un usuario administrador. El usuario administrador se denomina Admin 1 y tiene dos permisos.

**Tabla 6-3. Permisos en la pestaña Administradores y grupos para Admin 1**

Función	Grupo de acceso
Administradores de inventario	MarketingDesktops
Administradores (solo lectura)	/

El primer permiso muestra que Admin 1 tiene la función Administradores de inventario en el grupo de acceso denominado MarketingDesktops. El segundo permiso muestra que Admin 1 tiene la función Administradores (solo lectura) en el grupo de acceso raíz.

[Tabla 6-4. Permisos en la pestaña Carpetas para MarketingDesktops](#) muestra cómo el mismo permiso aparece en View Administrator cuando selecciona el grupo de acceso MarketingDesktops.

**Tabla 6-4. Permisos en la pestaña Carpetas para MarketingDesktops**

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



El primer permiso es igual que el primer permiso que aparece en [Tabla 6-3. Permisos en la pestaña Administradores y grupos para Admin 1](#). El segundo permiso se hereda del que aparece en [Tabla 6-3. 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.

[Tabla 6-5. Permisos en la pestaña Función para Administradores de inventario](#) muestra cómo el primer permiso de [Tabla 6-3. Permisos en la pestaña Administradores y grupos para Admin 1](#) aparece en View Administrator cuando selecciona la función Administradores de inventario.

**Tabla 6-5. Permisos en la pestaña Función para Administradores de inventario**

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

## Administrar administradores

Los usuarios con función de administradores pueden usar View Administrator para agregar o eliminar grupos y usuarios administradores.

La función de administradores es la función con más poder en View Administrator. Los miembros de la cuenta de View Administrator poseen inicialmente la función de administradores. La cuenta de View Administrator se especifica al instalar el servidor de conexión de View. La cuenta de View Administrator puede ser el grupo de administradores local (BUILTIN\Administrators) en el equipo del servidor de conexión de View 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 de View Administrator 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 View, elimine el grupo de administradores del dominio del grupo local de administradores.

### ■ [Crear un administrador](#)

Para crear un administrador, seleccione uno de los grupos y usuarios de Active Directory en View Administrator y asigne una función de administrador.

### ■ [Eliminar un administrador](#)

Puede eliminar un grupo o un usuario administradores. No puede eliminar el último superadministrador del sistema. Un superadministrador es un administrador que tiene la función Administradores en el grupo de acceso raíz.

## Crear un administrador

Para crear un administrador, seleccione uno de los grupos y usuarios de Active Directory en View Administrator y asigne una función de administrador.

## Requisitos previos

- Familiarícese con las funciones de administrador predefinidas. Consulte [Funciones y privilegios predefinidos](#).
- Familiarícese con las prácticas recomendadas para crear grupos e usuarios administradores. Consulte [Prácticas recomendadas para grupos y usuarios administradores](#).
- Para asignar una función personalizada al administrador, cree la función. Consulte [Agregar una función personalizada](#).
- Para crear un administrador que pueda gestionar grupos de escritorios específicos, cree un grupo de acceso y mueva los grupos de escritorios a ese grupo de acceso. Consulte [Administrar y consultar los grupos de acceso](#).

## Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Administradores y grupos**, haga clic en **Agregar usuarios al grupo**.
- 3 Haga clic en **Agregar**, seleccione uno o varios criterios de búsqueda y haga clic en **Buscar** para filtrar los grupos o los usuarios de Active Directory según sus criterios de búsqueda.
- 4 Seleccione el grupo o el usuario de Active Directory que desea que sea el usuario o grupo administrador, haga clic en **Aceptar** y, a continuación, en **Siguiente**.

Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios.

- 5 Seleccione la función que desee asignar al grupo o usuario administrador.

La columna **Se aplica a un grupo de acceso** indica si una función se aplica a los grupos de acceso. Solo las funciones que incluyen privilegios específicos de objeto se aplican a los grupos de acceso. Las funciones que incluyen privilegios específicos de objeto pueden aplicarse a grupos de acceso.

Opción	Acción
La función que seleccionó se aplica a los grupos de acceso	Seleccione uno o varios grupos de acceso y haga clic en <b>Siguiente</b> .
Desea que la función se aplique a todos los grupos de acceso	Seleccione el grupo de acceso raíz y haga clic en <b>Siguiente</b> .

- 6 Haga clic en **Finalizar** para crear el grupo o usuario administrador.

El nuevo grupo o usuario administrador aparece en el panel izquierdo y la función y el grupo de acceso que seleccionó aparecen en el panel derecho de la pestaña **Administradores y grupos**.

## Eliminar un administrador

Puede eliminar un grupo o un usuario administradores. No puede eliminar el último superadministrador del sistema. Un superadministrador es un administrador que tiene la función **Administradores** en el grupo de acceso raíz.

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Administradores y grupos** seleccione el grupo o el usuario administradores, haga clic en **Eliminar usuario o grupo** y haga clic en **Aceptar**.

El grupo o el usuario administradores ya no aparecen en la pestaña **Administradores y grupos**.

## Administrar y consultar los permisos

Puede usar View Administrator para agregar, eliminar y consultar los permisos de los grupos y usuarios administradores específicos, de las funciones específicas y de los grupos de acceso específicos.

### ■ [Agregar un permiso](#)

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

### ■ [Eliminar un permiso](#)

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

### ■ [Revisar los permisos](#)

Es posible revisar los permisos que incluyan a un grupo o un administrador específicos, una función específica o un grupo de acceso específico.

## Agregar un permiso

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

### Procedimiento

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

## 2 Cree el permiso.

Opción	Acción
<b>Crear un permiso que incluya un grupo o un usuario administrador específico</b>	<ul style="list-style-type: none"> <li>a En la pestaña <b>Administradores y grupos</b>, seleccione el administrador o el grupo y haga clic en <b>Agregar permiso</b>.</li> <li>b Seleccione una función.</li> <li>c Si la función no se aplica a los grupos de acceso, haga clic en <b>Finalizar</b>.</li> <li>d Si la función se aplica a los grupos de acceso, haga clic en <b>Siguiente</b>, seleccione uno o varios grupos de acceso y haga clic en <b>Finalizar</b>. Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso.</li> </ul>
<b>Crear un permiso que incluya una función específica</b>	<ul style="list-style-type: none"> <li>a En la pestaña <b>Funciones</b>, seleccione la función, haga clic en <b>Permisos</b> y, a continuación, haga clic en <b>Agregar permiso</b>.</li> <li>b Haga clic en <b>Agregar</b>, seleccione uno o varios criterios de búsqueda y, a continuación, haga clic en <b>Buscar</b> para buscar los grupos o los usuarios administradores que coincidan con sus criterios de búsqueda.</li> <li>c Seleccione un usuario administrador o un grupo para incluir en el permiso y haga clic en <b>Aceptar</b>. Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios.</li> <li>d Si la función no se aplica a los grupos de acceso, haga clic en <b>Finalizar</b>.</li> <li>e Si la función se aplica a los grupos de acceso, haga clic en <b>Siguiente</b>, seleccione uno o varios grupos de acceso y haga clic en <b>Finalizar</b>. Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso.</li> </ul>
<b>Crear un permiso que incluya un grupo de acceso específico</b>	<ul style="list-style-type: none"> <li>a En la pestaña <b>Grupos de acceso</b>, seleccione el grupo de acceso y haga clic en <b>Agregar permiso</b>.</li> <li>b Haga clic en <b>Agregar</b>, seleccione uno o varios criterios de búsqueda y, a continuación, haga clic en <b>Buscar</b> para buscar los grupos o los usuarios administradores que coincidan con sus criterios de búsqueda.</li> <li>c Seleccione un usuario administrador o un grupo para incluir en el permiso y haga clic en <b>Aceptar</b>. Pulse las teclas Ctrl y Mayús para seleccionar varios grupos y usuarios.</li> <li>d Haga clic en <b>Siguiente</b>, seleccione una función y, a continuación, haga clic en <b>Finalizar</b>. Una función debe contar con, al menos, un privilegio específico de objeto para aplicarlo a un grupo de acceso.</li> </ul>

## Eliminar un permiso

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

Si elimina el último permiso de un grupo o de un usuario administrador, estos últimos también se eliminan. Dado que al menos un administrador debe tener la función Administradores en el grupo de acceso raíz, no puede eliminar un permiso que elimine al administrador. No puede eliminar un permiso heredado.

### Procedimiento

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

- 2 Seleccione el permiso que va a eliminar.

Opción	Acción
Eliminar un permiso que se aplica a un grupo o administrador específicos	Seleccione el grupo o el administrador en la pestaña <b>Administradores y grupos</b> .
Eliminar un permiso que se aplica a una función	Seleccione la función en la pestaña <b>Funciones</b> .
Eliminar un permiso que se aplica a un grupo de acceso específico	Seleccione la carpeta en la pestaña <b>Grupos de acceso</b> .

- 3 Seleccione el permiso y haga clic en **Eliminar permiso**.

## Revisar los permisos

Es posible revisar los permisos que incluyan a un grupo o un administrador específicos, una función específica o un grupo de acceso específico.

### Procedimiento

- 1 Seleccione **Configuración de View > Administradores**.
- 2 Revise los permisos.

Opción	Acción
Revisar los permisos que incluyan un grupo o un usuario administrador específico	Seleccione el grupo o el administrador en la pestaña <b>Administradores y grupos</b> .
Revisar los permisos que incluyan una función específica	Seleccione la función en la pestaña <b>Funciones</b> y haga clic en <b>Permisos</b> .
Revisar los permisos que incluyan un grupo de acceso específico	Seleccione la carpeta en la pestaña <b>Grupos de acceso</b> .

## Administrar y consultar los grupos de acceso

Puede usar View Administrator para agregar y eliminar grupos de acceso y para consultar los equipos y los grupos de escritorios de un grupo de acceso particular.

### ■ [Agregar un grupo de acceso](#)

Cree grupos de acceso para delegar la administración de determinadas máquinas, grupos de escritorios o granjas en otros administradores. De forma predeterminada, las granjas y los grupos de escritorios o de aplicaciones se encuentran en el grupo de acceso root.

### ■ [Mover un grupo de escritorios o una granja a un grupo de acceso diferente](#)

Después de crear un grupo de acceso, puede mover los grupos de escritorios automáticos, los grupos manuales o las granjas al nuevo grupo de acceso.

### ■ Eliminar un grupo de acceso

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

### ■ Revisar las granjas o los grupos de escritorios o de aplicaciones de un grupo de acceso

Puede consultar las granjas o los grupos de escritorios o de aplicaciones que se encuentran en un grupo de acceso concreto de View Administrator.

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

Puede ver las máquinas virtuales de vCenter de un grupo de acceso concreto de View Administrator. Una máquina virtual de vCenter hereda el grupo de acceso de su grupo.

## Agregar un grupo de acceso

Cree grupos de acceso para delegar la administración de determinadas máquinas, grupos de escritorios o granjas en otros administradores. De forma predeterminada, las granjas y los grupos de escritorios o de aplicaciones se encuentran en el grupo de acceso root.

Puede tener un máximo de 100 grupos de acceso, incluido el grupo de acceso raíz.

### Procedimiento

- 1 En View Administrator, diríjase al cuadro de diálogo Agregar grupo de acceso.

Opción	Acción
En Catálogo	<ul style="list-style-type: none"> <li>■ Seleccione <b>Catálogo &gt; Grupos de escritorios</b>.</li> <li>■ En el menú desplegable <b>Grupo de acceso</b> situado en el panel de ventana superior, seleccione <b>Nuevo grupo de acceso</b>.</li> </ul>
En Recursos	<ul style="list-style-type: none"> <li>■ Seleccione <b>Recursos &gt; Granjas</b>.</li> <li>■ En el menú desplegable <b>Grupo de acceso</b> situado en el panel de ventana superior, seleccione <b>Nuevo grupo de acceso</b>.</li> </ul>
En Configuración de View	<ul style="list-style-type: none"> <li>■ Seleccione <b>Configuración de View &gt; Administradores</b>.</li> <li>■ En la pestaña <b>Grupos de acceso</b>, seleccione <b>Agregar grupo de acceso</b>.</li> </ul>

- 2 Introduzca un nombre y una descripción para el grupo de acceso y haga clic en **Aceptar**.

La descripción es opcional.

### Pasos siguientes

Desplace uno o más objetos al grupo de acceso.

## Mover un grupo de escritorios o una granja a un grupo de acceso diferente

Después de crear un grupo de acceso, puede mover los grupos de escritorios automáticos, los grupos manuales o las granjas al nuevo grupo de acceso.

**Procedimiento**

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios o Recursos > Granjas**.
- 2 Seleccione un grupo o una granja.
- 3 Seleccione **Cambiar grupo de acceso** en el menú desplegable **Grupo de acceso** que aparece en el panel de ventana superior.
- 4 Seleccione el grupo de acceso y haga clic en **Aceptar**.

View Administrator mueve el grupo al grupo de acceso que seleccionó.

## Eliminar un grupo de acceso

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

**Requisitos previos**

Si el grupo de acceso contiene objetos, mueva esos objetos a otro grupo de acceso o al grupo de acceso raíz. Consulte [Mover un grupo de escritorios o una granja a un grupo de acceso diferente](#).

**Procedimiento**

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Grupos de acceso**, seleccione el grupo de acceso y haga clic en **Eliminar grupo de acceso**.
- 3 Haga clic en **Aceptar** para eliminar el grupo de acceso.

## Revisar las granjas o los grupos de escritorios o de aplicaciones de un grupo de acceso

Puede consultar las granjas o los grupos de escritorios o de aplicaciones que se encuentran en un grupo de acceso concreto de View Administrator.

**Procedimiento**

- 1 En View Administrator, diríjase a la página principal de los objetos.

Objeto	Acción
Grupos de escritorios	Seleccione <b>Catálogo &gt; Grupos de escritorios</b> .
Grupos de aplicaciones	Seleccione <b>Catálogo &gt; Grupos de aplicaciones</b> .
Granjas	Seleccione <b>Recursos &gt; Granjas</b> .

De forma predeterminada, se muestran los objetos de todos los grupos de acceso.

- 2 Seleccione un grupo de acceso del menú desplegable **Grupo de acceso** que aparece en el panel de ventana principal.

Aparecen los objetos del grupo de acceso que seleccionó.

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

Puede ver las máquinas virtuales de vCenter de un grupo de acceso concreto de View Administrator. Una máquina virtual de vCenter hereda el grupo de acceso de su grupo.

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Máquinas**.
- 2 Seleccione la pestaña **Máquinas virtuales de vCenter**.  
De forma predeterminada, se muestran las máquinas virtuales de vCenter de todos los grupos de acceso.
- 3 Seleccione un grupo de acceso en el menú desplegable **Agregar grupo de acceso**.  
Aparecerán las máquinas virtuales de vCenter del grupo de acceso que seleccionó.

## Administrar funciones personalizadas

Puede usar View Administrator para agregar, modificar y eliminar funciones personalizadas.

- [Agregar una función personalizada](#)  
Si las funciones de administrador predefinidas no responden a sus necesidades, puede combinar privilegios específicos para crear sus propias funciones en View Administrator.
- [Modificar los privilegios de una función personalizada](#)  
Puede modificar los privilegios de una función personalizada. Sin embargo, no puede modificar las funciones de administrador predefinidas.
- [Eliminar una función personalizada](#)  
Puede eliminar una función personalizada si no está incluida en un permiso. No puede eliminar las funciones de administrador predefinidas.

## Agregar una función personalizada

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

### Requisitos previos

Familiarícese con los privilegios de administrador disponibles para crear funciones personalizadas. Consulte [Funciones y privilegios predefinidos](#).

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Funciones**, haga clic en **Agregar función**.



- 3 Escriba un nombre y una descripción para la función nueva, seleccione uno o más privilegios y haga clic en **Aceptar**.

La función nueva aparece en el panel izquierdo.

## Modificar los privilegios de una función personalizada

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

### Requisitos previos

Familiarícese con los privilegios de administrador disponibles para crear funciones personalizadas. Consulte [Funciones y privilegios predefinidos](#).

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Funciones**, seleccione la función.
- 3 Haga clic en **Privilegios** para mostrar los privilegios de la función y seleccione **Editar**.
- 4 Seleccione privilegios o anule su selección.
- 5 Haga clic en **Aceptar** para guardar los cambios.

## Eliminar una función personalizada

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

### Requisitos previos

Si la función está incluida en un permiso, elimine el permiso. Consulte [Eliminar un permiso](#).

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Administradores**.
- 2 En la pestaña **Funciones**, seleccione la función y haga clic en **Eliminar función**.

El botón **Eliminar función** no está disponible para las funciones predefinidas o para las funciones personalizadas que se incluyen en un permiso.

- 3 Haga clic en **Aceptar** para eliminar la función.

## Funciones y privilegios predefinidos

View Administrator incluye funciones predefinidas que puede asignar a sus grupos y usuarios administradores. También puede combinar privilegios seleccionados para crear sus propias funciones de administrador.

- **Funciones de administrador predefinidas**

Las funciones de administrador predefinidas combinan todos los privilegios individuales necesarios para realizar las tareas de administración habituales. Estas funciones no se pueden modificar.

- **Privilegios globales**

Los privilegios globales controlan las operaciones de todo el sistema, como ver y cambiar la configuración global. Las funciones que incluyen privilegios específicos de objeto no se pueden aplicar a grupos de acceso.

- **Privilegios específicos de objeto**

Los privilegios específicos de objeto controlan las operaciones de determinados tipos de objetos del inventario. Las funciones que incluyen privilegios específicos de objeto pueden aplicarse a grupos de acceso.

- **Privilegios internos**

Algunas de las funciones de administrador predefinidas contienen privilegios internos. No puede seleccionar los privilegios internos cuando crea funciones personalizadas.

## Funciones de administrador predefinidas

Las funciones de administrador predefinidas combinan todos los privilegios individuales necesarios para realizar las tareas de administración habituales. Estas funciones no se pueden modificar.

[Tabla 6-6. Funciones predefinidas de View Administrator](#) describe las funciones predefinidas e indica si se pueden aplicar a un grupo de acceso.

Tabla 6-6. Funciones predefinidas de View Administrator

Función	Características del usuario	Se aplica a un grupo de acceso
Administradores	<p>Realizar todas las operaciones de administrador, que incluyen la creación de más grupos y usuarios administradores. En un entorno de arquitectura de Cloud Pod, los administradores que tengan esta función pueden configurar y gestionar una federación de pods, así como administrar sesiones de pods remotos.</p> <p>Los administradores que tengan la función Administradores en el grupo de acceso raíz son superusuarios porque tienen acceso completo a todos los objetos del inventario del sistema. Dado que esta función reúne todos los privilegios, debe asignarla a un número limitado de usuarios. Inicialmente, se asigna esta función a los miembros del grupo de administradores local del host del servidor de conexión de View en el grupo de acceso raíz.</p> <hr/> <p><b>Importante</b> 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"> <li>■ Agregar y eliminar grupos de acceso.</li> <li>■ Administrar aplicaciones ThinApp y sus opciones de configuración en View Administrator.</li> <li>■ Usar los comandos vdmadmin, vdmimport y lmvutil.</li> </ul>	Sí
Administradores (solo lectura)	<ul style="list-style-type: none"> <li>■ Ver, pero no modificar, la configuración global y los objetos del inventario.</li> <li>■ Ver, pero no modificar, las aplicaciones ThinApp y su configuración.</li> <li>■ Ejecutar todos los comandos PowerShell y las utilidades de la línea de comandos, incluido vdmexport, pero no vdmadmin, vdmimport ni lmvutil.</li> </ul> <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

Función	Características del usuario	Se aplica a un grupo de acceso
Administradores de inventario	<ul style="list-style-type: none"> <li>■ Ejecutar todas las operaciones relacionadas con los grupos, las sesiones y las máquinas.</li> <li>■ Administrar discos persistentes.</li> <li>■ Resincronizar, actualizar y volver a equilibrar grupos de clones vinculados y cambiar la imagen de grupo predeterminada.</li> </ul> <p>Cuando los administradores tienen esta función en un grupo de acceso, solo pueden realizar estas operaciones en los objetos del inventario del mismo.</p>	Sí
Administradores de inventario (solo lectura)	<p>Ver, pero no modificar, los objetos del inventario.</p> <p>Cuando los administradores tienen esta función en un grupo de acceso, solo pueden ver los objetos del inventario del mismo.</p>	Sí
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>	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>	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.

[Tabla 6-7. Privilegios globales](#) describe los privilegios globales y enumera las funciones predefinidas que contiene cada privilegio.

Tabla 6-7. Privilegios globales

Privilegio	Características del usuario	Funciones predefinidas
<b>Interacción de consola</b>	Inicie sesión y use View Administrator.	Administradores Administradores (solo lectura) Administradores de inventario Administradores de inventario (solo lectura) Configuración global y administradores de directivas Configuración global y administradores de directivas (solo lectura)
<b>Interacción directa</b>	Ejecute todos los comandos PowerShell y las utilidades de la línea de comandos, excepto vdmadmin y vdmimport.  Los administradores deben tener la función Administradores en el grupo de acceso raíz para usar los comandos vdmadmin, vdmimport y lmvutil.	Administradores Administradores (solo lectura)
<b>Administrar configuración global y directivas</b>	Vea y modifique las directivas globales y las opciones de la configuración, excepto los permisos y las funciones de administrador.	Administradores Configuración global y administradores de directivas
<b>Administrar sesiones globales</b>	Administre sesiones globales en un entorno de arquitectura Cloud Pod.	Administradores
<b>Administrar funciones y permisos</b>	Cree, modifique y elimine los permisos y las funciones de administrador.	Administradores
<b>Registrar agente</b>	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 de View.	Administradores Administradores de registro de agente

## Privilegios específicos de objeto

Los privilegios específicos de objeto controlan las operaciones de determinados tipos de objetos del inventario. Las funciones que incluyen privilegios específicos de objeto pueden aplicarse a grupos de acceso.

[Tabla 6-8. Privilegios específicos de objeto](#) describe los privilegios específicos de objeto. Las funciones predeterminadas de Administradores y Administradores de inventario incluyen todos estos privilegios.

Tabla 6-8. Privilegios específicos de objeto

Privilegio	Características del usuario	Objeto
Habilitar granjas y grupos de aplicaciones y escritorios	Habilitar y deshabilitar grupos de escritorios.	Grupo de escritorios, granja
Autorizar grupos de escritorios y aplicaciones	Agregar y eliminar autorizaciones de usuario.	Grupo de escritorios, grupo de aplicación
Administrar la imagen de grupo de escritorios Composer	Resincronizar, actualizar y volver a equilibrar grupos de clonación vinculada y cambiar la imagen de grupo predeterminada.	Grupo de escritorios
Administrar máquina	Ejecutar operaciones relacionadas con todas las máquinas y sesiones.	Máquina
Administrar discos persistentes	Ejecutar todas las operaciones de discos persistentes de View Composer, como conectar, desconectar e importar discos persistentes.	Disco persistente
Administrar granjas y grupos de aplicaciones y escritorios	Agregar, modificar y eliminar granjas. Agregar, eliminar y autorizar grupos de aplicaciones y escritorios. Agregar y eliminar máquinas.	Grupo de escritorios, grupo de aplicaciones, granja
Administrar sesiones	Desconectar y cerrar sesiones y enviar mensajes a usuarios.	Sesión
Administrar operación de reinicio	Restablecer las máquinas virtuales o reiniciar los escritorios virtuales.	Máquina

## Privilegios internos

Algunas de las funciones de administrador predefinidas contienen privilegios internos. No puede seleccionar los privilegios internos cuando crea funciones personalizadas.

[Tabla 6-9. Privilegios internos](#) describe los privilegios internos y enumera las funciones predefinidas que contiene cada privilegio.

Tabla 6-9. Privilegios internos

Privilegio	Descripción	Funciones predefinidas
Completo (solo lectura)	Otorga acceso de solo lectura a toda la configuración.	Administradores (solo lectura)
Administrar inventario (solo lectura)	Otorga acceso de solo lectura a los objetos del inventario.	Administradores de inventario (solo lectura)
Administrar configuración global y directivas (solo lectura)	Otorga acceso de solo lectura a las opciones de configuración y las directivas globales excepto para las funciones y los administradores.	Configuración global y administradores de directivas (solo lectura)

## Privilegios necesarios para las tareas comunes

Muchas tareas comunes de administración necesitan un conjunto coordinado de privilegios. Además, algunas operaciones necesitan permiso en el grupo de acceso raíz para acceder al objeto con el que se está trabajando.

### Privilegios para administrar grupos

Los administradores deben tener ciertos privilegios para administrar los grupos de View Administrator.

[Tabla 6-10. Privilegios y tareas para administrar los grupos](#) muestra las tareas comunes para administrar los grupos y los privilegios necesarios para realizar cada tarea.

**Tabla 6-10. Privilegios y tareas para administrar los grupos**

Tarea	Privilegios necesarios
Habilitar o deshabilitar un grupo de escritorios	Habilitar granjas y grupos de aplicaciones y escritorios
Autorizar o eliminar una autorización de usuarios a un grupo	Autorizar grupos de escritorios y aplicaciones
Agregar un grupo	Administrar granjas y grupos de aplicaciones y escritorios
Modificar o eliminar un grupo	Administrar granjas y grupos de aplicaciones y escritorios
Agregar o eliminar escritorios de un grupo	Administrar granjas y grupos de aplicaciones y escritorios
Actualizar, recomponer, volver a equilibrar o cambiar la imagen de View Composer predeterminada	Administrar la imagen de grupo de escritorios Composer
Cambiar grupos de acceso	Administrar granjas y grupos de aplicaciones y escritorios en los grupos de acceso de origen y de destino.

### Privilegios para administrar máquinas

Los administradores deben tener ciertos privilegios para administrar las máquinas de View Administrator.

[Tabla 6-11. Privilegios y tareas para administrar las máquinas](#) muestra las tareas comunes para administrar las máquinas y los privilegios necesarios para realizar cada tarea.

**Tabla 6-11. Privilegios y tareas para administrar las máquinas**

Tarea	Privilegios necesarios
Eliminar una máquina virtual	Administrar máquina
Restablecer una máquina virtual	Administrar operación de reinicio
Reiniciar un escritorio virtual	Administrar operación de reinicio
Asignar o eliminar la propiedad del usuario	Administrar máquina
Activar el modo de mantenimiento o salir de él	Administrar máquina
Desconectar o cerrar las sesiones	Administrar sesiones

## Privilegios para administrar discos persistentes

Los administradores deben tener ciertos privilegios para administrar los discos persistentes de View Administrator.

[Tabla 6-12. Privilegios y tareas para administrar los discos persistentes](#) muestra las tareas comunes para administrar los discos persistentes y los privilegios necesarios para realizar cada tarea. Realice estas tareas en la página Discos persistentes de View Administrator.

**Tabla 6-12. Privilegios y tareas para administrar los discos persistentes**

Tarea	Privilegios necesarios
Desconectar un disco	<b>Administrar discos persistentes</b> en el disco y <b>Administrar granjas y grupos de aplicaciones y escritorios</b> en el grupo.
Conectar un disco	<b>Administrar discos persistentes</b> en el disco y <b>Administrar granjas y grupos de aplicaciones y escritorios</b> en el equipo.
Editar un disco	<b>Administrar discos persistentes</b> en el disco y <b>Administrar granjas y grupos de aplicaciones y escritorios</b> en el grupo seleccionado.
Cambiar grupos de acceso	<b>Administrar discos persistentes</b> en los grupos de acceso de origen y de destino.
Volver a crear un escritorio	<b>Administrar discos persistentes</b> en el disco y <b>Administrar granjas y grupos de aplicaciones y escritorios</b> en el último grupo.
Importar desde vCenter	<b>Administrar discos persistentes</b> en la carpeta y <b>Administrar grupo</b> en el grupo.
Eliminar un disco	<b>Administrar discos persistentes</b> en el disco.

## Privilegios para administrar los usuarios y los administradores

Los administradores deben tener ciertos privilegios para administrar los usuarios y los administradores de View Administrator.

[Tabla 6-13. Privilegios y tareas para administrar usuarios y administradores](#) 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 View Administrator y los administradores en la página Ver administradores globales de View Administrator.

**Tabla 6-13. Privilegios y tareas para administrar usuarios y administradores**

Tarea	Privilegios necesarios
Actualizar la información general del usuario	<b>Administrar configuración global y directivas</b>
Enviar mensajes a los usuarios	<b>Administrar sesiones remotas</b> en la máquina.
Agregar un grupo o un usuario administrador	<b>Administrar funciones y permisos</b>
Agregar, modificar o eliminar un permiso de administrador	<b>Administrar funciones y permisos</b>
Agregar, modificar o eliminar una función de administrador	<b>Administrar funciones y permisos</b>



## 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.

[Tabla 6-14. Privilegios para los comandos y las tareas de administración general](#) muestra los privilegios necesarios para ejecutar tareas de administración general y ejecutar las utilidades de la línea de comandos.

**Tabla 6-14. Privilegios para los comandos y las tareas de administración general**

Tarea	Privilegios necesarios
Agregar o eliminar un grupo de acceso	Debe tener la función Administrador en el grupo de acceso raíz.
Administrar las aplicaciones ThinApp y su configuración en View 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	<b>Registrar agente</b>
Ver o modificar las opciones de configuración (excepto para los administradores) en View Administrator	<b>Administrar configuración global y directivas</b>
Ejecute todos los comandos PowerShell y las utilidades de la línea de comandos excepto vdmadmin y vdmimport.	<b>Interacción directa</b>
Usar los comandos vdmadmin y vdmimport	Debe tener la función Administrador en el grupo de acceso raíz.
Usar el comando vdmexport	Debe tener la función Administradores o la función Administradores (solo lectura) en el grupo de acceso raíz.

## Prácticas recomendadas para grupos y usuarios administradores

Para aumentar la seguridad y manejabilidad del entorno View, debe seguir las prácticas recomendadas para administrar grupos y usuarios administradores.

- Cree nuevos grupos de usuarios en Active Directory y asígneles funciones administrativas de View. Evite usar grupos integrados de Windows u otros grupos existentes que puedan incluir usuarios que no necesiten o no debieran tener privilegios de View.
- Mantenga al mínimo el número de usuarios con privilegios administrativos de View.
- 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 separados que puedan modificar las directivas globales y la configuración de View.

# Configurar directivas en Horizon Administrator y en Active Directory

# 7

Puede usar Horizon Administrator si desea configurar directivas para las sesiones cliente. Puede configurar las opciones de la directiva de grupo de Active Directory para controlar el comportamiento del servidor de conexión de View, el protocolo de visualización PCoIP, el registro de Horizon 7 y las alarmas de rendimiento.

También puede configurar las opciones de la directiva de grupo de Active Directory para controlar el comportamiento de Horizon Agent, de Horizon Client para Windows, de Horizon Persona Management y de algunas funciones. Para obtener más información sobre la configuración de estas directivas, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Establecer directivas en View Administrator](#)
- [Uso de los archivos de plantillas administrativas de la directiva de grupo de Horizon 7](#)

## Establecer directivas en View Administrator

View Administrator permite configurar directivas para las sesiones de cliente.

Puede establecer estas directivas para que afecten a usuarios específicos, a grupos de escritorios específicos o a todos los usuarios de las sesiones de cliente. Las directivas que afectan a grupos de escritorios y usuarios específicos se denominan directivas de nivel de usuario y directivas de nivel de grupo. Las directivas que afectan a todas las sesiones y usuarios se denominan directivas globales.

Las directivas de nivel de usuario heredan la configuración de las directivas de nivel de grupo. De forma similar, las directivas de nivel de grupo de escritorio heredan la configuración de las directivas globales equivalentes. La configuración de la directiva de nivel de escritorio tiene preferencia sobre la configuración de la directiva global equivalente. La configuración de la directiva de nivel de usuario tiene preferencia sobre la configuración de la directiva global equivalente y la directiva de nivel de grupo de escritorios.

La configuración de la directiva de nivel inferior puede ser más o menos restrictiva que la configuración de nivel superior equivalente. Por ejemplo, puede establecer una directiva global en **Denegar** y la directiva equivalente de nivel del grupo de escritorios en **Permitir** o viceversa.

---

**Nota** Solo las directivas globales están disponibles para los grupos de aplicaciones y los escritorios RDS. No puede establecer directivas de nivel de usuario ni de nivel de grupo para los grupos de aplicaciones y los escritorios RDS.

---

- **Configurar las opciones de la directiva global**

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

- **Configurar directivas para los grupos de escritorios**

Puede configurar directivas en el nivel de escritorios para que afecten a grupos de escritorios específicos. La configuración de las directivas en el nivel de escritorios tiene preferencia sobre la configuración de directivas global equivalente.

- **Configurar directivas para los usuarios**

Puede configurar directivas en el nivel de usuarios para que afecten a usuarios específicos. La configuración de la directiva a nivel de usuario siempre tiene preferencia ante la configuración de directivas global equivalente y las directivas en el nivel de grupo de escritorios.

- **Directivas de View**

Puede configurar las directivas de View para que afecten a todas las sesiones de cliente, o bien puede aplicarlas para que afecten a usuarios o grupos de escritorios específicos.

## Configurar las opciones de la directiva global

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

### Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de View](#).

### Procedimiento

- 1 En View Administrator, seleccione **Directivas > Directivas globales**.
- 2 Haga clic en **Editar directivas** en el panel **Directivas de View**.
- 3 Haga clic en **Aceptar** para guardar los cambios.

## Configurar directivas para los grupos de escritorios

Puede configurar directivas en el nivel de escritorios para que afecten a grupos de escritorios específicos. La configuración de las directivas en el nivel de escritorios tiene preferencia sobre la configuración de directivas global equivalente.

## Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de View](#).

## Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo de escritorios y haga clic en la pestaña **Directivas**.  
La pestaña **Directivas** muestra la configuración de directivas actual. Cuando se hereda una opción de la directiva global equivalente, **Heredada** aparece en la columna **Directiva del grupo de escritorios**.
- 3 Haga clic en **Editar directivas** en el panel **Directivas de View**.
- 4 Haga clic en **Aceptar** para guardar los cambios.

## Configurar directivas para los usuarios

Puede configurar directivas en el nivel de usuarios para que afecten a usuarios específicos. La configuración de la directiva a nivel de usuario siempre tiene preferencia ante la configuración de directivas global equivalente y las directivas en el nivel de grupo de escritorios.

## Requisitos previos

Familiarícese con las descripciones de las directivas. Consulte [Directivas de View](#).

## Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo de escritorios y haga clic en la pestaña **Directivas**.  
La pestaña **Directivas** muestra la configuración de directivas actual. Cuando se hereda una opción de la directiva global equivalente, **Heredada** aparece en la columna **Directiva del grupo de escritorios**.
- 3 Haga clic en **Reemplazos del usuario** y, a continuación, en **Agregar usuario**.
- 4 Para buscar un usuario, haga clic en **Agregar**, escriba el nombre o la descripción del usuario y, a continuación, haga clic en **Buscar**.
- 5 Seleccione uno o varios usuarios de la lista, haga clic en **Aceptar** y, a continuación, en **Siguiente**.  
Aparece el cuadro de diálogo Agregar directiva individual.
- 6 Configure las directivas de View y haga clic en **Finalizar** para guardar los cambios.

## Directivas de View

Puede configurar las directivas de View para que afecten a todas las sesiones de cliente, o bien puede aplicarlas para que afecten a usuarios o grupos de escritorios específicos.

[Tabla 7-1. Directivas de View](#) describe cada opción de las directivas de View.

Tabla 7-1. Directivas de View

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 <b>Denegar</b>.</p> <p>Si los sistemas cliente no tienen recursos suficientes para administrar la descodificación multimedia local, mantenga la opción como <b>Denegar</b>.</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 <b>Permitir</b>. Para evitar el uso de dispositivos externos por seguridad, cambie la opción a <b>Denegar</b>.</p>
Aceleración de hardware PColP	<p>Determina si desea habilitar la aceleración del hardware del protocolo de visualización PColP y especifica la prioridad de aceleración que está asignada a la sesión del usuario de PColP.</p> <p>Esta opción solo tiene efecto si el dispositivo de aceleración del hardware PColP se encuentra en el equipo físico que aloja el escritorio remoto.</p> <p>El valor predeterminado es <b>Permitir</b> con la prioridad <b>Media</b>.</p>

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

Horizon 7 proporciona varios archivos de plantillas administrativas (ADM y ADMX) de la directiva de grupo. Puede optimizar y asegurar las aplicaciones y los escritorios remotos al agregar la configuración de la directiva de estos archivos de plantilla ADMX y ADM en un GPO nuevo o ya existente de Active Directory.

**Nota** En la versión 7.1 de Horizon 7, los archivos de plantilla ADM quedan obsoletos y se agregan los archivos de plantilla ADMX.

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

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

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

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

## Archivos de plantilla ADM y ADMX de Horizon 7

Los archivos de plantilla ADMX y ADM de Horizon 7 proporcionan una configuración de directiva de grupo que le permite controlar y optimizar los componentes de Horizon 7.

**Nota** En la versión 7.1 de Horizon 7, los archivos de plantilla ADM quedan obsoletos y se agregan los archivos de plantilla ADMX.

**Tabla 7-2. Archivos de plantilla ADM y ADMX de Horizon**

Nombre de plantilla	Archivo de plantilla	Descripción
Configuración de Horizon Agent	vdm_agent.admx vdm_agent.adm	<p>Contiene la configuración de las directivas relacionada con los componentes de entorno y de autenticación de Horizon Agent.</p> <p>Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>
Configuración de Horizon Client	vdm_client.admx vdm_client.adm	<p>Contiene la configuración de las directivas relacionada con Horizon Client para Windows.</p> <p>Los clientes que se conectan desde fuera del dominio del host del servidor de conexión no se ven afectados por las directivas que se aplican a Horizon Client.</p> <p>Consulte el documento <i>Uso de VMware Horizon Client para Windows</i>.</p>

Nombre de plantilla	Archivo de plantilla	Descripción
Redireccionamiento URL de VMware Horizon	urlRedirection-enUS.admx urlRedirection-enUS.adm	<p>Contiene la configuración de las directivas relacionada con la función de redireccionamiento de contenido URL. Si agrega esta plantilla a un GPO para un grupo de aplicaciones o de escritorios remotos, algunos vínculos URL a los que se hacen clic dentro de las aplicaciones o los escritorios remotos se pueden redireccionar a un cliente basado en Windows y se pueden abrir en un navegador del cliente.</p> <p>Si agrega esta plantilla en una GPO del cliente, cuando un usuario hace clic en ciertos vínculos URL en un sistema cliente basado en Windows, la URL se puede abrir en una aplicación o un escritorio remotos.</p> <p>Consulte los documentos <i>Configurar funciones de escritorios remotos en Horizon 7</i> y <i>Uso de VMware Horizon Client para Windows</i>.</p>
Configuración del servidor de conexión	vdm_server.admx vdm_server.adm	<p>Contiene la configuración de las directivas relacionadas con el servidor de conexión.</p> <p>Consulte <a href="#">Configuración de las plantillas ADM o ADMX de configuración del servidor de conexión de Horizon</a>.</p>
Configuración común de View	vdm_common.admx vdm_common.adm	<p>Contiene la configuración de las directivas que son comunes a todos los componentes de Horizon.</p> <p>Consulte <a href="#">Configuración de las plantillas ADM y ADMX de configuración común de Horizon 7</a>.</p>
Variables de las sesiones de PCoIP	pcoip.admx pcoip.adm	<p>Contiene la configuración de directivas relacionada con el protocolo de visualización PCoIP.</p> <p>Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>
Variables de las sesiones del cliente PCoIP	pcoip.client.admx pcoip.client.adm	<p>Contiene la configuración de las directivas relacionada con el protocolo de visualización PCoIP que afecta a Horizon Client para Windows.</p> <p>Consulte el documento <i>Uso de VMware Horizon Client para Windows</i>.</p>
Configuración de Horizon Persona Management	ViewPM.admx ViewPM.adm	<p>Contiene la configuración de directivas relacionadas con Horizon Persona Management.</p> <p>Consulte el documento <i>Configurar escritorios virtuales en Horizon 7</i>.</p>
Servicios de Escritorio remoto	vmware_rdsh.admx vmware_rdsh.adm	<p>Contiene la configuración de las directivas relacionadas con los Servicios de Escritorio remoto.</p> <p>Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>
Configuración Audio/vídeo en tiempo real	vdm_agent_rtav.admx vdm_agent_rtav.adm	<p>Contiene la configuración de las directivas relacionada con las cámaras web que se usan con la función Audio/vídeo en tiempo real.</p> <p>Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i>.</p>



Nombre de plantilla	Archivo de plantilla	Descripción
Redireccionamiento de escáner	vdm_agent_scanner.admx vdm_agent_scanner.adm	Contiene la configuración de las directivas relacionadas con dispositivos de escáner que se redireccionan para usarlos en aplicaciones y dispositivos publicados.  Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .
Redireccionamiento de puerto serie	vdm_agent_serialport.admx vdm_agent_serialport.adm	Contiene la configuración de las directivas relacionadas con los puertos (COM) serie que se redireccionan para usarlos en escritorios virtuales.  Consulte el documento <i>Configurar funciones de escritorios remotos en Horizon 7</i> .

## Configuración de las plantillas ADM o ADMX de configuración del servidor de conexión de Horizon

Los archivos de plantillas ADMX de configuración de View Server (`vdm_server.admx`) o ADM (`vdm_server.adm`) incluyen la configuración de la directiva relacionada con todos los servidores de conexión de Horizon.

[Tabla 7-3. Opciones de la plantilla de configuración de Horizon Server](#) describe cada opción de las directivas del archivo de plantilla ADM o ADMX de configuración del servidor de conexión. La plantilla contiene únicamente las opciones de Configuración del equipo. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración del servidor de VMware View** en el Editor de administración de directivas de grupo.

**Nota** En la versión 7.1 de Horizon 7, los archivos de plantilla ADM quedan obsoletos y se agregan los archivos de plantilla ADMX.

Tabla 7-3. Opciones de la plantilla de configuración de Horizon Server

Ajuste	Propiedades
Enumerate Forest Trust Child Domains	<p>Determina si se enumeran todos los dominios de confianza del dominio en el que se encuentra el servidor. Para establecer una cadena completa de confianza, los dominios en los que confían cada dominio de confianza también se enumeran y el proceso continúa recursivamente hasta que se detectan todos los dominios de confianza. Esta información se envía al servidor de conexión para garantizar que todos los dominios de confianza estén disponibles cuando el cliente inicia sesión.</p> <p>Esta propiedad está habilitada de forma predeterminada. Cuando está deshabilitada, solo se enumeran los dominios de confianza directamente y no se establece la conexión a los controladores de dominios remotos.</p> <p><b>Nota</b> En entornos con relaciones de dominio complejas, como las que usan varias estructuras de bosques con dominios de confianza entre dominios, el proceso puede durar varios minutos en completarse.</p>
Recursive Enumeration of Trusted Domains	<p>Determina si se enumeran todos los dominios de confianza del dominio en el que se encuentra el servidor. Para establecer una cadena completa de confianza, los dominios en los que confían cada dominio de confianza también se enumeran y el proceso continúa recursivamente hasta que se detectan todos los dominios de confianza. Esta información se envía al servidor de conexión de View para que todos los dominios de confianza estén disponibles cuando el cliente inicia sesión.</p> <p>Esta configuración está habilitada de forma predeterminada. Cuando está deshabilitada, solo se enumeran los dominios de confianza directamente y no se establece la conexión a los controladores de dominios remotos.</p> <p>En entornos con relaciones de dominio complejas, como las que usan varias estructuras de bosques con dominios de confianza entre dominios, este proceso puede durar varios minutos en completarse.</p>
Windows Password Authentication Mode	<p>Seleccione el modo de autenticación de contraseñas para Windows.</p> <ul style="list-style-type: none"> <li>■ KerberosOnly. Autenticar con Kerberos.</li> <li>■ KerberosWithFallbackToNTLM. Autenticar con Kerberos pero, en caso de fallo, utilizar NTLM.</li> <li>■ Legacy. Autenticar con NTLM pero, en caso de fallo, utilizar Kerberos. Se utiliza para admitir controladores de dominio NT heredados.</li> </ul> <p>El valor predeterminado es KerberosOnly.</p>

## Configuración de las plantillas ADM y ADMX de configuración común de Horizon 7

Los archivos de las plantillas ADMX de configuración común (vdm\_common.admx) y ADM (vdm\_common.adm) de Horizon 7 incluyen la configuración de la directiva común en todos los componentes de Horizon. Estas plantillas contienen únicamente las opciones de Configuración del equipo. En la versión 7.1 de Horizon 7, los archivos de plantilla ADM quedan obsoletos y se agregan los archivos de plantilla ADMX.

## Opciones de configuración del registro

Tabla 7-4. Plantilla de configuración común de View: opciones de configuración de registro describe la opción de las directivas de configuración del registro de los archivos de plantillas ADM y ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View > Configuración de registro** del Editor de administración de directivas de grupo.

**Tabla 7-4. Plantilla de configuración común de View: opciones de configuración de registro**

Ajuste	Propiedades
Number of days to keep production logs	Especifica el número de días durante los cuales los archivos de registro se mantienen en el sistema. Si no se establece ningún valor, se aplica el valor predeterminado y los archivos de registro se mantienen durante siete días.
Maximum number of debug logs	Especifica el número máximo de archivos de registro de depuración que se mantienen en el sistema. Cuando un archivo de registro alcanza su tamaño máximo, no se agregan más entradas y se crea un nuevo archivo de registro. Cuando el número de archivos de registro previos alcanza este valor, se elimina el archivo más antiguo.
Maximum debug log size in Megabytes	Especifica el tamaño máximo en megabytes que un registro de depuración puede alcanzar después de que se cierre el archivo de registro y se cree uno nuevo.
Log Directory	Especifica la ruta completa al directorio de los archivos de registro. Si no se puede escribir en la ubicación, se usa la predeterminada. Para los archivos de registro cliente, se crea un directorio adicional con el nombre del cliente.
Send logs to a Syslog server	<p>Permite que se envíen los registros de View Server a un servidor syslog como VMware vCenter Log Insight. Los registros se envían desde todos los View Servers de la OU o del dominio en el que está configurado este GPO.</p> <p>Puede enviar los registros de Horizon Agent a un servidor syslog si habilita esta opción en una GPO que esté vinculada a una OU que contenga el escritorio.</p> <p>Para enviar los datos de registro a un servidor syslog, habilite esta opción y especifique el nivel de registro y el nombre de dominio completo (FQDN) del servidor o la dirección IP. Puede especificar un puerto alternativo si no desea usar el puerto 514 predeterminado. Separe cada elemento de la especificación con una barra vertical ( ). Utilice la siguiente sintaxis:</p> <p>Nivel de registro FQDN o IP del servidor [ Número de puerto(514 predeterminado)]</p> <p>Por ejemplo: Depuración 192.0.2.2</p> <p><b>Importante</b> Los datos de syslog se envían a través de la red sin el cifrado basado en software. Como los registros de View Server pueden contener datos personales, evite enviar datos syslog en una red que no sea segura. Si es posible, use la seguridad de nivel de vínculo como IPsec para evitar la posibilidad de que se supervisen estos datos en la red.</p>

## Configuración de las alarmas de rendimiento

[Tabla 7-5. Plantilla de configuración común de View: configuración de las alarmas de rendimiento](#) describe la configuración de la alarma de rendimiento en los archivos de plantillas ADM y ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View > Alarmas de rendimiento** del Editor de administración de directivas de grupo.

**Tabla 7-5. Plantilla de configuración común de View: configuración de las alarmas de rendimiento**

Ajuste	Propiedades
CPU and Memory Sampling Interval in Seconds	Especifica la CPU y la CPU del intervalo de sondeo de la memoria. Un bajo intervalo de muestreo puede provocar un nivel elevado de salida del registro.
Overall CPU usage percentage to issue log info	Especifica el umbral al que se registra el uso de la CPU general del sistema. Cuando están disponibles varios procesadores, este porcentaje representa el uso combinado.
Overall memory usage percentage to issue log info	Especifica el umbral al que se registra el uso general de la memoria del sistema asignada. La memoria asignada del sistema es la memoria que se asignó a través de procesos y a la que el sistema operativo asignó memoria física o una ranura de página en el archivo de paginación.
Process CPU usage percentage to issue log info	Especifica el umbral al que se registra el uso de CPU de cualquier proceso individual.
Process memory usage percentage to issue log info	Especifica el umbral al que se registra el uso de la memoria de cualquier proceso individual.
Process to check, comma separated name list allowing wild cards and exclusion	<p>Especifica una lista de consultas separada por comas que corresponde al nombre de uno o más procesos que se deben examinar. Puede filtrar la lista usando caracteres comodines dentro de cada consulta.</p> <ul style="list-style-type: none"> <li>■ Un asterisco (*) coincide con cero o más caracteres.</li> <li>■ Un signo de interrogación (?) coincide exactamente con un carácter.</li> <li>■ Un signo de exclamación (!) al comienzo de una consulta excluye todos los resultados de dicha consulta.</li> </ul> <p>Por ejemplo, la siguiente consulta selecciona todos los procesos que comienzan por <b>ws</b> y excluye todos los procesos que acaban con <b>sys</b>:</p> <p><b>'!*sys,ws*'</b></p>

**Nota** La configuración de la alarma de rendimiento se aplica únicamente a los sistemas Horizon Agent y al servidor de conexión de Horizon. No se aplican a los sistemas Horizon Client.

## Configuración de seguridad

[Tabla 7-6. Plantilla de configuración común de View: configuración de seguridad](#) describe la configuración de seguridad de los archivos de plantillas ADM y ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View > Configuración de seguridad** del Editor de administración de directivas de grupo.

**Tabla 7-6. Plantilla de configuración común de View: configuración de seguridad**

Ajuste	Propiedades
Only use cached revocation URLs	La comprobación de revocación de certificados accederá únicamente a las URL en caché. El valor predeterminado, si no está configurado, es false.
Revocation URL check timeout milliseconds	El tiempo de espera acumulado en todas las recuperaciones de filtrado de URL de revocación en milisegundos. Si el valor no está configurado o está establecido en 0, esto significa que se utiliza la manipulación predeterminada de Microsoft.
Type of certificate revocation check	Seleccione el tipo de comprobación de revocación de certificados que se va a realizar: <ul style="list-style-type: none"> <li>■ Ninguna</li> <li>■ EndCertificateOnly</li> <li>■ WholeChain</li> <li>■ WholeChain</li> </ul> El valor predeterminado es WholeChainButRoot.

## Configuración general

[Tabla 7-7. Plantilla de configuración común de View: configuración general](#) describe la configuración general en los archivos de plantillas ADM y ADMX de configuración común de Horizon. Todas las opciones de configuración se encuentran en la carpeta **Configuración del equipo > Directivas > Plantillas administrativas > Configuración común de VMware View** en el Editor de administración de directivas de grupo.

**Tabla 7-7. Plantilla de configuración común de View: configuración general**

Ajuste	Propiedades
Disk threshold for log and events in Megabytes	Especifica el umbral mínimo de espacio de disco restante para los registros y los eventos. Si no se especifica ningún valor, el predeterminado es 200. Cuando se alcanza el valor especificado, se detiene el registro de eventos.
Enable extended logging	Determina si los eventos de depuración y de seguimiento se incluyen en los archivos de registro.
Override the default View Windows event generation	Se admiten los siguientes valores: <ul style="list-style-type: none"> <li>■ 0 = solo se generan entradas del registro de eventos para los eventos de View (no se generan entradas del registro de eventos para los mensajes de registro)</li> <li>■ 1 = se generan entradas del registro de eventos en el modo de compatibilidad 4.5 (y versiones anteriores). No se generan entradas del registro de eventos para los eventos de View estándar. Las entradas del registro de eventos se basan exclusivamente en el texto del archivo de registro.</li> <li>■ 2 = se generan entradas del registro de eventos en el modo de compatibilidad 4.5 (y versiones anteriores) con eventos de View incluidos.</li> </ul>

# Mantener los componentes de View

## 8

Para mantener los componentes de View 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 View](#)
- [Supervisar los componentes de View](#)
- [Supervisar el estado de las máquinas](#)
- [Comprender los servicios de View](#)
- [Cambiar la clave de licencia del producto](#)
- [Supervisar la licencia y el uso del producto](#)
- [Actualizar la información general del usuario desde Active Directory](#)
- [Migrar View Composer a otro equipo](#)
- [Actualizar los certificados en una instancia del servidor de conexión de View, en el servidor de seguridad o en View Composer](#)
- [Información recopilada por el programa de mejora de la experiencia de cliente](#)

## Realizar una copia de seguridad y restaurar los datos de configuración de View

Para hacer una copia de seguridad de los datos de configuración de View y de View Composer, programe o ejecute copias de seguridad automáticas en View Administrator. Para restaurar la configuración de View, importe de forma manual los archivos de la copia de seguridad de LDAP de View y los archivos de la base de datos de View Composer.

Puede usar las funciones de restauración y de copia de seguridad para conservar y migrar los datos de configuración de View.

## Realizar una copia de seguridad de los datos del servidor de conexión de View y de View Composer

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

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

Cuando utiliza View Administrator para realizar copias de seguridad, View realiza una copia de seguridad de los datos de configuración de LDAP de View y la base de datos de View Composer. Ambos conjuntos de archivos de copias de seguridad se almacenan en la misma ubicación. Los datos de LDAP de View se exportan en formato de intercambio de datos LDAP (LDIF) cifrado. Para obtener una descripción de LDAP de View, consulte [Directorio LDAP de View](#).

Puede realizar copias de seguridad siguiendo varios procedimientos.

- Programe copias de seguridad automáticas usando la función de copia de seguridad de la configuración de View.
- Inicie una copia de seguridad en el momento usando la función **Hacer copia de seguridad ahora** en View Administrator.
- Exporte de forma manual los datos LDAP de View usando la utilidad vdmexport. Esta utilidad se proporciona con cada instancia del servidor de conexión de View.

La utilidad vdmexport puede exportar los datos LDAP de View como datos LDIF cifrados, texto sin formato o texto sin formato con contraseñas y otra información confidencial eliminada.

---

**Nota** La herramienta vdmexport solo realiza la copia de seguridad de los datos LDAP de View. Esta herramienta no hace copias de seguridad de la información de la base de datos de View Composer.

---

Para obtener más información sobre vdmexport, consulte [Exportar los datos de configuración del servidor de conexión de View](#).

Las siguientes instrucciones se aplican a las copias de seguridad de los datos de configuración de View:

- View puede exportar los datos de configuración desde cualquier instancia del servidor de conexión de View.
- Si cuenta con varias instancias del servidor de conexión de View 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 de View como mecanismo de copia de seguridad. Cuando View sincroniza los datos en instancias replicadas del servidor de conexión de View, los datos que se pierdan en una instancia se pueden perder en todos los miembros del grupo.

- Si el servidor de conexión de View usa varias instancias de vCenter Server con varios servicios de View Composer, View realiza una copia de seguridad de todas las base de datos asociadas con las instancias de vCenter Server.

## Programar copias de seguridad de la configuración de View

Puede programar que se realicen copias de seguridad de los datos de la configuración de View a intervalos regulares. View realiza copias de seguridad de los contenidos de los repositorios LDAP de View en los que las instancias del servidor de conexión de View 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 View](#).

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión de View de la que desee hacer la copia de seguridad y haga clic en **Editar**.
- 3 En la pestaña **Copia de seguridad**, especifique las opciones de la copia de seguridad de la configuración de View 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 View

View puede realizar una copia de seguridad de los datos de configuración del servidor de conexión de View y de View Composer en intervalos regulares. En View Administrator, puede establecer la frecuencia y otros aspectos de las operaciones de la copia de seguridad.



**Tabla 8-1. Opciones de copia de seguridad de la configuración de View**

Configuración	Descripción
Frecuencia de copia de seguridad automática	<p>Cada hora. Se realiza una copia de seguridad cada hora en punto.</p> <p>Cada 6 horas. Las copias de seguridad se realizan a medianoche, a las 6:00, al mediodía y a las 18:00.</p> <p>Cada 12 horas. Las copias de seguridad se realizan a medianoche y al mediodía.</p> <p>Cada día. Las copias de seguridad se realizan cada día a medianoche.</p> <p>Cada 2 días. Las copias de seguridad se realizan a medianoche los sábados, los lunes, los miércoles y los viernes.</p> <p>Cada semana. Las copias de seguridad se realizan semanalmente el sábado a medianoche.</p> <p>Cada 2 semanas. Las copias de seguridad se realizan una de cada dos semanas el sábado a medianoche.</p> <p>Nunca. Las copias de seguridad no se realizan automáticamente.</p>
Número máximo de copias de seguridad	<p>Número de archivos de copia de seguridad que se pueden almacenar en la instancia del servidor de conexión de View. El número debe ser un entero superior a 0.</p> <p>Cuando se alcanza el número máximo, View 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 <b>Hacer copia de seguridad ahora</b>.</p>
Ubicación de la carpeta	<p>La ubicación predeterminada de los archivos de la copia de seguridad donde se ejecuta el servidor de conexión de View: C:\Programdata\VMware\VDM\backups</p> <p>Cuando usa <b>Hacer copia de seguridad ahora</b>, View también almacena los archivos de copia de seguridad en esta ubicación.</p>

## Exportar los datos de configuración del servidor de conexión de View

Puede hacer una copia de seguridad de los datos de configuración de una instancia del servidor de conexión de View 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 de View. Si cuenta con varias instancias del servidor de conexión de View en un grupo replicado, solo es necesario que exporte la información desde una instancia. Todas las instancias replicadas contienen los mismos datos de configuración.

**Nota** El comando `vdmexport.exe` solo realiza la copia de seguridad de los datos LDAP de View. Este comando no hace copias de seguridad de la información de la base de datos de View Composer.

### Requisitos previos

- Ubique el archivo ejecutable del comando `vdmexport.exe` con el servidor de conexión de View en la ruta predeterminada.

C:\Program Files\VMware\VMware View\Server\tools\bin

- Inicie sesión en la instancia del servidor de conexión de View 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 View*.

### Pasos siguientes

Puede restaurar o transferir la información de la configuración del servidor de conexión de View 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 View y de View Composer](#).

## Restaurar los datos de configuración del servidor de conexión de View y de View Composer

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

Puede ejecutar distintas utilidades para restaurar el servidor de conexión de View y los datos de configuración de View Composer.

Antes de restaurar los datos de configuración, compruebe que realizó una copia de seguridad de los datos de configuración en View Administrator. Consulte [Realizar una copia de seguridad de los datos del servidor de conexión de View y de View Composer](#).

La utilidad `vdmimport` permite importar los datos del servidor de conexión de View desde los archivos de la copia de seguridad LDIF al repositorio LDAP de View en la instancia del servidor de conexión de View.

La utilidad `SviConfig` le permitirá importar los datos de View Composer desde los archivos de la copia de seguridad `.svi` a la base de datos SQL de View Composer.

---

**Nota** En determinadas situaciones, es posible que deba instalar la versión actual de una instancia del servidor de conexión de View y restaurar la configuración existente de View si importa los archivos de configuración de LDAP del servidor de conexión de View. 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 View existente o por otras razones. Para obtener más información consulte el documento "Volver a instalar el servidor de conexión de View con una configuración de seguridad" en el documento *Instalación de View*.

---

## Importar los datos de configuración en el servidor de conexión de View

Puede restaurar los datos de configuración de una instancia del servidor de conexión de View 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 de View.

Si realizó una copia de seguridad de la configuración LDAP de View con View Administrator o el comando `vdmexport` predeterminado, el archivo LDIF exportado estará cifrado. Debe descifrar el archivo LDIF antes de importarlo.

Si el archivo LDIF exportado posee un texto sin formato, no debe descifrarlo.

---

**Nota** No importe un archivo LDIF en formato limpio, es decir, en texto sin formato, contraseñas ni información confidencial. En caso de hacerlo, la información de configuración crítica no estará presente en el repositorio LDAP de View.

---

Para obtener más información sobre cómo realizar una copia de seguridad del repositorio LDAP de View, consulte [Realizar una copia de seguridad de los datos del servidor de conexión de View y de View Composer](#).

### Requisitos previos

- Ubique el archivo ejecutable del comando `vdmimport` con el servidor de conexión de View en la ruta predeterminada.

`C:\Program Files\VMware\VMware View\Server\tools\bin`

- Inicie sesión en la instancia del servidor de conexión de View como usuario con la función de administrador.

- Compruebe que conoce la contraseña de Data Recovery. Si se configuró un recordatorio de contraseña, puede mostrar el recordatorio al ejecutar el comando `vdmimport` sin la opción de contraseña.

### Procedimiento

- 1 Detenga el servicio Windows de VMware Horizon View Composer en los servidores donde se ejecuta View Composer para detener todas las instancias de dicho servicio.
- 2 Detenga el servicio Windows del servidor de seguridad VMware Horizon en todos los servidores de seguridad para detener todas las instancias de dichos servidores.
- 3 Desinstale todas las instancias del servidor de conexión de View.

Desinstale los servidores de conexión de VMware Horizon View y la instancia de AD LDS VMwareVDMDS.

- 4 Instale una instancia del servidor de conexión de View.
- 5 Detenga el servicio Windows del servidor de conexión VMware Horizon para detener la instancia del servidor de conexión de View.
- 6 Haga clic en **Iniciar > Ventana del símbolo del sistema**.
- 7 Descifre el archivo LDIF cifrado.

En la ventana del símbolo del sistema, escriba el comando `vdmimport`. Especifique la opción `-d`, la opción `-p` con la contraseña de Data Recovery y la opción `-f` con un archivo LDIF cifrado existente seguido de un nombre para el archivo LDIF descifrado. Por ejemplo:

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

Si no recuerda la contraseña de Data Recovery, escriba el comando sin la opción `-p`. La utilidad muestra el recordatorio de contraseña y pide al usuario que introduzca la contraseña.

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

Especifique la opción `-f` con el archivo LDIF descifrado. Por ejemplo:

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

- 9 Desinstale el servidor de conexión de View.  
Desinstale solo el paquete del servidor de conexión de VMware Horizon View.
- 10 Vuelva a instalar el servidor de conexión de View.
- 11 Inicie sesión en View Administrator y compruebe que la configuración sea correcta.
- 12 Inicie las instancias de View Composer.
- 13 Vuelva a instalar las instancias del servidor de réplica.
- 14 Inicie las instancias del servidor de seguridad.

Si existe riesgo de que la configuración de los servidores de seguridad sea incoherente, deben desinstalarse también en lugar de detenerlos y volver a instalarlos al final del proceso.

El comando `vdmimport` actualiza el repositorio LDAP de View en el servidor de conexión de View con los datos de configuración del archivo LDIF. Para obtener más información sobre el comando `vdmimport`, consulte el documento *Integración de View*.

---

**Nota** Asegúrese de que la configuración restaurada coincida con las máquinas virtuales que conozcan vCenter Server y View Composer, si se encuentra en uso. Si es necesario, restaure la configuración de View Composer a partir de la copia de seguridad. Consulte [Restaurar una base de datos de View Composer](#). Tras restaurar la configuración de View Composer, puede que tenga que resolver de forma manual las incoherencias si las máquinas virtuales en vCenter Server cambiaron desde que se realizó la copia de seguridad de la configuración de View Composer.

---

## Restaurar una base de datos de View Composer

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

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

---

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

---

### Requisitos previos

Compruebe la ubicación de los archivos de copia de seguridad de la base de datos de View Composer. De forma predeterminada, View almacena los archivos de copia de seguridad en la unidad C: del equipo del servidor de conexión de View en `C:\Programdata\VMWare\VDM\backups`.

Los archivos de copia de seguridad de View Composer usan una convención de nomenclatura con la fecha y el sufijo `.svi`.

*Backup–AñoMesDíaNúmero–Nombre de dominio\_Nombre vCenter Server.svi*

Por ejemplo: `Backup–20090304000010–foobar_test_org.svi`

Familiarícese con los parámetros de `SviConfig restoredata`:

- **DsnName**: el DSN que se usa para conectarse a la base de datos. El parámetro `DsnName` es obligatorio y no puede estar vacío.
- **Username**: el nombre de usuario que se usa para conectarse a la base de datos. Si este parámetro no se especificó, se usa la autenticación de Windows.
- **Password**: la contraseña del usuario que se conecta a la base de datos. Si este parámetro no se especifica y no se usa la autenticación de Windows, se le pedirá que introduzca la contraseña más adelante.

- BackupFilePath: la ruta del archivo de la copia de seguridad de View Composer.

Los parámetros DsnName y BackupFilePath son obligatorios y no pueden estar vacíos. Los parámetros Username y Password son opcionales.

### Procedimiento

- 1 Copie los archivos de copia de seguridad de View Composer del equipo del servidor de conexión de View en una ubicación a la que pueda acceder el equipo donde está instalado el servicio de VMware Horizon View Composer.

- 2 En el equipo donde View Composer está instalado, detenga el servicio de VMware Horizon View Composer.

- 3 Abra una ventana de símbolo de sistema de Windows y diríjase al archivo ejecutable SviConfig.

El archivo se encuentra con la aplicación View Composer. La ruta predeterminada es C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe.

- 4 Ejecute el comando SviConfig restoredata.

```
sviconfig -operation=restoredata
          -DsnName=nombre_recurso_base_de_datos_destino_(DSN)
          -Username=nombre_usuario_administrador_base_de_datos
          -Password=contraseña_administrador_base_de_datos
          -BackupFilePath=ruta_al_archivo_de_copia_de_seguridad_de_View_Composer
```

Por ejemplo:

```
sviconfig -operation=restoredata -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 View Composer.

### Pasos siguientes

Para los códigos de resultado de salida del comando SviConfig restoredata, consulte [Códigos de resultado de la restauración de la base de datos de View Composer](#).

## Códigos de resultado de la restauración de la base de datos de View Composer

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

**Tabla 8-2. Códigos de resultado de restoredata**

Código	Descripción
0	La operación finalizó correctamente.
1	No se encuentra el DSN proporcionado.

Código	Descripción
2	Se proporcionaron credenciales de administrador de la base de datos no válidas.
3	La unidad de la base de datos no es compatible.
4	Se produjo un problema inesperado y el comando no se completó.
14	Hay otra aplicación utilizando el servicio de VMware Horizon View Composer. Desconecte el servicio antes de ejecutar el comando.
15	Se produjo un problema durante el proceso de restauración. Los detalles aparecen en la salida del registro en pantalla.

## Exportar datos en la base de datos de View Composer

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

**Importante** Use la utilidad SviConfig solo si es un administrador de View Composer con experiencia.

### Requisitos previos

De forma predeterminada, View almacena los archivos de copia de seguridad en la unidad C: del equipo del servidor de conexión de View en C:\Programdata\VMware\VDM\backups.

Familiarícese con los parámetros de SviConfig `exportdata`:

- **DsnName:** el DSN que se usa para conectarse a la base de datos. Si no está especificado, el nombre de DNS, el nombre de usuario y la contraseña se recuperarán del archivo de configuración del servidor.
- **Username:** el nombre de usuario que se usa para conectarse a la base de datos. Si este parámetro no se especificó, se usa la autenticación de Windows.
- **Password:** la contraseña del usuario que se conecta a la base de datos. Si este parámetro no se especifica y no se usa la autenticación de Windows, se le pedirá que introduzca la contraseña más adelante.
- **OutputFilePath:** la ruta del archivo de salida.

### Procedimiento

- 1 En el equipo donde View Composer está instalado, detenga el servicio de VMware Horizon View Composer.

- 2 Abra una ventana de símbolo de sistema de Windows y diríjase al archivo ejecutable SviConfig.

El archivo se encuentra con la aplicación View Composer.

*View-Composer-installation-directory\sviconfig.exe*

### 3 Ejecute el comando SviConfig exportdata.

```
sviconfig -operation=exportdata
          -DsnName=nombre_recurso_base_de_datos_destino_(DSN)
          -Username=nombre_usuario_administrador_base_de_datos
          -Password=contraseña_administrador_base_de_datos
          -OutputFilePath=ruta_al_archivo_de_salida_de_View_Composer
```

Por ejemplo:

```
sviconfig -operation=exportdata -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 exportar la base de datos de View Composer](#).

### Códigos de resultado de exportar la base de datos de View Composer

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

**Tabla 8-3. Códigos Exportdata ExitStatus**

Código	Descripción
0	Los datos se exportan correctamente.
1	No se encuentra el nombre DSN proporcionado.
2	Las credenciales no son válidas.
3	El controlador no es compatible con la base de datos proporcionada.
4	Se produjo un problema inesperado.
18	No se puede conectar con el servidor de la base de datos.
24	No se puede abrir el archivo de salida.

## Supervisar los componentes de View

Puede utilizar el panel de control de View Administrator para consultar el estado de los componentes de vSphere y View en la implementación de View.



View Administrator muestra información para supervisar las instancias del servidor de conexión de View, la base de datos de eventos, los servidores de seguridad, los servicios de View Composer, los almacenes de datos, las instancias de vCenter Server y los dominios.

---

**Nota** View no puede determinar los datos sobre el estado de los dominios de Kerberos. View Administrator muestra el estado de los dominios de Kerberos como desconocido aunque un dominio esté configurado y funcione.

---

### Procedimiento

- 1 En View Administrator, haga clic en **Panel**.
- 2 En el panel Estado del sistema, expanda **Componentes de View**, **Componentes de vSphere** u **Otros componentes**.
  - Si aparece una flecha hacia arriba de color verde, significa que el componente no tiene ningún problema.
  - La flecha hacia abajo de color rojo indica que el componente no está disponible o no funciona.
  - Si se muestra una flecha doble amarilla, el componente presenta un estado de advertencia.
  - Cuando el estado de un componente es desconocido, aparece un signo de interrogación.
- 3 Haga clic en el nombre de un componente.

Se mostrará un cuadro de diálogo con el nombre, la versión, el estado y otra información sobre el componente.

### Pasos siguientes

Utilice vCenter Server para supervisar cualquier clúster de Virtual SAN y los discos que formen parte de un almacén de datos Virtual SAN. Para obtener más información sobre cómo supervisar Virtual SAN en la actualización 1 de vSphere 5.5, consulte el documento *Almacenamiento de vSphere* y la documentación *Supervisión y rendimiento de vSphere*. Para obtener más información sobre cómo supervisar Virtual SAN en vSphere 6 o versiones posteriores, consulte el documento *Administrar VMware Virtual SAN*.

## Supervisar el estado de las máquinas

Puede supervisar el estado de las máquinas de la implementación de View usando el panel de control de View Administrator. Por ejemplo, puede mostrar todas las máquinas desconectadas o las máquinas que estén en modo mantenimiento.

### Requisitos previos

Familiarícese con los valores de estado de las máquinas virtuales. Consulte [Estado de las máquinas virtuales de vCenter Server](#).

### Procedimiento

- 1 En View Administrator, haga clic en **Panel**.

- 2 En el panel Estado de la máquina, expanda una carpeta de estado.

Opción	Descripción
Preparando	Muestra los estados mientras la máquina se aprovisiona, se elimina o está en modo mantenimiento.
Máquinas con problemas	Muestra los estados de error.
Preparado para su uso	Muestra los estados cuando la máquina está lista para su uso.

- 3 Ubique el estado de la máquina y haga clic en el número hipervinculado que aparece junto a ella.

La página **Máquinas** muestra todas las máquinas con el estado seleccionado.

#### Pasos siguientes

Puede hacer clic en el nombre de una máquina para ver los detalles sobre la máquina o en la flecha de retroceso de View Administrator para volver a la página Panel.

## Comprender los servicios de View

La operación de las instancias del servidor de seguridad de View 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 View. Si detiene los servicios de View en un host del servidor de conexión de View 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 View que controla no responde.

## Detener e iniciar servicios de View

La operación de las instancias del servidor de seguridad de View 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 View.

Al detener los servicios de View, 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 de View 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 de View y los servidores de seguridad, como se describe en [Servicios en un host del servidor de conexión de View](#) 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 de View 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 en un host del servidor de conexión de View

La operación de View depende de varios dispositivos que se ejecutan en el host del servidor de conexión de View.

**Tabla 8-4. Servicios de los hosts del servidor de conexión de View**

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 de View 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 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.
Componente de bus de mensajería VMware Horizon View	Manual	Proporciona servicios de mensajería entre los componentes de View. 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 al servidor de conexión de View a través de la puerta de enlace segura de PCoIP.
VMware Horizon View Script Host	Deshabilitada	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.

Nombre del servicio	Tipo de inicio	Descripción
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 View, este servicio asegura que los datos existentes se migren correctamente.

## Servicios de un servidor de seguridad

La operación de View depende de varios dispositivos que se ejecutan en el servidor de seguridad.

**Tabla 8-5. Servicios del servidor de seguridad**

Nombre del servicio	Tipo de inicio	Descripción
Puerta de enlace segura de Blast VMware Horizon View	Automático	Proporciona servicios HTML Access y Blast Extreme seguros. Este servicio debe ejecutarse si los clientes se conectan a este servidor de seguridad a través de la puerta de enlace segura de Blast.
Servidor de seguridad de VMware Horizon View	Automático	Proporciona servicios del servidor de seguridad. Este servicio siempre debe estar en ejecución. Al iniciar o detener este servicio, también se inician o se detienen los servicios de la puerta de enlace de seguridad y el marco de trabajo.
Componente de marco de trabajo VMware Horizon View	Manual	Proporciona servicios de registro de eventos, seguridad y marco de trabajo COM+. Este servicio siempre debe estar en ejecución.
Puerta de enlace segura PCoIP de VMware Horizon View	Manual	Proporciona servicios de la puerta de enlace segura de PCoIP. Este servicio debe ejecutarse si los clientes se conectan a este servidor de seguridad a través de la puerta de enlace segura de PCoIP.
Componente de puerta de enlace de seguridad de VMware Horizon View	Manual	Proporciona servicios de puerta de enlace común. Este servicio siempre debe estar en ejecución.

## Cambiar la clave de licencia del producto

Si caduca la licencia actual en un sistema o si desea acceder a funciones de View que no tienen licencia en ese momento, puede usar View Administrator para cambiar la clave de licencia del producto.

Puede agregar una licencia a View mientras View 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 View y de funciones de los complementos como View Composer y las aplicaciones remotas, obtenga una clave de licencia del producto válida.

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Licencia y uso del producto**.

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

- 2 Haga clic en **Editar licencia**.

- 3 Introduzca el número de serie de la licencia y haga clic en **Aceptar**.

La ventana **Licencia de producto** muestra la información actualizada de la licencia.

- 4 Verifique la fecha de caducidad de la licencia.

- 5 Verifique que las licencias de View Composer, de escritorio y de aplicaciones remotas estén habilitadas o deshabilitadas, según la edición de VMware Horizon 7 que la licencia de producto le permita utilizar.

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

- 6 Verifique que el modelo de uso de la licencia coincida con el modelo que se usa en la licencia de producto.

El uso se contabiliza según el número de usuarios con nombre o de usuarios simultáneos, dependiendo de la edición y el acuerdo de uso de la licencia de producto.

## Supervisar la licencia y el uso del producto

En View Administrator, puede supervisar los usuarios activos que están conectados a View en ese momento. La página **Licencia y uso del producto** muestra los números de uso histórico actuales y más elevados. Puede usar estos números para realizar un seguimiento del uso de la licencia del producto. También puede restablecer los datos históricos de uso y volver a comenzar con los datos actuales.

View proporciona dos modelos de uso de la licencia, uno para los usuarios designados y otro para los usuarios simultáneos. View 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, View cuenta el número de usuarios únicos que accedieron al entorno de View. Si un usuario designado ejecuta varios escritorios de usuario único, escritorios RDS y aplicaciones remotas, este usuario solo se cuenta una vez.

Para los usuarios designados, la columna **Actual** de la página **Licencia y uso del producto** muestra el número de usuarios desde que la implementación de View 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, View 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 RDS se cuentan por usuario. Si un usuario simultáneo ejecuta varias aplicaciones y sesiones de escritorios RDS, este usuario solo se cuenta una vez, aunque se alojen aplicaciones o escritorios RDS diferentes en hosts RDS diferentes. Si un usuario simultáneo ejecuta un escritorio de usuario único y aplicaciones y escritorios RDS adicionales, el usuario solo se cuenta una vez.

Para los usuarios simultáneos, la columna **El más alto** de la página **Licencia y uso del producto** muestra el número más elevado de los usuarios de aplicaciones y escritorios RDS y las sesiones de escritorios simultáneos desde que la implementación de View se configuró por primera vez o desde la última vez que restableció el **recuento máximo**.

## Restablecer los datos de uso de la licencia del producto

En View Administrator, puede restablecer los datos históricos de uso del producto y volver a comenzar con los datos actuales.

Un administrador con el privilegio **Administrar configuración global y directivas** puede seleccionar las opciones **Restablecer el recuento máximo** y **Restablecer el recuento de usuarios designados**. Para restringir el acceso a esas opciones, otorgue este privilegio únicamente a administradores designados.

### Requisitos previos

Familiarícese con el uso de la licencia del producto. Consulte [Supervisar la licencia y el uso del producto](#).

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Licencia y uso del producto**.
- 2 (opcional) En el panel **Uso**, seleccione **Restablecer el recuento máximo**.  
El número histórico máximo de conexiones simultáneas se restablece al número actual.
- 3 (opcional) En el panel **Uso**, seleccione **Restablecer el recuento de usuarios designados**.  
El número histórico máximo de usuarios designados se restablece a 0.

---

**Nota** Al seleccionar **Actualizar la información general del usuario** en la página **Usuarios y grupos** también restablece a 0 el número máximo de usuarios designados.

---

## Actualizar la información general del usuario desde Active Directory

Puede actualizar View con la información de usuario actual que se almacena en Active Directory. Esta función actualiza el nombre, el teléfono, el correo electrónico, el nombre de usuario y el dominio de Windows predeterminado de los usuarios de View. También se actualizan los dominios externos de confianza.

Use esta función si modifica la lista de dominios externos de confianza en Active Directory, sobre todo si las relaciones de confianza modificadas entre los dominios afectan a los permisos de usuario en View.

Esta función examina Active Directory para encontrar la información de usuario más reciente y actualiza la configuración de View.

Al actualizar la información de usuario general, también se restablece el número de usuarios designados a 0. Este número aparece en la página **Licencia y uso del producto** de View Administrator. Consulte [Restablecer los datos de uso de la licencia del producto](#).

También puede usar el comando `vdmadmin` para actualizar la información de dominio y de usuario. Consulte [Actualizar las entidades de seguridad externa con la opción -F](#).

### Requisitos previos

Compruebe que pueda iniciar sesión en View Administrator como administrador con el privilegio **Administrar configuración global y directivas**.

### Procedimiento

- 1 En View Administrator, haga clic en **Usuarios y grupos**.
- 2 Seleccione si desea actualizar la información de todos los usuarios o de uno individual.

Opción	Acción
Para todos los usuarios	Haga clic en <b>Actualizar la información general del usuario</b> . Si actualiza todos los usuarios y los grupos, esta acción puede tardar un tiempo prolongado.
Para un usuario individual	<ol style="list-style-type: none"> <li>a Haga clic en el nombre del usuario que desea actualizar.</li> <li>b Haga clic en <b>Actualizar la información general del usuario</b>.</li> </ol>

## Migrar View Composer a otro equipo

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

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

- **Directrices para migrar View Composer**

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

- **Migrar View Composer con una base de datos existente**

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

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

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

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

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

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

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

## Directrices para migrar View Composer

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

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

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

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



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

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

---

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

---

## Migrar View Composer con una base de datos existente

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

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

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

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

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

### Requisitos previos

- Familiarícese con los requisitos de migración de View Composer. Consulte [Directrices para migrar View Composer](#).
- Familiarícese con los pasos para migrar el contenedor de claves RSA al nuevo servicio VMware Horizon View Composer. Consulte [Preparar Microsoft .NET Framework para migrar las claves RSA y Migrar el contenedor de claves RSA al nuevo servicio de View Composer](#).
- Familiarícese con la instalación del servicio de VMware Horizon View Composer. Consulte "Instalar View Composer" en el documento *Instalación de View*.

- Familiarícese con la configuración de los certificados SSL para View Composer. Consulte "Configurar certificados SSL para View Servers" en el documento *Instalación de View*.
- Familiarícese con la configuración de View Composer en View Administrator. Consulte [Configurar las opciones de View Composer](#) y [Configurar los dominios de View Composer](#).

## Procedimiento

- 1 Deshabilite el aprovisionamiento de la máquina virtual en la instancia de vCenter Server que esté asociada con el servicio VMware Horizon View Composer.
  - a En View Administrator, seleccione **Configuración de View > Servidores**.
  - b En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server y haga clic en **Deshabilitar aprovisionamiento**.
- 2 (opcional) Migre la base de datos de View Composer a una nueva ubicación.  
 Si necesita realizar este paso, consulte al administrador de base de datos para obtener instrucciones sobre la migración.
- 3 Desinstale el servicio VMware Horizon View Composer de la máquina actual.
- 4 (opcional) Migre el contenedor de claves RSA a la nueva máquina.
- 5 Instale el servicio VMware Horizon View Composer en la nueva máquina.  
 Durante la instalación, especifique el DSN de la base de datos que utilizó el servicio original VMware Horizon View Composer. Especifique también el nombre de usuario de administrador del dominio y la contraseña que se proporcionaron para el origen de datos ODBC de dicha base de datos.  
 Si migró la base de datos, el DSN y la información del origen de datos se dirigen a la nueva ubicación de la base de datos. Independientemente de que se migrara o no la base de datos, el nuevo servicio VMware Horizon View Composer debe tener acceso a la información de la base de datos original sobre los clones vinculados.
- 6 Configure un certificado de servidor SSL para View Composer en la nueva máquina.  
 Puede copiar el certificado que se instaló para View Composer en la máquina original o instalar uno nuevo.
- 7 En View Administrator, establezca la nueva configuración de View Composer.
  - a En View Administrator, seleccione **Configuración de View > Servidores**.
  - b En la pestaña **vCenter Servers**, seleccione la instancia de vCenter Server que esté asociada con dicho servicio de View Composer y haga clic en **Editar**

- c En el panel Configuración del servidor View Composer, haga clic en **Editar** e introduzca la nueva configuración de View Composer.

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

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

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

## Migrar View Composer sin máquinas virtuales de clones vinculados

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

### Requisitos previos

- Familiarícese con la instalación del servicio de VMware Horizon View Composer. Consulte "Instalar View Composer" en el documento *Instalación de View*.
- Familiarícese con la configuración de los certificados SSL para View Composer. Consulte "Configurar certificados SSL para View Servers" en el documento *Instalación de View*.
- Familiarícese con los pasos para eliminar View Composer de View Administrator. Consulte [Eliminar View Composer de View](#).

Antes de eliminar View Composer, verifique que ya no administre ningún escritorio de clones vinculados. Si aparece alguno, debe eliminarlo.

- Familiarícese con la configuración de View Composer en View Administrator. Consulte [Configurar las opciones de View Composer](#) y [Configurar los dominios de View Composer](#).

### Procedimiento

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

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

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

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

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

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

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

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

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

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

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

## Preparar Microsoft .NET Framework para migrar las claves RSA

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

### Requisitos previos

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

### Procedimiento

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

## Pasos siguientes

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

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

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

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

### Requisitos previos

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

### Procedimiento

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

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

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

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

- 3 Copie el archivo `keys.xml` en el equipo de destino en el que desea instalar el nuevo servicio de VMware Horizon View Composer.

- 4 En el equipo de destino, abra una ventana de símbolo de sistema y diríjase al directorio %windir%\Microsoft.NET\Framework\v2.0xxxxx.

- 5 Escriba el comando `aspnet_regiis` para migrar los datos del par de claves RSA.

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

donde *ruta* es la ruta del archivo exportado.

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

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

### Pasos siguientes

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

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

## Actualizar los certificados en una instancia del servidor de conexión de View, en el servidor de seguridad o en View Composer

Cuando recibe certificados intermedios o certificados SSL de servidor actualizados, importe los certificados en el almacén de certificados del equipo local Windows de cada host de View Composer, del servidor de seguridad o del servidor de conexión de View.

Normalmente, los certificados del servidor caducan después de 12 meses. Los certificados raíz e intermediarios caducan después de 5 o 10 años.

Para obtener más información sobre cómo importar servidores y certificados intermedios, consulte "Configurar el servidor de conexión de View, el servidor de seguridad o View Composer para usar un nuevo certificado SSL" en el documento *Instalación de View*.

### Requisitos previos

- Obtenga los certificados intermedios y los servidores actualizados desde la CA antes de que caduquen los certificados que son válidos en ese momento.
- Compruebe que el complemento Certificado se agregó a MMC en el Windows Server en el que se instaló la instancia del servidor de conexión de View, el servidor de seguridad o el servicio de VMware Horizon View Composer.

### Procedimiento

- 1 Importe el certificado de servidor SSL firmado en el almacén de certificados del equipo local Windows del host de Windows Server.
  - a En el complemento Certificado, importe el certificado del servidor en la carpeta **Certificados (equipo local) > Personal > Certificados**.
  - b Seleccione **Marcar esta clave como exportable**.
  - c Haga clic en **Siguiente** y en **Finalizar**.

- 2 En el servidor de conexión de View o el servidor de seguridad, elimine el certificado Nombre descriptivo, **vdm**, del certificado antiguo que se expidió para View Server.
  - a Haga clic con el botón secundario en el certificado antiguo y, a continuación, en **Propiedades**.
  - b En la pestaña General, elimine el texto de Nombre descriptivo, **vdm**.
- 3 En el servidor de conexión de View o en el servidor de seguridad, agregue el certificado Nombre descriptivo, **vdm**, al nuevo certificado que reemplaza al certificado anterior.
  - a Haga clic con el botón secundario en el nuevo certificado y, a continuación, en **Propiedades**.
  - b En la pestaña General, en el campo Nombre descriptivo, escriba **vdm**.
  - c Haga clic en **Aplicar** y en **Aceptar**.
- 4 En un certificado de servidor que se expidió para View Composer, ejecute la utilidad SviConfig ReplaceCertificate para enlazar el nuevo certificado al puerto que usa View Composer.  
 Esta utilidad reemplaza el enlace con el antiguo certificado por el enlace con el nuevo.
  - a Detenga el servicio de VMware Horizon View Composer.
  - b Abra una ventana de símbolo de sistema de Windows y diríjase al archivo ejecutable SviConfig.  
 El archivo se encuentra con la aplicación View Composer. La ruta predeterminada es C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe.
  - c Escriba el comando SviConfig ReplaceCertificate. Por ejemplo:
 

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

La utilidad muestra una lista numerada de certificados SSL que están disponibles en el almacén de certificados del equipo local Windows.
  - d Para seleccionar un certificado, escriba su número y pulse Intro.
- 5 Si se expiden certificados intermedios para un host de View Composer, del servidor de seguridad o del servidor de conexión de View, importe la actualización más reciente del certificado intermedio en la carpeta **Certificados (equipo local) > Entidades de certificación > Certificados** en el almacén de certificados de Windows.
- 6 Reinicie el servicio del servidor de conexión VMware Horizon View, del servidor de seguridad VMware Horizon View o de VMware Horizon View Composer para que se realicen los cambios.

## Información recopilada por el programa de mejora de la experiencia de cliente

Puede participar en un programa de mejora de la experiencia de cliente (CEIP). Si participa en el programa, VMware recopila datos anónimos sobre la implementación para mejorar la respuesta de VMware a los requisitos de los usuarios. VMware usa esta información para mejorar la calidad, la fiabilidad y el rendimiento de los productos. No se recopila ningún dato que identifique a su organización.

La participación en este programa es opcional. Si no desea participar, desmarque la opción cuando instala el servidor de conexión de View con una configuración nueva. Si cambia de opinión después de la instalación, puede unirse al programa o descartar su participación editando la página Licencia y uso del producto en View Administrator.

Antes de recopilar la información, VMware convierte en anónimos todos los campos que contengan información específica de su organización. Los campos saneados identifican los equipos, el almacenamiento de datos, las funciones de red, las aplicaciones y los usuarios. Por ejemplo, las direcciones IP y las especificaciones de personalización de las máquinas virtuales pasan a ser anónimas.

VMware sanea un campo generando un hash del valor real. Cuando se recopila un valor hash, VMware no puede identificar el valor real, pero puede detectar los cambios que se producen en el valor si modifica el entorno.

Para ayudarle a determinar si unirse al programa o no, puede consultar los campos desde los que VMware recopila datos. También puede examinar todos los campos saneados. Los campos están organizados por el componente View. Consulte [Datos de View globales recopilados por VMware](#) y los temas relacionados que aparecen a continuación.

## Cómo VMware asegura su privacidad

VMware se compromete a proteger su privacidad y realiza diferentes pasos para asegurarse de que ningún dato recopilado por el programa de mejora de la experiencia de cliente incluya información personal que pueda identificar de forma única un usuario o cliente particular. El programa no recopila ninguna información que se pueda utilizar para identificarle o ponerse en contacto con usted. No se recopila ningún dato que identifique a su organización o a los usuarios.

Cuando la función CEIP está habilitada, el servidor de conexión de View recopila información desde la implementación y realiza las siguientes acciones con los datos:

- 1 Los datos que puedan identificar de forma única a su implementación, como los usuarios, nombres de servidores, direcciones IP y rutas del servidor de red pasan a ser anónimos al ejecutar una función hash unidireccional en los datos. Este procedimiento permite a VMware recopilar información útil sobre cómo se incluyen en la implementación varios usuarios, equipos y servidores únicos sin recopilar direcciones, nombres de usuarios o nombres de servidores específicos.
- 2 El conjunto de datos completo se cifra con una clave pública. La clave privada que es necesaria para descifrar el conjunto de datos está disponible únicamente para VMware.
- 3 La información cifrada y anónima se envía a VMware a través de HTTPS.

Puede revisar la lista completa de campos desde los que se recopilan los datos, incluidos los campos que se vuelven anónimos. Consulte [Datos de View globales recopilados por VMware](#) y los temas relacionados que aparecen a continuación.



## Previsualizar los datos recopilados para el programa de mejora de la experiencia de cliente

Puede previsualizar los datos que VMware recibirá antes de que se cifren y se envíen. Cuando habilita esta opción, el servidor de conexión de View escribe el conjunto de datos en el disco en lugar de cifrar y enviar los datos a VMware.

Configure la opción para escribir los datos del CEIP en el disco en lugar de enviar los datos a VMware como una opción global en el directorio LDAP de View. La utilidad Editor ADSI le permitirá modificar el LDAP de View. La utilidad Editor ADSI se instala con el servidor de conexión de View. Cuando cambia el LDAP de View en una instancia del servidor de conexión de View, el cambio se propaga a todas las instancias replicadas del servidor de conexión de View.

### Procedimiento

- 1 Inicie la utilidad Editor ADSI en el host del servidor de conexión de View.
- 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 plenamente cualificado (FQDN) del host del servidor de conexión de View seguido por el puerto 389.  
Por ejemplo: localhost:389 o miequipo.midominio.com:389
- 4 En el objeto **CN=Common, OU=Global, OU=Properties**, establezca el valor del atributo **pae-ceipDumpOnly** en 1.
- 5 Reinicie el servidor de conexión de View.

Los archivos de datos se escriben en formato JSON de texto sin formato en el directorio %PROGRAMFILES%\VMware\VMware View\Server\broker\temp\spool de la instancia del servidor de conexión de View.

### Pasos siguientes

Para revertir la opción y comenzar a enviar datos a VMware, cambie el valor del atributo **pae-ceipDumpOnly** a 0 y reinicie el servidor de conexión de View.

## Información adicional sobre el Programa de mejora de la experiencia de cliente

Tras seleccionar participar en el CEIP, se recopilan los datos de la primera instancia del servidor de conexión de View que se inicia en una implementación de View. Los datos de la configuración se recopilan semanalmente. Los datos de uso y de rendimiento se recopilan cada hora. Si la instancia del servidor de conexión de View no tiene acceso a Internet, la información se guarda en el disco hasta que vuelva a estar disponible la conexión a Internet.

Si decide participar, puede dejar de hacerlo en cualquier momento. Puede unirse o dejar de participar al editar la opción **Enviar datos anónimos a VMware** en la página Licencia y uso del producto en View Administrator. Para que se apliquen los cambios, reinicie cada instancia del servidor de conexión de View en el entorno.

La recopilación de datos del CEIP no supone un impacto en el uso del disco ni un rendimiento negativo de la implementación de View. La información que se recopila para VMware se envía a la instancia del servidor de conexión de View independientemente de si la función CEIP está habilitada. De forma predeterminada, habilitar la función puede consumir un máximo de 100 MB de espacio de disco en la instancia del servidor de conexión de View para almacenar información antes de enviarla a VMware. De forma predeterminada, se descartan los datos no enviados con más de ocho días.

Si un firewall bloquea el acceso a Internet de las instancias del servidor de conexión de View, puede seguir usando el CEIP. Cuando el CEIP está habilitado, las instancias del servidor de conexión de View intentan conectarse periódicamente con HTTPS a la URL de recopilación de datos en <https://ceip.vmware.com>. Si la conexión está bloqueada o no es accesible debido a una restricción del firewall o del servidor del proxy, el servidor de conexión de View almacena los datos del CEIP hasta que los registros superen la antigüedad máxima configurada, ocho días de forma predeterminada, o bien los datos totales recopilados superen el tamaño de spool, 100 MB de forma predeterminada.

Puede cambiar la ubicación, el tamaño máximo y la antigüedad máxima del spool de datos del CEIP. El tamaño y la ubicación del spool se rige por la siguiente configuración en la base de datos LDAP de View:

<b>pae-ceipSpoolDirectory</b>	Directorio en el que se almacena en caché los datos del CEIP antes de enviarlos a VMware.  Predeterminado: Program Files\VMware\VMware View\Server\broker\temp\spool
<b>pae-ceipMaxSpoolSize</b>	Tamaño máximo, en bytes, de los datos de spool temporales.  Predeterminado: 100 MB
<b>pae-ceipMaxSpoolAge</b>	Antigüedad máxima de los datos en el spool local temporal.  Predeterminado: 8 días

Si participa en el CEIP, no recibirá correos no deseados ni se pondrán en contacto con usted. El CEIP no recopila información de contacto como el nombre, la dirección postal, la dirección de correo electrónico o el número de teléfono. El CEIP no le pedirá que participe en encuestas o que lea correos electrónicos no deseados ni se pondrá en contacto con usted de ninguna otra forma.

## Datos de View globales recopilados por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopila datos globales sobre el entorno de View. Los campos que contienen información personal son anónimos.

**Tabla 8-6. Información sobre las opciones de configuración global**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Vida útil máxima, en segundos, de una sesión del servidor de conexión de View	No	180.000
Cantidad de tiempo, en segundos, antes de que el servidor de conexión de View desconecte de forma forzada a los usuarios si no se envía ningún dato desde el cliente	No	36.000
Cantidad de tiempo en segundos, durante el que un usuario puede estar inactivo antes de que el servidor de conexión de View bloquee las credenciales Single Sign-On (SSO) del usuario	No	900
Cantidad de tiempo, en minutos, antes de que las credenciales SSO se borren para los inicios de los escritorios	No	-1 (significa nunca)
Cantidad de tiempo, en minutos, antes de que las credenciales SSO se borren para los inicios de las aplicaciones	No	-1 (significa nunca)
Tiempo de espera de la sesión de la consola de View Administrator, en segundos	No	3.000
Muestra un mensaje previo al inicio de sesión cuando los usuarios se conectan a las instancias del servidor de conexión de View en este pod	No	0 o 1
El escritorio remoto puede ejecutar un sistema operativo de servidor	No	True o false
El servidor de Mirage está habilitado	No	True o false
URL del servidor de Mirage, incluido el número de puerto	Yes	Ninguno
¿Está habilitado True SSO?	Sí	Ninguno
¿Existe algún servidor de inscripciones principal configurado para True SSO?	Sí	Ninguno
¿Existe algún servidor de inscripciones secundario configurado para True SSO?	Sí	Ninguno

**Tabla 8-7. Información de estado global**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
View Servers pueden ponerse en contacto con el controlador de dominio.	No	True o false
El DNS del dominio de Active Directory	Yes	Ninguna
El dominio es un dominio estilo NT4.	No	True o false
El nombre del dominio	Yes	Ninguna
El estado del dominio	No	Aceptar
El tipo de relación de confianza con el dominio	No	Dominio principal, bidireccional, bosque bidireccional, etc.

## Datos del servidor de conexión de View recopilados por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopila datos de algunos campos del servidor de conexión de View. Los campos que contienen información personal son anónimos.

**Tabla 8-8. Información de configuración recopilada desde el servidor de conexión de View**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
El nombre común (CN) de la entrada del servidor de conexión de View en el LDAP de View	Yes	Ninguno
El servidor de conexión de View está deshabilitado	No	True o false
La autenticación SecureID está configurada y activa	No	True o false
La autenticación RADIUS está configurada y activa	No	True o false
La autenticación del servidor SAML se permite, es obligatoria o está deshabilitada	No	0 = Deshabilitada 1 = Permitida 2 = Obligatoria
Tipo de instalación del servidor de conexión de View	No	0 = servidor de conexión de View 1 = servidor de seguridad
¿Debe coincidir el nombre de la autenticación SecureID con el nombre de Active Directory?	No	True = el nombre de la autenticación SecureID está asignado False = el nombre de la autenticación SecureID no está asignado
¿Se permite a los clientes que pasen por el túnel de seguridad?	No	True o false
¿Se permite a los clientes que se deriven por la puerta de enlace segura PCoIP?	No	True o false
Configuración de la autenticación con tarjeta inteligente	No	Desactivado, opcional u obligatorio
¿Se debe cerrar la sesión de los usuarios automáticamente cuando se extraiga las tarjetas inteligentes?	No	True o false
Carpeta en la que las copias de seguridad de LDAP de View se almacenan	Yes	Ninguno
Unidades de tiempo para establecer la frecuencia de las copias de seguridad de LDAP de View	No	Hora, día o semana
Frecuencia de copias de seguridad de LDAP de View	No	Entero
Hora de la copia de seguridad de LDAP de View	No	Entero
Número máximo de copias de seguridad de LDAP de View que se deben almacenar	No	Entero
Hora de la última copia de seguridad de LDAP de View	No	21 de febrero de 2014, 12:00:10
Estado de la última copia de seguridad de LDAP de View	No	Aceptar
Está pendiente la copia de seguridad de LDAP de View inmediata	No	True o false
Etiquetas asociadas con la instancia del servidor de conexión de View	Yes	Ninguna

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Si la instancia del servidor de conexión de View está emparejada con el servidor de seguridad	No	0 = No emparejada 1 = Emparejada
El nombre distintivo (DN) de la instancia del servidor de conexión de View en el LDAP	Yes	Ninguna
Periodo de tiempo durante el cual la contraseña de emparejamiento de los servidores de seguridad es válida	No	
El host/nombre del nodo de la instancia del servidor de conexión de View	Yes	Ninguna
El número de la versión solamente de la instancia del servidor de conexión de View	No	6.0.0
La versión y la compilación completas de la instancia del servidor de conexión de View	No	6.0.0-123455
Volver a conectarse a la puerta de enlace segura	No	True o false
Protocolo del cliente de túnel	No	
Protocolo al que escuchan la instancia del servidor de conexión de View o el servidor de seguridad	No	

**Tabla 8-9. Información del estado recopilada desde el servidor de conexión de View**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
El número de compilación de la instancia del servidor de conexión de View	No	123456
Nombre del grupo replicado del servidor de conexión de View, normalmente el primer nombre del nodo de la instancia del servidor de conexión de View	Yes	Ninguna
El nombre DNS de la instancia del servidor de conexión de View	Yes	Ninguna
La dirección IP de la instancia del servidor de conexión de View	Yes	Ninguna
El nombre del host NetBIOS de la instancia del servidor de conexión de View	Yes	Ninguna
El número actual de sesiones en esta instancia del servidor de conexión de View	No	Entero
El número máximo de sesiones en esta instancia del servidor de conexión de View	No	Entero
El número actual de sesiones de View Composer en esta instancia del servidor de conexión de View	No	Entero
El número máximo de sesiones de View Composer en esta instancia del servidor de conexión de View	No	Entero
La versión de la instancia del servidor de conexión de View	No	6.0.0

**Tabla 8-10. Datos de uso dinámico recopilados desde el servidor de conexión de View**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Número de veces que se invocaron los cmdlets de PowerShell individuales	No	Lista de enteros
Número de veces que se invocaron los métodos de la API de View individuales durante el minuto anterior	No	Lista de enteros
Tasa de inicio de sesión, con contraseñas, en todo momento	No	Flotante
Tasa de inicio de sesión, con certificado del servidor SSL, en todo momento	No	Flotante
Tasa de inicio de sesión, con autenticación delegada como SAML, en todo momento	No	Flotante
Porcentaje del uso medio de la CPU	No	Entero
Porcentaje del uso medio de la memoria	No	Entero
Inicios de sesión medio con y sin contraseñas disponibles para SSO	No	Flotante
Número de veces que se iniciaron las conexiones de escritorios con cada tipo de protocolos de visualización (PCoIP, RDP y VMware Blast)	No	Lista de enteros
Número de veces que se estableció una nueva conexión cliente a una aplicación remota, para cada tipo de protocolo de visualización (PCoIP, RDP y VMware Blast)	No	Lista de enteros
Número de veces que el inicio de una aplicación remota resulta en una nueva conexión, una conexión reutilizada, una conexión de sesión nueva y una conexión de sesión reutilizada	No	Lista de enteros
Número de veces que las conexiones a los escritorios se iniciaron para un usuario que tiene autorización para $n$ número de escritorios	No	Lista de enteros, como una lista de cuántos usuarios tienen autorización para 1 escritorios, 2 escritorios, 3 escritorios, etc.
Número de veces que las conexiones a las aplicaciones se iniciaron para un usuario que tiene autorización para $n$ número de aplicaciones	No	Lista de enteros
Número de veces $n$ que las sesiones de los protocolos (como PCoIP) existieron cuando otro usuario inicia otra aplicación. Por ejemplo, un usuario inicia una quinta aplicación, pero como todas las aplicaciones están en la misma granja del servidor, solo existe una sesión.	No	Lista de enteros, como una lista de cuántos usuarios tienen una sola sesión, cuántos tienen dos sesiones, etc.

## Datos del servidor de seguridad recopilados por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopilará información de los campos del servidor de seguridad. Los campos que contienen información personal son anónimos.

**Tabla 8-11. Información del servidor de seguridad**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
El número de sesiones PCoIP que se están ejecutando en la puerta de enlace segura del servidor de seguridad	No	Entero
El número de sesiones de cualquier tipo que se están ejecutando en la puerta de enlace segura del servidor de seguridad	No	Entero
El número de compilación del servidor de seguridad	No	123456
El nombre del host del servidor de seguridad	Yes	Ninguno
IPsec está activo	No	True o false
La puerta de enlace segura está inactiva	No	True o false
El número actual de sesiones	No	Entero
La URL de la puerta de enlace segura	Yes	Ninguno
El número de la versión del servidor de seguridad	No	6.0.0

## Información del grupo de escritorios recopilada por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopilará información de ciertos campos del grupo de escritorios. Los campos que contienen información personal son anónimos.

**Tabla 8-12. Información sobre la configuración recopilada desde grupos de escritorios**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
El nombre común (common name, CN) para la entrada del grupo de escritorios en el LDAP de View	Yes	Ninguna
El nombre descriptivo para mostrar del grupo de escritorios	Yes	Ninguna
El grupo de escritorios está deshabilitado	No	True o false
Tipo de grupo de escritorios	No	Uno de los siguientes: IndividualVC, IndividualUnmanaged, Persistent, NonPersistent, SviPersistent, SviNonPersistent, ManualVCPersistent, Manual, ManualUnmanagedPersistent, ManualUnmanagedNonPersistent, TerminalService, OnRequestVcPersistent, OnRequestVcNonPersistent, OnRequestSviPersistent, OnRequestSviNonPersistent
La carpeta de View Administrator en la que el grupo de escritorios se encuentra	Yes	Ninguna

Descripción	¿Es anónimo este campo?	Valor de ejemplo
La lista de nombres distintivos (Distinguished Names, DN) de máquinas virtuales que pertenecen al grupo de escritorios	No	Un ejemplo sobre elementos de la lista: ["CN=8f11d7cf-b0ef-43ad-92ce-691aa929d3c4,OU=Servers,DC=vdi,DC=vmware,DC=int"]
¿Se permiten varias sesiones en el grupo de escritorios?	No	True o false
¿Los usuarios de este grupo de escritorios tienen permiso para restablecer sus máquinas virtuales?	No	Desactivado, opcional u obligatorio
Tiempo tras el cual se muestra un mensaje de cierre de sesión forzado	No	True o false
El nombre distintivo de la instancia de vCenter Server que administra las máquinas virtuales en el grupo	No	"CN=e7a718de-d0f7-444a-9452-156dce289028,OU=VirtualCenter,OU=Properties,DC=vd i,DC=vmware,DC=int"
Número mínimo de máquinas virtuales en el grupo de escritorios	No	Entero
Número máximo de máquinas virtuales en el grupo de escritorios	No	Entero
Número de máquinas virtuales aprovisionadas de reserva en el grupo de escritorios	No	Entero
Directiva de eliminación para el grupo de escritorios	No	Default (predeterminado), DeleteOnUse o RefreshOnUse
Sufijo DNS utilizado para aprovisionar	Yes	Ninguna
El patrón de nombres (prefijo) para nombres de máquinas virtuales que se implementan automáticamente	Yes	Ninguna
La plantilla para clonar máquinas virtuales	Yes	Ninguna
La carpeta en vCenter Server donde se almacenan las máquinas virtuales implementadas	Yes	Ninguna
El grupo de recursos utilizado para las máquinas virtuales	Yes	Ninguna
Una lista de almacenes de datos	Yes	Ninguna
La especificación personalizada para implementar máquinas virtuales	Yes	Ninguna
Habilitar el aprovisionamiento automático para el grupo de escritorios	No	True o false
Los errores producidos durante el aprovisionamiento	No	
Detener el aprovisionamiento cuando se produce un error	No	True o false
Iniciar el aprovisionamiento	No	True o false
Se han calculado los valores del grupo	No	True o false
La máquina virtual principal utilizada para aprovisionar el clon vinculado	Yes	Ninguna
El nombre de la snapshot utilizada para aprovisionar clones vinculados	Yes	Ninguna
El ID de la snapshot utilizada para aprovisionar clones vinculados	No	"snapshot-38685"



Descripción	¿Es anónimo este campo?	Valor de ejemplo
El ID del grupo de implementación utilizado para el servicio VMware Horizon View Composer	No	"7119316f-00a8-463d-bbba-c3000f105aeb"
La ruta de almacén de datos del disco persistente de View Composer	Yes	Ninguna
Tipo de disco de View Composer	No	"SystemDisposable", UserProfile, etc.
Crear un disco persistente como disco de reserva	No	True o false
La letra de montaje de unidad para el disco persistente o el disco de datos descartables	No	"*", "C", etc.
El tamaño de destino del disco persistente	No	Entero
Tipo de directiva de actualización	No	Always (siempre), Never (nunca) o Conditional (condicional)
Umbral de uso para operaciones de actualización	No	Entero
Umbral de tiempo para operaciones de actualización	No	Entero
Nivel de sobreasignación para un almacén de datos que aloja clones vinculados	No	None (ninguno), Conservative (conservador), Moderate (moderado), Aggressive (agresivo)
Ruta del almacén de datos que aloja clones vinculados	Yes	Ninguna
Lista de ID que utiliza este almacén de datos	No	Lista de GUID, como los siguientes: ["7119316f-00a8-463d-bbba-c3000f105aeb"]
Estado de la máquina virtual	No	Ready (listo), Pre-provisioned (aprovisionado previamente), Cloning (clonando), Cloning Error (error de clonación), Customizing (personalizando), Deleting (eliminando), Maintenance (mantenimiento), Error (error) o Logout (cerrar sesión)
Asignar una máquina virtual a un usuario cuando inicie sesión por primera vez	No	True o false
Indicadores para el grupo de escritorios	No	
Opciones de configuración multimonitor	No	svga.maxWidth:int, svga.vramSize:int, svga.maxHeight:int, svga.enable3d:bool, svga.numDisplays:int
Una máquina virtual individual se convirtió en un grupo manual	No	True o false
El grupo de clones vinculados utiliza clonaciones de snapshots nativas con VAAI	No	True o false
El Acelerador de almacenamiento de View (CBRC) está habilitado	No	True o false
Frecuencia de actualización del caché CBRC	No	Entero

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Periodos sin disponibilidad de actualización del caché CBRC	No	Lista
Los tipos de disco guardados en la caché para CBRC (discos de SO, discos persistentes)	No	Lista
La recuperación de espacio de disco de la máquina virtual (formato fragmentado para optimizar el espacio) está habilitada	No	True o false
El umbral de recuperación de espacio de disco en bytes	No	
Número mínimo de máquinas virtuales listas durante una operación de reajuste	No	
El grupo de escritorios utiliza un almacén de datos Virtual SAN	No	True o false
Número de autorizaciones de escritorios remotos para este grupo de servidores	No	0 o 1
Número de autorizaciones de aplicaciones remotas para este grupo	No	0 o 1
Protocolo de visualización predeterminado	No	PCoIP, RDP o Blast
El usuario puede elegir el protocolo de visualización que desee utilizar	No	True o false
HTML Access está habilitado	No	True o false
Nivel de calidad de Flash	No	None used (sin utilizar), low (bajo), medium (medio), high (alto)
Límite de Flash	No	None used (sin utilizar), conservative (conservador), moderate (moderado), aggressive (agresivo)
El grupo está deshabilitado	No	True o false
El grupo está marcado para su eliminación	No	True o false
Etiquetas asociadas con la instancia del servidor de conexión de View	Yes	Ninguna
Utilice un servidor de Mirage diferente al especificado en la configuración global	No	True o false
El servidor de Mirage está habilitado	No	True o false
URL del servidor de Mirage, incluido el número de puerto	Yes	Ninguna
Número de clones por grupo	No	Entero

## Datos de las máquinas recopilados por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopila datos de los campos de View y de vCenter Server que describen máquinas virtuales. Los campos que contienen información personal son anónimos.

Tabla 8-13. Datos de las máquinas recopilados desde View

Descripción	¿Es anónimo este campo?	Valor de ejemplo
La máquina está marcada como modificada. La máquina virtual se usó cuando se estableció useonce=true y, por lo tanto, no debería aceptar nuevas sesiones	No	True o false
Asignación de dispositivos para cambiar los ID	No	Un conjunto de ID como el siguiente: 2000=01874583;01874583&2016=3910f513;3910f513
Un identificador de la máquina que se usa para correlacionar los datos	No	vm-10
La personalización de sysprep se usa en el sistema operativo invitado	No	True o false
Valor de tiempo de espera. El periodo de tiempo antes de que se desconecte la máquina.	No	Hora
Un ID aleatorio de View Agent o Horizon Agent de esta máquina	No	GUID
Varios valores de configuración	No	Enteros y booleanos (true o false)
Identificador LDAP de View del disco persistente de View Composer previo	No	Entrada LDAP
ThinApps autorizadas en esta máquina	Yes	Ninguna
ThinApps pendientes de desinstalarse	Yes	Ninguna
ThinApps instaladas en esta máquina	Yes	Ninguna
El estado de la máquina	No	No definido, preaprovisionado, clonación, error de clonación, personalizar, listo, eliminar, mantenimiento, error o cierre de sesión
Marca de tiempo de cuando comenzó la personalización	No	Entero
La máquina está encendida para la personalización	No	Entero. Los valores son 0 o 1.
La máquina está encendida	No	True o false
La máquina está en suspensión	No	True o false
El estado de la máquina es en transición	No	True o false
La máquina está configurada	No	True o false
La ruta de la máquina virtual en vCenter Server	Yes	Ninguna
Plantilla de personalización usada para personalizar la máquina	Yes	Ninguna
ID de clones vinculados de View Composer de la máquina	No	GUID del clon vinculado
La máquina virtual no se encuentra en vCenter Server	No	True o false
Número de veces que View intentó apagar la máquina	No	Entero
Estado de CBRC (Acelerador de almacenamiento de View)	No	Desconectado, actual, desactualizado o error
Hora de la última actualización CBRC	No	Fecha

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Hora del último error CBRC	No	Entero
Hora del último intento incompleto de configurar CBRC	No	Entero
La versión de View Agent o de Horizon Agent instalada en la máquina	No	6.0.0-551711
View Persona Management está habilitado en la máquina	No	True o false
Última cantidad, en bites, de espacio de disco de equipo recuperado (si se usa el formato fragmentado para optimizar el espacio)	No	
Hora de la última recuperación de espacio	No	Marca de tiempo

**Tabla 8-14. Datos de la máquina virtual recopilados desde vCenter Server**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
La versión del hardware de la máquina virtual	No	v8
La cantidad de RAM que está asignada a la máquina virtual	No	1024
El número de CPU virtuales que están configuradas en la máquina virtual	No	Entero
El sistema operativo instalado en la máquina virtual	No	Microsoft Windows 7 (32 bits), Microsoft Windows 8 (32 bits), Microsoft Windows Server 2008 R2 (64 bits), Microsoft Windows Server 2012 R2 (64 bits), etc.

## Datos de vCenter Server recopilados por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopila datos de algunos campos de vCenter Server. Los campos que contienen información personal son anónimos.

**Tabla 8-15. Información del sistema del host recopilada por vCenter Server**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
La hora a la que View se comunicó por última vez con este host de vCenter Server	No	Entero
La URL de la instancia de vCenter Server	Yes	Ninguno
La versión de la API de la instancia de vCenter Server	No	5.0
El número de compilación de la instancia de vCenter Server	No	456789
El número de versión de la instancia de vCenter Server	No	5.0.0

**Tabla 8-16. Información del estado del host recopilada por vCenter Server**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
El código interno del estado de la conexión entre vCenter Server y el servidor de conexión de View	No	Status_Up
Descripción del código del estado de conexión	No	Conectado
El certificado SSL de vCenter Server es válido	No	True o false
La razón por la que el certificado SSL no es válido	No	Los nombres no coinciden, no es de confianza, no se puede comprobar la revocación, etc.

**Tabla 8-17. Datos del almacén de datos recopilados desde vCenter Server**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Capacidad de disco de este almacén de datos	No	Entero
Espacio de disco libre en este espacio de disco	No	Entero
El tipo de almacenamiento	No	NFS, VMFS
Varios hosts puede acceder a este almacén de datos al mismo tiempo.	No	True o false

**Tabla 8-18. Información del nodo ESX**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Identificador del vCenter Server que administra un host ESXi concreto, junto con un identificador del host ESXi	No	1234-ADEE-BECF-41AA-4950BCDA-host-14

**Tabla 8-19. Información sobre el almacenamiento de conexión directa para un host ESXi**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Proveedor de hardware del disco físico	No	SEAGATE
Modelo del disco físico	No	ST9300653SS
SSD	No	True o false
Capacidad, en bites	No	
Identificador del host ESXi	No	host-123
Identificador del vCenter Server que administra un host ESXi particular	No	1234-ADEE-BECF-41AA-4950BCDA

## Datos de ThinApp recopilados por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopila datos de algunos campos de ThinApp. Los campos que contienen información personal son anónimos.

**Tabla 8-20. Información de ThinApp**

Descripción	¿Es anónimo este campo?	Tipo de valor
Nombre para mostrar del paquete ThinApp	No	
Número de paquetes MSI asociados con ThinApp	No	Entero
Número de asignaciones para una instalación completa	No	Entero
Lista de grupos configurados para usar la instalación completa	Yes	Lista con el hash de CN (nombre común)
Escritorios remotos configurados para usar una instalación completa	No	Lista con los CN (GUID) de los escritorios
Número de asignaciones para transmitir ThinApp	No	Entero
Lista de grupos configurados para transmitir ThinApp	Yes	Lista con el hash de CN (nombre común)
Escritorios remotos configurados para transmitir ThinApp	No	Lista con los CN (GUID) de los escritorios
ThinApps de un grupo configuradas para usar una instalación completa	No	Lista con la ID de las ThinApps

## Información de Arquitectura de Cloud Pod recopilada por VMware

Si se une al programa de mejora de la experiencia de cliente, VMware recopila datos de ciertos campos de Arquitectura de Cloud Pod. Los campos que contienen información personal son anónimos.

**Tabla 8-21. Información recopilada sobre Arquitectura de Cloud Pod**

Descripción	¿Es anónimo este campo?	Ejemplo o tipo
La función Arquitectura de Cloud Pod está habilitada	No	True o false
ID del pod local	No	
Frecuencia en segundos en la que el sistema realizará una comprobación de estado de pods	No	Entero
Máxima diferencia de tiempo permitida entre pods, en segundos	No	Entero
Nombre común del sitio al que pertenece el pod	No	
Lista de los ID de autorizaciones globales (por ejemplo, un pod tiene grupos de escritorios que admite las autorizaciones globales)	No	Lista de cadenas
Nombre común del endpoint de pods, que se corresponde con una instancia del servidor de conexión de View	Yes	
Nombre común del pod que contiene este endpoint	No	
El endpoint del pod está deshabilitado	No	True o false
Peso que se debe aplicar cuando se seleccionan endpoints de forma aleatoria (instancias del servidor de conexión de View) para las sesiones remotas	No	Entero

Descripción	¿Es anónimo este campo?	Ejemplo o tipo
La autorización global está deshabilitada	No	True o false
La búsqueda del escritorio se inicia desde el sitio de inicio del usuario (Si está establecido como false, la búsqueda se inicia en el pod local)	No	True o false
La autorización global es para un escritorio dedicado	No	0 = No 1 = Sí
Ámbito para el cual se debe realizar la búsqueda de la sesión existente	No	CUALQUIERA, SITIO o LOCAL
Ámbito para el cual se debe realizar la búsqueda de la ubicación existente	No	CUALQUIERA, SITIO o LOCAL
El sitio de inicio del usuario es obligatorio para esta autorización global	No	True o false
La limpieza automática de la sesión está habilitada	No	True o false

## Datos de Horizon Client recopilados por VMware

Si su compañía participa en el programa de mejora de la experiencia de cliente, VMware recopila datos de ciertos campos de Horizon Client. Los campos que contienen información personal son anónimos.

Aunque la información esté cifrada mientras se envía al servidor de conexión, la información en el sistema cliente se registra sin cifrar en un directorio específico. Los registros no contienen información de identificación personal.

**Tabla 8-22. Datos recopilados de las instancias de Horizon Client para el programa de mejora de la experiencia de cliente**

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Compañía que desarrolló la aplicación Horizon Client	No	VMware
Nombre de producto	No	VMware Horizon Client
Versión del producto del cliente	No	(El formato es x.x.x-yyyyyy, donde x.x.x es el número de la versión cliente e yyyyyy es el número de compilación).
Arquitectura binaria del cliente	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ i386</li> <li>■ x86_64</li> <li>■ arm</li> </ul>

Descripción	¿Es anónimo este campo?	Valor de ejemplo
Nombre de compilación del cliente	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ VMware-Horizon-Client-Win32-Windows</li> <li>■ VMware-Horizon-Client-Linux</li> <li>■ VMware-Horizon-Client-iOS</li> <li>■ VMware-Horizon-Client-Mac</li> <li>■ VMware-Horizon-Client-Android</li> <li>■ VMware-Horizon-Client-WinStore</li> </ul>
Sistema operativo del host	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ Windows 8.1</li> <li>■ Windows 7, 64 bits Service Pack 1 (Compilación 7601)</li> <li>■ iPhone OS 5.1.1 (9B206)</li> <li>■ Ubuntu 12.04.4 LTS</li> <li>■ Mac OS X 10.8.5 (12F45)</li> </ul>
Kernel del sistema operativo del host	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ Windows 6.1.7601 SP1</li> <li>■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X</li> <li>■ Darwin 11.4.2</li> <li>■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012</li> <li>■ desconocido (para la Tienda Windows)</li> </ul>
Arquitectura del sistema operativo del host	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ x86_64</li> <li>■ i386</li> <li>■ armv71</li> <li>■ ARM</li> </ul>
Modelo de sistema del host	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ Dell Inc. OptiPlex 960</li> <li>■ iPad3,3</li> <li>■ MacBookPro8,2</li> <li>■ Estación de trabajo Dell Inc. Precision T3400 (A04 03/21/2008)</li> </ul>
CPU de sistema del host	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH</li> <li>■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH</li> <li>■ desconocido (para iPad)</li> </ul>
Número de núcleos en el procesador del sistema del host	No	Por ejemplo: 4
MB de memoria en el sistema del host	No	<p>Ejemplos que incluyen los siguientes valores:</p> <ul style="list-style-type: none"> <li>■ 4096</li> <li>■ desconocido (para la Tienda Windows)</li> </ul>
Número de dispositivos USB conectados	No	2 (el redireccionamiento de dispositivos USB es compatible solo con los clientes Linux, Windows y Mac).



Descripción	¿Es anónimo este campo?	Valor de ejemplo
Número máximo de conexiones simultáneas de dispositivos USB	No	2
ID del proveedor del dispositivo USB	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ Kingston</li> <li>■ NEC</li> <li>■ Nokia</li> <li>■ Wacom</li> </ul>
ID del producto del dispositivo USB	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ Data Traveler</li> <li>■ Controlador para juegos</li> <li>■ Unidad de almacenamiento</li> <li>■ Mouse inalámbrico</li> </ul>
Familia de dispositivos USB	No	Ejemplos que incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ Seguridad</li> <li>■ Dispositivo de interfaz de usuario</li> <li>■ Imágenes</li> </ul>
Recuento del uso del dispositivo USB	No	(Número de veces que se compartió el dispositivo)

## Datos recopilados por VMware

Si su compañía participa en el programa de mejora de la experiencia de cliente, VMware recopila datos de ciertos campos de los clientes. Los campos que contienen información personal son anónimos.

**Tabla 8-23. Datos de los clientes recopilados para el programa de mejora de la experiencia de cliente**

Descripción	Nombre del campo	¿Es anónimo este campo?	Valor de ejemplo
Compañía que desarrolló la aplicación	<client-vendor>	No	VMware
Nombre de producto	<client-product>	No	
Versión del producto del cliente	<client-version>	No	4.4.0-número_compilación
Arquitectura binaria del cliente	<client-arch>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ navegador</li> <li>■ arm</li> </ul>
Arquitectura nativa del navegador	<browser-arch>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ Win32</li> <li>■ Win64</li> <li>■ MacIntel</li> <li>■ iPad</li> </ul>

Descripción	Nombre del campo	¿Es anónimo este campo?	Valor de ejemplo
Cadena agente del usuario del navegador	<browser-user-agent>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ Mozilla/5.0 (Windows NT 6.1; WOW64)</li> <li>■ AppleWebKit/703.00 (KHTML, like Gecko)</li> <li>■ Chrome/3.0.1750</li> <li>■ Safari/703.00</li> <li>■ Edge/13.10586</li> </ul>
Cadena de la versión interna del navegador	<browser-version>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ 7.0.3 (para Safari),</li> <li>■ 44.0 (para Firefox)</li> <li>■ 13.10586 (para Edge)</li> </ul>
Implementación del núcleo del navegador	<browser-core>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> <li>■ Chrome</li> <li>■ Safari</li> <li>■ Firefox</li> <li>■ Internet Explorer</li> <li>■ Edge</li> </ul>
Si los navegadores se ejecutan en un dispositivo portátil	<browser-is-handheld>	No	true

# Administrar máquinas virtuales de escritorios de clones vinculados de View Composer

## 9

Puede actualizar las máquinas de escritorios de clones vinculados de View Composer, reducir el tamaño de los datos del sistema operativo y volver a equilibrar los equipos que se encuentran entre los almacén de datos. También puede administrar los discos persistentes asociados con clones vinculados.

Este capítulo incluye los siguientes temas:

- [Reducir el tamaño de clones vinculados con una actualización de máquinas](#)
- [Actualizar los escritorios de clones vinculados](#)
- [Volver a equilibrar máquinas virtuales de clones vinculados](#)
- [Administrar los discos persistentes de View Composer](#)

## Reducir el tamaño de clones vinculados con una actualización de máquinas

Al actualizar una máquina, el disco del sistema operativo de cada clon vinculado se restaura a su estado y tamaño original, por lo que se reducen los costes de almacenamiento.

Si es posible, programe las operaciones de actualización fuera de horas pico.

Para obtener más instrucciones, consulte [Operaciones de actualización de la máquina](#).

### Requisitos previos

- Decida cuándo programar una operación de actualización. De forma predeterminada, View Composer inicia la operación inmediatamente.

Puede programar una única operación de actualización en un momento dado para un conjunto determinado de clones vinculados. Puede programar varias operaciones de actualización si afectan a diferentes clones vinculados.

- Decida si desea forzar que todos los usuarios cierren sesión cuando comience la operación o esperar a que cada uno lo haga antes de actualizar el escritorio de clones vinculados de dicho usuario.

Si obliga a los usuarios a cerrar sesión, View se lo notifica a los usuarios antes de que se desconecten y les permite cerrar las aplicaciones y cerrar sesión.

Si obliga a los usuarios a cerrar sesión, el número máximo de operaciones de actualización simultáneas en escritorios remotos que requieran de un cierre de sesión supondrá la mitad del valor de la opción de configuración **Operaciones de mantenimiento simultáneas máximas de View Composer**. Por ejemplo, si esta opción se configura como 24 y obliga a los usuarios a cerrar sesión, el número máximo de operaciones de actualización simultáneas en escritorios remotos que requieran un cierre de sesión será 12.

- Si la implementación incluye instancias del servidor de conexión de View, compruebe que todas las instancias tengan instaladas la misma versión.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Seleccione el grupo de escritorios que desea actualizar haciendo doble clic en el ID de grupo en la columna izquierda.
- 3 Seleccione si desea actualizar varias máquinas virtuales o solo una máquina virtual.

Opción	Acción
<b>Actualizar todas las máquinas virtuales en el grupo de escritorios</b>	<ol style="list-style-type: none"> <li>a En View Administrator, seleccione <b>Catálogo &gt; Grupos de escritorios</b>.</li> <li>b Seleccione el grupo de escritorios que desea actualizar haciendo doble clic en el ID de grupo en la columna izquierda.</li> <li>c En la pestaña <b>Inventario</b>, haga clic en <b>Máquinas</b>.</li> <li>d Pulse la tecla Ctrl o Mayús para seleccionar todos los ID de máquinas en la columna izquierda.</li> <li>e Seleccione <b>Actualizar</b> del menú desplegable <b>View Composer</b>.</li> </ol>
<b>Actualizar solo una máquina virtual</b>	<ol style="list-style-type: none"> <li>a En View Administrator, seleccione <b>Recursos &gt; Máquinas</b>.</li> <li>b Seleccione la máquina que desea actualizar haciendo doble clic en su ID en la columna izquierda.</li> <li>c En la pestaña <b>Resumen</b>, seleccione <b>Actualizar</b> del menú desplegable <b>View Composer</b>.</li> </ol>

- 4 Siga las instrucciones del asistente.

Los discos de SO se reducen a su tamaño original.

En vCenter Server, puede supervisar el progreso de la actualización en las máquinas virtuales de clones vinculados.

En View Administrator, seleccione **Catálogo > Grupos de escritorios**, haga doble clic en el ID de grupo y luego en la pestaña **Tareas** para supervisar la operación. Para finalizar, suspender o reanudar una tarea, haga clic en **Cancelar tarea**, **Poner tarea en pausa** o **Reanudar tarea**.

## Operaciones de actualización de la máquina

El disco del SO del clon crece a medida que el usuario interactúa con los clones vinculados. Al actualizar una máquina, los discos del SO se restauran a su estado y tamaño original, por lo que se reducen los costos de almacenamiento.

Una operación de actualización no afecta a los discos persistentes de View Composer.

Un clon vinculado usa menos espacio de almacenamiento que la máquina virtual principal, que contiene todos los datos del SO. Sin embargo, el disco de SO de un clon se expande cada vez que los datos se escriben desde el sistema operativo invitado.

Cuando View Composer crea un clon vinculado, realiza una snapshot del disco de SO del clon. La snapshot solo identifica la máquina virtual de clones vinculados. Una operación de actualización revierte el disco de SO a la snapshot.

View Composer puede actualizar un clon vinculado en el tiempo que tarda en eliminar y volver a crear el clon.

Aplice estas directivas a las operaciones de actualización:

- Puede actualizar un grupo de escritorios a demanda, como un evento programado o cuando los datos del SO alcanzan un tamaño específico.

Puede programar una única operación de actualización en un momento dado para un conjunto determinado de clones vinculados. Si inicia una operación de actualización de forma inmediata, la operación sobrescribe cualquier tarea programada previamente.

Puede programar varias operaciones de actualización si afectan a diferentes clones vinculados.

Antes de programar una nueva operación de actualización, debe cancelar cualquier tarea programada previamente.

- Puede actualizar grupos de asignación dedicada o flotante.
- La actualización solo se puede realizar si los usuarios se desconectaron de sus escritorios de clones vinculados.
- Una actualización conserva la información única del equipo configurada por QuickPrep o Sysprep. No es necesario que vuelva a ejecutar Sysprep después de una actualización para restaurar el SID o los GUID del software de terceros instalados en la unidad del sistema.
- Después de volver a componer un clon vinculado, Horizon 7 realiza una nueva snapshot del disco del SO de los clones vinculados. Las futuras operaciones de actualización restaurarán los datos del SO a esa snapshot, no a la que se realizó originalmente cuando el clon vinculado se creó por primera vez.

Si usa la tecnología de snapshot NFS nativa (VAAI) para generar clones vinculados, algunos dispositivos NAS de los proveedores realizan snapshots del disco de réplica cuando actualizan los discos del SO de los clones vinculados. Estos dispositivos NAS no admiten la realización de snapshots directas del disco del SO de cada clon.

- Puede establecer un mínimo de escritorios aprovisionados y preparados que estén disponibles para que los usuarios se conecten durante la operación de actualización. Consulte "Mantener los escritorios de clones vinculados aprovisionados y preparados durante las operaciones de View Composer" en el documento *Configurar escritorios virtuales en Horizon 7*.

**Nota** Puede ralentizar el crecimiento de clones vinculados redireccionando los archivos de paginación y los archivos temporales del sistema a un disco temporal. Cuando un clon vinculado está apagado, Horizon 7 reemplaza el disco temporal por una copia del disco temporal original que creó View Composer con el grupo de clones vinculados. Esta operación reduce el disco temporal a su tamaño original.

Puede configurar esta opción cuando cree un grupo de escritorios de clones vinculados.

## Actualizar los escritorios de clones vinculados

Para actualizar las máquinas virtuales de clones vinculados, cree una nueva imagen de base en la máquina virtual principal y utilice la función de recomposición para distribuir la imagen actualizada a los clones vinculados.

- **Preparar una máquina virtual principal para recomponer clones vinculados**  
Antes de recomponer un grupo de escritorios de clones vinculados, debe actualizar la máquina virtual principal que se utilizó como imagen base para los clones vinculados.
- **Recomponer máquinas virtuales de clones vinculados**  
La recomposición de las máquinas actualiza de forma simultánea todas las máquinas virtuales de clones vinculados ancladas a una máquina virtual principal.
- **Actualizar clones vinculados mediante una recomposición**  
Durante una recomposición, puede aplicar revisiones al sistema operativo, instalar o actualizar aplicaciones o modificar la configuración de hardware de la máquina virtual en todos los clones vinculados del grupo de escritorios.
- **Corregir una recomposición que no se realizó correctamente**  
Puede corregir una recomposición que no se realizó correctamente. También puede realizar esta acción si recompuso accidentalmente clones vinculados usando una imagen base diferente a la que pretendía usar.

## Preparar una máquina virtual principal para recomponer clones vinculados

Antes de recomponer un grupo de escritorios de clones vinculados, debe actualizar la máquina virtual principal que se utilizó como imagen base para los clones vinculados.

View Composer no permite volver a componer clones vinculados que utilicen un sistema operativo diferente al que use la máquina virtual principal. Por ejemplo, no puede utilizar una snapshot de una máquina virtual principal con Windows 8 para volver a componer un clon vinculado con Windows 7.

## Procedimiento

- 1 En vCenter Server, actualice la máquina virtual principal para volver a componer.
  - Instale revisiones de SO o service pack, nuevas aplicaciones, actualizaciones de aplicaciones o realice otros cambios en la máquina virtual principal.
  - También puede preparar otra máquina virtual para que sea seleccionada como una principal nueva durante la recomposición.
- 2 En vCenter Server, apague la máquina virtual principal nueva o actualizada.
- 3 En vCenter Server, tome una snapshot de la máquina virtual principal.

## Pasos siguientes

Vuelva a componer el grupo de escritorios de clones vinculados.

## Recomponer máquinas virtuales de clones vinculados

La recomposición de las máquinas actualiza de forma simultánea todas las máquinas virtuales de clones vinculados ancladas a una máquina virtual principal.

Si es posible, programe las recomposiciones fuera de horas punta.

## Requisitos previos

- Compruebe que tenga una snapshot de la máquina virtual principal. Consulte [Preparar una máquina virtual principal para recomponer clones vinculados](#).
- Familiarícese con las directrices de recomposición. Consulte [Actualizar clones vinculados mediante una recomposición](#).
- Decida cuándo programar la recomposición. De forma predeterminada, View Composer inicia la recomposición inmediatamente.

Puede programar una única recomposición en un momento dado para un conjunto determinado de clones vinculados. Puede programar varias recomposiciones si afectan a diferentes clones vinculados.

- Decida si desea cerrar las sesiones de usuario de forma forzada cuando comience la recomposición o esperar a que cada uno lo haga antes de recomponer el escritorio de clones vinculados de dicho usuario.

Si obliga a los usuarios a cerrar sesión, Horizon 7 se lo notifica a los usuarios antes de que se desconecten y les permite cerrar las aplicaciones y cerrar sesión.

- Decida si desea detener el aprovisionamiento cuando se produce el primer error. Si selecciona esta opción y se produce un error cuando View Composer aprovisiona un clon vinculado, se detiene el aprovisionamiento en todos los clones del grupo de escritorios. Puede seleccionar esta opción para asegurarse de que recursos como el almacenamiento no se consuman de forma innecesaria.

Si selecciona la opción **Detener en el primer error**, esto no afecta a la personalización. Si se produce un error de personalización en un clon vinculado, se siguen aprovisionando y personalizando otros clones.

- Compruebe que el aprovisionamiento del grupo de escritorios esté habilitado. Cuando el aprovisionamiento del grupo de escritorios esté deshabilitado, Horizon 7 detiene la personalización de los escritorios después de que se recompongan.
- Si la implementación incluye instancias replicadas del servidor de conexión de Horizon, compruebe que todas las instancias tengan instaladas la misma versión.

## Procedimiento

- 1 Seleccione si desea recomponer todo el grupo de escritorios o solo un equipo.

Opción	Acción
<b>Recomponer todas las máquinas virtuales en el grupo de escritorios</b>	<ol style="list-style-type: none"> <li>a En Horizon Administrator, seleccione <b>Catálogo &gt; Grupos de escritorios</b>.</li> <li>b Seleccione el grupo de escritorios que desea recomponer haciendo doble clic en el ID de grupo en la columna izquierda.</li> <li>c En la pestaña <b>Inventario</b>, haga clic en <b>Máquinas</b>.</li> <li>d Pulse las teclas Ctrl o Mayús para seleccionar todos los ID de máquinas en la columna izquierda.</li> <li>e Seleccione <b>Recomponer</b> del menú desplegable <b>View Composer</b>.</li> </ol>
<b>Recomponer las máquinas virtuales seleccionadas</b>	<ol style="list-style-type: none"> <li>a En Horizon Administrator, seleccione <b>Recursos &gt; Máquinas</b>.</li> <li>b Seleccione la máquina que desea recomponer haciendo doble clic en su ID en la columna izquierda.</li> <li>c En la pestaña <b>Resumen</b>, seleccione <b>Recomponer</b> del menú desplegable <b>View Composer</b>.</li> </ol>

- 2 Siga las instrucciones del asistente.

Puede seleccionar una nueva máquina virtual para usarla como la máquina virtual principal del grupo de escritorios.

En la página Listo para finalizar, puede hacer clic en **Mostrar detalles** para visualizar los escritorios de clones vinculados que se recompondrán.

Las máquinas virtuales de clones vinculados se actualizan. Los discos de SO se reducen a su tamaño original.

En un grupo de asignaciones dedicadas, los clones vinculados sin asignar se eliminan y se vuelven a crear. Se mantiene el número especificado de máquinas virtuales de reserva.

En un grupo de asignaciones flotantes, se recomponen todos los clones vinculados seleccionados.

En vCenter Server, puede supervisar de la recomposición de las máquinas virtuales de clones vinculados.



En Horizon Administrator, puede supervisar la operación haciendo clic en **Catálogo > Grupos de escritorios**; a continuación en el ID de grupo y luego en la pestaña **Tareas**. Para finalizar, suspender o reanudar una tarea, haga clic en **Cancelar tarea**, **Poner tarea en pausa** o **Reanudar tarea**.

**Nota** Si utilizó una especificación de personalización Sysprep para personalizar los clones vinculados al crear el grupo de escritorios, se generarán nuevos SID para las máquinas virtuales que se volvieron a componer. Para obtener más información, consulte "Recomponer clones vinculados personalizados con Sysprep" en el documento *Configurar escritorios virtuales en Horizon 7*.

## Actualizar clones vinculados mediante una recomposición

Durante una recomposición, puede aplicar revisiones al sistema operativo, instalar o actualizar aplicaciones o modificar la configuración de hardware de la máquina virtual en todos los clones vinculados del grupo de escritorios.

Para volver a componer las máquinas virtuales de clonación vinculada, actualice la máquina virtual principal en vCenter Server o seleccione otra diferente para que sea la principal. A continuación, tome una snapshot de la configuración de la nueva máquina virtual principal.

Puede modificar la máquina virtual principal sin que afecte a los clones vinculados, ya que están vinculados a la réplica y no directamente a la máquina principal.

Seleccione la snapshot que será la nueva imagen de base del grupo de escritorios para iniciar la recomposición. View Composer crea una nueva réplica, copia el disco de SO reconfigurado a los clones vinculados y ancla los clones vinculados a la nueva réplica.

Al volver a componer, también se actualizan los clones vinculados, por lo que se reduce el tamaño de los discos del sistema operativo.

Volver a componer el escritorio no afecta a los discos persistentes de View Composer.

Aplique estas directrices al volver a componer:

- Puede volver a componer grupos de escritorios de asignación dedicada o flotante.
- Puede volver a componer grupos de escritorios a petición o programar un evento para ello.

Puede programar una única recomposición en un momento dado para un conjunto determinado de clonación vinculada. Antes de programar una nueva recomposición, debe cancelar cualquier tarea programada con anterioridad o esperar hasta que la operación anterior finalice. Antes de empezar una nueva recomposición inmediatamente, debe cancelar cualquier tarea programada con anterioridad.

Puede programar varias recomposiciones si afectan a diferentes clonaciones vinculadas.

- Puede volver a componer algunos o todos los clones vinculados de un grupo de escritorios.
- Si los clones vinculados de un grupo de escritorios derivan de diferentes snapshots de una o varias imágenes base, el grupo de escritorios incluirá más de una réplica.
- La recomposición solo se puede realizar si los usuarios cerraron la sesión en sus escritorios de clones vinculados.

- No puede volver a componer clones vinculados que utilicen un sistema operativo diferente al de la máquina virtual principal nueva o actualizada.
- No puede volver a componer clones vinculados en una versión de hardware anterior a la actual. Por ejemplo, no puede volver a componer clones con una versión de hardware 8 a una máquina virtual principal cuya versión de hardware sea 7.
- Puede establecer un mínimo de escritorios aprovisionados y listos que estén disponibles para que los usuarios se conecten durante la operación de recomposición. Consulte "Mantener los escritorios de clonación vinculada aprovisionados y preparados durante las operaciones de View Composer" en el documento *Configurar escritorios virtuales en Horizon 7*.

---

**Nota** Si utilizó una especificación de personalización Sysprep para personalizar los clones vinculados al crear el grupo de escritorios, se generarán nuevos SID para las máquinas virtuales que se volvieron a componer. Para obtener más información, consulte "Recomponer clonaciones vinculadas personalizadas con Sysprep" en el documento *Configurar escritorios virtuales en Horizon 7*.

---

## Corregir una recomposición que no se realizó correctamente

Puede corregir una recomposición que no se realizó correctamente. También puede realizar esta acción si recompuso accidentalmente clones vinculados usando una imagen base diferente a la que pretendía usar.

### Problema

Las máquinas virtuales se encuentran en un estado desactualizado o de error como resultado de una recomposición que no se realizó correctamente.

### Causa

Se pudo producir un error en el sistema o un problema en el host de vCenter Server, en vCenter Server o en un almacén de datos durante la recomposición.

De forma alternativa, la recomposición pudo usar una snapshot con un sistema operativo diferente al de la máquina virtual principal original. Por ejemplo, pudo usar una snapshot de Windows 8 para recomponer los clones vinculados de Windows 7.

### Solución

- 1 Seleccione la snapshot que se usó la última vez que se realizó una recomposición correctamente.

También puede seleccionar una nueva snapshot para actualizar los clones vinculados a un nuevo estado.

La snapshot debe usar el mismo sistema operativo que la snapshot de la máquina virtual principal original.

- 2 Vuelva a componer el grupo de escritorios.

View Composer crea una imagen base para la snapshot y vuelve a crear los discos de SO de los clones vinculados.

Los discos persistentes de View Composer que contienen opciones y datos de usuarios se conservan durante la recomposición.

Según las condiciones de la recomposición que no se realizó correctamente, podría actualizar o volver a equilibrar los clones vinculados en lugar o además de recomponerlos.

---

**Nota** Si no configura los discos persistentes de View Composer, todas las recomposiciones eliminan los cambios generados por el usuario en las máquinas virtuales de clones vinculados.

---

## Volver a equilibrar máquinas virtuales de clones vinculados

La operación para volver a equilibrar distribuye uniformemente las máquinas virtuales de clones vinculados entre los almacenes de datos disponibles.

También puede usar la operación para volver a equilibrar si desea migrar las máquinas virtuales de clones vinculados a otro almacén de datos. No utilice vSphere Client ni vCenter Server para migrar o administrar máquinas virtuales de clones vinculados. Consulte [Migrar las máquinas virtuales de clones vinculados a otro almacén de datos](#).

Si es posible, programe las operaciones para volver a equilibrar fuera de horas punta.

Para obtener más instrucciones, consulte [Volver a equilibrar clones vinculados entre unidades lógicas](#).

### Requisitos previos

- Familiarícese con la operación para volver a equilibrar. Consulte [Volver a equilibrar clones vinculados entre unidades lógicas](#).
- Decida cuándo programar una operación para volver a equilibrar. De forma predeterminada, View Composer inicia la operación inmediatamente.

Puede programar una única operación para volver a equilibrar en un momento dado para un conjunto determinado de clones vinculados. Puede programar varias operaciones para volver a equilibrar si afectan a diferentes clones vinculados.

- Decida si desea cerrar las sesiones de usuario de forma forzada cuando comience la operación o esperar a que cada usuario lo haga antes de volver a equilibrar el escritorio de clones vinculados de dicho usuario.

Si obliga a los usuarios a cerrar sesión, View se lo notifica a los usuarios antes de que se desconecten y les permite cerrar las aplicaciones y cerrar sesión.

Si obliga a los usuarios a cerrar sesión, el número máximo de operaciones simultáneas para volver a equilibrar en escritorios remotos que requieran un cierre de sesión supondrá la mitad del valor de la opción **Operaciones de mantenimiento simultáneas máximas de View Composer**. Por ejemplo, si esta opción se configura como 24 y obliga a los usuarios a cerrar sesión, el número máximo de operaciones simultáneas para volver a equilibrar en escritorios remotos que requieran un cierre de sesión será 12.

- Compruebe que el aprovisionamiento del grupo de escritorios esté habilitado. Cuando el aprovisionamiento de grupo esté deshabilitado, View detiene la personalización de las máquinas virtuales después de que se vuelvan a equilibrar.
- Si la implementación incluye instancias del servidor de conexión de View, compruebe que todas las instancias tengan instaladas la misma versión.

## Procedimiento

- 1 Seleccione si desea volver a equilibrar todo el grupo o solo una máquina virtual.

Opción	Acción
<b>Volver a equilibrar todas las máquinas virtuales en el grupo de escritorios</b>	<ol style="list-style-type: none"> <li>a En View Administrator, seleccione <b>Catálogo &gt; Grupos de escritorios</b>.</li> <li>b Para seleccionar el grupo que desea volver a equilibrar, haga doble clic en el ID de grupo en la columna izquierda.</li> <li>c En la pestaña <b>Inventario</b>, haga clic en <b>Máquinas</b>.</li> <li>d Pulse las teclas Ctrl o Mayús para seleccionar varios o todos los ID de máquinas en la columna izquierda.</li> <li>e Seleccione <b>Reequilibrar</b> en el menú desplegable <b>View Composer</b>.</li> </ol>
<b>Volver a equilibrar solo una máquina virtual</b>	<ol style="list-style-type: none"> <li>a En View Administrator, seleccione <b>Recursos &gt; Máquinas</b>.</li> <li>b Para seleccionar la máquina que desea volver a equilibrar, haga doble clic en su ID en la columna izquierda.</li> <li>c En la pestaña <b>Resumen</b>, seleccione <b>Reequilibrar</b> en el menú desplegable <b>View Composer</b>.</li> </ol>

- 2 Siga las instrucciones del asistente.

Las máquinas virtuales de clones vinculados se actualizan y se vuelven a equilibrar. Los discos de SO se reducen a su tamaño original.

En View Administrator, seleccione **Catálogo > Grupos de escritorios**, haga doble clic en el ID de grupo y luego en la pestaña **Tareas** para supervisar la operación. Para finalizar, suspender o reanudar una tarea, haga clic en **Cancelar tarea**, **Poner tarea en pausa** o **Reanudar tarea**.

## Volver a equilibrar clones vinculados entre unidades lógicas

La operación para volver a equilibrar vuelve a distribuir uniformemente las máquinas virtuales de clonación vinculada entre las unidades lógicas disponibles. Ahorra espacio de almacenamiento en unidades sobrecargadas y asegura que ninguna unidad se infrutilice.

Al crear grandes grupos de escritorios de clones vinculados y utilizar varios números de unidad lógica (logical unit numbers, LUN), es posible que el espacio no se use de forma eficiente si el tamaño inicial no fuera el correcto. Si establece una sobreasignación agresiva de almacenamiento, los clones vinculados pueden crecer rápidamente y consumir el espacio libre en el almacén de datos.

Cuando las máquinas virtuales utilizan el 95 % del espacio en el almacén de datos, Horizon 7 genera una entrada de registro de advertencia.

Al volver a equilibrar, también se actualizan los clones vinculados y se reduce el tamaño de los discos de SO. No afecta a los discos persistentes de View Composer.

Aplique estas directrices para volver a equilibrar:

- Puede volver a equilibrar grupos de escritorios de asignación dedicada o flotante.
- Puede volver a equilibrar todos o algunos clones vinculados de un grupo.
- Puede volver a equilibrar un grupo de escritorios a petición o programar un evento para ello.

Puede programar una única operación para volver a equilibrar en un momento dado para un conjunto determinado de clonación vinculada. Si inicia una operación para volver a equilibrar de forma inmediata, la operación sobrescribe cualquier tarea programada previamente.

Puede programar varias operaciones para volver a equilibrar si afectan a diferentes clonaciones vinculadas.

Antes de programar una nueva operación para volver a equilibrar, debe cancelar cualquier tarea programada previamente.

- Solo se pueden volver a equilibrar las máquinas virtuales que aparecen con los estados Disponible, Error o Personalizando, sin ninguna cancelación pendiente o programada.
- Como práctica recomendada, no mezcle máquinas virtuales de clonación vinculada con otro tipo de máquinas virtuales en el mismo almacén de datos. De esta manera, View Composer puede volver a equilibrar todas las máquinas virtuales en el almacén de datos.
- Si edita un grupo y cambia el host o clúster y los almacenes de datos donde se almacenan los clones vinculados, solo podrá volver a equilibrar los clones vinculados si el host o clúster recién seleccionado tiene acceso completo tanto al almacén de datos original como al nuevo. Todos los hosts en el clúster nuevo deben tener acceso al almacén de datos nuevo y al original.

Por ejemplo, puede crear un grupo de escritorios de clones vinculados en un host independiente y seleccionar un almacén de datos local para almacenar los clones. Si edita el grupo de escritorios y selecciona un clúster y un almacén de datos compartido, la operación para volver a equilibrar fallará, ya que los hosts en el clúster no podrán acceder al almacén de datos local original.

- Puede establecer un mínimo de máquinas virtuales aprovisionadas y listas que estén disponibles para que los usuarios se conecten a ellas durante la operación para volver a equilibrar. Consulte "Mantener los escritorios de clonación vinculada aprovisionados y preparados durante las operaciones de View Composer" en el documento *Configurar escritorios virtuales en Horizon 7*.

---

**Importante** Si utiliza un almacén de datos Virtual SAN, puede realizar la operación para volver a equilibrar solo para migrar todas las máquinas virtuales en un grupo de escritorios desde dicho almacén a otro tipo de almacén de datos, o viceversa. Si un grupo de escritorios utiliza un almacén de datos Virtual SAN, Virtual SAN ofrece la función de equilibrio de carga y optimiza el uso de los recursos en todo el clúster ESXi.

---

## Migrar las máquinas virtuales de clones vinculados a otro almacén de datos

Para migrar las máquinas virtuales de clones vinculados de un conjunto de almacenes de datos a otro, use la operación para volver a equilibrar.

Cuando use el reequilibrio, View Composer administra el movimiento de los clones vinculados entre almacenes de datos. View Composer asegura que el acceso de los clones vinculados a la réplica se mantenga durante y después de la operación para volver a equilibrar. Si es necesario, View Composer crea una instancia de la réplica en el almacén de datos de destino.

---

**Nota** No utilice vSphere Client ni vCenter Server para migrar o administrar máquinas virtuales de clones vinculados. No use Storage vMotion para migrar las máquinas virtuales de clones vinculados a otros almacenes de datos.

---

### Requisitos previos

Familiarícese con la operación para volver a equilibrar. Consulte [Volver a equilibrar máquinas virtuales de clones vinculados](#) y [Volver a equilibrar clones vinculados entre unidades lógicas](#).

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorio**, seleccione el grupo de escritorio que desee migrar y haga clic en **Editar**.
- 2 En la pestaña **Configuración de vCenter**, diríjase a **Almacenes de datos** y haga clic en **Examinar**.
- 3 En la página Seleccionar almacenes de datos del clon vinculado, desmarque los almacenes de datos que almacenan en ese momento los clones vinculados, seleccione los almacenes de datos de destino y haga clic en **Aceptar**.
- 4 En la ventana **Editar**, haga clic en **Aceptar**.
- 5 En la página Grupos de escritorios, seleccione el grupo haciendo doble clic en el ID de grupo en la columna izquierda.
- 6 Seleccione **Reequilibrar** en el menú desplegable **View Composer** y siga las instrucciones del asistente para volver a equilibrar las máquinas virtuales de clones vinculados.

Las máquinas virtuales de clones vinculados se actualizan y se migran a los almacenes de datos de destino.

## Nombres de archivos de discos de clones vinculados después de una operación para volver a equilibrar

Cuando vuelva a equilibrar máquinas virtuales de clones vinculados, vCenter Server cambia los nombres de los archivos de los discos persistentes de View Composer y los discos de datos disponibles en clones vinculados que se envían a un nuevo almacén de datos.

Los nombres de archivo originales identifican el tipo de disco. Los discos renombrados no incluyen las etiquetas de identificación.

Un disco persistente original tiene un nombre de archivo con una etiqueta user-disk:

*nombre\_escritorio-vdm-user-disk-D-ID.vmdk.*

Un disco de datos disponibles original tiene un nombre de archivo con una etiqueta disponible:

*nombre\_escritorio-vdm-disponible-ID.vmdk.*

Después de que una operación para volver a equilibrar envíe un clon vinculado a un nuevo almacén de datos, vCenter Server usa una sintaxis de nombre de archivo común para ambos tipos de disco:  
*nombre\_escritorio\_n.vmdk.*

## Administrar los discos persistentes de View Composer

Puede desconectar un disco persistente de View Composer de una máquina virtual de clones vinculados y conectarlo a otro clon vinculado. Esta función le permite administrar la información del usuario de forma independiente de las máquinas virtuales de clones vinculados.

### Discos persistentes de View Composer

Con View Composer, puede configurar los datos del SO y la información del usuario en discos separados de las máquinas virtuales de clones vinculados. View Composer conserva la información del usuario en el disco persistente cuando los datos del SO se actualiza o se vuelve a equilibrar.

Un disco persistente de View Composer contiene la configuración del usuario y otros datos generados por el usuario. Puede crear discos persistentes cuando cree un grupo de escritorios de clones vinculados. Consulte la sección sobre cómo utilizar la hoja de cálculo para crear un grupo de escritorios de clones vinculados en el documento *Configurar escritorios virtuales en Horizon 7*.

Puede desconectar un disco persistente de su máquina virtual de clones vinculados y almacenar el disco en su almacén de datos original u otro diferente. Después de desconectar el disco, se elimina la máquina virtual de clones vinculados. Un disco persistente desconectado ya no está asociado a ninguna máquina virtual.

Puede usar varios métodos para conectar un disco persistente desconectado a otra máquina virtual de clones vinculados. Esta flexibilidad tiene varios usos:

- Cuando un clon vinculado se elimina, puede conservar los datos del usuario.
- Cuando un empleado deja la compañía, otro empleado puede acceder a los datos de usuario de este empleado.
- Un usuario que tenga varios escritorios remotos puede unir los datos del usuario en un único escritorio remoto.
- Si no se puede acceder a una máquina virtual en vCenter Server, pero el disco persistente está intacto, puede importar el disco persistente y crear un clon vinculado nuevo utilizando el disco.

---

**Nota** Los discos persistentes se pueden volver a conectar al sistema operativo que se usó cuando se creó. Por ejemplo, no puede desconectar un disco persistente de un clon vinculado de Windows 7 y volver a crear o conectar el disco persistente a un clon vinculado de Windows 8.

Horizon 7 puede administrar los discos persistentes desde los grupos de clones vinculados que se crearon en View 4.5 o posterior. Los discos persistentes que se crearon en versiones anteriores de Horizon 7 no se pueden administrar y no aparecen en la página Discos persistentes de Horizon Administrator.

---

## Desconectar un disco persistente de View Composer

Cuando desconecta un disco persistente de View Composer de una máquina virtual de clones vinculados, el disco se almacena y el clon vinculado se elimina. Si desconecta un disco persistente, puede almacenar y volver a usar la información específica de un usuario en otra máquina virtual.

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Discos persistentes**.
- 2 Seleccione el disco persistente que desee desconectar y haga clic en **Desconectar**.
- 3 Seleccione dónde almacenar el disco persistente.

Opción	Descripción
Utilizar almacén de datos actual	Almacene el disco persistente en el almacén de datos en el que está ubicado en ese momento.
Usar el siguiente almacén de datos	<p>Seleccione un nuevo almacén de datos en el que almacenar el disco persistente. Haga clic en <b>Examinar</b>, haga clic en la flecha desplegable y seleccione un nuevo almacén de datos en el menú <b>Elegir un almacén de datos</b>.</p> <p>No puede seleccionar ningún almacén de datos local para almacenar un disco persistente desconectado. Debe usar un almacén de datos compartido o un almacén de datos Virtual SAN.</p> <p>Si el disco persistente se almacenó originalmente en un almacén de datos Virtual SAN, puede seleccionar un almacén de datos Virtual SAN o que no sea Virtual SAN para almacenar el disco persistente desconectado. De forma similar, si el disco persistente se almacenó en un almacén que no es Virtual SAN, puede desconectar el disco de un almacén de datos Virtual SAN o que no sea Virtual SAN.</p>

El disco persistente de View Composer se guarda en el almacén de datos. La máquina virtual de clones vinculados se elimina y no aparece en View Administrator.

## Conectar un disco persistente de View Composer a otro clon vinculado

Puede conectar un disco persistente que no esté conectado a otra máquina virtual de clones vinculados. Si conecta un disco persistente, esto supone que la configuración del usuario y la información del disco estará disponible para el usuario de otra máquina virtual.

Puede conectar un disco persistente desconectado como un disco secundario en la máquina virtual de clones vinculados seleccionada. El nuevo usuario del clon vinculado tiene acceso al disco secundario y a la configuración y la información del usuario existente.

No puede conectar un disco persistente almacenado en un almacén de datos que no sea Virtual SAN a una máquina virtual que esté almacenada en un almacén de datos Virtual SAN. De forma similar, no puede conectar un disco que esté almacenado en un almacén de datos Virtual SAN a una máquina virtual que esté almacenada en un almacén de datos que no sea Virtual SAN. View Administrator evita que seleccione máquinas virtuales que amplíen los almacenes de datos que sean Virtual SAN y los que no lo sean.



Para trasladar un disco persistente desconectado a Virtual SAN, puede volver a crear el disco en una máquina virtual que esté en un almacén de datos que no sea Virtual SAN y volver a equilibrar el grupo de escritorios de la máquina virtual a un almacén de datos Virtual SAN. Consulte [Volver a crear un clon vinculado con un disco persistente desconectado](#).

#### Requisitos previos

- Compruebe que la máquina virtual seleccionada use el mismo sistema operativo que el clon vinculado en la que se creó el disco persistente.

#### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Discos persistentes**.
- 2 En la pestaña **Separado**, seleccione el disco persistente y haga clic en **Conectar**.
- 3 Seleccione una máquina virtual de clones vinculados a la que conectar el disco persistente.
- 4 Seleccione **Asociar como disco secundario**.
- 5 Haga clic en **Finalizar**.

#### Pasos siguientes

Asegúrese de que el usuario del clon vinculado cuente con privilegios suficientes para usar el disco secundario conectado. Por ejemplo, si el usuario original tiene ciertos permisos de acceso en el disco persistente y este último está conectado como la unidad D en la nuevo clon vinculado, el nuevo usuario del clon vinculado debe tener los permisos de acceso del usuario original en la unidad D.

Inicie sesión en el sistema operativo invitado del clon vinculado como un administrador y asigne al nuevo usuario los privilegios apropiados.

## Editar un usuario o un grupo de discos persistentes de View Composer

Puede asignar un disco persistente desconectado de View Composer a un nuevo usuario o grupo de escritorios si el usuario o el grupo de escritorios original se eliminó de View.

Un disco persistente desconectado sigue asociado al usuario y al grupo de escritorios originales. Si el usuario o el grupo de escritorios se eliminó de View, no podrá usar el disco persistente para volver a crear una máquina virtual de clones vinculados.

Al editar el usuario y el grupo de escritorios, puede usar el disco persistente desconectado para volver a crear una máquina virtual en el nuevo grupo de escritorios. La máquina virtual se asigna al nuevo usuario.

Puede seleccionar un nuevo grupo de escritorios, un nuevo usuario o ambos.

#### Requisitos previos

- Verifique que el usuario o el grupo de escritorios del disco persistente se eliminó de View.
- Verifique que el nuevo grupo de escritorios use el mismo sistema operativo que el grupo de escritorios en el que se creó el disco persistente.

**Procedimiento**

- 1 En View Administrator, seleccione **Recursos > Discos persistentes**
- 2 Seleccione el disco persistente del que se eliminó el usuario o el grupo de escritorios y haga clic en **Editar**.
- 3 (opcional) Seleccione un grupo de escritorios de clonación vinculada de la lista.
- 4 (opcional) Seleccione un usuario del disco persistente.

Puede examinar Active Directory para obtener el dominio y el nombre de usuario.

**Pasos siguientes**

Vuelva a crear una máquina virtual de clones vinculados con el disco persistente desconectado.

## Volver a crear un clon vinculado con un disco persistente desconectado

Cuando desconecta un disco persistente de View Composer, se elimina el clon vinculado. Puede proporcionar al usuario original acceso a la información y a la configuración del usuario desconectado recreando la máquina virtual de clones vinculados desde el disco desconectado.

---

**Nota** Si vuelve a crear una máquina virtual de clones vinculados en un grupo de escritorios que alcanzó su tamaño máximo, la máquina virtual que se volvió a crear sigue siendo parte del grupo de escritorios. El grupo de escritorios crece y supera el tamaño máximo especificado.

---

Si el usuario o el grupo de escritorios original del disco persistente se eliminaron de View, puede asignar uno nuevo para el disco persistente. Consulte [Editar un usuario o un grupo de discos persistentes de View Composer](#).

View no admite volver a crear una máquina virtual con un disco persistente que no esté almacenado en un almacén de datos de que no sea Virtual SAN si la nueva máquina virtual está almacenada en un almacén de datos Virtual SAN. De forma similar, si el disco persistente está almacenado en Virtual SAN, View no admite volver a crear una máquina virtual en un almacenamiento que no sea Virtual SAN.

Para trasladar un disco persistente desconectado a Virtual SAN, puede volver a crear el disco en una máquina virtual que esté en un almacén de datos que no sea Virtual SAN y volver a equilibrar el grupo de escritorios de la máquina virtual a un almacén de datos Virtual SAN.

**Procedimiento**

- 1 En View Administrator, seleccione **Recursos > Discos persistentes**.
- 2 En la pestaña **Separado**, seleccione el disco persistente y haga clic en **Volver a crear la máquina**.  
Puede seleccionar varios discos persistentes para volver a crear una máquina virtual de clones vinculados para cada disco.
- 3 Haga clic en **Aceptar**.

View crea una máquina virtual de clones vinculados para cada disco persistente que seleccionó y agrega la máquina virtual al grupo de escritorios original.

Los discos persistentes se mantienen en el almacén de datos en el que se almacenaron.

## Restaurar un clon vinculado importando un disco persistente desde vSphere

Si una máquina virtual de clones vinculados se vuelve inaccesible en View, puede restaurar la máquina virtual si se configuró con un disco persistente de View Composer. Puede importar el disco persistente de un almacén de datos de vSphere en View.

Importe el archivo de disco persistente como un disco persistente conectado en View. Puede conectar el disco desconectado a una máquina virtual existente o volver a crear el clon vinculado original en View.

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Discos persistentes**.
- 2 En la pestaña **Separado**, haga clic en **Importar desde vCenter**.
- 3 Seleccione una instancia de vCenter Server.
- 4 Seleccione la base de datos donde se encuentra el archivo de disco.
- 5 Seleccione un grupo de escritorios de clones vinculados en el que desee crear una nueva máquina virtual con el disco persistente.
- 6 En el cuadro de texto **Archivo de disco persistente**, haga clic en **Examinar**; a continuación, haga clic en la flecha hacia abajo y seleccione un almacén de datos del menú **Elegir un almacén de datos**.

No puede importar un disco persistente desde un almacén de datos local. Solo los almacenes de datos compartidos están disponibles.

- 7 Haga clic en el nombre del almacén de datos para mostrar los archivos de almacenamiento en disco y los archivos de la máquina virtual.
- 8 Seleccione el archivo de disco persistente que desee importar.
- 9 En el cuadro de texto **Usuario**, haga clic en **Examinar**, seleccione el usuario que desee asignar a la máquina virtual y haga clic en **Aceptar**.

El archivo de disco se importa en View como un disco persistente desconectado.

### Pasos siguientes

Para restaurar la máquina virtual de clones vinculados, puede volver a crear la máquina virtual original o conectar el disco persistente desconectado a otra máquina virtual.

Para obtener más información, consulte [Volver a crear un clon vinculado con un disco persistente desconectado](#) y [Conectar un disco persistente de View Composer a otro clon vinculado](#).

## Eliminar un disco persistente desconectado de View Composer

Cuando elimina un disco persistente desconectado, puede eliminar el disco de View y dejarlo en el almacén de datos o eliminarlo de View y del almacén de datos.

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Discos persistentes**.
- 2 En la pestaña **Separado**, seleccione el disco persistente y haga clic en **Eliminar**.
- 3 Seleccione si desea eliminar el disco del almacén de datos o mantenerlo en el almacén de datos después de eliminarlo de View.

Opción	Descripción
<b>Eliminar del disco</b>	Después de la eliminación, el disco persistente ya no existe.
<b>Eliminar únicamente de View</b>	Después de la eliminación, ya no se puede acceder al disco persistente en View pero se mantiene en el almacén de datos.

- 4 Haga clic en **Aceptar**.

# Administrar grupos de escritorios, equipos y sesiones

# 10

En View Administrator, puede administrar grupos de escritorios, escritorios basados en máquinas virtuales, escritorios basados en equipos físicos, sesiones de escritorio y de aplicaciones.

Este capítulo incluye los siguientes temas:

- [Administrar grupos de escritorios de clones instantáneos](#)
- [Administrar grupos de escritorios](#)
- [Administrar escritorios basados en máquinas virtuales](#)
- [Gestionar equipos no administrados](#)
- [Administrar sesiones de aplicaciones y escritorios publicados](#)
- [Exportar información de View a archivos externos](#)

## Administrar grupos de escritorios de clones instantáneos

En View Administrator, puede realizar las tareas administrativas en un grupo de escritorios de clones instantáneos como la programación de una operación de inserción de imagen.

### Cambiar la imagen de un grupo de escritorios de clones instantáneos

Puede cambiar la imagen de un grupo de escritorios de clones instantáneos para enviar cambios o volver a una imagen previa. También puede seleccionar que cualquier snapshot de una máquina virtual sea la nueva imagen.

#### Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo.
- 3 Seleccione **Insertar imagen > Programar**.

Se abre la ventana **Programar la inserción de la imagen**.

#### 4 Siga las indicaciones.

Puede programar que la tarea se inicie inmediatamente o en el futuro. En el caso de las clonaciones con sesiones de usuario, puede especificar si obligar a los usuarios a cerrar sesión o esperar. Cuando los usuarios cierran sesión, Horizon 7 vuelve a crear las clonaciones.

#### 5 En la página Listo para finalizar, haga clic en **Mostrar detalles** para ver la lista de escritorios en el grupo.

Después de iniciar esta operación, se inicia inmediatamente la publicación de la nueva imagen. Para obtener más información sobre cómo publicar, consulte "Grupos de escritorios de clones instantáneos" en el documento *Configurar escritorios virtuales en Horizon 7*. El proceso de volver a crear las clonaciones inicia a la hora que especificó en el asistente **Programar la inserción de la imagen**.

## Supervisar una operación de inserción de imagen

Puede supervisar el progreso de una operación de inserción de imagen en un grupo de escritorios de clones instantáneos en View Administrator.

### Procedimiento

#### 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.

#### 2 Haga doble clic en el ID del grupo.

La tabla **Resumen** muestra la información de la imagen pendiente y de la imagen actual.

#### 3 Haga clic en la pestaña **Tareas**.

Aparece la lista de tareas que están asociadas a la operación de inserción de imagen

## Volver a programar o cancelar una operación de inserción de imagen

Puede volver a programar o cancelar una operación de inserción de imagen en un grupo de escritorios de clones instantáneos en View Administrator.

### Procedimiento

#### 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.

#### 2 Haga doble clic en el ID del grupo.

La tabla **Resumen** muestra la información de la imagen pendiente y de la imagen actual.

#### 3 Seleccione **Insertar imagen > Reprogramar** o **Insertar imagen > Cancelar**.

#### 4 Siga las indicaciones.

Si cancela la operación de inserción de imagen mientras la creación del clon está en curso, los clones que tienen la nueva imagen siguen en el grupo y este tiene una mezcla de clones, algunos con la nueva imagen y otros con la antigua. Para asegurarse de que todas las clonaciones tengan la misma imagen, puede eliminar todas las clonaciones. View vuelve a crear las clonaciones con la misma imagen.

# Administrar grupos de escritorios

En View Administrator, puede realizar tareas administrativas en un grupo de escritorios como editar las propiedades, habilitar, deshabilitar o eliminar el grupo.

## Editar un grupo de escritorios

Puede editar un grupo de escritorios existente para configurar opciones como las especificaciones del número de máquinas de reserva, de los almacenes de datos y de personalización.

### Requisitos previos

Familiarícese con las opciones del grupo de escritorios que puede y que no puede cambiar después de que se cree un grupo de escritorios. Consulte [Modificar la configuración de un grupo de escritorios existente](#) y [Opciones mantenidas en un grupo de escritorios existente](#).

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Seleccione un grupo de escritorios y haga clic en **Editar**.
- 3 Haga clic en una pestaña del cuadro de diálogo Editar y vuelva a configurar las opciones del grupo de escritorios.
- 4 Haga clic en **Aceptar**.

Si cambia la imagen de un grupo de escritorios de clones instantáneos, la operación de publicación de imagen se iniciará inmediatamente. En View Administrator la página de resumen de los grupos de escritorios muestra el estado de la imagen pendiente como Publicando: cambio de infraestructura.

Si cambia el clúster de un grupo de escritorios de clones instantáneos, se crearán las máquinas virtuales principal y de réplica en el nuevo clúster. Puede iniciar una inserción de imagen con la misma imagen para tener nuevas clonaciones creadas en el nuevo clúster. Sin embargo, la máquina virtual de plantilla que se usa en el proceso de clonación se mantiene en el clúster antiguo. Puede poner el host ESXi en el que está la máquina virtual de plantilla en modo de mantenimiento, pero no puede migrar la máquina virtual de plantilla. Para eliminar completamente todas las máquinas virtuales de infraestructura, incluida la máquina virtual de plantilla, del clúster anterior, puede iniciar una inserción de imagen con una imagen nueva.

## Modificar la configuración de un grupo de escritorios existente

Después de crear un grupo de escritorios, puede cambiar algunas opciones de configuración.

Tabla 10-1. Opciones editables de un grupo de escritorios existente

Pestaña Configuración	Descripción
General	<p>Edite las opciones de nombre de escritorio y la configuración de administración de directivas de almacenamiento. La configuración de administración de directivas de almacenamiento determina si se puede usar un almacén de datos Virtual SAN. Si no utiliza Virtual SAN, puede seleccionar almacenes de datos independientes para los discos de SO y réplicas.</p> <p><b>Nota</b> En el caso de los clones vinculados de View Composer, debe usar una operación para volver a equilibrar si quiere migrar todas las máquinas virtuales del grupo de escritorios al almacén de datos Virtual SAN al que se cambia.</p>
Configuración del grupo de escritorios	<p>Edite la configuración de las máquinas, como la directiva de alimentación, el protocolo de visualización y las opciones de Adobe Flash. En Horizon 7.0, la directiva de alimentación no es compatible con los clones instantáneos.</p>
Configuración de aprovisionamiento	<p>Edite las opciones de aprovisionamiento del grupo de escritorios y agregue máquinas a este. Esta pestaña está disponible únicamente para los grupos de escritorios automáticos.</p>
Configuración de vCenter	<p>Edite la plantilla de máquinas virtuales o la imagen base predeterminada. Puede agregar o cambiar las instancias de vCenter Server, el clúster o host ESXi, los almacenes de datos y otras funciones de vCenter.</p> <p>Los nuevos valores solo afectan a las máquinas virtuales creadas después de modificar la configuración. Los ajustes nuevos no se aplican a las máquinas virtuales existentes.</p> <p>Esta pestaña está disponible únicamente para los grupos de escritorios automáticos.</p>
Personalización de invitado	<p>Si seleccionó Sysprep, puede cambiar la especificación de personalización. En Horizon 7.0, Sysprep no está disponible para los clones instantáneos.</p> <p>Si seleccionó QuickPrep, puede cambiar el contenedor y el dominio de Active Directory, así como especificar los scripts de desconexión y postsincronización.</p> <p>Si seleccionó ClonePrep, puede cambiar el contenedor de Active Directory, así como especificar los scripts de desconexión y postsincronización. Sin embargo, no puede modificar el dominio.</p> <p><b>Nota</b> Si cambia el nombre del script de desconexión o postsincronización o los parámetros de los clones instantáneos y el nuevo script existe en la imagen actual, este se ejecutará y se utilizarán los nuevos parámetros cuando se cree un clon. Si el nuevo script no existe en la imagen actual, debe seleccionar o crear una imagen que lo tenga y hacer una inserción de imagen.</p> <p>En el caso de los clones vinculados de View Composer, si cambia el nombre del script de desconexión o postsincronización, el cambio se aplica a la siguiente operación de recomposición. Sin embargo, los cambios de los parámetros de los scripts de desconexión o postsincronización se aplican a las clonaciones creadas con la snapshot actual.</p> <p>Esta pestaña está disponible únicamente para los grupos de escritorios automáticos.</p>



Pestaña	
Configuración	Descripción
<b>Almacenamiento avanzado &gt; Usar el acelerador de almacenamiento de View</b>	<p>Si selecciona <b>Usar el acelerador de almacenamiento de View</b>, anula su selección o reprograma cuando los archivos de resumen del acelerador de almacenamiento de View se regeneran, la configuración sí se aplica a las máquinas virtuales existentes. Si modifica la configuración del acelerador de almacenamiento de View de un grupo de escritorios existente, los cambios no se implementan hasta que las máquinas virtuales del grupo de escritorios se desconectan. Consulte "Configurar el acelerador de almacenamiento para los clones vinculados de View Composer" en el documento <i>Configurar escritorios virtuales en Horizon 7</i>.</p> <p><b>Nota</b> Si selecciona <b>Usar el acelerador de almacenamiento de View</b> en un clon vinculado de un grupo de escritorios existente y la réplica no tenía habilitado el acelerador de almacenamiento de View previamente, es posible que esta función no se aplique directamente. El acelerador de almacenamiento de View no se puede habilitar mientras se utiliza la réplica. Para forzar esta acción, puede recomponer el grupo de escritorios en una máquina virtual principal nueva.</p> <p>Esta opción se habilita automáticamente en los clones instantáneos.</p>
<b>Almacenamiento avanzado &gt; Reclamar espacio de disco de la máquina virtual</b>	<p>Si selecciona <b>Reclamar espacio de disco de la máquina virtual</b>, anula su selección o reprograma cuando se produce la recuperación de espacio de disco de la máquina virtual, la nueva configuración no afecta a las máquinas virtuales existentes si se crearon con discos eficientes de espacio. Consulte "Recuperar espacio de disco en las máquinas virtuales de clones vinculados" en el documento <i>Configurar escritorios virtuales en Horizon 7</i>.</p> <p>Esta opción no se aplica a los clones instantáneos.</p>
<b>Almacenamiento avanzado &gt; Usar snapshots NFS nativas (VAAI)</b>	<p>Si selecciona <b>Usar snapshots NFS nativas (VAAI)</b> o anula su selección, la nueva configuración solo afecta a las máquinas virtuales creadas después del cambio. Puede modificar las máquinas virtuales existentes para que sean clonaciones de snapshots NFS nativas y, si es necesario, volver a equilibrar el grupo de escritorios. Consulte "Usar la integración matriz de View Composer con la tecnología de snapshot nativa NFS" en el documento <i>Configurar escritorios virtuales en Horizon 7</i>.</p> <p>Esta opción no es compatible con los clones instantáneos.</p>
<b>Almacenamiento avanzado &gt; Ámbito de compartir página transparente</b>	<p>Si cambia la opción <b>Ámbito de compartir página transparente</b>, la nueva configuración se aplicará la próxima vez que se encienda la máquina virtual.</p> <p>Seleccione el nivel al que desea permitir que se compartan las páginas transparentes (TPS). Las opciones son <b>Máquina virtual</b> (predeterminada), <b>Grupo</b>, <b>Pod</b> o <b>Global</b>. Si activa TPS en todos los equipos del grupo, del pod o de forma global, el host ESXi elimina las copias redundantes de las páginas de memoria que se producen si el equipo usa el mismo sistema operativo invitado o las mismas aplicaciones.</p> <p>La acción de compartir páginas tiene lugar en el host ESXi. Por ejemplo, si habilita TPS en el nivel de grupo, pero dicho grupo se encuentra a través de varios hosts ESXi, solo se compartirán las máquinas virtuales del mismo host y dentro del mismo grupo. En el nivel global, todos los equipos gestionados por Horizon 7 en el mismo host ESXi pueden compartir páginas de memoria, independientemente del grupo en el que se encuentren.</p> <p><b>Nota</b> La opción predeterminada es no compartir páginas de memoria entre equipos porque TPS puede suponer un riesgo de seguridad. La investigación indica que se puede abusar de TPS para obtener acceso sin autorización a los datos en escenarios de configuración muy limitadas.</p> <p>Esta opción se habilita automáticamente en los clones instantáneos.</p>

Si edita un grupo de escritorios de clones instantáneos para agregar o eliminar almacenes de datos, se vuelven a equilibrar las máquinas virtuales cuando debe crearse un clon, por ejemplo, cuando un usuario cierra sesión o cuando aumenta el tamaño del grupo. Si quiere que se vuelvan a equilibrar de forma más rápida, haga lo siguiente:

- Si elimina un almacén de datos, elimine manualmente los escritorios que contenga para que los nuevos se creen en los almacenes de datos restantes.
- Si agrega un almacén de datos, elimine manualmente algunos escritorios de los almacenes de datos originales para que los nuevos escritorios se creen en el nuevo. También puede eliminar todos los escritorios para que se distribuyan de forma uniforme entre los almacenes de datos cuando se creen.

## Opciones mantenidas en un grupo de escritorios existente

Después de crear un grupo de escritorios, no puede cambiar algunas opciones de configuración.

**Tabla 10-2. Opciones mantenidas en un grupo de escritorios existente**

Configuración	Descripción
Tipo de grupo	Después de crear un grupo de escritorios RDS, manual o automático, no puede cambiar el tipo de grupo.
Asignación de usuario	No puede cambiar entre asignaciones dedicadas y flotantes.
Tipo de máquina virtual	No puede cambiar entre máquinas virtuales completas y de clones vinculados.
ID de grupo	No puede cambiar el ID del grupo.
Nomenclatura de la máquina y método de aprovisionamiento	Para agregar máquina virtual a un grupo de escritorios, debe usar el método de aprovisionamiento que se usó para crear el grupo. No puede cambiar entre especificar nombres de máquinas de forma manual y usar un patrón de nomenclatura. Si especifica los nombres de forma manual, puede agregar nombres a la lista de nombres de máquinas. Si usa un patrón de nomenclatura, puede aumentar el número máximo de máquinas.
Configuración de vCenter	No puede cambiar la configuración de vCenter para las máquinas virtuales existentes. Puede cambiar la configuración de vCenter en el cuadro de diálogo Editar, pero los valores solo afectan a las nuevas máquinas virtuales que se crean después de que la configuración se cambie.
Discos persistentes de View Composer	No puede configurar discos persistentes después de crear un grupo de escritorios de clones vinculados sin discos persistentes.
Método de personalización de View Composer	Después de personalizar un grupo de escritorios de clones vinculados con QuickPrep o Sysprep, no puede cambiar el otro método de personalización cuando cree o vuelva a componer las máquinas virtuales en el grupo.

## Cambiar el tamaño de un grupo automático aprovisionado por un patrón de nomenclatura

Cuando aprovisiona un grupo de escritorios automático con un patrón de nomenclatura, puede aumentar o disminuir el tamaño del grupo cambiando el número máximo de equipos.

## Requisitos previos

- Verifique que aprovisionó el grupo de escritorios usando un patrón de nomenclatura. Si especificó los nombres de los equipos de forma manual, consulte [Agregar máquinas a un grupo automatizado aprovisionado con una lista de nombres](#).
- Compruebe que el grupo de escritorios sea automático.

## Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Seleccione el grupo de escritorios y haga clic en **Editar**.
- 3 En la pestaña **Configuración de aprovisionamiento**, escriba el nuevo número de máquinas del grupo de escritorios en el cuadro de texto **Número máximo de máquinas**.

Si aumenta el tamaño del grupo de escritorios, se pueden agregar nuevas máquinas al grupo hasta alcanzar el número máximo.

Si disminuye el tamaño de un grupo de asignaciones flotantes, se eliminan las máquinas que no se utilicen. Si existen un número superior al nuevo máximo de usuarios con la sesión iniciada en el grupo, el tamaño del grupo disminuye después de que los usuarios cierren sesión.

Si disminuye el tamaño de un grupo de asignaciones dedicadas, se eliminan las máquinas que no se estén asignadas. Si existe un tamaño superior de usuarios asignados a máquinas al nuevo máximo, el tamaño del grupo disminuye después de anular la asignación de los usuarios.

---

**Nota** Cuando disminuya el tamaño de un grupo de escritorios, el número real de máquinas puede ser superior a **Número máximo de máquinas** si existe un valor superior de usuarios que iniciaron sesión o asignados a máquinas al especificado en **Número máximo de máquinas**.

---

## Agregar máquinas a un grupo automatizado aprovisionado con una lista de nombres

Para agregar máquinas a un grupo de escritorios automatizado que esté aprovisionado con nombres especificados de forma manual, proporcione otra lista de nuevos nombres de máquinas. Esta función le permite expandir un grupo de escritorios y continuar usando las convenciones de nomenclatura de su compañía.

En Horizon 7.0, esta función no es compatible con los clones instantáneos.

Siga estas directrices para agregar manualmente nombres de máquinas de forma manual:

- Escriba cada nombre de equipo en una línea independiente.
- El nombre de una máquina puede tener hasta 15 caracteres alfanuméricos.
- Puede agregar un nombre de usuario a cada entrada de máquina. Use una coma para separar el nombre de usuario y el nombre de máquina.

En este ejemplo, se agregaron dos máquinas. La segunda máquina está asociada a un usuario:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

**Nota** En un grupo de asignaciones flotantes, no es posible asociar nombres de usuarios con nombres de máquinas. Las máquinas no están dedicadas a los usuarios asociados. En un grupo de asignaciones flotantes, todas las máquinas que no estén en uso se mantienen accesibles para cualquier usuario que inicie sesión.

### Requisitos previos

Compruebe que creó el grupo de escritorios especificando los nombres de las máquinas de forma manual. No puede agregar máquinas con nombres nuevos si creó el grupo proporcionando un patrón de nomenclatura.

### Procedimiento

- 1 Cree un archivo de texto que contenga la lista de nombres de máquinas adicionales.  
Si solo pretende agregar algunas máquinas, puede escribir sus nombres directamente en el asistente **Agregar grupo de escritorios**. No es necesario que cree un archivo de texto independiente.
- 2 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 3 Seleccione el grupo de escritorios que desea expandir.
- 4 Haga clic en **Editar**.
- 5 Haga clic en la pestaña **Configuración de aprovisionamiento**.
- 6 Haga clic en **Agregar máquinas**.
- 7 Copie la lista de nombres en la página **Introducir nombres de máquinas** y haga clic en **Siguiente**.  
El asistente **Introducir nombres de máquinas** muestra la lista e indica los errores de validación con una **X** roja.
- 8 Corrija los nombres de las máquinas que no sean válidos.
  - a Coloque el cursor sobre un nombre no válido para que aparezca el mensaje de error relacionado en la parte inferior de la página.
  - b Haga clic en **Volver**.
  - c Edite los nombres incorrectos y haga clic en **Siguiente**.
- 9 Haga clic en **Finalizar**.
- 10 Haga clic en **Aceptar**.

En vCenter Server, puede supervisar la creación de las nuevas máquinas virtuales.

En View Administrator puede ver las máquinas al agregarse al grupo de escritorios seleccionando **Catálogo > Grupos de escritorios**.

## Deshabilitar o habilitar un grupo de escritorios

Cuando deshabilite un grupo de escritorios, este grupo ya no se presenta a los usuarios y se detiene el aprovisionamiento de grupos. Los usuarios no tienen acceso al grupo. Después de deshabilitar un grupo, puede volver a habilitarlo.

Puede deshabilitar un grupo de escritorios para evitar que los usuarios accedan a los escritorios remotos mientras prepara el escritorio para su uso. Si ya no se necesita un grupo de escritorios, puede usar la función Deshabilitar para descartar que el grupo se use de forma activa sin tener que eliminar la definición del grupo de escritorios de View.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Seleccione un grupo de escritorios y cambie el estado del grupo.

Opción	Acción
Deshabilitar el grupo	Seleccione <b>Deshabilitar grupo de escritorios</b> del menú desplegable <b>Estado</b> .
Habilitar el grupo	Seleccione <b>Habilitar grupo de escritorios</b> del menú desplegable <b>Estado</b> .

- 3 Haga clic en **Aceptar**.

## Habilitar o deshabilitar el aprovisionamiento en un grupo de escritorios automático

Cuando deshabilita el aprovisionamiento en un grupo de escritorios automático, View deja de aprovisionar nuevas máquinas virtuales para el grupo. Después de deshabilitar el aprovisionamiento, puede volverlo a habilitar.

Antes de cambiar la configuración de un grupo de escritorios, puede deshabilitar el aprovisionamiento para asegurar que no se creó ninguna máquina nueva con la configuración anterior. También puede deshabilitar el aprovisionamiento para evitar que View use un almacenamiento adicional cuando un grupo está a punto de llenar el espacio disponible.

Cuando el aprovisionamiento está deshabilitado en un grupo de escritorios vinculado, View detiene el aprovisionamiento de las nuevas máquinas y detiene su personalización después de que se vuelvan a componer o a equilibrar.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Seleccione un grupo de escritorios y cambie el estado del grupo.

Opción	Acción
Deshabilitar aprovisionamiento	Seleccione <b>Deshabilitar aprovisionamiento</b> del menú desplegable <b>Estado</b> .
Habilitar aprovisionamiento	Seleccione <b>Habilitar aprovisionamiento</b> del menú desplegable <b>Estado</b> .

- Haga clic en **Aceptar**.

## Configurar los límites y la calidad de Adobe Flash

Puede establecer los modos de límites y calidad de Adobe Flash para reducir la cantidad de ancho de banda que usan los contenidos de Adobe Flash en los escritorios remotos. Esta reducción puede mejorar la experiencia de navegación general y hacer que otras aplicaciones que se ejecutan en el escritorio remoto respondan mejor.

### Requisitos previos

Familiarícese con las opciones de límites y calidad de Adobe Flash. Consulte [Límites y calidad de Adobe Flash](#).

### Procedimiento

- En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- Seleccione un grupo de escritorios y haga clic en **Editar**.
- En la pestaña **Configuración del grupo de escritorio**, seleccione un modo de calidad en el menú **Calidad de Adobe Flash** y un modo de límites en el menú **Límite de Adobe Flash**.
- Haga clic en **Aceptar**.

**Nota** Las opciones de reducción de ancho de banda de Adobe Flash no se aplican hasta que Horizon Client se vuelva a conectar con el escritorio remoto.

## Límites y calidad de Adobe Flash

Puede establecer un nivel máximo permitido de calidad del contenido de Adobe Flash que reemplaza a la configuración de las páginas web. Si la calidad de Adobe Flash para una página web es superior al nivel máximo permitido, esta se reduce al máximo especificado. Una calidad más baja supone un mayor ahorro del ancho de banda.

Para utilizar la configuración de la reducción del ancho de banda de Adobe Flash, este no se debe ejecutar en modo de pantalla completa.

[Tabla 10-3. Configuración de calidad de Adobe Flash](#) muestra la configuración disponible de la calidad del procesamiento de Adobe Flash.

**Tabla 10-3. Configuración de calidad de Adobe Flash**

Configuración de calidad	Descripción
<b>No controlar</b>	La calidad está determinada según la configuración de la página web.
<b>Baja</b>	Esta configuración supone el mayor ahorro de ancho de banda.
<b>Media</b>	Esta configuración supone un ahorro de ancho de banda moderado.
<b>Alta</b>	Esta configuración supone el menor ahorro de ancho de banda.

Si no se especificó ningún nivel máximo de calidad, el sistema establece el valor predeterminado **Baja**.

Adobe Flash usa un temporizador para actualizar lo que aparece en pantalla en un tiempo determinado. Un intervalo de tiempo de Adobe Flash típico se encuentra entre 4 y 50 milisegundos. Al limitar o prolongar el intervalo, puede reducir la velocidad de fotogramas y, por lo tanto, reducir el ancho de banda.

[Tabla 10-4. Configuración de límites de Adobe Flash](#) muestra las opciones de los límites de Adobe Flash disponibles.

**Tabla 10-4. Configuración de límites de Adobe Flash**

Opción de limitación	Descripción
<b>Deshabilitado</b>	No se establece ningún límite. El intervalo de tiempo no se modifica.
<b>Conservador</b>	El intervalo de tiempo es 100 milisegundos. Esta opción tiene como resultado el menor número de fotogramas descartados.
<b>Moderado</b>	El intervalo de tiempo es 500 milisegundos.
<b>Agresivo</b>	El intervalo de tiempo es 2500 milisegundos. Esta opción tiene como resultado el mayor número de fotogramas descartados.

La velocidad del audio se mantiene constante, independientemente de qué opción seleccione.

## Eliminar un grupo de escritorios

Cuando elimine un grupo de escritorios, los usuarios no podrán iniciar nuevos escritorios remotos en el grupo.

Dependiendo del tipo de grupo de escritorios, tiene varias opciones en función del modo en que View administra los grupos persistentes, las máquinas virtuales completas de vCenter Server y las sesiones activas de los usuarios.

De forma predeterminada, puede eliminar un grupo de escritorios aunque existan equipos de escritorio en el grupo. View no le advierte sobre ello. Puede configurar View para que no permita la eliminación de un grupo que contiene equipos de escritorio. Para obtener más información, consulte [Configurar View para no permitir la eliminación de un grupo que contiene equipos de escritorio](#). Si configuró la opción, debe eliminar todos los equipos de un grupo de escritorios antes de poder eliminar el grupo.

Con un grupo de escritorios automático de clones instantáneos o clones vinculados de View Composer, View siempre elimina las máquinas virtuales del disco.

**Importante** No elimine las máquinas virtuales de vCenter Server antes de eliminar un grupo de escritorios con View Administrator. Esta acción puede implicar que los componentes de View tengan un estado incoherente.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Seleccione un grupo de escritorios y haga clic en **Eliminar**.

### 3 Seleccione cómo eliminar el grupo de escritorios.

Grupo	Opciones
<b>Grupo automático de escritorio de clones instantáneos o clones vinculados sin discos persistentes.</b>	Sin opciones disponible. View elimina todas las máquinas virtuales del disco. Se cierran las sesiones de los usuarios en sus escritorios remotos.
<b>Grupo automático de escritorio de clones vinculados con discos persistentes.</b>	<p>Seleccione si desea desconectar o eliminar los discos persistentes cuando se eliminan las máquinas virtuales de clones vinculados.</p> <p>En ambos casos, View elimina todas las máquinas virtuales del disco y se cierran las sesiones de los usuarios en sus escritorios remotos.</p> <p>Si desconecta un disco persistente, la máquina virtual de clones vinculados que contiene el disco persistente se puede volver a crear, o bien, el disco persistente se puede conectar a otra máquina virtual. Puede almacenar discos persistentes desconectados en el mismo almacén de datos o en uno diferente. Si selecciona un almacén de datos diferente, no puede almacenar discos persistentes desconectados en un almacén de datos local. Debe usar un almacén de datos compartido.</p> <p>Solo puede desconectar discos persistentes que se crearon en View 4.5 o en versiones posteriores.</p>
<b>Grupos automáticos de escritorios de máquinas virtuales completas.</b> <b>Grupo manual de escritorios de las máquinas virtuales de vCenter Server.</b>	Seleccione si desea mantener o eliminar las máquinas virtuales en vCenter Server.
<b>Grupo de escritorios RDS.</b> <b>Grupos automáticos de escritorios de máquinas virtuales completas.</b> <b>Grupo de escritorios manual.</b>	Si existen usuarios que estén conectados a sus escritorios remotos, seleccione si desea mantener las sesiones activas o finalizarlas. Tenga en cuenta que el servidor de conexión de View no realiza un seguimiento de las sesiones que siguen activas.

Cuando elimine un grupo de escritorios, las cuentas de equipo de las máquinas virtuales de clones vinculados se eliminarán de Active Directory. Las cuentas de los equipos de las máquinas virtuales completas se mantienen en Active Directory. Para eliminar estas cuentas, debe eliminarlas de forma manual desde Active Directory.

Si elimina un grupo de escritorios de un clon instantáneo, View puede tardar en eliminar las máquinas virtuales internas de vCenter Server. No elimine vCenter Server de View Administrator hasta que no verifique que todas las máquinas virtuales internas se eliminaron.

## Configurar View para no permitir la eliminación de un grupo que contiene equipos de escritorio

Puede configurar View para que no permita la eliminación de un grupo que contiene equipos de escritorio. De forma predeterminada, View permite la eliminación de ese tipo de grupos.

Si configuró esta opción, debe eliminar todos los equipos de un grupo de escritorios antes de poder eliminar el grupo.



## 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 de View.
- 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 plenamente cualificado (FQDN) del host del servidor de conexión de View 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-NameValuePair** y agregue el valor **cs-disableNonEmptyPoolDelete=1**.

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

# Administrar escritorios basados en máquinas virtuales

Un escritorio basado en una máquina virtual es un escritorio que proviene de un grupo de escritorios automático o de un grupo de escritorios manual que contiene máquinas virtuales de vCenter Server.

## Asignar una máquina a un usuario

En un grupo de asignación dedicada, puede establecer que un usuario sea el propietario de la máquina virtual que aloja un escritorio remoto. Solo el usuario asignado podrá iniciar sesión y conectarse al escritorio remoto.

View asigna máquinas a usuarios en los siguientes casos.

- Si crea un grupo de escritorios y selecciona la función **Habilitar asignación automática**.

---

**Nota** Puede seguir asignando máquinas a usuarios de forma manual si selecciona la función **Habilitar asignación automática**.

---

- Si crea un grupo automatizado, seleccione la función **Especificar nombres de forma manual** y luego introduzca nombres de usuario para los nombres de máquinas.

Si no selecciona ninguna opción de configuración en un grupo de asignación dedicada, los usuarios no tendrán acceso a escritorios remotos. Deberá asignar de forma manual una máquina a cada usuario.

También puede usar el comando `vdmadmin` para asignar máquinas a los usuarios. Consulte [Asignar máquinas dedicadas usando la opción -L](#).

## Requisitos previos

- Compruebe que la máquina virtual del escritorio remoto pertenezca a un grupo de asignación dedicada. En View Administrator, la asignación de grupos de escritorios aparece en la columna de Grupos de escritorios de la página de Máquinas.

## Procedimiento

- 1 En View Administrator, seleccione **Recursos > Máquinas** o seleccione **Catálogo > Grupos de escritorios**, haga doble clic en el ID de grupo y haga clic en la pestaña de **Inventario**.
- 2 Seleccione la máquina.
- 3 Seleccione **Asignar usuario** del menú desplegable **Más comandos**.
- 4 Decida si desea buscar usuarios o grupos, seleccione un dominio e introduzca una cadena de búsqueda en el cuadro de texto **Nombre** o **Descripción**.
- 5 Seleccione el nombre de usuario o grupo y haga clic en **Aceptar**.

## Eliminar la asignación de un usuario de una máquina dedicada

En un grupo de asignaciones dedicadas, puede eliminar una asignación de una máquina a un usuario.

El comando `vdadmin` permite eliminar la asignación de una máquina a un usuario. Consulte [Asignar máquinas dedicadas usando la opción -L](#).

## Procedimiento

- 1 En View Administrator, seleccione **Recursos > Máquinas** o seleccione **Catálogo > Grupos de escritorios**, haga doble clic en el ID de grupo y haga clic en la pestaña de **Inventario**.
- 2 Seleccione la máquina.
- 3 Seleccione **Eliminar la asignación del usuario** del menú desplegable **Más comandos**.
- 4 Haga clic en **Aceptar**.

La máquina está disponible y se puede asignar a otro usuario.

## Personalizar los equipos existentes en modo de mantenimiento

Después de que se cree un grupo de escritorios, puede personalizar, modificar o realizar pruebas en los equipos individuales activando su modo de mantenimiento. Cuando un equipo se encuentra en modo de mantenimiento, los usuarios no pueden acceder al escritorio de la máquina virtual.

Solo se puede poner un equipo en modo de mantenimiento de forma simultánea. Puede eliminar varios equipos del modo de mantenimiento en una sola operación.

Cuando crea un grupo de escritorios, puede iniciar todos los equipos del grupo en modo de mantenimiento si especifica los nombres de equipos de forma manual. Para obtener más información, consulte "Personalizar escritorios en modo de mantenimiento" en el documento *Configurar escritorios virtuales en Horizon 7*.

En Horizon 7.0, esta función no es compatible con los clones instantáneos.

## Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Máquinas** o seleccione **Catálogo > Grupos de escritorios**, haga doble clic en el ID de grupo y seleccione la pestaña **Inventario**.
- 2 Seleccione un equipo.
- 3 Seleccione **Entrar en modo de mantenimiento** del menú desplegable **Más comandos**.
- 4 Personalice, modifique o pruebe el escritorio de la máquina virtual.
- 5 Repita [Paso 2](#) a través de [Paso 4](#) en todas las máquinas virtuales que desee personalizar.
- 6 Seleccione los equipos personalizados y seleccione **Salir del modo de mantenimiento** en el menú desplegable **Más comandos**.

Los escritorios de las máquinas virtuales modificados están disponibles para los usuarios.

## Supervisar el estado del escritorio de la máquina virtual

Puede supervisar el estado de los escritorios de las máquinas virtuales de la implementación de View usando el panel de control de View Administrator. Por ejemplo, puede mostrar todas las máquinas virtuales desconectadas o que estén en modo de mantenimiento.

### Requisitos previos

Familiarícese con los estados de las máquinas virtuales. Consulte [Estado de las máquinas virtuales de vCenter Server](#).

## Procedimiento

- 1 En View Administrator, haga clic en **Panel**.
- 2 En el panel Estado de la máquina, expanda una carpeta de estado.

Opción	Descripción
<b>Preparando</b>	Muestra los estados de la máquina mientras esta se aprovisiona, se elimina o está en modo de mantenimiento.
<b>Máquinas con problemas</b>	Muestra los estados de error de la máquina.
<b>Preparado para su uso</b>	Muestra los estados de la máquina cuando la máquina virtual está lista para su uso.

- 3 Ubique el estado de la máquina y haga clic en el número hipervinculado que aparece junto a ella.

La página Máquinas muestra todas las máquinas virtuales con el estado seleccionado.

### Pasos siguientes

Puede hacer clic en el nombre de una máquina virtual para ver los detalles sobre la máquina o haga clic en la flecha de retroceso de View Administrator para volver a la página del panel de control.

## Estado de las máquinas virtuales de vCenter Server

Las máquinas virtuales que administra vCenter Server pueden tener varios estados de operación y disponibilidad. En Horizon Administrator, puede realizar un seguimiento del estado de las máquinas en la columna situada en la parte derecha de la página Máquinas.

[Tabla 10-5. Estados de las máquinas virtuales que administra vCenter Server](#) muestra el estado de los escritorios de las máquinas virtuales no administradas que aparecen en Horizon Administrator. Un escritorio solo puede tener un estado al mismo tiempo.

**Tabla 10-5. Estados de las máquinas virtuales que administra vCenter Server**

Estado	Descripción
Aprovisionamiento	Se están aprovisionando las máquinas virtuales.
Personalizando	Se está personalizando la máquina virtual de un grupo automático.
Eliminar	Se marcó la máquina virtual para su eliminación. Horizon 7 eliminará la máquina virtual pronto.
Esperando al agente	El servidor de conexión de Horizon está esperando para establecer la comunicación con View Agent o con Horizon Agent en una máquina virtual de un grupo de escritorios.
Modo de mantenimiento	La máquina virtual está en modo de mantenimiento. Los usuarios no pueden iniciar sesión ni usar la máquina virtual.
Inicio	View Agent o Horizon Agent se iniciaron en la máquina virtual, pero aún se están iniciando otros servicios requeridos, como el protocolo de visualización. Por ejemplo, View Agent no puede establecer una conexión RDP con equipos cliente hasta que RDP acabe de iniciarse. El periodo de inicio del agente permite que se inicien otros procesos como los servicios de protocolo.
Agente deshabilitado	Este estado se puede producir en dos casos. En primer lugar, en un grupo de escritorios con las opciones <b>Eliminar o actualizar la máquina al cerrar sesión</b> o <b>Eliminar máquina después de cerrar sesión</b> habilitadas, una sesión de escritorio está cerrada, pero la máquina virtual aún no se actualizó ni se eliminó. En segundo lugar, el servidor de conexión de View deshabilita View Agent o Horizon Agent antes de enviar una solicitud para desconectar la máquina virtual. Este estado asegura que no se pueda iniciar una nueva sesión de escritorio en la máquina virtual.
Agente inaccesible	El servidor de conexión de View no puede establecer la comunicación con View Agent ni con Horizon Agent en la máquina virtual.
IP no válida	La opción del registro de máscara de subred se configura en la máquina virtual y ningún adaptador de red activo tiene una dirección IP dentro del rango configurado.
El agente necesita reiniciarse	Se actualizó un componente de Horizon 7 y la máquina virtual se debe reiniciar para permitir que View Agent o Horizon Agent funcionen con el componente actualizado.
Error de protocolo	No se inició ningún protocolo de visualización antes de que caducara el periodo de inicio de Horizon Agent o de View Agent.

**Nota** View Administrator puede mostrar máquinas con el estado **Error de protocolo** si se produjo un error en un protocolo, pero los demás se iniciaron correctamente. Por ejemplo, el estado **Error de protocolo** puede aparecer si se produjo un error en HTML Access, pero PCoIP y RDP siguen funcionando. En este caso, las máquinas están disponibles y los dispositivos de Horizon Client pueden acceder a ellas a través de PCoIP o RDP.

Estado	Descripción
Error de dominio	Se produjo un problema en la máquina virtual al alcanzar el dominio. No se pudo acceder al servidor de dominio o se produjo un error en la autenticación del dominio.
Ya en uso	<p>En un grupo de escritorios con las opciones <b>Eliminar o actualizar la máquina al cerrar sesión</b> o <b>Eliminar máquina después de cerrar sesión</b> habilitadas, no existe ninguna sesión activa en la máquina virtual, pero la última sesión no se cerró.</p> <p>Esta condición se puede producir si una máquina virtual se apaga de forma inesperada o si el usuario restablece la máquina durante una sesión. De forma predeterminada, cuando una máquina virtual está en este estado, Horizon 7 evita que otros dispositivos de Horizon Client accedan al escritorio.</p>
Error de configuración	No está habilitado ningún protocolo de visualización como RDP o PCoIP.
Error de aprovisionamiento	Se produjo un error durante el aprovisionamiento.
Error	Se produjo un error desconocido en la máquina virtual.
Usuario sin asignar conectado	Un usuario distinto al asignado inició sesión en una máquina virtual de un grupo dedicado. Por ejemplo, este estado se puede producir si un administrador inicia vSphere Client, abre una consola en la máquina virtual e inicia sesión.
Usuario sin asignar desconectado	Un usuario distinto al usuario asignado inició sesión en una máquina virtual de un grupo de asignación dedicada y se desconectó de ella.
Desconocido	La máquina virtual se encuentra en un estado desconocido.
Aprovisionada	La máquina virtual está desconectada o suspendida.
Disponible	La máquina virtual está encendida y lista para realizar una conexión. En un grupo dedicado, la máquina virtual se asigna a un usuario y se iniciará cuando el usuario inicie sesión.
Conectado	La máquina virtual está en una sesión y tiene una conexión remota al dispositivo de Horizon Client.
Desconectado	La máquina virtual está en una sesión, pero está desconectada del dispositivo de Horizon Client.
En curso	La máquina virtual está en un estado de transición durante una operación de mantenimiento.

Mientras una máquina está en un estado concreto, puede estar sujeta a otras condiciones. Horizon Administrator muestra estas condiciones como sufijos del estado de la máquina. Por ejemplo, Horizon Administrator puede tener el estado Personalizar (falta).

[Tabla 10-6. Condiciones del estado de la máquina](#) muestra estas condiciones adicionales.

Tabla 10-6. Condiciones del estado de la máquina

Condición	Descripción
Falta	<p>La máquina virtual no se encuentra en vCenter Server.</p> <p>Es posible que la máquina virtual se eliminara de vCenter Server, pero que la configuración LDAP de Horizon aún tenga un registro de la máquina.</p>
Tarea detenida	<p>Se detuvo una tarea de clonación instantánea, como una operación de inserción de imagen o de View Composer, por ejemplo, de actualización, recomposición o para volver a equilibrar.</p> <p>Para obtener más información sobre cómo solucionar un problema de una operación de recomposición, consulte <a href="#">Corregir una recomposición que no se realizó correctamente</a>.</p> <p>Para obtener más información sobre los estados de error de View Composer, consulte "Errores de aprovisionamiento de View Composer" en el documento <i>Configurar escritorios virtuales en Horizon 7</i>.</p> <p>La condición Tarea detenida se aplica a todas las máquinas virtuales que se seleccionaron para la operación, pero en las que aún no se inició. Las máquinas virtuales del grupo que no se seleccionaron para la operación no tienen la condición Tarea detenida.</p>

Un estado de máquina puede estar sujeto a ambas condiciones, (falta, tarea detenida), si se detuvo una tarea de View Composer y no se encuentra la máquina virtual en vCenter Server.

## Eliminar escritorios de máquina virtual

Cuando elimine un escritorio de máquina virtual, los usuarios ya no tendrán acceso al escritorio. Un escritorio de máquina virtual puede ser una máquina virtual de vCenter Server o una máquina virtual sin administrar.

Los usuarios que tengan sesiones activas en ese momento pueden continuar usando los escritorios de máquina virtual completos si los mantiene en vCenter Server. Después de que los usuarios cierren sesión, no podrán acceder a los escritorios de máquina virtual eliminados.

Con las máquinas virtuales de clones vinculados y de clones instantáneos, vCenter Server siempre elimina las máquinas virtuales del disco.

**Nota** No elimine las máquinas virtuales de vCenter Server antes de eliminar los escritorios de la máquina virtual con View Administrator. Esta acción puede implicar que los componentes de View tengan un estado incoherente.

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Máquinas**.
- 2 Seleccione la pestaña **Máquinas virtuales de vCenter** o la pestaña **Otros**.
- 3 Seleccione una o varias máquinas y haga clic en **Eliminar**.

#### 4 Seleccione cómo eliminar el escritorio de la máquina virtual.

Opción	Descripción
<b>Grupo que contiene escritorios de máquina virtual completa</b>	<p>Seleccione si desea mantener o eliminar las máquinas virtuales en vCenter Server.</p> <p>Si elimina las máquinas virtuales del disco, los usuarios con sesiones activas se desconectan de sus escritorios.</p> <p>Si mantiene las máquinas virtuales en vCenter Server, seleccione si desea permitir que los usuarios con sesiones activas sigan conectados a los escritorios o si desea desconectarlos.</p>
<b>Grupo de clones vinculados de View Composer con discos persistentes</b>	<p>Seleccione si desea desconectar o eliminar los discos persistentes cuando se eliminan los escritorios de máquina virtual.</p> <p>En ambos casos, vCenter Server elimina las máquinas virtuales de clones vinculados del disco. Los usuarios con sesiones activas en ese momento se desconectan de los escritorios remotos.</p> <p>Si desconecta un disco persistente, la máquina virtual de clones vinculados que contiene el disco persistente se puede volver a crear, o bien, el disco persistente se puede conectar a otra máquina virtual. Puede almacenar discos persistentes desconectados en el mismo almacén de datos o en uno diferente. Si selecciona un almacén de datos diferente, no puede almacenar discos persistentes desconectados en un almacén de datos local. Debe usar un almacén de datos compartido.</p> <p>Solo puede desconectar discos persistentes que se crearon en View 4.5 o en versiones posteriores.</p>
<b>Grupo de clones instantáneos y grupo de clones vinculados de View Composer sin discos persistentes</b>	<p>vCenter Server elimina las máquinas virtuales de clones vinculados del disco. Los usuarios con sesiones activas en ese momento se desconectan de los escritorios remotos.</p>

Cuando elimine escritorios de la máquina virtual, las cuentas de equipo de la máquina virtual de clones vinculados se eliminarán de Active Directory. Las cuentas de las máquinas virtuales completas se mantienen en Active Directory. Para eliminar estas cuentas, debe eliminarlas de forma manual desde Active Directory.

## Recuperar los escritorios de clones instantáneos

Cuando un escritorio de clones instantáneos se encuentra en un estado de error, tiene la opción de recuperarlo. El escritorio se vuelve a crear desde la imagen de base actual.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupo de escritorios**, haga doble clic en un ID de grupo y, a continuación, en la pestaña **Inventario**.
- 2 Seleccione una o varias máquinas y haga clic en **Recuperar**.

## Gestionar equipos no administrados

En View Administrator, puede agregar y eliminar equipos no administrados de los grupos de escritorios manuales y eliminar los equipos registrados de View. Los equipos no administrados incluyen equipos físicos y máquinas virtuales que vCenter Server no administra.

Para obtener más información sobre cómo eliminar un grupo que contenga equipos no administrados, consulte [Eliminar un grupo de escritorios](#).

Cuando vuelva a configurar una opción que afecte a un equipo no administrado, la nueva opción puede tardar hasta 10 minutos en aplicarse. Por ejemplo, si cambia Modo de seguridad del mensaje en la Configuración global o cambia la opción **Cerrar sesión automáticamente tras desconectarse** View, podría tardar hasta 10 minutos en volver a configurar los equipos afectados sin administrar.

---

**Nota** Los hosts RDS también son equipos no administrados, ya que no se generan desde una máquina virtual principal o una plantilla y los administran vCenter Server. Los hosts RDS admiten aplicaciones y escritorios basados en sesiones y se tratan como categorías independientes. Consulte [Administrar los hosts RDS](#).

---

## Agregar un equipo no administrado a un grupo manual

Puede aumentar el tamaño de un grupo de escritorios manual al agregar equipos no administrados al grupo.

### Requisitos previos

Compruebe que Horizon Agent esté instalado en el equipo no administrado. Para obtener más información sobre cómo preparar una máquina sin administrar, consulte "Instalar Horizon Agent en una máquina sin administrar" en el documento *Configurar escritorios virtuales en Horizon 7*.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo manual.
- 3 En la pestaña **Inventario**, haga clic en **Agregar**.
- 4 Seleccione los equipos no administrados en la ventana **Agregar escritorio** y haga clic en **Aceptar**.

Los equipos no administrados se agregan al grupo.

## Eliminar un equipo no administrado de un grupo de escritorios manual

Puede reducir el tamaño de un grupo de escritorios manual al eliminar equipos no administrados del grupo.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios**.
- 2 Haga doble clic en el ID del grupo manual.
- 3 Seleccione la pestaña **Inventario**.
- 4 Seleccione los equipos no administrados que desee eliminar.
- 5 Haga clic en **Eliminar**.



- 6 Si los usuarios iniciaron sesión en los escritorios basados en equipos no administrados, seleccione si desea finalizar las sesiones o mantenerlas activas.

Opción	Descripción
Mantener activa	Las sesiones activas se mantienen hasta que el usuario cierra sesión. El servidor de conexión de View no realiza ningún seguimiento de estas sesiones.
Terminar	Las sesiones activas se finalizan inmediatamente.

- 7 Haga clic en **Aceptar**.

Los equipos no administrados se eliminan del grupo.

## Eliminar las máquinas registradas de View

Si no tiene pensado volver a usar una máquina registrada, puede eliminarla de View.

Existen dos tipos de máquinas registradas en View: Hosts RDS y Otros. Las máquinas sin administrar están en la categoría Otros. Los equipos no administrados incluyen equipos físicos y máquinas virtuales que vCenter Server no administra. Se usan para formar grupos de escritorios manuales que no contengan máquinas virtuales de vCenter Server.

Después de eliminar una máquina registrada, ya no está disponible en View. Para que la máquina vuelva a estar disponible, debe volver a instalar Horizon Agent.

### Requisitos previos

Compruebe que las máquinas registradas que desee eliminar no se utilizan en ningún grupo de escritorios.

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Máquinas registradas**.
- 2 Haga clic en la pestaña **Otros**.
- 3 Seleccione una o varias máquinas y haga clic en **Eliminar**.  
Solo puede seleccionar la máquinas que ningún grupo de escritorios esté utilizando.
- 4 Haga clic en **Aceptar** para confirmar.

## Estado de las máquinas no administradas

Las máquinas no administradas, que son máquinas virtuales o equipos físicos que no están administrados por vCenter Server, pueden estar en varios estados de operación y disponibilidad. En View Administrator, puede realizar un seguimiento del estado de las máquinas no administradas en la columna situada en la parte derecha de la página Máquinas bajo las pestaña **Otros**.

[Tabla 10-7. Estado de las máquinas no administradas](#) muestra el estado operativo de las máquinas no administradas que aparecen en View Administrator. Un equipo solo puede tener un estado a la vez.

Tabla 10-7. Estado de las máquinas no administradas

Estado	Descripción
Inicio	View Agent o Horizon Agent se iniciaron en la máquina, pero aún se están iniciando otros servicios obligatorios, como el protocolo de visualización. El periodo de inicio del agente permite que se inicien otros procesos como los servicios de protocolo.
Validando	Este estado se produce después de que el servidor de conexión de View reconozca por primera vez la máquina, normalmente después de que el servidor de conexión de View se inicie o se reinicie y después de la primera comunicación correcta con View Agent o Horizon Agent en la máquina. Normalmente, este estado es transitorio. Este no es el mismo que el estado Agente inaccesible, que indica un problema de comunicación.
Agente deshabilitado	Este estado se puede producir si el servidor de conexión de View deshabilita View Agent o Horizon Agent. Este estado garantiza que no se pueda iniciar una nueva sesión de escritorio en la máquina.
Agente inaccesible	El servidor de conexión de View no puede establecer la comunicación con View Agent ni Horizon Agent en la máquina. La máquina se podría desconectar.
IP no válida	La opción del registro de máscara de subred se configura en la máquina y ningún adaptador de red activo tiene una dirección IP dentro del rango configurado.
El agente necesita reiniciarse	Se actualizó un componente de View y la máquina se debe reiniciar para permitir que View Agent o Horizon Agent funcionen con el componente actualizado.
Error de protocolo	<p>No se inició ningún protocolo de visualización antes de que caducara el periodo de inicio de Horizon Agent o de View Agent.</p> <p><b>Nota</b> View Administrator puede mostrar máquinas con el estado <b>Error de protocolo</b> si se produjo un error en un protocolo, pero los demás se iniciaron correctamente. Por ejemplo, el estado <b>Error de protocolo</b> puede aparecer si se produjo un error en HTML Access, pero PCoIP y RDP siguen funcionando. En este caso, las máquinas están disponibles y los dispositivos de Horizon Client pueden acceder a ellas a través de PCoIP o RDP.</p>
Error de dominio	Se produjo un problema en la máquina al alcanzar el dominio. No se pudo acceder al servidor de dominio o se produjo un error en la autenticación del dominio.
Error de configuración	No se habilitó ningún protocolo de visualización como RDP ni otro protocolo.
Usuario sin asignar conectado	<p>Un usuario distinto al asignado inició sesión en una máquina de un grupo de asignación dedicada.</p> <p>Por ejemplo, este estado se puede producir si un administrador inicia sesión en la máquina no administrada sin usar Horizon Client.</p>
Usuario sin asignar desconectado	Un usuario distinto al usuario asignado inició sesión en una máquina de un grupo de asignación dedicada y se desconectó de ella.
Desconocido	La máquina se encuentra en un estado desconocido.
Disponible	El equipo de origen del escritorio está encendido y el escritorio está preparado para establecer o recibir una conexión. En un grupo dedicado, el escritorio se asigna a un usuario. El escritorio se inicia cuando el usuario inicia sesión.
Conectado	El escritorio está en una sesión y tiene una conexión remota a un dispositivo de Horizon Client.
Desconectado	El escritorio está en una sesión pero está desconectado del dispositivo de Horizon Client.

# Administrar sesiones de aplicaciones y escritorios publicados

Cuando un usuario inicia una aplicación o un escritorio publicados, se crea una sesión. Puede desconectar y cerrar las sesiones, enviar mensajes a los clientes, restablecer y reiniciar las máquinas virtuales.

## Procedimiento

- 1 En Horizon Administrator, diríjase al lugar donde aparece la información de la sesión.

Tipo de sesión	Navegación
Sesiones de escritorios remotos	Seleccione <b>Catálogo &gt; Grupo de escritorios</b> , haga doble clic en un ID de grupo y, a continuación, en la pestaña <b>Sesiones</b> .
Sesiones de aplicaciones y escritorios remotos	Seleccione <b>Supervisión &gt; Sesiones</b> .
Sesiones asociadas a un usuario o grupo de usuarios	<ul style="list-style-type: none"> <li>■ Seleccione <b>Usuarios y grupos</b>.</li> <li>■ Haga doble clic en un nombre de usuario o un nombre de grupo de usuarios.</li> <li>■ Haga clic en la pestaña <b>Sesiones</b>.</li> </ul>

- 2 Seleccione una sesión.

Para enviar un mensaje a los usuarios, puede seleccionar varias sesiones. Puede realizar las otras operaciones en una sola sesión al mismo tiempo.

- 3 Seleccione si desea desconectarse, cerrar sesión, enviar un mensaje o restablecer una máquina virtual.

Opción	Descripción
Desconectar sesión	Desconecta el usuario de la sesión.
Cerrar sesión	Cierra la sesión del usuario. Se pierden los datos que no se guardaron.
Enviar mensaje	Enviar un mensaje a Horizon Client. Puede etiquetar este mensaje como <b>Información</b> , <b>Advertencia</b> o <b>Error</b> .

- 4 Haga clic en **Aceptar**.

## Exportar información de View a archivos externos

En View Administrator puede exportar la información de la tabla de View a archivos externos. Puede exportar las tablas que muestran usuarios y grupos, grupos, máquinas, discos persistentes de View Composer, aplicaciones ThinApp, eventos y sesiones VDI. Puede ver y administrar la información en una hoja de cálculo u otra herramienta.

Por ejemplo, puede recopilar información sobre los equipos que están administrados por más de una instancia del servidor de conexión de View o por un grupo de instancias replicadas del servidor de conexión de View. Puede exportar la tabla Máquinas de cada interfaz de View Administrator y verla en una hoja de cálculo.

Cuando exporte una tabla de View Administrator, esta se guarda como un archivo de valores separados por coma (CSV). Esta función exporta la tabla completa, no páginas individuales.

### Procedimiento

- 1 En View Administrator, acceda la tabla que quiere exportar.

Por ejemplo, haga clic en **Recursos > Máquinas** para mostrar la tabla de máquinas.

- 2 Haga clic en el icono de exportación situado en la esquina superior derecha de la tabla.

Cuando se sitúe sobre el icono, aparecerá la información sobre herramientas Exportar contenido de la tabla.

- 3 Introduzca un nombre para el archivo CSV en el cuadro de diálogo Seleccionar ubicación de descarga.

El nombre de archivo predeterminado es `global_table_data_export.csv`.

- 4 Examine una ubicación para almacenar el archivo.

- 5 Haga clic en **Guardar**.

### Pasos siguientes

Abra una hoja de cálculo u otra herramienta para ver el archivo CSV.

# Administrar hosts RDS, granjas y grupos de aplicaciones

# 11

En Horizon Administrator, puede realizar operaciones de administración como la configuración o la eliminación de hosts RDS, de granjas o de grupos de escritorios.

Este capítulo incluye los siguientes temas:

- [Administrar grupos de aplicaciones](#)
- [Administrar granjas](#)
- [Administrar los hosts RDS](#)
- [Configurar el equilibrio de carga de los hosts RDS](#)
- [Configurar una regla anti-compatibilidad para un grupo de aplicaciones](#)

## Administrar grupos de aplicaciones

Puede agregar, editar, eliminar o autorizar grupos de aplicaciones en Horizon Administrator.

Para agregar un grupo de aplicaciones, consulte "Crear grupos de aplicaciones" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para autorizar un grupo de aplicaciones, consulte "Autorizar usuarios y grupos" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

## Editar un grupo de aplicaciones

Puede editar un grupo de aplicaciones existente para configurar las opciones como el nombre para mostrar, la versión, el publicador, la ruta, la carpeta de inicio, los parámetros y la descripción. No puede cambiar el ID ni el grupo de acceso de un grupo de aplicaciones.

Si necesita comprobar que el servidor de conexión de View inicia la aplicación únicamente en hosts RDS con recursos suficientes para ejecutar la aplicación, consulte [Configurar una regla anti-compatibilidad para un grupo de aplicaciones](#).

### Requisitos previos

Familiarícese con las opciones de un grupo de aplicaciones. Consulte la sección "Crear grupos de aplicaciones" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de aplicaciones**.
- 2 Seleccione un grupo y haga clic en **Editar**.
- 3 Realice los cambios en las opciones del grupo.
- 4 Haga clic en **Aceptar**.

## Eliminar un grupo de aplicaciones

Cuando elimine un grupo de aplicaciones, los usuarios no podrán iniciar nuevas aplicaciones en el grupo.

Puede eliminar un grupo de aplicaciones aunque los usuarios accedan en ese momento a la aplicación. Después de que los usuarios cierren la aplicación, no podrán acceder a ella.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de aplicaciones**.
- 2 Seleccione uno o varios grupos de aplicaciones y haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar** para confirmar.

## Administrar granjas

En Horizon Administrator, puede agregar, editar, eliminar, habilitar y deshabilitar granjas.

Para agregar una granja, consulte "Crear granjas" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para obtener más información sobre grupos de acceso, consulte [Capítulo 6 Configurar la administración delegada basada en funciones](#).

Después de crear una granja, puede agregar o eliminar hosts RDS para permitir más o menos usuarios.

## Editar una granja

Puede realizar cambios en las opciones de configuración en una granja existente.

### Requisitos previos

Familiarícese con las opciones de una granja. Consulte "Crear granjas" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Granjas**.
- 2 Seleccione una granja y haga clic en **Editar**.
- 3 Realice los cambios en las opciones de la granja.
- 4 Haga clic en **Aceptar**.

## Eliminar una granja

Puede eliminar una granja si ya no la necesita o si desea crear una nueva con hosts RDS diferentes. Solo puede eliminar una granja que no esté asociada a un grupo de escritorios RDS o a un grupo de aplicaciones.

### Requisitos previos

Verifique que la granja no esté asociada a ningún grupo de escritorios o de aplicaciones.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Granjas**.
- 2 Seleccione una o varias granjas y haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar** para confirmar.

## Habilitar o deshabilitar una granja

Cuando deshabilita una granja, los usuarios ya no pueden iniciar escritorios RDS o aplicaciones desde los grupos de escritorios RDS y los grupos de escritorios que están asociados a la granja. Los usuarios pueden continuar usando las aplicaciones y los escritorios RDS que estén abiertos en ese momento.

Puede deshabilitar una granja si tiene pensado realizar una operación de mantenimiento en los hosts RDS de la granja o en los grupos de aplicaciones y escritorios RDS que están asociados a la granja. Después de deshabilitar una granja, es posible que algunos usuarios puedan seguir usando aplicaciones o escritorios RDS que abrieron después de deshabilitar la granja.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Granjas**.
- 2 Seleccione una o varias granjas y haga clic en **Más comandos**.
- 3 Haga clic en **Habilitar** o **Deshabilitar**.
- 4 Haga clic en **Aceptar** para confirmar.

El estado de los grupos de aplicaciones y de escritorios RDS que están asociados a la granja tienen el estado No disponible. Puede ver el estado de los grupos seleccionando **Catálogo > Grupos de escritorios** o **Catálogo > Grupos de aplicaciones**.

## Recomponer una granja automática de clones vinculados

Con la operación de recomposición de View Composer, puede actualizar la imagen de la máquina en todos los hosts RDS de una granja automática de clones vinculados. Puede actualizar la configuración del hardware o el software de la máquina virtual principal y ejecutar la operación de recomposición para guardar los cambios propagados a todos los hosts RDS de la granja.

Puede realizar cambios en la máquina virtual principal sin que estos afecten a los host RDS de clones vinculados, ya que los clones están vinculados a una réplica de la principal. La operación de recomposición elimina la réplica antigua y crea una nueva para que se vinculen las clonaciones. La recomposición crea nuevos clones vinculados, que suelen usar menos almacenamiento, ya que los archivos de disco de los clones vinculados suelen aumentar de tamaño con el paso del tiempo.

Puede recomponer una granja automática pero no los hosts RDS individuales de la granja. No puede recomponer clones vinculados en una versión de hardware anterior a la actual.

Si es posible, programe las operaciones de recomposición fuera de las horas punta ya que la operación puede requerir mucho tiempo.

### Requisitos previos

- Compruebe que tenga una snapshot de una máquina virtual principal. Debe especificar una snapshot cuando realice la operación de recomposición. La snapshot puede estar en la máquina virtual principal actual o en una diferente.
- Decida cuándo programar una operación de recomposición. De forma predeterminada, View Composer inicia la operación inmediatamente.

Solo puede programar una operación de recomposición al mismo tiempo en una granja. Puede recomponer varias granjas de forma simultánea.

- Decida si desea cerrar las sesiones de los usuarios de forma forzada cuando comience la operación de recomposición o esperar a que cada uno lo haga antes de recomponer el escritorio del equipo de dicho usuario.

Si obliga a los usuarios a cerrar sesión, Horizon 7 se lo notifica a los usuarios antes de que se desconecten y les permite cerrar las aplicaciones y cerrar sesión.

- Decida si desea detener el aprovisionamiento cuando se produce el primer error. Si selecciona esta opción y se produce un error cuando View Composer aprovisiona un clon vinculado, se detiene el aprovisionamiento. Puede seleccionar esta opción para asegurarse de que recursos como el almacenamiento no se consuman de forma innecesaria.

Si selecciona la opción **Detener en el primer error**, esto no afecta a la personalización. Si se produce un error de personalización en un clon vinculado, se siguen aprovisionando y personalizando otros clones.

- Compruebe que el aprovisionamiento esté habilitado. Cuando el aprovisionamiento esté deshabilitado, Horizon 7 detiene la personalización de las máquinas después de que se recompongan.
- Si la implementación incluye instancias del servidor de conexión, compruebe que todas las instancias tengan instaladas la misma versión.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Granjas**.
- 2 Haga doble clic en el ID del grupo de la granja que desee recomponer.



3 Haga clic en **Recomponer**.

4 (opcional) Haga clic en **Cambiar** para cambiar la máquina virtual principal.

La nueva máquina virtual principal debe ejecutar la misma versión del sistema operativo de la máquina virtual principal.

5 Seleccione una snapshot.

6 (opcional) Haga clic en Detalles de la snapshot para visualizar más información sobre la snapshot.

7 Haga clic en **Siguiente**.

8 (opcional) Programe una hora de inicio.

La hora actual aparece rellena de forma predeterminada.

9 (opcional) Especifique si desea cerrar las sesiones de los usuarios de forma forzada o esperar a que estos cierren sesión.

La opción para obligar que los usuarios cierren sesión está seleccionada de forma predeterminada.

10 (opcional) Especifique si desea detener el aprovisionamiento cuando se produce el primer error.

Esta opción está seleccionada de manera predeterminada.

11 Haga clic en **Siguiente**.

Aparece la página Listo para finalizar.

12 (opcional) Haga clic en **Mostrar detalles** para visualizar más información sobre la operación de recomposición.

13 Haga clic en **Finalizar**.

En vCenter Server, puede supervisar el progreso de recomposición en las máquinas virtuales de clones vinculados.

---

**Nota** Durante la operación de recomposición, View Composer vuelve a ejecutar Sysprep en los clones vinculados. Es posible que se generen nuevos SID y GUID de terceros para las máquinas virtuales recompuestas. Para obtener más información, consulte "Recomponer clones vinculados personalizados con Sysprep" en el documento *Configurar escritorios virtuales en Horizon 7*.

---

## Programar el mantenimiento para una granja automática de clones instantáneos

Con la operación de mantenimiento, puede programar el mantenimiento periódico o inmediato de todos los hosts RDS de una granja automática de clones instantáneos. Durante cada ciclo de mantenimiento, se actualizan todos los hosts RDS de la máquina virtual principal.

Puede realizar cambios en la máquina virtual principal sin que estos afecten a los clones instantáneos del host RDS, debido a que la snapshot de la máquina virtual principal actual se usa para el mantenimiento. Los clones instantáneos creados en la granja automática usan la información de la máquina virtual principal para la configuración del sistema.

Puede programar el mantenimiento en una granja automática pero no en los hosts RDS individuales de la granja.

Si es posible, programe las operaciones de mantenimiento fuera de las horas punta para garantizar que todos los hosts RDS finalicen el mantenimiento y estén disponibles durante las horas de mayor actividad.

### Requisitos previos

- Decida cuándo programar una operación de mantenimiento. De forma predeterminada, el servidor de conexión inicia la operación inmediatamente.

Puede programar un mantenimiento inmediato, un mantenimiento periódico o ambos para una granja. Puede programar operaciones de mantenimiento en varias granjas de forma simultánea.

- Decida si desea cerrar las sesiones de los usuarios de forma forzada cuando comience la operación de mantenimiento o esperar a que cada uno lo haga antes de recomponer el escritorio del equipo de dicho usuario.

Si obliga a los usuarios a cerrar sesión, Horizon 7 se lo notifica a los usuarios antes de que se desconecten y les permite cerrar las aplicaciones y cerrar sesión.

- Decida el tamaño mínimo de la granja. El tamaño mínimo de la granja es el número de hosts RDS que están siempre disponibles para permitir que los usuarios continúen usando la granja. Por ejemplo, si el tamaño de la granja es diez y el tamaño mínimo de la granja es dos, el mantenimiento se realizará en ocho hosts RDS. Los hosts restantes pasarán al modo de mantenimiento a medida que los hosts RDS que están en mantenimiento vuelvan a estar disponibles. Todos los hosts RDS se administran de forma individual, por lo que cuando un host está disponible, se activará el modo de mantenimiento en uno de los hosts restantes.

Sin embargo, si programa el mantenimiento inmediato, se activará el modo de mantenimiento en todos los hosts RDS de la granja.

Todos los hosts RDS también estarán sujetos a la directiva y tendrán que esperar para cerrar las sesiones o para obligar a los usuarios que la cierren según la directiva que esté configurada.

- Decida si desea detener el aprovisionamiento cuando se produce el primer error. Si selecciona esta opción y se produce un error cuando el servidor de conexión aprovisiona un clon instantáneo, se detiene el aprovisionamiento. Puede seleccionar esta opción para asegurarse de que recursos como el almacenamiento no se consuman de forma innecesaria.

Si selecciona la opción **Detener en el primer error**, esto no afecta a la personalización. Si se produce un error de personalización en un clon instantáneo, se siguen aprovisionando y personalizando otros clones.

- Compruebe que el aprovisionamiento esté habilitado. Cuando el aprovisionamiento esté deshabilitado, Horizon 7 detiene la personalización de las máquinas después de que se actualicen.
- Si la implementación incluye instancias del servidor de conexión, compruebe que todas las instancias tengan instaladas la misma versión.

## Procedimiento

- 1 En Horizon Administrator, seleccione **Recursos > Granjas**.
- 2 Haga doble clic en el ID del grupo de la granja para la que desea programar un proceso de mantenimiento.
- 3 Haga clic en **Mantenimiento > Programar**.
- 4 En el asistente **Programar el mantenimiento periódico**, seleccione un modo de mantenimiento.

Opción	Acción
Periódico	<p>Programa el mantenimiento periódico de todos los servidores de los hosts RDS de una granja.</p> <ul style="list-style-type: none"> <li>■ Seleccione la fecha y la hora a partir de las que se aplicará el mantenimiento.</li> <li>■ Seleccione un periodo de mantenimiento. Puede seleccionar periodos diarios, semanales o mensuales.</li> <li>■ Seleccione un intervalo de repetición en días para que se vuelva a realizar la operación de mantenimiento.</li> </ul> <p>Si se programa un mantenimiento inmediato en una granja, la fecha de este pasará a ser la fecha efectiva para todos los mantenimientos periódicos. Si cancela el mantenimiento inmediato, la fecha actual pasa a ser la fecha efectiva para el mantenimiento periódico.</p>
Inmediato	<p>Programa el mantenimiento inmediato de todos los servidores de los hosts RDS de una granja. El mantenimiento inmediato crea una programación única para realizar un mantenimiento inmediato o próximo. Utilice el mantenimiento inmediato para actualizar la granja desde una nueva snapshot o imagen de máquina virtual principal cuando quiera aplicar revisiones de seguridad urgentes.</p> <p>Seleccione una configuración del mantenimiento inmediato.</p> <ul style="list-style-type: none"> <li>■ Seleccione <b>Empezar ahora</b> para iniciar la operación de mantenimiento inmediatamente.</li> <li>■ Seleccione <b>Iniciar a las</b> para comenzar la operación de mantenimiento en la fecha y la hora que especifique. Introduzca la fecha y la hora local del navegador web.</li> </ul> <p><b>Nota</b> El mantenimiento periódico se suspenderá hasta que el mantenimiento inmediato se complete.</p>

- 5 Haga clic en **Siguiente**.
- 6 (opcional) Haga clic en **Cambiar** para cambiar la máquina virtual principal.
- 7 Seleccione una snapshot.
 

No puede seleccionar una snapshot diferente si no desmarca la casilla de verificación **Usar la imagen de la máquina virtual principal actual**.
- 8 (opcional) Haga clic en **Detalles de la snapshot** para visualizar más información sobre la snapshot.
- 9 Haga clic en **Siguiente**.

- 10** (opcional) Especifique si desea cerrar las sesiones de los usuarios de forma forzada o esperar a que estos cierren sesión.

La opción para obligar que los usuarios cierren sesión está seleccionada de forma predeterminada.

- 11** (opcional) Especifique si desea detener el aprovisionamiento cuando se produce el primer error.

Esta opción está seleccionada de manera predeterminada.

- 12** Haga clic en **Siguiente**.

Aparece la página **Listo para finalizar**.

- 13** Haga clic en **Finalizar**.

## Administrar los hosts RDS

Puede administrar los hosts RDS que configuró manualmente y los hosts RDS que se crean automáticamente cuando agrega una granja automática.

Cuando configura de forma manual un host RDS, este se registra automáticamente con el servidor de conexión de Horizon. No puede registrar de forma manual un host RDS con el servidor de conexión. Consulte "Configurar hosts de sesiones de escritorios remotos" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*. En un host que configuró de forma manual, puede realizar las siguientes tareas de administración:

- Editar el host RDS.
- Agregar el host RDS a una granja manual.
- Eliminar el host RDS de una granja.
- Habilitar el host RDS.
- Deshabilitar el host RDS.

En un host RDS que se creó automáticamente al agregar una granja automática, puede realizar las siguientes tareas de administración:

- Eliminar el host RDS de una granja.
- Habilitar el host RDS.
- Deshabilitar el host RDS.

## Editar un host RDS

Puede cambiar el número de conexiones que pueda admitir un host RDS. Esta opción es la única que puede cambiar. El valor predeterminado es 150. Puede configurarlo con un número positivo o de forma ilimitada.

Solo puede editar los hosts RDS configurados de forma manual, no los que están en una granja automática.

**Procedimiento**

- 1 En View Administrator, seleccione **Configuración de View > Máquinas registradas**.
- 2 Seleccione un host RDS y haga clic en **Editar**.
- 3 Especifique un valor para la configuración **Número de conexiones**.
- 4 Haga clic en **Aceptar**.

## Agregar un host RDS a una granja manual

Puede agregar un host RDS que configuró de forma manual a una granja manual para aumentar la escala de la granja o por otras razones. Solo puede agregar hosts RDS a una granja manual.

**Procedimiento**

- 1 En View Administrator, seleccione **Recursos > Granjas**.
- 2 Haga doble clic en el ID del grupo de la granja.
- 3 Seleccione la pestaña **Hosts RDS**.
- 4 Seleccione uno o varios hosts RDS.
- 5 Haga clic en **Aceptar**.

## Eliminar un host RDS de una granja

Puede eliminar un host RDS de una granja manual para reducir la escala de esta última, realizar trabajos de mantenimiento en el host RDS o por otros motivos. Como práctica recomendada, deshabilite el host RDS y asegúrese de que los usuarios cerraron las sesiones activas antes de eliminar el host de la granja.

Si los usuarios tienen sesiones de escritorios o aplicaciones en los hosts que desea eliminar, las sesiones se mantendrán activas, pero View no podrá realizar un seguimiento de ellas. El usuario que desconecte la sesión no podrá volver a conectarla y se perderán todos los datos no guardados.

También puede eliminar un host RDS de una granja automatizada. Una posible causa sería que el host RDS estuviera en un estado de error irrecuperable. View Composer crea de forma automática un host RDS nuevo para sustituir el que se eliminó.

**Procedimiento**

- 1 En View Administrator, seleccione **Recursos > Granjas**.
- 2 Haga doble clic en el ID del grupo.
- 3 Seleccione la pestaña **Hosts RDS**.
- 4 Seleccione uno o varios hosts RDS.
- 5 Haga clic en **Eliminar de la granja**.
- 6 Haga clic en **Aceptar**.

## Eliminar un host RDS de Horizon 7

Puede eliminar de Horizon 7 un host RDS que configuró de forma manual y que no seguirá utilizando. El host RDS no puede estar en una granja manual.

### Requisitos previos

Compruebe que el host RDS no pertenezca a una granja.

### Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Máquinas registradas**.
- 2 Seleccione un host RDS y haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar**.

Después de eliminar un host RDS, debe volver a instalar Horizon Agent para usarlo de nuevo. Consulte "Configurar hosts de sesiones de escritorios remotos" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

## Deshabilitar o habilitar un host RDS

Cuando deshabilite un host RDS, View ya no podrá seguir usándolo para alojar nuevas aplicaciones o escritorios RDS. Los usuarios pueden continuar usando las aplicaciones y los escritorios RDS que estén abiertos en ese momento.

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Granjas**.
- 2 Haga doble clic en el ID del grupo de una granja.
- 3 Seleccione la pestaña **Hosts RDS**.
- 4 Seleccione un host RDS y haga clic en **Más comandos**.
- 5 Haga clic en **Habilitar** o **Deshabilitar**.
- 6 Haga clic en **Aceptar**.

Si habilita el host RDS, una marca de verificación aparece en la columna **Habilitado** y en la columna **Estado** aparece **Disponible**. Si deshabilita el host RDS, la columna **Habilitado** está vacía y aparece **Deshabilitado** en la columna **Estado**.

## Supervisar los hosts RDS

Puede supervisar el estado y ver las propiedades de los hosts RDS en View Administrator.

## Procedimiento

- ◆ En View Administrator, diríjase a la página que muestra las propiedades que desee ver.

Propiedades	Acción
Host RDS, Granja, Grupo de escritorios, Versión del agente, Sesiones, Estado	<ul style="list-style-type: none"> <li>■ En View Administrator, seleccione <b>Recursos &gt; Máquinas</b>.</li> <li>■ Haga clic en la pestaña <b>Host RDS</b>. Aparecen los hosts RDS de clones vinculados y los hosts RDS que se configuran de forma manual.</li> </ul>
Nombre DNS, Tipo, Granja RDS, Número máximo de conexiones, Versión del agente, Habilitado, Estado	<ul style="list-style-type: none"> <li>■ En View Administrator, seleccione <b>Configuración de View &gt; Máquinas registradas</b>.</li> <li>■ Haga clic en la pestaña <b>Host RDS</b>. Solo aparecen los hosts RDS que se configuran manualmente.</li> </ul>

Se muestran las propiedades y tienen los siguientes significados:

Propiedad	Descripción
Host RDS	Nombre del host RDS.
Granja	Granja a la que pertenece el host RDS.
Grupo de escritorios	Grupo de escritorios RDS asociados a la granja.
Versión del agente	Versión de View Agent o Horizon Agent que se ejecuta en el host RDS.
Sesiones	Número de sesiones cliente.
Nombre DNS	Nombre DNS del host RDS.
Tipo	Versión de Windows Server que se ejecuta en el host RDS.
Granja de RDS	Granja a la que pertenece el host RDS.
Número máximo de conexiones	Número máximo de conexiones que el host RDS puede admitir.
Habilitado	Si el host RDS está habilitado.
Estado	Estado del host RDS. Consulte <a href="#">Estado de los hosts RDS</a> para obtener una descripción de los estados posibles.

## Estado de los hosts RDS

Un host RDS puede tener varios estados desde el momento en el que se inicia. Como práctica recomendada, compruebe que los hosts RDS estén en el estado en el que deben estar antes y después de realizar tareas u operaciones en ellos.

**Tabla 11-1. Estado de un host RDS**

Estado	Descripción
Inicio	View Agent o Horizon Agent se iniciaron en el host RDS, pero aún se están iniciando otros servicios requeridos, como el protocolo de visualización. El periodo de inicio del agente también permite que se inicien otros procesos como los servicios de protocolo.
Deshabilitación en curso	El host RDS está en proceso de deshabilitarse mientras las sesiones aún se ejecutan en el host. Cuando la sesión acaba, el estado cambia a Deshabilitado.
Deshabilitado	Se completó el proceso para deshabilitar el host RDS.

Estado	Descripción
Validando	Se produce después de que el servidor de conexión de View reconozca por primera vez el host RDS, normalmente después de que el servidor de conexión de View se inicie o se reinicie y tras la primera comunicación correcta con View Agent o Horizon Agent en el host RDS. Normalmente, este estado es transitorio. Este estado no es el mismo que el estado Agente inaccesible, que indica un problema de comunicación.
Agente deshabilitado	Ocorre si el servidor de conexión de View deshabilita View Agent o Horizon Agent. Este estado garantiza que una nueva sesión de escritorios o de aplicaciones no se pueda iniciar en el host RDS.
Agente inaccesible	El servidor de conexión de View no puede establecer la comunicación con View Agent ni Horizon Agent en un host RDS.
IP no válida	La opción del registro de máscara de subred se configura en el host RDS y ningún adaptador de red activo tiene una dirección IP dentro del rango configurado.
El agente necesita reiniciarse	El componente de View se actualizó y el host RDS se debe reiniciar para permitir que View Agent o Horizon Agent funcionen con el componente actualizado.
Error de protocolo	El protocolo de visualización RDP no se ejecuta correctamente. Si RDP no se ejecuta y PCoIP sí, los clientes no se pueden conectar con RDP ni PCoIP. Sin embargo, si RDP se está ejecutando y PCoIP no, los clientes se pueden conectar mediante RDP.
Error de dominio	Se produjo un problema en el host RDS al alcanzar el dominio. No se pudo acceder al servidor de dominio o se produjo un error en la autenticación del dominio.
Error de configuración	La función RDS no está habilitada en el servidor.
Desconocido	El host RDS se encuentra en un estado desconocido.
Disponible	El host RDS está disponible. Si el host está en una granja y la granja está asociada a un RDS o un grupo de aplicaciones, se usará para enviar aplicaciones o escritorios RDS a los usuarios.
Aprovisionamiento	(Solo para hosts RDS de clonación vinculada) El aprovisionamiento de la máquina virtual está en curso.
Personalizando	(Solo para hosts RDS de clonación vinculada) La personalización de la máquina virtual está en curso.
Eliminar	(Solo para hosts RDS de clonación vinculada) La eliminación de la máquina virtual está en curso.
Esperando al agente	(Solo para hosts RDS de clonación vinculada) El servidor de conexión de View está esperando para establecer la comunicación con View Agent o Horizon Agent.
Modo de mantenimiento	(Solo para hosts RDS de clonación vinculada) La máquina virtual está en modo de mantenimiento y no está disponible para los usuarios.
Aprovisionada	(Solo para hosts RDS de clonación vinculada) Se completó el aprovisionamiento de la máquina virtual.
Error de aprovisionamiento	(Solo para hosts RDS de clonación vinculada) Se produjo un error durante el aprovisionamiento.
Error	(Solo para hosts RDS de clonación vinculada) Se produjo un error desconocido en la máquina virtual.

## Configurar el límite de Adobe Flash con Internet Explorer en escritorios RDS

Para asegurarse de que el límite de Adobe Flash funcione con Internet Explorer en escritorios RDS, los usuarios deben habilitar las extensiones de navegador de terceros.



## Procedimiento

- 1 Inicie Horizon Client e inicie sesión en un escritorio remoto de usuario.
- 2 En Internet Explorer, haga clic en **Herramientas > Opciones de Internet**.
- 3 Haga clic en la pestaña **Opciones avanzadas**, seleccione **Habilitar extensiones de explorador de terceros** y haga clic en **Aceptar**.
- 4 Reinicie Internet Explorer.

## Configurar el equilibrio de carga de los hosts RDS

De forma predeterminada, el servidor de conexión de View usa el límite y el recuento de la sesión actual para equilibrar la ubicación de las nuevas sesiones de aplicaciones en hosts RDS. Puede sobrescribir este comportamiento predeterminado y controlar la ubicación de las nuevas sesiones de aplicaciones escribiendo y configurando los scripts de equilibrio de carga.

Un script de equilibrio de carga devuelve un valor de carga. El valor de carga puede basarse en cualquier métrica del host, como la utilización de la CPU o de la memoria. Horizon Agent asigna el valor de carga a una preferencia de carga e informa al servidor de conexión de View sobre esta preferencia. El servidor de conexión de View usa estas preferencias de carga para determinar dónde ubicar las nuevas sesiones de aplicaciones.

Puede escribir sus propios scripts de equilibrio de carga o puede usar uno de los scripts de equilibrio de carga de ejemplo proporcionados con Horizon Agent.

La configuración de los scripts de equilibrio de carga incluye habilitar el servicio del host de scripts de VMware Horizon View y configurar una clave de registro en cada host RDS de una granja.

## Preferencias de carga asignada y valores de carga

Horizon Agent asigna a una preferencia de carga el valor de carga que un script de equilibrio de carga devuelve. El servidor de conexión de View usa estas preferencias de carga para determinar dónde ubicar las nuevas sesiones de aplicaciones.

La siguiente tabla muestra los valores de carga válidos que un script de equilibrio de carga puede devolver y describe las preferencias de carga asociadas.

**Tabla 11-2. Preferencias de carga asignada y valores de carga válidos**

Valor de carga válido	Preferencia de carga notificada por Horizon Agent	Descripción
0	BLOQUE	No seleccione este host RDS.
1	BAJA	Preferencia baja/carga alta.
2	MED	Preferencia media/carga normal.
3	ALTA	Preferencia alta/carga baja.

## Límites de la función de equilibrio de carga

La función de equilibrio de carga del host RDS tiene algunos límites.

- Las reglas antiafinidad pueden evitar que una aplicación se ubique en un host RDS, sin tener en cuenta la preferencia de carga notificada. Si desea obtener más información, consulte [Configurar una regla anti-compatibilidad para un grupo de aplicaciones](#).
- El equilibrio de carga solo afecta a las nuevas sesiones de aplicaciones. Un host RDS con sesiones en las que un usuario ejecutó previamente una aplicación siempre se vuelve a usar para la misma aplicación. Este comportamiento sobrescribe las preferencias de carga notificadas y las reglas anticompatibilidad.
- Las aplicaciones se inician en un host RDS en el que un usuario ya tiene una sesión, aunque el host RDS notifique una preferencia de carga BLOQUE.
- Los límites de la sesión RDS evitan que se creen las sesiones de aplicaciones, independientemente de la preferencia de carga notificada.

## Escribir un script de equilibrio de carga para un host RDS

Puede escribir un script de equilibrio de carga para generar un valor de carga basado en cualquier métrica del host RDS que desee usar para equilibrar la carga. También puede escribir un script de equilibrio de carga simple que devuelva un valor de carga fija.

El script de equilibrio de carga debe devolver un número único que se encuentre en el intervalo de 0 a 3. Para obtener descripciones de los valores de carga válidos, consulte [Preferencias de carga asignada y valores de carga](#).

Si al menos un host RDS de la granja devuelve un valor de carga válido, el servidor de conexión de View asume un valor de carga de 2 (se asignó la preferencia de carga MED) para el resto de hosts RDS de la granja hasta que los scripts de equilibrio de carga devuelvan valores válidos. Si ningún host RDS de la granja devuelve un valor de carga válido, la función de equilibrio de carga está deshabilitada para la granja.

Si el script de equilibrio de carga devuelve un valor de carga que no es válido o si no termina de ejecutarse en 10 segundos, Horizon Agent establece la preferencia de carga a BLOQUE y el host RDS tiene un estado de error de configuración. Estos valores eliminan efectivamente el host RDS de la lista de hosts RDS disponibles para nuevas sesiones.

Copie el script de equilibrio de carga en el directorio Horizon Agentscripts (C:\Program Files\VMware\VMware View\Agent\scripts) de cada host RDS de la granja. Debe copiar el mismo script en cada host RDS de cada granja.

Para obtener un ejemplo sobre cómo escribir un script de equilibrio de carga, consulte los scripts de ejemplo del directorio Horizon Agentscripts. Si desea obtener más información, consulte [Scripts de equilibrio de carga de muestra de los hosts RDS](#).

## Scripts de equilibrio de carga de muestra de los hosts RDS

Cuando instale Horizon Agent en un host RDS, el instalador ubica scripts de equilibrio de carga de muestra en el directorio Horizon Agentscripts (C:\Program Files\VMware\VMware View\Agent\scripts).

**Tabla 11-3. Scripts de equilibrio de carga de muestra**

Nombre	Descripción
cpuutilisation.vbs	<p>Lee el porcentaje de CPU del registro que se utilizó y devuelve los siguientes valores de carga:</p> <ul style="list-style-type: none"> <li>■ 0, si el uso de la CPU es superior al 90 por ciento</li> <li>■ 1, si el uso de la CPU es superior al 75 por ciento</li> <li>■ 2, si el uso de la CPU es superior al 25 por ciento</li> <li>■ 3, si el uso de la CPU es menor o igual al 25 por ciento</li> </ul>
memoryutilisation.vbs	<p>Calcula el porcentaje de memoria que se utilizó y devuelve los siguientes valores de carga:</p> <ul style="list-style-type: none"> <li>■ 0, si el uso de la memoria es superior al 90 por ciento</li> <li>■ 1, si el uso de la memoria es superior al 75 por ciento</li> <li>■ 2, si el uso de la memoria es superior al 25 por ciento</li> <li>■ 3, si el uso de la memoria es menor o igual al 25 por ciento</li> </ul>

**Nota** Como el script `cpuutilisation.vbs` utiliza datos medios graduales que se muestrean cada cinco minutos, los eventos de uso elevado pero de corta duración no se reflejan en las preferencias de carga notificadas. Puede reducir el periodo de muestra a un mínimo de dos minutos, pero es posible que el rendimiento del host RDS se vea afectado. El intervalo de muestreo se controla a través de la entrada del registro `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Performance Stats\SamplingIntervalSeconds`. El valor predeterminado es 300 segundos.

## Habilitar el servicio de VMware Horizon View Script Host en un host RDS

Debe habilitar el servicio de VMware Horizon View Script Host en un host RDS antes de configurar un script de equilibrio de carga. El servicio de VMware Horizon View Script Host está deshabilitado de forma predeterminada.

### Procedimiento

- 1 Inicie sesión en el host RDS como administrador.
- 2 Inicie el administrador de servidores.
- 3 Seleccione **Herramientas > Servicios** y diríjase al servicio de VMware Horizon View Script Host.
- 4 Haga clic con el botón secundario en **VMware Horizon View Script Host** y seleccione **Propiedades**.
- 5 En el cuadro de diálogo Propiedades, seleccione **Automático** en el menú desplegable **Tipo de inicio** y haga clic en **Aceptar** para guardar los cambios.

- 6 Haga clic con el botón secundario en **VMware Horizon View Script Host** y seleccione **Iniciar** para iniciar el servicio de VMware Horizon View Script Host.

El servicio de VMware Horizon View Script Host se reinicia automáticamente cada vez que se inicia es host RDS.

### Pasos siguientes

Configure el script del equilibrio de carga en cada host RDS de la granja. Consulte [Configurar un script de equilibrio de carga en un host RDS](#).

## Configurar un script de equilibrio de carga en un host RDS

Debe configurar el mismo script de equilibrio de carga en cada host RDS de la granja. La configuración de un script de equilibrio de carga supone establecer una clave de registro en el host RDS.

Si utiliza una granja automática, realice este procedimiento en la máquina virtual principal de la granja automática.

---

**Importante** Debe configurar el script del equilibrio de carga en todos los hosts RDS de una granja o en ninguno de ellos. Si configura un script de equilibrio de carga solo en algunos hosts RDS de una granja, View Administrator establece el estado de la granja como amarillo.

---

### Requisitos previos

- Escriba un script de equilibrio de carga y cópielo en el directorio Horizon Agentscripts de cada host RDS de la granja. Consulte [Escribir un script de equilibrio de carga para un host RDS](#).
- Habilite el servicio del host del script de VMware Horizon View en el host RDS. Consulte [Habilitar el servicio de VMware Horizon View Script Host en un host RDS](#)

### Procedimiento

- 1 Inicie sesión en el host RDS como administrador.
- 2 Inicie el administrador de servidores.
- 3 Seleccione **Herramientas > Configuración del sistema**, haga clic en la pestaña **Herramientas** e inicie el Editor del Registro.
- 4 En el registro, diríjase a `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.
- 5 En el área de navegación, seleccione la clave **RdshLoad**.  
  
Los valores de la clave **RdshLoad**, si existen, aparecen en el área de temas (panel de la derecha).
- 6 Haga clic en el área de temas de la clave **RdshLoad**, seleccione **Nuevo > Valor de cadena** y cree un nuevo valor de cadena.

Como práctica recomendada, use el nombre que representa al script de equilibrio de carga que se debe ejecutar, por ejemplo **cpuutilisationScript** para el script `cpuutilisation.vbs`.

- 7 Haga clic con el botón secundario en la entrada del nuevo valor de cadena que creó y seleccione **Modificar**.
- 8 En el cuadro de texto **Datos de valor**, escriba la línea de comandos que invoca al script de equilibrio de carga y haga clic en **Aceptar**.

Escriba la ruta completa del script de equilibrio de carga.

Por ejemplo: `cscript.exe "C:\Program Files\VMware\VMware View Agent\scripts\cpuutilisation.vbs"`

- 9 Reinicie el servicio de Horizon Agent en el host RDS para que se apliquen los cambios.

El script de equilibrio de carga comienza a ejecutarse en el host RDS.

### Pasos siguientes

Repita este procedimiento en cada host RDS de la granja. Si realizó este procedimiento en la máquina virtual principal para una granja automática, aprovisiona esta granja.

Para verificar que el script de equilibrio de carga funciona correctamente, consulte [Verificar un script de equilibrio de carga](#).

## Verificar un script de equilibrio de carga

Puede verificar que el script del equilibrio de carga funcione correctamente al revisar la información del host RDS y de la granja RDS en View Administrator.

### Procedimiento

- 1 En View Administrator, haga clic en **Panel** y expanda **Granjas RDS** del panel Estado del sistema.
- 2 Compruebe el estado de la granja que contiene los hosts RDS.

El estado de la granja debe aparecer en verde. Si un script de equilibrio de carga solo está configurado en algunos hosts RDS de una granja, View Administrator establece el estado de la granja en amarillo. Debe configurar el script del equilibrio de carga en todos los hosts RDS de una granja o en ninguno de ellos.

- 3 Expanda la granja y haga clic en el nombre de cada host RDS para ver su preferencia de equilibrio.

El campo Cargar al servidor del cuadro de diálogo Detalles muestra la preferencia de carga sobre la que informa Horizon Agent, por ejemplo Carga ligera, se aceptan nuevas sesiones. Si Horizon Agent no informó sobre una preferencia de carga, el campo Cargar al servidor muestra Carga no comunicada.

### Pasos siguientes

Si el equilibrio de carga no funciona como debería, compruebe el contenido del script del equilibrio de carga. Si se escribió el script correctamente, compruebe que el servicio de VMware Horizon View Script Host se esté ejecutando correctamente y que el mismo script de equilibrio de carga esté configurado en cada host RDS de la granja.

## Ejemplos de ubicación de sesiones de equilibrio de carga

Estos ejemplos muestran dos escenarios de ubicación de sesiones del equilibrio de carga.

### Ejemplo 1: no existe ninguna sesión de usuario

Este ejemplo muestra cómo se puede ubicar una sesión de una granja que contenga seis hosts RDS cuando ninguna sesión de usuario existe en ese momento en ningún host RDS.

- 1 Horizon Agent muestra las siguientes preferencias de carga para cada host RDS de la granja.

Host RDS	Preferencia de carga
1	ALTA
2	BAJA
3	ALTA
4	MED
5	BLOQUE
6	BAJA

- 2 View ordena los hosts RDS en tres depósitos según la preferencia de carga. View descarga el host RDS 5 porque Horizon Agent notificó una preferencia de carga BLOQUE.

Depósito	Preferencia de carga	Host RDS
1	ALTA	1
	ALTA	3
2	MED	4
3	BAJA	2
	BAJA	6

- 3 Como el depósito 2 solo tiene un host RDS, View combina el depósito 2 y el 3

Depósito	Preferencia de carga	Host RDS
1	ALTA	1
	ALTA	3
	MED	4
2	BAJA	2
	BAJA	6

- 4 View aleatoriza el orden de los depósitos.

Depósito	Preferencia de carga	Host RDS
1	MED	4
	ALTA	3
	MED	1
2	BAJA	6
	BAJA	2

- El servidor de conexión de View intenta ubicar una nueva sesión de aplicaciones en el host RDS 4 primero, seguido del host RDS 3 y así sucesivamente.

Orden de ubicación de las sesiones del host RDS
4
3
1
6
2

**Nota** Las reglas antiafinidad pueden evitar que una aplicación se ubique en un host RDS, sin tener en cuenta la preferencia de carga notificada. Si desea obtener más información, consulte [Configurar una regla anti-compatibilidad para un grupo de aplicaciones](#).

## Ejemplo 2: existe una sesión de usuario

Este ejemplo muestra cómo se puede ubicar una sesión de una granja que contenga seis hosts RDS cuando una sesión de usuario existe en ese momento en uno de los hosts RDS. Un host RDS que contenga una sesión en la que un usuario ejecutó una aplicación se reutiliza siempre para la misma aplicación.

- Una sesión de usuario ya existe en el host RDS 3. El host RDS 3 tiene una preferencia de carga MED. El RDS restante en los hosts de la granja (la lista de reserva) tiene las siguientes preferencias de carga.

Host RDS	Preferencia de carga
1	MED
2	BAJA
4	ALTA
5	BAJA
6	BLOQUE

- View ordena los hosts RDS de la lista de reserva en dos depósitos según la preferencia de carga. View descarga el host RDS 6 porque Horizon Agent notificó una preferencia de carga notificada BLOQUE.

Depósito	Preferencia de carga	Host RDS
1	ALTA	4
	MED	1
2	BAJA	2
	BAJA	5

- 3 View aleatoriza el orden de los depósitos.

Depósito	Preferencia de carga	Host RDS
1	ALTA	4
	MED	1
2	BAJA	5
	BAJA	2

- 4 View agrega el host RDS que contiene la sesión existente en la parte superior de la nueva lista ordenada de depósitos.

Orden de ubicación de las sesiones del host RDS
3
4
1
5
2

## Configurar una regla anti-compatibilidad para un grupo de aplicaciones

Si configura una regla anti-compatibilidad para un grupo de aplicaciones, el servidor de conexión de Horizon intenta iniciar la aplicación solo en hosts RDS que tengan suficientes recursos para ejecutar la aplicación. Esta función puede ser útil para controlar aplicaciones que consuman una gran cantidad de CPU o recursos de memoria.

Una regla anti-compatibilidad consta de un patrón de correspondencia de aplicación y un recuento máximo. Por ejemplo, el patrón de correspondencia de aplicación podría ser `autocad.exe` y el recuento máximo 2.

El servidor de conexión envía la regla anti-compatibilidad a Horizon Agent en un host RDS. Si una aplicación que se esté ejecutando en el host RDS incluye nombres de procesos que coinciden con el patrón de correspondencia de aplicación, Horizon Agent realiza en ese momento el recuento de instancias de las aplicaciones y compara el número con el máximo. Si se supera el recuento máximo, el servidor de conexión omitirá ese host RDS al seleccionar un host RDS donde ejecutar nuevas sesiones de la aplicación.

### Requisitos previos

- Cree el grupo de aplicaciones. Consulte la sección "Crear grupos de aplicaciones" en el documento de *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Familiarícese con las restricciones de la función anti-compatibilidad. Consulte [Restricciones de la función Anticompatibilidad](#).



## Procedimiento

- 1 En Horizon Administrator, seleccione **Catálogo > Grupos de aplicaciones**.
- 2 Seleccione el grupo que desea modificar y haga clic en **Editar**.
- 3 En el cuadro de texto **Patrones de anti-afinidad**, escriba una lista de patrones separados por comas que coincidan con los nombres de procesos de otras aplicaciones ejecutándose en hosts RDS.

Las cadenas de patrones pueden incluir los caracteres comodín '\*', que significa cero o más caracteres, o '?', que significa cualquier carácter.

Por ejemplo, **\*pad.exe,\*notepad.???** coincidiría con wordpad.exe, notepad.exe y notepad.bat, pero no lo haría con wordpad.bat o notepad.script.

---

**Nota** Horizon 7 cuenta varios patrones que coinciden con una aplicación en una sola sesión como una única correspondencia.

---

- 4 En el cuadro de texto **Recuento anti-afinidad**, escriba el número máximo del resto de aplicaciones que puedan ejecutarse en el host RDS antes de que nuevas sesiones de aplicaciones lo rechacen.  
El recuento máximo puede ser un entero entre 1 y 20.
- 5 Haga clic en **Aceptar** para guardar los cambios.

## Restricciones de la función Anticompatibilidad

La función Anticompatibilidad tiene algunas restricciones.

- Las reglas anticompatibilidad únicamente afectan a las nuevas sesiones de aplicaciones. Un host RDS con sesiones en las que un usuario ejecutó previamente una aplicación siempre se vuelve a usar para la misma aplicación. Este comportamiento sobrescribe las preferencias de carga notificadas y las reglas anticompatibilidad.
- Las reglas anticompatibilidad no afectan a la aplicación que se inicia desde dentro de una sesión de escritorio RDS.
- Los límites de la sesión RDS evitan que se creen las sesiones de aplicaciones, independientemente de las reglas anticompatibilidad.
- En algunas circunstancias, es posible que las instancias de las aplicaciones del host RDS no se restrinjan al número máximo especificado. Por ejemplo, View no puede determinar el número exacto de la instancia si otras aplicaciones de sesiones pendientes están en proceso de iniciarse.
- No se admiten las reglas anticompatibilidad entre aplicaciones. Por ejemplo, las aplicaciones de gran tamaño, como las instancias de Visual Studio y Autocad, no se pueden contar en una única regla.
- No use las reglas anticompatibilidad en entornos donde los usuarios finales utilizan Horizon Client en clientes móviles. Las reglas anticompatibilidad pueden suponer varias sesiones de un usuario final en la misma granja. La reconexión de varias sesiones en clientes móviles pueden suponer un comportamiento indeterminado.

# Administrar las aplicaciones ThinApp en View Administrator

# 12

Puede usar View Administrator para distribuir y administrar las aplicaciones empaquetadas con VMware ThinApp. La administración de aplicaciones ThinApp en View Administrator incluye tareas como capturar y almacenar paquetes de aplicaciones, agregar las aplicaciones ThinApp a View Administrator y asignar las aplicaciones ThinApp a grupos de escritorios y equipos.

Debe tener una licencia para usar la función de administración ThinApp en View Administrator.

---

**Importante** Si, en lugar de distribuir las ThinApps asignándolas a grupos de escritorios y a equipos, prefiere asignar las ThinApps a los usuarios y grupos de Active Directory, puede usar VMware Identity Manager.

---

Este capítulo incluye los siguientes temas:

- [Requisitos de View para las aplicaciones ThinApp](#)
- [Capturar y almacenar paquetes de aplicaciones](#)
- [Asignar aplicaciones ThinApp a grupos de escritorios y máquinas](#)
- [Mantener las aplicaciones ThinApp en View Administrator](#)
- [Supervisar y solucionar problemas de las aplicaciones ThinApp en View Administrator](#)
- [Ejemplo de configuración ThinApp](#)

## Requisitos de View para las aplicaciones ThinApp

Cuando se capturen y se almacenen las aplicaciones ThinApp que se transmitirán a los escritorios remotos en View Administrator, debe cumplir ciertos requisitos.

- Debe empaquetar las aplicaciones en paquetes de Microsoft Installation (MSI).
- Debe usar la versión 4.6 de ThinApp o una versión posterior para crear o volver a empaquetar los paquetes MSI.
- Debe almacenar los paquetes MSI en un recurso compartido de red Windows que se encuentre en un dominio de Active Directory al que pueda acceder el host del servidor de conexión de View y los escritorios remotos. El servidor del archivo debe admitir los permisos de archivo y de autenticación que se basan en cuentas de equipos.

- Debe configurar el archivo y los permisos de uso compartido en el recurso compartido de red que aloja los paquetes MSI para proporcionarle Acceso de lectura en el grupo integrado Equipos del dominio de Active Directory. Si tiene pensado distribuir las aplicaciones ThinApp a los controladores de dominio, también debe proporcionarle Acceso de lectura al grupo integrado Controladores de dominio de Active Directory.
- Para permitir que los usuarios accedan a las transmisiones de paquetes de aplicaciones ThinApp, debe establecer el permiso NTFS en el recurso compartido de red que aloja los paquetes ThinApp como Lectura y ejecución para los usuarios.
- Asegúrese de que un espacio de nombres independiente no evite que los equipos que pertenecen al dominio accedan al recurso compartido de red que aloja los paquetes MSI. Un espacio de nombres independiente se produce cuando un nombre de dominio de Active Directory es diferente al espacio de nombres DNS que usan los equipos en dicho dominio. Consulte el artículo 1023309 de la base de conocimientos (KB) de VMware para obtener más información.
- Para ejecutar aplicaciones ThinApp transmitidas en los escritorios remotos, los usuarios deben tener acceso al recurso compartido de red que aloja los paquetes MSI.

## Capturar y almacenar paquetes de aplicaciones

ThinApp ofrece virtualización de aplicaciones mediante el desacoplamiento de una aplicación desde el sistema operativo subyacente y sus bibliotecas y entorno, y el agrupamiento de la aplicación en un único archivo ejecutable denominado paquete de la aplicación.

Para administrar las aplicaciones ThinApp en View Administrator, debe usar el asistente para **Configurar la captura** de ThinApp a fin de capturar y empaquetar sus aplicaciones en formato MSI y almacenar los paquetes MSI en un repositorio de aplicaciones.

El repositorio de una aplicación es un recurso compartido en red de Windows. Use View Administrator para registrar el recurso compartido como un repositorio de la aplicación. Puede registrar varios repositorios de aplicaciones.

---

**Nota** Si posee varios repositorios de aplicaciones, puede usar soluciones de terceros para administrar el equilibrio de carga y la disponibilidad. View no incluye el equilibrio de carga o las soluciones de disponibilidad.

---

Consulte la *Introducción a VMware ThinApp* y la *Guía de usuario de ThinApp* para obtener información completa de las funciones ThinApp y sobre cómo utilizar el asistente para **Configurar la captura** de ThinApp.

### Procedimiento

#### 1 [Empaquetar aplicaciones](#)

El asistente de ThinApp **Configurar la captura** permite capturar y empaquetar aplicaciones.

## 2 Crear un recurso compartido de red de Windows

Debe crear un recurso compartido en red de Windows para alojar los paquetes MSI distribuidos a los grupos y los escritorios remotos de View Administrator.

## 3 Registrar un repositorio de aplicaciones

Debe registrar un recurso compartido de red de Windows que aloje los paquetes MSI como un repositorio de aplicaciones en View Administrator.

## 4 Agregar aplicaciones ThinApp a View Administrator

Para agregar aplicaciones ThinApp a View Administrator, examine el repositorio de aplicaciones y seleccione las aplicaciones ThinApp. Después de agregar una aplicación ThinApp a View Administrator, puede asignarla a los equipos o a los grupos de escritorios.

## 5 Crear una plantilla ThinApp

Puede crear una plantilla en View Administrator para especificar un grupo de aplicaciones ThinApp. Puede usar plantillas para agrupar aplicaciones por función, proveedor o cualquier otra agrupación lógica que sea efectiva para su organización.

# Empaquetar aplicaciones

El asistente de ThinApp **Configurar la captura** permite capturar y empaquetar aplicaciones.

### Requisitos previos

- Descargue el software de ThinApp en <http://www.vmware.com/products/thinapp> e instálelo en un equipo limpio. View es compatible con ThinApp 4.6 y versiones posteriores.
- Familiarícese con los requisitos del software de ThinApp y las instrucciones para empaquetar aplicaciones de la *Guía de usuario de ThinApp*.

### Procedimiento

- 1 Inicie el asistente de ThinApp **Configurar la captura** y siga las instrucciones que se indican.
- 2 Cuando el asistente de ThinApp **Configurar la captura** le solicite una ubicación de proyecto, seleccione **Compilar paquete MSI**.
- 3 Si quiere enviar la aplicación a escritorios remotos, asigne el valor 1 a la propiedad MSISstreaming en el archivo `package.ini`.

```
MSISstreaming=1
```

El asistente de ThinApp **Configurar la captura** encapsula la aplicación y todos los componentes necesarios para ejecutarla en un paquete MSI.

### Pasos siguientes

Cree un recurso compartido de red de Windows para almacenar los paquetes MSI.

## Crear un recurso compartido de red de Windows

Debe crear un recurso compartido en red de Windows para alojar los paquetes MSI distribuidos a los grupos y los escritorios remotos de View Administrator.

### Requisitos previos

- Use el asistente de ThinApp **Configurar la captura** para empaquetar las aplicaciones.
- Compruebe que el recurso compartido de red cumpla los requisitos de View para almacenar las aplicaciones ThinApp. Consulte [Requisitos de View para las aplicaciones ThinApp](#) para obtener más información.

### Procedimiento

- 1 Cree una carpeta compartida en un equipo de un dominio de Active Directory a la que pueda acceder desde el host del servidor de conexión de View y los escritorios remotos.
- 2 Configure el archivo y los permisos de uso compartido de la carpeta compartida para proporcionar Acceso de lectura al grupo de Active Directory integrado Equipos del dominio.
- 3 Si tiene pensado asignar aplicaciones ThinApp a controladores de dominio, proporcione Acceso de lectura en el grupo de Active Directory integrado Equipo de dominio.
- 4 Si tiene pensado usar paquetes de aplicaciones ThinApp secuenciales, configure el permiso NTF en el recurso compartido de red que aloja los paquetes ThinApp como Leer y ejecutar para los usuarios.
- 5 Copie los paquetes MSI en la carpeta compartida.

### Pasos siguientes

Registre el recurso compartido de red de Windows como un repositorio de aplicaciones en View Administrator.

## Registrar un repositorio de aplicaciones

Debe registrar un recurso compartido de red de Windows que aloje los paquetes MSI como un repositorio de aplicaciones en View Administrator.

Puede registrar varios repositorios de aplicaciones.

### Requisitos previos

Cree un recurso compartido de red de Windows.

### Procedimiento

- 1 En View Administrator, seleccione **Configuración de View > Configuración de ThinApp** y haga clic en **Agregar repositorio**.
- 2 Escriba un nombre para mostrar del repositorio de aplicaciones en el cuadro de texto **Nombre para mostrar**.

- 3 Escriba la ruta al recurso compartido de red de Windows que aloja los paquetes de aplicaciones en el cuadro de texto **Ruta del recurso compartido**.

La ruta del recurso compartido de red debe tener el formato `\\ServerComputerName\ShareName`, donde *ServerComputerName* es el nombre DNS del equipo del servidor. No especifique ninguna dirección IP.

Por ejemplo: `\\server.domain.com\MSIPackages`

- 4 Haga clic en **Guardar** para registrar el repositorio de aplicaciones con View Administrator.

## Agregar aplicaciones ThinApp a View Administrator

Para agregar aplicaciones ThinApp a View Administrator, examine el repositorio de aplicaciones y seleccione las aplicaciones ThinApp. Después de agregar una aplicación ThinApp a View Administrator, puede asignarla a los equipos o a los grupos de escritorios.

### Requisitos previos

Registre un repositorio de aplicaciones con View Administrator.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApps**.
- 2 En la pestaña **Resumen**, haga clic en **Examinar ThinApps nuevas**.
- 3 Seleccione el repositorio de aplicaciones y la carpeta que desee examinar y haga clic en **Siguiente**.  
Si el repositorio de aplicaciones contiene subcarpetas, puede expandir la carpeta raíz y seleccionar una.
- 4 Seleccione las aplicaciones ThinApp que desee agregar a View Administrator.  
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias aplicaciones ThinApp.
- 5 Haga clic en **Examinar** para comenzar a examinar los paquetes MSI que seleccionó.  
Puede hacer clic en **Detener exploración** si necesita detenerla.  
View Administrator informa sobre el estado de cada operación de exploración y el número de aplicaciones ThinApp que se agregaron a View Administrator. Si selecciona una aplicación que ya está en View Administrator, esta no se vuelve a agregar.
- 6 Haga clic en **Finalizar**.  
Las nuevas aplicaciones ThinApp aparecen en la tabla **Resumen**.

### Pasos siguientes

(Opcional) Cree plantillas ThinApp.

## Crear una plantilla ThinApp

Puede crear una plantilla en View Administrator para especificar un grupo de aplicaciones ThinApp. Puede usar plantillas para agrupar aplicaciones por función, proveedor o cualquier otra agrupación lógica que sea efectiva para su organización.

Con las plantillas ThinApp, puede simplificar la distribución de varias aplicaciones. Cuando asigne una plantilla ThinApp a una máquina o un grupo de escritorios, View Administrator instala todas las aplicaciones que se encuentran en ese momento en la plantilla.

La creación de plantillas ThinApp es opcional.

---

**Nota** Si agrega una aplicación a una plantilla ThinApp después de asignar la plantilla a un equipo o un grupo de escritorios, View Administrator no asigna automáticamente la nueva aplicación al grupo de escritorio o al equipo. Si elimina una aplicación de una plantilla ThinApp que se asignó previamente a un grupo de escritorios o a un equipo, la aplicación sigue asignada a esos elementos.

---

### Requisitos previos

Agregue las aplicaciones ThinApp seleccionadas a View Administrator.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApp** y haga clic en **Nueva plantilla**.
- 2 Escriba un nombre para la plantilla y haga clic en **Agregar**.  
Todas las aplicaciones ThinApp aparecen en la tabla.
- 3 Para buscar una aplicación ThinApp en concreto, escriba el nombre de la aplicación en el cuadro de texto **Buscar** y haga clic en **Buscar**.
- 4 Seleccione las aplicaciones ThinApp que desee incluir en la plantilla y haga clic en **Agregar**.  
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias aplicaciones.
- 5 Haga clic en **Aceptar** para guardar la plantilla.

## Asignar aplicaciones ThinApp a grupos de escritorios y máquinas

Para instalar una aplicación ThinApp en un escritorio remoto, use View Administrator para asignar esta aplicación a una máquina o un grupo de escritorios.

Cuando asigne una aplicación ThinApp a una máquina, View Administrator comienza a instalar la aplicación en la máquina virtual unos minutos después. Cuando asigne una aplicación ThinApp a un grupo de escritorios, View Administrator comienza a instalar la aplicación la primera vez que un usuario inicia sesión en un escritorio remoto del grupo.

### Secuencial

View Administrator instala un acceso directo a la aplicación ThinApp en el escritorio remoto. El acceso directo lleva a la aplicación ThinApp en el recurso compartido de red que aloja el repositorio. Los usuarios deben

tener acceso al recurso compartido de red para ejecutar las aplicaciones ThinApp transmitidas.

## Completa

View Administrator instala la aplicación ThinApp completa en el sistema de archivos local.

La cantidad de tiempo que tarda en instalar una aplicación ThinApp depende del tamaño de la aplicación.

---

**Importante** Puede asignar aplicaciones ThinApp a escritorios basados en máquinas virtuales y grupos de escritorios automáticos o grupos manuales que contienen máquinas virtuales de vCenter Server. No puede asignar aplicaciones ThinApp a escritorios RDS o a equipos tradicionales.

---

- [Prácticas recomendadas para asignar aplicaciones ThinApp](#)

Siga las prácticas recomendadas cuando asigne aplicaciones ThinApps a grupos de escritorios y máquinas.

- [Asignar una aplicación ThinApp a varias máquinas](#)

Puede asignar una ThinApp en particular a una o varias máquinas.

- [Asignar varias aplicaciones ThinApps a una máquina](#)

Puede asignar una o varias aplicaciones ThinApps a una máquina.

- [Asignar una aplicación ThinApp a varios grupos de escritorios](#)

Puede asignar una aplicación ThinApp determinada a uno o más grupos de escritorios.

- [Asignar varias aplicaciones ThinApps a un grupo de escritorios](#)

Puede asignar una o varias aplicaciones ThinApps a un grupo de escritorios en particular.

- [Asignar una plantilla ThinApp a una máquina o grupo de escritorios](#)

Puede simplificar la distribución de varias aplicaciones ThinApp al asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

- [Revisar las asignaciones de las aplicaciones ThinApp](#)

Puede revisar todas las máquinas y los grupos de escritorios a los que una aplicación ThinApp está asignada en ese momento. También puede revisar todas las aplicaciones ThinApp que están asignadas a un grupo de escritorios o a una máquina en concreto.

- [Visualizar información del paquete MSI](#)

Después de agregar una aplicación ThinApp a View Administrator, puede visualizar información sobre su paquete MSI.



## Prácticas recomendadas para asignar aplicaciones ThinApp

Siga las prácticas recomendadas cuando asigne aplicaciones ThinApps a grupos de escritorios y máquinas.

- Para instalar una aplicación ThinApp en un escritorio remoto en concreto, asigne la aplicación a la máquina virtual que aloja el escritorio. Si usa una convención de nomenclatura común para sus máquinas, puede usar las asignaciones de máquinas para distribuir rápidamente las aplicaciones a todas las máquinas que usen dicha convención.
- Para instalar una aplicación ThinApp en todas las máquinas de un grupo de escritorios, asigne la aplicación al grupo de escritorios. Si organiza los grupos de escritorios por tipo de usuario o departamento, puede usar las asignaciones de los grupos de escritorios para distribuir rápidamente las aplicaciones a usuarios o departamentos específicos. Por ejemplo, si tiene un grupo de escritorios para los usuarios del departamento de contabilidad, puede distribuir la misma aplicación a todos los usuarios de este departamento asignando la aplicación al grupo de contabilidad.
- Para perfeccionar la distribución de varias aplicaciones ThinApp, incluya las aplicaciones en una plantilla ThinApp. Cuando asigne una plantilla ThinApp a una máquina o un grupo de escritorios, View Administrator instala todas las aplicaciones que se encuentran en ese momento en la plantilla.
- No asigne una plantilla ThinApp a una máquina o un grupo de escritorios si la plantilla contiene una aplicación ThinApp que ya está asignada a esa máquina o grupo de escritorios. Tampoco asigne una plantilla ThinApp a la misma máquina o grupo de escritorios más de una vez con un tipo de instalación diferente. View Administrator devolverá errores de asignación de ThinApp en ambas situaciones.

## Asignar una aplicación ThinApp a varias máquinas

Puede asignar una ThinApp en particular a una o varias máquinas.

### Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a View Administrator. Consulte [Agregar aplicaciones ThinApp a View Administrator](#).

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApps** y seleccione la aplicación ThinApp.
- 2 Seleccione **Asignar máquinas** en el menú desplegable **Agregar asignación**.

Las máquinas que aún no tengan asignadas la aplicación ThinApp aparecen en la tabla.

Opción	Acción
Buscar una máquina específica	Escriba el nombre de la máquina en el cuadro de texto <b>Buscar</b> y haga clic en <b>Buscar</b> .
Buscar todas las máquinas que sigan la misma convención de nomenclatura	Escriba parte de un nombre de una máquina en el cuadro de texto <b>Buscar</b> y haga clic en <b>Buscar</b> .

- 3 Seleccione las máquinas que desee asignar a la aplicación ThinApp y haga clic en **Agregar**.  
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias máquinas.
- 4 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
<b>Secuencial</b>	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
<b>Completa</b>	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

View Administrator comienza a instalar la aplicación ThinApp unos minutos después. Tras finalizar la instalación, la aplicación está disponible para todos los usuarios de los escritorios remotos alojados en las máquinas virtuales.

## Asignar varias aplicaciones ThinApps a una máquina

Puede asignar una o varias aplicaciones ThinApps a una máquina.

### Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a View Administrator. Consulte [Agregar aplicaciones ThinApp a View Administrator](#).

### Procedimiento

- 1 En View Administrator, seleccione **Recursos > Máquinas** y haga doble clic en el nombre de la máquina que aparece en la columna Máquina.
- 2 En la tabla **Resumen**, haga clic en **Agregar asignación** en el panel ThinApps.  
Las aplicaciones ThinApp que no aún no están asignadas a la máquina aparecen en la tabla.
- 3 Para buscar una aplicación en concreto, escriba el nombre de la aplicación en el cuadro de texto **Buscar** y haga clic en **Buscar**.
- 4 Seleccione la aplicación ThinApp que desee asignar a la máquina y haga clic en **Agregar**.  
Repita este paso para agregar varias aplicaciones.
- 5 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
<b>Secuencial</b>	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
<b>Completa</b>	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

View Administrator comienza a instalar las aplicaciones ThinApp unos minutos después. Tras finalizar la instalación, las aplicaciones están disponibles para todos los usuarios del escritorio remoto que está alojado en la máquina virtual.

## Asignar una aplicación ThinApp a varios grupos de escritorios

Puede asignar una aplicación ThinApp determinada a uno o más grupos de escritorios.

Si asigna una aplicación ThinApp a un grupo de clonación vinculada y, posteriormente, actualiza, recompone o vuelve a equilibrar el grupo, View Administrator vuelve a instalar la aplicación. No es necesario que vuelva a instalar la aplicación de forma manual.

### Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a View Administrator. Consulte [Agregar aplicaciones ThinApp a View Administrator](#).

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApps** y seleccione la aplicación ThinApp.

- 2 Seleccione **Asignar grupos de escritorios** del menú desplegable **Agregar asignación**.

Los grupos de escritorios que todavía no asignó la aplicación ThinApp aparecerán en la tabla.

Opción	Acción
<b>Buscar un grupo de escritorio determinado</b>	Escriba el nombre del grupo de escritorios en el cuadro de texto <b>Buscar</b> y haga clic en <b>Buscar</b> .
<b>Buscar todos los grupos de escritorios que sigan la misma convención de nomenclatura</b>	Escriba parte del nombre de un grupo de escritorios en el cuadro de texto <b>Buscar</b> y haga clic en <b>Buscar</b> .

- 3 Seleccione los grupos de escritorios que desea asignar a la aplicación ThinApp y haga clic en **Agregar**.

Haga clic mientras mantiene pulsada la tecla Ctrl o Mayús para seleccionar varios grupos de escritorios.

- 4 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
<b>Secuencial</b>	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
<b>Completa</b>	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

View Administrator comienza la instalación de la aplicación ThinApp cuando un usuario inicia sesión en un escritorio del grupo por primera vez. Al finalizar la instalación, la aplicación estará disponible para todos los usuarios del grupo de escritorios.

## Asignar varias aplicaciones ThinApps a un grupo de escritorios

Puede asignar una o varias aplicaciones ThinApps a un grupo de escritorios en particular.

Si asigna una aplicación ThinApp a un grupo de clones vinculados y, posteriormente, actualiza, recompone o vuelve a equilibrar el grupo, View Administrator vuelve a instalar la aplicación. No es necesario que vuelva a instalar la aplicación de forma manual.

### Requisitos previos

Examine un repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas a View Administrator. Consulte [Agregar aplicaciones ThinApp a View Administrator](#).

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios** y haga doble clic en el ID del grupo.
- 2 En la pestaña **Inventario**, haga clic en **ThinApps** y, a continuación, en **Agregar asignación**.  
Las aplicaciones ThinApp que no aún no están asignadas al grupo aparecen en la tabla.
- 3 Para buscar una aplicación en concreto, escriba el nombre de la aplicación ThinApp en el cuadro de texto **Buscar** y haga clic en **Buscar**.
- 4 Seleccione la aplicación ThinApp que desee asignar al grupo y haga clic en **Agregar**.  
Repita este paso para seleccionar varias aplicaciones.
- 5 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
<b>Secuencial</b>	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
<b>Completa</b>	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

View Administrator comienza a instalar las aplicaciones ThinApp la primera vez que un usuario inicia sesión en un escritorio del grupo. Tras finalizar la instalación, las aplicaciones están disponibles para todos los usuarios del grupo de escritorios.

## Asignar una plantilla ThinApp a una máquina o grupo de escritorios

Puede simplificar la distribución de varias aplicaciones ThinApp al asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

Si asigna una plantilla ThinApp a una máquina o un grupo de escritorios, View Administrator instala las aplicaciones ThinApp que estén presente en ese momento en la plantilla.

### Requisitos previos

Cree una plantilla ThinApp. Consulte [Crear una plantilla ThinApp](#).

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApps**.
- 2 Seleccione la plantilla ThinApp.
- 3 Seleccione **Asignar máquinas** o **Asignar grupos de escritorios** del menú desplegable **Agregar asignación**.

Todos los grupos de escritorios y máquinas aparecerán en la tabla.

Opción	Acción
<b>Buscar una máquina o un grupo de escritorios determinado</b>	Escriba el nombre de la máquina o del grupo de escritorios en el cuadro de texto <b>Buscar</b> y haga clic en <b>Buscar</b> .
<b>Buscar todos los grupos de escritorios y máquinas que sigan la misma convención de nomenclatura</b>	Escriba parte del nombre de la máquina o del grupo de escritorios en el cuadro de texto <b>Buscar</b> y haga clic en <b>Buscar</b> .

- 4 Seleccione las máquinas y grupos de escritorios a los que desea asignar la plantilla ThinApp y haga clic en **Agregar**.

Repita el mismo paso para seleccionar varias máquinas y grupos de escritorios.

- 5 Seleccione un tipo de instalación y haga clic en **Aceptar**.

Opción	Acción
<b>Secuencial</b>	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
<b>Completa</b>	Instale la aplicación completa en el sistema de archivos local de la máquina.

Algunas aplicaciones ThinApp no admiten ambos tipos de instalación. La forma en la que se creó la aplicación determina los tipos de instalación que están disponibles.

Al asignar una plantilla de ThinApp a una máquina, View Administrator comienza la instalación de aplicaciones en la plantilla unos minutos después. Al asignar una plantilla de ThinApp a un grupo de escritorios, View Administrator comienza la instalación de las aplicaciones en la plantilla cuando un usuario inicia sesión en un escritorio del grupo por primera vez. Al finalizar la instalación, la aplicación está disponible para todos los usuarios de la máquina o del grupo de escritorio.

View Administrator devuelve un mensaje de error si una plantilla ThinApp incluye una aplicación que ya esté asignada a la máquina o el grupo de escritorios.

## Revisar las asignaciones de las aplicaciones ThinApp

Puede revisar todas las máquinas y los grupos de escritorios a los que una aplicación ThinApp está asignada en ese momento. También puede revisar todas las aplicaciones ThinApp que están asignadas a un grupo de escritorios o a una máquina en concreto.

### Requisitos previos

Familiarícese con los valores de estado de la instalación ThinApp en [Valores del estado de instalación de la aplicación ThinApp](#).

### Procedimiento

- ◆ Seleccione las asignaciones de aplicaciones ThinApp que desee revisar.

Opción	Acción
Revisar todas las máquinas y los grupos de escritorios a los que una aplicación ThinApp está asignada	<p>Seleccione <b>Catálogo &gt; ThinApp</b> y haga doble clic en el nombre de la aplicación ThinApp.</p> <p>La pestaña <b>Asignaciones</b> muestra las máquinas y los grupos de escritorios a los que la aplicación está asignada en el momento e incluye el tipo de instalación.</p> <p>La pestaña <b>Máquinas</b> muestra las máquinas que están asociadas en el momento a la aplicación e incluye la información del estado de instalación.</p> <hr/> <p><b>Nota</b> Cuando asigne una aplicación ThinApp a un grupo, las máquinas del grupo aparecen en la pestaña <b>Máquinas</b> únicamente después de que se instale la aplicación.</p>
Revisar todas las aplicaciones ThinApp que están asignadas a un equipo en concreto	<p>Seleccione <b>Recursos &gt; Máquinas</b> y haga doble clic en el nombre de la máquina que aparece en la columna Máquina.</p> <p>El panel ThinApp de la pestaña <b>Resumen</b> muestra todas las aplicaciones que están asignadas en el momento a la máquina e incluye el estado de instalación.</p>
Revisar todas las aplicaciones ThinApp que están asignadas a un grupo de escritorios en concreto	<p>Seleccione <b>Catálogo &gt; Grupos de escritorios</b>, haga doble clic en el ID del grupo, seleccione la pestaña <b>Inventario</b> y haga clic a continuación en <b>ThinApp</b>.</p> <p>El panel Asignaciones de ThinApp muestra todas las aplicaciones que están asignadas en el momento al grupo de escritorios.</p>

## Valores del estado de instalación de la aplicación ThinApp

Después de asignar una aplicación ThinApp a una máquina o a un grupo, View Administrator indica el estado de la instalación.

[Tabla 12-1. Estado de instalación de la aplicación ThinApp](#) describe cada valor del estado.

**Tabla 12-1. Estado de instalación de la aplicación ThinApp**

Estado	Descripción
Asignado	La aplicación ThinApp está asignada a la máquina.
Error en la instalación	Se produjo un error cuando View Administrator intentó instalar la aplicación ThinApp.
Error al desinstalar	Se produjo un error cuando View Administrator intentó desinstalar la aplicación ThinApp.
Instalado	La aplicación ThinApp está instalada.
Instalación pendiente	View Administrator está intentando instalar la aplicación ThinApp. No puede anular la asignación de una aplicación con este estado.  <b>Nota</b> Este valor no aparece para las máquinas de los grupos de escritorios.
Desinstalación pendiente	View Administrator está intentando desinstalar la aplicación ThinApp.

## Visualizar información del paquete MSI

Después de agregar una aplicación ThinApp a View Administrator, puede visualizar información sobre su paquete MSI.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApps**.  
La pestaña **Resumen** muestra las aplicaciones que se encuentran disponibles y el número de asignaciones completas y secuenciales.
- 2 Haga doble clic en el nombre de la aplicación en la columna ThinApp.
- 3 Seleccione la pestaña **Resumen** para ver la información general sobre el paquete MSI.
- 4 Haga clic en **Información del paquete** para ver información detallada sobre el paquete MSI.

## Mantener las aplicaciones ThinApp en View Administrator

Si desea mantener las aplicaciones ThinApp en View Administrator, esto incluye tareas como eliminar asignaciones de aplicaciones ThinApp, eliminar los repositorios de aplicaciones y las aplicaciones ThinApp, así como modificar y eliminar las plantillas ThinApp.

**Nota** Para actualizar una aplicación ThinApp, debe anular la asignación, eliminar la versión antigua de la aplicación y agregar y asignar la versión más actual.

- **Eliminar una asignación de aplicaciones ThinApp de varias máquinas**  
Puede eliminar una asignación de aplicaciones ThinApp determinada de una o varias máquinas.
- **Eliminar varias asignaciones de aplicaciones ThinApp de una máquina**  
Puede eliminar las asignaciones a una o varias aplicaciones ThinApps de una máquina particular.

- [Eliminar una asignación de aplicaciones ThinApp de varios grupos de escritorios](#)

Puede eliminar una asignación de aplicaciones ThinApp determinada de uno o varios grupos de escritorios.

- [Eliminar varias asignaciones de aplicaciones ThinApp de un grupo de escritorios](#)

Puede eliminar una o varias asignaciones de aplicaciones ThinApp de un grupo de escritorios en particular.

- [Eliminar una aplicación ThinApp de View Administrator](#)

Cuando elimine una aplicación ThinApp de View Administrator, ya no podrá asignarla a las máquinas o a los grupos de escritorios.

- [Modificar o eliminar una plantilla ThinApp](#)

Puede agregar o eliminar aplicaciones de una plantilla ThinApp. También es posible eliminar la plantilla.

- [Eliminar el repositorio de una aplicación](#)

Puede eliminar el repositorio de una aplicación de View Administrator.

## Eliminar una asignación de aplicaciones ThinApp de varias máquinas

Puede eliminar una asignación de aplicaciones ThinApp determinada de una o varias máquinas.

### Requisitos previos

Notifique a los usuarios de los escritorios remotos que se alojan en las máquinas de que pretende eliminar la aplicación.

### Procedimiento

- 1 En View Administrator, seleccione **Catálogo > ThinApp** y haga doble clic en el nombre de la aplicación ThinApp.
- 2 En la pestaña **Asignaciones**, seleccione una máquina y haga clic en **Eliminar asignación**.  
Puede pulsar la tecla Ctrl o la tecla Mayús mientras hace clic para seleccionar varias máquinas.

View Administrator desinstala la aplicación ThinApp unos minutos después.

---

**Importante** Si un usuario final usa la aplicación ThinApp al mismo tiempo que View Administrator intenta desinstalar la aplicación, se produce un error y el estado de la aplicación cambia a Error al desinstalar. Cuando se produce este error, en primer lugar debe desinstalar de forma manual los archivos de la aplicación ThinApp de la máquina y luego hacer clic en **Eliminar estado de la aplicación para el escritorio** en View Administrator.

---

## Eliminar varias asignaciones de aplicaciones ThinApp de una máquina

Puede eliminar las asignaciones a una o varias aplicaciones ThinApps de una máquina particular.



**Requisitos previos**

Notifique a los usuarios del escritorio remoto que aloja la máquina que pretende eliminar las aplicaciones.

**Procedimiento**

- 1 En View Administrator, seleccione **Recursos > Máquinas** y haga doble clic en el nombre de la máquina que aparece en la columna Máquina.
- 2 En la pestaña **Resumen**, seleccione la aplicación ThinApp y haga clic en **Eliminar asignación** que aparece en el panel ThinApps.

Repita este paso para eliminar otra asignación de aplicaciones.

View Administrator desinstala la aplicación ThinApp unos minutos después.

---

**Importante** Si un usuario final usa la aplicación ThinApp al mismo tiempo que View Administrator intenta desinstalar la aplicación, se produce un error y el estado de la aplicación cambia a Error al desinstalar. Cuando se produce este error, en primer lugar debe desinstalar de forma manual los archivos de la aplicación ThinApp de la máquina y luego hacer clic en **Eliminar estado de la aplicación para el escritorio** en View Administrator.

---

## Eliminar una asignación de aplicaciones ThinApp de varios grupos de escritorios

Puede eliminar una asignación de aplicaciones ThinApp determinada de uno o varios grupos de escritorios.

**Requisitos previos**

Notifique a los usuarios de los escritorios remotos de los grupos de que pretende eliminar la aplicación.

**Procedimiento**

- 1 En View Administrator, seleccione **Catálogo > ThinApp** y haga doble clic en el nombre de la aplicación ThinApp.
- 2 En la pestaña **Asignaciones**, seleccione un grupo de escritorios y haga clic en **Eliminar asignación**.

Haga clic mientras mantiene pulsada la tecla Ctrl o Mayús para seleccionar varios grupos de escritorios.

View Administrator desinstala la aplicación ThinApp la primera vez que un usuario inicia sesión en un escritorio remoto del grupo.

## Eliminar varias asignaciones de aplicaciones ThinApp de un grupo de escritorios

Puede eliminar una o varias asignaciones de aplicaciones ThinApp de un grupo de escritorios en particular.

**Requisitos previos**

Notifique a los usuarios de los escritorios remotos del grupo de que pretende eliminar las aplicaciones.

**Procedimiento**

- 1 En View Administrator, seleccione **Catálogo > Grupos de escritorios** y haga doble clic en el ID del grupo.
- 2 En la pestaña **Inventario**, haga clic en **ThinApps**, seleccione la aplicación ThinApp y haga clic en **Eliminar asignación**.

Repita este paso para eliminar varias aplicaciones.

View Administrator desinstala las aplicaciones ThinApp la primera vez que un usuario inicia sesión en un escritorio remoto del grupo.

**Eliminar una aplicación ThinApp de View Administrator**

Cuando elimine una aplicación ThinApp de View Administrator, ya no podrá asignarla a las máquinas o a los grupos de escritorios.

Es posible que necesite eliminar una aplicación ThinApp si su organización decide reemplazarla por una aplicación diferente del proveedor.

---

**Nota** No puede eliminar una aplicación ThinApp si ya está asignada a una máquina o a un grupo de escritorios o si está en estado Desinstalación pendiente.

---

**Requisitos previos**

Si una aplicación ThinApp ya está asignada a un grupo de escritorios o a un equipo, elimine la asignación del grupo de escritorios o de la máquina.

**Procedimiento**

- 1 En View Administrator, seleccione **Catálogo > ThinApps** y seleccione la aplicación ThinApp.
- 2 Haga clic en **Eliminar ThinApp**.
- 3 Haga clic en **Aceptar**.

**Modificar o eliminar una plantilla ThinApp**

Puede agregar o eliminar aplicaciones de una plantilla ThinApp. También es posible eliminar la plantilla.

Si agrega una aplicación a una plantilla ThinApp después de asignar la plantilla a un equipo o un grupo de escritorios, View Administrator no asigna automáticamente la nueva aplicación al grupo de escritorio o al equipo. Si elimina una aplicación de una plantilla ThinApp que se asignó previamente a un grupo de escritorios o a un equipo, la aplicación sigue asignada a esos elementos.

**Procedimiento**

- ◆ En View Administrator, seleccione **Catálogo > ThinApps** y elija la plantilla ThinApp.

Opción	Acción
Agregar aplicaciones ThinApp a una plantilla o eliminarlas	Haga clic en <b>Editar plantilla</b> .
Eliminar la plantilla	Haga clic en <b>Eliminar plantilla</b> .

## Eliminar el repositorio de una aplicación

Puede eliminar el repositorio de una aplicación de View Administrator.

Es posible que necesite eliminar el repositorio de una aplicación si ya no necesita los paquetes MSI incluidos o si necesita mover dichos paquetes a otro recurso compartido en red. No se puede editar la ruta del recurso compartido del repositorio de una aplicación en View Administrator.

**Procedimiento**

- 1 En View Administrator, seleccione **Configuración de View > Configuración de ThinApp** y seleccione el repositorio de la aplicación.
- 2 Haga clic en **Eliminar repositorio**.

## Supervisar y solucionar problemas de las aplicaciones ThinApp en View Administrator

View Administrator registra los eventos relacionados con la administración de las aplicaciones ThinApp en la base de datos de eventos e informes. Puede ver esos eventos en la página **Eventos** de View Administrator.

Un evento puede aparecer en la página **Eventos** cuando se producen las siguientes situaciones.

- Se asignó una aplicación ThinApp o se eliminó una asignación de aplicación
- Se instaló o se desinstaló una aplicación ThinApp en un equipo
- No se puede instalar ni desinstalar una aplicación ThinApp
- Se registró, se modificó o se eliminó un repositorio de aplicaciones ThinApp de View Administrator
- Se agregó una aplicación ThinApp a View Administrator

Existen consejos para solucionar problemas comunes relacionados con la administración de aplicaciones ThinApp.

## No se puede registrar un repositorio de aplicaciones

No puede registrar un repositorio de aplicaciones en View Administrator.

## Problema

Recibe un mensaje de error al intentar registrar un repositorio de aplicaciones en View Administrator.

## Causa

El host del servidor de conexión de View no puede acceder al recurso compartido de red que aloja el repositorio de aplicaciones. La ruta del recurso compartido de red que introdujo en el cuadro de diálogo **Ruta del recurso compartido** puede no ser correcta, el recurso compartido de red que aloja el repositorio de aplicaciones está en un dominio al que no se puede acceder desde el host del servidor de conexión de View o bien los permisos del recurso compartido de red no se configuraron correctamente.

- Si la ruta del recurso compartido de red es incorrecta, escriba la correcta. No se admiten las rutas de recursos compartidos de red que contienen direcciones IP.
- Si el recurso compartido de red no es un dominio al que se pueda acceder, copie los paquetes de aplicaciones a un recurso compartido de red en un dominio al que se pueda acceder desde el host del servidor de conexión de View.
- Compruebe que el archivo y los permisos de uso compartido de la carpeta compartida proporcione Acceso de lectura al grupo de Active Directory integrado Equipos del dominio. Si piensa asignar aplicaciones ThinApps a controladores de dominio, compruebe que el archivo y los permisos de uso compartido también proporcionen Acceso de solo lectura al grupo de Active Directory integrado Controladores de dominio. Tras establecer o cambiar los permisos, es posible que transcurran 20 minutos hasta que se pueda acceder al recurso compartido de red.

## No se puede agregar aplicaciones ThinApp a View Administrator

View Administrator no puede agregar aplicaciones ThinApp a View Administrator.

## Problema

Ningún paquete MSI está disponible cuando hace clic en **Examinar ThinApps nuevas** en View Administrator.

## Causa

Ni los paquetes de aplicaciones que no están en formato MSI ni el host del servidor de conexión de View pueden acceder a los directorios en el recurso compartido de red.

- Compruebe que los paquetes de aplicaciones del repositorio estén en formato MSI.
- Compruebe que el recurso compartido de red cumpla los requisitos de View para las aplicaciones ThinApp. Consulte [Requisitos de View para las aplicaciones ThinApp](#) para obtener más información.
- Compruebe que los directorios del recurso compartido de red tengan los permisos correspondientes. Consulte [No se puede registrar un repositorio de aplicaciones](#) para obtener más información.

Aparecen mensajes en el archivo de registro de depuración del servidor de conexión de View cuando se examina un repositorio de aplicaciones. Los archivos de registro del servidor de conexión de View se encuentran en el host de dicho servidor en el directorio `unidad:\Documents and Settings\All Users\Application Data\VMware\VDM\logs`.

## No se puede asignar una plantilla ThinApp

No puede asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

### Problema

View Administrator devuelve un error de asignación cuando intenta asignar una plantilla ThinApp a una máquina o un grupo de escritorios.

### Causa

La plantilla ThinApp contiene una aplicación que ya está asignada a la máquina o al grupo de escritorios, o bien la plantilla ThinApp se asignó previamente a la máquina o al grupo de escritorios con un tipo de instalación diferente.

Si la plantilla contiene una aplicación ThinApp que ya está asignada a la máquina o al grupo de escritorios, cree una nueva plantilla que no contenga la aplicación o edite la plantilla existente y elimine la aplicación. Asigne la plantilla nueva o modificada a la máquina o al grupo de escritorios.

Para cambiar el tipo de instalación de una aplicación ThinApp, debe eliminar la asignación de la aplicación existente de la máquina o del grupo de escritorios. Después de desinstalar la aplicación ThinApp, puede asignarla a la máquina o al grupo de escritorios con un tipo de instalación diferente.

## La aplicación ThinApp no está instalada

View Administrator no puede instalar una aplicación ThinApp.

### Problema

El estado de la instalación de la aplicación ThinApp es Instalación pendiente o Error en la instalación.

### Causa

Entre las causas comunes de este problema se encuentran las siguientes:

- No hay espacio de disco suficiente en el equipo para instalar la aplicación ThinApp.
- Se perdió la conectividad de red entre el host del servidor de conexión de View y el equipo o entre el host del servidor de conexión de View y el repositorio de la aplicación.
- No se puede acceder a la aplicación ThinApp en el recurso compartido de red.
- La aplicación ThinApp se instaló previamente, o bien el directorio o el archivo ya existe en el equipo.

Puede consultar los archivos de registro de Horizon Agent y del servidor de conexión de View para obtener más información sobre la causa del problema.

Los archivos de registro de Horizon Agent se encuentran la ruta *unidad*: \ProgramData\VMware\VDM \logs del equipo.

Los archivos de registro del servidor de conexión de View se encuentran en el host de dicho servidor en el directorio *unidad*: \Documents and Settings\All Users\Application Data\VMware\VDM\logs.

## Solución

- 1 En View Administrator, seleccione **Catálogo > ThinApps**.
- 2 Haga clic en el nombre de la aplicación ThinApp.
- 3 En la pestaña **Máquinas**, seleccione el equipo y haga clic en **Volver a intentar la instalación** para volver a instalar la aplicación ThinApp.

## La aplicación ThinApp no está desinstalada

View Administrator no puede desinstalar una aplicación ThinApp.

## Problema

El estado de la instalación de la aplicación ThinApp muestra Error al desinstalar.

## Causa

Entre las causas comunes de este error se encuentran las siguientes:

- La aplicación ThinApp estaba ocupada cuando View Administrator intentó desinstalarla.
- Se perdió la conectividad a la red entre el host del servidor de conexión de View y el equipo.

Puede consultar los archivos de registro de Horizon Agent y del servidor de conexión de View para obtener más información sobre la causa del problema.

Los archivos de registro Horizon Agent se encuentran en la ruta *unidad:*\Documents and Settings\All Users\Application Data\VMware\VDM\logs en los sistemas Windows XP y en *unidad:*\ProgramData\VMware\VDM\logs en los sistemas Windows 7.

Los archivos de registro del servidor de conexión de View se encuentran en el host de dicho servidor en el directorio *unidad:*\Documents and Settings\All Users\Application Data\VMware\VDM\logs.

## Solución

- 1 En View Administrator, seleccione **Catálogo > ThinApps**.
- 2 Haga clic en el nombre de la aplicación ThinApp.
- 3 Haga clic en la pestaña **Máquinas**, seleccione el equipo y haga clic en **Volver a intentar la desinstalación** para volver a intentar realizar la operación de desinstalación.
- 4 Si aún se produce algún error en la operación de desinstalación, elimine de forma manual la aplicación ThinApp del equipo y vuelva a hacer clic en **Eliminar estado de la aplicación para el escritorio**.

Este comando borra la asignación de la aplicación ThinApp en View Administrator. No elimina ningún archivo ni configuración del equipo.

---

**Importante** Use este comando únicamente después de eliminar manualmente la aplicación ThinApp del equipo.

---

## El paquete MSI no es válido

View Administrator notifica que un paquete MSI de un repositorio de aplicaciones no es válido.

### Problema

View Administrator notifica que un paquete MSI no es válido durante una operación de análisis.

### Causa

Entre las causas comunes de este problema se encuentran las siguientes:

- El archivo MSI está dañado.
- El archivo MSI no se creó con ThinApp.
- El archivo MSI se creó o se volvió a empaquetar con una versión de ThinApp que no es compatible. Debe usar la versión 4.6 de ThinApp o una versión posterior.

Consulte la *Guía de usuario de ThinApp* para obtener más información sobre cómo solucionar los problemas de los paquetes MSI.

## Ejemplo de configuración ThinApp

El ejemplo de configuración ThinApp lo guía paso a paso a través de una configuración ThinApp típica, desde la captura y el empaquetado de las aplicaciones hasta la comprobación del estado de una instalación.

### Requisitos previos

Consulte estos temas para obtener una información completa sobre cómo realizar estos pasos en este ejemplo.

- [Capturar y almacenar paquetes de aplicaciones](#)
- [Asignar aplicaciones ThinApp a grupos de escritorios y máquinas](#)

### Procedimiento

#### Procedimiento

- 1 Descargue el software de ThinApp en <http://www.vmware.com/products/thinapp> e instálelo en un equipo limpio.  
  
View es compatible con ThinApp 4.6 y versiones posteriores.
- 2 Use el asistente de ThinApp **Configurar la captura** para capturar y empaquetar las aplicaciones en formato MSI.

- 3 Cree una carpeta compartida en un equipo de un dominio de Active Directory a la que se pueda acceder desde el host del servidor de conexión de View y desde los escritorios remotos y, a continuación, configure el archivo y los permisos de uso compartido en la carpeta compartida para proporcionar Acceso de lectura al grupo de Active Directory integrado Equipos del dominio.

Si tiene pensado asignar aplicaciones ThinApp a controladores de dominio, proporcione también Acceso de lectura en el grupo de Active Directory integrado Controladores de dominio.

- 4 Copie los paquetes MSI en la carpeta compartida.
- 5 Registre la carpeta compartida como un repositorio de aplicaciones en View Administrator.
- 6 En View Administrator, examine los paquetes MSI del repositorio de aplicaciones y agregue las aplicaciones ThinApp seleccionadas en View Administrator.
- 7 Decida si desea asignar las aplicaciones ThinApp a grupos de escritorios o a máquinas.

Si usa una convención de nomenclatura común para sus máquinas, puede usar las asignaciones de máquinas para distribuir rápidamente las aplicaciones a todas las máquinas que usen dicha convención. Si organiza los grupos de escritorios por tipo de usuario o departamento, puede usar las asignaciones de los grupos de escritorios para distribuir rápidamente las aplicaciones a usuarios o departamentos específicos.

- 8 En View Administrator, seleccione las aplicaciones ThinApp que desea asignar a las máquinas o a los grupos de escritorios y especifique el método de instalación.

Opción	Acción
<b>Secuencial</b>	Instale un acceso directo a la aplicación en la máquina. El acceso directo lleva a la aplicación en el recurso compartido de red que aloja el repositorio. Los usuarios deben tener acceso al recurso compartido de red para ejecutar la aplicación.
<b>Completa</b>	Instale la aplicación completa en el sistema de archivos local de la máquina.

- 9 En View Administrator, compruebe el estado de instalación de las aplicaciones ThinApp.



# Configurar clientes en modo de pantalla completa

# 13

Puede establecer que los clientes desatendidos puedan obtener acceso a los escritorios desde View.

Un cliente en modo de pantalla completa es un cliente ligero o un equipo bloqueado que ejecuta Horizon Client para conectarse a la instancia del servidor de conexión de View y ejecutar una sesión remota. No es necesario que los usuarios finales inicien sesión para acceder al dispositivo cliente, aunque el escritorio remoto pueda solicitarles que proporcionen información de autenticación para algunas aplicaciones. Entre las aplicaciones de ejemplo se incluyen estaciones de trabajo en las que se introducen datos médicos, estaciones de facturación de líneas aéreas, puntos de autoservicio para los clientes y terminales de información para el acceso público.

Debe comprobar que la aplicación del escritorio implemente los mecanismos de autenticación para realizar transacciones seguras, que la red física sea segura ante ataques snooping y manipulaciones y que todos los dispositivos conectados a la red sean de confianza.

Los clientes en modo de pantalla completa admiten las funciones estándar en el acceso remoto como, por ejemplo, el redireccionamiento automático de dispositivos USB a las sesiones remotas y la impresión según ubicación.

View usa la función Autenticación flexible en View 4.5 y en versiones posteriores para autenticar un dispositivo cliente en modo de pantalla completa en lugar del usuario final. Puede configurar una instancia del servidor de conexión de View para autenticar clientes que se identifiquen por la dirección MAC, por nombre de usuario que comience por los caracteres "custom-" o por una cadena de prefijos alternativo que definiera en ADAM. Si configura que un cliente que tenga una contraseña generada automáticamente, puede ejecutar Horizon Client en el dispositivo sin especificar una contraseña. Si configura una contraseña explícita, debe especificarla en Horizon Client. Al ejecutar normalmente Horizon Client desde un script y aparecer la contraseña como texto no cifrado, debería tomar precauciones para hacer que el script sea ilegible por los usuarios sin privilegios.

Solamente las instancias del servidor de conexión de View que habilite para autenticar clientes en modo de pantalla completa pueden aceptar conexiones desde cuentas que comiencen por los caracteres "cm-" seguidos por una dirección MAC, por los caracteres "custom-" o por la cadena alternativa que definiera. Horizon Client en View 4.5 y versiones posteriores no permite que se introduzcan de forma manual los nombres de usuario que utilicen estas formas.

Como práctica recomendada, use las instancias del servidor de conexión de View dedicadas para administrar clientes en modo de pantalla completa y para crear grupos y unidades organizativas dedicadas en Active Directory para las cuentas de dichos clientes. Esta práctica no solo realiza particiones en estos sistemas ante intrusiones no deseadas, sino que también facilita la configuración y la administración de los clientes.

Este capítulo incluye los siguientes temas:

- [Configurar clientes en modo de pantalla completa](#)

## Configurar clientes en modo de pantalla completa

Para configurar Active Directory y View de forma que admitan clientes en modo de pantalla completa, debe realizar varias tareas en secuencia.

### Requisitos previos

Compruebe que tenga los privilegios necesarios para realizar las tareas de configuración.

- Las credenciales **Admins. del dominio** u **Opsr. de cuentas** en Active Directory para realizar cambios en las cuentas de usuarios y grupos de un dominio.
- Las funciones **Administradores**, **Administradores de inventario** o una equivalente para usar View Administrator para autorizar el uso de escritorios remotos por parte de usuarios o grupos.
- La función **Administradores** o una equivalente para ejecutar el comando `vdadmin`.

### Procedimiento

#### 1 [Preparar Active Directory y View para clientes en modo de pantalla completa](#)

Debe configurar Active Directory para que acepte las cuentas que cree para autenticar dispositivos cliente. Cuando cree un grupo, también debe autorizarlo para acceder al grupo de escritorios al que tiene acceso un cliente. También puede preparar el grupo de escritorios que los clientes utilizan.

#### 2 [Establecer valores predeterminados para clientes en modo de pantalla completa](#)

Puede utilizar el comando `vdadmin` para establecer los valores predeterminados sobre la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de Active Directory de los clientes en modo de pantalla completa.

#### 3 [Visualizar las direcciones MAC de dispositivos cliente](#)

Si desea crear una cuenta para un cliente que se basa en su dirección MAC, puede usar Horizon Client para ver la dirección MAC del dispositivo cliente.

#### 4 [Agregar cuentas de clientes en modo de pantalla completa](#)

Puede usar el comando `vdadmin` para agregar cuentas de clientes a la configuración de un grupo de servidores de conexión de View. Después de agregar un cliente, este se encuentra disponible para su uso con una instancia del servidor de conexión de View en la que habilitó la autenticación de los clientes. También puede actualizar la configuración de los clientes o eliminar las cuentas del sistema.

## 5 Habilitar la autenticación de clientes en modo de pantalla completa

Puede utilizar el comando `vdadmin` para habilitar la autenticación de clientes que intenten conectarse a sus escritorios remotos a través de la instancia del servidor de conexión de View.

## 6 Verificar la configuración de los clientes en modo de pantalla completa

Puede usar el comando `vdadmin` para mostrar información sobre los clientes en modo de pantalla completa y las instancias del servidor de conexión de View que se configuraron para autenticar dichos clientes.

## 7 Conectarse a escritorios remotos desde clientes en modo de pantalla completa

Puede ejecutar el cliente desde una línea de comandos o usar un script para conectar un cliente a una sesión remota.

# Preparar Active Directory y View para clientes en modo de pantalla completa

Debe configurar Active Directory para que acepte las cuentas que cree para autenticar dispositivos cliente. Cuando cree un grupo, también debe autorizarlo para acceder al grupo de escritorios al que tiene acceso un cliente. También puede preparar el grupo de escritorios que los clientes utilizan.

La práctica recomendada es crear una unidad organizativa independiente y un grupo para reducir el trabajo a la hora de administrar clientes en modo de pantalla completa. Puede agregar cuentas independientes de clientes que no pertenecen a ningún grupo, pero así genera gastos de administración elevados si configura más de un pequeño número de clientes.

## Procedimiento

- 1 En Active Directory, cree un grupo y una unidad organizativa independientes para utilizarlos con los clientes en modo de pantalla completa.

Debe asignarle al grupo un nombre anterior a Windows 2000. Utilice este nombre para identificar al grupo con el comando `vdadmin`.

- 2 Cree la imagen o plantilla de la máquina virtual invitada.

Puede utilizar una máquina virtual administrada por vCenter Server como plantilla para un grupo automático, como principal de un grupo de clones vinculados o como máquina virtual en un grupo de escritorios manual. También puede instalar y configurar aplicaciones en el sistema operativo invitado.

- 3 Configure el sistema operativo invitado para que los clientes no se bloqueen cuando no estén atendidos.

View elimina el mensaje previo al inicio de sesión para los clientes que se conectan en modo de pantalla completa. Si requiere un evento para desbloquear la pantalla y mostrar un mensaje, puede configurar una aplicación adecuada en el sistema operativo invitado.

- 4 En View Administrator, cree un grupo de escritorios para que los clientes lo utilicen y autorícelo a acceder al grupo.

Por ejemplo, puede elegir crear un grupo de escritorios de clones vinculados y asignaciones flotantes como la opción más adecuada para los requisitos de la aplicación cliente. También puede asociar una o varias aplicaciones ThinApp al grupo de escritorios.

---

**Importante** No autorice a un cliente ni a un grupo a acceder a más de un grupo de escritorios. Si lo hace, View asigna al cliente un escritorio remoto al azar entre los grupos para los que el cliente está autorizado y genera un evento de advertencia.

---

- 5 Si desea habilitar la impresión según ubicación para los clientes, configure la opción AutoConnect Location-based Printing for VMware View de la directiva de grupo de Active Directory, que se encuentra en el Editor de objetos de directiva de grupo de Microsoft. Para acceder a ella, seleccione Configuración del equipo y abra la carpeta Configuración de software.

- 6 Configure otras directivas que necesite optimizar y asegure los escritorios remotos de los clientes.

Por ejemplo, puede anular las directivas que conectan los dispositivos USB locales al escritorio remoto cuando este se inicia o al conectar los dispositivos. De forma predeterminada, Horizon Client para Windows habilita estas directivas para los clientes en modo de pantalla completa.

## Ejemplo: Preparar Active Directory para clientes en modo de pantalla completa

La intranet tiene un dominio MYORG y su unidad organizativa tiene el nombre distintivo OU=myorg-ou,DC=myorg,DC=com. En Active Directory, cree la unidad organizativa kiosk-ou con el nombre distintivo OU=kiosk-ou,DC=myorg,DC=com y el grupo kc-grp para utilizarlo con los clientes en modo de pantalla completa.

### Pasos siguientes

Defina los valores predeterminados de los clientes.

## Establecer valores predeterminados para clientes en modo de pantalla completa

Puede utilizar el comando `vdmadmin` para establecer los valores predeterminados sobre la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de Active Directory de los clientes en modo de pantalla completa.

Debe ejecutar el comando `vdmadmin` en una de las instancias del servidor de conexión de View del grupo que contiene la instancia que los clientes usarán para conectarse a sus escritorios remotos.

Al configurar los valores predeterminados sobre la caducidad de la contraseña y afiliación a grupos de Active Directory, estas opciones se comparten con todas las instancias del servidor de conexión de View en un grupo.

## Procedimiento

- ◆ Establezca los valores predeterminados para clientes.

```
vdmadmin
-Q
-clientauth
-setdefaults [-b argumentos_autenticación] [-ouDN] [ -expirepassword | -noexpirepassword ]
[-groupnombre_grupo | -nogroup]
```

Opción	Descripción
<b>-expirepassword</b>	Especifica el mismo periodo de caducidad para las contraseñas de las cuentas cliente que el del grupo del servidor de conexión de View. Si no se definió un periodo de caducidad para el grupo, las contraseñas nunca expirarán.
<b>-group <i>nombre_grupo</i></b>	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.
<b>-noexpirepassword</b>	Especifica que las contraseñas de las cuentas cliente no expiran.
<b>-nogroup</b>	Borra la configuración para el grupo predeterminado.
<b>-ou <i>DN</i></b>	Especifica el nombre distintivo de la unidad organizativa predeterminada a la que se agregan las cuentas cliente. Por ejemplo: OU=kiosk-ou,DC=myorg,DC=com
<b>Nota</b> No puede utilizar el comando para cambiar la configuración de una unidad organizativa.	

El comando actualiza los valores predeterminados para los clientes en el grupo del servidor de conexión de View.

## Ejemplo: Establecer valores predeterminados para clientes en modo de pantalla completa

Establezca los valores predeterminados de la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de clientes.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

### Pasos siguientes

Encuentre las direcciones MAC de los dispositivos cliente que utilicen dichas direcciones para autenticarse.

## Visualizar las direcciones MAC de dispositivos cliente

Si desea crear una cuenta para un cliente que se basa en su dirección MAC, puede usar Horizon Client para ver la dirección MAC del dispositivo cliente.

## Requisitos previos

Inicie sesión en la consola del cliente.

## Procedimiento

- ◆ Para ver la dirección MAC, escriba el comando apropiado según la plataforma.

Opción	Acción
Windows	<p>Introduzca</p> <pre>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo.</pre> <p>El cliente usa la instancia del servidor de conexión de View predeterminada que configuró para ella. Si no configuró un valor predeterminado, el cliente le solicitará el valor.</p> <p>El comando muestra la dirección IP, la dirección MAC y el nombre del equipo del dispositivo cliente.</p>
Linux	<p>Introduzca <code>vmware-view --printEnvironmentInfo -s <i>connection_server</i></code>.</p> <p>Debe especificar la dirección IP o el FQDN de la instancia del servidor de conexión de View que el cliente usará para conectarse al escritorio.</p> <p>El comando muestra la dirección IP, la dirección MAC, el nombre de la máquina, el dominio, el nombre y el dominio de cualquier usuario con la sesión iniciada y la zona horaria del dispositivo cliente.</p>

## Pasos siguientes

Agregue las cuentas de los clientes.

## Agregar cuentas de clientes en modo de pantalla completa

Puede usar el comando `vdadmin` para agregar cuentas de clientes a la configuración de un grupo de servidores de conexión de View. Después de agregar un cliente, este se encuentra disponible para su uso con una instancia del servidor de conexión de View en la que habilitó la autenticación de los clientes. También puede actualizar la configuración de los clientes o eliminar las cuentas del sistema.

Debe ejecutar el comando `vdadmin` en una de las instancias del servidor de conexión de View del grupo que contiene la instancia que los clientes usarán para conectarse a sus escritorios remotos.

Cuando agrega un cliente en modo de pantalla completa, View crea una cuenta de usuario para el cliente en Active Directory. Si especifica un nombre para el cliente, este nombre debe comenzar por una cadena de prefijo reconocida, como "custom-", o bien con una cadena de prefijo alternativa que definió en ADAM y que no puede ser superior a 20 caracteres. Si no especifica un nombre para un cliente, View 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 de View que habilitó para la autenticación de los clientes.

**Importante** No use un nombre especificado con más de un dispositivo cliente. Es posible que las próximas versiones no admitan esta configuración.

## Procedimiento

- ◆ Ejecute el comando `vdmadmin` con las opciones `-domain` y `-clientid` para especificar el dominio y el nombre o la dirección MAC del cliente.

```
vdmadmin
-Q
-clientauth
-add [-bargumentos_autenticación] -domainnombre_dominio-clientidid_cliente [-password
"contraseña" | -genpassword] [-ouDN] [-expirepassword | -noexpirepassword] [-groupnombre_grupo |
-nogroup] [-description "texto_descripción"]
```

Opción	Descripción
<code>-clientid id_cliente</code>	Especifica el nombre o la dirección MAC del cliente.
<code>-description "texto_descripción"</code>	Crea una descripción de la cuenta del dispositivo cliente en Active Directory.
<code>-domain nombre_dominio</code>	Especifica el dominio del cliente.
<code>-expirepassword</code>	Especifica que el tiempo de caducidad de la contraseña de la cuenta es el mismo que el del grupo del servidor de conexión de View. Si no se definió el tiempo de caducidad, la contraseña no caduca.
<code>-genpassword</code>	Genera una contraseña para la cuenta del cliente. Este es el comportamiento predeterminado si no especifica <code>-password</code> ni <code>-genpassword</code> . Una contraseña generada tiene 16 caracteres, contiene al menos una letra en mayúscula, una en minúscula, un símbolo y un número. Además, puede contener caracteres repetidos. Si necesita una contraseña más segura, use la opción <code>-password</code> para especificar la contraseña.
<code>-group nombre_grupo</code>	Especifica el nombre del grupo al que se agregó la cuenta del cliente. El nombre del grupo debe especificarse como el nombre del grupo de Active Directory anterior a Windows 2000. Si estableció previamente un grupo predeterminado, la cuenta del cliente se agrega a este grupo.
<code>-noexpirepassword</code>	Especifica que la contraseña de la cuenta del cliente no caduca.
<code>-nogroup</code>	Especifica que la cuenta del cliente no se agrega al grupo predeterminado.
<code>-ou DN</code>	Especifica el nombre distintivo de la unidad organizativa a la que se agregó la cuenta del cliente. Por ejemplo: OU=kiosk-ou,DC=myorg,DC=com
<code>-password "contraseña"</code>	Especifica una contraseña explícita para la cuenta del cliente.

El comando crea una cuenta de usuario en Active Directory para el cliente en el dominio y grupo especificados (si existe alguno).

## Ejemplo: Agregar cuentas para los clientes

Agregue una cuenta para un cliente especificado por la dirección MAC al dominio MYORG, usando la configuración predeterminada del grupo `kc-grp`.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Agregue una cuenta para un cliente especificado por su dirección MAC al dominio MYORG, usando una contraseña generada automáticamente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

Agregue una cuenta para un cliente con nombre y especifique la contraseña que se usará con el cliente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Agregue una cuenta para un cliente con nombre, usando una contraseña generada automáticamente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

### Pasos siguientes

Habilite la autenticación de los clientes.

## Habilitar la autenticación de clientes en modo de pantalla completa

Puede utilizar el comando `vdmadmin` para habilitar la autenticación de clientes que intenten conectarse a sus escritorios remotos a través de la instancia del servidor de conexión de View.

Debe ejecutar el comando `vdmadmin` en una de las instancias del servidor de conexión de View del grupo que contiene la instancia que los clientes usarán para conectarse a sus escritorios remotos.

Aunque habilite la autenticación para una instancia independiente del servidor de conexión de View, todas sus instancias en el grupo comparten el resto de opciones de configuración para la autenticación de cliente. Solo es necesario agregar una vez una cuenta para un cliente. En un grupo del servidor de conexión de View, cualquier instancia habilitada de dicho servidor puede autenticar el cliente.

Si planea utilizar la pantalla completa con un escritorio de View basado en sesiones de un host RDS, debe agregar también la cuenta de usuario al grupo Usuarios de escritorio remoto.



## Procedimiento

- 1 Habilitar la autenticación de clientes en una instancia del servidor de conexión de View.

```
vdmadmin
-Q
-enable [-bargumentos_autenticación] -s servidor_conexión [-requirepassword]
```

Opción	Descripción
<b>-requirepassword</b>	Especifique que los clientes deben facilitar contraseñas.  <b>Importante</b> Si especifica esta opción, la instancia del servidor de conexión de View no puede autenticar clientes que hayan generado contraseñas de forma automática. Si cambia la configuración de una instancia del servidor de conexión de View para especificar esta opción, dichos clientes no podrán autenticarse ellos mismos y obtendrán el mensaje de error Nombre de usuario desconocido o contraseña incorrecta.
<b>-s servidor_conexión</b>	Especifique el nombre NetBIOS de la instancia del servidor de conexión de View donde se habilitará la autenticación de clientes.

El comando habilita la instancia especificada del servidor de conexión de View para autenticar clientes.

- 2 Si un host RDS de Microsoft proporciona el escritorio remoto, inicie sesión en el host RDS y agregue la cuenta de usuario al grupo Usuarios de escritorio remoto.

Por ejemplo, supongamos que, en View Server, permite a la cuenta de usuario custom-11 utilizar un escritorio de View basado en sesiones de un host RDS. Debe iniciar sesión después en el host RDS y agregar el usuario custom-11 al grupo Usuarios de escritorio remoto desde el **Panel de control > Sistema y seguridad > Sistema > Configuración remota > Seleccionar usuarios > Agregar**.

## Ejemplo: Habilitar la autenticación de clientes en modo de pantalla completa

Habilite la autenticación de clientes en la instancia csvr-2 del servidor de conexión de View. 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 de View y solicite al cliente que especifique sus contraseñas en Horizon Client. Los clientes con contraseñas generadas de forma automática no pueden autenticarse por sí solos.

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

## Pasos siguientes

Compruebe la configuración de las instancias del servidor de conexión de View y los clientes.

## Verificar la configuración de los clientes en modo de pantalla completa

Puede usar el comando `vdadmin` para mostrar información sobre los clientes en modo de pantalla completa y las instancias del servidor de conexión de View que se configuraron para autenticar dichos clientes.

Debe ejecutar el comando `vdadmin` en una de las instancias del servidor de conexión de View del grupo que contiene la instancia que los clientes usarán para conectarse a sus escritorios remotos.

### Procedimiento

- ◆ Visualice la información sobre los clientes en modo de pantalla completa y la autenticación de los clientes.

```
vdadmin
-Q
-clientauth
-list [-b argumentos_autenticación] [-xml]
```

El comando muestra información sobre los clientes en modo de pantalla completa y las instancias del servidor de conexión de View en la que habilitó la autenticación del cliente.

### Ejemplo: Mostrar la información de los clientes en modo de pantalla completa

Muestra la información sobre los clientes en formato de texto. El cliente `cm-00_0c_29_0d_a3_e6` tiene una contraseña generada de forma automática y no requiere un script de una aplicación o un usuario final para especificar esta contraseña a Horizon Client. El cliente `cm-00_22_19_12_6d_cf` tiene una contraseña especificada explícitamente y requiere que el usuario final la proporcione. La instancia del servidor de conexión de View `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:\> vdadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
Domain              : myorg.com
Password Generated: true

GUID                : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID            : cm-00_22_19_12_6d_cf
Domain              : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name          : CONSVR1
Client Authentication Enabled : false
```

```
Password Required      : false
Common Name           : CONSVR2
Client Authentication Enabled : true
Password Required      : false
```

### Pasos siguientes

Compruebe que los clientes se puedan conectar a los escritorios remotos.

## Conectarse a escritorios remotos desde clientes en modo de pantalla completa

Puede ejecutar el cliente desde una línea de comandos o usar un script para conectar un cliente a una sesión remota.

Lo habitual es usar un script de comandos para ejecutar Horizon Client en un dispositivo cliente implementado.

---

**Nota** En un cliente Mac o Windows, los dispositivos USB no se reenvían automáticamente de forma predeterminada si otra aplicación u otro servicio los están utilizando cuando se inicia la sesión del escritorio remoto. En todos los clientes, los dispositivos de interfaz de usuario (HID) y los lectores de tarjetas inteligentes no se reenvían de forma predeterminada.

---

## Procedimiento

- ◆ Para conectarse a una sesión remota, introduzca el comando apropiado según la plataforma que utilice.

Opción	Descripción
Windows	<p>Introduzca</p> <pre>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL <i>servidor_conexión</i>] [-userName <i>nombre_usuario</i>] [-password <i>contraseña</i>]</pre> <p><b>-password</b><i>contraseña</i> Especifica la contraseña para la cuenta del cliente. Si definió una contraseña para la cuenta, debe especificarla.</p> <p><b>-serverURL</b><i>servidor_conexión</i> Especifica la dirección IP o el FQDN de la instancia del servidor de conexión de View que Horizon Client usará para conectarse al escritorio. Si no especifica la dirección IP o el FQDN de la instancia del servidor de conexión de View que el cliente usará para conectarse al escritorio remoto, el cliente usa la instancia predeterminada del servidor de conexión de View que configuró para ello.</p> <p><b>-userName</b><i>nombre_usuario</i> Especifica el nombre de la cuenta del cliente. Si desea que un cliente se autentique con un nombre de cuenta que comienza con una cadena de prefijo reconocida, como "custom-", en lugar de usar la dirección MAC, debe especificar este nombre.</p>
Linux	<p>Introduzca</p> <pre>vmware-view --unattended -s <i>servidor_conexión</i> [--once] [-u <i>nombre_usuario</i>] [-p <i>contraseña</i>]</pre> <p><b>--once</b> Especifica que no desea que Horizon Client vuelva a intentar conectarse si se produce un error.</p> <p><b>Importante</b> Normalmente, es necesario que especifique esta opción y que use el código de salida para solucionar el error. De lo contrario, será difícil terminar el proceso vmware-view de forma remota.</p> <p><b>-p</b><i>contraseña</i> Especifica la contraseña para la cuenta del cliente. Si definió una contraseña para la cuenta, debe especificarla.</p> <p><b>-s</b><i>servidor_conexión</i> Especifica la dirección IP o el FQDN de la instancia del servidor de conexión de View que el cliente usará para conectarse al escritorio.</p> <p><b>-u</b><i>nombre_usuario</i> Especifica el nombre de la cuenta del cliente. Si desea que un cliente se autentique con un nombre de cuenta que comienza con una cadena de prefijo reconocida, como "custom-", en lugar de usar la dirección MAC, debe especificar este nombre.</p>

Si el servidor autentica el cliente en modo de pantalla completa y un escritorio remoto está disponible, el comando inicia la sesión remota.

## Ejemplo: Ejecutar Horizon Client en clientes en modo de pantalla completa

Ejecute Horizon Client en un cliente Windows cuyo nombre de cuenta esté basado en su dirección MAC y que tenga una contraseña generada automáticamente.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL  
consvr2.myorg.com
```

Ejecute Horizon Client en un cliente Linux utilizando una contraseña y un nombre asignados.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

# Solucionar problemas relacionados con View

# 14

Existen varios procedimientos para diagnosticar y arreglar los problemas que pueda encontrar cuando utilice View. Puede utilizar estos procedimientos para investigar las causas de los problemas e intentar corregirlos usted mismo, o bien puede solicitar ayuda al equipo de asistencia técnica de VMware.

Para obtener información sobre la solución de problemas relacionados con los escritorios y grupos de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7*.

Este capítulo incluye los siguientes temas:

- [Supervisar el estado del sistema](#)
- [Supervisar eventos en View](#)
- [Recopilar información de diagnóstico para View](#)
- [Actualizar las solicitudes de soporte](#)
- [Solucionar un emparejamiento de servidor de seguridad con el servidor de conexión de View que no se realizó correctamente](#)
- [Solucionar problemas relacionados con la comprobación de revocación de certificados de View Server](#)
- [Solucionar problemas relacionados con la comprobación de revocación de la tarjeta inteligente](#)
- [Más información para solucionar problemas](#)

## Supervisar el estado del sistema

Puede usar el panel de control del estado del sistema en View Administrator para ver rápidamente los problemas que puedan afectar la operación de View o el acceso de los usuarios finales a los escritorios remotos.

El panel de control del estado del sistema que aparece en la parte superior izquierda de la pantalla de View Administrator proporciona un número de vínculos que puede usar para ver informes sobre la operación de View:

<b>Sesiones</b>	Proporciona un vínculo a la pantalla Sesiones, donde aparece información sobre el estado de las sesiones de las aplicaciones y los escritorios remotos.
<b>Máquinas virtuales de vCenter con problemas</b>	Proporciona un vínculo a la pantalla Máquinas, donde aparece información sobre las máquinas virtuales de vCenter, los hosts RDS y otras máquinas que View marcó con problemas.
<b>Host RDS con problemas</b>	Proporciona un vínculo a la pestaña <b>Host RDS</b> en la pantalla Máquinas, donde aparece información sobre los hosts RDS que View marcó con problemas.
<b>Eventos</b>	Proporciona vínculos a la pantalla Eventos filtrada por los eventos de error y los eventos de advertencia.
<b>Estado del sistema</b>	Proporciona vínculos a la pantalla Panel, donde aparecen resúmenes del estado de los componentes de View, los componentes vSphere, los dominios, los escritorios y el uso del almacén de datos.

El panel de control del estado del sistema muestra un vínculo numerado con cada elemento. Este valor indica el número de elementos sobre los que el informe vinculado proporciona información.

## Supervisar eventos en View

La base de datos de los eventos almacena información sobre los eventos que tienen lugar en el grupo o el host del servidor de conexión de View, en Horizon Agent y en View Administrator y le notifica el número de eventos del panel de control. Puede examinar todos los detalles de los eventos en la pantalla Eventos.

---

**Nota** Los eventos aparecen en la interfaz de View Administrator durante un periodo de tiempo limitado. Después, los eventos solo están disponibles en las tablas históricas de la base de datos. Puede usar las herramientas de informe de la base de datos de Oracle o Microsoft SQL Server para examinar los eventos de las tablas de la base de datos. Para obtener más información, consulte el documento *Integración de View*.

---

Además de supervisar eventos en View Administrator, puede generar los eventos de View en formato syslog para que los software de análisis puedan acceder a la información de los eventos. Consulte [Generar mensajes de registro de eventos de View en formato syslog con la opción -l](#) y cómo configurar los registros de eventos para los servidores syslog en el documento *Instalación de View*.

### Requisitos previos

Cree y configure la base de datos de eventos como aparece descrito en el documento *Instalación de View*.

## Procedimiento

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

## Mensajes de eventos de View

View 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.

[Tabla 14-1. Tipos de eventos notificados por View](#) muestra los tipos de eventos sobre los que informa View.

**Tabla 14-1. Tipos de eventos notificados por View**

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 View.
Error	Notifica que View no realizó una operación correctamente.
Información	Notifica las operaciones normales de View.
Advertencia	Notifica problemas menores con las opciones de configuración o de operación que pueden derivar a problemas más graves con el tiempo.

Es posible que sea necesario realizar alguna acción si aparecen mensajes relacionados con Error de auditoría, Error o Eventos de advertencia. No es necesario que realice ninguna acción cuando aparecen eventos de Información o de Auditoría correcta.

## Recopilar información de diagnóstico para View

Puede recopilar información de diagnóstico para ayudar al equipo de soporte técnico de VMware a diagnosticar y resolver problemas con View.

Puede recopilar información de diagnóstico para varios componentes de View. La forma de recopilar dicha información varía en función del componente de View.

### ■ [Crear un paquete de herramientas de recopilación de datos para Horizon Agent](#)

Para ayudar al equipo de soporte técnico de VMware a solucionar los problemas de Horizon Agent, es posible que necesite usar el comando `vdmaadmin` para crear un paquete de herramientas de recopilación de datos (DCT). También puede obtener el paquete DCT de forma manual sin usar `vdmaadmin`.

### ■ [Guardar información de diagnóstico de Horizon Client](#)

Si al utilizar Horizon Client encuentra problemas que no puede solucionar con las técnicas generales, puede guardar una copia de los archivos de registro y la información de la configuración.



- [Recopilar información de diagnóstico de View Composer con el script de soporte](#)

Puede usar el script de soporte de View Composer para recopilar datos de configuración y generar archivos de registro de View Composer. Esta información ayuda al equipo de asistencia al cliente de VMware a diagnosticar cualquier problema que se produzca con View Composer.

- [Recopilar información de diagnóstico del servidor de conexión de Horizon](#)

Puede usar la herramienta de soporte para establecer niveles de registro y generar archivos de registro del servidor de conexión de Horizon.

- [Recopilar información de diagnóstico de Horizon Agent, de Horizon Client o del servidor de conexión de Horizon desde la consola](#)

Si cuenta con acceso directo a la consola, puede usar los scripts de soporte para generar archivos de registro del servidor de conexión, de Horizon Client o de los escritorios remotos que ejecutan Horizon Agent. Esta información ayuda al equipo de asistencia técnica de VMware a diagnosticar cualquier problema que se produzca con estos componentes.

## Crear un paquete de herramientas de recopilación de datos para Horizon Agent

Para ayudar al equipo de soporte técnico de VMware a solucionar los problemas de Horizon Agent, es posible que necesite usar el comando `vdmdadmin` para crear un paquete de herramientas de recopilación de datos (DCT). También puede obtener el paquete DCT de forma manual sin usar `vdmdadmin`.

Para su comodidad, puede usar el comando `vdmdadmin` en una instancia del servidor de conexión de View para solicitar un paquete DCT desde un escritorio remoto. El paquete se devuelve al servidor de conexión de View.

Puede iniciar sesión de forma alternativa en un escritorio remoto específico y ejecutar un comando `support` que cree el paquete DCT en ese escritorio. Si Control de cuentas de usuario (UAC) está activado, debe obtener el paquete DCT de esta manera.

### Procedimiento

- 1 Inicie sesión como un usuario con los privilegios necesarios.

Opción	Acción
En el servidor de conexión de View, con <code>vdmdadmin</code>	Inicie sesión en el servidor de conexión de View estándar o réplica como un usuario con la función <b>Administradores</b> .
En el escritorio remoto	Inicie sesión en el escritorio remoto como un usuario con privilegios administrativos.

- 2 Abra una ventana de símbolo de sistema y ejecute el comando para generar el paquete DCT.

Opción	Acción
En el servidor de conexión de View, con vdmadmin	<p>Para especificar los nombres en el archivo del paquete de salida, el grupo de escritorios y el equipo, use las opciones <code>-outfile</code>, <code>-d</code> y <code>-m</code> con el comando <code>vdmadmin</code>.</p> <pre>vdmadmin-A [-bargumentos_autenticación] -getDCT-outfilearchivo_local-descriptorio -mequipo</pre>
En el escritorio remoto	<p>Cambie los directorios a <code>c:\Program Files\VMware\VMware View\Agent\DCT</code> y ejecute el siguiente comando:</p> <pre>support</pre>

El comando registra el paquete en el archivo de salida especificado.

### Ejemplo: Usar vdmadmin para crear un archivo de paquete para Horizon Agent

Cree el paquete DCT para la máquina `machine1` en el grupo de escritorios `dtpool2` y regístrelo en el archivo zip `C:\myfile.zip`.

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

#### Pasos siguientes

Si tiene una solicitud de soporte ya existente, puede actualizarla adjuntando el archivo del paquete DCT.

## Guardar información de diagnóstico de Horizon Client

Si al utilizar Horizon Client encuentra problemas que no puede solucionar con las técnicas generales, puede guardar una copia de los archivos de registro y la información de la configuración.

Puede intentar solucionar los problemas de conexión de Horizon Client antes de guardar la información de diagnóstico y contactar con el equipo de soporte técnico de VMware. Para obtener más información, consulte "Problemas de conexión entre Horizon Client y el servidor de conexión de Horizon" en el documento *Configurar escritorios virtuales en Horizon 7*.

#### Procedimiento

- 1 En Horizon Client, haga clic en **Información de soporte técnico** o bien seleccione **Opciones > Información de soporte técnico** en el menú del escritorio remoto.
- 2 En la ventana **Información de soporte**, haga clic en **Recopilar datos del soporte técnico** y haga clic en **Sí** cuando se le solicite.

El progreso de recopilación de información se mostrará en una ventana de comandos. Este proceso puede tardar varios minutos.

- 3 En la ventana de comandos, para responder a las solicitudes, introduzca las URL de las instancias del servidor de conexión de Horizon en las que quiere probar la configuración de Horizon Client y, si es necesario, seleccione la opción para generar los volcados del diagnóstico de los procesos de Horizon 7.

La información se escribe en un archivo zip dentro de una carpeta del escritorio del equipo cliente.

- 4 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte el archivo zip de salida.

## Recopilar información de diagnóstico de View Composer con el script de soporte

Puede usar el script de soporte de View Composer para recopilar datos de configuración y generar archivos de registro de View Composer. Esta información ayuda al equipo de asistencia al cliente de VMware a diagnosticar cualquier problema que se produzca con View Composer.

### Requisitos previos

Inicie sesión en el equipo en el que View Composer está instalado.

Como debe utilizar la utilidad Windows Script Host (cscript) para ejecutar el script de soporte, familiarícese con ella usando cscript. Consulte <http://technet.microsoft.com/library/bb490887.aspx>.

### Procedimiento

- 1 Abra una ventana de símbolo del sistema y cambie el directorio C:\Program Files\VMware\VMware View Composer.

Si no instaló el software en los directorios predeterminados, sustituya la ruta y la letra de la unidad que correspondan.

- 2 Escriba el comando para ejecutar el script svi-support.

```
cscript ".\svi-support.wsf" /zip
```

Puede usar la opción /? para visualizar información sobre otras opciones de comandos que están disponibles con el script.

Cuando el script finalice, le informa del nombre y la ubicación del archivo de salida.

- 3 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte el archivo de salida.

## Recopilar información de diagnóstico del servidor de conexión de Horizon

Puede usar la herramienta de soporte para establecer niveles de registro y generar archivos de registro del servidor de conexión de Horizon.

La herramienta de soporte recopila datos de registro del servidor de conexión. Esta información ayuda al equipo de asistencia técnica de VMware a diagnosticar cualquier problema que se produzca con el servidor de conexión. La herramienta de soporte no está destinada a recopilar información de Horizon Client o de Horizon Agent. En su lugar debe usar el script de soporte. Consulte [Recopilar información de diagnóstico de Horizon Agent, de Horizon Client o del servidor de conexión de Horizon desde la consola](#).

### Requisitos previos

Inicie sesión en la instancia del servidor de conexión estándar o réplica como un usuario con la función **Administradores**.

### Procedimiento

- 1 Seleccione **Inicio > Todos los programas > VMware > Establecer los niveles del servidor de conexión de View**.
- 2 En el cuadro de texto **Elección**, escriba un valor numérico para establecer el nivel de registro y pulse Intro.

Opción	Descripción
0	Restablece el nivel de registro al valor predeterminado.
1	Selecciona un nivel normal de registro.
2	Selecciona un nivel de depuración de registro (predeterminada).
3	Selecciona un registro completo.

El sistema comienza a recopilar información de registro con el nivel de detalle que seleccionó.

- 3 Cuando recopile información suficiente sobre el comportamiento del servidor de conexión, seleccione **Inicio > Todos los programas > VMware > Generar paquete de registro del servidor de conexión de View**.

La herramienta de soporte crea los archivos de registro en una carpeta denominada vdm-sdct en el escritorio de la instancia del servidor de conexión.

- 4 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte los archivos de salida.

## Recopilar información de diagnóstico de Horizon Agent, de Horizon Client o del servidor de conexión de Horizon desde la consola

Si cuenta con acceso directo a la consola, puede usar los scripts de soporte para generar archivos de registro del servidor de conexión, de Horizon Client o de los escritorios remotos que ejecutan Horizon Agent. Esta información ayuda al equipo de asistencia técnica de VMware a diagnosticar cualquier problema que se produzca con estos componentes.

## Requisitos previos

Inicie sesión en el sistema en el que quiere recopilar información. Debe iniciar sesión como un usuario con privilegios de administrador.

- Para Horizon Agent, inicie sesión en la máquina virtual que tenga Horizon Agent instalado.
- Para Horizon Client, inicie sesión en el sistema con Horizon Client instalado.
- Para el servidor de conexión, inicie sesión en el host del servidor de conexión.

## Procedimiento

- 1 Abra una ventana de símbolo del sistema y cambie al directorio apropiado de los componentes de Horizon 7 de los que desee recopilar información de diagnóstico.

Opción	Descripción
<b>Horizon Agent</b>	Cambiar al directorio C:\Program Files\VMware View\Agent\DCT.
<b>Horizon Client</b>	Cambiar al directorio C:\Program Files\VMware View\Client\DCT.
<b>Servidor de conexión de View</b>	Cambiar al directorio C:\Program Files\VMware View\Server\DCT.

Si no instaló el software en los directorios predeterminados, sustituya la ruta y la letra de la unidad que correspondan.

- 2 Escriba el comando para ejecutar el script de soporte.

```
.\support.bat [loglevels]
```

Si desea habilitar el inicio de sesión avanzado, especifique la opción `loglevels` e introduzca el valor numérico del nivel de registro cuando se solicite.

Opción	Descripción
<b>0</b>	Restablece el nivel de registro al valor predeterminado.
<b>1</b>	Selecciona un nivel normal de registro.
<b>2</b>	Selecciona un nivel de depuración de registro (predeterminada).
<b>3</b>	Selecciona un registro completo.
<b>4</b>	Selecciona el registro informativo de PColP (únicamente Horizon Agent y Horizon Client).
<b>5</b>	Selecciona el registro de depuración de PColP (únicamente Horizon Agent y Horizon Client).
<b>6</b>	Selecciona el registro informativo de los canales virtuales (únicamente Horizon Agent y Horizon Client).
<b>7</b>	Selecciona el registro de depuración de los canales virtuales (únicamente Horizon Agent y Horizon Client).
<b>8</b>	Selecciona el registro de seguimiento de los canales virtuales (únicamente Horizon Agent y Horizon Client).

El script crea los archivos de registros comprimidos en la carpeta `vdm-sdct` del escritorio.

- 3 Puede encontrar los registros del agente invitado de View Composer en el directorio C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support.
- 4 Registre una solicitud de soporte en la página Soporte del sitio web de VMware y adjunte el archivo de salida.

## Actualizar las solicitudes de soporte

Puede actualizar la solicitud de soporte existente en el sitio web Soporte.

Después de registrar una solicitud de soporte, es posible que reciba una solicitud por correo electrónico del equipo de soporte técnico de VMware en la que le pidan el archivo de salida de los scripts support o svi-support. Cuando ejecuta los scripts, obtiene información sobre el nombre y la ubicación del archivo de salida. Responda al mensaje y adjunte a la respuesta el archivo de salida.

Si el archivo de salida es demasiado grande para incluirlo como archivo adjunto (10 MB o más), póngase en contacto con el equipo de soporte técnico de VMware, dígales el número de la solicitud de soporte y solicite instrucciones para cargarlo por FTP. De forma alternativa, puede adjuntar el archivo a la solicitud de soporte existente a través del sitio web de Soporte.

### Procedimiento

- 1 Visite la página Soporte en el sitio web de VMware e inicie sesión.
- 2 Haga clic en **Historial de solicitudes de soporte** y busque el número de solicitud de soporte aplicable.
- 3 Actualice la solicitud de soporte y adjunte el archivo saliente que obtuvo al ejecutar los scripts support o svi-support.

## Solucionar un emparejamiento de servidor de seguridad con el servidor de conexión de View que no se realizó correctamente

Es posible que un servidor de seguridad no funcione si no se emparejó correctamente con una instancia del servidor de conexión de View.

### Problema

Pueden producirse los siguientes problemas del servidor de seguridad si no se empareja correctamente con un servidor de conexión de View:

- Cuando intenta instalar el servidor de seguridad por segunda vez, este no puede conectarse al servidor de conexión de View.
- Horizon Client no puede conectarse a View. Aparece el siguiente mensaje de error: Se produjo un error en la autenticación del servidor de conexión de View. Ninguna puerta de enlace está disponible para proporcionar una conexión segura a un escritorio. Póngase en contacto con su administrador de red.

- El servidor de seguridad aparece en el panel de control de View Administrator como Fuera de servicio.

### Causa

Este problema se puede producir si comenzó a instalar un servidor de seguridad y se canceló o se anuló el proceso después de introducir una contraseña de emparejado del servidor de seguridad.

Si tiene pensado mantener el servidor de seguridad en el entorno de View, siga estos pasos:

- 1 En View Administrator, seleccione **Configuración de View > Servidores**.
- 2 En la pestaña **Servidores de seguridad**, seleccione un servidor de seguridad; a continuación, seleccione **Preparar para la actualización o para la reinstalación** en el menú desplegable **Más comandos** y haga clic en **Aceptar**.
- 3 En la pestaña **Servidores de conexión**, seleccione la instancia del servidor de conexión de View que desee emparejar con el servidor de seguridad, seleccione **Especificar contraseña para emparejar al servidor de seguridad** en el menú desplegable **Más comandos**, escriba una contraseña y haga clic en **Aceptar**.
- 4 Vuelva a instalar el servidor de seguridad.

Si pretende eliminar la entrada del servidor de seguridad del entorno de View, ejecute el comando `vdmadmin -S`.

Por ejemplo: `vdmadmin -S -r -s nombre_servidor_seguridad`

## Solucionar problemas relacionados con la comprobación de revocación de certificados de View Server

Un servidor de seguridad o una instancia del servidor de conexión de View que se utilice para conexiones de Horizon Client seguras aparecerá en rojo en View Administrator si la comprobación de revocación de certificados no se puede realizar en el certificado SSL del servidor.

### Problema

El icono del servidor de seguridad o del servidor de conexión de View aparece en color rojo en el panel de control de View Administrator. El estado del servidor de View muestra el siguiente mensaje: El certificado del servidor no se puede comprobar.

### Causa

La comprobación de revocación de certificados puede fallar si la organización utiliza un servidor proxy para acceder a Internet o si la instancia del servidor de conexión de View no puede alcanzar los servidores que ofrecen la comprobación de revocación debido al firewall u otros controles.

Una instancia del servidor de conexión de View comprueba la revocación de certificados en su propio certificado y en los servidores de seguridad emparejados. De forma predeterminada, el servicio del servidor de conexión de VMware Horizon View se inicia con la cuenta LocalSystem. Al ejecutarse con LocalSystem, la instancia del servidor de conexión de View no puede utilizar la configuración de proxy de Internet Explorer para acceder a la URL de puntos de distribución de listas de revocación de certificados o al respondedor OCSP para determinar el estado de revocación del certificado.

Puede utilizar el comando Netshell de Microsoft para importar la configuración de proxy a la instancia del servidor de conexión de View y que así el servidor pueda acceder a los sitios de comprobación de revocación de certificados en Internet.

### Solución

- 1 En el equipo del servidor de conexión de View, abra una ventana de línea de comando con la opción **Ejecutar como administrador**.

Por ejemplo: haga clic en **Iniciar**, escriba **cmd**, haga clic con el botón secundario en el icono **cmd.exe** y seleccione **Ejecutar como administrador**.

- 2 Escriba **netsh** y pulse Intro.
- 3 Escriba **winhttp** y pulse Intro.
- 4 Escriba **show proxy** y pulse Intro.

Netshell muestra que la conexión del proxy se configuró como DIRECT. Con esta configuración, el equipo del servidor de conexión de View no puede conectarse a Internet si la organización está usando el proxy.

- 5 Configure las opciones del proxy.

Por ejemplo: en la solicitud **netsh winhttp>**, escriba **import proxy source=ie**.

La configuración del proxy se importa al equipo del servidor de conexión de View.

- 6 Escriba **show proxy** para comprobar la configuración del proxy.
- 7 Reinicie el servicio del servidor de conexión VMware Horizon View.
- 8 En el panel de control de View Administrator, compruebe que el icono del servidor de conexión de View o del servidor de seguridad aparezca en verde.

## Solucionar problemas relacionados con la comprobación de revocación de la tarjeta inteligente

La instancia del servidor de conexión de View o el servidor de seguridad que tengan la tarjeta inteligente conectada no pueden realizar comprobaciones de revocación del certificado a menos que configurara la comprobación de revocación del certificado de la tarjeta inteligente.



## Problema

Se puede producir un error en la comprobación de revocación de certificados si la organización utiliza un servidor proxy para acceder a Internet, o bien si una instancia del servidor de conexión de View o el servidor de seguridad no puede acceder a los servidores que ofrecen la comprobación de revocación debido al firewall u otros controles.

---

**Importante** Asegúrese de que el archivo CRL esté actualizado.

---

## Causa

View admite la comprobación de revocación de certificados con listas de revocación de certificados (CRL) y con el protocolo de estado de certificado en línea (OCSP). Una CRL es una lista de certificados revocados publicada por la autoridad de certificación (CA) que los emitió. OCSP es un protocolo de validación de certificados que se utiliza para obtener el estado de revocación de un certificado X.509. Es necesario que se pueda acceder a la CA desde el host del servidor de conexión de View o del servidor de seguridad. Este problema puede ocurrir si configuró la comprobación de revocación de los certificados de tarjetas inteligentes. Consulte [Uso de la comprobación de revocación de certificados de tarjeta inteligente](#).

## Solución

- 1 Cree su propio procedimiento (manual) para descargar y actualizar la CRL en una ruta de View Server desde el sitio web de la CA que utiliza.
- 2 Cree o edite el archivo `locked.properties` en la carpeta de configuración de la puerta de enlace SSL en el host del servidor de seguridad o el servidor de conexión de View.  
  
Por ejemplo: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 3 Agregue las propiedades `enableRevocationChecking` y `crlLocation` en el archivo `locked.properties` de la ruta local donde la CRL está almacenada.
- 4 Reinicie el servicio del servidor de conexión de View o el servicio del servidor de seguridad para que se apliquen los cambios.

## Más información para solucionar problemas

Puede encontrar más información para solucionar problemas en los artículos de la base de conocimientos de VMware.

La base de conocimientos de VMware (KB) se actualiza de forma continua con nueva información para solucionar los problemas de los productos de VMware.

Para obtener más información sobre cómo solucionar los problemas de View, consulte los artículos de la KB que están disponibles en el sitio web de la KB de VMware:

<http://kb.vmware.com/selfservice/microsites/microsite.do>

## Usar el comando vdmadmin

Puede usar la interfaz de línea de comandos `vdmadmin` para realizar varias tareas de administración en una instancia del servidor de conexión de View.

Puede usar `vdmadmin` para realizar tareas de administración que no se puedan hacer desde la interfaz de usuario de View Administrator o para realizar tareas de administración que se tengan que ejecutar automáticamente desde scripts.

Para obtener una comparación de las operaciones que se pueden realizar con View Administrator, con cmdlets de View y con `vdmadmin`, consulte el documento *Integración de View*.

- **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.

- **Establecer el nombre del grupo del servidor de conexión de View con la opción -C**

El comando `vdmadmin` con la opción `-C` permite establecer el nombre de un grupo del servidor de conexión de View. La consola de Microsoft System Center Operations Manager (SCOM) muestra este nombre para ayudarle a identificar el grupo dentro de SCOM.

- **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 View y para mostrar los detalles de una instancia específica de supervisión o de supervisión de estado.

- **Especificar y visualizar informes sobre el funcionamiento de View con la opción -I**

Puede usar el comando `vdmadmin` con la opción `-I` para mostrar los informes disponibles sobre el funcionamiento de View y los resultados tras ejecutar uno de dichos informes.

- **Generar mensajes de registro de eventos de View en formato syslog con la opción -I**

Puede usar el comando `vdadmin` con la opción `-I` para registrar mensajes de eventos de View 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 View 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 de View 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 de View 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 de View o del servidor de seguridad de la configuración de View.

- [Proporcionar credenciales secundarias para los administradores con la opción -T](#)

Puede usar el comando `vdmadmin` 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 colisiones de entradas LDAP usando la opción -X](#)

Puede usar el comando `vdmadmin` con la opción `-X` para detectar y resolver las entradas LDAP en conflicto en las instancias del servidor de conexión de View replicadas en un grupo.

## Uso del comando `vdmadmin`

La sintaxis de los comandos de `vdmadmin` controla su funcionamiento.

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

```
vdmadmin
opción_comando [opción_adicionalargumento] ...
```

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.

View Administrator permite asignar la función **de administradores** a un usuario. Consulte [Capítulo 6 Configurar la administración delegada basada en funciones](#).

Si inició sesión como un usuario con privilegios insuficientes, puede usar la opción `-b` para ejecutar el comando como un usuario al que se le asignara la función **Administradores**, si conoce la contraseña del usuario. Puede especificar la opción `-b` para ejecutar el comando `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.

[Tabla 15-1. Opciones para seleccionar el formato de salida](#) muestra las opciones que el comando `vdadmin` proporciona para designar un 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.

Tabla 15-2. Opciones del comando `vdmadmin` muestra las opciones de comando que puede usar con el comando `vdmadmin` para controlar y examinar la operación de View.

**Tabla 15-2. Opciones del comando `vdmadmin`**

Opción	Descripción
-A	Administra la información que Horizon Agent incluye en los archivos de registro. Consulte <a href="#">Configurar los registros en Horizon Agent con la opción -A</a> . Sobrescribe la dirección IP que envía Horizon Agent. Consulte <a href="#">Sobrescribir direcciones IP con la opción -A</a> .
-C	Establece el nombre de un grupo del servidor de conexión de View. Consulte <a href="#">Establecer el nombre del grupo del servidor de conexión de View con la opción -C</a> .
-F	Actualiza las Entidades de seguridad externa (FSP) en Active Directory para todos los usuarios o para los usuarios especificados. Consulte <a href="#">Actualizar las entidades de seguridad externa con la opción -F</a> .
-H	Muestra información del estado de los servicios de View. Consulte <a href="#">Enumerar y mostrar las supervisiones de estado con la opción -H</a> .
-I	Genera los informes de la operación de View. Consulte <a href="#">Especificar y visualizar informes sobre el funcionamiento de View con la opción -I</a> .
-L	Asigna un escritorio dedicado a un usuario o elimina una asignación. Consulte <a href="#">Asignar máquinas dedicadas usando la opción -L</a> .
-M	Muestra información sobre una máquina virtual o un equipo físico. Consulte <a href="#">Visualizar información sobre las máquinas con la opción -M</a> .
-N	Configura los dominios que un grupo o una instancia del servidor de conexión de View disponen para Horizon Client. Consulte <a href="#">Configurar filtros de dominios con la opción -N</a> .
-O	Muestra los escritorios remotos que están asignados a los usuarios que ya no tienen autorización para usarlos. Consulte <a href="#">Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P</a> .
-P	Muestra las directivas de usuario que están asociadas con los escritorios remotos de los usuarios sin autorización. Consulte <a href="#">Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P</a> .
-Q	Configura la cuenta de Active Directory y la configuración de View de un dispositivo cliente en modo de pantalla completa. Consulte <a href="#">Configurar clientes en modo de pantalla completa con la opción -Q</a> .
-R	Informa sobre el primer usuario que accedió a un escritorio remoto. Consulte <a href="#">Visualizar el primer usuario de un equipo con la opción -R</a> .
-S	Elimina una entrada de la configuración para una instancia del servidor de conexión de View desde la configuración de View. Consulte <a href="#">Eliminar una entrada de una instancia del servidor de conexión de View o del servidor de seguridad con la opción -S</a> .
-T	Proporciona credenciales secundarias de Active Directory para los usuarios administradores. Consulte <a href="#">Proporcionar credenciales secundarias para los administradores con la opción -T</a> .
-U	Muestra información sobre un usuario, incluidas las autorizaciones de escritorio remoto y las asignaciones ThinApp, así como las funciones de Administrador. Consulte <a href="#">Visualizar información sobre los usuarios con la opción -U</a> .
-V	Bloquea o desbloquea las máquinas virtuales. Consulte <a href="#">Bloquear o desbloquear las máquinas virtuales con la opción -V</a> .
-X	Detecta y resuelve las entradas de LDAP duplicadas en las instancias del servidor de conexión de View replicadas. Consulte <a href="#">Detectar y resolver colisiones de entradas LDAP usando la opción -X</a> .

# 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

[Tabla 15-3. Opciones para configurar los registros en Horizon Agent](#) muestra las opciones que puede especificar para configurar los registros en Horizon Agent.

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

Opción	Descripción						
<code>-d escritorio</code>	Especifica el grupo de escritorios.						
<code>-getDCT</code>	Crea un paquete de herramientas de recopilación de datos (DCT) y lo guarda en un archivo local.						
<code>-getlogfile archivo de registro</code>	Especifica el nombre del archivo de registro del que guardar una copia.						
<code>-getloglevel</code>	Muestra el nivel de registro actual de Horizon Agent.						
<code>-getstatus</code>	Muestra el estado de Horizon Agent.						
<code>-getversion</code>	Muestra la versión de Horizon Agent.						
<code>-list</code>	Muestra los archivos de registro de Horizon Agent.						
<code>-m máquina</code>	Especifica la máquina dentro de un grupo de escritorios.						
<code>-outfile archivo_local</code>	Especifica el nombre del archivo local en el que se guarda un paquete DCT o una copia del archivo de registro.						
<code>-setloglevel nivel</code>	<p>Establece el nivel de los registros de Horizon Agent.</p> <table> <tr> <td><b>debug</b></td><td>Registra los eventos de errores, de advertencias y de depuración.</td></tr> <tr> <td><b>normal</b></td><td>Registra los eventos de errores y de advertencias.</td></tr> <tr> <td><b>trace</b></td><td>Registra los eventos informativos, de errores, de advertencias y de depuración.</td></tr> </table>	<b>debug</b>	Registra los eventos de errores, de advertencias y de depuración.	<b>normal</b>	Registra los eventos de errores y de advertencias.	<b>trace</b>	Registra los eventos informativos, de errores, de advertencias y de depuración.
<b>debug</b>	Registra los eventos de errores, de advertencias y de depuración.						
<b>normal</b>	Registra los eventos de errores y de advertencias.						
<b>trace</b>	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.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -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-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 de View. En las configuraciones seguras en las que la instancia del servidor de conexión de View 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

[Tabla 15-4. Opciones para sobrescribir direcciones IP](#) muestra las opciones que puede especificar para sobrescribir direcciones IP.

**Tabla 15-4. Opciones para sobrescribir direcciones IP**

Opción	Descripción
<code>-d escritorio</code>	Especifica el grupo de escritorios.
<code>-i ip_o_dns</code>	Especifica la dirección IP o nombre del dominio que se puede resolver en el DNS.
<code>-m máquina</code>	Especifica el nombre de la máquina en un grupo de escritorios.
<code>-override</code>	Especifica una operación para sobrescribir direcciones IP.
<code>-r</code>	Elimina una dirección IP sobrescrita.

## Ejemplos

Sobrescriba la dirección IP de la máquina machine2 del grupo de escritorios dtpool2.

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

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

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

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

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

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

```
vdmadmin -A -override -r -d dtpool3
```

## Establecer el nombre del grupo del servidor de conexión de View con la opción -C

El comando `vdmadmin` con la opción `-C` permite establecer el nombre de un grupo del servidor de conexión de View. La consola de Microsoft System Center Operations Manager (SCOM) muestra este nombre para ayudarle a identificar el grupo dentro de SCOM.

## Sintaxis

```
vdmadmin
-C [-b argumentos_autenticación] [-c nombredegrupo]
```

## Notas de uso

Debe asignar un nombre a un grupo del servidor de conexión de View si pretende usar SCOM para supervisar y administrar el estado de los componentes de View. View Administrator no muestra el nombre de un grupo. Ejecute el comando de un miembro del grupo al que desee asignarle un nombre.

Si no especifica un nombre para el grupo, el comando devuelve el GUID del grupo al que pertenece la instancia del servidor de conexión de View local. Puede usar el GUID para verificar si una instancia del servidor de conexión de View corresponde a un miembro del mismo grupo del servidor de conexión de View que otra instancia de dicho servidor de conexión.

Para obtener una descripción sobre cómo usar SCOM con View, consulte el documento *Integración de View*.

## Opciones

La opción `-c` especifica el nombre del grupo del servidor de conexión de View. Si no especifica esta opción, el comando devuelve el GUID del grupo.

## Ejemplos

Asigne el nombre VCSG01 a un grupo del servidor de conexión de View.

```
vdadmin -C -c VCSG01
```

Devuelva el GUID del grupo.

```
vdadmin -C
```

## 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 [-bargumentos_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.

```
vdmadmin -F -u EXTERNAL\Jim
```

Actualice las FSP de todos los usuarios en Active Directory.

```
vdmadmin -F
```

## 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 View y para mostrar los detalles de una instancia específica de supervisión o de supervisión de estado.

### Sintaxis

```
vdmadmin
-H [-b argumentos_autenticación] -list-xml [-w | -n]
```

```
vdmadmin
-H [-b argumentos_autenticación] -list-monitorid id_supervisión -xml [-w | -n]
```

```
vdmadmin
-H [-b argumentos_autenticación] -monitorid id_supervisión -instanceid id_instancia -xml [-w | -n]
```

### Notas de uso

[Tabla 15-5. Supervisiones de estado](#) muestra las supervisiones de estado que View usa para supervisar el estado de sus componentes.

**Tabla 15-5. Supervisiones de estado**

Supervisor	Descripción
CBMonitor	Supervisa el estado de las instancias del servidor de conexión de View.
DBMonitor	Supervisa el estado de la base de datos de eventos.
DomainMonitor	Supervisa el estado del dominio local del host del servidor de conexión de View 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, View 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

[Tabla 15-6. Opciones para enumerar y mostrar las supervisiones de estado](#) 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 View con la opción -l

Puede usar el comando `vdadmin` con la opción `-l` para mostrar los informes disponibles sobre el funcionamiento de View y los resultados tras ejecutar uno de dichos informes.

## Sintaxis

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

```
vdmadmin
-I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

## Notas de uso

Puede utilizar el comando para visualizar los informes y vistas disponibles, además de la información que View almacenó para un informe y vista determinados.

También puede utilizar el comando `vdmadmin` con la opción `-I` para generar los mensajes de registro de View en formato `syslog`. Consulte [Generar mensajes de registro de eventos de View en formato syslog con la opción -I](#).

## Opciones

[Tabla 15-7. Opciones para especificar y visualizar informes y vistas](#) 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 yyyy-MM-dd-HH:mm:ss</code>	Especifica un límite superior para la fecha de información que se visualizará.
<code>-list</code>	Enumera los informes y vistas disponibles.
<code>-report <i>report</i></code>	Especifica un informe.
<code>-startdate yyyy-MM-dd-HH:mm:ss</code>	Especifica un límite inferior para la fecha de información que se visualizará.
<code>-view <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 View en formato syslog con la opción -I

Puede usar el comando `vdmadmin` con la opción `-I` para registrar mensajes de eventos de View 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 View en formato syslog. En un archivo syslog, los mensajes del registro de eventos de View 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 View 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 View 5.2 o una versión posterior Consulte "Configurar el registro de eventos para servidor Syslog" en el documento *Instalación de View*.

**Tabla 15-8. Opciones para generar los mensajes del registro de eventos de View en formato syslog**

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

## Ejemplos

Deshabilite la generación de eventos de View en formato syslog.

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

Dirija la salida de syslog de los eventos de View únicamente al sistema local.

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

Dirija la salida de syslog de los eventos de View a una ruta especificada.

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



Dirija la salida de syslog de los eventos de View a una ruta especificada que requiera el acceso por parte de un usuario de dominio autorizado.

```
vdadmin -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 -u dominio\usuario
```

```
vdadmin
-L [-bargumentos_autenticación] -descriptorio [-m máquina | -u dominio\usuario] -r
```

### Notas de uso

View 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 View 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 mientras se está recuperando de la pérdida de datos LDAP de View en una instancia del servidor de conexión de View, o bien cuando desee cambiar la propiedad de una máquina en concreto.

Después de que un usuario se conecte a un escritorio remoto que View asigna desde un grupo dedicado, ese escritorio remoto sigue asignado al usuario durante la sesión de la máquina virtual que aloja el escritorio. Es posible que desee eliminar la asignación de una máquina a un usuario que dejó la organización, que ya no necesite acceso al escritorio o que usará un escritorio en un grupo de escritorios diferente. También puede eliminar las asignaciones de todos los usuarios que tienen acceso a un grupo de escritorios.

**Nota** El comando `vdmadmin -L` no asigna la propiedad de los discos persistentes de View Composer. Para asignar escritorios de clones vinculados con discos persistentes, use la opción del menú **Asignar usuario** en View Administrator o View PowerCLI Update-UserOwnership cmdlet.

Si utiliza `vdmadmin -L` para asignar a un usuario un escritorio de clones vinculados con un disco persistente, se pueden producir resultados inesperados en algunas situaciones. Por ejemplo, si desconecta un disco persistente y lo usa para volver a crear un escritorio, este escritorio no se asigna al propietario del original.

## Opciones

Tabla 15-9. Opciones para asignar escritorios dedicados 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 View 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

[Tabla 15-10. Opciones para visualizar la información sobre las máquinas](#) 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.

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

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

```
vdadmin -M -m machine3 -csv
```

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

El comando `vdadmin` con la opción `-M` permite seleccionar una máquina virtual de clones vinculados en la que realizar una operación de recuperación de espacio de disco. Horizon 7 dirige el host ESXi para recuperar espacio de disco del SO de clones vinculados sin esperar a que el espacio sin utilizar del disco del SO alcance el umbral mínimo que se especifica en Horizon Administrator.

## Sintaxis

```
vdadmin
-M [-b argumentos_autenticación] -d escritorio -m equipo-markForSpaceReclamation
```

## Notas de uso

Con esta opción, puede iniciar la recuperación del espacio de disco en una máquina virtual en concreto para solucionar problemas o para realizar demostraciones.

La recuperación del espacio no se realiza si ejecuta este comando durante un periodo sin disponibilidad.

Para poder recuperar el espacio de disco mediante el comando `vdadmin` con la opción `-M`, se deben cumplir los siguientes requisitos previos:

- Compruebe que Horizon 7 esté usando vCenter Server y ESXi con la versión 5.1 o con una versión posterior.

- Compruebe que la instancia de VMware Tools que se proporciona con vSphere versión 5.1 o posterior está instalada en la máquina virtual.
- Compruebe que la máquina virtual tenga la versión 9 del hardware virtual o una versión posterior.
- En Horizon Administrator, compruebe que la opción **Habilitar recuperación de espacio** esté seleccionada para vCenter Server. Consulte [Permitir que vSphere recupere espacio de disco de máquinas virtuales de clones vinculados](#).
- En Horizon Administrator, compruebe que la opción **Reclamar espacio de disco de la máquina virtual** esté seleccionada para el grupo de escritorios. Consulte la sección sobre cómo recuperar el espacio de disco en los clones vinculados de View Composer en el documento *Configurar escritorios virtuales en Horizon 7*.
- Compruebe que la máquina virtual esté encendida antes de iniciar la operación de recuperación de espacio.
- Compruebe que no se esté aplicando ningún periodo sin disponibilidad. Consulte la sección sobre cómo establecer el acelerador de almacenamiento y las horas sin disponibilidad de recuperación de espacio para los clones vinculados de View Composer en el documento *Configurar escritorios virtuales en Horizon 7*.

## Opciones

Tabla 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.

```
vdadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

## Configurar filtros de dominios con la opción -N

Puede usar el comando `vdadmin` con la opción `-N` para los dominios que View tiene disponibles para los usuarios finales.

## Sintaxis

```
vdadmin
```

```
-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

[Tabla 15-12. Opciones para configurar los filtros de dominios](#) 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.

Opción	Descripción
<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 de View y para el grupo del servidor de conexión de View.
<code>-list -active</code>	Muestra los dominios disponibles para la instancia del servidor de conexión de View 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 de View. Puede especificar la instancia del servidor de conexión de View 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 de View 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 del servidor de conexión de View csvr1.

```
vdadmin -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 de View.

```
vdadmin -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 de View del grupo.

```
C:\ vdadmin -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 :

View limita la búsqueda de dominios en cada host del servidor de conexión de View del grupo para excluir los dominios FARDOM y DEPTX. Los caracteres (\*) junto a la lista de exclusión para CONSVR-1 indican que View 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.

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

Muestra los dominios que están disponibles para View en la instancia del servidor de conexión de View.

```
C:\ vdadmin -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 de View.

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

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

```
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 de View o un servidor de seguridad tienen disponibles para los usuarios finales.



View 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 de View o el servidor de seguridad. En un conjunto de dominios reducido y conectados correctamente, View 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. View 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 de 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 de View 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 de View en la que tenga configurada esta clave.

**Tabla 15-13. Tipos de lista de dominios** 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 View 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 View excluye de los resultados de una búsqueda de dominios. No puede excluir el dominio primario.
Lista de inclusión	Especifica los dominios que View 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. View 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 de View.
- 2 Lista de exclusión configurada para el grupo del servidor de conexión de View.
- 3 Lista de inclusión configurada para la instancia del servidor de conexión de View.
- 4 Lista de inclusión configurada para el grupo del servidor de conexión de View.

View 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, View no incluye ese dominio en la lista de dominios activos.

No puede excluir el dominio primario al que pertenecen el servidor de conexión de View o el servidor de seguridad.

## Ejemplo de filtrado para incluir dominios

Puede utilizar una lista de inclusión para especificar los dominios que View 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 de View 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 de View.

```
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 de View 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
```

View aplica la lista de inclusión a los resultados de una búsqueda de dominios. Si la jerarquía de dominio es muy compleja o la conectividad de red a algunos dominios es de baja intensidad, la búsqueda de dominios puede ser lenta. En esos casos, use la exclusión de búsqueda en su lugar.

## Ejemplo de filtrado para excluir dominios

Puede utilizar una lista de inclusión para especificar los dominios que View excluirá de los resultados de la búsqueda de dominios.

Un grupo de dos instancias del servidor de conexión de View, 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 a fin de que puedan acceder al grupo del servidor de conexión de View en el dominio MYDOM.

Mostrar los dominios activos en ese momento para un miembro del grupo del servidor de conexión de View.

```
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 de View.

```
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 View 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 :
```

View limita la búsqueda de dominios en cada host del servidor de conexión de View del grupo para excluir los dominios FARDOM y DEPTX. Los caracteres (\*) junto a la lista de exclusión para CONSVR-1 indican que View excluye el dominio YOURDOM de los resultados de la búsqueda de dominios en CONSVR-1.

Muestra los dominios activos en ese momento en CONSVR-1.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

Muestra los dominios activos en ese momento en CONSVR-2.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-2)
```

```
=====
```

```
Primary Domain: MYDOM
```

Domain: MYDOM DNS:mydom.mycorp.com  
 Domain: YOURDOM DNS:yourdom.mycorp.com

## Visualizar las máquinas y las directivas de usuarios sin autorización con las opciones -O y -P

Puede usar el comando `vdmadmin` con las opciones `-O` y `-P` para mostrar las directivas y las máquinas virtuales que están asignadas a usuarios que ya no tienen autorización para usar el sistema.

### Sintaxis

```
vdmadmin
-O [-b argumentos_autenticación] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath ruta]]
```

```
vdmadmin
-P [-b argumentos_autenticación] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath ruta]]
```

### Notas de uso

Si revoca una autorización de usuario a una máquina virtual persistente o a un sistema físico, la asignación del escritorio remoto asociado no se revoca automáticamente. Esta condición se puede aceptar si suspendió de forma temporal una cuenta de usuario o si el usuario está ausente durante una larga temporada. Cuando vuelva a habilitar la autorización, el usuario puede continuar con la misma máquina virtual como hacía antes. Si un usuario dejó la organización, los otros usuarios no pueden acceder a la máquina virtual y se considera huérfana. También es posible que desee examinar las directivas que se asignaron a usuarios sin autorización.

### Opciones

[Tabla 15-14. Opciones para visualizar las máquinas y las directivas de usuarios sin autorización](#) 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
<code>-ld</code>	Ordena las entradas de los resultados por máquina.
<code>-lu</code>	Ordena las entradas de los resultados por usuario.
<code>-noxslt</code>	Especifica que las hojas de estilo predeterminadas no se deben aplicar a la salida XML.
<code>-xsltpath ruta</code>	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.xsl	Transforma los informes que contienen una lista de máquinas virtuales sin autorización, agrupadas por usuario o sistema, y que están asignadas a un usuario en ese momento. Esta hoja de estilo es la predeterminada.
unentitled-policies.xsl	Transforma los informes que contienen una lista de máquinas virtuales con directivas en el nivel de usuarios que se aplican a usuarios sin autorización.

## Ejemplos

Visualice las máquinas virtuales que se asignaron a los usuarios sin autorización, agrupadas por máquinas virtuales en formato de texto.

```
vdadmin -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.xsl y redireccione los resultados del archivo uu-output.html.

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

Visualice las directivas de usuario que están asociadas con las máquinas virtuales de los usuarios, agrupadas por escritorio en formato XML con caracteres Unicode.

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

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

```
vdadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > 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

```

vdmadmin
-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"]

```

```

vdmadmin
-Q
-disable [-bargumentos_autenticación] -s servidor_conexión

```

```

vdmadmin
-Q
-enable [-bargumentos_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] [-ouDM] [ -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 de View del grupo que los clientes utilizarán para conectarse a los escritorios remotos.

Al configurar los valores predeterminados sobre la caducidad de la contraseña y afiliación a grupos de Active Directory, estas opciones se comparten con todas las instancias del servidor de conexión de View en un grupo.

Cuando agrega un cliente en modo de pantalla completa, View 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 de View. Evite usar estos prefijos con cuentas normales de usuarios.

Si no especifica un nombre para un cliente, View 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 de View que habilitó para la autenticación de los 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, View 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 de View 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 de View, 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 View 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 de View no puede autenticar clientes que generaron contraseñas de forma automática. Si cambia la configuración de una instancia del servidor de conexión de View para especificar esta opción, dichos clientes no podrán autenticarse y obtendrán el mensaje de error Nombre de usuario desconocido o contraseña incorrecta.

## Opciones

Tabla 15-16. Opciones para configurar clientes en pantalla completa 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 de View 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 de View 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 de View. 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.

Opción	Descripción
<code>-group nombre_grupo</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 de View 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 DN</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 <b>Nota</b> No puede utilizar la opción <code>-setdefaults</code> para cambiar la configuración de una unidad organizativa.
<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. View no aceptará contraseñas generadas para las nuevas conexiones.
<code>-s servidor_conexión</code>	Especifica el nombre NetBIOS de la instancia del servidor de conexión de View donde se habilitará o se deshabilitará la autenticación de clientes en modo de pantalla completa.
<code>-setdefaults</code>	Establece los valores predeterminados que se usan para agregar cuentas cliente.
<code>-update</code>	Actualiza una cuenta de clientes en modo de pantalla completa.

## Ejemplos

Establezca los valores predeterminados de la unidad organizativa, la caducidad de la contraseña y la afiliación a grupos de clientes.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Obtenga los valores predeterminados actuales de los clientes en texto sin formato.

```
vdmadmin -Q -clientauth -getdefaults
```

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

```
vdmadmin -Q -clientauth -getdefaults -xml
```

Agregue una cuenta para un cliente especificado por la dirección MAC al dominio MYORG y use la configuración predeterminada del grupo kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Agregue una cuenta para un cliente especificado por su dirección MAC al dominio MYORG y use una contraseña generada automáticamente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -group kc-grp
```

Agregue una cuenta para un cliente con nombre y especifique la contraseña que se usará con el cliente.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Actualice una cuenta para un cliente especificando una nueva contraseña y un texto descriptivo.

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -description "Foyer Entry Workstation"
```

Elimine la cuenta de un cliente en modo de pantalla completa especificado por su dirección MAC desde el dominio MYORG.

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

Elimine las cuentas de todos los clientes sin solicitar la confirmación de esta acción.

```
vdmadmin -Q -clientauth -removeall -force
```

Habilite la autenticación de clientes en la instancia csvr-2 del servidor de conexión de View. 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 de View y solicite al cliente que especifique 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 de View.

```
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 de View CONSVR2 acepta las solicitudes de autenticación de clientes con contraseñas generadas de forma automática. CONSVR1 no acepta solicitudes de autenticación desde clientes en modo de pantalla completa.

```
C:\> vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
Domain              : myorg.com
Password Generated: true

GUID                : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID            : cm-00_22_19_12_6d_cf
Domain              : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name          : CONSVR1
Client Authentication Enabled : false
Password Required    : false

Common Name          : CONSVR2
Client Authentication Enabled : true
Password Required    : false
```

## Visualizar el primer usuario de un equipo con la opción -R

Puede usar el comando `vdmadmin` con la opción `-R` para encontrar la asignación inicial de una máquina virtual administrada. Por ejemplo, en el caso de perder datos LDAP, es posible que necesite esta información para poder volver a asignar las máquinas virtuales a los usuarios.

**Nota** El comando `vdmadmin` con la opción `-R` funciona únicamente en máquinas virtuales que tienen una versión anterior a View Agent 5.1. En máquinas virtuales que ejecutan View Agent 5.1 y versiones posteriores, así como Horizon Agent 7.0 y versiones posteriores, esta opción no funciona. Para ubicar el primer usuario de una máquina virtual, use la base de datos de eventos para determinar los usuarios que iniciaron sesión en la máquina.

## Sintaxis

```
vdmadmin
-R
-i
```

```
dirección_red
```

## Notas de uso

No puede usar la opción `-b` para ejecutar este comando como un usuario con privilegios. Debe iniciar sesión como un usuario con la función **Administrador**.

## Opciones

La opción `-i` especifica la dirección IP de la máquina virtual.

## Ejemplos

Vea el primer usuario que accedió a la máquina virtual en la dirección IP 10.20.34.120.

```
vdmadmin -R -i 10.20.34.120
```

## Eliminar una entrada de una instancia del servidor de conexión de View o del servidor de seguridad con la opción -S

Puede usar el comando `vdmadmin` con la opción `-S` para eliminar la entrada de la instancia del servidor de conexión de View o del servidor de seguridad de la configuración de View.

## Sintaxis

```
vdmadmin  
-S [-b argumentos_autenticación] -r-s servidor
```

## Notas de uso

Para proporcionar una alta disponibilidad, View le permite configurar una o varias instancias de réplica del servidor de conexión de View en un grupo de servidores de conexión de View. Si deshabilita una instancia del servidor de conexión de View en un grupo, la entrada del servidor se mantiene en la configuración de View.

También puede usar el comando `vdmadmin` con la opción `-S` para eliminar un servidor de seguridad del entorno de View. 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 de View o el servidor de seguridad del equipo Windows Server al ejecutar el instalador del servidor de conexión de View.
- 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 de View, use el comando `vdmadmin` para eliminar la entrada de la instancia del servidor de conexión de View desinstalada o el servidor de seguridad de la configuración.

Si desea volver a instalar View en los sistemas eliminados sin replicar la configuración View del grupo original, reinicie todos los hosts del servidor de conexión de View en el grupo original antes de reinstalar. Esto evita que las instancias del servidor de conexión de View reciban actualizaciones de la configuración desde el grupo original.

## Opciones

La opción `-s` especifica el nombre NetBIOS de la instancia del servidor de conexión de View o el servidor de seguridad que se eliminarán.

## Ejemplos

Elimina la entrada de la instancia del servidor de conexión de View `connsvr3`.

```
vdmadmin -S -r -s connsvr3
```

## Proporcionar credenciales secundarias para los administradores con la opción -T

Puede usar el comando `vdmadmin` con la opción `-T` para proporcionar credenciales secundarias de Active Directory a los usuarios administradores.

## Sintaxis

```
vdmadmin
-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 de View, debe proporcionar credenciales secundarias para los usuarios administradores en View 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 View Administrator, no para escritorios de usuarios finales ni sesiones de aplicaciones. Solo los usuarios administradores necesitan credenciales secundarias.

El comando `vdmadmin` 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. El servidor de conexión de View podrá enumerar a continuación 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)

## 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 View.

- 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.

```
vdadmin -U -u CORP\Jo -n -xml
```

## Bloquear o desbloquear las máquinas virtuales con la opción -V

Puede usar el comando `vdadmin` con la opción `-V` para bloquear o desbloquear las máquinas virtuales en el centro de datos.

### Sintaxis

```
vdadmin
-V [-bargumentos_autenticación] -e-descriptorio-mmáquina [-m máquina] ...
```

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

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

```
vdadmin
-V [-b argumentos_autenticación] -p-vcdndn_vCenter-vmpathruta_inventario
```

### Notas de uso

Solo debe usar el comando `vdadmin` 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

[Tabla 15-18. Opciones para bloquear o desbloquear las máquinas virtuales](#) 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
-d <i>escritorio</i>	Especifica el grupo de escritorios.
-e	Desbloquea una máquina virtual.
-m <i>máquina</i>	Especifica el nombre de la máquina virtual.
-p	Bloquea una máquina virtual.
-vcdn <i>dn_vCenter</i>	Especifica el nombre distintivo de vCenter Server.
-vmopath <i>ruta_inventario</i>	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 colisiones de entradas LDAP usando la opción -X

Puede usar el comando vdmadmin con la opción -X para detectar y resolver las entradas LDAP en conflicto en las instancias del servidor de conexión de View replicadas en un grupo.

## Sintaxis

```
vdmadmin
-X [-bargumentos_autenticación] -collisions [-resolve]
```

## Notas de uso

Si se crean entradas LDAP duplicadas en dos o más instancias del servidor de conexión de View, esto puede causar problemas con la integridad de los datos LDAP en View. Por ejemplo, esta condición se puede producir durante una actualización mientras la replicación LDAP no está operativa. Aunque View busque esta condición de error en intervalos regulares, puede ejecutar el comando vdmadmin en una de las instancia del servidor de conexión de View del grupo para detectar y resolver conflictos de entradas LDAP de forma manual.

## Opciones

[Tabla 15-19. Opciones para detectar y resolver entradas LDAP en conflicto](#) muestra las opciones que puede especificar para detectar y resolver las entradas LDAP en conflicto.

**Tabla 15-19. Opciones para detectar y resolver entradas LDAP en conflicto**

Opción	Descripción
<code>-collisions</code>	Especifica una operación para detectar conflictos de LDAP en el grupo de servidores de conexión de View.
<code>-resolve</code>	Resuelve todos los conflictos LDAP detectados.

## Ejemplos

Detecte los conflictos de entrada LDAP en un grupo del servidor de conexión de View.

```
vdmadmin -X -collisions
```

Detecte y resuelva los conflictos de entradas LDAP.

```
vdmadmin -X -collisions -resolve
```