

# Guía del portal para tenants de vCloud Director

28 de marzo de 2019  
VMware Cloud Director 9.7

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

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

**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 © 2017-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

# Contenido

Guía del portal para tenants de vCloud Director 10

## 1 Introducción al portal para tenants de vCloud Director 11

- Descripción general de VMware vCloud Director 11
- Iniciar sesión en el portal para tenants de vCloud Director 13
- Funciones y derechos del portal para tenants de vCloud Director 13
- Usar el portal para tenants de vCloud Director 14
- Usar la búsqueda global de vCloud Director 15
- Ver tareas 16
- Detener una tarea en curso 17
- Ver eventos 18

## 2 Trabajar con máquinas virtuales 19

- Arquitectura de máquina virtual 20
- Ver y editar máquinas virtuales 21
- Crear una nueva máquina virtual independiente 22
- Abrir una consola de máquina virtual 23
  - Instalar VMware Remote Console en un cliente 23
  - Abrir una consola remota de máquina virtual 24
  - Abrir una consola web 25
- Realizar operaciones de encendido y apagado en las máquinas virtuales 26
  - Encender una máquina virtual 26
  - Apagar una máquina virtual 26
  - Desconectar un sistema operativo invitado 27
  - Restablecer una máquina virtual 27
  - Suspender una máquina virtual 28
  - Descartar el estado suspendido de una máquina virtual 28
- Instalar VMware Tools en una máquina virtual 29
- Actualizar la versión de hardware virtual de una máquina virtual 30
- Editar propiedades de una máquina virtual 31
  - Cambiar las propiedades generales de una máquina virtual 31
  - Cambiar las propiedades de hardware de una máquina virtual 32
  - Cambiar las propiedades de personalización del sistema operativo invitado de una máquina Virtual 35
  - Cambiar las propiedades avanzadas de una máquina virtual 39
- Insertar medios 42
- Expulsar medio 42
- Copiar una máquina virtual en otra vApp 43

Mover una máquina virtual a otra vApp	43
Afinidad y antiafinidad de máquinas virtuales	45
Ver reglas de afinidad y antiafinidad	45
Crear una regla de afinidad	46
Crear una regla de antiafinidad	46
Editar una regla de afinidad o de antiafinidad	47
Eliminar una regla de afinidad o de antiafinidad	47
Supervisar máquinas virtuales	48
Trabajar con instantáneas	49
Tomar una instantánea de una máquina virtual	49
Revertir una máquina virtual a una instantánea	51
Quitar una instantánea de una máquina virtual	51
Renovar una concesión de máquina virtual	52
Eliminar una máquina virtual	52

### 3 Trabajar con vApp 53

Ver vApps	54
Generar una nueva vApp	54
Crear una vApp a partir de un paquete OVF	56
Crear una vApp a partir de una plantilla de vApp	58
Abrir una vApp	59
Realizar operaciones de encendido y apagado en vApps	60
Encender una vApp	60
Apagar una vApp	60
Detener una vApp	61
Restablecer una vApp	61
Suspender una vApp	62
Descartar el estado de suspensión de una vApp	62
Editar propiedades de una vApp	63
Editar las propiedades generales de la vApp	63
Editar las propiedades avanzadas de una vApp	64
Compartir una vApp	65
Mostrar un diagrama de red de vApp	66
Trabajar con redes en una vApp	67
Ver las redes de una vApp	67
Colocar una barrera de red de vApp	68
Agregar una red a una vApp	69
Configuración de servicios de redes para una red de vApp	70
Eliminar una red de vApp	74
Trabajar con instantáneas	75
Tomar una instantánea de una vApp	75

Revertir una vApp a una instantánea	76
Quitar una instantánea de una vApp	77
Cambiar el propietario de una vApp	77
Mover una vApp a otro centro de datos virtual	78
Copiar una vApp detenida en otro centro de datos virtual	78
Copiar una vApp encendida	79
Agregar una máquina virtual a una vApp	80
Guardar una vApp como plantilla de vApp en un catálogo	81
Descargar una vApp como un paquete OVF	82
Renovar una concesión de vApp	83
Eliminar una vApp	83

#### 4 Administrar redes de VDC de organización 85

Ver las redes de VDC de organización disponibles	87
Agregar una red de centros de datos virtuales de organización aislada	88
Agregar una red de centros de datos virtuales de organización enrutada	89
Agregar una red de centros de datos virtuales de organización directa	91
Editar la configuración general de una red de centros de datos virtuales de organización	92
Convertir una red de centros de datos virtuales de organización	93
Convertir la interfaz de una red de VDC de organización enrutada	94
Ver las direcciones IP usadas para una red de centros de datos virtuales de organización	94
Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización	95
Editar o eliminar rangos de IP utilizados en una red de centros de datos virtuales de organización	96
Editar la configuración de DNS de una red de centros de datos virtuales de organización	96
Configurar las opciones de DHCP para una red de centros de datos virtuales de organización aislada	97
Editar o eliminar un grupo DHCP existente para una red	98
Restablecer una red de centros de datos virtuales de organización	99
Eliminar una red de centros de datos virtuales de organización	99

#### 5 Administrar redes entre los centros de datos virtuales 101

Administrar grupos de centros de datos	102
Crear y configurar un grupo de centros de datos con una configuración de salida común	102
Crear y configurar un grupo de centros de datos con una configuración de salida de dominio de error	105
Ver un grupo de centros de datos	107
Agregar un centro de datos virtual a un grupo de centros de datos	108
Eliminar un centro de datos virtual de un grupo de centros de datos	108
Sincronizar un grupo de centros de datos	109

Intercambiar puntos de salida en un grupo de centros de datos con una configuración de salida común	110
Reemplazar la puerta de enlace Edge de un punto de salida	110
Eliminar un punto de salida	111
Sincronizar rutas y puntos de salida	112
Administrar redes extendidas	113
Agregar una red extendida	113
Ver o editar una red extendida	115
Eliminar una red extendida	115
Sincronizar una red extendida	116

## 6 Capacidades de red avanzadas para tenants de vCloud Director 118

Introducción a las redes avanzadas de vCloud Director	119
Configuración de firewall mediante el portal para tenants	120
Firewall de puerta de enlace Edge	121
Administrar un firewall de puerta de enlace Edge	121
Firewall distribuido	125
Habilitar el firewall distribuido en un centro de datos virtual de organización mediante el portal para tenants	126
Administrar reglas de firewall distribuido mediante el portal para tenants	127
Administrar DHCP de puerta de enlace Edge	132
Agregar un grupo de direcciones IP de DHCP	133
Agregar enlaces de DHCP	135
Configurar la retransmisión de DHCP para puertas de enlace Edge	136
Especificar una configuración de retransmisión de DHCP para una puerta de enlace Edge	137
Administrar la traducción de direcciones de red mediante el portal para tenants	138
Agregar una regla SNAT o DNAT	139
Configuración avanzada de enrutamiento	141
Especificar la configuración de enrutamiento predeterminada de la puerta de enlace Edge	142
Agregar una ruta estática	143
Configurar OSPF	144
Configurar un BGP	147
Configurar redistribuciones de rutas	150
Equilibrio de carga	151
Acerca del equilibrio de carga	151
Acceso seguro mediante redes privadas virtuales	166
Configurar VPN-Plus de SSL	167
Configurar VPN de IPsec	181
Configurar VPN de capa 2	188
Quitar la configuración del servicio VPN de capa 2 de una puerta de enlace Edge	193
Administración de certificados SSL	194

Generar una solicitud de firma de certificado para una puerta de enlace Edge	195
Importar el certificado firmado por CA correspondiente a la solicitud CSR generada para una puerta de enlace Edge	196
Configurar un certificado de servicio autofirmado	197
Agregar un certificado de CA a la puerta de enlace Edge para la verificación de confianza de certificados SSL	198
Agregar una lista de revocación de certificados a una puerta de enlace Edge	199
Agregar un certificado de servicio a la puerta de enlace Edge	200
Objetos de agrupamiento personalizados	201
Crear un conjunto de direcciones IP para usarlas en las reglas de firewall y la configuración de retransmisión de DHCP	201
Crear un conjunto de direcciones MAC para utilizarlas en las reglas de firewall	202
Ver los servicios disponibles para reglas de firewall	203
Ver los grupos de servicios disponibles para reglas de firewall	204
Estadísticas y logs para una puerta de enlace Edge	205
Ver estadísticas	205
Habilitar registro	205
Habilitar el acceso de la línea de comandos SSH a una puerta de enlace Edge	207
Trabajar con etiquetas de seguridad	207
Crear y asignar etiquetas de seguridad	208
Cambiar la asignación de etiquetas de seguridad	209
Ver las etiquetas de seguridad aplicadas	210
Editar una etiqueta de seguridad	210
Eliminar una etiqueta de seguridad	211
Trabajar con grupos de seguridad	212
Crear un grupo de seguridad	212
Editar un grupo de seguridad	213
Eliminar un grupo de seguridad	215
<b>7 Usar discos independientes y revisar políticas de almacenamiento</b>	<b>217</b>
Crear y usar discos independientes	217
Crear un disco independiente	217
Editar un disco independiente	218
Eliminar un disco independiente	218
Revisar las propiedades de la política de almacenamiento	219
<b>8 Revisar las propiedades del centro de datos virtual</b>	<b>220</b>
Revisar las propiedades del centro de datos virtual	220
Revisar los metadatos del centro de datos virtual	220
<b>9 Trabajar con SDDC y proxies de SDDC</b>	<b>222</b>
Configurar el navegador con la configuración de proxy	222

[Activar o desactivar un proxy de SDDC](#) 223

[Iniciar sesión en la interfaz de usuario de un componente de SDDC con proxy](#) 224

## **10 Trabajar con plantillas de vApp** 226

[Ver una plantilla de vApp](#) 226

[Crear una plantilla de vApp desde un archivo OVF](#) 227

[Descargar una plantilla de vApp](#) 228

[Eliminar una plantilla de vApp](#) 229

## **11 Trabajar con archivos de medios** 230

[Cargar archivos de medios](#) 230

[Eliminar un archivo de medios](#) 231

[Descargar un archivo de medios](#) 231

## **12 Trabajar con catálogos** 233

[Ver catálogos](#) 234

[Crear un catálogo](#) 234

[Compartir un catálogo](#) 235

[Eliminar un catálogo](#) 236

[Administrar metadatos de un catálogo](#) 237

[Publicar un catálogo](#) 237

[Suscribirse a un catálogo externo](#) 238

[Actualizar la dirección URL de ubicación y la contraseña de un catálogo suscrito](#) 238

[Sincronizar un catálogo suscrito](#) 239

## **13 Trabajar con plantillas de centros de datos virtuales de organización** 241

[Ver plantillas disponibles del centro de datos virtual](#) 241

[Crear un centro de datos virtual a partir de una plantilla](#) 242

## **14 Administración de usuarios, grupos y funciones** 243

[Administración de usuarios](#) 243

[Crear un usuario](#) 243

[Importar usuarios](#) 245

[Modificar un usuario](#) 246

[Deshabilitar o habilitar una cuenta de usuario](#) 246

[Eliminar un usuario](#) 247

[Desbloquear una cuenta de usuario bloqueada](#) 247

[Administración de grupos](#) 248

[Importar un grupo](#) 248

[Eliminar un grupo](#) 248

[Editar un grupo](#) 249



Funciones y derechos	249
Funciones predeterminadas y sus derechos	250
Crear una función de tenant personalizada	259
Editar una función de tenant personalizada	259
Eliminar una función	260
<b>15</b>	<b>Habilitar el uso de un proveedor de identidad SAML en la organización 261</b>
<b>16</b>	<b>Administrar la organización 264</b>
Editar el nombre y la descripción de la organización	264
Modificar la configuración de correo electrónico	265
Probar la configuración SMTP	266
Modificar la configuración de dominio para las máquinas virtuales de la organización	266
Trabajar con varios sitios	267
Configurar y administrar implementaciones multisitio	267
Entender las concesiones	268
Modificar las políticas de concesión de la vApp y la plantilla de vApp dentro de la organización	269
Modificar las cuotas predeterminadas para las máquinas virtuales en la organización	270
Modificar las políticas de cuenta de usuario y contraseña en la organización	271
<b>17</b>	<b>Trabajar con Biblioteca de servicios 272</b>
Buscar un servicio	272
Ejecutar un servicio	273
<b>18</b>	<b>Trabajar con definiciones de entidad personalizada 274</b>
Buscar una entidad personalizada	274
Editar una definición de entidad personalizada	275
Agregar una definición de entidad personalizada	276
Instancias de entidades personalizadas	276
Asociar una acción a una entidad personalizada	277
Anular la asociación de una acción de una entidad personalizada	278
Publicar una entidad personalizada	279
Eliminar una entidad personalizada	279

# Guía del portal para tenants de vCloud Director

La *Guía del portal para tenants de VMware vCloud Director* proporciona información acerca de cómo utilizar el portal para tenants de VMware vCloud Director. En esta versión, utilice el portal para tenants para administrar su organización, crear y configurar máquinas virtuales, vApp y redes dentro de vApp. También puede configurar capacidades de redes avanzadas proporcionadas por VMware NSX<sup>®</sup> for vSphere<sup>®</sup> dentro de un entorno de vCloud Director. En el portal para tenants de vCloud Director, también puede crear y administrar catálogos, vApp y plantillas de VDC, así como crear y administrar redes entre centros de datos virtuales.

## Público objetivo

Esta guía está destinada a quienes deseen utilizar las capacidades que se ofrecen en el portal para tenants de vCloud Director. La información está escrita principalmente para los **administradores de organización** que utilicen el portal para tenants para administrar su organización, máquinas virtuales, vApp, redes, etc.

## Documentación relacionada

Consulte la *Guía del usuario de vCloud Director* para obtener información sobre las funciones y las capacidades disponibles para los administradores de organización mediante la consola web de vCloud Director en lugar de con el portal para tenants de vCloud Director.

## Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware proporciona un glosario de términos con los que puede no estar familiarizado. Para ver las definiciones de los términos que se utilizan en la documentación técnica de VMware, visite <http://www.vmware.com/support/pubs>.

# Introducción al portal para tenants de vCloud Director

# 1

Cuando se inicia sesión en el portal para tenants, se pueden completar una serie de tareas, como la creación de máquinas virtuales y vApps, o la configuración de ajustes de redes avanzadas y la ejecución de flujos de trabajo de vRealize Orchestrator.

Este capítulo incluye los siguientes temas:

- Descripción general de VMware vCloud Director
- Iniciar sesión en el portal para tenants de vCloud Director
- Funciones y derechos del portal para tenants de vCloud Director
- Usar el portal para tenants de vCloud Director
- Usar la búsqueda global de vCloud Director
- Ver tareas
- Detener una tarea en curso
- Ver eventos

## Descripción general de VMware vCloud Director

VMware vCloud Director proporciona acceso basado en funciones a un portal para tenants con base en web que permite a los miembros de una organización interactuar con los recursos de dicha organización para crear vApps y máquinas virtuales, así como para trabajar con ellas.

Antes de poder acceder a la organización, un **administrador del sistema** de vCloud Director debe crear la organización, asignarle recursos y proporcionar la dirección URL para acceder al portal para tenants. Cada organización incluye uno o varios **administradores de organización**, los cuales finalizan la configuración de la organización agregando miembros y definiendo políticas y preferencias. Tras configurar la organización, los usuarios que no son administradores pueden iniciar sesión pueden crear, usar y administrar máquinas virtuales y las vApp.

## Organizaciones

Una organización es una unidad de administración de un grupo de usuarios, grupos y recursos informáticos. Para autenticarse en el nivel de organización, los usuarios proporcionan las credenciales que estableció un **administrador de organización** cuando se creó o importó el usuario. Los **administradores del sistema** crean y aprovisionan organizaciones, mientras que los **administradores de organización** gestionan usuarios, grupos y catálogos de organización.

## Usuarios y grupos

Una organización puede contener un número arbitrario de usuarios y grupos. El administrador de organización puede crear usuarios localmente o importarlos de un servicio de directorios. Los grupos se deben importar desde un servicio de directorios. Los permisos dentro de una organización se controlan mediante la asignación de derechos y funciones a usuarios y grupos.

## Centros de datos virtuales

Un centro de datos virtual de organización proporciona recursos a una organización. Los centros de datos virtuales de organización proporcionan un entorno donde se pueden almacenar, implementar y manejar sistemas virtuales. También proporcionan almacenamiento para medios virtuales de CD y DVD. Una organización puede tener varios centros de datos virtuales.

## Redes de centros de datos virtuales de organización

Una red de centros de datos virtuales de organización se ubica dentro de un centro de datos virtual de organización de vCloud Director y se encuentra disponible para todas las vApps de la organización. Una red de centros de datos virtuales de organización permite que las vApps de una organización se comuniquen entre sí. Una red de centros de datos virtuales de organización puede estar conectada a una red externa o estar aislada y ser interna de la organización. Solo los **administradores del sistema** pueden crear redes de centros de datos virtuales de organización, pero los **administradores de organización** pueden administrar redes de centros de datos virtuales de organización, incluyendo los servicios de red que proporcionan.

## Redes de vApp

Una red de vApp forma parte de una vApp y permite que las máquinas virtuales de la vApp se comuniquen entre sí. Puede conectar una red de vApp a una red de centros de datos virtuales de organización para permitir que la vApp se comunique con otras vApps dentro y fuera de la organización, si la red de centros de datos virtuales de organización está conectada a una red externa.

## Catálogos

Las organizaciones pueden utilizar catálogos para almacenar plantillas de vApp y archivos de medios. Los miembros de una organización que tienen acceso a un catálogo pueden utilizar sus plantillas de vApp y archivos de medios para crear sus propias vApps. Los **administradores de organización** pueden copiar en los catálogos de su organización elementos de catálogos públicos.

## SDDC y servidores proxy de SDDC

Un centro de datos definido por software (Software-Defined Data Center, SDDC) encapsula un entorno completo de vCenter Server. Un SDDC puede incluir uno o varios servidores proxy de SDDC que proporcionan acceso a diferentes componentes del entorno subyacente. El **administrador del sistema** puede publicar uno o varios SDDC en su organización. Es posible utilizar los servidores proxy de SDDC contenedores para acceder a la interfaz de usuario o a la API de los componentes de proxy.

## Iniciar sesión en el portal para tenants de vCloud Director

Puede acceder al portal para tenants de vCloud Director mediante una dirección URL específica de su organización.

Si desconoce la dirección URL del portal para tenants de la organización, comuníquese con el **administrador de organización**. Consulte las *Notas de la versión de vCloud Director* para obtener información sobre los navegadores y las configuraciones compatibles.

### Procedimiento

- 1 En un explorador web, desplácese hasta la dirección URL del portal para tenants de su organización.

Por ejemplo, *<https://vcloud.example.com/tenant/myOrg>*.

- 2 Introduzca el nombre de usuario y la contraseña, y haga clic en **Iniciar sesión**.

## Funciones y derechos del portal para tenants de vCloud Director

vCloud Director incluye un conjunto configurado previamente de funciones de usuario y derechos. Las funciones que pueden acceder al portal para tenants de vCloud Director son las creadas de forma predeterminada en cualquier organización, o bien aquellas funciones creadas por el administrador de organización.

Los usuarios a los que se les asignan las siguientes funciones de organización pueden acceder al portal para tenants. Los elementos que se ven y las acciones que se pueden realizar dependen de los derechos asociados a una función determinada.

- **Administrador de organización**
- **Autor de catálogo**
- **Autor de vApp**
- **Usuario de vApp**
- **Solo acceso a la consola**

Para obtener más información acerca de las funciones predefinidas y sus derechos, consulte [Funciones predeterminadas y sus derechos](#).

## Usar el portal para tenants de vCloud Director

Si tiene más de un centro de datos virtual, cuando inicie sesión en el portal para tenants de vCloud Director, se le mostrará la pantalla del panel de control **Centros de datos virtuales**. Si solo tiene un centro de datos virtual, cuando inicie sesión en el portal para tenants de vCloud Director, se desplazará directamente al centro de datos.

La pantalla del panel de control **Centros de datos virtuales** forma parte de la función multisitio de vCloud Director que permite a los tenants ver su entorno de nube distribuido geográficamente como una sola entidad. Para obtener más información acerca de la función de multisitio, consulte [Trabajar con varios sitios](#).

El panel de control es una vista unificada de los sitios y los centros de datos virtuales de vCloud Director no solo para una única organización. En un entorno de varias celdas y varias organizaciones, también puede ver los centros de datos virtuales de todas las demás organizaciones asociadas.

**Nota** En función de los derechos, los usuarios del tenant pueden ver todos los sitios miembros de una organización o solo un subconjunto de sitios.

La información acerca de la organización se muestra en la parte superior de la cinta de resumen.



Si inicia sesión como **administrador de organización**, puede ver:

- El número de sitios, organizaciones y centros de datos virtuales.
- El número total de vApps y máquinas virtuales en ejecución.
- Los recursos de hardware utilizados, como CPU, memoria y almacenamiento.

Los centros de datos virtuales se muestran en una vista de tarjetas. Cada tarjeta contiene información sobre la organización a la que pertenece el centro virtual, el número de vApps, el número total de máquinas virtuales y el número de máquinas virtuales que se están ejecutando. La tarjeta también muestra la capacidad de CPU, memoria y almacenamiento disponible para el centro de datos y especifica métricas en tiempo real sobre las asignaciones y las reservas de recursos actuales.

En el menú principal (), puede desplazarse hasta los diferentes elementos del menú.

Elemento del menú	Descripción
Centros de datos	Le dirige a la pantalla <b>Centros de datos virtuales</b> donde se muestran los centros de datos virtuales dentro de la organización.
Grupos de centros de datos	Lo desplaza hasta la pantalla <b>Grupos de centros de datos</b> para la administración de Cross VDC Networking. De forma predeterminada, solo el <b>administrador del sistema</b> puede ver este elemento de menú.
Bibliotecas	Le dirige a una vista consolidada de plantillas de vApp, catálogos, medios y otros tipos de archivos. Utilice estas plantillas y archivos para implementar máquinas virtuales o vApps.

Elemento del menú	Descripción
Administración	Le dirige a la pantalla de administración multisitio, en la que los <b>administradores de organización</b> pueden crear una asociación de confianza con otra organización.
Tareas	Le dirige a la pantalla <b>Tareas</b> que muestra las tareas notificadas por vCloud Director.
Eventos	Le dirige a la pantalla <b>Eventos</b> que muestra los eventos notificadas por vCloud Director.
Operaciones	Le dirige a la pantalla <b>Biblioteca de servicios</b> . La <b>Biblioteca de servicios</b> contiene grupos de componentes de vCloud Director para los que puede ejecutar flujos de trabajo de vRealize Orchestrator.

Puede personalizar el portal para tenants de vCloud Director con las vCloud OpenAPI de Branding. Para obtener información sobre el uso de vCloud OpenAPI, consulte el documento *Primeros pasos con vCloud OpenAPI* en <https://code.vmware.com>.

## Usar la búsqueda global de vCloud Director

Puede utilizar la búsqueda global de vCloud Director para realizar una búsqueda por nombre o parte de un nombre de los objetos de su entorno. También puede buscar una máquina virtual por su dirección IP si la dirección IP de la máquina virtual es estática.



La lista de objetos predefinidos es:

- Centros de datos
- Plantillas de vApp
- vApps
- Máquinas virtuales
- Redes de vApp
- Catálogos

Si una máquina virtual utiliza una dirección IP asignada por DHCP, la búsqueda no devuelve su dirección IP. Si desea buscar una máquina virtual que tenga una dirección IP asignada por DHCP, debe buscar por nombre.

De forma predeterminada, puede buscar solo en los objetos de su sitio local. Si cuenta con un entorno multisitio, puede buscar en varios sitios.

### Procedimiento

- 1 En la esquina superior derecha del portal para tenants de vCloud Director, haga clic en el icono **Buscar** (.
- 2 (opcional) Para anclar el panel de búsqueda, haga clic en el icono **Anclar** (.
- 3 En el cuadro de texto **Buscar**, introduzca un símbolo, una parte de un nombre o una dirección IP para buscar los nombres de objetos que coincidan o las direcciones IP estáticas de las máquinas virtuales.

4 Si emplea un entorno multisitio, seleccione los sitios en los que desea realizar la búsqueda.

5 Pulse **Entrar**.

### Resultados

Se muestran los cinco resultados coincidentes principales por tipo de objeto. Los resultados se ordenan alfabéticamente.

### Pasos siguientes

- Para ver más resultados, si los hubiere, haga clic en **Cargar más** en cada tipo de objeto.
- Para ver más información sobre un objeto específico de los resultados de la búsqueda, apunte al objeto.
- Para administrar un objeto específico, por ejemplo, para ver o modificar su configuración, haga clic en el objeto. Los detalles sobre el objeto se muestran a la izquierda.

## Ver tareas

Desde el portal para tenants, puede ver la lista de tareas recientes, así como sus detalles y el estado. Además, también puede ver la lista de todas las tareas.


De forma predeterminada, el panel **Tareas recientes** se muestra en la parte inferior del portal para tenants y contiene una lista de las tareas que se han ejecutado recientemente. Cuando se inicia una operación (por ejemplo, para crear una máquina virtual), se muestra la tarea en el panel. En caso de que minimice el panel **Tareas recientes**, seguirá viendo el número de tareas recientes en ejecución o con errores. Siempre puede hacer clic en las flechas dobles para volver a abrir el panel **Tareas recientes**.

La vista de tareas muestra todas las tareas, cuándo se ejecutaron y si se completaron correctamente. Esta vista es el primer paso para solucionar problemas en su entorno. La vista de tareas contiene operaciones de larga ejecución, como la creación de vApps o máquinas virtuales.

### Procedimiento

- 1 En el menú principal () , seleccione **Tareas** o haga clic en **Más tareas** en el panel **Tareas recientes**.

Se muestra la lista de todas las tareas, junto con la hora de ejecución y el estado de la tarea.

- 2 Haga clic en el icono de editor () para cambiar los detalles que desea ver acerca de las tareas.

- 3 (opcional) Para ver los detalles de la tarea, haga clic en el nombre de la tarea.

Entre los detalles de la tarea se incluye información como el motivo del error, cuándo falló la tarea, entre otros datos.



Detalle	Descripción
Operación	Nombre de la operación realizada.
ID del trabajo	Identificador de la tarea.
Tipo	El objeto en el que se realizó la tarea. Por ejemplo, si ha creado una máquina virtual, el tipo es <code>vm</code> .
Organización	Nombre de la organización.
Estado	Estado de la tarea, como Correcto, En ejecución o Fallido.
Iniciador	Usuario que inició la operación.
Hora de inicio	Fecha y hora en que se realizó la operación.
Hora de finalización	Fecha y hora en que la operación se realizó correctamente o falló.
Espacio de nombres del servicio	Nombre del servicio, como <code>com.vmware.vcloud</code> .
Detalles	Motivo del error de la tarea. Por ejemplo, si se intenta crear una instantánea de una máquina virtual y se produce un error en la operación debido a que no existe suficiente almacenamiento, los detalles de la tarea son del tipo: La operación solicitada superará la cuota de almacenamiento del VDC: la política de almacenamiento "*" tiene 8.693 MB restantes, pero se solicitaron 41.472 MB.

## Detener una tarea en curso

Si inicia una operación por accidente antes de aplicar o revisar todos los ajustes necesarios, puede detener la tarea en curso.

De forma predeterminada, el panel **Tareas recientes** se muestra en la parte inferior del portal para tenants. Cuando se inicia una operación (por ejemplo, para crear una máquina virtual), se muestra la tarea en el panel.

### Requisitos previos

El panel **Tareas recientes** debe estar abierto.

### Procedimiento

- 1 Inicie una operación de ejecución prolongada.

Las operaciones de ejecución prolongada son operaciones como la creación de una máquina virtual o una vApp, las operaciones de energía que se realizan en máquinas virtuales y vApps, etc.

- 2 En el panel **Tareas recientes**, haga clic en el icono **Cancelar** (✕).
- 3 En el cuadro de diálogo **Cancelar tarea**, haga clic en **Aceptar** para confirmar que desea cancelar la tarea.

### Resultados


La operación se detiene.

## Ver eventos


Desde el portal puede ver la lista de todos los eventos, así como sus detalles y estados.

La vista de eventos es una forma de ver el estado de los eventos en el portal. Esta vista muestra cuándo han ocurrido los eventos y si se realizaron correctamente. La vista de eventos contiene acontecimientos ocurridos por única vez, como los inicios de sesión del usuario y la creación o eliminación de objetos.

### Procedimiento

- 1 En el menú principal () , seleccione **Eventos**.

La lista de todas las pantallas de eventos, así como la hora en que se produjo el evento y su estado.

- 2 Haga clic en el icono de editor () para cambiar los detalles que desea ver acerca de los eventos.
- 3 (opcional) Haga clic en un evento para ver sus detalles.

Detalle	Descripción
Evento	Nombre del evento. Por ejemplo, si modifica una vApp para que incluya máquinas virtuales, el evento que inicia la operación completa es <i>Task 'Modify vApp' start</i> .
ID de evento	Identificador de la tarea.
Tipo	El objeto en el que se realizó la tarea. Por ejemplo, si ha creado una máquina virtual, el tipo es <i>vm</i> .
Destino	El objeto de destino del evento. Por ejemplo, cuando se modifica una vApp para que incluya máquinas virtuales, el destino del evento <i>Task 'Modify vApp' start</i> es <i>vdcUpdateVapp</i> .
Estado	Estado del evento, como Correcto o Fallido.
Espacio de nombres del servicio	Nombre del servicio, como <i>com.vmware.vcloud</i> .
Organización	Nombre de la organización.
Propietario	Usuario que desencadenó el evento.
Hora en que se produjo	Fecha y hora en que se produjo el evento.

# Trabajar con máquinas virtuales

## 2

Una máquina virtual es un equipo con software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. La máquina virtual está compuesta de un conjunto de archivos de configuración y especificación, y cuenta con el respaldo de los recursos físicos de un host. Todas las máquinas virtuales tienen dispositivos virtuales que ofrecen la misma funcionalidad que un hardware físico, pero son más portátiles, más seguras y más fáciles de administrar.

Además de las operaciones que se pueden ejecutar en una máquina física, las máquinas virtuales de vCloud Director admiten operaciones de infraestructura virtual, como crear una instantánea del estado de una máquina virtual y mover una máquina virtual de un host a otro.

A partir de vCloud Director 9.5, las máquinas virtuales admiten la conectividad IPv6. Puede asignar direcciones IPv6 para máquinas virtuales conectadas a redes IPv6.

---

**Importante** Todos los pasos para trabajar con máquinas virtuales están documentados a partir de la vista de tarjeta y se asume que tiene más de un centro de datos virtual. También es posible completar los mismos procedimientos desde la vista de cuadrícula, pero los pasos pueden variar ligeramente.

---

Este capítulo incluye los siguientes temas:

- [Arquitectura de máquina virtual](#)
- [Ver y editar máquinas virtuales](#)
- [Crear una nueva máquina virtual independiente](#)
- [Abrir una consola de máquina virtual](#)
- [Realizar operaciones de encendido y apagado en las máquinas virtuales](#)
- [Instalar VMware Tools en una máquina virtual](#)
- [Actualizar la versión de hardware virtual de una máquina virtual](#)
- [Editar propiedades de una máquina virtual](#)
- [Insertar medios](#)
- [Expulsar medio](#)
- [Copiar una máquina virtual en otra vApp](#)
- [Mover una máquina virtual a otra vApp](#)

- [Afinidad y antiafinidad de máquinas virtuales](#)
- [Supervisar máquinas virtuales](#)
- [Trabajar con instantáneas](#)
- [Renovar una concesión de máquina virtual](#)
- [Eliminar una máquina virtual](#)

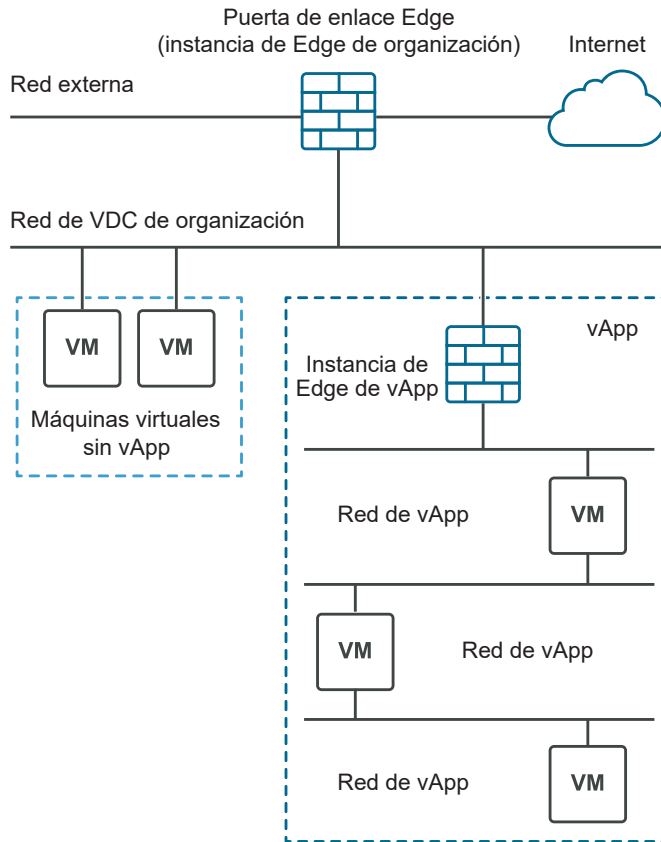
## Arquitectura de máquina virtual

Una máquina virtual puede existir como una máquina independiente o dentro de una vApp.

Una máquina virtual es un equipo con software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. La máquina virtual está compuesta de un conjunto de archivos de configuración y especificación, y cuenta con el respaldo de los recursos físicos de un host. Todas las máquinas virtuales tienen dispositivos virtuales que ofrecen la misma funcionalidad que un hardware físico, pero son más portátiles, más seguras y más fáciles de administrar. Las máquinas virtuales pueden ser independientes o estar dentro de una vApp. Una vApp es un objeto compuesto que consta de una o varias máquinas virtuales, así como de una o varias redes.

La figura siguiente muestra las distintas opciones para crear una máquina virtual. Puede crear una máquina virtual independiente o una máquina virtual dentro de una vApp. La máquina virtual independiente se conecta directamente al centro de datos virtual de organización. También puede crear una máquina virtual dentro de una vApp. Al crear una máquina virtual dentro de una vApp, puede agrupar varias máquinas virtuales y sus redes asociadas. Las vApps le permiten generar aplicaciones complejas y guardarlas en un catálogo para su uso posterior.




**Figura 2-1. Las máquinas virtuales son independientes o se encuentran dentro de una vApp**



## Ver y editar máquinas virtuales


Puede ver las máquinas virtuales independientes o que forman parte de una vApp. Puede ver las máquinas virtuales en una vista de cuadrícula o en una vista de tarjetas.

### Procedimiento


- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 Para ver las máquinas virtuales en una vista de cuadrícula, haga clic en el . O bien, para verlas en una vista de tarjeta, haga clic en el .

La lista de máquinas virtuales se muestra en una vista de cuadrícula o como una lista de tarjetas.

- 4 (opcional) Configure la vista de cuadrícula para que contenga los detalles que desea ver acerca de cada máquina virtual.

- a En la vista de cuadrícula, haga clic en el icono **Editor de cuadrícula** ().
- b Para seleccionar los detalles de la máquina virtual que desea incluir en la vista de cuadrícula, marque la casilla de verificación junto a cada detalle que desea ver.  
  
Entre los detalles se incluye información sobre la versión de hardware, VMware Tools, memoria, entre otros elementos.
- c Para guardar los cambios, haga clic en **Aceptar**.


Los detalles seleccionados aparecen como columnas para cada máquina virtual.

- 5 (opcional) En la vista de cuadrícula, haga clic en el  a la izquierda de una máquina virtual para mostrar las acciones que puede realizar con la máquina virtual seleccionada.  
  
Por ejemplo, puede apagar una máquina virtual.
- 6 Para acceder a la interfaz del sistema operativo invitado de la máquina virtual, haga clic en el icono de escritorio en la esquina superior derecha de la vista de tarjetas.

## Crear una nueva máquina virtual independiente

Puede crear una nueva máquina virtual independiente.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 Haga clic en **Nueva máquina virtual**.
- 4 Introduzca el nombre y el nombre del equipo de la máquina virtual.

---

**Importante** El nombre de equipo solo puede contener caracteres alfanuméricos y guiones. Un nombre de equipo no puede constar solo de dígitos y no puede contener espacios.

---

- 5 (opcional) Introduzca una descripción significativa.
- 6 Seleccione si desea que la máquina virtual se encienda inmediatamente después de crearse.

## 7 Seleccione cómo desea implementar la máquina virtual.

Opción	Acción
Nuevo	<p>Implementa una nueva máquina virtual con una configuración personalizable.</p> <ul style="list-style-type: none"> <li>a Seleccione una familia de sistema operativo y un sistema operativo.</li> <li>b (Opcional) Seleccione una imagen de arranque.</li> <li>c Seleccione la política de recursos informáticos.</li> <li>d Seleccione el tamaño de la máquina virtual en las opciones de tamaño predefinidas o haga clic en <b>Opciones de tamaño personalizadas</b> para introducir manualmente la cantidad de CPU virtuales, núcleos por socket y configuración de memoria.</li> </ul> <p>Los tamaños predefinidos de la máquina virtual son: <b>Pequeño, Mediano y Grande</b>.</p> <ul style="list-style-type: none"> <li>e Especifique la configuración de almacenamiento para la máquina virtual, como la política de almacenamiento y el tamaño en GB.</li> <li>f Especifique la configuración de red para la máquina virtual, como red, modo de IP, dirección IP y NIC primaria.</li> </ul>
A partir de plantilla	<p>Implementa una máquina virtual a partir de una plantilla seleccionada del catálogo de plantillas.</p> <ul style="list-style-type: none"> <li>a Seleccione una plantilla de máquina virtual a partir de la lista de plantillas disponibles.</li> <li>b (Opcional) Seleccione esta opción para usar una política de almacenamiento personalizada y seleccione la política de almacenamiento que desea usar del menú desplegable <b>Política de almacenamiento personalizada que se usará</b>.</li> <li>c Lea y acepte el contrato de licencia de usuario final, si lo hubiere.</li> </ul>

## 8 Haga clic en **Aceptar** para guardar la configuración de la máquina virtual e iniciar el proceso de creación.

Puede ver la tarjeta de la máquina virtual en el catálogo. Hasta que se cree la máquina virtual, su estado se mostrará como Ocupada.

## Abrir una consola de máquina virtual

Al obtener acceso a la consola de una máquina virtual, se puede ver información acerca de la máquina virtual, trabajar con el sistema operativo invitado y realizar operaciones que afecten a dicho sistema.

### Requisitos previos

La máquina virtual debe estar encendida.

## Instalar VMware Remote Console en un cliente

VMware Remote Console proporciona una interacción integrada entre el usuario y el invitado en todas las máquinas virtuales aprovisionadas y administradas por vCloud Director. En esta sección se describen las tareas necesarias para instalar VMware Remote Console en Windows, Apple OS X y Linux.

## Requisitos previos

Esta operación requiere los derechos incluidos en la función **Usuario de vApp** predefinida o un conjunto equivalente de derechos.

## Procedimiento

### 1 Descargue el instalador.

- Desplácese hasta la página de descargas de VMware Remote Console y seleccione el vínculo para su plataforma.  
[www.vmware.com/go/download-vmrc](http://www.vmware.com/go/download-vmrc)
- En la pantalla del panel **Centros de datos virtuales** del portal para tenants de vCloud Director, haga clic en la tarjeta del centro de datos virtual que desea explorar. Seleccione una máquina virtual y, en el menú **Acciones**, seleccione **Descargar VMRC**.

### 2 Ejecute la instalación para su plataforma.

- Windows  
Haga doble clic en el instalador `.msi` y siga las indicaciones.
- Linux  
Con privilegios raíz, ejecute el instalador `.bundle` y siga las indicaciones.
- Mac  
Haga doble clic en el archivo `.dmg` para abrirlo y, a continuación, haga doble clic en el icono de VMware Remote Console dentro del archivo para copiarlo en la carpeta Aplicaciones.

## Resultados

Tras la instalación, VMware Remote Console se abre al hacer clic en los identificadores uniformes de recursos (Uniform Resource Identifiers, URI) que comienzan con el esquema `vmrc://`. VMware Workstation, Player y Fusion también gestionan el esquema de URI `vmrc://`.

## Abrir una consola remota de máquina virtual


Puede abrir una consola de máquina virtual con VMware Remote Console mediante el portal para tenants de vCloud Director.

## Requisitos previos

- Compruebe que VMware Remote Console esté instalado en su sistema local.
- Asegúrese de que la máquina virtual seleccionada esté encendida.
- Esta operación requiere los derechos incluidos en la función **Usuario de vApp** predefinida o un conjunto equivalente de derechos.



## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual, seleccione **Iniciar consola remota de MV**.

---

**Nota** Si VMware Remote Console no está instalado, una ventana emergente le solicitará que instale VMware Remote Console o utilice la consola web.

---

## Resultados

La consola de máquina virtual se abre como una consola remota virtual externa.

---

**Nota** Cuando se conecta a una máquina virtual de vCloud Director mediante VMware Remote Console, solo se puede interactuar con la consola (enviando Ctrl+Alt+Del). No puede realizar operaciones de dispositivos, operaciones de encendido y apagado, ni administración de configuración.

---


## Abrir una consola web

Aunque no se haya instalado VMware Remote Console en el sistema local, podrá conectarse a la consola de una máquina virtual.

### Requisitos previos

- Compruebe que la máquina virtual esté encendida.
- Esta operación requiere los derechos incluidos en la función **Usuario de vApp** predefinida o un conjunto equivalente de derechos.

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual, seleccione **Iniciar consola web**.

## Resultados

La consola de máquina virtual se abrirá en una nueva pestaña del explorador mediante VMware HTML Console SDK.

## Pasos siguientes

Haga clic en cualquier parte dentro de la ventana de la consola para comenzar a utilizar el ratón, el teclado y otros dispositivos de entrada en la consola.

---

**Nota** Para obtener información sobre los teclados internacionales compatibles, consulte la documentación de VMware HTML Console SDK en <https://www.vmware.com/support/developer/html-console/>.

---

## Realizar operaciones de encendido y apagado en las máquinas virtuales

Puede realizar operaciones de alimentación en las máquinas virtuales, como el encendido o el apagado de una máquina virtual, la suspensión o el restablecimiento de una máquina virtual, o el apagado del sistema operativo invitado de una máquina virtual.

### Encender una máquina virtual


Encender una máquina virtual equivale a encender una máquina física.

No se puede encender máquinas virtuales que tengan habilitada la personalización de invitado, a menos que dichas máquinas tengan una versión actualizada de VMware Tools instalada.

#### Requisitos previos

La máquina virtual debe estar apagada.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea iniciar, seleccione **Encender**.

#### Resultados

Una máquina virtual encendida se muestra con el estado Encendido en color verde.


### Apagar una máquina virtual

Apagar una máquina virtual equivale a apagar una máquina física.

#### Requisitos previos

La máquina virtual debe estar encendida.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea apagar, seleccione **Apagar**.

### Resultados

Una máquina virtual apagada se muestra con el estado Apagado en color rojo.


## Desconectar un sistema operativo invitado

Apagar el sistema operativo invitado de una máquina virtual equivale a apagar una máquina física.

### Requisitos previos

La máquina virtual y el sistema operativo invitado deben estar encendidos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual, seleccione **Desconectar SO invitado**.

### Resultados

El SO invitado se desconectará.

## Restablecer una máquina virtual


Al restablecer una máquina virtual, se borra el estado (memoria, caché, etc.), pero la máquina virtual sigue en ejecución. Restablecer una máquina virtual equivale a presionar el botón de restablecimiento en una máquina física. Inicia un restablecimiento completo del sistema operativo sin cambiar el estado de encendido de la máquina virtual.

### Requisitos previos

Su máquina virtual está encendida.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.

- 
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea restablecer, seleccione **Restablecer**.

#### Resultados

Se borrará el estado de la máquina virtual.

## Suspender una máquina virtual


La suspensión de una máquina virtual conserva su estado actual escribiendo la memoria en el disco.

La función para suspender y reanudar es útil cuando se desea guardar el estado actual de una máquina virtual y reanudar el trabajo más tarde con el mismo estado.

#### Requisitos previos

La máquina virtual debe estar encendida.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea suspender, seleccione **Suspender**.

#### Resultados

La máquina virtual se suspenderá, pero se conservará su estado.

## Descartar el estado suspendido de una máquina virtual


Si una máquina virtual está en estado de suspensión y ya no es necesario reanudar el uso de la máquina, puede descartar el estado de suspensión. Al descartar el estado de suspensión, se elimina la memoria guardada y la máquina vuelve a un estado de apagado.

#### Requisitos previos

Debe haber una máquina virtual suspendida.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.

- Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- En el menú **Acciones** de la máquina virtual, seleccione **Descartar estado de suspensión**.

#### Resultados

El estado se descarta y la máquina virtual se apaga.

## Instalar VMware Tools en una máquina virtual


vCloud Director depende de VMware Tools para personalizar un SO invitado.

VMware Tools mejora la administración y el rendimiento de la máquina virtual mediante el reemplazo de controladores de sistemas operativos genéricos por controladores de VMware optimizados para hardware virtual. VMware Tools se instala en el sistema operativo invitado. Si bien el sistema operativo invitado puede ejecutarse sin VMware Tools, hacerlo implica perder conveniencia y funciones importantes.

#### Requisitos previos

- La máquina virtual debe estar encendida.
- Si una máquina virtual creada recientemente no tiene sistema operativo invitado, debe instalarlo antes para poder instalar VMware Tools.
- La personalización de invitado debe estar deshabilitada antes de instalar VMware Tools.
- Si la versión de VMware Tools es anterior a 7299 en una máquina virtual de una vApp, debe actualizarla.

#### Procedimiento

- En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- En el menú **Acciones** de la máquina virtual donde desea instalar VMware Tools, seleccione **Instalar VMware Tools**.

VMware Tools se instala en el sistema operativo invitado de destino. Si se produce un error durante la instalación, se muestra un mensaje de error. También puede consultar el progreso de la operación de instalación en la ventana **Tareas**.

- Para abrir la consola web de la máquina virtual, desde el menú **Acciones**, seleccione **Iniciar la consola web**.
- Siga las instrucciones en el [artículo 1014294 de la Base de conocimientos de VMware](#) para configurar VMware Tools para su sistema operativo específico.

## Resultados

VMware Tools está instalado y configurado en el sistema operativo invitado.

# Actualizar la versión de hardware virtual de una máquina virtual

Puede actualizar la versión de hardware virtual de una máquina virtual. Las versiones posteriores de hardware virtual admiten más funciones.

No se puede cambiar a una versión anterior de hardware de las máquinas virtuales de una vApp.

vCloud Director admite versiones de hardware en función de los recursos de vSphere de respaldo. La versión de hardware admitida depende de la versión de hardware virtual más reciente compatible en el VDC de proveedor de respaldo. Un **administrador de la organización** o un **administrador del sistema** pueden configurar la versión de hardware en una versión anterior a la más reciente admitida por el hardware subyacente. El portal para tenants de vCloud Director configura dinámicamente la lista de versiones de hardware virtual seleccionables en función del hardware de respaldo del VDC de organización o el VDC de proveedor.


Para obtener información sobre las características de hardware disponibles con la configuración de compatibilidad de máquina virtual, consulte *Administración de máquinas virtuales de vSphere*.

Para obtener información sobre los productos de VMware y su versión de hardware virtual, consulte <https://kb.vmware.com/s/article/1003746>.

## Requisitos previos

- Detenga la máquina virtual o la vApp que contiene la máquina virtual.
- Verifique que la versión más reciente de VMware Tools esté instalada en las máquina virtual.

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea actualizar, seleccione **Actualizar versión de hardware virtual**.
- 4 Haga clic en **Aceptar**.

## Resultados

La máquina virtual se actualizará a la versión más reciente.

# Editar propiedades de una máquina virtual

Puede editar las propiedades de una máquina virtual, incluidos el nombre y la descripción de la máquina virtual, los ajustes de hardware y de red, la configuración de sistema operativo invitado, etc.


## Cambiar las propiedades generales de una máquina virtual

Puede revisar y cambiar el nombre, descripción y otras propiedades generales de una máquina virtual.

### Requisitos previos

La modificación de propiedades como el sistema operativo requiere que la máquina esté apagada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.
- 4 La lista de propiedades que puede ver o editar en **General** se expande de forma predeterminada.

Opción	Acción
<b>Nombre de máquina virtual</b>	Edite el nombre de la máquina virtual. Esta propiedad se puede editar con la máquina virtual encendida.
<b>Nombre de equipo</b>	Edite el nombre del equipo y del host establecido en el sistema operativo invitado que identifica la máquina virtual en una red. Este campo está restringido a 15 caracteres debido a la limitación del SO Windows en los nombres de equipo. Esta propiedad se puede editar con la máquina virtual encendida.
<b>Descripción</b>	Edite la descripción opcional de la máquina virtual. Esta propiedad se puede editar con la máquina virtual encendida.
<b>Familia del sistema operativo</b>	Seleccione la familia de sistema operativo en el menú desplegable. Esta propiedad se puede editar con la máquina virtual apagada. Además, no puede editar esta propiedad si ya hay un sistema operativo en la máquina virtual.
<b>Sistema operativo</b>	Seleccione un sistema operativo en el menú desplegable. Esta propiedad se puede editar con la máquina virtual apagada. Además, no puede editar esta propiedad si ya hay un sistema operativo en la máquina virtual.

Opción	Acción
<b>Retardo de inicio</b>	<p>Especifique el tiempo en milisegundos para retrasar la operación de arranque.</p> <p>Puede transcurrir poco tiempo entre el momento en que la máquina virtual se enciende y en el que sale de BIOS e inicia el software del sistema operativo invitado. Puede cambiar el retraso de arranque para proporcionar más tiempo.</p>
<b>Directiva de almacenamiento</b>	<p>Seleccione en el menú desplegable una directiva de almacenamiento para utilizarla en la máquina virtual.</p> <p>Esta propiedad se puede editar con la máquina virtual encendida.</p>
<b>Centro de datos virtuales</b>	Vea el nombre del centro de datos virtual al que pertenece esta máquina virtual.
<b>VMware Tools</b>	Compruebe si VMware Tools está instalado en la máquina virtual.
<b>Versión del hardware virtual</b>	Observe la versión del hardware virtual de la máquina virtual.
<b>Actualizar a:</b>	Para realizar la actualización, seleccione una versión en el menú desplegable.
<b>Hora de inicio de la sincronización</b>	Active esta casilla de verificación para habilitar la sincronización de hora entre el sistema operativo invitado de la máquina virtual y el centro de datos virtual en el que se está ejecutando.
<b>Introducir configuración de BIOS</b>	<p>Seleccione si desea forzar la entrada a la pantalla de configuración de BIOS la próxima vez que arranque la máquina virtual.</p> <p>Esta propiedad se puede editar mientras la máquina virtual está apagada.</p>

5 Una vez que termine de aplicar los cambios, haga clic en **Guardar**.


## Cambiar las propiedades de hardware de una máquina virtual

Puede revisar y cambiar las propiedades de hardware de una máquina virtual.

### Requisitos previos

La máquina virtual debe estar apagada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.



- 4 Haga clic en **Hardware** para expandir la lista de propiedades de hardware que puede ver y editar.

Opción	Descripción
<b>Número de CPU virtuales</b>	<p>Edite el número de CPU existentes.</p> <p>El número máximo de CPU virtuales que puede asignar a una máquina virtual depende del número de CPU lógicas en el host y el tipo de sistema operativo invitado que está instalado en la máquina virtual.</p>
<b>Núcleos por socket</b>	<p>Edite los núcleos por socket.</p> <p>Puede configurar el modo en que las CPU virtuales se asignan desde el punto de vista de núcleos y núcleos por socket. Determine la cantidad de núcleos de CPU que desea que tenga la máquina virtual y, a continuación, seleccione la cantidad de núcleos que desea para cada socket, en función de si desea una CPU de un solo núcleo, una CPU de dos núcleos, una CPU de tres núcleos, etc.</p>
<b>Exponer virtualización de CPU asistida por hardware en SO invitado</b>	<p>Puede exponer la virtualización de CPU completa al sistema operativo invitado para que las aplicaciones que requieran virtualización de hardware puedan ejecutarse en máquinas virtuales sin paravirtualización ni traducción de binarios.</p>
<b>Memoria total</b>	<p>Edite la configuración de recursos de memoria de una máquina virtual. El tamaño de la memoria de la máquina virtual tiene que ser un múltiplo de 4 MB.</p> <p>Esta opción determina la cantidad de memoria del host ESXi que se asigna a la máquina virtual. El tamaño de la memoria de hardware virtual determina la cantidad de memoria que hay disponible para las aplicaciones que se ejecutan en la máquina virtual. Una máquina virtual no puede beneficiarse de más recursos de memoria que el tamaño de memoria de hardware virtual que se ha configurado.</p>
<b>Agregado en caliente de la memoria</b>	<p>Si habilita el agregado en caliente de memoria, es posible agregar recursos de memoria a una máquina virtual mientras esta está encendida. Esta función solo se admite en determinados sistemas operativos invitados y versiones de hardware de máquinas virtuales superiores a la 7.</p>
<b>Agregado en caliente de la CPU virtual</b>	<p>Si habilita el agregado en caliente de CPU virtual, es posible agregar CPU virtuales a la máquina virtual mientras esta está encendida. Solo puede agregar múltiplos del número de núcleos por socket. Esta función solo la admiten ciertos sistemas operativos invitados y versiones de hardware de máquinas virtuales.</p>
<b>Número de sockets</b>	<p>Observe el número de sockets.</p> <p>El número de sockets se determina en función del número de CPU virtuales disponibles. El número cambia cuando se actualiza la cantidad de CPU virtuales.</p>
<b>Medios extraíbles</b>	<p>Observe los medios extraíbles disponibles, como la unidad de CD/DVD y de disquete conectada.</p>

## 5 En **Discos duros**, haga clic en **Agregar** para agregar un disco duro.

Opción	Descripción
Tamaño	<p>Introduzca el tamaño del disco duro en MB. Puede aumentar el tamaño del disco duro más adelante.</p> <p><b>Nota</b> Puede aumentar el tamaño de un disco duro existente si la máquina virtual no es un clon vinculado ni tiene instantáneas.</p>
Política	<p>De forma predeterminada, se utiliza la política de almacenamiento para la máquina virtual.</p> <p>De manera predeterminada, todos los discos duros adjuntados a una máquina virtual usan la política de almacenamiento especificada para esta. Puede reemplazar este valor predeterminado para cualquiera de estos discos cuando crea una máquina virtual o modifica sus propiedades. La columna Tamaño de cada disco duro incluye un menú desplegable que enumera todas las políticas de almacenamiento disponibles para esta máquina virtual.</p>
Tipo de bus	<p>Seleccione el tipo de bus.</p> <p>Las opciones son <b>Paravirtual (SCSI)</b>, <b>LSI Logic paralelo (SCSI)</b>, <b>LSI Logic SAS (SCSI)</b>, <b>IDE</b> y <b>SATA</b>. Para obtener más información sobre los tipos de controladores de almacenamiento y su compatibilidad, consulte <i>Guía de administración de máquinas virtuales de vSphere</i>.</p>
Número de bus	Escriba el número de bus.
Número de unidad	Introduzca el número de unidad lógica de la unidad de disco duro.

## 6 En **NIC**, haga clic en **Agregar** para agregar una nueva NIC.

Puede añadir hasta 10 NIC. Para obtener información sobre el número de NIC admitidas en función de la versión de hardware de la máquina virtual, consulte: <http://kb.vmware.com/s/article/2051652>. vCloud Director admite la modificación de las NIC de máquina virtual mientras esta se está ejecutando. Para obtener información sobre los tipos de adaptador de red admitidos, consulte <http://kb.vmware.com/kb/1001805>.

Opción	Descripción
NIC primario	<p>Se muestra una marca cuando se selecciona el NIC primario.</p> <p>Seleccione un NIC primario. La configuración del NIC primario determina la puerta de enlace predeterminada y única de la máquina virtual. La máquina virtual puede usar cualquier NIC para conectarse a máquinas virtuales y físicas que estén conectadas directamente a la misma red que el NIC, pero solo puede usar el NIC primario para conectarse a máquinas de redes que requieran una conexión de puerta de enlace.</p>
NIC	Número de la NIC.
Conectado	Active la casilla de verificación para conectar una NIC.
Red	Seleccione una red en el menú desplegable.

Opción	Descripción
Modo de IP	<p>Seleccione un modo de IP:</p> <ul style="list-style-type: none"> <li>■ <b>Estática - Grupo de direcciones IP</b> Extrae una dirección IP estática del grupo de direcciones IP de red.</li> <li>■ <b>Estática - Manual</b> Le permite especificar una dirección IP concreta de forma manual. Si selecciona esta opción, debe introducir una dirección IP en la columna <b>Dirección IP</b>.</li> <li>■ <b>DHCP</b> Extrae una dirección IP de un servidor DHCP.</li> </ul>
Dirección MAC	Escriba la dirección MAC de la interfaz de red.

7 Haga clic en **Guardar**.

## Cambiar las propiedades de personalización del sistema operativo invitado de una máquina Virtual

La personalización del SO invitado en vCloud Director es opcional en todas las plataformas. Es necesaria para las máquinas virtuales que deben unirse a un dominio de Windows.


Parte de la información solicitada en este menú se aplica solo a las plataformas de Windows. El panel Personalización de SO invitado incluye la información necesaria para que la máquina virtual se una a un dominio de Windows. Un **administrador de organización** puede especificar valores predeterminados para un dominio al cual los invitados de Windows en la organización se pueden unir. No todas las máquinas virtuales de Windows deben unirse a un dominio, pero, en la mayoría de las instalaciones empresariales, una máquina virtual que no pertenece a un dominio no puede acceder a muchos de los recursos de red disponibles.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.
- Para realizar la personalización del invitado, es necesario que la máquina virtual ejecute VMware Tools.
- Antes de poder personalizar un sistema operativo invitado de Windows, el **administrador del sistema** debe instalar los archivos de Microsoft Sysprep adecuados en el grupo de servidores de vCloud Director. Consulte la *Guía de instalación y actualización de vCloud Director*.
- Para la personalización de sistemas operativos invitados Linux, es necesario que Perl esté instalado en el invitado.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.

- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.
- 4 Haga clic en **Propiedades y personalización de SO invitado** para expandir la lista de ajustes del sistema operativo invitado.

Opción	Descripción
Habilitar personalización de invitado	Seleccione esta opción para habilitar la personalización de invitado.
Cambiar SID	<p>Seleccione esta opción para cambiar el identificador de seguridad (Security ID, SID) de Windows.</p> <p>Esta opción es específica de las máquinas virtuales que ejecutan un sistema operativo invitado de Windows. En algunos sistemas operativos de Windows, se usa el SID para identificar de manera exclusiva los sistemas y los usuarios. Si no selecciona esta opción, la nueva máquina virtual tendrá el mismo SID que la máquina virtual o la plantilla que se tomó como base. Los SID duplicados no causan problemas cuando los equipos forman parte de un dominio y solo se usan cuentas de usuario de dominio. No obstante, si las máquinas forman parte de un grupo de trabajo o se usan cuentas de usuario locales, los SID duplicados pueden perjudicar los controles de acceso a los archivos. Para obtener más información, consulte la documentación de su sistema operativo Microsoft Windows.</p>
Permitir contraseña del administrador local	<p>Seleccione esta opción para permitir la configuración de una contraseña de administrador en el sistema operativo invitado.</p> <p>a Permite especificar una contraseña para el administrador local.</p> <p>Si se deja en blanco el cuadro de texto <b>Especificar contraseña</b>, se genera automáticamente una contraseña.</p> <p>b Permite especificar el número de veces que se permitirá el inicio de sesión automático.</p> <p>Si introduce cero, se deshabilita el inicio de sesión automático como administrador.</p>
Solicitar a los administradores que cambien la contraseña la primera vez que inicien sesión	Seleccione esta opción para exigir que los administradores cambien la contraseña del sistema operativo invitado en el primer inicio de sesión. Por motivos de seguridad, se recomienda utilizar esta opción.
Generar contraseña automáticamente	Seleccione esta opción para permitir la generación automática de contraseñas.

Opción	Descripción
Habilitar esta MV para que se una a un dominio	<p>Puede seleccionar esta opción para unir la máquina virtual a un dominio de Windows. Puede utilizar el dominio de la organización, o bien reemplazarlo y especificar las propiedades de dominio.</p> <ul style="list-style-type: none"> <li>a Introduzca el nombre de dominio.</li> <li>b Introduzca el nombre de usuario y la contraseña.</li> <li>c Introduzca la unidad organizativa de la cuenta.</li> </ul>
Script	<p>Puede usar un script de personalización para modificar el sistema operativo invitado de la máquina virtual. Al agregar un script de personalización a una máquina virtual, se llama al script solo en la personalización inicial y cuando se fuerza una nueva personalización. Si se establece el parámetro de línea de comandos <code>precustomization</code>, se llama al script antes de que comience la personalización de invitado. Si se establece el parámetro de línea de comandos <code>postcustomization</code>, se llama al script una vez finalizada la personalización de invitado.</p> <ul style="list-style-type: none"> <li>■ Haga clic en el botón de cargar debajo del cuadro de texto del script para navegar hasta un script de personalización en la máquina local.</li> <li>■ Escriba el script de personalización directamente en el cuadro de texto <b>Archivo de script</b>.</li> </ul> <p>Un script de personalización que introduce directamente en el cuadro de texto <b>Archivo de script</b> no puede contener más de 1.500 caracteres. Para obtener más información, consulte el artículo de la Base de conocimientos de VMware <a href="https://kb.vmware.com/kb/1026614">https://kb.vmware.com/kb/1026614</a>.</p>

5 Una vez que termine de aplicar los cambios, haga clic en **Guardar**.

## Entender la personalización de invitado

Cuando se personaliza un sistema operativo invitado existen algunas configuraciones y opciones que debe conocer.

### Casilla Habilitar personalización de invitado

Esta casilla se encuentra en la pestaña **Personalización de SO invitado** en la pantalla **Propiedades** de la máquina virtual. El objetivo de la personalización de invitado consiste en configurar en función de las opciones seleccionadas en la pantalla **Propiedades**. Si esta casilla está activada, se personaliza o se vuelve a personalizar el invitado cuando se necesite.

Este proceso es necesario para que sean operativas todas las funciones de personalización de invitado, como: nombre de equipo, configuración de red, definición y caducidad de las contraseñas raíz y de administrador, cambio del SID en sistemas operativos Windows, etc. Esta opción debe activarse para que **Encender y forzar volver a personalizar** funcione.

Si casilla está activada y los parámetros de configuración de máquinas virtuales presentes en vCloud Director no están sincronizados con la configuración contenida en el SO invitado, la pestaña **Perfil** de la pantalla **Propiedades** de las máquinas virtuales indica que la configuración no está sincronizada con el SO invitado y que la máquina virtual requiere personalización de invitado.

## Comportamiento de personalización de invitado para vApp y máquinas virtuales

Las casillas están desactivadas.

- **Habilitar la personalización de invitado**
- En los sistemas operativos Windows, **Cambiar SID**
- **Restablecer contraseña**

Si desea personalizar (o ha realizado cambios en la configuración de red que deben reflejarse en el SO invitado), active la casilla **Habilitar personalización de invitado** y establezca las opciones en la pestaña **Personalización de SO invitado** de la página **Propiedades** de la máquina virtual. Cuando se utilizan máquinas virtuales a partir de plantillas de vApp para crear una vApp y después se agrega una máquina virtual, las plantillas de vApp actúan como bloques de creación. Al agregar máquinas virtuales desde un catálogo a una nueva vApp, las máquinas virtuales se habilitan para personalización de invitado de manera predeterminada. Cuando se guarda una plantilla de vApp desde un catálogo como una vApp, las máquinas virtuales se habilitan para la personalización de invitado solo si la casilla **Habilitar personalización de invitado** está activada.

Estos son los valores predeterminados de la configuración de personalización de invitados:

- La casilla **Habilitar personalización de invitado** es la misma que la de la máquina virtual de origen del catálogo.
- En las máquinas virtuales invitadas de Windows, la opción **Cambiar SID** tiene la misma configuración que en la máquina virtual de origen del catálogo.
- La configuración para restablecer la contraseña es la misma que en la máquina virtual del origen del catálogo.

Si fuera necesario, desactive la casilla **Habilitar personalización de invitado** antes de iniciar la vApp.

Si se agregan máquinas virtuales en blanco, que estén pendientes de una instalación de SO invitado, a una vApp, la casilla **Habilitar personalización de invitado** estará desactivada de manera predeterminada porque dichas máquinas no están listas aún para la personalización.

Después de instalar el SO invitado y VMware Tools, apague las máquinas virtuales, detenga la vApp, active la casilla **Habilitar personalización de invitado** e inicie la vApp y las máquinas virtuales para realizar la personalización de invitado.

Si el nombre de máquina virtual y la configuración de red se actualizan en una máquina virtual que se ha personalizado, la máquina se volverá a personalizar la próxima vez que se encienda, lo cual volverá a sincronizar la máquina virtual invitada con vCloud Director.

## Encender y forzar volver a personalizar una máquina virtual

Puede encender una máquina virtual y forzar volver a personalizar una máquina virtual.


Si la configuración de una máquina virtual no está sincronizada con vCloud Director o se ha producido un error en el intento de realizar una personalización de invitado, puede forzar una nueva personalización de la máquina virtual.

Asegúrese de que la aplicación que se está ejecutando en la máquina virtual se pueda volver a personalizar. Si cambia un controlador de dominio mediante Microsoft Sysprep y también cambia el SID, podría dañarse la máquina virtual. Para reducir el riesgo de daños a la máquina virtual, cree una instantánea antes de volver a personalizarla.

#### Requisitos previos

- Debe ser un administrador de organización.
- La máquina virtual debe estar apagada.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Alimentación** de la máquina virtual que desee encender y personalizar, seleccione **Encender y forzar volver a personalizar**.

#### Resultados

La máquina virtual se volverá a personalizar y se encenderá.

## Cambiar las propiedades avanzadas de una máquina virtual

En la configuración de **Avanzado**, puede configurar la asignación de recursos (cuota, reserva y límite) para determinar la cantidad de recursos de CPU, memoria y almacenamiento que se proporcionan para una máquina virtual.

Utilice la configuración de asignación de recursos (cuotas, reserva y límite) para establecer la cantidad de recursos de CPU, memoria y almacenamiento que se proporcionan a una máquina virtual.

#### Cuotas de asignación de recursos

Las cuotas indican la importancia relativa de una máquina virtual dentro de un centro de datos virtual. Si una máquina virtual tiene el doble de cuotas de un recurso que otra máquina virtual, tendrá derecho a consumir el doble de dicho recurso cuando estas dos máquinas virtuales estén compitiendo por la obtención de recursos. La disponibilidad de cuotas se suele especificar como Alta, Normal o Baja. Estos parámetros indican los valores de cuotas con una proporción de 4:2:1, respectivamente. También puede seleccionar Personalizada para asignar un número específico de cuotas (que expresa una ponderación proporcional) a cada máquina virtual. Al asignar cuotas a una máquina virtual, siempre se especifica la prioridad de dicha máquina en relación a otras máquinas virtuales encendidas.

#### Reserva de asignación de recursos

La reserva especifica la asignación mínima garantizada de una máquina virtual. vCloud Director permite encender una máquina virtual solo si hay suficientes recursos sin reservar para satisfacer la reserva de la máquina virtual. El centro de datos virtual garantiza dicha cantidad incluso cuando sus recursos se encuentran considerablemente cargados. La reserva se expresa en unidades concretas (megahercios o megabytes).

Por ejemplo, supongamos que dispone de 2 GHz y se especifica una reserva de asignación de recursos de 1 GHz para la máquina virtual 1 y 1 GHz para la máquina virtual 2. De este modo, cada máquina virtual tendrá garantizado 1 GHz si lo necesita. Sin embargo, si la máquina virtual 1 solo utiliza 500 MHz, la máquina virtual 2 puede utilizar 1,5 GHz.

El valor predeterminado de reserva es 0. Especifique una reserva si necesita garantizar que las cantidades mínimas requeridas de CPU o memoria estén siempre disponibles para la máquina virtual.

### Límite de asignación de recursos

El límite especifica el máximo de recursos de memoria y de CPU que se pueden asignar a una máquina virtual. Un centro de datos virtual puede asignar más recursos que los de reserva a una máquina virtual, pero nunca más allá del límite, aunque existan recursos sin utilizar en el sistema. El límite se expresa en unidades concretas (megahercios o megabytes).


Los valores predeterminados de los límites de recursos de memoria y de CPU son ilimitados. Cuando el límite de memoria es ilimitado, la cantidad de memoria que se configuró para la máquina virtual durante su creación pasa a ser el límite efectivo en la mayoría de los casos.

Generalmente, no es necesario especificar un límite. Si se especifica, puede que se malgasten recursos inactivos. El sistema no permite que una máquina virtual utilice más recursos que el límite, aunque el sistema no se esté utilizando por completo y existan recursos inactivos disponibles. Especifique un límite solo cuando tenga buenas razones para hacerlo.

### Requisitos previos

- Un centro de datos virtual del grupo de reservas.
- Asegúrese de que el centro de datos virtual proporciona cierta cantidad de memoria de una máquina virtual.
- Asegúrese de que siempre se asigne a una máquina virtual en concreto un porcentaje superior de recursos del centro de datos virtual con respecto a otras máquinas virtuales.
- Establezca un límite máximo de recursos que se pueden asignar a una máquina virtual.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.



- 3 En la tarjeta de la máquina virtual que desea editar, haga clic en **Detalles**.
- 4 Haga clic en **Avanzado**.
- 5 Para configurar las cuotas de asignación de recursos correspondientes a la configuración de CPU, seleccione una opción en el menú desplegable **Prioridad**.

Opción	Descripción
Baja	Asigna 500 cuotas por CPU virtual.
Normal	Asigna 1.000 cuotas por CPU virtual.
Alta	Asigna 2.000 cuotas por CPU virtual.
Personalizada	<p>Permite asignar una cantidad específica de cuotas. Para ello, introduzca la cantidad de cuotas (lo que expresa una ponderación proporcional) de cada máquina virtual.</p> <p>Al asignar cuotas a una máquina virtual, siempre se especifica la prioridad de dicha máquina en relación a otras máquinas virtuales encendidas.</p>

- 6 Especifique la reserva para la configuración de CPU. Para ello, introduzca la reserva en MHz y, de manera opcional, el límite para la configuración de CPU en MHz.

Opción	Descripción
Sin límite	La opción de recursos de CPU predeterminada.
Máxima	Especifique un máximo de recursos de CPU que se pueden asignar a una máquina virtual en MHz.

- 7 Para configurar las cuotas de asignación de recursos correspondientes a la configuración de memoria, seleccione una opción en el menú desplegable **Prioridad**.

Opción	Descripción
Baja	Asigna 5 cuotas por megabyte de memoria de máquina virtual configurada.
Normal	Asigna 10 cuotas por megabyte de memoria de máquina virtual configurada.
Alta	Asigna 20 cuotas por megabyte de memoria de máquina virtual configurada.
Personalizada	Permite asignar una cantidad específica de cuotas. Para ello, introduzca la cantidad de cuotas.

- 8 Especifique la reserva para la configuración de memoria en MB y, de manera opcional, el límite para la configuración de memoria en MB.

Opción	Descripción
Sin límite	La opción de recursos de CPU predeterminada.
Máxima	Especifique un máximo de recursos de CPU que se pueden asignar a una máquina virtual en MHz.

- 9 Haga clic en **Agregar en Metadatos** para especificar los metadatos.

Por ejemplo, puede agregar metadatos sobre la fecha de creación o el propietario.

**10** Una vez que termine de aplicar los cambios, haga clic en **Guardar**.


## Insertar medios

Puede insertar medios, como imágenes de CD/DVD, desde catálogos para utilizarlos en un sistema operativo invitado de máquina virtual. Puede utilizar estos archivos de medios para instalar un sistema operativo en la máquina virtual, diversas aplicaciones, controladores, etc.

### Requisitos previos

Debe tener acceso a un catálogo con archivos de medios.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 Seleccione la máquina virtual a la que desea agregar los medios.
- 4 En el menú **Acciones**, seleccione **Insertar medios**.
- 5 En la ventana **Insertar CD**, seleccione el archivo de medios que desea insertar en la máquina virtual.
- 6 Haga clic en **Insertar**.


## Expulsar medio

Puede expulsar el archivo de medios cuando haya terminado de usar un CD o un DVD en la máquina virtual.

### Requisitos previos

Un archivo de medios se insertó previamente en la máquina virtual.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 Seleccione la máquina virtual cuyo medio desea expulsar.
- 4 En el menú **Acciones**, seleccione **Expulsar medios**.

## Resultados

Se expulsará el archivo de medios.

## Copiar una máquina virtual en otra vApp


Puede copiar una máquina virtual a otra vApp. Al copiar una máquina virtual, la máquina virtual original permanece en la vApp de origen.

Cuando se copia una máquina virtual, las instantáneas no se incluyen en la copia.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.
- Apague la máquina virtual.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea copiar, seleccione **Copiar a**.
- 4 Seleccione la vApp de destino a la que desea copiar la máquina virtual y haga clic en **Siguiente**.
- 5 Configure los recursos, como el nombre de la máquina virtual y el nombre del equipo y, de manera opcional, la política de almacenamiento y las NIC, y haga clic en **Siguiente**.

---

**Importante** El nombre de equipo solo puede contener caracteres alfanuméricos y guiones. No puede constar solo de dígitos y no puede contener espacios.

---

- 6 En la página **Listo para completar**, revise su configuración y haga clic en **Listo**.

## Mover una máquina virtual a otra vApp

Puede mover una máquina virtual a otra vApp. Al mover una máquina virtual, la máquina virtual original se elimina de la vApp de origen.

Cuando se mueve una máquina virtual a una vApp diferente, se pierden las instantáneas que se hayan tomado.

A partir de vCloud Director 9.5, el movimiento de máquinas virtuales entre diferentes vApps depende de VMware vSphere® vMotion® y Enhanced vMotion Compatibility (EVC). Es posible mover una máquina virtual a una vApp diferente que pertenece al mismo VDC de organización o a uno distinto dentro del mismo VDC de proveedor.

Mientras se mueve una máquina virtual a una vApp diferente, es posible realizar reconfiguraciones, como cambiar la red y el perfil de almacenamiento.


**Tabla 2-1. Reconfiguraciones durante los movimientos de máquinas virtuales y estados de máquinas virtuales**

Reconfiguración	Estado de la máquina virtual si la vApp de destino se encuentra en el mismo VDC de organización	Estado de la máquina virtual si la vApp de destino se encuentra en otro VDC de organización en el mismo VDC de proveedor
Cambiar la red	Apagada	N/D
Quitar la red	Encendida o apagada	N/D
Cambiar el perfil de almacenamiento	Encendida o apagada	Apagada

#### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.
- Verifique que los recursos subyacentes de vSphere sean compatibles con EVC y vMotion. Para obtener información sobre los requisitos y las limitaciones de vMotion y EVC, consulte *Administrar vCenter Server y hosts*.
- Si desea cambiar la red de máquinas virtuales o el perfil de almacenamiento, compruebe si debe apagar la máquina virtual. Consulte la tabla *Reconfiguraciones durante los movimientos de máquinas virtuales y los estados de máquinas virtuales*.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina que desea mover, seleccione **Mover a**.
- 4 Seleccione la vApp de destino y haga clic en **Siguiente**.
- 5 Configure los recursos, como el nombre de la máquina virtual y el nombre del equipo y, de manera opcional, la política de almacenamiento y las NIC, y haga clic en **Siguiente**.

**Importante** El nombre de equipo solo puede contener caracteres alfanuméricos y guiones. No puede constar solo de dígitos y no puede contener espacios.

- 6 En la página **Listo para completar**, revise su configuración y haga clic en **Listo**.

## Afinidad y antiafinidad de máquinas virtuales

Las reglas de afinidad y antiafinidad permiten distribuir un grupo de máquinas virtuales entre diferentes hosts ESXi o mantener un grupo de máquinas virtuales en un host ESXi en particular.

Una regla de afinidad ubica un grupo de máquinas virtuales en un host específico a fin de que pueda auditar fácilmente el uso de dichas máquinas virtuales. Una regla de antiafinidad ubica un grupo de máquinas virtuales en diferentes hosts, lo que impide que todas las máquinas virtuales presenten errores de manera simultánea en caso de que un solo host falle.

Las reglas de afinidad y antiafinidad pueden ser obligatorias o preferidas.

### Regla obligatoria

Si no se pueden cumplir las reglas de afinidad o de antiafinidad, las máquinas virtuales que se agreguen a la regla no se encenderán.

### Regla preferida

Si se infringen las reglas de afinidad o de antiafinidad, el clúster o el host aún encienden las máquinas virtuales.

Por ejemplo, si tiene una regla de antiafinidad entre dos máquinas virtuales, pero hay un solo host físico disponible, una regla obligatoria (afinidad fuerte) no permite que se enciendan ambas máquinas virtuales. Si la regla de antiafinidad es preferida (afinidad débil), se permite el encendido de las dos máquinas virtuales.

## Vídeos relacionados




Afinidad de MV y MV en vCloud Director

([https://vmwaretv.vmware.com/media/t/1\\_we23vrud](https://vmwaretv.vmware.com/media/t/1_we23vrud))

## Ver reglas de afinidad y antiafinidad

Puede ver tanto las reglas de afinidad y antiafinidad existentes como sus propiedades (por ejemplo, las máquinas virtuales afectadas por ellas y si dichas reglas están habilitadas).

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Reglas de afinidad** en el panel izquierdo.
- 2 (opcional) Haga clic en el icono **Editor de cuadrícula** () y seleccione qué detalles sobre las reglas quiere que se muestren.

### Resultados

Verá la lista de reglas de afinidad y antiafinidad existentes, si se necesitan o no es así, las máquinas virtuales y el estado habilitado de cada regla.

## Crear una regla de afinidad

Cree una regla de afinidad para ubicar un grupo específico de máquinas virtuales en un solo host a fin de que se pueda auditar el uso de esas máquinas virtuales.

### Procedimiento

1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Reglas de afinidad** en el panel izquierdo.

2 En **Reglas de afinidad**, haga clic en **Nuevo**.

3 Introduzca un nombre de regla.

4 Anule la selección de **Habilitado** para crear la regla sin habilitarla.

De forma predeterminada, la casilla se encuentra seleccionada y las reglas se habilitan una vez creadas.

5 Anule la selección de **Obligatoria** para crear una regla preferida. Esto significa que las máquinas virtuales agregadas a la regla se encenderán incluso cuando se infrinja la regla.

De forma predeterminada, la casilla se encuentra seleccionada y la regla es obligatoria. Si no se puede cumplir la regla, las máquinas virtuales agregadas a la regla no se encenderán.

6 Seleccione las máquinas virtuales que desea agregar a la regla de afinidad.

7 Haga clic en **Guardar**.

### Resultados

vCloud Director ubica las máquinas virtuales asociadas con la regla de afinidad en un solo host.

## Crear una regla de antiafinidad

Cree una regla de antiafinidad para ubicar un grupo específico de máquinas virtuales en varios hosts a fin de evitar errores simultáneos de esas máquinas virtuales en el caso de que se produzca un error en un solo host.

### Procedimiento

1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Reglas de afinidad** en el panel izquierdo.

2 En **Reglas de antiafinidad**, haga clic en **Nuevo**.

3 Introduzca un nombre de regla.

4 Anule la selección de **Habilitado** para crear la regla sin habilitarla.

De forma predeterminada, la casilla se encuentra seleccionada y las reglas se habilitan una vez creadas.

- 5 Anule la selección de **Obligatoria** para crear una regla preferida y permitir que el clúster encienda las máquinas virtuales incluso cuando se infrinja la regla.

De forma predeterminada, la casilla se encuentra seleccionada y la regla es obligatoria. Si no se puede cumplir la regla, las máquinas virtuales agregadas a la regla no se encenderán.

- 6 Seleccione las máquinas virtuales que desea agregar a la regla de antiafinidad.
- 7 Haga clic en **Guardar**.

#### Resultados

vCloud Director ubica las máquinas virtuales asociadas con la regla de antiafinidad en diferentes hosts.

## Editar una regla de afinidad o de antiafinidad

Puede editar una regla de afinidad o antiafinidad para habilitar o deshabilitar la regla, agregar o eliminar máquinas virtuales, cambiar el nombre de la regla o la preferencia de la regla.

#### Requisitos previos

Esta operación requiere el derecho `Organization vDC: VM-VM Affinity Edit`. Este derecho se incluye en las funciones predefinidas **Autor de catálogo**, **Autor de vApp** y **Administrador de organización**.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Reglas de afinidad** en el panel izquierdo.
- 2 Haga clic en el botón de radio junto al nombre de la regla que desea editar y haga clic en **Editar**.
- 3 Edite las propiedades de la regla.
  - a Cambie el nombre de la regla según sea necesario.
  - b Seleccione si desea habilitar o deshabilitar la regla.
  - c Seleccione si la regla debe ser obligatoria o preferida.
  - d Agregue o elimine máquinas virtuales.
- 4 Haga clic en **Guardar**.

## Eliminar una regla de afinidad o de antiafinidad

Si ya no desea utilizar una regla de afinidad o de antiafinidad, puede eliminarla.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Reglas de afinidad** en el panel izquierdo.

- 2 Haga clic en el botón de radio junto al nombre de la regla que desea eliminar y haga clic en **Eliminar**.
- 3 Para confirmar que desea eliminar la regla, haga clic en **Aceptar**.

#### Resultados

vCloud Director elimina la regla de afinidad o antiafinidad.

## Supervisar máquinas virtuales


Si el administrador de vCloud Director ha habilitado la función de supervisión de máquinas virtuales, puede ver el gráfico de supervisión en el portal para tenants.

Utilice esta función para conocer el estado de una máquina virtual determinada a lo largo del tiempo (días, semanas o meses).

#### Requisitos previos

Esta función solo está disponible si el administrador de vCloud Director la ha habilitado.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 Seleccione la máquina virtual que desea supervisar y haga clic en **Detalles**.
- 4 Haga clic en **Gráfico de supervisión** para expandir la vista de supervisión.

Se muestra el gráfico de supervisión.

5

- 6 Seleccione una opción de métrica para supervisar las máquinas virtuales.

La lista en el menú desplegable **Métrica** varía en función de las opciones del **administrador del sistema**. Verá algunas opciones o todas.

Métrica	Descripción
Disco aprovisionado más reciente	Se especifica en KB. Elija la vista de día, semana o mes.
Promedio de lectura de disco	Se especifica como un porcentaje. Elija la vista de día, semana o mes.
Promedio de escritura de disco	Se especifica como un porcentaje. Elija la vista de día, semana o mes.
Promedio de uso de CPU	Se especifica como un porcentaje. Elija la vista de día, semana o mes.



Métrica	Descripción
Promedio de uso de CPU en MHz	Se especifica en MHz. Elija la vista de día, semana o mes.
Uso máximo de CPU	Se especifica como un porcentaje. Elija la vista de día, semana o mes.
Promedio de uso de memoria	Se especifica como un porcentaje. Elija la vista de día, semana o mes.
Disco usado más reciente	Se especifica en KB. Elija la vista de día, semana o mes.

Se mostrará un nuevo gráfico cada vez que seleccione un valor diferente de la lista.

- 7 (opcional) Cambie el intervalo de tiempo para la recopilación de métricas.
- 8 Haga clic en **Actualizar**.
- 9 Para guardar los cambios, haga clic en **Guardar**.

## Trabajar con instantáneas

Las instantáneas conservan el estado y los datos de una máquina virtual en el momento que crea dicha instantánea. Cuando se crea una instantánea de una máquina virtual, esta no se ve afectada, y solamente se copia y se almacena una imagen de ella en un estado determinado. Las instantáneas son útiles cuando es necesario volver en repetidas ocasiones al mismo estado de la máquina virtual, pero no se desean crear varias máquinas virtuales.

Las instantáneas son útiles como una solución a corto plazo para probar software con efectos desconocidos o potencialmente dañinos. Por ejemplo, puede utilizar una instantánea a modo de punto de restauración durante un proceso lineal o iterativo, como la instalación de paquetes de actualización, o durante un proceso de ramificación, como la instalación de diferentes versiones de un programa.

Se recomienda utilizar una instantánea al actualizar el sistema operativo de una máquina virtual. Por ejemplo, antes de actualizar la máquina virtual, debe crear una instantánea para conservar el momento específico antes de la actualización. Si no hay problemas durante la actualización, puede quitar la instantánea, lo que confirmará los cambios realizados durante la actualización. Sin embargo, si se ha producido un problema, puede revertir a la instantánea, lo que restaurará el estado guardado que tenía la máquina virtual antes de la actualización.

Con vCloud Director puede tener una sola instantánea de una máquina virtual. Cada intento de crear una nueva instantánea de una máquina virtual elimina la anterior.

## Tomar una instantánea de una máquina virtual

Puede tomar una instantánea de una máquina virtual. Después de tomar la instantánea, puede revertir la máquina virtual a la instantánea o eliminar la instantánea.

## Requisitos previos

Compruebe que la máquina virtual no esté conectada a un disco independiente.


---

**Nota** Las instantáneas no capturar configuraciones NIC.

---

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.

- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.

- 3 En el menú **Acciones** de la máquina virtual de la que desea tomar una instantánea, seleccione **Crear instantánea**.

Al tomar una instantánea de una máquina virtual, se reemplaza la instantánea existente, si existe una.

- 4 (opcional) Seleccione si desea crear una instantánea de la memoria de la máquina virtual.

Cuando se captura el estado de la memoria de la máquina virtual, la instantánea retiene el estado activo de la máquina virtual. Las instantáneas creadas con memoria realizan una instantánea en un momento preciso, por ejemplo, para actualizar software que aún está en funcionamiento. Si crea una instantánea de memoria y la actualización no finaliza de la manera esperada, o si el software no cumple con sus expectativas, puede realizar una reversión al estado anterior de la máquina virtual.

Cuando se captura el estado de la memoria, no es necesario poner en modo inactivo los archivos de la máquina virtual. Si no se captura el estado de la memoria, la instantánea no guarda el estado activo de la máquina virtual y los discos tienen coherencia ante fallos, a menos que se pongan en modo inactivo.

- 5 (opcional) Seleccione si desea poner en modo inactivo el sistema de archivos invitado.

Para esta operación, VMware Tools debe estar instalado en la máquina virtual. Cuando se pone una máquina virtual en modo inactivo, VMware Tools pone en modo inactivo al sistema de archivos de la máquina virtual. Una operación de puesta en modo inactivo garantiza que el disco de la instantánea represente un estado coherente de los sistemas de archivo invitados. Las instantáneas en modo inactivo resultan adecuadas para las copias de seguridad automatizadas o periódicas. Por ejemplo, si se desconoce la actividad de la máquina virtual, pero se desea disponer de varias copias de seguridad recientes para realizar reversiones, es posible poner los archivos en modo inactivo.

Las máquinas virtuales que tienen discos de gran capacidad no se pueden poner en modo inactivo.

- 6 Haga clic en **Aceptar**.

## Resultados

La instantánea permite revertir la máquina virtual a la instantánea más reciente.


## Revertir una máquina virtual a una instantánea

Puede restaurar una máquina virtual al estado en el que se encontraba cuando se creó la instantánea.

### Requisitos previos

La máquina virtual tiene una instantánea.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea revertir a una instantánea, seleccione **Revertir a instantánea**.
- 4 Haga clic en **Aceptar**.

## Resultados

La máquina virtual se revertirá a la instantánea guardada.

## Quitar una instantánea de una máquina virtual


Puede quitar una instantánea de una máquina virtual.

Al eliminar una instantánea, se elimina el estado de la máquina virtual conservada y ya no es posible volver a ese estado. Quitar una instantánea no afecta al estado actual de la máquina virtual.

### Requisitos previos

Una máquina virtual con una instantánea almacenada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual de la cual desea eliminar una instantánea, seleccione **Quitar instantánea**.

- 4 Haga clic en **Aceptar**.


## Renovar una concesión de máquina virtual

Si la concesión de una máquina virtual caducará pronto, es posible renovarla.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual con la concesión a punto de caducar, seleccione **Renovar concesión**.

### Resultados

La concesión se renovará. Puede ver el nuevo período de tiempo de concesión en el campo **Concesión**.


## Eliminar una máquina virtual

Puede eliminar una máquina virtual de una organización.

### Requisitos previos

La máquina virtual debe estar apagada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Máquinas virtuales** en el panel izquierdo.
- 2 Haga clic en  para ver la lista en una vista de tarjetas y, de manera opcional, filtrar la lista de máquinas virtuales desde el menú desplegable **Buscar en**.
- 3 En el menú **Acciones** de la máquina virtual que desea eliminar, seleccione **Eliminar**.
- 4 Confirme la eliminación.

### Resultados

Se eliminará la máquina virtual.

# Trabajar con vApp

# 3

Una vApp consta de una o varias máquinas virtuales que se comunican en una red y utilizan recursos y servicios en un entorno implementado. Una vApp puede contener varias máquinas virtuales.

A partir de vCloud Director 9.5, las vApps admiten la conectividad IPv6. Puede asignar direcciones IPv6 para máquinas virtuales conectadas a redes IPv6.

---

**Importante** Todos los pasos para trabajar con vApps están documentados a partir de la vista de tarjeta y se asume que tiene más de un centro de datos virtual. También es posible completar los mismos procedimientos desde la vista de cuadrícula, pero los pasos pueden variar ligeramente.

---

Este capítulo incluye los siguientes temas:



- [Ver vApps](#)
- [Generar una nueva vApp](#)
- [Crear una vApp a partir de un paquete OVF](#)
- [Crear una vApp a partir de una plantilla de vApp](#)
- [Abrir una vApp](#)
- [Realizar operaciones de encendido y apagado en vApps](#)
- [Editar propiedades de una vApp](#)
- [Mostrar un diagrama de red de vApp](#)
- [Trabajar con redes en una vApp](#)
- [Trabajar con instantáneas](#)
- [Cambiar el propietario de una vApp](#)
- [Mover una vApp a otro centro de datos virtual](#)
- [Copiar una vApp detenida en otro centro de datos virtual](#)
- [Copiar una vApp encendida](#)
- [Agregar una máquina virtual a una vApp](#)
- [Guardar una vApp como plantilla de vApp en un catálogo](#)

- [Descargar una vApp como un paquete OVF](#)
- [Renovar una concesión de vApp](#)
- [Eliminar una vApp](#)


## Ver vApps

Puede ver las vApps en una vista de cuadrícula o en una vista de tarjetas.


### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Para ver las vApps en una vista de cuadrícula, haga clic en el . Para verlas en una vista de tarjeta, haga clic en el .

La lista de vApps se muestra en una cuadrícula o como una lista de tarjetas.

- 3 (opcional) Configure la vista de cuadrícula para que contenga los detalles que desea ver.
  - a En la vista de cuadrícula, haga clic en el icono **Editor de cuadrícula** ().
  - b Para seleccionar los detalles de las vApps que desea incluir en la vista de cuadrícula, marque la casilla de verificación junto a cada detalle que desea ver.

Los detalles seleccionados aparecen como columnas para cada vApp.

- 4 (opcional) En la vista de cuadrícula, haga clic en el  a la izquierda de una vApp para mostrar las acciones que puede realizar con la vApp seleccionada.

Por ejemplo, puede apagar una vApp.

## Generar una nueva vApp

En lugar de crear una vApp basada en una plantilla de vApp, puede optar por crear una vApp nueva mediante máquinas virtuales de catálogos, máquinas virtuales nuevas o una combinación de ambas.

Para generar una vApp, es necesario proporcionar un nombre y, de manera opcional, una descripción de la vApp. Es posible regresar y agregar máquinas virtuales a la vApp en una etapa posterior.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en **Nueva vApp**.
- 3 Introduzca un nombre y, si lo desea, una descripción de la vApp.
- 4 (opcional) Busque máquinas virtuales en el catálogo para agregarlas a esta vApp o haga clic en **Agregar máquina virtual** para agregar una máquina virtual vacía nueva.

Si no existe ninguna máquina virtual en el catálogo, cree una máquina virtual y agréguela a la vApp.

- a Introduzca el nombre y el nombre del equipo de la máquina virtual.

---

**Importante** El nombre de equipo solo puede contener caracteres alfanuméricos y guiones. Un nombre de equipo no puede constar solo de dígitos y no puede contener espacios.

---

- b (opcional) Introduzca una descripción significativa.
- c Seleccione cómo desea implementar la máquina virtual.

Opción	Acción
<b>Nuevo</b>	<p>Implementa una nueva máquina virtual con una configuración personalizable.</p> <ol style="list-style-type: none"> <li>1 Seleccione una familia de sistema operativo y un sistema operativo.</li> <li>2 (Opcional) Seleccione una imagen de arranque.</li> <li>3 Seleccione la política de recursos informáticos.</li> <li>4 Seleccione el tamaño de la máquina virtual o haga clic en <b>Opciones de tamaño personalizadas</b> para especificar manualmente la configuración de recursos informáticos, memoria y almacenamiento.</li> </ol> <p>Los tamaños predefinidos de la máquina virtual son pequeño, mediano o grande.</p> <ol style="list-style-type: none"> <li>5 Especifique las opciones de almacenamiento, como la política de almacenamiento y el tamaño en GB.</li> <li>6 Especifique la configuración de red para la máquina virtual, como red, modo de IP, dirección IP y NIC primaria.</li> </ol>
<b>A partir de plantilla</b>	<p>Implementa una máquina virtual a partir de una plantilla seleccionada del catálogo de plantillas.</p> <ol style="list-style-type: none"> <li>1 Seleccione la plantilla de máquina virtual a partir del catálogo.</li> <li>2 (Opcional) Seleccione esta opción para usar una política de almacenamiento personalizada y seleccione la política en <b>Política de almacenamiento personalizada que se usará</b>.</li> <li>3 Si hay un contrato de licencia de usuario final disponible, debe revisarlo y aceptarlo.</li> </ol>

- d Para agregar la máquina virtual a la vApp, haga clic en **Aceptar**.

Puede ver la máquina virtual que se agregó al catálogo.

- 5 (opcional) Repita el [paso 4](#) para cada máquina virtual adicional que desee crear dentro de la vApp.
- 6 Para completar la creación de la vApp, haga clic en **Crear**.

### Resultados

Se crea la vApp en un estado apagado. Al encender la vApp, se crean y se encienden las máquinas virtuales dentro de la vApp.


## Crear una vApp a partir de un paquete OVF

Puede crear e implementar una vApp directamente desde un paquete OVF sin crear una plantilla de vApp ni el correspondiente elemento del catálogo.

### Requisitos previos

Compruebe que tiene un paquete OVF para cargarlo y que dispone de permiso para cargar paquetes OVF e implementar vApps.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en **Agregar vApp desde OVF**.
- 3 Haga clic en el botón **Cargar** () para desplazarse hasta una ubicación accesible desde el equipo y seleccione el archivo de plantilla OVF/OVA.  
  
La ubicación puede ser el disco duro local, un recurso compartido de red o una unidad de CD/DVD. Las extensiones de archivo admitidas incluyen `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` y `.strings`. Si opta por cargar un archivo OVF, que hace referencia a más archivos de los que intenta cargar, por ejemplo, un archivo VMDK, debe examinar y seleccionar todos los archivos.
- 4 Haga clic en **Siguiente**.
- 5 Verifique los detalles de la plantilla OVF/OVA que va a implementar y haga clic en **Siguiente**.
- 6 Introduzca un nombre y, de manera opcional, una descripción para la vApp, y haga clic en **Siguiente**.
- 7 (opcional) Cambie el nombre del equipo de la vApp para que contenga únicamente caracteres alfanuméricos.

Este paso es obligatorio solo si el nombre de la vApp contiene espacios o caracteres especiales. De forma predeterminada, el nombre del equipo se rellena automáticamente con el nombre de la máquina virtual. Sin embargo, los nombres de equipo deben contener solamente caracteres alfanuméricos.



- 8 En el menú desplegable **Política de almacenamiento**, seleccione una política de almacenamiento para cada una de las máquinas virtuales de la vApp y haga clic en **Siguiente**.
- 9 Seleccione las redes a las que desea conectar cada máquina virtual.

- Seleccione una red para cada máquina virtual en el menú desplegable **Red**.
- Puede seleccionar la casilla de verificación **Cambiar al flujo de trabajo de redes avanzadas** e introducir manualmente la configuración de red, como la NIC primaria, el tipo de adaptador de red, la red, la asignación de IP y la dirección IP de cada máquina virtual en la vApp.

Puede configurar propiedades adicionales para las máquinas virtuales después de finalizar el asistente.

- 10 Haga clic en **Siguiente**.
- 11 Personalice el hardware de las máquinas virtuales de la vApp y haga clic en **Siguiente**.

Opción	Descripción
<b>Número de CPU virtuales</b>	Introduzca el número de CPU virtuales para cada máquina virtual de la vApp. El número máximo de CPU virtuales que puede asignar a una máquina virtual depende del número de CPU lógicas en el host y el tipo de sistema operativo invitado que está instalado en la máquina virtual.
<b>Núcleos por socket</b>	Introduzca el número de núcleos por socket para cada máquina virtual de la vApp.  Puede configurar el modo en que las CPU virtuales se asignan desde el punto de vista de núcleos y núcleos por socket. Determine la cantidad de núcleos de CPU que desea que tenga la máquina virtual y, a continuación, seleccione la cantidad de núcleos que desea para cada socket, en función de si desea una CPU de un solo núcleo, una CPU de dos núcleos, una CPU de tres núcleos, etc.
<b>Número de núcleos</b>	Vea la cantidad de núcleos para cada máquina virtual de la vApp. El número cambia cuando se actualiza la cantidad de CPU virtuales.
<b>Memoria total (MB)</b>	Introduzca la memoria en MB para cada máquina virtual de la vApp. Esta opción determina la cantidad de memoria del host ESXi que se asigna a la máquina virtual. El tamaño de la memoria de hardware virtual determina la cantidad de memoria que hay disponible para las aplicaciones que se ejecutan en la máquina virtual. Una máquina virtual no puede beneficiarse de más recursos de memoria que el tamaño de memoria de hardware virtual que se ha configurado.

- 12 En la página Listo para completar, revise su configuración y haga clic en **Finalizar**.

## Resultados

La nueva vApp aparecerá en la vista de tarjetas.

## Crear una vApp a partir de una plantilla de vApp



Puede crear una vApp nueva basada en una plantilla de vApp almacenada en un catálogo al que tenga acceso.

Si la plantilla de vApp está basada en un archivo OVF que incluye las propiedades OVF para personalizar sus máquinas virtuales, dichas propiedades se traspasan a la vApp. Si el usuario puede configurar algunas de dichas propiedades, especifique los valores.

### Requisitos previos

- Solo los administradores de organización y los autores de vApp pueden obtener acceso a las plantillas de vApp de los catálogos públicos.
- Los usuarios de vApp o superiores pueden obtener acceso a las plantillas de vApp de los catálogos de organización que estén compartidos para ellos.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Plantillas de vApp** en el panel izquierdo.  
  
La lista de plantillas se muestra en una vista de cuadrícula.
- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda de la plantilla de vApp que desea implementar como una vApp y seleccione **Crear vApp**.
- 3 En la página **Aceptar licencias** del asistente, lea el contrato de licencia de usuario final y haga clic en **Aceptar**.
- 4 Haga clic en **Siguiente**.
- 5 Introduzca un nombre y, si lo desea, una descripción de la vApp.
- 6 Especifique la cantidad de horas o días durante los cuales se puede ejecutar la vApp antes de detenerse automáticamente.
- 7 Especifique la cantidad de horas o días durante los cuales permanece disponible la vApp detenida antes de limpiarse de manera automática.
- 8 Haga clic en **Siguiente**.
- 9 Seleccione el centro de datos virtual en el que desea crear la vApp.
- 10 Seleccione una política de almacenamiento.
- 11 Haga clic en **Siguiente**.
- 12 Seleccione las redes a las que desea conectar cada máquina virtual.
  - Seleccione una red para cada máquina virtual en el menú desplegable **Red**.

- Puede seleccionar la casilla de verificación **Cambiar al flujo de trabajo de redes avanzadas** e introducir manualmente la configuración de red, como la NIC primaria, el tipo de adaptador de red, la red, la asignación de IP y la dirección IP de cada máquina virtual en la vApp.

Puede configurar propiedades adicionales para las máquinas virtuales después de finalizar el asistente.

**13** Haga clic en **Siguiente**.

**14** Personalice el hardware de las máquinas virtuales de la vApp y haga clic en **Siguiente**.

Opción	Descripción
Número de CPU virtuales	Introduzca el número de CPU virtuales para cada máquina virtual de la vApp. El número máximo de CPU virtuales que puede asignar a una máquina virtual depende del número de CPU lógicas en el host y el tipo de sistema operativo invitado que está instalado en la máquina virtual.
Núcleos por socket	Introduzca el número de núcleos por socket para cada máquina virtual de la vApp. Puede configurar el modo en que las CPU virtuales se asignan desde el punto de vista de núcleos y núcleos por socket. Determine la cantidad de núcleos de CPU que desea que tenga la máquina virtual y, a continuación, seleccione la cantidad de núcleos que desea para cada socket, en función de si desea una CPU de un solo núcleo, una CPU de dos núcleos, una CPU de tres núcleos, etc.
Número de núcleos	Vea la cantidad de núcleos para cada máquina virtual de la vApp. El número cambia cuando se actualiza la cantidad de CPU virtuales.
Memoria total (MB)	Introduzca la memoria en MB para cada máquina virtual de la vApp. Esta opción determina la cantidad de memoria del host ESXi que se asigna a la máquina virtual. El tamaño de la memoria de hardware virtual determina la cantidad de memoria que hay disponible para las aplicaciones que se ejecutan en la máquina virtual. Una máquina virtual no puede beneficiarse de más recursos de memoria que el tamaño de memoria de hardware virtual que se ha configurado.
Propiedades del disco duro	Introduzca el tamaño del disco duro de la máquina virtual en MB.

**15** En la página Listo para completar, revise su configuración y haga clic en **Finalizar**.


## Resultados

La nueva vApp aparecerá en la vista de tarjetas.

## Abrir una vApp

Puede abrir una vApp para ver las máquinas virtuales y las redes que contiene. También puede ver un diagrama donde se muestra la forma en que están conectadas las máquinas virtuales y las redes.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la vista de tarjetas, puede obtener información general, como el número de máquinas virtuales asociadas con la vApp, la información de concesión, la cantidad total de CPU, la memoria y el almacenamiento total, las redes asociadas y si se tomó una instantánea.
- 4 Para ver la configuración detallada de una vApp seleccionada, haga clic en **Detalles** en la tarjeta de la vApp.

## Realizar operaciones de encendido y apagado en vApps

Puede realizar operaciones de alimentación de las vApps, como el encendido, el apagado, la suspensión o el restablecimiento de una vApp.


### Encender una vApp

Al encender una vApp, se encienden todas las máquinas virtuales de la vApp que estaban apagadas.

#### Requisitos previos

Debe ser al menos autor de vApps.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea encender, seleccione **Encender**.

#### Resultados

La vApp se encenderá.


### Apagar una vApp

Al desconectar una vApp, se apagan todas las máquinas virtuales de dicha vApp. Para poder realizar ciertas acciones, antes debe apagar una vApp. Por ejemplo, agregar la vApp a un catálogo, copiarla o moverla a otro VDC.

#### Requisitos previos

La vApp debe estar iniciada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea detener, seleccione **Apagar**.
- 4 Haga clic en **Aceptar**.

### Resultados

Todas las máquinas virtuales en la vApp y la propia vApp se apagan.


## Detener una vApp

Al detener una vApp se apagan o desconectan todas las máquinas virtuales de dicha vApp. Para realizar ciertas acciones es necesario detener antes la vApp. Por ejemplo, agregar la vApp a un catálogo, copiarla o moverla a otro VDC.

### Requisitos previos

La vApp debe estar iniciada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea detener, seleccione **Detener**.
- 4 Haga clic en **Aceptar**.

### Resultados

Todas las máquinas virtuales en la vApp y la propia vApp se desconectan o se apagan.

## Restablecer una vApp


Al restablecer una vApp, se borra el estado (memoria, caché, etc.), pero la vApp sigue ejecutándose.

### Requisitos previos

La vApp está iniciada y las máquinas virtuales que contiene están encendidas.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.

- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea restablecer, seleccione **Restablecer**.

#### Resultados

Se borrará el estado y la vApp seguirá ejecutándose.


## Suspender una vApp

La suspensión de una vApp conserva su estado actual escribiendo la memoria en el disco.

#### Requisitos previos

La vApp debe estar en ejecución.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea suspender, seleccione **Suspender**.

#### Resultados

Se suspende la vApp y se conserva su estado.


## Descartar el estado de suspensión de una vApp

Si una vApp está en estado de suspensión y ya no es necesario reanudar el uso de la vApp, puede descartar el estado de suspensión. Al descartar el estado de suspensión, se quita la memoria guardada y la vApp vuelve a un estado de apagado.

#### Requisitos previos

La vApp debe estar en estado de suspensión.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp suspendida, seleccione **Descartar estado de suspensión**.

#### Resultados

El estado se descarta y la vApp se apaga.

## Editar propiedades de una vApp

Puede editar las propiedades de una vApp existente, incluidos el nombre y la descripción de la vApp, la configuración de concesiones, el orden en el que se deben iniciar las máquinas virtuales en la vApp, la configuración de uso compartido y la configuración de red.


### Editar las propiedades generales de la vApp

Puede revisar y cambiar el nombre, la descripción y otras propiedades generales de una vApp.

#### Requisitos previos

Compruebe que la vApp está apagada.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles** para ver y editar las propiedades de la vApp.
- 4 Revise y cambie las propiedades según sea necesario y luego haga clic en **Guardar**.

Opción	Acción
Nombre	Escriba un nombre nuevo para la vApp.
Descripción	Escriba una descripción opcional de la vApp.
Centro de datos virtuales	El nombre del centro de datos al que pertenece la vApp.
Instantánea	Si hay una instantánea, se muestran sus detalles.
Concesiones	<p>Seleccione <b>Renovar</b> para renovar la concesión.</p> <p>a Programe la concesión de tiempo de ejecución en número de horas o días.</p> <p>Define durante cuánto tiempo se puede ejecutar la vApp antes de detenerse automáticamente.</p> <p>b Programe la concesión de almacenamiento en número de horas o días.</p> <p>Define durante cuánto tiempo la vApp permanece disponible antes de eliminarse automáticamente.</p>

#### Resultados

La configuración general se guardará.

## Editar las propiedades avanzadas de una vApp


Puede configurar el orden de inicio y detención de las máquinas virtuales dentro de la vApp. Configure el orden de inicio y detención si tiene aplicaciones instaladas en las máquinas virtuales que se deben iniciar y detener en un orden determinado.

Esta configuración resulta útil si tiene que iniciar y detener las máquinas virtuales en un orden determinado. Por ejemplo, una máquina virtual contiene un servidor de base de datos, otra alberga un servidor de aplicaciones y la última contiene un servidor web. Para que las funciones relacionadas funcionen correctamente, primero debe iniciarse el servidor de base de datos, después el servidor de aplicaciones y, por último, el servidor web.

### Requisitos previos

Compruebe que la vApp está apagada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles** y desplácese hacia abajo hasta llegar a las propiedades avanzadas de la vApp.
- 4 Introduzca las propiedades de orden de inicio y detención de cada máquina virtual y haga clic en **Guardar**.

Opción	Acción
<b>Orden de inicio</b>	Especifique el orden en el que desea que se inicie la máquina virtual. Debe escribir un valor para cada máquina en la secuencia.
<b>Acción de inicio</b>	<p>Seleccione una acción de inicio.</p> <p>La acción de inicio determina lo que le sucede a una máquina virtual cuando se inicia la vApp que la contiene. Esta opción está establecida en <b>Encender</b> de manera predeterminada.</p>
<b>Espera de inicio</b>	<p>Especifique el tiempo de espera de inicio.</p> <p>El tiempo de espera de inicio es la cantidad de tiempo (en segundos) que desea esperar antes de que vCloud Director inicie la siguiente máquina en la secuencia.</p>




Opción	Acción
Acción de detención	<p>Seleccione la acción de detención.</p> <p>La acción de detención es la acción que realiza la máquina virtual cuando se detiene la vApp que la contiene. Si selecciona <b>Apagar</b>, la máquina virtual se apaga sin realizar acciones de desconexión que garanticen la estabilidad (lo que equivaldría a desconectar un cable de un enchufe). Seleccione esta acción si no ha instalado VMware Tools. De lo contrario, seleccione <b>Desconectar</b> para garantizar la estabilidad durante la desconexión.</p>
Espera de detención	<p>Especifique el tiempo de espera de detención.</p> <p>El tiempo de espera de detención es la cantidad de tiempo (en segundos) que desea esperar antes de que vCloud Director desconecte la siguiente máquina virtual en la secuencia.</p>

## Compartir una vApp

Puede compartir las vApps con otros grupos o usuarios dentro de la organización. Los controles de acceso establecidos determinan las operaciones que se pueden completar en las vApps compartidas.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles** y desplácese hacia abajo hasta llegar a las propiedades de uso compartido de la vApp.

#### 4 Seleccione los usuarios con los cuales desea compartir la vApp y haga clic en **Guardar**.

Opción	Acción
<b>Compartir con todos en la organización</b>	<p>Seleccione esta opción para compartir con todos los usuarios de la organización y seleccione el nivel de acceso.</p> <ul style="list-style-type: none"> <li>■ Para conceder un control total, seleccione <b>Control total</b>.</li> </ul> <p>Todos los usuarios en la organización pueden abrir, iniciar, guardar una vApp como una plantilla de vApp, agregar la plantilla a un catálogo, cambiar el propietario de la vApp, copiar en un catálogo y modificar las propiedades.</p> <ul style="list-style-type: none"> <li>■ Para conceder acceso de solo lectura, seleccione <b>Solo lectura</b>.</li> </ul>
<b>Compartir con usuarios y grupos específicos</b>	<p>Seleccione esta opción para compartir únicamente con los usuarios que especifique.</p> <ol style="list-style-type: none"> <li>Seleccione los nombres en el panel <b>Usuarios y grupos sin acceso</b> para moverlos al panel <b>Usuarios y grupos con acceso</b>.</li> <li>Seleccione un nivel de acceso para los usuarios y los grupos especificados. <ul style="list-style-type: none"> <li>■ Para otorgar un control total, seleccione <b>Control total</b>.</li> </ul> <p>Los usuarios con control total pueden abrir, iniciar, guardar una vApp como una plantilla de vApp, agregar la plantilla a un catálogo, cambiar el propietario de la vApp, copiar en un catálogo y modificar las propiedades.</p> <ul style="list-style-type: none"> <li>■ Para otorgar acceso de solo lectura, seleccione <b>Solo lectura</b>.</li> </ul> </li> </ol>

#### Resultados

La vApp se compartirá con los usuarios o grupos especificados.


## Mostrar un diagrama de red de vApp

Un diagrama de red de vApp proporciona una vista gráfica de las máquinas virtuales y redes de una vApp.

#### Requisitos previos

Para ver el diagrama de red de vApp, su vApp debe contener menos de 40 máquinas virtuales. Si contiene más de 40 máquinas virtuales, el diagrama no estará disponible.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.

#### 4 Haga clic en la pestaña **Diagrama de redes**.

Aparece el diagrama que muestra cómo se conectan las máquinas virtuales y las redes en la vApp. El símbolo de estrella representa una NIC primaria. Si una NIC está conectada, su color es verde. Si no está conectada, su color es blanco.

#### 5 (opcional) Para resaltar las redes y las máquinas virtuales conectadas, haga clic en una red o una máquina virtual.

Se resaltarán los objetos conectados y las conexiones entre ellos.

#### Pasos siguientes

Puede agregar máquinas virtuales o redes desde esta página.

## Trabajar con redes en una vApp

Las máquinas virtuales de una vApp pueden conectarse a redes de vApp (aisladas o enrutadas) y a redes de centros de datos virtuales de organización (directas o con barreras). Puede agregar redes de distintos tipos a una vApp para resolver varios escenarios de redes.

Las máquinas virtuales de la vApp pueden conectarse a las redes que están disponibles en una vApp. Si desea conectar una máquina virtual con una red distinta, primero debe agregarla a la vApp.

Una vApp puede incluir redes de vApp y redes de centros de datos virtuales de organización. Una red de vApp puede estar aislada o enrutada. Una red de vApp aislada está dentro de la vApp. También puede enrutar una red de vApp a una red de centros de datos virtuales de organización para proporcionar conectividad a máquinas virtuales fuera de la vApp. Para redes de vApp enrutadas, puede configurar servicios de redes, tal como un firewall y enrutamiento estático.

Puede conectar una vApp directamente a una red de centros de datos virtuales de organización. Si tiene varias vApps que contienen máquinas virtuales idénticas conectadas a la misma red de centros de datos virtuales de organización y desea iniciar las vApps al mismo tiempo, puede crear barreras para la vApp. Esto le permite encender las máquinas virtuales sin que se produzcan conflictos mediante el aislamiento de las direcciones MAC e IP.

Las redes que se agregan a la vApp utilizan el grupo de redes que está asociado con el centro de datos virtual de organización en el que se creó la vApp.



## Ver las redes de una vApp

Puede obtener acceso y ver las redes de una vApp.

#### Requisitos previos

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.

- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 Haga clic en la pestaña **Redes**.  
Se muestra la lista de redes, si existen. Puede ver información acerca de cada red, como el nombre, la puerta de enlace, la máscara de red y la conexión, y conservar recursos IP y de NAT.
- 5 (opcional) Para editar las columnas que desea ver, haga clic en el icono **Editor de cuadrícula** () y seleccione o anule la selección de las casillas de verificación de las columnas que desea mostrar u ocultar, respectivamente.

## Colocar una barrera de red de vApp


Encender máquinas virtuales idénticas que están incluidas en distintas vApps podría provocar un conflicto. Para permitir el encendido de máquinas virtuales idénticas en diferentes vApps sin conflictos, debe colocar una barrera en la vApp.

La barrera de una vApp aísla las direcciones IP y MAC de las máquinas virtuales y cambia el tipo de conexión de redes de VDC de organización directas a redes con barrera. En las redes con barrera, el firewall se habilita y se configura automáticamente para permitir solo tráfico saliente. Cuando se coloca una barrera en una vApp, también se pueden configurar las reglas de firewall y NAT en las redes con barrera.

### Requisitos previos

- Solo se pueden colocar barreras en redes de vApp directas. Si la vApp utiliza más de una red y las otras redes son, por ejemplo, enrutadas, solo se colocará una barrera en la red directa.
- Las máquinas virtuales de la vApp que utilizan la red directa deben detenerse para que la red de vApp directa no esté en uso en ese momento.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Detalles**.
- 4 Haga clic en la pestaña **Redes**.
- 5 Si la vApp no tiene barreras, haga clic en el botón **Editar**.
- 6 Active la opción **Crear barrera en vApp** y haga clic en **Aceptar**.

## Resultados

Las direcciones IP y MAC de las máquinas virtuales se aíslan. Puede encender máquinas virtuales idénticas en diferentes vApps sin que ocurran conflictos.

## Agregar una red a una vApp

Es posible agregar una red a una vApp para que la red esté disponible para las máquinas virtuales de la vApp. Se puede agregar una red de vApps o una red de centros de datos virtuales de organización a una vApp.


Las conexiones pueden ser directas o con barrera. La barrera permite que se enciendan sin dificultades máquinas virtuales idénticas en distintas vApp al aislar las direcciones MAC e IP de las máquinas virtuales.

Cuando se habilita la barrera y se enciende la vApp, se crea una red aislada a partir del grupo de redes de centros de datos virtuales de organización. Se crea una puerta de enlace Edge que se conecta a la red aislada y a la red de centros de datos virtuales de organización. El tráfico hacia las máquinas virtuales y desde ellas pasa a través de la puerta de enlace Edge, lo cual traduce la dirección IP mediante NAT y proxy-AR. Esto permite que un enrutador pase tráfico entre dos redes mediante el mismo espacio IP.

### Requisitos previos

Para agregar una red de centros de datos virtuales de organización, el administrador debe haber creado una red de ese tipo.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta de la vApp seleccionada, haga clic en **Acciones** y seleccione **Agregar red**.
- 4 Seleccione el tipo de red que desea agregar.

Opción	Acción
Red de VDC de organización	Seleccione una red de centros de datos virtuales de organización a partir de la lista de redes disponibles.
Red de vApp	<ol style="list-style-type: none"> <li>a Introduzca un nombre y, si lo desea, una descripción de la red.</li> <li>b Introduzca el CIDR de la puerta de enlace de red.</li> <li>c (Opcional) Introduzca el DNS primario, el DNS secundario y el sufijo DNS.</li> <li>d (Opcional) Seleccione si desea permitir una VLAN invitada.</li> <li>e (Opcional) Introduzca la configuración del grupo de direcciones IP estáticas, como los rangos de IP.</li> <li>f (Opcional) Para poder conectarse a una red de centros de datos virtuales de organización, alterne la opción <b>Conectarse a una red de VDC de organización</b> y seleccione una red de la lista.</li> </ol>

5 Haga clic en **Agregar**.

#### Resultados

La red se agregará a la vApp.

#### Pasos siguientes

Conecte una máquina virtual en la vApp a la red.

## Configuración de servicios de redes para una red de vApp

Puede configurar los servicios de red, tal como DHCP, firewall, conversión de direcciones de red (NAT), VPN y enrutamiento estático para ciertas redes de vApp.

Los servicios de redes disponibles dependen del tipo de red de vApp.


Tabla 3-1. Servicios de red disponibles por tipo de red

Tipo de red de vApp	DHCP	Firewall	NAT	Enrutamiento estático
Directa				
Con enrutamiento	X	X	X	X
Aislada	X			

## Ver y editar los detalles generales de la red

Puede ver y editar los detalles generales de la red de vApp, por ejemplo el nombre de la red y su descripción.


#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **General**, revise la información de la red.
- 6 Haga clic en **Editar**.
- 7 Edite el nombre y la descripción de la red de vApp.
- 8 Haga clic en **Guardar**.

## Editar la configuración del grupo de direcciones IP estáticas de una red de vApp

Puede configurar una red de vApp a fin de proporcionar direcciones IP estáticas para las máquinas virtuales de la vApp; para ello, intégrealas desde un grupo de direcciones IP estáticas.


### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Administración de direcciones IP**, haga clic en **Grupos estáticos**.
- 6 Haga clic en **Editar**.
- 7 Introduzca un rango de IP y haga clic en **Agregar**.
- 8 Haga clic en **Guardar**.

### Editar la configuración de DNS de una red de vApp

Después de crear una red de vApp, puede ver y editar la configuración de DNS en cualquier momento.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Administración de direcciones IP**, haga clic en **DNS**.  
Se mostrará la configuración de DNS.
- 6 Haga clic en **Editar**.
- 7 Edite el DNS primario, el DNS secundario y el sufijo DNS.
- 8 Haga clic en **Guardar**.

### Configurar DHCP para una red de vApp


Puede configurar ciertas redes de vApp para proporcionar los servicios de DHCP a máquinas virtuales en vApp.

Al habilitar DHCP para una red de vApp, conecte una NIC en una máquina virtual de la vApp para esa red y seleccione DHCP como el modo de IP para esa NIC. vCloud Director asigna una dirección IP de DHCP a la máquina virtual cuando esta se enciende.

## Requisitos previos

Una red de vApp enrutada o una red de vApp aislada.


### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Administración de direcciones IP**, haga clic en **DHCP**.  
Se muestra el estado de DHCP.
- 6 Haga clic en **Editar**.
- 7 Haga clic en **Habilitado**.
- 8 En el cuadro de texto **Grupo de direcciones IP**, introduzca un rango de direcciones IP.  
vCloud Director utiliza estas direcciones para responder a las solicitudes DHCP. El rango de las direcciones IP de DHCP no puede superponerse con el grupo de direcciones IP estáticas para la red de vApp.
- 9 Establezca el tiempo de concesión predeterminado y máximo en segundos.
- 10 Haga clic en **Guardar**.

## Mostrar las asignaciones de IP de una red de vApp

Puede revisar las asignaciones de IP de las redes de vApp de su organización.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Administración de direcciones IP**, haga clic en **Asignaciones de IP**.  
Se mostrarán las direcciones IP asignadas.

## Configurar el enrutamiento estático para una red de vApp

Puede configurar ciertas redes de vApp para que proporcionen servicios de enrutamiento estático a fin de permitir que las máquinas virtuales de distintas redes de vApp se comuniquen.




Cualquier ruta estática que se cree se habilita automáticamente.

### Requisitos previos

Debe existir una red de vApp con enrutamiento.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.
- 5 En la pestaña **Enrutamiento**, haga clic en **Editar**.

Puede habilitar o deshabilitar el enrutamiento estático para la red.

## Agregar enrutamiento estático para una red de vApp

Puede agregar rutas estáticas entre dos redes de vApp enrutadas a la misma red de centros de datos virtuales de organización. Las rutas estáticas permiten el tráfico entre redes.


No puede agregar rutas estáticas a una vApp con barreras o entre redes que se solapan. Tras agregar una ruta estática en una red de vApp, configure las reglas de firewall de red para permitir el tráfico en la ruta estática. Para vApps con rutas estáticas, utilice las direcciones IP asignadas hasta que se eliminen la vApp o las redes asociadas.

Las rutas estáticas solo funcionan cuando se ejecutan las vApp que contienen las rutas. Si cambia la red principal de una vApp, elimina una vApp o elimina una red de vApp y la vApp incluye rutas estáticas, dichas rutas no pueden funcionar y se deben quitar manualmente.

### Requisitos previos

- Dos redes de vApp se enrutan a la misma red de centros de datos virtuales de organización.
- Las redes de vApp se encuentran en vApp que fueron iniciadas al menos una vez.
- El enrutamiento estático está habilitado en ambas redes de vApp.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, haga clic en una red para ver los detalles de la red.

- 5 En la pestaña **Enrutamiento**, haga clic en **Agregar** bajo Enrutamiento estático.  
Se mostrarán las direcciones IP asignadas.
- 6 Introduzca el nombre de la ruta estática.
- 7 Introduzca la dirección de red con el formato CIDR.  
La dirección de red es para la red de vApp a la que se agrega una ruta estática.
- 8 Introduzca la dirección IP del próximo salto.  
La dirección IP del próximo salto es la dirección IP externa de ese enrutador de la red de vApp.
- 9 Haga clic en **Guardar**.
- 10 Repita el mismo procedimiento para la segunda red de vApp.

### Ejemplo: Ejemplo de enrutamiento estático

La red de vApp 1 y la red de vApp 2 se enrutan a una red de organización compartida. Puede crear una ruta estática en cada red de vApp para permitir el tráfico entre las redes. Puede utilizar información acerca de las redes de vApp para crear las rutas estáticas.

**Tabla 3-2. Información de red**

Nombre de red	Especificación de red	Dirección IP externa del enrutador
Red de vApp 1	192.168.1.0/24	192.168.0.100
Red de vApp 2	192.168.2.0/24	192.168.0.101
Red de organización compartida	192.168.0.0/24	No corresponde

En la Red de vApp 1, cree una ruta estática para la Red de vApp 2. En la Red de vApp 2, cree una ruta estática para la Red de vApp 1.

**Tabla 3-3. Configuración de enrutamiento estático**

Red de vApp	Nombre de ruta	Red	Dirección IP de siguiente salto
Red de vApp 1	tovapp2	192.168.2.0/24	192.168.0.101
Red de vApp 2	tovapp1	192.168.1.0/24	192.168.0.100


## Eliminar una red de vApp

Puede eliminar redes de una vApp cuando ya no las necesite.

### Requisitos previos

Se ha detenido una vApp y no hay máquinas virtuales en la vApp conectadas a la red.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En la tarjeta del dispositivo virtual seleccionado, haga clic en **Detalles**.
- 4 En la pestaña **Redes**, seleccione la red que desea eliminar, haga clic en **Eliminar** y confirme la eliminación.

## Trabajar con instantáneas

La creación de una instantánea conserva el estado y los datos de las máquinas virtuales en una vApp en un momento específico. Las instantáneas no están diseñadas con el objetivo de utilizarse para períodos largos de tiempo ni en lugar de copias de seguridad de la vApp.

Se recomienda utilizar una instantánea al actualizar las máquinas virtuales de una vApp. Por ejemplo, antes de actualizar las máquinas virtuales, debe crear una instantánea para conservar el momento específico antes de la actualización. Para ello, debe guardar una instantánea antes de actualizar y, a continuación, puede realizar la actualización. Si no hay problemas durante la actualización, puede quitar la instantánea, lo que confirmará los cambios realizados durante la actualización. Sin embargo, si se ha producido un problema, puede revertir a la instantánea, que restaurará el estado guardado que tenía la vApp antes de la actualización.


### Tomar una instantánea de una vApp

Al tomar una instantánea de una vApp, se crean instantáneas de todas las máquinas virtuales en la vApp. Después de tomar la instantánea, puede restaurar todas las máquinas virtuales de la vApp a la instantánea o eliminar la instantánea si no la necesita.

Las instantáneas de vApps tienen algunas limitaciones.

- Las instantáneas de vApps no capturan configuraciones de NIC.
- Si una máquina virtual de la vApp está conectada a un disco independiente, no se puede tomar una instantánea de la vApp.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp de la que desea tomar una instantánea, seleccione **Crear instantánea**.

Al tomar una instantánea de una vApp, se reemplaza la instantánea existente, si existe una.

**4** (opcional) Seleccione si desea crear una instantánea de la memoria de la vApp.

Cuando se captura el estado de la memoria de vApp, la instantánea retiene el estado activo de la vApp y las máquinas virtuales de la vApp. Las instantáneas creadas con memoria realizan una instantánea en un momento preciso, por ejemplo, para actualizar software que aún está en funcionamiento. Si crea una instantánea de memoria y la actualización no finaliza de la manera esperada, o si el software no cumple con sus expectativas, puede realizar una reversión al estado anterior de la máquina virtual.

Cuando se captura el estado de la memoria, no es necesario poner en modo inactivo los archivos de la vApp. Si no se captura el estado de la memoria, la instantánea no guarda el estado activo de la vApp y los discos tienen coherencia ante fallos, a menos que se pongan en modo inactivo.

**5** (opcional) Seleccione si desea poner en modo inactivo el sistema de archivos invitado.

Para esta operación, VMware Tools debe estar instalado en las máquinas virtuales de la vApp. Cuando se pone una máquina virtual en modo inactivo, VMware Tools pone en modo inactivo al sistema de archivos de la máquina virtual. Una operación de puesta en modo inactivo garantiza que el disco de la instantánea represente un estado coherente de los sistemas de archivo invitados. Las instantáneas en modo inactivo resultan adecuadas para las copias de seguridad automatizadas o periódicas. Por ejemplo, si se desconoce la actividad de la máquina virtual, pero se desea disponer de varias copias de seguridad recientes para realizar reversiones, es posible poner los archivos en modo inactivo.

Las vApps que tienen discos de gran capacidad no se pueden poner en modo inactivo.

**6** Haga clic en **Aceptar**.

**Resultados**

Se crea una instantánea de la vApp.

**Pasos siguientes**

Puede revertir todas las máquinas virtuales de la vApp a la instantánea más reciente.

## Revertir una vApp a una instantánea

Puede revertir todas las máquinas virtuales de una vApp al estado en el que se encontraban cuando se creó la instantánea de la vApp.

**Requisitos previos**

Compruebe que la vApp tenga una instantánea.

**Procedimiento**

**1** En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.

**2** Haga clic en  para ver las vApps en una vista de tarjetas.

3 En el menú **Acciones** de la vApp que desea revertir, seleccione **Revertir a instantánea**.

4 Haga clic en **Aceptar**.

#### Resultados

Todas las máquinas virtuales de la vApp se revertirán al estado de la instantánea.

## Quitar una instantánea de una vApp


Puede quitar una instantánea de una vApp.

Al eliminar una instantánea de la vApp, se elimina el estado de las máquinas virtuales en la instantánea de la vApp y ya no es posible volver a ese estado. Eliminar una instantánea no afecta al estado actual de la vApp.

#### Requisitos previos

Ha tomado una instantánea de la vApp.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp de la cual desea eliminar una instantánea, seleccione **Quitar instantánea**.
- 4 Haga clic en **Aceptar**.

#### Resultados

Se quitará la instantánea.


## Cambiar el propietario de una vApp

Es posible cambiar el propietario de una vApp, por ejemplo, cuando el propietario deja la empresa o su función cambia dentro de la misma.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.

- 3 En el menú **Acciones** de la vApp cuyo propietario desea cambiar, seleccione **Cambiar propietario**.
- 4 Seleccione un usuario de la lista.
- 5 Haga clic en **Aceptar**.

#### Resultados

Se cambia el propietario de la vApp.


## Mover una vApp a otro centro de datos virtual

Al mover una vApp a otro centro de datos virtual, la vApp se elimina del centro de datos virtual de origen.

#### Requisitos previos

- Debe ser al menos **autor de vApp**.
- La vApp está apagada.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea mover, seleccione **Mover a**.
- 4 Seleccione el centro de datos virtual al que desea mover la vApp y haga clic en **Aceptar**.
- 5 (opcional) Seleccione la política de almacenamiento.
- 6 Haga clic en **Aceptar**.

#### Resultados

La vApp se quitará del centro de datos de origen y se moverá al centro de datos de destino.


## Copiar una vApp detenida en otro centro de datos virtual

Al copiar una vApp en otro centro de datos virtual, la vApp original permanece en el centro de datos virtual de origen.

#### Requisitos previos

- Debe ser al menos **autor de vApp**.
- La vApp está apagada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea copiar, seleccione **Copiar a**.
- 4 Escriba un nombre y descripción.
- 5 Seleccione el centro de datos virtual en el que desea crear una copia de la vApp.
- 6 (opcional) Seleccione una política de almacenamiento.
- 7 Haga clic en **Aceptar**.

### Resultados

La vApp se copia con el nombre y la descripción que proporcionó en el centro de datos virtual especificado.

## Copiar una vApp encendida


Para crear una vApp nueva basada en otra existente, puede copiar una vApp y modificar la copia para satisfacer sus necesidades. No necesita apagar las máquinas virtuales de la vApp para copiar la vApp. El estado de memoria de las máquinas virtuales en ejecución se conserva en la vApp copiada.

### Requisitos previos

Verifique que se cumplan las siguientes condiciones.

- Debe ser al menos **usuario de vApp**.
- El centro de datos virtual de organización está respaldado por vCenter Server 5.5 o posterior.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea copiar, seleccione **Copiar a**.
- 4 Escriba un nombre y descripción.
- 5 Seleccione el centro de datos virtual en el que desea crear una copia de la vApp.
- 6 (opcional) Seleccione una política de almacenamiento.
- 7 Haga clic en **Aceptar**.

## Resultados

Se crea una copia de la vApp en un estado de suspensión. Se habilita la barrera de red en la vApp copiada.

## Pasos siguientes

Modifique las propiedades de red de la nueva vApp o encienda la vApp.

# Agregar una máquina virtual a una vApp

Puede agregar una máquina virtual a una vApp.

## Requisitos previos

Debe ser **administrador de organización** o **autor de vApp** para acceder a las máquinas virtuales de catálogos públicos.

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.

- 2 Haga clic en  para ver las vApps en una vista de tarjetas.

- 3 En el menú **Acciones** de la vApp a la que desea agregar una máquina virtual, seleccione **Agregar MV**.

La lista de máquinas virtuales asociadas a la vApp se muestra en la ventana **Agregar MV**.

- 4 Para crear una nueva máquina virtual y asociarla a la vApp de forma automática, haga clic en **Agregar máquina virtual**.

- 5 Introduzca el nombre y el nombre del equipo de la máquina virtual.

---

**Importante** El nombre de equipo solo puede contener caracteres alfanuméricos y guiones. Un nombre de equipo no puede constar solo de dígitos y no puede contener espacios.

---

- 6 (opcional) Introduzca una descripción significativa.
- 7 Seleccione si desea que la máquina virtual se encienda inmediatamente después de crearse.



## 8 Seleccione cómo desea implementar la máquina virtual.

Opción	Acción
<b>Nuevo</b>	<p>Implementa una nueva máquina virtual con una configuración personalizable.</p> <ul style="list-style-type: none"> <li>a Seleccione una familia de sistema operativo y un sistema operativo.</li> <li>b (Opcional) Seleccione una imagen de arranque.</li> <li>c Seleccione la política de recursos informáticos.</li> <li>d Seleccione el tamaño de la máquina virtual o haga clic en <b>Opciones de tamaño personalizadas</b> para especificar manualmente la configuración de recursos informáticos, memoria y almacenamiento.</li> </ul> <p>Las opciones de tamaño predefinidas son pequeño, mediano o grande.</p> <ul style="list-style-type: none"> <li>e Especifique la configuración de almacenamiento de la máquina virtual, como la política de almacenamiento y el tamaño en GB.</li> <li>f Especifique la configuración de red para la máquina virtual, como red, modo de IP, dirección IP y NIC primaria.</li> </ul>
<b>A partir de plantilla</b>	<p>Implementa una máquina virtual a partir de una plantilla seleccionada del catálogo de plantillas.</p> <ul style="list-style-type: none"> <li>a Seleccione la plantilla de máquina virtual a partir del catálogo.</li> <li>b (Opcional) Seleccione esta opción para usar una política de almacenamiento personalizada y seleccione la política en <b>Política de almacenamiento personalizada que se usará</b>.</li> <li>c Si hay un contrato de licencia de usuario final disponible, debe revisarlo y aceptarlo.</li> </ul>

9 Haga clic en **Aceptar** para crear la máquina virtual.

10 Haga clic en **Agregar** para agregar la máquina virtual a la vApp.


## Guardar una vApp como plantilla de vApp en un catálogo

Al agregar una vApp a un catálogo, se convierte esa vApp determinada en una plantilla de vApp.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.
- La organización debe tener un catálogo y un centro de datos virtual con espacio disponible.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.

- 3 En el menú **Acciones** de la vApp que desea agregar a un catálogo, seleccione **Agregar a catálogo**.

**Nota** Puede agregar vApps a un catálogo incluso si las máquinas virtuales que pertenecen a la vApp están en ejecución. Sin embargo, si selecciona una vApp en ejecución, esta se añade al catálogo como una plantilla de vApp y todas las máquinas virtuales se encuentran en estado de suspensión.

- 4 Seleccione el catálogo de destino del menú desplegable **Catálogo**.
- 5 Escriba un nombre y, si lo desea, una descripción para la plantilla de vApp.
- 6 (opcional) Si desea que el nuevo elemento de catálogo sobrescriba cualquier plantilla de vApp existente, seleccione **Sobrescribir elemento de catálogo** y el elemento de catálogo que desea sobrescribir.

Por ejemplo, al cargar una nueva versión de una vApp en el catálogo, es posible que desee sobrescribir la versión anterior.

- 7 Especifique cómo se utilizará la plantilla.

La configuración se aplica al crear una vApp basada en la plantilla de vApp. En cambio, se omite al generar una vApp mediante máquinas virtuales independientes a partir de esta plantilla.

Opción	Descripción
<b>Realizar copia idéntica</b>	Seleccione esta opción para realizar una copia idéntica de la vApp cuando se crea una vApp a partir de la plantilla de vApp.
<b>Personalizar configuración de MV</b>	Seleccione esta opción para habilitar la personalización de la configuración de máquina virtual cuando se crea una vApp a partir de la plantilla de vApp.

- 8 Haga clic en **Aceptar** para completar la creación de la plantilla de vApp.

#### Resultados

La vApp se guardará como una plantilla de vApp y aparecerá en el catálogo especificado.


## Descargar una vApp como un paquete OVF

Puede descargar una vApp como un paquete OVF o como un archivo OVA, que es una distribución de un solo archivo del mismo paquete de archivos OVF.

#### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.
- Compruebe que la vApp esté apagada y sin implementar.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Haga clic en  para ver las vApps en una vista de tarjetas.
- 3 En el menú **Acciones** de la vApp que desea descargar, seleccione **Descargar**.
- 4 Seleccione el formato en que desea descargar la vApp.
- 5 (opcional) Seleccione **Proteger información de identidad** para incluir los UUID y las direcciones MAC de las máquinas virtuales que residen en la vApp en el paquete OVF descargado.  
  
Esto limita la portabilidad del paquete y debe utilizarse solo cuando sea necesario.
- 6 Haga clic en **Aceptar** para confirmar la selección e iniciar la descarga.

### Resultados

De forma predeterminada, el paquete se descarga en la carpeta *Descargas* del navegador.

## Renovar una concesión de vApp

Si la concesión de una vApp ha caducado o está a punto de caducar, puede renovarla.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Usuario de vApp** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Seleccione la vApp que desea renovar.
- 3 En el menú **Acciones**, seleccione **Renovar concesión**.

### Resultados

La concesión se renovará. Puede ver el nuevo período de tiempo de concesión en el campo **Concesión**.

## Eliminar una vApp

Al eliminar una vApp, desaparece de la organización.

### Requisitos previos

Debe detener la vApp.

Debe ser al menos **autor de vApp**.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **vApps** en el panel izquierdo.
- 2 Seleccione la vApp que desea eliminar.
- 3 En el menú **Acciones**, seleccione **Eliminar**.
- 4 Haga clic en **Aceptar**.

#### Resultados

Se eliminará la vApp.

# Administrar redes de VDC de organización

# 4

Un **administrador de organización** o un **administrador del sistema** crean redes de centros de datos virtuales de organización y las asignan al centro de datos virtual de organización. Los **administradores de organización** pueden visualizar la información acerca de las redes o configurar servicios de red, entre otras cosas.

---

**Nota** En este capítulo, se supone que los recursos de red subyacentes están respaldados por NSX Data Center for vSphere. Para los centros de datos virtuales de organización que respalda NSX-T Data Center, solo el **proveedor de servicios** puede crear redes de centros de datos virtuales de organización.

---

Puede utilizar redes de centros de datos virtuales de organización directas, enrutadas, internas o entre VDC.

**Tabla 4-1. Tipos de redes de centros de datos virtuales de organización**

Red de tipo de centro de datos	Descripción
Directa	<p>Varios VDC de organización pueden obtener acceso. Las máquinas virtuales que pertenecen a VDC de organización distintos pueden conectarse y ver el tráfico de esta red.</p> <p>La red proporciona conectividad de capa 2 directa a las máquinas virtuales fuera del VDC de organización. Dichas máquinas pueden conectarse directamente a las máquinas virtuales en el VDC de organización.</p> <p><b>Nota</b> Solo el <b>administrador del sistema</b> puede agregar una red de VDC de organización directa.</p> <p>Puede ser IPv4 o IPv6.</p>
Aislada (interna)	<p>Solo el mismo VDC organización puede obtener acceso. Las máquinas virtuales en este VDC de organización son las únicas que pueden conectarse a la red de VDC de organización interna y ver el tráfico de esta.</p> <p>La red de VDC de organización aislada proporciona a un VDC de organización una red privada y aislada a la que se pueden conectar varias máquinas virtuales y vApps. La red no proporciona conectividad con máquinas virtuales fuera del VDC de organización. Dichas máquinas no tienen conectividad con las máquinas del VDC de organización. Puede estar respaldada por un grupo de redes o un conmutador lógico de NSX-T.</p> <p><b>Nota</b> Solo el <b>proveedor de servicios</b> puede agregar redes de centros de datos virtuales de organización de NSX-T. Puede agregar una red de VDC de organización aislada respaldada solo por un grupo de redes.</p> <p>Solo puede ser IPv4.</p>
Con enrutamiento	<p>Solo el mismo VDC organización puede obtener acceso. Las máquinas virtuales de este VDC organización son las únicas que pueden conectarse a la red.</p> <p>Además, esta red proporciona un acceso controlado a una red externa. Como <b>administrador del sistema</b> o <b>administrador de la organización</b>, puede configurar los ajustes de traducción de direcciones de red (Network Address Translation, NAT), firewall y VPN para que sea posible acceder a máquinas virtuales específicas desde la red externa.</p> <p>Puede ser IPv4 o IPv6.</p>
Entre VDC	<p>Esta red forma parte de una red extendida que abarca un grupo de centros de datos. Un grupo de centros de datos puede incluir entre dos y cuatro centros de datos virtuales de organización en una implementación de vCloud Director de uno o varios sitios.</p> <p>Las máquinas virtuales conectadas a esta red se conectan a la red expandida subyacente.</p> <p>Solo puede ser IPv4.</p> <p>Para obtener información sobre las redes de Cross-VDC, consulte <a href="#">Capítulo 5 Administrar redes entre los centros de datos virtuales</a>.</p>

Todos los pasos para administrar las redes de centros de datos virtuales de la organización se documentan suponiendo que tiene más de un centro de datos virtual.

Este capítulo incluye los siguientes temas:

- [Ver las redes de VDC de organización disponibles](#)
- [Agregar una red de centros de datos virtuales de organización aislada](#)

- [Agregar una red de centros de datos virtuales de organización enrutada](#)
- [Agregar una red de centros de datos virtuales de organización directa](#)
- [Editar la configuración general de una red de centros de datos virtuales de organización](#)
- [Convertir una red de centros de datos virtuales de organización](#)
- [Convertir la interfaz de una red de VDC de organización enrutada](#)
- [Ver las direcciones IP usadas para una red de centros de datos virtuales de organización](#)
- [Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización](#)
- [Editar o eliminar rangos de IP utilizados en una red de centros de datos virtuales de organización](#)
- [Editar la configuración de DNS de una red de centros de datos virtuales de organización](#)
- [Configurar las opciones de DHCP para una red de centros de datos virtuales de organización aislada](#)
- [Editar o eliminar un grupo DHCP existente para una red](#)
- [Restablecer una red de centros de datos virtuales de organización](#)
- [Eliminar una red de centros de datos virtuales de organización](#)

## Ver las redes de VDC de organización disponibles

Puede ver las redes de centros de datos virtuales de organización disponibles.

### Requisitos previos

Esta operación requiere las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.

### Procedimiento

- ◆ En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.

### Resultados

Verá una lista de las redes disponibles que puede ordenar por nombre.

### Pasos siguientes

Puede agregar una red nueva. También puede editar, eliminar o restablecer una red existente.

## Agregar una red de centros de datos virtuales de organización aislada

Puede agregar una red de VDC de organización aislada a la que solo pueda acceder esta organización. La red no proporciona conectividad con máquinas virtuales fuera de la organización. Esas máquinas no tendrán conectividad con las máquinas virtuales de la organización.

Puede agregar una combinación de redes de VDC de organización aisladas y enrutadas para satisfacer las necesidades de su organización. Por ejemplo, puede aislar una red que contiene información confidencial y tener una red independiente asociada con una puerta de enlace Edge y conectada a Internet.

Puede crear una red de VDC aislada que un grupo de redes respalde. El proveedor de servicios también puede crear una red de VDC aislada que esté respaldada por un conmutador lógico de NSX-T.

Puede crear solo una red de VDC de organización aislada IPv4.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en **Agregar**.
- 3 En la página **Seleccionar tipo de red**, seleccione **Aislada** y haga clic en **Siguiente**.
- 4 Introduzca un nombre significativo para la red de VDC de organización.
- 5 Introduzca la configuración de enrutamiento de interdominios sin clases (Classless Inter-Domain Routing, CIDR) para la red aislada.

Utilice el formato *dirección\_IP\_de\_puerta\_de\_enlace\_de\_red/longitud\_de\_prefijo\_de\_subred* (por ejemplo, **192.167.1.1/24**).

- 6 (opcional) Introduzca una descripción de la red de VDC de organización.
- 7 (opcional) Con el fin de que la red de VDC de organización esté disponible para otros VDC de organización en la misma organización, active la opción **Compartida**.

Un posible caso de uso para esta opción consiste en la existencia de una aplicación en un VDC de organización que tiene un grupo de asignaciones o reservas establecido como el modelo



de asignación. En este caso, es posible que no haya espacio suficiente para ejecutar más máquinas virtuales. Para solucionar este problema, puede crear una instancia secundaria de VDC de organización con pago por uso y ejecutar más máquinas virtuales en esa red de forma temporal.

**Nota** Las instancias de VDC de organización deben estar respaldadas por la misma instancia de VDC de proveedor.

- 8 Haga clic en **Siguiente**.
- 9 (opcional) Si desea reservar una o más direcciones IP para la asignación a máquinas virtuales que requieren direcciones IP estáticas, configure los **Grupos de IP estáticas** para la red.
  - a Introduzca la dirección IP o el rango de direcciones IP y haga clic en **Agregar**.
  - b Para agregar varias direcciones IP estáticas o rangos, repita este paso.
  - c (opcional) Para modificar o eliminar direcciones IP y rangos de direcciones IP, haga clic en **Modificar** o **Eliminar**.
- 10 Haga clic en **Siguiente**.
- 11 (opcional) Establezca la configuración de DNS.

Opción	Acción
DNS primario	Introduzca la dirección IP del servidor DNS primario.
DNS secundario	Introduzca la dirección IP del servidor DNS secundario.
Sufijo DNS	Especifique el sufijo DNS. El sufijo DNS es el nombre de DNS sin incluir el nombre de host.

- 12 Haga clic en **Siguiente**.
- 13 En la página **Listo para completar**, revise la configuración de la red de VDC de organización que ha proporcionado y haga clic en **Finalizar**.

## Agregar una red de centros de datos virtuales de organización enrutada

Para controlar el acceso a una red externa, puede agregar una red de VDC de organización enrutada. Los **administradores del sistema** y los **administradores de la organización** pueden configurar los ajustes de la traducción de direcciones de red (Network Address Translation, NAT), del firewall y de la VPN para que sea posible acceder a máquinas virtuales específicas desde la red externa.

Puede agregar una combinación de redes de VDC de organización enrutadas y aisladas para satisfacer las necesidades de su organización. Por ejemplo, puede agregar una red que está asociada con una puerta de enlace Edge y conectada a Internet mientras se cuenta con una red aislada que contiene información confidencial.

Puede agregar una red de VDC de organización enrutada IPv4 o IPv6.

## Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en **Agregar**.
- 3 En la página **Seleccionar tipo de red**, seleccione **Enrutada** y haga clic en **Siguiente**.
- 4 Introduzca un nombre significativo para la red de VDC de organización.

- 5 Introduzca la configuración de enrutamiento de interdominios sin clases (Classless Inter-Domain Routing, CIDR) para la red de VDC de organización enrutada.

Utilice el formato *dirección\_IP\_de\_puerta\_de\_enlace\_de\_red/longitud\_de\_prefijo\_de\_subred* (por ejemplo, **192.167.1.1/24**).

- 6 (opcional) Introduzca una descripción de la red de VDC de organización.
- 7 (opcional) Con el fin de que la red de VDC de organización esté disponible para otros VDC de organización en la misma organización, active la opción **Compartida**.

Un posible caso de uso consiste en una aplicación en una instancia de VDC de organización que tiene un grupo de asignaciones o reservas establecido como el modelo de asignación. En este caso, es posible que no haya espacio suficiente para ejecutar más máquinas virtuales. Para solucionar este problema, puede crear una instancia secundaria de VDC de organización con pago por uso y ejecutar más máquinas virtuales en esa red de forma temporal.

---

**Nota** Los VDC de organización deben compartir el mismo grupo de redes.

---

- 8 Haga clic en **Siguiente**.
- 9 En la página **Conexión de Edge**, seleccione una puerta de enlace Edge con la cual asociar la red de VDC de organización.

Si el VDC de organización incluye más de una puerta de enlace Edge, debe seleccionar una a la que la red debe conectarse. Para admitir otra red enrutada, la puerta de enlace Edge debe mostrar un valor de al menos 1 en la columna N.º de redes disponibles.

- 10 En el menú desplegable **Tipo de interfaz**, seleccione el tipo de interfaz.

Opción	Descripción
Interna	Se conecta a una de las interfaces internas de la puerta de enlace Edge. La cantidad máxima de redes permitidas es 9.
Distribuida	Crea la red en un enrutador lógico distribuido conectado a esta puerta de enlace Edge. La cantidad máxima de redes permitidas es 400.
Subinterfaz	Amplía una red de VDC de organización. vCloud Director identifica la red que se utilizará para ampliar a través de una VPN de capa 2. vCloud Director, con la ayuda de la virtualización de red de NSX, crea un tipo de interfaz troncal para esta red. La cantidad máxima de redes permitidas es 200.

- 11 (opcional) Para habilitar el etiquetado de VLAN invitadas en esta red, active la opción **Admite VLAN invitada**.
- 12 Haga clic en **Siguiente**.
- 13 (opcional) Si desea reservar una o más direcciones IP para la asignación a máquinas virtuales que requieren direcciones IP estáticas, configure los **Grupos de IP estáticas** para la red.
- a Introduzca la dirección IP o el rango de direcciones IP y haga clic en **Agregar**.
  - b Para agregar varias direcciones IP estáticas o rangos, repita este paso.
  - c (opcional) Para modificar o eliminar direcciones IP y rangos de direcciones IP, haga clic en **Modificar** o **Eliminar**.
- 14 Haga clic en **Siguiente**.
- 15 (opcional) Establezca la configuración de DNS.

Opción	Acción
DNS primario	Introduzca la dirección IP del servidor DNS primario.
DNS secundario	Introduzca la dirección IP del servidor DNS secundario.
Sufijo DNS	Especifique el sufijo DNS. El sufijo DNS es el nombre de DNS sin incluir el nombre de host.

- 16 Haga clic en **Siguiente**.
- 17 En la página **Listo para completar**, revise la configuración de la red de VDC de organización que ha proporcionado y haga clic en **Finalizar**.

## Agregar una red de centros de datos virtuales de organización directa

Para conectarse a una red externa mediante una ruta directa, los **administradores del sistema** pueden establecer una conexión directa.

Si inicia sesión en el portal para tenants de vCloud Director como **administrador de organización** e intenta crear una red de centros de datos virtuales de organización directa, recibirá un mensaje de advertencia en el que se indica que no tiene suficientes derechos.

#### Requisitos previos

Esta operación está limitada a los administradores del sistema.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en **Agregar**.
- 3 En la página **Seleccionar tipo de red**, seleccione **Directa** y haga clic en **Siguiente**.
- 4 Introduzca un nombre significativo para la red de VDC de organización.
- 5 (opcional) Introduzca una descripción de la red de VDC de organización.
- 6 (opcional) Con el fin de que la red de VDC de organización esté disponible para otros VDC de organización en la misma organización, active la opción **Compartida**.
- 7 En la página **Conexión de red externa**, seleccione la red externa a la que desea que se conecte directamente la nueva red de centros de datos virtuales de organización y haga clic en **Siguiente**.
- 8 En la página **Listo para completar**, revise la configuración de la red de VDC de organización que ha proporcionado y haga clic en **Finalizar**.

## Editar la configuración general de una red de centros de datos virtuales de organización

Puede modificar las propiedades de redes de VDC de organización.

#### Requisitos previos

Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red de VDC de organización que desea ver o editar.

- 3 En la pestaña **General**, haga clic en **Editar**.
  - a Edite el nombre y la descripción de la red.
  - b Active o desactive la opción de alternancia **Compartida** para compartir o no compartir la red de VDC de organización con otros centros de datos virtuales dentro de la misma organización.
- 4 Haga clic en **Guardar**.

## Convertir una red de centros de datos virtuales de organización

Después de crear una red de VDC de organización, puede convertir la red de aislada a enrutada y viceversa.

### Requisitos previos

Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red de VDC de organización que desea convertir.
- 3 En la pestaña **General**, haga clic en **Editar**.
- 4 Haga clic en **Conexión**.
- 5 Para conectarse a una puerta de enlace Edge o para aislar la red del resto de las redes, alterne la opción **Conectarse a una puerta de enlace Edge** o desactive la misma opción.

Opción	Acción
Convierta una red aislada en una red enrutada.	<ol style="list-style-type: none"> <li>1 Alterne la opción <b>Conectarse a una puerta de enlace Edge</b>.</li> <li>2 Seleccione la puerta de enlace Edge a la que se conectará en la lista de puertas de enlace Edge disponibles.</li> <li>3 Seleccione el tipo de interfaz.</li> <li>4 Para permitir una VLAN invitada, active la opción <b>Admite VLAN invitada</b>.</li> </ol>
Convierta una red enrutada en una red aislada.	Desactive la opción <b>Conectarse a una puerta de enlace Edge</b> .

- 6 Haga clic en **Guardar**.

### Resultados

Ha convertido la red de VDC de organización.

## Convertir la interfaz de una red de VDC de organización enrutada

Es posible cambiar la interfaz de una red de interna a subinterfaz o enrutamiento distribuido, por ejemplo, mediante la edición de las propiedades de red.

**Nota** No se pueden convertir instancias de Cross VDC Networking.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red que desea convertir.
- 3 Haga clic en el nombre de la red de VDC de organización que desea editar.
- 4 En la pestaña **General**, haga clic en **Editar**.
- 5 Haga clic en **Conexión**.
- 6 En el menú desplegable **Tipo de interfaz**, seleccione el tipo de interfaz.

Opción	Descripción
<b>Interna</b>	Se conecta a una de las interfaces internas de la puerta de enlace Edge. La cantidad máxima de redes permitidas es 9.
<b>Distribuida</b>	Crea la red en un enrutador lógico distribuido conectado a esta puerta de enlace Edge. La cantidad máxima de redes permitidas es 400.
<b>Subinterfaz</b>	Amplía una red de VDC de organización. vCloud Director identifica la red que se utilizará para ampliar a través de VPN de capa 2. vCloud Director, con la ayuda de la virtualización de red de NSX, crea un tipo de interfaz troncal para esta red. La cantidad máxima de redes permitidas es 200.

- 7 Haga clic en **Guardar**.

## Ver las direcciones IP usadas para una red de centros de datos virtuales de organización

Puede ver una lista de las direcciones IP de un grupo de direcciones IP de la red de centros de datos virtuales de organización que se estén utilizando en estos momentos.

### Requisitos previos

- Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red cuyas direcciones IP utilizadas desea ver.
- 3 Haga clic en la pestaña **Administración de direcciones IP**.
- 4 Haga clic en **Asignaciones de IP** para ver las direcciones IP que están en uso actualmente.

## Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización

Cuando una red de centros virtuales de organización se está quedando sin direcciones IP, se pueden agregar más al grupo de direcciones IP.

No se puede agregar direcciones IP a redes de centros de datos virtuales de organización externas que tengan conexión directa.

### Requisitos previos

- Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 Haga clic en la pestaña **Administración de direcciones IP**.

La opción **Grupos de IP estáticas** está seleccionada de forma predeterminada.

- 4 Haga clic en el botón **Editar** situado a la derecha.

En la ventana **Editar red**, puede ver el CIDR de la puerta de enlace y los rangos de direcciones IP, si los hubiera.

- 5 En el cuadro de texto **Grupos de IP estáticas**, introduzca la dirección IP o el rango de direcciones IP, y haga clic en **Agregar**.

---

**Nota** Para las instancias de Cross VDC Networking, las direcciones IP no deben superponerse con las direcciones IP que se asignan a las otras redes de VDC de organización de la misma red extendida.

---

- 6 Haga clic en **Guardar**.

#### Resultados

La dirección IP o el rango de direcciones IP se agregan al grupo de direcciones IP de red.

## Editar o eliminar rangos de IP utilizados en una red de centros de datos virtuales de organización

Si una red de centros de datos virtuales de organización contiene direcciones IP que ya no necesita, puede editarlas o eliminarlas del grupo de direcciones IP.

#### Requisitos previos

- Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 Haga clic en la pestaña **Administración de direcciones IP**.

La opción **Grupos de IP estáticas** está seleccionada de forma predeterminada.

- 4 Haga clic en el botón **Editar** en la derecha.
  - Para modificar un rango de IP, seleccione el rango, haga los cambios necesarios y haga clic en **Modificar**.
  - Para eliminar un rango de IP, seleccione el rango y haga clic en **Eliminar**.

- 5 Haga clic en **Guardar**.

## Editar la configuración de DNS de una red de centros de datos virtuales de organización

Puede editar la configuración de DNS de una red de centros de datos virtuales de organización.



### Requisitos previos

- Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada o enrutada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 Haga clic en la pestaña **Administración de direcciones IP**.
- 4 Seleccione **DNS** y haga clic en el botón **Editar** ubicado a la derecha.
- 5 Edite el DNS principal, el DNS secundario y la información del sufijo DNS según corresponda.
- 6 Haga clic en **Guardar**.

## Configurar las opciones de DHCP para una red de centros de datos virtuales de organización aislada

Puede editar la configuración de DHCP de una red de VDC de organización aislada. El servicio DHCP de una red de VDC de organización proporciona direcciones IP de su grupo de direcciones a las NIC de la máquina virtual que se configuran para solicitar una dirección de DHCP. El servicio proporciona la dirección cuando se enciende la máquina virtual.

### Requisitos previos

- Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 Haga clic en la pestaña **Administración de direcciones IP**.
- 4 Seleccione **DHCP**.  
La configuración de DHCP se muestra a la derecha.
- 5 Para habilitar DHCP, haga clic en **Editar** a la derecha de **Servicio de grupos DHCP**.

- 6 Alterne la opción **Servicio de grupos DHCP** y haga clic en **Guardar**.

Las direcciones solicitadas por los clientes DHCP se extraen de un grupo DHCP.

- 7 Cree un grupo DHCP para la red.

- a Haga clic en **Agregar**.

- b Introduzca un rango de direcciones IP para el grupo.

El rango de direcciones IP que especifique no puede superponerse con el grupo de direcciones IP estáticas para el centro de datos virtual de organización.

- c Especifique el tiempo de concesión predeterminado para las direcciones DHCP en segundos.

El valor predeterminado es de 3.600 segundos.

- d Especifique el tiempo de concesión máximo para las direcciones DHCP en segundos.

Esta es la cantidad máxima de tiempo que las direcciones IP asignadas por DHCP se concesionan a las máquinas virtuales. El valor predeterminado es de 7.200 segundos.

- 8 Haga clic en **Guardar**.

## Editar o eliminar un grupo DHCP existente para una red

Si ya no necesita un grupo DHCP dentro de la red de centros de datos virtuales de organización aislada, puede eliminar el grupo o editarlo.

### Requisitos previos

- Estas operaciones requieren las funciones predefinidas **administrador de la organización** o **administrador del sistema**, o una función que incluya un conjunto equivalente de derechos.
- Compruebe que la red sea una red de centros de datos virtuales de organización aislada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Haga clic en el nombre de la red que desea editar.
- 3 Haga clic en la pestaña **Administración de direcciones IP**.
- 4 Seleccione **DHCP**.

La configuración de DHCP se muestra a la derecha.

## 5 Edite o elimine un grupo DHCP existente.

Opción	Acción
Edite un grupo DHCP.	<ol style="list-style-type: none"> <li>1 Seleccione el grupo DHCP que desea editar.</li> <li>2 Haga clic en el botón <b>Editar</b>.</li> <li>3 Actualice el rango de direcciones IP para el grupo.</li> <li>4 Edite el tiempo de concesión predeterminado para las direcciones DHCP en segundos.</li> <li>5 Edite el tiempo de concesión máximo para las direcciones DHCP en segundos.</li> <li>6 Haga clic en <b>Guardar</b>.</li> </ol>
Elimine un grupo DHCP.	<ol style="list-style-type: none"> <li>1 Seleccione el grupo DHCP que desea eliminar.</li> <li>2 Haga clic en el botón <b>Eliminar</b>.</li> </ol>

## Restablecer una red de centros de datos virtuales de organización

Si los servicios de red, como la configuración de DHCP o de firewall que están asociados a una red de centros de datos virtuales de organización no funcionan según lo esperado, puede restablecer la red.

Al restablecer la red de centros de datos virtuales de organización, fuerce la reimplementación de la puerta de enlace del servicio DHCP de red. Esta operación provocará una interrupción temporal de los servicios DHCP, y no habrá servicios de red disponibles mientras se restablece la red.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- La red no está conectada a ninguna máquina virtual, vApp u otra red.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Seleccione una red de VDC de organización.
- 3 Haga clic en **Restablecer** y confirme la operación de restablecimiento.

## Eliminar una red de centros de datos virtuales de organización

Si ya no necesita una red de centros de datos virtuales de organización, puede eliminarla.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

- La red no está conectada a máquinas virtuales, vApps u otras redes.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Redes** en el panel izquierdo.
- 2 Seleccione una red de VDC de organización.
- 3 Haga clic en **Eliminar** y confirme la operación de eliminación.

# Administrar redes entre los centros de datos virtuales

## 5

Para crear una red entre varios centros de datos virtuales de organización, primero deberá agrupar los centros de datos virtuales y, a continuación, crear una red extendida en el grupo de centros de datos. Un grupo de centros de datos puede tener una configuración de punto de salida común o una configuración de punto de salida para cada dominio de errores de red.

### Grupo de centros de datos

Un grupo de hasta cuatro centros de datos virtuales que están configurados para compartir varios puntos de salida. Un grupo de centros de datos puede tener una de las siguientes configuraciones de puntos de salida:

Tipo de configuración de puntos de salida	Descripción
Configuración común de puntos de salida	El grupo de centros de datos puede configurarse con un punto de salida activo y un punto de salida en espera. Los dos puntos de salida son comunes a todos los centros de datos virtuales participantes entre todos los dominios de errores de red del grupo de centros de datos.
Configuración de puntos de salida por dominio de error	El grupo de centros de datos puede configurarse con un punto de salida activo para cada dominio de errores de red del grupo de centros de datos. No se pueden crear salidas en espera.

Una organización puede tener varios grupos de centros de datos. Un centro de datos virtual de organización puede participar en varios grupos de centros de datos.

Los centros de datos virtuales de organización participantes pueden pertenecer a distintos sitios de vCloud Director. Consulte [Configurar y administrar implementaciones multisitio](#).

### Dominio de error de red

El alcance del proveedor de red, que por lo general representa la instancia de vCenter Server subyacente con el NSX Manager asociado.

### Punto de salida

Una puerta de enlace Edge que conecta a Internet un dominio de errores de red o un grupo de centros de datos. La puerta de enlace Edge debe pertenecer a un centro de datos virtual del grupo de centros de datos. Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del grupo de centros de datos virtuales o del dominio de errores de red. Las rutas que existen en la puerta de enlace Edge no se ven afectadas.

## Red extendida

Una red de capa 2 que se extiende a través de todos los centros de datos virtuales de un grupo de centros de datos. Solo puede ser IPv4.

Este capítulo incluye los siguientes temas:

- [Administrar grupos de centros de datos](#)
- [Administrar redes extendidas](#)

## Administrar grupos de centros de datos

Después de crear un grupo de centros de datos, puede editar la topología de la red de un grupo de centros de datos. Puede agregar y eliminar los centros de datos virtuales del grupo. Puede intercambiar, reemplazar y eliminar los puntos de salida. Puede realizar distintas tareas de sincronización para corregir errores de configuración.

No puede convertir una configuración de salida común en una configuración de salida por dominio de errores, ni viceversa.

## Crear y configurar un grupo de centros de datos con una configuración de salida común

Se puede crear y configurar un grupo de centros de datos virtuales con una configuración de salida común, en la que se establece un par de puertas de enlace Edge que actúan como puntos de salida activos y en espera para todos los centros de datos virtuales participantes.

### Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- Ha habilitado los centros de datos virtuales de destino para Cross VDC Networking. Para obtener información sobre la configuración de Cross VDC Networking, consulte la *Guía del administrador de vCloud Director*.

### Procedimiento

#### 1 [Crear un grupo de centros de datos con una configuración de salida común](#)

Puede agrupar entre dos y cuatro centros de datos virtuales en un grupo de centros de datos con una configuración de salida común.

## 2 Agregar un punto de salida activo

Para conectar el grupo de centros de datos a Internet, debe agregar un punto de salida activo a su topología de red.


## 3 Agregar un punto de salida en espera

En los grupos de centros de datos virtuales con configuraciones de salida comunes, puede agregar un punto de salida secundario, el cual actúa como un punto de salida en espera para escenarios de tolerancia a errores.

## Crear un grupo de centros de datos con una configuración de salida común

Puede agrupar entre dos y cuatro centros de datos virtuales en un grupo de centros de datos con una configuración de salida común.

### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 Haga clic en **Nuevo grupo de centros de datos**.
- 3 Introduzca un nombre y, si lo desea, una descripción para el nuevo grupo de centros de datos.
- 4 Seleccione **Puntos de salida comunes** y haga clic en **Siguiente**.
- 5 En la página de **Centros de datos**, seleccione al menos dos y hasta cuatro centros de datos para el nuevo grupo de centros de datos y, luego, haga clic en **Siguiente**.  
La página **Centros de datos** contiene una lista de los centros de datos virtuales que están habilitados para redes entre centros de datos virtuales a través del **administrador del sistema**.
- 6 Revise los detalles del grupo de centros de datos y haga clic en **Finalizar**.

### Resultados

El grupo de centros de datos virtuales recién creado aparece en la vista **Grupos de centros de datos**.

## Agregar un punto de salida activo

Para conectar el grupo de centros de datos a Internet, debe agregar un punto de salida activo a su topología de red.

### Requisitos previos

El **administrador del sistema** ha creado al menos una puerta de enlace Edge en cualquiera de los centros de datos virtuales que participan en el grupo de centros de datos.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Haga clic en **Agregar punto de salida**.

La página **Agregar punto de salida activo** que se abre proporciona una lista de las puertas de enlace Edge que pertenecen a los centros de datos virtuales participantes.

- 4 Seleccione la puerta de enlace Edge que desea que actúe como un punto de salida activo para este grupo de centros de datos y haga clic en **Agregar**.

## Resultados

Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del grupo de centros de datos virtuales. Las rutas que existen en la puerta de enlace Edge no se ven afectadas.

El diagrama de la topología de red se actualiza con el punto de salida recién agregado. El tráfico proveniente de los centros de datos virtuales participantes que fluye hacia Internet se representa con una línea sólida de color azul.

## Agregar un punto de salida en espera

En los grupos de centros de datos virtuales con configuraciones de salida comunes, puede agregar un punto de salida secundario, el cual actúa como un punto de salida en espera para escenarios de tolerancia a errores.

## Requisitos previos

Además de la puerta de enlace Edge que actúa como un punto de salida activo, debe tener al menos una puerta de enlace Edge adicional en cualquiera de los centros de datos virtuales que participan en el grupo.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.



- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Haga clic en **Agregar punto de salida en espera**.

Se abrirá la página **Agregar punto de salida en espera**, la cual proporciona una lista de las puertas de enlace Edge sin utilizar que pertenecen a los centros de datos virtuales participantes. No se muestra la puerta de enlace Edge que el punto de salida activo emplea en este grupo de centros de datos virtuales.

- 4 Seleccione la puerta de enlace Edge que desea que actúe como un punto de salida en espera para este grupo de centros de datos y haga clic en **Agregar**.

### Resultados

Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del grupo de centros de datos virtuales. Las rutas que existen en la puerta de enlace Edge no se ven afectadas.

El diagrama de la topología de red se actualiza con el punto de salida recién agregado. El tráfico proveniente de los centros de datos virtuales participantes que fluye hacia Internet en escenarios de tolerancia a errores se representa con una línea discontinua de color azul.

## Crear y configurar un grupo de centros de datos con una configuración de salida de dominio de error

Puede crear y configurar un grupo de centros de datos virtuales con una configuración de salida de dominio de error, en la que se configura una puerta de enlace Edge que actúa como un punto de salida activo para cada dominio de error de red del grupo. No se pueden crear salidas en espera en un grupo de centros de datos con una configuración de salida de dominio de error.

### Requisitos previos

Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.

### Procedimiento

- 1 [Crear un grupo de centros de datos con una configuración de salida de dominio de error](#)

Puede agrupar entre dos y cuatro centros de datos virtuales en un grupo de centros de datos con una configuración de salida de dominio de error.

## 2 Agregar un punto de salida para un dominio de error

Para conectar con Internet los centros de datos virtuales de un dominio de error de red en un grupo de centros de datos, debe agregar un punto de salida a este dominio de error de red. Puede agregar un punto de salida a cada dominio de error de red en el grupo de centros de datos. Los puntos de salida en espera no se admiten en un grupo de centros de datos con una configuración de salida de dominio de error.


### Crear un grupo de centros de datos con una configuración de salida de dominio de error

Puede agrupar entre dos y cuatro centros de datos virtuales en un grupo de centros de datos con una configuración de salida de dominio de error.

#### Requisitos previos

El **administrador del sistema** ha habilitado los centros de datos virtuales de destino para Cross VDC Networking.

#### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 Haga clic en **Nuevo grupo de centros de datos**.
- 3 Introduzca un nombre y, si lo desea, una descripción para el nuevo grupo de centros de datos.
- 4 Seleccione **Puntos de salida por dominio de error** y haga clic en **Siguiente**.
- 5 En la página de **Centros de datos**, seleccione al menos dos y hasta cuatro centros de datos para el nuevo grupo de centros de datos y, luego, haga clic en **Siguiente**.  
La página **Centros de datos** contiene una lista de los centros de datos virtuales que están habilitados para redes entre centros de datos virtuales a través del **administrador del sistema**.
- 6 Revise los detalles del grupo de centros de datos y haga clic en **Finalizar**.

#### Resultados

El grupo de centros de datos virtuales recién creado aparece en la vista **Grupos de centros de datos**.

### Agregar un punto de salida para un dominio de error

Para conectar con Internet los centros de datos virtuales de un dominio de error de red en un grupo de centros de datos, debe agregar un punto de salida a este dominio de error de red. Puede agregar un punto de salida a cada dominio de error de red en el grupo de centros de datos. Los puntos de salida en espera no se admiten en un grupo de centros de datos con una configuración de salida de dominio de error.

## Requisitos previos

Además de las puertas de enlace Edge que se emplean como puntos de salida en este grupo de centros de datos, debe tener al menos una puerta de enlace Edge sin utilizar en cualquiera de los centros de datos virtuales participantes.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 En el diagrama de la topología de red, haga clic en el dominio de error de red de destino.

Los dominios de error de red se representan con líneas sólidas y sus nombres aparecen en la parte inferior del diagrama.

Los dominios de error seleccionados se marcan con color azul.

- 4 Haga clic en **Agregar punto de salida**.

Se abre la página **Agregar punto de salida activo**, la cual proporciona una lista de las puertas de enlace Edge que pertenecen a los centros de datos virtuales participantes.

- 5 Seleccione la puerta de enlace Edge que desea que actúe como punto de salida para este dominio de error y haga clic en **Agregar**.

## Resultados

Las rutas de BGP se configuran en la puerta de enlace Edge que representa el punto de salida y el enrutador universal del dominio de error de red. Las rutas que existen en la puerta de enlace Edge no se ven afectadas.

El diagrama de la topología de red se actualiza con el punto de salida recién agregado. El tráfico proveniente de los centros de datos virtuales en el dominio de error de red que fluye hacia Internet se representa con una línea sólida de color azul.

## Ver un grupo de centros de datos

Puede ver los grupos de centros de datos de la organización y los detalles sobre su configuración actual.

## Requisitos previos

Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Ver grupo de VDC** publicado en la organización.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

## Agregar un centro de datos virtual a un grupo de centros de datos

Puede agregar un centro de datos virtual a un grupo de centros de datos y, como resultado, extender las redes existentes al nuevo centro de datos virtual.

### Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- El grupo de centros de datos contiene menos de cuatro centros de datos virtuales.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Haga clic en **Agregar centro de datos**.

- 4 En la página **Centros de datos**, seleccione el centro de datos que desea agregar al grupo de centros de datos y haga clic en **Finalizar**.

La página **Centros de datos** contiene una lista de centros de datos virtuales que el administrador del sistema habilita para Cross VDC Networking.

---

**Nota** Un grupo de centros de datos debe contener hasta cuatro centros de datos virtuales.

---


## Eliminar un centro de datos virtual de un grupo de centros de datos

Puede eliminar un centro de datos virtual de un grupo de centros de datos. Como resultado, se reducirá la extensión de las redes existentes desde este centro de datos virtual.

### Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- El grupo de centros de datos debe contener al menos tres centros de datos virtuales.
- El centro de datos virtual que desea eliminar no debe proporcionar un punto de salida para el grupo de centros de datos.

### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.  
Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 En la esquina superior derecha de la tarjeta del centro de datos virtual de destino, haga clic en los tres puntos y haga clic en **Quitar**.
- 4 Para confirmar, haga clic en **Quitar**.

### Resultados

El centro de datos virtual se quita del diagrama de topología de red del grupo de centros de datos.

## Sincronizar un grupo de centros de datos

Para volver a aplicar las configuraciones de red del grupo de centros de datos y asegurarse de que todos los centros de datos virtuales participantes están activos, puede sincronizar ese grupo de centros de datos.

---


**Nota** Durante el proceso de sincronización de los grupos de centros de datos, el grupo de centros de datos deja de estar disponible durante unos segundos debido a que el enrutador universal se sincroniza en NSX.

---

### Requisitos previos

Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.

### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Haga clic en **Sincronizar grupo de centros de datos**.

- 4 Para confirmar, haga clic en **Aceptar**.

## Intercambiar puntos de salida en un grupo de centros de datos con una configuración de salida común

Después de configurar un punto de salida activo y otro en espera en un grupo de centros de datos con una configuración de salida común, puede intercambiar las funciones de esos puntos de salida. El punto de salida activo puede convertirse en punto de salida en espera y a la inversa.

### Requisitos previos

Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.

### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Haga clic en **Intercambiar puntos de salida**.

- 4 Para confirmar, haga clic en **Aceptar**.

### Resultados

El diagrama de la topología de red se actualiza con las nuevas rutas del tráfico. El tráfico de Internet ahora se redirige al nuevo punto de salida activo.


## Reemplazar la puerta de enlace Edge de un punto de salida

En un grupo de centros de datos, puede reemplazar la puerta de enlace Edge que representa un punto de salida activo o en espera.

## Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- La nueva puerta de enlace Edge no puede estar en uso por otros puntos de salida del grupo de centros de datos.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.  
Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 Si va a reemplazar un punto de salida de una configuración de dominio de errores de red, seleccione en el diagrama de topología de red el dominio de errores de red del punto de salida de destino.  
Los dominios de errores de red se representan con líneas sólidas y nombres de dominio en la parte inferior del diagrama.  
El dominio de errores de red seleccionado está marcado en azul.
- 4 En la esquina superior derecha de la tarjeta del punto de salida de destino, haga clic en los tres puntos y después haga clic en **Reemplazar**.  
Se abrirá la página **Reemplazar punto de salida**, que muestra la lista de las puertas de enlace Edge que pertenecen a los centros de datos virtuales participantes.
- 5 Seleccione la nueva puerta de enlace Edge y haga clic en **Reemplazar**.

## Resultados

Las rutas BGP se eliminan de la puerta de enlace Edge anterior y se configuran en la nueva puerta de enlace Edge que representa el punto de salida y el enrutador universal del grupo de centros de datos virtual.

El diagrama de topología de red se actualiza con el nombre de la nueva puerta de enlace Edge.

## Eliminar un punto de salida

Para desconectar un dominio de errores de red o un grupo de centros de datos desde Internet, puede eliminar su punto de salida.

### Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.
- Si desea eliminar un punto de salida activo que está emparejado con un punto de salida en espera, debe intercambiar los puntos de salida o eliminar el punto de salida en espera.

### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Si va a quitar un punto de salida de una configuración de dominio de errores de red, en el diagrama de la topología de la red, seleccione el dominio de errores de red del punto de salida de destino.

Los dominios de errores de red se representan con líneas sólidas y nombres de dominio en la parte inferior del diagrama.

El dominio de errores de red seleccionado está marcado en azul.

- 4 En la esquina superior derecha de la tarjeta del punto de salida de destino, haga clic en los tres puntos y después haga clic en **Eliminar**.

- 5 Para confirmar, haga clic en **Aceptar**.

### Resultados

Las rutas BGP se eliminan de la puerta de enlace Edge que representa el punto de salida si no está en uso por otros enrutadores universales.

El punto de salida se quita del diagrama de topología de red.

## Sincronizar rutas y puntos de salida

Para volver a aplicar la configuración de enrutamiento dinámico a un grupo de centros de datos o a un dominio de errores de red y sus puntos de salida asociados, puede sincronizar las rutas. Para asegurarse de que un punto de salida está conectado correctamente al grupo de centros de datos, puede sincronizar ese punto de salida.

### Requisitos previos

- Esta operación requiere la función **Administrador del sistema** o una función con el derecho **Grupo de VDC: Configurar grupo de VDC** publicado en la organización.



- Ha configurado un punto de salida para el dominio de errores de red o para el grupo de centros de datos de destino.

#### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.

La lista de grupos de centros de datos se muestra en una vista de tarjeta.

- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.

Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.

- 3 Si está realizando la sincronización de un dominio de errores de red contenido en un grupo de centros de datos, seleccione en el diagrama de topología de la red el dominio de errores de red de destino.

Los dominios de errores de red se representan con líneas sólidas y nombres de dominio en la parte inferior del diagrama.

El dominio de errores de red seleccionado está marcado en azul.

- 4 Para volver a aplicar la configuración de enrutamiento dinámico al grupo o al dominio de errores de red y sus puntos de salida asociados, haga clic en **Sincronizar rutas** y haga clic en **Aceptar**.
- 5 Para sincronizar un punto de salida con su grupo de centros de datos, en la esquina superior derecha de la tarjeta del punto de salida de destino, haga clic en los tres puntos, haga clic en **Sincronizar** y haga clic en **Aceptar**.

## Administrar redes extendidas

Después de crear y configurar un grupo de centros de datos, puede crear y administrar redes de capa 2 extendidas que comprenden los centros de datos virtuales participantes.

A nivel del centro de datos virtual, las redes extendidas aparecen como redes del centro de datos virtual de organización con tipo de enrutamiento entre VDC.

### Agregar una red extendida


Puede crear una red extendida entre todos los centros de datos virtuales que participan en un grupo de centros de datos.

Puede agregar solo una red extendida IPv4.

#### Requisitos previos

Esta operación requiere la función predefinida **Administrador de organización** o una función con el derecho **Red de VDC de organización: Editar propiedades**.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.  
Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 En el panel izquierdo, haga clic en **Redes extendidas**.  
La lista de redes extendidas se muestra en una vista de cuadrícula.
- 4 Haga clic en **Agregar**.
- 5 Introduzca un nombre y, si lo desea, una descripción para la nueva red extendida.
- 6 Introduzca la configuración de enrutamiento entre dominios sin clases (Classless Inter-Domain Routing, CIDR) para la red y haga clic en **Crear**.  
Utilice el formato *dirección\_IP\_de\_puerta\_de\_enlace\_de\_red/longitud\_de\_prefijo\_de\_subred* (por ejemplo, **192.167.1.1/24**).

## Resultados

Puede ver la red recién creada en la lista de redes extendidas del grupo de centros de datos.

Se crea una red de centros de datos virtuales de organización del tipo de enrutamiento Cross VDC para cada centro de datos virtual participante. Puede ver las redes recién creadas en la vista **Centros de datos** de los centros de datos virtuales participantes haciendo clic en **Redes**. Si una máquina virtual o una vApp se conectan a tal red de centros de datos virtuales de organización, la máquina virtual o la vApp se conectan a la red extendida.

## Pasos siguientes

Para cada red de centros de datos virtuales de organización Cross VDC correspondiente, puede asignar grupos de direcciones IP y direcciones IP estáticas. Consulte [Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización](#).

Para las configuraciones DNS y DHCP de las máquinas virtuales conectadas a una red extendida, puede usar vCloud OpenAPI. Para consultar la documentación de vCloud OpenAPI, desplácese hasta [https://nombre\\_de\\_host\\_o\\_dirección\\_IP\\_de\\_vCloud\\_Director/docs](https://nombre_de_host_o_dirección_IP_de_vCloud_Director/docs). Para ver muestras de código y probar llamadas de vCloud OpenAPI, desplácese hasta [https://nombre\\_de\\_host\\_o\\_dirección\\_IP\\_de\\_vCloud\\_Director/api-explorer?scope=nombre\\_de\\_organización](https://nombre_de_host_o_dirección_IP_de_vCloud_Director/api-explorer?scope=nombre_de_organización).

## Ver o editar una red extendida


Puede ver el nombre, la descripción y la configuración de CIDR de una red extendida. Solo puede editar el nombre y la descripción de una red extendida.

Para obtener información sobre cómo editar la asignación del grupo de direcciones IP estáticas para una red extendida a nivel del centro de datos virtual, consulte [Agregar direcciones IP a un grupo de direcciones IP de red de centros virtuales de organización](#).

### Requisitos previos

- La visualización de redes extendidas requiere la función predefinida **Administrador de organización** o una función con el derecho **Red de VDC de organización: Ver propiedades**.
- La edición de redes extendidas requiere la función predefinida **Administrador de organización** o una función con el derecho **Red de VDC de organización: Editar propiedades**.

### Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.  
Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 En el panel izquierdo, haga clic en **Redes extendidas**.  
La lista de redes extendidas se muestra en una vista de cuadrícula.
- 4 Haga clic en el botón de radio junto al nombre de la red de destino y haga clic en **Editar**.
- 5 Edite los detalles de la red y haga clic en **Guardar**.


## Eliminar una red extendida

Puede quitar una red extendida que ya no utilice.

### Requisitos previos

- Esta operación requiere la función predefinida **Administrador de organización** o una función con el derecho **Red de VDC de organización: Editar propiedades**.
- Las redes de centros de datos virtuales de organización correspondientes no se deben conectar con las máquinas virtuales o las vApps.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.  
Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 En el panel izquierdo, haga clic en **Redes extendidas**.  
La lista de redes extendidas se muestra en una vista de cuadrícula.
- 4 Haga clic en el botón de radio junto al nombre de la red de destino y haga clic en **Eliminar**.
- 5 Para confirmar, haga clic en **Eliminar**.

## Resultados

Las redes de centros de datos virtuales de organización correspondientes se quitan de todos los centros de datos virtuales participantes.


## Sincronizar una red extendida

Para asegurarse de que todos los centros de datos virtuales participantes pueden acceder a su red extendida, puede sincronizar la red extendida.

## Requisitos previos

Esta operación requiere la función predefinida **Administrador de organización** o una función con el derecho **Red de VDC de organización: Editar propiedades**.

## Procedimiento

- 1 En el menú principal () , seleccione **Grupos de centros de datos**.  
La lista de grupos de centros de datos se muestra en una vista de tarjeta.
- 2 En la tarjeta del grupo de centros de datos de destino, haga clic en **Detalles**.  
Se lo redirigirá a la vista **Topología de red** de este grupo de centros de datos. Puede ver un diagrama de la topología de la red actual, que muestra los centros de datos virtuales participantes con sus dominios de errores de red, los puntos de salida si están configurados y las rutas de tráfico.
- 3 En el panel izquierdo, haga clic en **Redes extendidas**.  
La lista de redes extendidas se muestra en una vista de cuadrícula.
- 4 Haga clic en el botón de radio junto al nombre de la red de destino y haga clic en **Sincronizar**.

**5** Para confirmar, haga clic en **Aceptar**.

# Capacidades de red avanzadas para tenants de vCloud Director

## 6

vCloud Director proporciona capacidades de red avanzadas con tecnología del software de virtualización de red NSX que ofrece controles y enrutamiento de seguridad mejorados, así como capacidades de escalado de red en un entorno en la nube.

Con estas capacidades de red, puede alcanzar un nivel de seguridad y aislamiento sin precedentes en el centro de datos virtual de organización. Estas capacidades ofrecen las siguientes ventajas:

- Enrutamiento dinámico. Las capacidades de NSX en el entorno de vCloud Director admiten protocolos de enrutamiento, como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF) para simplificar la integración de red entre sistemas, con el fin de proporcionar redundancia y continuidad en la implementación de aplicaciones alojadas en la nube.
- Seguridad y aislamiento de red específicos. Las capacidades de NSX en el entorno de vCloud Director admiten el uso de las definiciones de regla basadas en objetos para proporcionar un aislamiento del tráfico de red con estado sin necesidad de contar con varias redes virtuales. Este modelo de seguridad sin confianza impide que los intrusos obtengan acceso a la red completa si una aplicación o una máquina virtual están en riesgo. Se simplifica la configuración de red utilizando las mismas políticas de seguridad de red para proteger las aplicaciones sin importar si están ubicadas físicamente en el entorno de vCloud Director, y para ampliar el modelo de seguridad sin confianza a la seguridad portátil independientemente de dónde se implemente una aplicación.
- Otras capacidades que ofrece NSX incluyen la compatibilidad mejorada con VPN para la conectividad de punto a sitio (VPN de IPsec) y de usuario (VPN-Plus de SSL), equilibrio de carga mejorado para HTTPS y mayor escalabilidad de red.

Puede configurar dos tipos de firewall: el firewall de puerta de enlace Edge y el distribuido. Para obtener más información sobre las diferencias entre estos firewall, consulte [Configuración de firewall mediante el portal para tenants](#).

Puede acceder a estas capacidades de red avanzadas mediante el portal para tenants de vCloud Director o vCloud Director Service Provider Admin Portal. La puerta de enlace Edge primero debe convertirse en una puerta de enlace Edge avanzada mediante la consola web de vCloud Director. Para conocer los pasos de conversión de una puerta de enlace Edge en una puerta de enlace Edge avanzada, consulte *Guía del administrador de vCloud Director*.

---

**Importante** Las puertas de enlace Edge IPv6 admiten servicios limitados. Las puertas de enlace Edge IPv6 admiten firewalls de Edge, firewalls distribuidos y enrutamiento estático.

---

Este capítulo incluye los siguientes temas:

- [Introducción a las redes avanzadas de vCloud Director](#)
- [Configuración de firewall mediante el portal para tenants](#)
- [Administrar DHCP de puerta de enlace Edge](#)
- [Administrar la traducción de direcciones de red mediante el portal para tenants](#)
- [Configuración avanzada de enrutamiento](#)
- [Equilibrio de carga](#)
- [Acceso seguro mediante redes privadas virtuales](#)
- [Administración de certificados SSL](#)
- [Objetos de agrupamiento personalizados](#)
- [Estadísticas y logs para una puerta de enlace Edge](#)
- [Habilitar el acceso de la línea de comandos SSH a una puerta de enlace Edge](#)
- [Trabajar con etiquetas de seguridad](#)
- [Trabajar con grupos de seguridad](#)

## Introducción a las redes avanzadas de vCloud Director

Se utilizan las redes avanzadas de vCloud Director para realizar tareas de administración en una organización de un sistema de vCloud Director. Puede administrar los firewalls distribuidos y otras capacidades de redes avanzadas proporcionadas por los componentes de software de VMware NSX<sup>®</sup> que un administrador del sistema de vCloud Director pone a disposición de una organización.

Para obtener una introducción al producto vCloud Director en general y al modo en que se configuran una organización y sus recursos en un sistema de vCloud Director, consulte la *Guía del usuario de vCloud Director*.

Los usuarios típicos de redes avanzadas son:

- **Administradores del sistema** de vCloud Director que pueden usar el portal para tenants para configurar el firewall distribuido y otras capacidades de redes avanzadas de una organización.

- **Administradores de organización** que usan el portal para tenants para administrar el firewall distribuido y otras capacidades de redes avanzadas que el **administrador del sistema** ha puesto a disposición de esa organización.

## Configuración de firewall mediante el portal para tenants

En el portal para tenants, puede configurar las capacidades de firewall que ofrece el software NSX en el centro de datos virtual de organización de vCloud Director. Puede crear reglas de firewall para firewalls distribuidos a fin de proporcionar seguridad entre las máquinas virtuales de un centro de datos virtual de organización y reglas de firewall que se apliquen a un firewall de puerta de enlace Edge a fin de proteger las máquinas virtuales de un centro de datos virtual de organización contra el tráfico de red externo.

---

**Nota** El portal para tenants proporciona la capacidad para configurar firewalls de puerta de enlace Edge y firewalls distribuidos.

---

La tecnología de firewall lógico de NSX consta de dos componentes para abordar escenarios de uso de implementación diferentes. El firewall de puerta de enlace Edge se centra en la aplicación de tráfico de norte a sur mientras que el firewall distribuido se centra en los controles de acceso de este a oeste.

## Diferencias clave entre los firewalls de puerta de enlace Edge y los firewalls distribuidos

Un firewall de puerta de enlace Edge supervisa el tráfico de norte a sur para proporcionar la funcionalidad de seguridad del perímetro, incluidos el firewall y la traducción de direcciones de red (Network Address Translation, NAT), así como la funcionalidad VPN de SSL y de IPsec de sitio a sitio.

Un firewall distribuido proporciona la capacidad para aislar y proteger cada máquina virtual y aplicación hacia abajo hasta el nivel de capa 2 (L2). La configuración de firewalls distribuidos coloca en cuarentena con eficacia todo riesgo de seguridad de red externo o interno, ya que aísla el tráfico de este a oeste entre las máquinas virtuales en el mismo segmento de red. Las políticas de seguridad se pueden administrar centralmente, así como heredar y anidar, para que los administradores de redes y seguridad pueden administrarlas a gran escala. Además, una vez implementadas, las políticas de seguridad definidas siguen a las máquinas virtuales o las aplicaciones cuando se mueven de un centro de datos virtual a otro.

## Acerca de las reglas de firewall

Como se describe en la documentación del producto NSX, en NSX, las reglas de firewall definidas en el nivel centralizado se conocen como reglas previas. También es posible agregar reglas en un nivel de puerta de enlace Edge individual. Estas reglas se denominan reglas locales.



Cada sesión de tráfico se compara con la regla principal de la tabla de firewall antes de bajar a las reglas subsiguientes de la tabla. Se aplica la primera regla de la tabla que coincide con los parámetros de tráfico. Las reglas se muestran en el siguiente orden:

- 1 Las reglas previas definidas por el usuario tienen la prioridad más alta y se aplican en orden de arriba a abajo con prioridad por nivel de NIC virtual.
- 2 Las reglas asociadas automáticamente (las reglas que permiten que el tráfico de control fluya en los servicios de puerta de enlace Edge).
- 3 Las reglas locales definidas en el nivel de puerta de enlace Edge.
- 4 La regla de firewall distribuido predeterminada.

Para obtener más información sobre cómo el software NSX aplica las reglas de firewall, consulte *Cambiar el orden de una regla de firewall* en la documentación de *administración de NSX*.

## Firewall de puerta de enlace Edge

El firewall de la puerta de enlace Edge ayuda a satisfacer los requisitos clave de seguridad del perímetro, como la creación de DMZ con base en construcciones IP/VLAN, el aislamiento de tenant a tenant en centros de datos virtuales de varios tenants, la traducción de direcciones de red (Network Address Translation, NAT), las VPN de socios (extranet) y las VPN de SSL basadas en usuarios.

El software NSX proporciona la capacidad de firewall de puerta de enlace Edge en el entorno de vCloud Director. En NSX, esta capacidad de firewall también se conoce como firewall de Edge. El firewall de puerta de enlace Edge supervisa el tráfico de norte a sur para proporcionar la funcionalidad de seguridad del perímetro, incluidos el firewall y la traducción de direcciones de red (Network Address Translation, NAT), así como la funcionalidad VPN de SSL y de IPsec de sitio a sitio.

Para obtener más información detallada sobre las capacidades que ofrece el firewall de puerta de enlace Edge del software NSX, consulte la documentación de *administración de NSX*.

## Administrar un firewall de puerta de enlace Edge

Para proteger el tráfico hacia y desde una puerta de enlace Edge, es posible crear y administrar reglas de firewall en esa puerta de enlace Edge.

Para obtener información sobre cómo proteger el tráfico que se transmite entre máquinas virtuales de un centro de datos virtual de organización, consulte [Administrar reglas de firewall distribuido mediante el portal para tenants](#).

Las reglas creadas en la pantalla de firewall distribuido en las que se ha especificado una puerta de enlace Edge avanzada en la columna Aplicado a no se muestran en la pantalla Firewall de dicha puerta de enlace Edge avanzada.

Las reglas de firewall de puerta de enlace Edge para una puerta de enlace Edge se muestran en la pantalla **Firewall** y se aplican en el siguiente orden:

- 1 Reglas internas (también conocidas como reglas asociadas automáticamente). Estas reglas internas permiten que el tráfico de control fluya en los servicios de puerta de enlace Edge.
- 2 Reglas definidas por el usuario.
- 3 Regla predeterminada.

La configuración de la regla predeterminada se aplica al tráfico que no coincide con ninguna de las reglas de firewall definidas por el usuario. La regla predeterminada se muestra en la parte inferior de las reglas en la pantalla Firewall.

En el portal para tenants, utilice el botón de alternancia **Habilitar** en la pantalla Reglas de firewall de la puerta de enlace Edge para deshabilitar o habilitar el firewall de una puerta de enlace Edge.

## Convertir una puerta de enlace Edge en una puerta de enlace Edge avanzada

Para trabajar con una puerta de enlace Edge en el portal para tenants, debe convertirla en una puerta de enlace Edge avanzada. Después de convertirla en una puerta de enlace Edge avanzada, puede utilizar el portal para tenants para configurar las capacidades de enrutamiento estáticas y dinámicas que proporciona el software NSX para las puertas de enlace Edge avanzadas.

### Requisitos previos

Debe tener una puerta de enlace Edge.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y seleccione **Instancias de Edge** en el panel izquierdo.
- 2 Seleccione la puerta de enlace Edge que se editará.
- 3 Haga clic en **Convertir en avanzada**.

### Resultados

La puerta de enlace Edge se convierte en una puerta de enlace Edge avanzada.

### Pasos siguientes

Después de convertirla en una puerta de enlace Edge avanzada, puede modificar la configuración seleccionando la puerta de enlace y haciendo clic en **Configurar servicios**.

## Agregar una regla de firewall de puerta de enlace Edge

Las reglas de firewall de la puerta de enlace Edge se agregan en la pantalla Firewall de la puerta de enlace Edge en cuestión. Puede agregar varias interfaces de NSX Edge y varios grupos de direcciones IP como origen y destino de estas reglas de firewall.

Si especifica **interno** para el origen o el destino de una regla, indica el tráfico de todas las subredes en los grupos de puertos conectados a la puerta de enlace NSX Edge. Si selecciona **interno** como el origen, la regla se actualiza automáticamente cuando se configuran interfaces internas adicionales en la puerta de enlace NSX Edge.

**Nota** Las reglas de firewall de puerta de enlace Edge en las interfaces internas no funcionan cuando la puerta de enlace Edge está configurada para el enrutamiento dinámico.

#### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Si la pantalla Reglas de firewall no se puede ver, haga clic en la pestaña **Firewall**.
- 3 Para agregar una regla debajo de una regla existente en la tabla de reglas de firewall, haga clic en la fila existente y, a continuación, haga clic en el botón **Crear**.

Se agrega una fila para la nueva regla debajo de la regla seleccionada y se le asigna un destino cualquiera, un servicio cualquiera y la acción **Permitir** de forma predeterminada. Cuando la regla predeterminada definida por el sistema es la única regla en la tabla de firewall, la nueva regla se agrega arriba de la regla predeterminada.

- 4 Haga clic en la celda **Nombre** y escriba un nombre.
- 5 Haga clic en la celda **Origen** y utilice los iconos que ahora pueden verse para seleccionar un origen y agregarlo a la regla:

Opción	Descripción
Hacer clic en el icono IP	<p>Escriba el valor de origen que desea utilizar. Los valores válidos son direcciones IP, CIDR, rangos de direcciones IP o la palabra clave <b>cualquiera</b>. El firewall de puerta de enlace Edge admite los formatos IPv4 e IPv6.</p>
Hacer clic en el icono +	<p>Use el icono + para especificar el origen como un objeto distinto de una dirección IP específica:</p> <ul style="list-style-type: none"> <li>■ Utilice la ventana <b>Seleccionar objetos</b> para agregar objetos que coincidan con los elementos seleccionados y haga clic en <b>Conservar</b> para agregarlos a la regla.</li> <li>■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana <b>Seleccionar objetos</b> y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla.</li> </ul> <p>Cuando se selecciona el icono para habilitar o deshabilitar la exclusión en el origen, la regla se aplica al tráfico proveniente de todos los orígenes, excepto del origen que se ha excluido. Cuando el icono para habilitar o deshabilitar la exclusión no se selecciona, la regla se aplica al tráfico proveniente del origen especificado en la ventana <b>Seleccionar objetos</b>.</p>

**6** Haga clic en la celda **Destino** y realice una de las siguientes acciones:

Opción	Descripción
Hacer clic en el icono IP	Escriba el valor de destino que desea utilizar. Los valores válidos son direcciones IP, CIDR, un rango de direcciones IP o la palabra clave <b>cualquiera</b> . El firewall de puerta de enlace Edge admite los formatos IPv4 e IPv6.
Hacer clic en el icono +	<p>Use el icono + para especificar el origen como un objeto distinto de una dirección IP específica:</p> <ul style="list-style-type: none"> <li>■ Utilice la ventana <b>Seleccionar objetos</b> para agregar objetos que coincidan con los elementos seleccionados y haga clic en <b>Conservar</b> para agregarlos a la regla.</li> <li>■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana <b>Seleccionar objetos</b> y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla.</li> </ul> <p>Cuando se selecciona el icono para habilitar o deshabilitar la exclusión en el origen, la regla se aplica al tráfico proveniente de todos los orígenes, excepto del origen que se ha excluido. Cuando el icono para habilitar o deshabilitar la exclusión no se selecciona, la regla se aplica al tráfico proveniente del origen especificado en la ventana <b>Seleccionar objetos</b>.</p>

**7** Haga clic en la celda **Servicio** de la nueva regla y haga clic en el icono + para especificar el servicio como una combinación de protocolo y puerto:

- Seleccione el protocolo de servicio.
- Escriba los números de puerto de los puertos de origen y destino, o bien especifique **cualquiera**.
- Haga clic en **Conservar**.

**8** En la celda **Acción** de la nueva regla, configure la acción de la regla.

Opción	Descripción
Aceptar	Permite el tráfico desde los orígenes, los destinos y los servicios especificados, o bien hacia los mismos.
Denegar	Bloquea el tráfico desde los orígenes, los destinos y los servicios especificados, o bien hacia los mismos.

**9** Haga clic en **Guardar cambios**.

La operación para guardar puede tardar un minuto en completarse.

## Modificar las reglas de firewall de una puerta de enlace Edge

Únicamente puede editar y eliminar las reglas de firewall definidas por el usuario que se hayan agregado a una puerta de enlace Edge. No se puede editar ni eliminar una regla generada automáticamente o una regla predeterminada, excepto para cambiar la configuración de la acción de la regla predeterminada. Puede cambiar el orden de prioridad de las reglas definidas por el usuario.

Para obtener más información sobre la configuración disponible para las diversas celdas de una regla, consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Firewall**.
- 3 Administre las reglas de firewall.
  - Para deshabilitar una regla, haga clic en la marca de verificación de color verde en la celda **N.º**. La marca de verificación de color verde se convierte en un icono de color rojo que indica que está deshabilitada. Si la regla está deshabilitada y desea habilitarla, haga clic en el icono de color rojo que indica que está deshabilitada.
  - Para editar el nombre de una regla, haga doble clic en la celda **Nombre** y escriba el nuevo nombre.
  - Para modificar la configuración de una regla, como la configuración de origen o acción, seleccione la celda adecuada y utilice los controles que se muestran.
  - Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar** situado encima de la tabla de reglas.
  - Oculte las reglas generadas por el sistema mediante el botón de alternancia **Mostrar solo reglas definidas por el usuario**.
  - Para subir o bajar una regla en la tabla de reglas, seleccione la regla y haga clic en los botones de flecha arriba y abajo situados encima de la tabla de reglas.
- 4 Haga clic en **Guardar cambios**.

## Firewall distribuido

El firewall distribuido permite segmentar las entidades de centros de datos virtuales de la organización, como las máquinas virtuales, en función de los atributos y los nombres de las máquinas virtuales.

vCloud Director admite servicios de firewall distribuido en centros de datos virtuales de organización respaldados por NSX Data Center for vSphere. Como se describe en la documentación de *administración de NSX*, el firewall distribuido es un firewall integrado en el kernel del hipervisor que proporciona visibilidad y control para las redes y las cargas de trabajo virtualizadas. Puede crear políticas de control de acceso basadas en objetos, como nombres de máquinas virtuales, y en construcciones de red, como direcciones IP o conjuntos de direcciones IP. Las reglas de firewall se aplican en el nivel de vNIC de cada máquina virtual

para proporcionar control de acceso consistente incluso cuando vSphere vMotion mueve la máquina virtual a un nuevo host ESXi. Este firewall distribuido es compatible con un modelo de seguridad de microsegmentación en el que se puede inspeccionar el tráfico de este a oeste en un procesamiento casi a velocidad de línea.

Como se describe en la documentación de *administración de NSX*, para los paquetes de capa 2 (Layer 2, L2), el firewall distribuido crea una caché para aumentar el rendimiento. Los paquetes de capa 3 (L3) se procesan en la siguiente secuencia:

- 1 Se comprueba el estado existente de todos los paquetes.
  - 2 Cuando se encuentra una coincidencia de estado, se procesan los paquetes.
  - 3 Cuando no se encuentra una coincidencia de estado, se procesan los paquetes mediante las reglas hasta que se encuentra una coincidencia.
- Para los paquetes TCP, solo se establece un estado para los paquetes con la marca SYN. Sin embargo, las reglas que no especifican un protocolo (servicio ANY), pueden hacer coincidir paquetes TCP con cualquier combinación de marcas.
  - Para los paquetes UDP, se extraen los detalles de 5-tupla de los paquetes. Cuando no existe un estado en la tabla de estado, se crea un nuevo estado mediante los detalles de 5-tupla extraídos. Los paquetes recibidos posteriormente se comparan con el estado que se acaba de crear.
  - Para los paquetes ICMP, la dirección de paquete, el código y el tipo de ICMP se utilizan para crear un estado.

El firewall distribuido también puede ayudar a crear reglas basadas en identidades. Los administradores pueden aplicar el control de acceso según la pertenencia a grupos del usuario definida en la instancia de Active Directory (AD) de la empresa. Algunos escenarios de uso cuando es posible utilizar reglas de firewall basadas en identidades son:

- Los usuarios acceden a aplicaciones virtuales con un equipo portátil o un dispositivo móvil en los que se utiliza AD para la autenticación de usuario
- Los usuarios acceden a aplicaciones virtuales mediante la infraestructura de VDI donde las máquinas virtuales se basan en Microsoft Windows

Para obtener información más detallada sobre las capacidades que ofrece el firewall distribuido del software NSX, consulte la documentación de *administración de NSX*.

## Habilitar el firewall distribuido en un centro de datos virtual de organización mediante el portal para tenants

Antes de utilizar el portal para tenants para trabajar con las capacidades de firewall distribuido en un centro de datos virtual de organización, se debe habilitar el firewall distribuido para ese centro de datos virtual de organización. Un administrador del sistema de vCloud Director o un usuario al que se haya concedido el derecho `ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE` puede habilitar el firewall distribuido en un centro de datos virtual de organización.

Se utiliza la pantalla Firewall distribuido del portal para tenants a fin de habilitar el firewall distribuido de un centro de datos virtual de organización.

### Requisitos previos

vCloud Director admite servicios de firewall distribuido en centros de datos virtuales de organización respaldados por NSX Data Center for vSphere.

Compruebe que se hayan asignado los siguientes derechos a la organización a la que pertenece el centro de datos virtual de organización:

- Firewall distribuido de VDC de organización: habilitar o deshabilitar
- Firewall distribuido de VDC de organización: configurar reglas
- Firewall distribuido de VDC de organización: ver reglas

El administrador del sistema de vCloud Director asigna derechos a una organización. El derecho Firewall distribuido de VDC de organización: habilitar o deshabilitar es necesario para habilitar el firewall distribuido mediante la interfaz de usuario en el portal para tenants. El derecho Firewall distribuido de VDC de organización: ver reglas es necesario para ver las reglas de firewall en el portal para tenants, mientras que el derecho Firewall distribuido de VDC de organización: configurar reglas es necesario para la configuración de las reglas de firewall mediante el portal para tenants.

Compruebe que se le haya asignado una función que le otorga el derecho llamado Firewall distribuido de VDC de organización: habilitar o deshabilitar. De las funciones predefinidas en un sistema de vCloud Director, solo la función de administrador del sistema tiene ese derecho de forma predeterminada.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione el centro de datos virtual de organización para el que desea configurar reglas de firewall distribuido.
- 3 Haga clic en **Configurar servicios**.
- 4 Habilite el firewall distribuido en la pestaña **Firewall distribuido**.

### Pasos siguientes

Para obtener una descripción de la regla de firewall distribuido predeterminada, consulte [Administrar reglas de firewall distribuido mediante el portal para tenants](#).

## Administrar reglas de firewall distribuido mediante el portal para tenants

Como se describe en la *guía de administración de NSX*, la configuración de firewall predeterminada se aplica al tráfico que no coincide con ninguna de las reglas de firewall definidas

por el usuario. En el vCloud Director Tenant Portal, la regla de firewall distribuido predeterminada tiene la etiqueta Regla para permitir predeterminada.

Para poder administrar la configuración del firewall distribuido mediante el vCloud Director Tenant Portal, es necesario habilitar la funcionalidad del firewall distribuido en un centro de datos virtual de organización.

Se configura la regla de firewall distribuido predeterminada para permitir que todo el tráfico de capa 3 y de capa 2 pase por el centro de datos virtual de organización. Esta configuración se indica mediante la opción Permitir establecida en la columna Acción de la interfaz de usuario. La regla predeterminada siempre se ubica en la parte inferior de la tabla de reglas.

---

**Importante** No puede eliminar ni modificar las reglas predeterminadas del firewall distribuido.

---

## Acceder a la configuración de reglas de firewall distribuido

La regla de firewall distribuido predeterminada se muestra en la pantalla Firewall distribuido del portal para tenants cuando se abre desde la consola web de vCloud Director.

### Procedimiento

- 1 Desplácese hasta una instancia de VDC de organización en la consola web de vCloud Director.
- 2 Haga clic con el botón secundario en la instancia de VDC de organización y seleccione **Administrar firewall**.

Tanto la pestaña General para el tráfico de 3 capas como la pestaña Ethernet para el tráfico de 2 capas tienen una regla de firewall distribuido predeterminada.

## Agregar una regla de firewall distribuido

Primero debe agregar una regla de firewall distribuido al alcance del centro de datos virtual de organización. A continuación, puede limitar el alcance en el que desea que se aplique la regla. El firewall distribuido permite añadir varios objetos en los niveles de origen y destino para cada regla, lo que permite reducir el número total de reglas de firewall que se añadirán.

Para obtener información sobre los servicios predefinidos y los grupos de servicios que se pueden utilizar en una regla, consulte [Ver los servicios disponibles para reglas de firewall](#) y [Ver los grupos de servicios disponibles para reglas de firewall](#).

### Requisitos previos

- [Habilitar el firewall distribuido en un centro de datos virtual de organización mediante el portal para tenants](#)
- Si desea utilizar un conjunto de direcciones IP como origen o destino en una regla, [Crear un conjunto de direcciones IP para usarlas en las reglas de firewall y la configuración de retransmisión de DHCP](#).
- Si desea utilizar un conjunto de direcciones MAC como origen o destino en una regla, [Crear un conjunto de direcciones MAC para utilizarlas en las reglas de firewall](#).



- Si desea utilizar un grupo de seguridad como origen o destino en una regla, [Crear un grupo de seguridad](#).

#### Procedimiento


- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.

- 2 Seleccione la red de VDC de servicios de seguridad para la que desea modificar las reglas de firewall y haga clic en **Configurar servicios**.

Aparecerá la pantalla Servicios de seguridad.

- 3 Seleccione el tipo de regla que desea crear. Puede crear una regla general o una regla de Ethernet.

Las reglas de capa 3 (Layer 3, L3) se configuran en la pestaña **General**. Las reglas de capa 2 (Layer 2, L2) se configuran en la pestaña **Ethernet**.

- 4 Para agregar una regla debajo de una regla existente en la tabla de firewall, haga clic en la fila existente y, a continuación, haga clic en el botón **Crear** ().

Se agrega una fila para la nueva regla debajo de la regla seleccionada y se le asigna un destino cualquiera, un servicio cualquiera y la acción **Permitir** de forma predeterminada. Cuando la regla definida por el sistema Permitir de manera predeterminada es la única regla en la tabla de firewall, la nueva regla se agrega arriba de la regla predeterminada.

- 5 Haga clic en la celda **Nombre** y escriba un nombre.

- 6 Haga clic en la celda **Origen** y utilice los iconos que ahora pueden verse para seleccionar un origen y agregarlo a la regla:

Acción	Descripción
Hacer clic en el icono IP	Se aplica a las reglas definidas en la pestaña <b>General</b> . Escriba el valor de origen que desea utilizar. Los valores válidos son direcciones IP, CIDR, un rango de direcciones IP o la palabra clave <b>cualquiera</b> . El firewall distribuido solo es compatible con el formato de IPv4.
Hacer clic en el icono +	Use el icono + para especificar el origen como un objeto distinto de una dirección IP específica: <ul style="list-style-type: none"> <li>■ Utilice la ventana <b>Seleccionar objetos</b> para agregar objetos que coincidan con los elementos seleccionados y haga clic en <b>Conservar</b> para agregarlos a la regla.</li> <li>■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana <b>Seleccionar objetos</b> y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla.</li> </ul> <p>Cuando se selecciona el icono para habilitar o deshabilitar la exclusión en el origen, la regla se aplica al tráfico proveniente de todos los orígenes, excepto del origen que se ha excluido. Cuando el icono para habilitar o deshabilitar la exclusión no se selecciona, la regla se aplica al tráfico proveniente del origen especificado en la ventana <b>Seleccionar objetos</b>.</p>

- 7 Haga clic en la celda **Destino** y realice una de las siguientes acciones:

Acción	Descripción
Hacer clic en el icono IP	Se aplica a las reglas definidas en la pestaña <b>General</b> . Escriba el valor de destino que desea utilizar. Los valores válidos son direcciones IP, CIDR, un rango de direcciones IP o la palabra clave <b>cualquiera</b> . El firewall distribuido solo es compatible con el formato de IPv4.
Hacer clic en el icono +	Use el icono + para especificar el origen como un objeto distinto de una dirección IP específica: <ul style="list-style-type: none"> <li>■ Utilice la ventana <b>Seleccionar objetos</b> para agregar objetos que coincidan con los elementos seleccionados y haga clic en <b>Conservar</b> para agregarlos a la regla.</li> <li>■ Para excluir un origen de la regla, agréguelo a esta regla mediante la ventana <b>Seleccionar objetos</b> y, a continuación, seleccione el icono para habilitar o deshabilitar la exclusión para excluir dicho origen de esta regla.</li> </ul> <p>Cuando se selecciona el icono para habilitar o deshabilitar la exclusión en el origen, la regla se aplica al tráfico proveniente de todos los orígenes, excepto del origen que se ha excluido. Cuando el icono para habilitar o deshabilitar la exclusión no se selecciona, la regla se aplica al tráfico proveniente del origen especificado en la ventana <b>Seleccionar objetos</b>.</p>

- 8 Haga clic en la celda **Servicio** de la nueva regla y realice una de las siguientes acciones:

Acción	Descripción
Hacer clic en el icono IP	Para especificar el servicio como una combinación de puerto y protocolo, realice lo siguiente: <ul style="list-style-type: none"> <li>a Seleccione el protocolo de servicio.</li> <li>b Escriba los números de puerto de los puertos de origen y destino (o especifique <b>cualquiera</b>), y haga clic en <b>Conservar</b>.</li> </ul>
Hacer clic en el icono +	Para seleccionar servicios o grupos de servicios predefinidos, o bien definir uno nuevo, realice lo siguiente: <ul style="list-style-type: none"> <li>a Seleccione uno o varios objetos, y añádalos al filtro.</li> <li>b Haga clic en <b>Conservar</b>.</li> </ul>

- 9 En la celda **Acción** de la nueva regla, configure la acción de la regla.

Opción	Descripción
Permitir	Permite el tráfico desde los orígenes, los destinos y los servicios especificados, o bien hacia los mismos.
Denegar	Bloquea el tráfico desde los orígenes, los destinos y los servicios especificados, o bien hacia los mismos.

- 10 En la celda **Dirección** de la nueva regla, determine si la regla se aplica al tráfico entrante, al tráfico saliente o a ambos.
- 11 Si se trata de una regla en la pestaña **General**, en la celda **Tipo de paquete** de la nueva regla, seleccione el tipo de paquete **Cualquiera**, **IPV4** o **IPV6**.
- 12 Seleccione la celda **Aplicado a** y use el icono + para definir el alcance de objetos al que se aplica esta regla.

Cuando la regla contiene máquinas virtuales en las celdas **Origen** y **Destino**, debe agregar las máquinas virtuales de origen y destino a la sección **Aplicado a** de la regla para que esta funcione correctamente.

**Importante** Los grupos de direcciones IP (conjuntos de direcciones IP), los grupos de direcciones MAC (conjuntos de direcciones MAC) y los grupos de seguridad que contienen conjuntos de direcciones IP o MAC no son parámetros de entrada válidos.


- 13 Haga clic en **Guardar cambios**.

## Editar una regla de firewall distribuido

En un entorno de vCloud Director, para modificar una regla de firewall distribuido existente de un centro de datos virtual de organización, utilice la pantalla **Firewall distribuido**.

Para obtener más información sobre la configuración disponible para las diversas celdas de una regla, consulte [Agregar una regla de firewall distribuido](#).

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione la red de VDC de servicios de seguridad para la que desea modificar las reglas de firewall y haga clic en **Configurar servicios**.  
Aparecerá la pantalla Servicios de seguridad.
- 3 Realice cualquiera de las siguientes acciones para administrar las reglas de firewall distribuido:
  - Para deshabilitar una regla, haga clic en la marca de verificación de color verde en la celda **N.º**.  
  
La marca de verificación de color verde se convierte en un icono de color rojo que indica que está deshabilitada. Si la regla está deshabilitada y desea habilitarla, haga clic en el icono de color rojo que indica que está deshabilitada.
  - Para editar el nombre de una regla, haga doble clic en la celda **Nombre** y escriba el nuevo nombre.
  - Para modificar la configuración de una regla, como la configuración de origen o acción, seleccione la celda adecuada y utilice los controles que se muestran.
  - Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar** () situado encima de la tabla de reglas.
  - Para subir o bajar una regla en la tabla de reglas, seleccione la regla y haga clic en los botones de flecha arriba y abajo situados encima de la tabla de reglas.
- 4 Haga clic en **Guardar cambios**.

## Administrar DHCP de puerta de enlace Edge

Las puertas de enlace Edge se configuran para prestar servicios de protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) a las máquinas virtuales conectadas a las redes de centros de datos virtuales de organización asociadas.

Tal como se describe en la [documentación de NSX](#), las capacidades de la puerta de enlace NSX Edge incluyen la agrupación de direcciones IP, la asignación uno a uno de direcciones IP estáticas y la configuración de servidores DNS externos. El enlace de direcciones IP estáticas se basa en el identificador del objeto administrado y el identificador de la interfaz de la máquina virtual del cliente que realiza la solicitud.

El servicio DHCP de una puerta de enlace NSX Edge realiza lo siguiente:

- Escucha en la interfaz interna de la puerta de enlace Edge para la detección DHCP.
- Utiliza la dirección IP de la interfaz interna de la puerta de enlace Edge como la dirección de puerta de enlace predeterminada para todos los clientes.

- Utiliza los valores de máscara de subred y difusión de la interfaz interna para la red de contenedor.

En las siguientes situaciones, debe reiniciar el servicio DHCP en las máquinas virtuales de cliente a las que DHCP ha asignado direcciones IP:

- Si ha cambiado o eliminado un grupo de DHCP, una puerta de enlace predeterminada o un servidor DNS.
- Si ha cambiado la dirección IP interna de la instancia de la puerta de enlace Edge.

---

**Nota** Si se modifica la configuración de DNS de una puerta de enlace Edge habilitada para DHCP, puede que la puerta de enlace Edge deje de proporcionar servicios DHCP. Si se produce esta situación, utilice el botón de alternancia **Estado del servicio DHCP** en la pantalla Grupos de DHCP para deshabilitar y volver a habilitar DHCP en dicha puerta de enlace Edge. Consulte [Agregar un grupo de direcciones IP de DHCP](#).

---

## Agregar un grupo de direcciones IP de DHCP

Es posible configurar los grupos de direcciones IP necesarios para un servicio DHCP de una puerta de enlace Edge avanzada. DHCP automatiza la asignación de direcciones IP a las máquinas virtuales conectadas con redes de centros de datos virtuales de organización.

Como se describe en la documentación de *administración de NSX*, el servicio DHCP requiere un grupo de direcciones IP. Un grupo de direcciones IP es un rango secuencial de direcciones IP dentro de la red. A las máquinas virtuales protegidas por la puerta de enlace Edge que no tienen un enlace de dirección se les asigna una dirección IP de este grupo. Los rangos de grupos de direcciones IP no pueden cruzarse entre sí, por lo que una dirección IP solo puede pertenecer a un grupo de direcciones IP.

---

**Nota** Se debe configurar al menos un grupo de direcciones IP de DHCP de manera que el estado del servicio DHCP esté activado.


---

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **DHCP > Grupos**.

- 3 Si el servicio DHCP no está habilitado, active el botón de alternancia **Estado del servicio DHCP**.

**Nota** Agregue al menos un grupo de direcciones IP de DHCP antes de guardar los cambios realizados después de activar el botón de alternancia **Estado del servicio DHCP**. Si no aparece ningún grupo de direcciones IP de DHCP en la pantalla, y si activa el botón de alternancia **Estado del servicio DHCP** y guarda los cambios, la pantalla se muestra con el botón de alternancia desactivado.

- 4 En Grupos de DHCP, haga clic en el botón **Crear** () , especifique los detalles del grupo de DHCP y haga clic en **Conservar**.

Opción	Descripción
Rango de IP	Escriba un rango de direcciones IP.
Nombre de dominio	Nombre de dominio del servidor DNS.
Autoconfigurar DNS	Active este botón de alternancia a fin de utilizar la configuración del servicio DNS para el enlace de DNS del grupo de direcciones IP. Si está habilitado, las opciones <b>Servidor de nombres principal</b> y <b>Servidor de nombres secundario</b> se establecen como <b>Automático</b> .
Servidor de nombres principal	Si no habilita <b>Autoconfigurar DNS</b> , escriba la dirección IP del servidor DNS primario. Esta dirección IP se utiliza para la resolución de un nombre de host como una dirección IP.
Servidor de nombres secundario	Si no habilita <b>Autoconfigurar DNS</b> , escriba la dirección IP del servidor DNS secundario. Esta dirección IP se utiliza para la resolución de un nombre de host como una dirección IP.
Puerta de enlace predeterminada	Escriba la dirección de puerta de enlace predeterminada. Cuando no se especifica la dirección IP de puerta de enlace predeterminada, la interfaz interna de la instancia de puerta de enlace Edge se toma como la puerta de enlace predeterminada.
Máscara de subred	Escriba la máscara de subred de la interfaz de puerta de enlace Edge.
La concesión no caduca nunca	Habilite este botón de alternancia para que se mantenga indefinidamente el enlace de las direcciones IP que se han asignado fuera de este grupo con sus máquinas virtuales asignadas. Cuando se selecciona esta opción, <b>Tiempo de concesión</b> se establece como infinito.
Tiempo de concesión (segundos)	Periodo de tiempo (en segundos) que las direcciones IP asignadas por DHCP se otorgan como concesión a los clientes. El tiempo de concesión predeterminado es un día (86.400 segundos).
<b>Nota</b> No se puede especificar un tiempo de concesión cuando se selecciona <b>La concesión no caduca nunca</b> .	

- 5 Haga clic en **Guardar cambios**.

## Resultados

vCloud Director actualiza la puerta de enlace Edge para proporcionar servicios DHCP.


## Agregar enlaces de DHCP

Si hay servicios en ejecución en una máquina virtual y no desea que la dirección IP cambie, puede enlazar la dirección MAC de la máquina virtual a la dirección IP. La dirección IP que enlace no debe superponerse con un grupo de direcciones IP de DHCP.

### Requisitos previos

Tiene las direcciones MAC de las máquinas virtuales para las que desea establecer enlaces.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 En la pestaña **DHCP > Enlaces**, haga clic en el botón **Crear** () , especifique los detalles para el enlace y haga clic en **Conservar**.

Opción	Descripción
Dirección MAC	Escriba la dirección MAC de la máquina virtual que desea enlazar a la dirección IP.
Nombre del host	Escriba el nombre del host que desea establecer para la máquina virtual cuando esta solicita una concesión de DHCP.
Dirección IP	Escriba la dirección IP que desea enlazar con la dirección MAC.
Máscara de subred	Escriba la máscara de subred de la interfaz de puerta de enlace Edge.
Nombre de dominio	Escriba el nombre de dominio del servidor DNS.
Autoconfigurar DNS	Habilite este botón de alternancia para utilizar la configuración del servicio DNS de este enlace de DNS.  Si está habilitado, las opciones <b>Servidor de nombres principal</b> y <b>Servidor de nombres secundario</b> se establecen como <b>Automático</b> .
Servidor de nombres principal	Si no selecciona <b>Autoconfigurar DNS</b> , escriba la dirección IP del servidor DNS primario.  Esta dirección IP se utiliza para la resolución de un nombre de host como una dirección IP.
Servidor de nombres secundario	Si no selecciona <b>Autoconfigurar DNS</b> , escriba la dirección IP del servidor DNS secundario.  Esta dirección IP se utiliza para la resolución de un nombre de host como una dirección IP.
Puerta de enlace predeterminada	Escriba la dirección de puerta de enlace predeterminada.  Cuando no se especifica la dirección IP de puerta de enlace predeterminada, la interfaz interna de la instancia de puerta de enlace Edge se toma como la puerta de enlace predeterminada.

Opción	Descripción
La concesión no caduca nunca	Habilite este botón de alternancia para conservar la dirección IP enlazada con esa dirección MAC por un tiempo indefinido. Cuando se selecciona esta opción, <b>Tiempo de concesión</b> se establece como infinito.
Tiempo de concesión (segundos)	Periodo de tiempo (en segundos) que las direcciones IP asignadas por DHCP se otorgan como concesión a los clientes. El tiempo de concesión predeterminado es un día (86.400 segundos).  <b>Nota</b> No se puede especificar un tiempo de concesión cuando se selecciona <b>La concesión no caduca nunca</b> .

3 Haga clic en **Guardar cambios**.

## Configurar la retransmisión de DHCP para puertas de enlace Edge

La capacidad de retransmisión de DHCP que ofrece NSX en el entorno de vCloud Director permite aprovechar la infraestructura de DHCP existente dentro del entorno de vCloud Director sin interrupciones a la administración de direcciones IP en la infraestructura de DHCP existente. Los mensajes DHCP se retransmiten de las máquinas virtuales a los servidores DHCP designados en la infraestructura física de DHCP, lo que permite que las direcciones IP que controla el software NSX sigan estando sincronizadas con las direcciones IP en el resto de los entornos controlados por DHCP.

La configuración de retransmisión de DHCP de una puerta de enlace Edge puede enumerar varios servidores DHCP. Las solicitudes se envían a todos los servidores enumerados. Mientras se retransmite la solicitud DHCP de las máquinas virtuales, la puerta de enlace Edge agrega una dirección IP de puerta de enlace a la solicitud. El servidor DHCP externo utiliza esta dirección de puerta de enlace para buscar una coincidencia de un grupo y asignar una dirección IP para la solicitud. La dirección de puerta de enlace debe pertenecer a una subred de la interfaz de la puerta de enlace Edge.

Puede especificar un servidor DHCP diferente para cada puerta de enlace Edge y puede configurar varios servidores DHCP en cada puerta de enlace Edge para ofrecer compatibilidad con varios dominios IP.

### Nota

- La retransmisión de DHCP no admite la superposición de espacios de direcciones IP.
- La retransmisión de DHCP y el servicio DHCP no se pueden ejecutar en la misma vNIC al mismo tiempo. Si se configura un agente de retransmisión en una vNIC, no se puede configurar un grupo de DHCP en las subredes de dicha vNIC. Consulte la *guía de administración de NSX* para obtener más detalles.



## Especificar una configuración de retransmisión de DHCP para una puerta de enlace Edge

El software NSX en el entorno de vCloud Director proporciona a la puerta de enlace Edge la capacidad para retransmitir los mensajes DHCP que se dirigen a los servidores DHCP externos al centro de datos virtual de organización de vCloud Director. Es posible configurar la capacidad de retransmisión de DHCP de la puerta de enlace Edge.

Como se describe en la documentación de *administración de NSX*, es posible especificar los servidores DHCP mediante un conjunto de direcciones IP, un bloque de direcciones IP o un dominio existentes, o bien con una combinación de todos los elementos anteriores. Los mensajes DHCP se retransmiten a cada servidor DHCP especificado.

También debe configurar al menos un agente de retransmisión de DHCP. Un agente de retransmisión de DHCP es una interfaz en la puerta de enlace Edge desde la que se retransmiten las solicitudes DHCP a los servidores DHCP externos.

### Requisitos previos


Si desea utilizar un conjunto de direcciones IP para especificar un servidor DHCP, compruebe que el conjunto de direcciones IP exista como un objeto de agrupamiento disponible para la puerta de enlace Edge. Consulte [Crear un conjunto de direcciones IP para usarlas en las reglas de firewall y la configuración de retransmisión de DHCP](#).

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **DHCP > Retransmisión**.
- 3 Utilice los campos que aparecen en pantalla para especificar los servidores DHCP por direcciones IP, nombres de dominio o conjuntos de direcciones IP.

Se selecciona de los conjuntos de direcciones IP existentes mediante el botón **Agregar**

() para examinar los conjuntos de direcciones IP disponibles.

- 4 Para configurar un agente de retransmisión de DHCP y agregar la configuración a la tabla en pantalla, haga clic en el botón **Agregar** () , seleccione una vNIC y su dirección IP de puerta de enlace, y, a continuación, haga clic en **Conservar**.

De forma predeterminada, la dirección IP de puerta de enlace coincide con la dirección principal de la vNIC seleccionada. Puede conservar el valor predeterminado o seleccionar una dirección alternativa si hay una en dicha vNIC.

- 5 Haga clic en **Guardar cambios**.

## Administrar la traducción de direcciones de red mediante el portal para tenants

El software NSX en el entorno de vCloud Director permite que las puertas de enlace Edge proporcionen un servicio de traducción de direcciones de red (Network Address Translation, NAT). Con esta capacidad, se reduce la cantidad de direcciones IP públicas que debe usar una organización para fines de seguridad y economía.

El servicio NAT de la puerta de enlace Edge proporciona la capacidad de asignar una dirección pública a una máquina virtual o un grupo de máquinas virtuales en una red privada. Para permitir que las puertas de enlace Edge proporcionen acceso a los servicios que se ejecutan en máquinas virtuales con direcciones privadas del centro de datos virtual de organización, debe configurar reglas NAT en las puertas de enlace Edge. En el caso más común, se asocia un servicio NAT con una interfaz de vínculo superior en una puerta de enlace Edge del entorno de vCloud Director para que las direcciones en las redes de centros de datos virtuales de organización no queden expuestas en la red externa.

La configuración del servicio NAT se separa en reglas NAT de origen (Source NAT, SNAT) y reglas NAT de destino (Destination NAT, DNAT). Cuando se configura una regla SNAT o DNAT en una puerta de enlace Edge en el entorno de vCloud Director, siempre se configura la regla desde la perspectiva del centro de datos virtual de organización. En concreto, eso significa que se deben configurar las reglas de las siguientes maneras:

- SNAT: el tráfico se transmite desde una máquina virtual en una red interna del centro de datos virtual de organización (origen) a través de Internet hasta la red externa (el destino). Una regla SNAT traduce la dirección IP de origen de los paquetes salientes de una red de centros de datos virtuales de organización que se envían a una red externa o a otra red de centros de datos virtuales de organización.
- DNAT: el tráfico se transmite desde Internet (origen) hasta una máquina virtual dentro del centro de datos virtual de organización (destino). Una regla DNAT traduce la dirección IP (y opcionalmente, el puerto) de los paquetes que recibe una red de centros de datos virtuales de organización de una red externa o de otra red de centros de datos virtuales de organización.

Puede configurar reglas NAT para crear un espacio de direcciones IP privadas dentro del centro de datos virtual de organización. Esta configuración ofrece la capacidad de mover un espacio de direcciones IP privadas de un centro de datos virtual de organización a otro. La configuración de reglas NAT permite utilizar las mismas direcciones IP privadas para máquinas virtuales de un centro de datos virtual de organización que se utilizaron en otro.

La capacidad de reglas NAT en el entorno de vCloud Director admite lo siguiente:

- Crear subredes dentro de un espacio de direcciones IP privadas
- Crear varios espacios de direcciones IP privadas para una puerta de enlace Edge

- Configurar varias reglas NAT en varias interfaces de puerta de enlace Edge

---

**Importante** Debe configurar reglas NAT y de firewall en la puerta de enlace Edge para que sea posible acceder a las máquinas virtuales en una red de la puerta de enlace Edge. De forma predeterminada, las puertas de enlace Edge se implementan con reglas de firewall configuradas para denegar todo el tráfico de red desde y hacia las máquinas virtuales en las redes de puerta de enlace Edge. Además, la opción NAT está deshabilitada de forma predeterminada en las puertas de enlace Edge de modo que dichas puertas no pueden traducir las direcciones IP del tráfico entrante y saliente, a menos que se configure NAT en las puertas de enlace Edge. Se producirá un error al intentar hacer ping en una máquina virtual de una red después de configurar una regla NAT a menos que se agregue una regla de firewall para permitir el tráfico correspondiente.

---

## Agregar una regla SNAT o DNAT

Puede crear una regla NAT (Source NAT, SNAT) de origen para cambiar la dirección IP de origen de pública a privada, o viceversa. Puede crear una regla NAT (Destination NAT, DNAT) de destino para cambiar la dirección IP de destino de pública a privada, o viceversa.

Al crear reglas NAT, puede especificar las direcciones IP originales y traducidas mediante los siguientes formatos:

- Dirección IP (por ejemplo, 192.0.2.0)
- Rango de direcciones IP (por ejemplo, 192.0.2.0-192.0.2.24)
- Dirección IP/máscara de subred (por ejemplo, 192.0.2.0/24)
- any

Cuando se configura una regla SNAT o DNAT en una puerta de enlace Edge en el entorno de vCloud Director, siempre se configura la regla desde la perspectiva del centro de datos virtual de organización. Una regla SNAT traduce la dirección IP de origen de los paquetes enviados de una red de centros de datos virtuales de organización a una red externa o a otra red de centros de datos virtuales de organización. Una regla DNAT traduce la dirección IP (y opcionalmente, el puerto) de los paquetes que recibe una red de centros de datos virtuales de organización de una red externa o de otra red de centros de datos virtuales de organización.

### Requisitos previos

Las direcciones IP públicas deben haberse agregado a la interfaz de puerta de enlace Edge en la que desea agregar la regla. Para las reglas DNAT, la dirección IP original (pública) debe haberse agregado a la interfaz de puerta de enlace Edge. En cambio, para las reglas SNAT, la dirección IP traducida (pública) debe haberse agregado a la interfaz.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.

- 2 Haga clic en **NAT** para ver la pantalla Reglas NAT.
- 3 Según el tipo de regla NAT que se crea, haga clic en **Regla DNAT** o en **Regla SNAT**.
- 4 Configure una regla NAT de destino (de afuera hacia adentro).

Opción	Descripción
Aplicado en	Seleccione la interfaz en la que se va a aplicar la regla.
IP/rango original	<p>Escriba la dirección IP requerida.</p> <p>Esta debe ser la dirección IP pública de la puerta de enlace Edge para la que se va a configurar la regla DNAT. En el paquete que se está inspeccionando, esta dirección IP o este rango serían los que se muestran como la dirección IP de destino del paquete. Estas direcciones de destino del paquete son las que traduce esta regla DNAT.</p>
Protocolo	Seleccione el protocolo al que se aplica la regla. Para aplicar esta regla a todos los protocolos, seleccione <b>Cualquiera</b> .
Puerto original	(Opcional) Seleccione el puerto o el rango de puertos que el tráfico entrante utiliza en la puerta de enlace Edge para conectarse a la red interna en la que se conectan las máquinas virtuales. Esta selección no está disponible cuando se establece <b>Protocolo</b> como <b>ICMP</b> o <b>Cualquiera</b> .
Tipo de ICMP	<p>Si selecciona <b>ICMP</b> (una utilidad de informe y diagnóstico de errores usada entre dispositivos para comunicar información de errores) en <b>Protocolo</b>, seleccione un valor de <b>Tipo de ICMP</b> del menú desplegable.</p> <p>Los mensajes de ICMP se identifican por campo de tipo. De forma predeterminada, el tipo de ICMP se establece en cualquiera.</p>
IP/rango traducido	<p>Escriba la dirección IP o un rango de direcciones IP a los que se traducirán las direcciones de destino en los paquetes entrantes.</p> <p>Estas direcciones son las direcciones IP de una o varias máquinas virtuales para las que se configura DNAT, de modo que puedan recibir tráfico de la red externa.</p>
Puerto traducido	(Opcional) Seleccione el puerto o el rango de puertos a los que se conecta el tráfico entrante en las máquinas virtuales de la red interna. Estos son los puertos a los que traduce la regla DNAT para los paquetes entrantes a las máquinas virtuales.
Descripción	(Opcional) Escriba una descripción que permita identificar lo que hace esta regla.
Habilitado	Active el botón de alternancia para habilitar esta regla.
Habilitar registro	Active el botón de alternancia para que se registre la traducción de direcciones realizada por esta regla.

## 5 Configure una regla NAT de origen (de adentro hacia afuera).

Opción	Descripción
Aplicado en	Seleccione la interfaz en la que se va a aplicar la regla.
IP/rango de origen original	<p>Escriba la dirección IP o el rango de direcciones IP originales que se va a aplicar a esta regla.</p> <p>Estas direcciones son las direcciones IP de una o varias máquinas virtuales para las que se configura la regla SNAT, de modo que puedan enviar tráfico a la red externa.</p>
IP/rango de origen traducido	<p>Escriba la dirección IP requerida.</p> <p>Esta dirección es siempre la dirección IP pública de la puerta de enlace para la que se va a configurar la regla SNAT. Especifica la dirección IP a la que se traducen las direcciones de origen (las máquinas virtuales) en paquetes salientes cuando envían tráfico a la red externa.</p>
Descripción	(Opcional) Escriba una descripción que permita identificar lo que hace esta regla.
Habilitado	Active el botón de alternancia para habilitar esta regla.
Habilitar registro	Active el botón de alternancia para que se registre la traducción de direcciones realizada por esta regla.

6 Haga clic en **Conservar** para agregar la regla a la tabla que aparece en pantalla.

7 Repita los pasos para configurar reglas adicionales.

8 Haga clic en **Guardar cambios** para guardar las reglas en el sistema.

### Pasos siguientes

Agregue reglas de firewall de puerta de enlace Edge correspondientes a las reglas SNAT o DNAT que acaba de configurar. Consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

## Configuración avanzada de enrutamiento

Es posible configurar las capacidades de enrutamiento estático y dinámico que proporciona el software de NSX para las puertas de enlace Edge.

Para habilitar el enrutamiento dinámico, configure una puerta de enlace Edge avanzada mediante los protocolos Border Gateway Protocol (BGP) o Open Shortest Path First (OSPF).

Para obtener información detallada sobre las funcionalidades de enrutamiento que proporciona NSX, consulte *Enrutamiento* en la documentación de *administración de NSX*.

Puede especificar el enrutamiento estático y dinámico de cada puerta de enlace Edge avanzada. La capacidad de enrutamiento dinámico brinda la información de reenvío necesaria entre los dominios de difusión de Capa 2, lo que permite reducir los dominios de difusión de Capa 2, así como mejorar la escala y la eficiencia de la red. NSX extiende esta inteligencia hasta las ubicaciones de las cargas de trabajo para el enrutamiento de este a oeste. Esta capacidad permite una comunicación más directa entre máquinas virtuales, sin el tiempo ni el coste adicionales necesarios para ampliar los saltos.

## Especificar la configuración de enrutamiento predeterminada de la puerta de enlace Edge

Puede especificar la configuración predeterminada del enrutamiento estático y del enrutamiento dinámico de una puerta de enlace Edge.

---

**Nota** Para quitar toda la configuración de enrutamiento, utilice el botón **BORRAR CONFIGURACIÓN GLOBAL** en la parte inferior de la pantalla **Configuración de enrutamiento**. Esta acción elimina toda la configuración de enrutamiento especificada actualmente en las subpantallas: configuración de enrutamiento predeterminada, rutas estáticas, OSPF, BGP y redistribución de rutas.

---

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Enrutamiento > Configuración de enrutamiento**.
- 3 Para habilitar el enrutamiento Equal Cost Multipath (ECMP) para esta puerta de enlace Edge, active el botón de alternancia **ECMP**.

Como se describe en la documentación de *administración de NSX*, ECMP es una estrategia de enrutamiento que permite que el reenvío de paquetes de siguiente salto a un destino único se produzca a través de varias de las mejores rutas. NSX determina cuáles son las mejores rutas de forma estática mediante rutas estáticas configuradas, o bien como resultado de cálculos de métricas mediante protocolos de enrutamiento dinámico como OSPF o BGP. Para especificar varias rutas de acceso para rutas estáticas, especifique varios saltos siguientes en la pantalla Rutas estáticas.

Para obtener más detalles sobre ECMP y NSX, consulte los temas relacionados con el enrutamiento en la *Guía de solución de problemas de NSX*.

- 4 Especifique la configuración de la puerta de enlace de enrutamiento predeterminada.
  - a Utilice la lista desplegable **Aplicado en** para seleccionar una interfaz desde la que se puede alcanzar el siguiente salto a la red de destino.  
  
Para ver detalles acerca de la interfaz seleccionada, haga clic en el icono de información de color azul.
  - b Escriba la dirección IP de la puerta de enlace.
  - c Escriba el valor de MTU.
  - d (opcional) Escriba una descripción opcional.
  - e Haga clic en **Guardar cambios**.

## 5 Especifique la configuración predeterminada de enrutamiento dinámico.

**Nota** Si ha configurado la VPN de IPsec en el entorno, no utilice el enrutamiento dinámico.

- a Seleccione un identificador de enrutador.  
Puede seleccionar un identificador de enrutador de la lista o utilizar el icono **+** para introducir uno nuevo. Este identificador de enrutador es la primera dirección IP de vínculo superior de la puerta de enlace Edge que inserta rutas en el kernel para el enrutamiento dinámico.
- b Configure el registro activando el botón de alternancia **Habilitar registro** y seleccionando el nivel de registro.
- c Haga clic en **Aceptar**.

## 6 Haga clic en **Guardar cambios**.

### Pasos siguientes

Agregue rutas estáticas. Consulte [Agregar una ruta estática](#).

Configure la redistribución de rutas. Consulte [Configurar redistribuciones de rutas](#).

Configure el enrutamiento dinámico. Consulte los siguientes temas:

- [Configurar un BGP](#)
- [Configurar OSPF](#)

## Agregar una ruta estática


Es posible agregar una ruta estática para un host o una subred de destino.

Si se habilita ECMP en la configuración de enrutamiento predeterminada, puede especificar varios saltos siguientes en las rutas estáticas. Consulte [Especificar la configuración de enrutamiento predeterminada de la puerta de enlace Edge](#) para conocer los pasos de habilitación de ECMP.

### Requisitos previos

Como se describe en la documentación de NSX, la dirección IP del siguiente salto de la ruta estática debe existir en una subred asociada con una de las interfaces de puerta de enlace Edge. De lo contrario, se produce un error en la configuración de esa ruta estática.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Enrutamiento > Rutas estáticas**.
- 3 Haga clic en el botón **Crear** ().

#### 4 Configure las siguientes opciones de la ruta estática:

Opción	Descripción
Red	Escriba la red con la notación de CIDR.
Siguiente salto	<p>Escriba la dirección IP del siguiente salto.</p> <p>La dirección IP del siguiente salto debe existir en una subred asociada con una de las interfaces de puerta de enlace Edge.</p> <p>Si se habilita ECMP, puede especificar varios saltos siguientes.</p>
MTU	<p>Edite el valor de transmisión máxima de los paquetes de datos.</p> <p>El valor de MTU no puede ser mayor que el que se ha configurado en la interfaz de puerta de enlace Edge seleccionada. Puede ver el valor de MTU configurado en la interfaz de puerta de enlace Edge de forma predeterminada en la pantalla Configuración de enrutamiento.</p>
Interfaz	Si lo desea, seleccione la interfaz de puerta de enlace Edge en la que quiere agregar una ruta estática. De forma predeterminada, se selecciona la interfaz que coincide con la dirección del siguiente salto.
Descripción	Si lo desea, escriba una descripción de la ruta estática.

#### 5 Haga clic en **Guardar cambios**.

##### Pasos siguientes

Configure una regla NAT para la ruta estática. Consulte [Agregar una regla SNAT o DNAT](#).

Agregue una regla de firewall para permitir que el tráfico recorra la ruta estática. Consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

## Configurar OSPF

Puede configurar el protocolo de enrutamiento de abrir primero la ruta más corta (Open Shortest Path First, OSPF) para las capacidades de enrutamiento dinámico de una puerta de enlace Edge. Una aplicación habitual de OSPF en una puerta de enlace Edge en un entorno de vCloud Director consiste en intercambiar información de enrutamiento entre puertas de enlace Edge en vCloud Director.

La puerta de enlace NSX Edge es compatible con OSPF, un protocolo de puerta de enlace interior que enruta los paquetes IP solo dentro de un único dominio de enrutamiento. Tal como se describe en la documentación de *administración de NSX*, la configuración de OSPF en una puerta de enlace NSX Edge permite que la puerta de enlace Edge aprenda y anuncie rutas. La puerta de enlace Edge utiliza OSPF para recopilar información de estado de vínculo de puertas de enlace Edge disponibles y crear un mapa de topología de la red. La topología determina la tabla de enrutamiento que se presenta a la capa de Internet, la cual toma decisiones de enrutamiento en función de la dirección IP de destino que se encuentra en los paquetes IP.



Por ello, las políticas de enrutamiento de OSPF ofrecen un proceso dinámico de equilibrio de carga del tráfico entre rutas de igual coste. Una red OSPF se divide en áreas de enrutamiento para optimizar el flujo de tráfico y limitar el tamaño de las tablas de enrutamiento. Un área es una recopilación lógica de redes OSPF, enrutadores y vínculos que tienen la misma identificación de área. Las áreas se identifican mediante un identificador de área.

### Requisitos previos


Debe configurarse un identificador de enrutador. [Especificar la configuración de enrutamiento predeterminada de la puerta de enlace Edge.](#)

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Enrutamiento > OSPF**.
- 3 Si OSPF no está habilitado, utilice el botón de alternancia **OSPF habilitado** para habilitarlo.
- 4 Configure las opciones de OSPF según las necesidades de su organización.

Opción	Descripción
Habilitar reinicio correcto	Especifica que el reenvío de paquetes no debe interrumpirse cuando se reinicien los servicios de OSPF.
Habilitar el origen predeterminado	Permite que la puerta de enlace Edge se anuncie como puerta de enlace predeterminada ante los elementos de mismo nivel de OSPF.


- 5 (opcional) Puede hacer clic en **Guardar cambios** o continuar con la configuración de definiciones de área y asignaciones de interfaces.

- 6 Para agregar una definición del área de OSPF, haga clic en el botón **Agregar** () , especifique los detalles de la asignación en el cuadro de diálogo y haga clic en **Conservar**.

**Nota** De forma predeterminada, el sistema configura un área NSSA (not-so-stubby area) con el identificador de área 51. Dicha área se muestra automáticamente en la tabla de definiciones de área en la pantalla OSPF. Puede modificar o eliminar el área NSSA.

Opción	Descripción
ID de área	Escriba un identificador de área con el formato de una dirección IP o un número decimal.
Tipo de área	<p>Seleccione <b>Normal</b> o <b>NSSA</b>.</p> <p>Las áreas NSSA impiden el desbordamiento de anuncios de estado de vínculo (Link-State Advertisement, LSA) ajenos al AS en áreas NSSA. Dependen del enrutamiento predeterminado a destinos externos. Por ello, las áreas NSSA deben ubicarse en el extremo de un dominio de enrutamiento de OSPF. Las áreas NSSA pueden importar rutas externas en el dominio de enrutamiento de OSPF, lo que proporciona un servicio de tránsito a dominios de enrutamiento pequeños que no forman parte del dominio de enrutamiento de OSPF.</p>
Autenticación de área	<p>Seleccione el tipo de autenticación que realizará OSPF en el nivel de área. En todas las puertas de enlace Edge dentro del área se debe configurar la misma autenticación y la contraseña correspondiente. Para que funcione la autenticación MD5, el transmisor y el receptor deben tener la misma clave de MD5.</p> <p>Las opciones son:</p> <ul style="list-style-type: none"> <li>■ <b>Ninguna</b> <p>No se requiere autenticación.</p> </li> <li>■ <b>Contraseña</b> <p>Con esta opción, la contraseña que se especifica en el campo <b>Valor de autenticación de área</b> se incluye en el paquete transmitido.</p> </li> <li>■ <b>MD5</b> <p>Con esta opción, la autenticación utiliza el cifrado MD5 (síntesis del mensaje de tipo 5). En el paquete transmitido se incluye una suma de comprobación de MD5. Escriba la clave de MD5 en el campo <b>Valor de autenticación de área</b>.</p> </li> </ul>

- 7 Haga clic en **Guardar cambios** para que las definiciones de área recién configuradas estén disponibles para seleccionarlas cuando se agreguen asignaciones de interfaz.

- 8 Para agregar una asignación de interfaz, haga clic en el botón **Agregar** () , especifique los detalles de la asignación en el cuadro de diálogo y haga clic en **Conservar**.

Con estas asignaciones, se pueden asignar interfaces de la puerta de enlace Edge a las áreas.

- En el cuadro de diálogo, seleccione la interfaz que desea asignar a una definición de área. La interfaz especifica la red externa a la que están conectadas las dos puertas de enlace Edge.
- Seleccione el identificador del área que se asignará a la interfaz seleccionada.
- (opcional) Cambie los valores predeterminados de la configuración de OSPF con el fin de personalizarlos para esta asignación de interfaz.

Al configurar una nueva asignación, se muestran los valores predeterminados de esta configuración. En la mayoría de los casos, se recomienda conservar la configuración predeterminada. Si cambia la configuración, asegúrese de que los elementos del mismo nivel de OSPF utilizan la misma configuración.

Opción	Descripción
Intervalo de saludo	Intervalo (en segundos) entre los paquetes de saludo que se envían en la interfaz.
Intervalo desactivado	Intervalo (en segundos) durante el cual se debe recibir al menos un paquete de saludo de un vecino antes de que dicho vecino se considere desactivado.
Prioridad	Prioridad de la interfaz. La interfaz con la prioridad más alta es el enrutador de la puerta de enlace Edge designada.
Coste	Sobrecarga requerida para enviar paquetes a través de esa interfaz. El coste de una interfaz es inversamente proporcional al ancho de banda de dicha interfaz. Cuanto mayor sea el ancho de banda, menor será el coste.

- Haga clic en **Conservar**.

- 9 Haga clic en **Guardar cambios** en la pantalla OSPF.

#### Pasos siguientes

Configure OSPF en las otras puertas de enlace Edge con las que desea intercambiar información de enrutamiento.

Agregue una regla de firewall que permita el tráfico entre las puertas de enlace Edge habilitadas para OSPF. Consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

Asegúrese de que la redistribución de rutas y la configuración de firewall permitan anunciar las rutas correctas. Consulte [Configurar redistribuciones de rutas](#).

## Configurar un BGP

Puede configurar un protocolo de puerta de enlace de borde (Border Gateway Protocol, BGP) para las capacidades de enrutamiento dinámico de una puerta de enlace Edge.

Tal como se describe en la *guía de administración de NSX*, BGP toma decisiones esenciales de enrutamiento mediante una tabla de prefijos o redes de IP que designan la disponibilidad de la red entre varios sistemas autónomos. En el campo de redes, el término orador de BGP hace referencia a un dispositivo de redes que ejecuta BGP. Dos oradores de BGP establecen una conexión antes de intercambiar cualquier información de enrutamiento. El término vecino de BGP hace referencia a un orador de BGP que ha establecido una conexión de este tipo. Tras establecer la conexión, los dispositivos intercambian rutas y sincronizan sus tablas. Cada dispositivo envía mensajes de conexión persistente para mantener activa esta relación.

## Procedimiento


- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Enrutamiento > BGP**.
- 3 Si BGP no está habilitado, utilice el botón de alternancia **Habilitar BGP** para habilitarlo.
- 4 Configure las opciones de BGP según las necesidades de su organización.

Opción	Descripción
<b>Habilitar reinicio correcto</b>	Especifica que el reenvío de paquetes no debe interrumpirse cuando se reinicien los servicios de BGP.
<b>Habilitar el origen predeterminado</b>	Permite que la puerta de enlace Edge se anuncie como puerta de enlace predeterminada ante los vecinos de BGP.
<b>AS local</b>	<p>Obligatorio. Especifique el número de identificador del sistema autónomo (Autonomous System, AS) que se usará para la función AS local del protocolo. El valor que especifique debe ser un número único global entre 1 y 65534.</p> <p>El AS local es una función de BGP. El sistema asigna el número de AS local a la puerta de enlace Edge que se va a configurar. La puerta de enlace Edge anuncia este identificador cuando la puerta de enlace Edge establece una relación de mismo nivel con los vecinos de BGP en otros sistemas autónomos. La ruta de acceso de los sistemas autónomos que atravesaría una ruta se utiliza como una métrica en el algoritmo de enrutamiento dinámico cuando se selecciona la mejor ruta de acceso a un destino.</p>

- 5 Puede hacer clic en **Guardar cambios** o continuar con la configuración de los vecinos de enrutamiento de BGP.

6 Para agregar una configuración de vecino de BGP, haga clic en el botón **Agregar**



() , especifique los detalles del vecino en el cuadro de diálogo y haga clic en **Conservar**.

Opción	Descripción
<b>Dirección IP</b>	Escriba la dirección IP de un vecino de BGP para esta puerta de enlace Edge.
<b>AS remoto</b>	Escriba un número único global entre 1 y 65534 para el sistema autónomo al que pertenece este vecino de BGP. Este número de AS remoto se utiliza en la entrada del vecino de BGP en la tabla de vecinos de BGP del sistema.
<b>Ponderación</b>	La ponderación predeterminada de la conexión de vecino. Ajuste este valor según las necesidades de la organización.
<b>Tiempo de conexión persistente</b>	La frecuencia con la que el software envía mensajes de conexión persistente al elemento de su mismo nivel. La frecuencia predeterminada es de 60 segundos. Ajuste los valores según las necesidades de su organización.
<b>Tiempo de espera de recuperación</b>	<p>El intervalo para el cual el software declara que un elemento de mismo nivel está inactivo tras no recibir ningún mensaje de conexión persistente. Este intervalo debe ser tres veces más grande el intervalo de conexión persistente. El intervalo predeterminado es de 180 segundos. Ajuste los valores según las necesidades de su organización.</p> <p>Una vez que se logra establecer una relación de mismo nivel entre dos vecinos de BGP, la puerta de enlace Edge inicia un temporizador de espera de recuperación. Cada mensaje de conexión persistente que recibe del vecino restablece el temporizador de espera de recuperación a 0. Si la puerta de enlace Edge no recibe tres mensajes de conexión persistente consecutivos, de modo que el temporizador de espera de recuperación llegue tres veces al intervalo de conexión persistente, la puerta de enlace Edge considera que el vecino está inactivo y elimina las rutas de este vecino.</p>
<b>Contraseña</b>	<p>Si este vecino de BGP requiere autenticación, escriba la contraseña de autenticación.</p> <p>Se comprobará cada segmento enviado en la conexión entre los vecinos. La autenticación MD5 debe configurarse con la misma contraseña en los dos vecinos de BGP; de lo contrario, no se establecerá la conexión entre ellos.</p>
<b>Filtros de BGP</b>	<p>Utilice esta tabla para especificar el filtrado de rutas mediante una lista de prefijos de este vecino de BGP.</p> <p><b>Precaución</b> Se aplica una regla bloquear todo al final de los filtros.</p> <p>Para agregar un filtro a la tabla, haga clic en el icono + y configure las opciones. Haga clic en <b>Conservar</b> para guardar cada filtro.</p> <ul style="list-style-type: none"> <li>■ Seleccione la dirección para indicar si se filtrará el tráfico que va hacia el vecino o que viene desde él.</li> <li>■ Seleccione la acción para indicar si permitirá o denegará el tráfico.</li> <li>■ Escriba la red que desea filtrar hacia el vecino o desde él. Escriba <b>ANY</b> o una red con formato CIDR.</li> <li>■ Escriba el <b>GE de prefijo de IP</b> y el <b>LE de prefijo de IP</b> para utilizar las palabras clave <b>le</b> y <b>ge</b> en la lista de prefijos de IP.</li> </ul>

7 Haga clic en **Guardar cambios** para guardar la configuración en el sistema.

## Pasos siguientes



Configure BGP en las otras puertas de enlace Edge con las que desea intercambiar información de enrutamiento.

Agregue una regla de firewall que permita el tráfico hacia las puertas de enlace Edge configuradas para BGP y desde estas. Para obtener información, consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

## Configurar redistribuciones de rutas

De forma predeterminada, el enrutador solo comparte rutas con otros enrutadores que ejecutan el mismo protocolo. Si tiene configurado un entorno con varios protocolos, deberá configurar la redistribución de rutas para permitir el uso compartido de rutas entre protocolos. Puede configurar la redistribución de rutas de una puerta de enlace Edge.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Enrutamiento > Redistribución de rutas**.
- 3 Utilice los botones de alternancia de protocolos para activar aquellos protocolos para los que desea habilitar la redistribución de rutas.
- 4 Agregue los prefijos de IP a la tabla que aparece en pantalla.
  - a Haga clic en el botón **Agregar** ().
  - b Escriba un nombre y la dirección IP de la red con formato CIDR.
  - c Haga clic en **Conservar**.
- 5 Para especificar los criterios de redistribución para cada prefijo de IP, haga clic en el botón **Agregar** () , especifique los criterios en el cuadro de diálogo y haga clic en **Conservar**.

Las entradas de la tabla se procesan de forma secuencial. Use las flechas arriba y abajo para ajustar la secuencia.

Opción	Descripción
Nombre del prefijo	Seleccione un prefijo de IP específico al que aplicar estos criterios o seleccione <b>Cualquiera</b> para aplicar los criterios a todas las rutas de red.
Protocolo de aprendiz	Seleccione el protocolo que va a aprender rutas de otros protocolos en este criterio de redistribución.

Opción	Descripción
Permitir el aprendizaje desde	Seleccione los tipos de redes desde los que se pueden aprender rutas para el protocolo seleccionado en la lista <b>Protocolo de aprendiz.</b>
Acción	Seleccione si desea permitir o denegar la redistribución de los tipos de redes seleccionados.

6 Haga clic en **Guardar cambios.**

## Equilibrio de carga

El equilibrador de carga distribuye las solicitudes de servicio entrantes entre varios servidores de manera que la distribución de la carga sea transparente para los usuarios. El equilibrio de carga permite lograr un uso óptimo de los recursos, lo que maximiza el rendimiento, minimiza el tiempo de respuesta y permite evitar sobrecargas.

### Acerca del equilibrio de carga

El equilibrador de carga NSX es compatible con dos motores de equilibrio de carga. El equilibrador de carga de 4 capas está basado en paquetes y proporciona un procesamiento de rutas de acceso rápidas. El equilibrador de carga de 7 capas se basa en sockets, y es compatible con las estrategias de administración de tráfico avanzadas y la mitigación de DDOS para los servicios back-end.

El equilibrio de carga para una puerta de enlace Edge se configura en la interfaz externa debido a que la carga de la puerta de enlace Edge equilibra el tráfico entrante de la red externa. Al configurar servidores virtuales para el equilibrio de carga, especifique una de las direcciones IP disponibles en el VDC de organización. Consulte la *Guía del usuario de vCloud Director*.

### Conceptos y estrategias de equilibrio de carga

Una estrategia de equilibrio de carga basado en paquetes se implementa en la capa de TCP y UDP. El equilibrio de carga basado en paquetes no detiene la conexión ni regula la solicitud completa. En lugar de eso, tras manipular el paquete, lo envía directamente al servidor seleccionado. Se mantienen las sesiones de TCP y UDP en el equilibrador de carga para que los paquetes de una sola sesión se dirijan al mismo servidor. Puede seleccionar Aceleración habilitada en la configuración global y la configuración de los servidores virtuales relevantes para habilitar el equilibrio de carga basado en paquetes.

Una estrategia de equilibrio de carga basado en sockets se implementa por encima de la interfaz de sockets. Se establecen dos conexiones para una sola solicitud: una conexión orientada al cliente y una conexión orientada al servidor. La conexión orientada al servidor se establece después de la selección del servidor. Para la implementación basada en sockets de HTTP, se recibe la solicitud completa antes de enviarla al servidor seleccionado con manipulación de 7

capas opcional. Para la implementación basada en sockets HTTPS, se intercambia la información de autenticación en la conexión orientada al cliente o la conexión orientada al servidor. El equilibrio de carga basado en sockets es el modo predeterminado para los servidores virtuales TCP, HTTP y HTTPS.

Los conceptos clave para el equilibrador de carga NSX son: servidor virtual, grupo de servidores, miembro de grupo de servidores y supervisión de servicio.

### **Servidor virtual**

Resumen de un servicio de aplicación, representado por una combinación única de IP, puerto, protocolos y perfil de aplicación, como TCP o UDP.

### **Grupo de servidores**

Grupo de servidores back-end.

### **Miembro de grupo de servidores**

El servidor back-end representado como miembro de un grupo.

### **Supervisión de servicio**

Definición de la forma de comprobar el estado de mantenimiento de un servidor back-end.

### **Perfil de aplicación**

Representación de la configuración de TCP, UDP, persistencia y certificación para una determinada aplicación.

## **Información general de configuración**

Para comenzar, configure las opciones globales para el equilibrador de carga. Ahora, cree un grupo de servidores compuesto por miembros de servidores back-end y asocie una supervisión de servicio al grupo para administrar y compartir los servidores back-end de forma eficiente.

A continuación, cree un perfil de aplicación para definir el comportamiento común de las aplicaciones en un equilibrador de carga, como el cliente SSL, el servidor SSL, el encabezado X-Forwarded-For o la persistencia. La persistencia envía solicitudes posteriores con características similares, como que la cookie o la dirección IP de origen envíen al mismo miembro de grupo, sin ejecutar el algoritmo de equilibrio de carga. Se puede reutilizar el perfil de aplicación en los servidores virtuales.

Cree una regla de aplicación opcional para configurar los ajustes específicos de la aplicación para la manipulación del tráfico, como la coincidencia de cierta dirección URL o nombre de host para que diferentes grupos puedan gestionar diferentes solicitudes. A continuación, cree una supervisión de servicio específica para la aplicación o utilice una supervisión de servicio existente que cumpla con sus necesidades.



Opcionalmente, puede crear una regla de aplicación para admitir la funcionalidad avanzada de servidores virtuales de 7 capas. Algunos escenarios de uso para reglas de aplicación incluyen la conmutación de contenido, la manipulación de encabezados, las reglas de seguridad y la protección de DOS.

Por último, cree un servidor virtual que conecte el grupo de servidores, el perfil de aplicación y cualquier posible regla de aplicación.

Cuando el servidor virtual recibe una solicitud, el algoritmo de equilibrio de carga tiene en cuenta la configuración del miembro de grupo y el estado de tiempo de ejecución. El algoritmo calcula el grupo apropiado para distribuir el tráfico compuesto por uno o varios miembros. La configuración del miembro de grupo incluye opciones como ponderación, conexión máxima y estado de condición. El estado de tiempo de ejecución incluye las conexiones actuales, el tiempo de respuesta y la información de comprobación de estado. Los métodos de cálculo pueden ser por turnos, por turnos ponderado, mínimo conectado, hash de IP de origen, mínimo conectado ponderado, URL, URI o encabezado HTTP.

Cada grupo se supervisa con la supervisión de servicio asociada. Cuando el equilibrador de carga detecta un problema con un miembro del grupo, el miembro se marca como INACTIVO. Solo se selecciona un servidor ACTIVO cuando se elige un miembro del grupo de servidores. Si no se configura una supervisión de servicio para el grupo de servidores, todos los miembros del grupo se consideran ACTIVOS.

## Configurar el servicio de equilibrador de carga

Los parámetros de configuración global del equilibrador de carga incluyen la habilitación general, la selección del motor de 4 capas o 7 capas, y la especificación de los tipos de eventos que se registrarán.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Equilibrador de carga > Configuración global**.

### 3 Seleccione las opciones que desea habilitar:

Opción	Acción
Estado	<p>Haga clic en el icono de alternancia para habilitar el equilibrador de carga. Habilite <b>Aceleración habilitada</b> para configurar el equilibrador de carga de modo que utilice el motor de capa 4 (el cual es más rápido) en lugar del motor de capa 7. La VIP de TCP de 4 capas se procesa antes que el firewall de puerta de enlace Edge, por lo que no se necesita ninguna regla para permitir el firewall.</p> <hr/> <p><b>Nota</b> Las VIP de capa 7 para HTTP y HTTPS se procesan después del firewall, de modo que, cuando no se habilita la aceleración, debe haber una regla de firewall de puerta de enlace Edge para permitir el acceso a la VIP de capa 7 para dichos protocolos. Cuando se habilita la aceleración y el grupo de servidores está en un modo no transparente, se agrega una regla SNAT, por lo que debe asegurarse de que el firewall esté habilitado en la puerta de enlace Edge.</p>
Habilitar registro	Habilite el registro para que el equilibrador de carga de la puerta de enlace Edge recopile logs de tráfico.
Nivel de registro	Elija la gravedad de los eventos que se recopilarán en los logs.

### 4 Haga clic en **Guardar cambios**.

La operación para guardar puede tardar un minuto en completarse.

#### Pasos siguientes

Configure perfiles de aplicación para el equilibrador de carga. Consulte [Crear un perfil de aplicación](#).


### Crear un perfil de aplicación

Un perfil de aplicación define el comportamiento del equilibrador de carga para un tipo determinado de tráfico de red. Tras configurar un perfil, este se asocia a un servidor virtual. A continuación, el servidor virtual procesa el tráfico según los valores especificados en el perfil. El uso de perfiles mejora el control de la administración del tráfico de red y hace que las tareas de administración de tráfico sean más sencillas y eficientes.

Al crear un perfil para el tráfico HTTPS, se permiten los siguientes patrones de tráfico HTTPS:

- Cliente -> HTTPS -> LB (finalizar SSL) -> HTTP -> servidores
- Cliente -> HTTPS -> LB (finalizar SSL) -> HTTPS -> servidores
- Cliente -> HTTPS -> LB (acceso directo SSL) -> HTTPS -> servidores
- Cliente -> HTTP -> LB -> HTTP -> servidores

## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Equilibrador de carga > Perfiles de aplicación**.
- 3 Haga clic en el botón **Crear** ().
- 4 Escriba un nombre para el perfil.
- 5 Configure el perfil de aplicación.

Opción	Descripción
<b>Tipo</b>	<p>Seleccione el tipo de protocolo usado para enviar solicitudes al servidor. La lista de parámetros obligatorios depende del protocolo seleccionado. No se pueden introducir parámetros que no sean aplicables para el protocolo seleccionado. Todos los demás parámetros son obligatorios.</p>
<b>Habilitar acceso directo SSL</b>	<p>Haga clic aquí para habilitar la autenticación SSL que se transferirá al servidor virtual.</p> <p>De lo contrario, la autenticación SSL se realizará en la dirección de destino.</p>
<b>URL de redirección HTTP</b>	<p>(HTTP y HTTPS) Introduzca la dirección URL a la que debe redirigirse el tráfico que llega a la dirección de destino.</p>

Opción	Descripción
Persistencia	<p>Especifique un mecanismo de persistencia para el perfil.</p> <p>La persistencia realiza el seguimiento de los datos de sesión y los almacena. Estos datos pueden ser, por ejemplo, el miembro de grupo específico que ha procesado una solicitud de cliente. Esto garantiza que las solicitudes de cliente se dirijan al mismo miembro de grupo durante toda una sesión o las sesiones posteriores. Las opciones son las siguientes:</p> <ul style="list-style-type: none"> <li>■ <b>IP de origen</b> <p>La persistencia de IP de origen realiza un seguimiento de las sesiones en función de la dirección IP de origen. Cuando un cliente solicita una conexión a un servidor virtual que admite la persistencia de afinidad de dirección de origen, el equilibrador de carga comprueba si ese cliente se ha conectado anteriormente y, si es así, devuelve el cliente al mismo miembro de grupo.</p> </li> <li>■ <b>MSRDP</b> <p>Solo TCP: la persistencia del protocolo de escritorio remoto de Microsoft (Microsoft Remote Desktop Protocol, MSRDP) mantiene sesiones persistentes entre clientes y servidores de Windows que ejecutan el servicio de protocolo de escritorio remoto (Remote Desktop Protocol, RDP) de Microsoft. El escenario recomendado para habilitar la persistencia de MSRDP consiste en crear un grupo de equilibrio de carga que conste de miembros que ejecuten un sistema operativo invitado de Windows Server, en el que todos los miembros pertenezcan a un clúster de Windows y participen en un directorio de sesión de Windows.</p> </li> <li>■ <b>ID de sesión SSL</b> <p>La persistencia del ID de sesión SSL está disponible cuando se habilita el acceso directo a SSL. La persistencia del ID de sesión SSL garantiza que las conexiones repetidas del mismo cliente se envíen al mismo servidor. La persistencia del ID de sesión permite el uso de la reanudación de la sesión SSL, lo que ahorra tiempo de procesamiento tanto para el cliente como para el servidor.</p> </li> </ul>
Nombre de cookie	<p>(HTTP y HTTPS) Si ha especificado <b>Cookie</b> como el mecanismo de persistencia, introduzca el nombre de la cookie. La persistencia de cookie usa una cookie para identificar de manera exclusiva la sesión la primera vez que un cliente accede al sitio. El equilibrador de carga hace referencia a esta cookie cuando conecta solicitudes posteriores en la sesión, de modo que todas van al mismo servidor virtual.</p>

Opción	Descripción
Modo	<p>Seleccione el modo mediante el cual debe insertarse la cookie. Se admiten los siguientes modos:</p> <ul style="list-style-type: none"> <li>■ <b>Insertar</b> <p>La puerta de enlace Edge envía una cookie. Cuando el servidor envía una o varias cookies, el cliente recibe una cookie adicional (las cookies del servidor más la cookie de la puerta de enlace Edge). Cuando el servidor no envía ninguna cookie, el cliente recibe únicamente la cookie de la puerta de enlace Edge.</p> </li> <li>■ <b>Prefijo</b> <p>Seleccione esta opción cuando el cliente no admite más de una cookie.</p> <p><b>Nota</b> Todos los navegadores aceptan varias cookies. No obstante, puede que una aplicación privada utilice un cliente privado que solo admita una cookie. El servidor web envía la cookie como de costumbre. La puerta de enlace Edge inserta (como un prefijo) la información de cookie en el valor de cookie del servidor. Esta información de cookie adicional se quita cuando la puerta de enlace Edge la envía al servidor.</p> </li> <li>■ <b>Sesión de app</b> Para esta opción, el servidor no envía una cookie. En su lugar, envía la información de la sesión del usuario como una URL. Por ejemplo, <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code>, donde <code>jsessionid</code> es la información de sesión del usuario y se utiliza para la persistencia. No es posible ver la tabla de persistencia de Sesión de aplicación para solucionar problemas.</li> </ul>
Caduca en (segundos)	<p>Escriba un período de tiempo en segundos durante el que la persistencia permanece en vigor. Debe ser un número entero positivo entre 1 y 86400.</p> <p><b>Nota</b> Para el equilibrio de carga de 7 capas mediante la persistencia de IP de origen de TCP, se agota el tiempo de espera de la entrada de persistencia si no se establecen nuevas conexiones TCP durante un período de tiempo, incluso si las conexiones existentes aún están activas.</p>
Insertar encabezado HTTP X-Forwarded-For	<p>HTTP y HTTPS: seleccione <b>Insertar encabezado HTTP X-Forwarded-For</b> para identificar la dirección IP de origen de un cliente que se conecta a un servidor web mediante el equilibrador de carga.</p>
Habilitar SSL del lado de grupo	<p>Solo HTTPS: seleccione <b>Habilitar SSL del lado de grupo</b> para definir el certificado, las CA o las CRL utilizados para autenticar el equilibrador de carga del lado de servidor en la pestaña Certificados del grupo.</p>

- 6 Solo HTTPS: configure los certificados que se utilizarán con el perfil de aplicación. Si no existen los certificados que necesita, puede crearlos en la pestaña **Certificados**.

Opción	Descripción
<b>Certificados del servidor virtual</b>	Seleccione el certificado, las CA o las CRL utilizadas para descifrar el tráfico HTTPS.
<b>Certificados del grupo</b>	Defina el certificado, las CA o las CRL utilizadas para autenticar el equilibrador de carga del lado servidor.  <b>Nota</b> Seleccione <b>Habilitar SSL del lado de grupo</b> para habilitar esta pestaña.
<b>Cifrado</b>	Seleccione los algoritmos de cifrado (o conjunto de cifrado) que se han negociado durante el protocolo de enlace SSL/TLS.
<b>Autenticación de cliente</b>	Especifique si la autenticación de cliente se ignorará o será obligatoria.  <b>Nota</b> Si se establece como <b>obligatoria</b> , el cliente debe proporcionar un certificado después de la solicitud o, de lo contrario, se cancelará el protocolo de enlace.

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

La operación puede tardar un minuto en completarse.


#### Pasos siguientes

Agregue supervisiones del servicio para que el equilibrador de carga defina las comprobaciones de estado para distintos tipos de tráfico de red. Consulte [Crear una supervisión del servicio](#).

### Crear una supervisión del servicio

Las supervisiones del servicio se crean para definir los parámetros de comprobación de estado de un tipo determinado de tráfico de red. Cuando se asocia una supervisión del servicio a un grupo, se supervisan los miembros del grupo según los parámetros de la supervisión de servicio.

#### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Equilibrador de carga > Supervisión del servicio**.
- 3 Haga clic en el botón **Crear** ().
- 4 Introduzca un nombre para la supervisión del servicio.

5 (opcional) Configure las siguientes opciones para la supervisión del servicio:

Opción	Descripción
Intervalo	Introduzca el intervalo en el que se supervisará un servidor mediante el valor de <b>Método</b> especificado.
Tiempo de espera	Introduzca el tiempo máximo en segundos durante el cual debe recibirse una respuesta del servidor.
Máximo de reintentos	Introduzca el número de veces que el valor de <b>Método</b> de supervisión especificado debe fallar de forma secuencial para que el servidor se considere inactivo.
Tipo	<p>Seleccione la manera en la que desea enviar la solicitud de comprobación de estado al servidor: HTTP, HTTPS, TCP, ICMP o UDP.</p> <p>En función del tipo seleccionado, las opciones restantes del cuadro de diálogo <b>Nueva supervisión del servicio</b> estarán habilitadas o deshabilitadas.</p>
Esperado	(HTTP y HTTPS) Introduzca la cadena que la supervisión espera hacer coincidir en la línea de estado de la respuesta HTTP o HTTPS (por ejemplo, HTTP/1.1).
Método	HTTP y HTTPS: seleccione el método que se utilizará para detectar el estado del servidor.
URL	<p>(HTTP y HTTPS) Introduzca la dirección URL que se utilizará en la solicitud de estado del servidor.</p> <p><b>Nota</b> Cuando se selecciona el método POST, debe especificar un valor para <b>Enviar</b>.</p>
Enviar	(HTTP, HTTPS y UDP) Introduzca los datos que se enviarán.
Recibir	<p>(HTTP, HTTPS y UDP) Introduzca la cadena que se buscará en el contenido de la respuesta para hacerla coincidir.</p> <p><b>Nota</b> Cuando <b>Esperado</b> no coincide, la supervisión no intenta hacer coincidir el contenido de <b>Recibir</b>.</p>
Extensión	<p>(TODO) Introduzca parámetros de supervisión avanzados como pares con el formato clave=valor. Por ejemplo, warning=10 indica que, cuando un servidor no responde en un intervalo de 10 segundos, su estado se establece como warning. Todos los elementos de extensión deben separarse con un carácter de retorno de carro. Por ejemplo:</p> <pre>&lt;extension&gt;delay=2 critical=3 escape&lt;/extension&gt;</pre>

6 Haga clic en **Conservar** para guardar los cambios.

La operación puede tardar un minuto en completarse.

## Ejemplo: Extensiones admitidas para cada protocolo

Tabla 6-1. Extensiones para los protocolos HTTP/HTTPS

Extensión de supervisión	Descripción
no-body	No espera un cuerpo de documento y detiene la lectura después del encabezado HTTP/HTTPS.  <b>Nota</b> Aún se envía HTTP GET o HTTP POST, pero no un método HEAD.
max-age= <i>SECONDS</i>	Advierte cuando un documento tiene una antigüedad superior a la cantidad de segundos indicada por <i>SECONDS</i> . El número puede tener el formato 10m para minutos, 10h para horas o 10d para días.
content-type= <i>STRING</i>	Especifica un tipo de medios para el encabezado Content-Type en las llamadas POST.
linespan	Permite que la expresión regular abarque líneas nuevas (debe preceder a -r o -R).
regex= <i>STRING</i> o ereg= <i>STRING</i>	Busca en la página una expresión regular que reemplaza a <i>STRING</i> en el ejemplo.
eregi= <i>STRING</i>	Busca en la página una expresión regular que no distingue mayúsculas de minúsculas que reemplaza a <i>STRING</i> en el ejemplo.
invert-regex	Devuelve CRITICAL cuando lo encuentra y OK cuando no lo encuentra.
proxy-authorization= <i>AUTH_PAIR</i>	Especifica el par nombre de usuario:contraseña en servidores proxy con autenticación básica.
useragent= <i>STRING</i>	Envía la cadena en el encabezado HTTP como User Agent.
header= <i>STRING</i>	Envía cualquier otra etiqueta en el encabezado HTTP. Utilícelo varias veces para encabezados adicionales.
onredirect=ok warning critical follow sticky stickyport	Indica cómo controlar páginas redirigidas. <i>sticky</i> es similar a <i>follow</i> , pero se queda con la dirección IP especificada. <i>stickyport</i> garantiza que el puerto permanezca igual.
pagesize= <i>INTEGER:INTEGER</i>	Especifica los tamaños de página máximo y mínimo necesarios en bytes.
warning=DOUBLE	Especifica el tiempo de respuesta en segundos que produce un estado de advertencia.
critical=DOUBLE	Especifica el tiempo de respuesta en segundos que produce un estado crítico.



**Tabla 6-2. Extensiones exclusivas para protocolo HTTPS**

Extensión de supervisión	Descripción
sni	Habilita la compatibilidad de extensión de nombre de host SSL/TLS (SNI).
certificate=INTEGER	Especifica el número mínimo de días que un certificado debe ser válido. El puerto predeterminado es 443. Cuando se utiliza esta opción, no se comprueba la dirección URL.
authorization=AUTH_PAIR	Especifica el par nombre de usuario:contraseña en sitios con autenticación básica.

**Tabla 6-3. Extensiones para protocolo TCP**

Extensión de supervisión	Descripción
escape	Permite el uso de \n, \r, \t o \ en una cadena send o quit. Debe aparecer antes de la opción send o quit. De forma predeterminada, no se agrega nada a send y se agrega \r\n al final de quit.
all	Especifica que todas las cadenas que se esperan deben estar presentes en una respuesta del servidor. De forma predeterminada, se utiliza any.
quit=STRING	Envía una cadena al servidor para cerrar la conexión correctamente.
refuse=ok warn crit	Acepta rechazos de TCP con los estados ok, warn o crit. De forma predeterminada, utiliza el estado crit.
mismatch=ok warn crit	Acepta faltas de coincidencia de la cadena esperada con los estados ok, warn o crit. De forma predeterminada, utiliza el estado warn.
jail	Oculto los resultados del socket TCP.
maxbytes=INTEGER	Cierra la conexión cuando se recibe una cantidad de bytes superior a la especificada.
delay=INTEGER	Espera el número de segundos especificado entre el envío de la cadena y el sondeo de una respuesta.
certificate=INTEGER[,INTEGER]	Especifica el número mínimo de días que un certificado debe ser válido. El primer valor es #days para la advertencia y el segundo valor es critical (si no se especifica: 0).
ssl	Usa SSL para la conexión.
warning=DOUBLE	Especifica el tiempo de respuesta en segundos que produce un estado de advertencia.
critical=DOUBLE	Especifica el tiempo de respuesta en segundos que produce un estado crítico.


## Pasos siguientes

Agregue grupos de servidores para el equilibrador de carga. Consulte [Agregar un grupo de servidores para el equilibrio de carga](#).

## Agregar un grupo de servidores para el equilibrio de carga

Puede añadir un grupo de servidores para gestionar y compartir servidores back-end de forma flexible y eficiente. Un grupo gestiona métodos de distribución de equilibrador de carga y está asociado a la supervisión del servicio para parámetros de comprobación de estado.


### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Equilibrador de carga > Grupos**.
- 3 Haga clic en el botón **Crear** ().
- 4 Escriba un nombre y, si lo desea, una descripción del grupo de equilibradores de carga.
- 5 Seleccione un método de equilibrio para el servicio en el menú desplegable **Algoritmo**:

Opción	Descripción
<b>ROUND-ROBIN</b>	Cada servidor se utiliza por turnos en función de la ponderación que tenga asignada. Es el algoritmo más uniforme y justo cuando el tiempo de proceso del servidor permanece distribuido de forma equitativa.
<b>IP-HASH</b>	Selecciona un servidor en función de un hash de la dirección IP de origen y de destino de cada paquete.
<b>LEASTCONN</b>	Distribuye las solicitudes del cliente a varios servidores en función del número de conexiones que ya están abiertas en el servidor. Las nuevas conexiones se envían al servidor que tenga el menor número de conexiones abiertas.
<b>URI</b>	Se hace hash de la parte izquierda del URI (delante del signo de interrogación) y se divide por la ponderación total de los servidores en ejecución. El resultado designa el servidor que recibirá la solicitud. Esta opción garantiza que siempre se dirija un URI al mismo servidor mientras que este no se desactive.

Opción	Descripción
HTTPHEADER	El nombre del encabezado HTTP se busca en cada solicitud HTTP. El nombre del encabezado entre paréntesis no distingue mayúsculas de minúsculas, lo que es similar a la función ACL 'hdr()'. Si el encabezado está ausente o no contiene ningún valor, se aplica el algoritmo por turnos. El parámetro del algoritmo HTTP HEADER tiene una opción <code>headerName=&lt;name&gt;</code> . Por ejemplo, puede utilizar <code>host</code> como el parámetro del algoritmo HTTP HEADER.
URL	El parámetro de URL especificado en el argumento se busca en la cadena de consulta de cada solicitud HTTP GET. Si al parámetro le sigue un signo igual (=) y un valor, al valor se le aplica hash y se divide por el peso total de los servidores en ejecución. El resultado determina el servidor que recibe la solicitud. Este proceso se utiliza para realizar un seguimiento de los identificadores de usuario de las solicitudes y asegurarse de que el mismo identificador de usuario se envíe siempre al mismo servidor, siempre que ningún servidor se active o desactive. Si no se encuentra ningún parámetro ni ningún valor, se aplica un algoritmo por turnos. El parámetro del algoritmo URL tiene una opción <code>urlParam=&lt;url&gt;</code> .

## 6 Agregue miembros al grupo.

- a Haga clic en el botón **Agregar** ().
  - b Introduzca el nombre del miembro de grupo.
  - c Introduzca la dirección IP del miembro de grupo.
  - d Introduzca el puerto en el que el miembro recibirá el tráfico desde el equilibrador de carga.
  - e Introduzca el puerto de supervisión en el que el miembro recibirá las solicitudes de supervisión de estado.
  - f En el cuadro de texto **Ponderación**, escriba la proporción de tráfico que gestionará este miembro. Debe ser un número entero entre 1 y 256.
  - g (opcional) En el cuadro de texto **Conexiones máximas**, escriba el número máximo de conexiones simultáneas que el miembro podrá gestionar.  
  
Cuando el número de solicitudes entrantes supera el valor máximo, las solicitudes se colocan en cola y el equilibrador de carga espera hasta que se libere una conexión.
  - h (opcional) En el cuadro de texto **Conexiones mínimas**, escriba el número mínimo de conexiones simultáneas que un miembro siempre debe aceptar.
  - i Haga clic en **Conservar** para agregar el nuevo miembro al grupo.
- La operación puede tardar un minuto en completarse.

- 7 (opcional) A fin de lograr que las direcciones IP de cliente sean visibles para los servidores back-end, seleccione **Transparente**.

Si no se selecciona **Transparente** (el valor predeterminado), los servidores back-end ven la dirección IP del origen del tráfico como la dirección IP interna del equilibrador de carga.

Cuando **Transparente** está seleccionado, la dirección IP de origen es la dirección IP real del cliente y la puerta de enlace Edge se debe establecer como la puerta de enlace predeterminada para garantizar que los paquetes devueltos pasen por la puerta de enlace Edge.

- 8 Haga clic en **Conservar** para guardar los cambios.

La operación puede tardar un minuto en completarse.


#### Pasos siguientes

Agregue servidores virtuales para el equilibrador de carga. Un servidor virtual tiene una dirección IP pública y atiende todas las solicitudes entrantes del cliente. Consulte [Agregar un servidor virtual](#).

## Agregar una regla de aplicación

Puede escribir una regla de aplicación para manipular y gestionar directamente el tráfico de aplicación de IP.

#### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Equilibrador de carga > Reglas de aplicación**.
- 3 Haga clic en el botón **Agregar** (.
- 4 Introduzca el nombre de la regla de aplicación.
- 5 Introduzca el script de la regla de aplicación.

Para obtener información sobre la sintaxis de las reglas de aplicación, consulte <http://cbonte.github.io/haproxy-dconv/configuration-1.5.html>.
- 6 Haga clic en **Conservar** para guardar los cambios.

La operación puede tardar un minuto en completarse.

#### Pasos siguientes


Asocie la nueva regla de aplicación con un servidor virtual agregado para el equilibrador de carga. Consulte [Agregar un servidor virtual](#).

## Agregar un servidor virtual

Agregue una puerta de enlace Edge interna o una interfaz de vínculo superior como un servidor virtual. Un servidor virtual tiene una dirección IP pública y atiende todas las solicitudes entrantes del cliente.

De forma predeterminada, el equilibrador de carga cierra la conexión TCP del servidor después de cada solicitud de cliente.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **Equilibrador de carga > Servidores virtuales**.
- 3 Haga clic en el botón **Agregar** ().
- 4 En la pestaña **General**, configure las siguientes opciones del servidor virtual:

Opción	Descripción
Habilitar servidor virtual	Haga clic aquí para habilitar el servidor virtual.
Habilitar aceleración	Haga clic aquí para habilitar la aceleración.
Perfil de aplicación	Seleccione un perfil de aplicación para asociarlo con el servidor virtual.
Nombre	Escriba un nombre para el servidor virtual.
Descripción	Escriba una descripción opcional del servidor virtual.
Dirección IP	Escriba o examine para seleccionar la dirección IP en la que el equilibrador de carga realiza la escucha.
Protocolo	Seleccione el protocolo que acepta el servidor virtual. Debe seleccionar el mismo protocolo que utiliza el <b>Perfil de aplicación</b> seleccionado.
Puerto	Escriba el número de puerto en el que el equilibrador de carga realiza la escucha.
Grupo predeterminado	Elija el grupo de servidores que va a utilizar el equilibrador de carga.
Límite de conexiones	(Opcional) Escriba el número máximo de conexiones simultáneas que puede procesar el servidor virtual.
Límite de velocidad de conexión (CPS)	(Opcional) Escriba el número máximo de nuevas solicitudes de conexión entrantes por segundo.

- 5 (opcional) Para asociar reglas de aplicación con el servidor virtual, haga clic en la pestaña **Avanzado** y realice los pasos siguientes:

- a Haga clic en el botón **Agregar** ()

Aparecen las reglas de aplicación creadas para el equilibrador de carga. Si es necesario, agregue reglas de aplicación para el equilibrador de carga. Consulte [Agregar una regla de aplicación](#).

- 6 Haga clic en **Conservar** para guardar los cambios.

La operación puede tardar un minuto en completarse.

#### Pasos siguientes

Cree una regla de firewall de puerta de enlace Edge para permitir el tráfico hacia el nuevo servidor virtual (la dirección IP de destino). Consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

## Acceso seguro mediante redes privadas virtuales

Es posible configurar las capacidades de VPN que proporciona el software NSX para las puertas de enlace Edge. Puede configurar conexiones de VPN con el centro de datos virtual de organización mediante un túnel VPN-Plus de SSL, un túnel VPN de IPsec o un túnel VPN de 2 capas.

Tal como se describe en la *guía de administración de NSX*, la puerta de enlace NSX Edge es compatible con estos servicios VPN:

- VPN-Plus de SSL, que permite a los usuarios remotos acceder a aplicaciones empresariales privadas.
- VPN de IPsec, que ofrece conectividad de sitio a sitio entre una puerta de enlace NSX Edge y sitios remotos que también tienen NSX, o bien que tienen enrutadores de hardware de terceros o puertas de enlace VPN.
- VPN de 2 capas, que posibilita la extensión del centro de datos virtual de organización al permitir que las máquinas virtuales conserven la conectividad de red sin necesidad de cambiar la dirección IP de una ubicación geográfica a otra.

En un entorno de vCloud Director, puede crear túneles VPN entre los siguientes elementos:

- Redes de centros de datos virtuales de organización en la misma organización
- Redes de centros de datos virtuales de organización en diferentes organizaciones
- Una red de centros de datos virtuales de organización y una red externa

---

**Nota** vCloud Director no admite varios túneles VPN entre dos puertas de enlace Edge idénticas. Si hay un túnel entre dos puertas de enlace Edge y desea añadir otra subred al túnel, elimine el túnel VPN existente y cree otro que incluya la nueva subred.

---

Después de configurar los túneles VPN de una puerta de enlace Edge, puede utilizar un cliente VPN de una ubicación remota para conectarse al centro de datos virtual de organización respaldado por esa puerta de enlace Edge.

## Configurar VPN-Plus de SSL

Los servicios VPN-Plus de SSL para una puerta de enlace Edge en el entorno de vCloud Director permiten que los usuarios remotos se conecten de forma segura a las aplicaciones y las redes privadas de los centros de datos virtuales de organización respaldados por esa puerta de enlace Edge. Es posible configurar varios servicios VPN-Plus de SSL en la puerta de enlace Edge.

En el entorno vCloud Director, la capacidad VPN-Plus de SSL de la puerta de enlace Edge es compatible con el modo de acceso a la red. Los usuarios remotos deben instalar un cliente SSL para establecer conexiones seguras y tener acceso a las redes y las aplicaciones detrás de la puerta de enlace Edge. Como parte de la configuración de VPN-Plus de SSL de la puerta de enlace Edge, debe agregar los paquetes de instalación para el sistema operativo y configurar determinados parámetros. Consulte [Agregar un paquete de instalación del cliente VPN-Plus de SSL](#) para obtener más detalles.

La configuración de VPN-Plus de SSL en una puerta de enlace Edge es un proceso de varios pasos.

### Requisitos previos

Compruebe que todos los certificados SSL necesarios para VPN-Plus de SSL se agregaron a la pantalla **Certificados**. Consulte [Administración de certificados SSL](#).

---

**Nota** En una puerta de enlace Edge, el puerto 443 es el puerto predeterminado de HTTPS. Para la funcionalidad VPN de SSL, debe ser posible acceder al puerto HTTPS de la puerta de enlace Edge desde redes externas. El cliente VPN de SSL requiere que sea posible acceder desde el sistema cliente al puerto y a la dirección IP de la puerta de enlace Edge configurados en la pestaña **VPN-Plus de SSL** de la pantalla Configuración del servidor. Consulte [Configurar ajustes de un servidor VPN de SSL](#).

---

### Procedimiento

#### 1 [Desplazarse a la pantalla VPN-Plus de SSL](#)

Es posible desplazarse hasta la pantalla VPN-Plus de SSL para comenzar a configurar el servicio VPN-Plus de SSL para una puerta de enlace Edge.

#### 2 [Configurar ajustes de un servidor VPN de SSL](#)

Esta configuración de servidor permite determinar los ajustes para el servidor VPN de SSL, como la dirección IP y el puerto de escucha para el servicio, la lista de cifrado del servicio y su certificado de servicio. Al conectarse a la puerta de enlace Edge, los usuarios remotos especifican la misma dirección IP y el puerto que se establecieron en esta configuración de servidor.

### 3 Crear un grupo de direcciones IP para usarlo con VPN-Plus de SSL en una puerta de enlace Edge

Se asignan direcciones IP virtuales a los usuarios remotos desde los grupos de direcciones IP estáticas que se configuran en la pantalla **Grupos de direcciones IP** de la pestaña **VPN-Plus de SSL**.

### 4 Agregar una red privada para usarla con VPN-Plus de SSL en una puerta de enlace Edge

Utilice la pantalla Redes privadas de la pestaña **VPN-Plus de SSL** para configurar las redes privadas. Las redes privadas son las recomendadas para el acceso de los clientes VPN, cuando los usuarios remotos se conectan mediante sus clientes VPN y el túnel VPN de SSL. Las redes privadas habilitadas se instalan en la tabla de enrutamiento del cliente VPN.

### 5 Configurar un servicio de autenticación para VPN-Plus de SSL en una puerta de enlace Edge

Utilice la pantalla **Autenticación** en la pestaña **VPN-Plus de SSL** para configurar un servidor de autenticación local para el servicio VPN de SSL de la puerta de enlace Edge y, de forma opcional, habilitar la autenticación del certificado de cliente. Este servidor de autenticación se utiliza para autenticar los usuarios que se conectan. Se autenticarán todos los usuarios configurados en el servidor de autenticación local.

### 6 Añadir usuarios de VPN-Plus de SSL al servidor local de autenticación de VPN-Plus de SSL

Utilice la pantalla **Usuarios** en la pestaña **VPN-Plus de SSL** para agregar cuentas de usuarios remotos al servidor local de autenticación para el servicio VPN de SSL de la puerta de enlace Edge.

### 7 Agregar un paquete de instalación del cliente VPN-Plus de SSL

Utilice la pantalla Paquetes de instalación de la pestaña **VPN-Plus de SSL** para crear paquetes de instalación con nombre del cliente VPN-Plus de SSL para los usuarios remotos.

### 8 Editar la configuración del cliente VPN-Plus de SSL

Utilice la pantalla **Configuración del cliente** de la pestaña **VPN-Plus de SSL** para personalizar el modo en el que el túnel del cliente VPN de SSL debe responder cuando el usuario remoto inicia sesión en VPN de SSL.

### 9 Personalizar la configuración general de VPN-Plus de SSL para una puerta de enlace Edge

De forma predeterminada, el sistema establece algunos ajustes de VPN-Plus de SSL para una puerta de enlace Edge en el entorno de vCloud Director. Puede utilizar la pantalla **Configuración general** en la pestaña **VPN-Plus de SSL** en el portal para tenants de vCloud Director para personalizar esta configuración.

## Desplazarse a la pantalla VPN-Plus de SSL

Es posible desplazarse hasta la pantalla VPN-Plus de SSL para comenzar a configurar el servicio VPN-Plus de SSL para una puerta de enlace Edge.



## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **VPN-Plus de SSL**.

## Pasos siguientes

En la pantalla **General**, configure los ajustes predeterminados de VPN-Plus de SSL. Consulte [Personalizar la configuración general de VPN-Plus de SSL para una puerta de enlace Edge](#).

## Configurar ajustes de un servidor VPN de SSL

Esta configuración de servidor permite determinar los ajustes para el servidor VPN de SSL, como la dirección IP y el puerto de escucha para el servicio, la lista de cifrado del servicio y su certificado de servicio. Al conectarse a la puerta de enlace Edge, los usuarios remotos especifican la misma dirección IP y el puerto que se establecieron en esta configuración de servidor.

Si la puerta de enlace Edge se configuró con varias redes de direcciones IP superpuestas en la interfaz externa, la dirección IP que seleccione para el servidor VPN de SSL puede ser diferente a la de la interfaz externa predeterminada de la puerta de enlace Edge.

Al determinar la configuración de un servidor VPN de SSL, debe elegir los algoritmos de cifrado que se utilizarán para el túnel VPN de SSL. Puede elegir uno o varios cifrados. Elija cuidadosamente los cifrados de acuerdo con los puntos fuertes y débiles de sus selecciones.

De forma predeterminada, el sistema utiliza el certificado autofirmado predeterminado que el sistema genera para cada puerta de enlace Edge como el certificado de identidad de servidor predeterminado para el túnel VPN de SSL. En lugar de esta opción predeterminada, puede utilizar un certificado digital que haya agregado al sistema en la pantalla **Certificados**.

## Requisitos previos

- Compruebe que cumple con los requisitos previos descritos en [Configurar VPN-Plus de SSL](#).
- Si decide utilizar un certificado de servicio diferente al predeterminado, importe el certificado requerido en el sistema. Consulte [Agregar un certificado de servicio a la puerta de enlace Edge](#).
- [Desplazarse a la pantalla VPN-Plus de SSL](#).

## Procedimiento

- 1 En la pantalla **VPN-Plus de SSL**, haga clic en **Configuración del servidor**.
- 2 Haga clic en **Habilitado**.
- 3 Seleccione una dirección IP del menú desplegable.

4 (opcional) Introduzca un número de puerto TCP.

El paquete de instalación de cliente de SSL utilizará el número de puerto TCP. De forma predeterminada, el sistema utiliza el puerto 443, que es el puerto predeterminado para el tráfico HTTPS/SSL. Si bien un número de puerto es obligatorio, se puede establecer cualquier puerto TCP para las comunicaciones.

---

**Nota** El cliente VPN de SSL requiere que la dirección IP y el puerto se configuren aquí para que sean accesibles desde los sistemas cliente de los usuarios remotos. Si cambia el número de puerto predeterminado, asegúrese de que se pueda acceder a la combinación de puerto y dirección IP desde los sistemas de los usuarios previstos.

---

5 Seleccione un método de cifrado de la lista de cifrados.

6 Configure la política de registro de syslog del servicio.

El registro está habilitado de forma predeterminada. Puede cambiar el nivel de los mensajes que se registran o deshabilitar el registro.

7 (opcional) Si desea utilizar un certificado de servicio en lugar del certificado autofirmado predeterminado que genera el sistema, haga clic en **Cambiar certificado del servidor**, seleccione un certificado y haga clic en **Aceptar**.

8 Haga clic en **Guardar cambios**.

**Pasos siguientes**

---

**Nota** Los usuarios remotos deben poder acceder a la dirección IP de puerta de enlace Edge y al número de puerto TCP que se establecen. Agregue una regla de firewall de puerta de enlace Edge que permita el acceso al puerto y a la dirección IP de VPN-Plus de SSL configurados en este procedimiento. Consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

---

Agregue un grupo de direcciones IP para que se asignen direcciones IP a los usuarios remotos cuando se conecten con VPN-Plus de SSL. Consulte [Crear un grupo de direcciones IP para usarlo con VPN-Plus de SSL en una puerta de enlace Edge](#).

## Crear un grupo de direcciones IP para usarlo con VPN-Plus de SSL en una puerta de enlace Edge

Se asignan direcciones IP virtuales a los usuarios remotos desde los grupos de direcciones IP estáticas que se configuran en la pantalla **Grupos de direcciones IP** de la pestaña **VPN-Plus de SSL**.


Cada grupo de direcciones IP agregado a esta pantalla hace que se configure una subred de direcciones IP en la puerta de enlace Edge. Los intervalos de IP utilizados en estos grupos de direcciones IP deben ser diferentes de los de todas las otras redes configuradas en la puerta de enlace Edge.

**Nota** VPN de SSL asigna direcciones IP de los grupos de direcciones IP a los usuarios remotos según el orden en el que se muestran los grupos de direcciones IP en la tabla en pantalla. Después de agregar los grupos de direcciones IP a la tabla en pantalla, puede ajustar sus posiciones en la tabla con las flechas hacia arriba y hacia abajo.

#### Requisitos previos

- [Desplazarse a la pantalla VPN-Plus de SSL.](#)
- [Configurar ajustes de un servidor VPN de SSL.](#)

#### Procedimiento

- 1 En la pestaña **VPN-Plus de SSL**, haga clic en **Grupos de direcciones IP**.
- 2 Haga clic en el botón **Crear** ()
- 3 Establezca la configuración del grupo de direcciones IP.

Opción	Acción
<b>Rango de IP</b>	<p>Introduzca un rango de direcciones IP para este grupo de direcciones IP (por ejemplo, <b>127.0.0.1-127.0.0.9</b>).</p> <p>Estas direcciones IP se asignarán a los clientes VPN cuando se autenticuen y se conecten al túnel VPN de SSL.</p>
<b>Máscara de red</b>	Introduzca la máscara de red del grupo de direcciones IP (por ejemplo, <b>255.255.255.0</b> ).
<b>Puerta de enlace</b>	<p>Introduzca la dirección IP que desea que la puerta de enlace Edge cree y asígnela como la dirección de puerta de enlace para este grupo de direcciones IP.</p> <p>Cuando se crea el grupo de direcciones IP, se crea un adaptador virtual en la máquina virtual de la puerta de enlace Edge y se configura esta dirección IP en esa interfaz virtual. Esta dirección IP puede ser cualquier IP dentro de la subred que no sea parte también del intervalo en el campo <b>Rango de IP</b>.</p>
<b>Descripción</b>	(Opcional) Introduzca una descripción para este grupo de direcciones IP.
<b>Estado</b>	Seleccione si desea habilitar o deshabilitar este grupo de direcciones IP.
<b>DNS primario</b>	(Opcional) Introduzca el nombre del servidor DNS primario que se utilizará para la resolución de nombres de estas direcciones IP virtuales.
<b>DNS secundario</b>	(Opcional) Introduzca el nombre del servidor DNS secundario que se usará.

Opción	Acción
Sufijo DNS	(Opcional) Introduzca el sufijo DNS del dominio en el que se alojan los sistemas del cliente para la resolución de nombres de host basada en dominios.
Servidor WINS	(Opcional) Introduzca la dirección del servidor WINS que satisfaga las necesidades de la organización.

#### 4 Haga clic en **Conservar**.

#### Resultados

La configuración del grupo de direcciones IP se agregará a la tabla en pantalla.

#### Pasos siguientes

Agregue las redes privadas a las que desea que los usuarios remotos puedan acceder mediante VPN-Plus de SSL. Consulte [Agregar una red privada para usarla con VPN-Plus de SSL en una puerta de enlace Edge](#).

### Agregar una red privada para usarla con VPN-Plus de SSL en una puerta de enlace Edge

Utilice la pantalla Redes privadas de la pestaña **VPN-Plus de SSL** para configurar las redes privadas. Las redes privadas son las recomendadas para el acceso de los clientes VPN, cuando los usuarios remotos se conectan mediante sus clientes VPN y el túnel VPN de SSL. Las redes privadas habilitadas se instalan en la tabla de enrutamiento del cliente VPN.

Las redes privadas forman una lista de todas las redes IP accesibles detrás de la puerta de enlace Edge con tráfico para un cliente VPN que se desea cifrar o excluir del cifrado. Se debe agregar cada red privada que requiera acceso a través de un túnel VPN de SSL como una entrada independiente. Puede utilizar las técnicas de resumen de rutas para limitar la cantidad de entradas.


- VPN-Plus de SSL permite que los usuarios remotos accedan a redes privadas según el orden de arriba abajo en que se muestran los grupos de direcciones IP en la tabla en pantalla. Después de agregar las redes privadas a la tabla en pantalla, puede ajustar sus posiciones en la tabla con las flechas hacia arriba y hacia abajo.
- Si decide habilitar la optimización de TCP para una red privada, puede que algunas aplicaciones, como FTP configurado en modo activo, no funcionen en esa subred. Para agregar un servidor FTP configurado en modo activo, debe agregar otra red privada para ese servidor FTP y deshabilitar la optimización de TCP para esa red privada. Además, la red privada para dicho servidor FTP debe estar habilitada y aparecer en la tabla en pantalla por encima de la red privada optimizada para TCP.

#### Requisitos previos

- [Desplazarse a la pantalla VPN-Plus de SSL](#).

- Crear un grupo de direcciones IP para usarlo con VPN-Plus de SSL en una puerta de enlace Edge.

#### Procedimiento

- 1 En la pestaña **VPN-Plus de SSL**, haga clic en **Redes privadas**.
- 2 Haga clic en el botón **Agregar** ()
- 3 Configure los ajustes de red privada.

Opción	Acción
Red	<p>Escriba la dirección IP de la red privada en formato CIDR (por ejemplo, <b>192169.1.0/24</b>).</p>
Descripción	<p>(Opcional) Escriba una descripción para la red.</p>
Enviar tráfico	<p>Especifique la manera en la que desea que el cliente VPN envíe el tráfico de Internet y de red privada.</p> <ul style="list-style-type: none"> <li>■ <b>A través del túnel</b> <p>El cliente VPN envía el tráfico de Internet y de red privada a través de la puerta de enlace Edge habilitada para VPN-Plus de SSL.</p> </li> <li>■ <b>Omitir el túnel</b> <p>El cliente VPN omite la puerta de enlace Edge y envía el tráfico directamente al servidor privado.</p> </li> </ul>
Habilitar optimización de TCP	<p>(Opcional) Para optimizar la velocidad de Internet de la mejor manera, cuando selecciona <b>A través del túnel</b> para enviar el tráfico, también debe seleccionar <b>Habilitar optimización de TCP</b></p> <p>La selección de esta opción mejora el rendimiento de los paquetes TCP en el túnel VPN, pero no mejora el rendimiento del tráfico UDP.</p> <p>El túnel VPN de SSL convencional de acceso completo envía datos de TCP/IP en una segunda pila de TCP/IP para el cifrado a través de Internet. Este método convencional encapsula los datos de la capa de aplicaciones en dos flujos de TCP distintos. Cuando se genera una pérdida de paquetes, lo que es posible incluso en condiciones óptimas de Internet, se produce un efecto de degradación de rendimiento denominado colapso de TCP sobre TCP. En un colapso de TCP sobre TCP, dos instrumentos TCP corrigen el mismo paquete de datos de IP, lo que socava el rendimiento de red y agota los tiempos de espera de conexión. La selección de <b>Habilitar optimización de TCP</b> elimina el riesgo de que se produzca este problema de TCP sobre TCP.</p> <p><b>Nota</b> Cuando se habilita la optimización de TCP:</p> <ul style="list-style-type: none"> <li>■ Debe especificar los números de puerto para los que se optimizará el tráfico de Internet.</li> <li>■ El servidor VPN de SSL abre la conexión TCP en nombre del cliente VPN. Cuando el servidor VPN de SSL abre la conexión TCP, se aplica la primera regla de firewall de Edge generada automáticamente, lo que permite que se aprueben todas las conexiones abiertas desde la puerta de enlace Edge. El tráfico no optimizado se evalúa con las reglas de firewall de Edge tradicionales. La regla TCP generada de forma predeterminada permite cualquier conexión.</li> </ul>

Opción	Acción
Puertos	Si selecciona <b>A través del túnel</b> , escriba el rango de números de puertos que desea abrir para que el usuario remoto acceda a los servidores internos, como <b>20–21</b> para el tráfico de FTP y <b>80–81</b> para el tráfico de HTTP. Para otorgar acceso sin restricciones a los usuarios, deje el campo en blanco.
Estado	Habilite o deshabilite la red privada.

4 Haga clic en **Conservar**.

5 Haga clic en **Guardar cambios** para guardar la configuración en el sistema.

#### Pasos siguientes

Agregue un servidor de autenticación. Consulte [Configurar un servicio de autenticación para VPN-Plus de SSL en una puerta de enlace Edge](#).

**Importante** Agregue las reglas de firewall correspondientes para permitir el tráfico de red a las redes privadas que agregó en esta pantalla. Consulte [Agregar una regla de firewall de puerta de enlace Edge](#).

## Configurar un servicio de autenticación para VPN-Plus de SSL en una puerta de enlace Edge

Utilice la pantalla **Autenticación** en la pestaña **VPN-Plus de SSL** para configurar un servidor de autenticación local para el servicio VPN de SSL de la puerta de enlace Edge y, de forma opcional, habilitar la autenticación del certificado de cliente. Este servidor de autenticación se utiliza para autenticar los usuarios que se conectan. Se autenticarán todos los usuarios configurados en el servidor de autenticación local.

Puede tener un solo servidor de autenticación local de VPN-Plus de SSL configurado en la puerta de enlace Edge. Si hace clic en **+ LOCAL** y especifica servidores de autenticación adicionales, se mostrará un mensaje de error al intentar guardar la configuración.

El tiempo máximo para autenticar a través de VPN de SSL es tres (3) minutos. Este valor máximo se determina según el tiempo de espera sin autenticación, el cual es 3 minutos de forma predeterminada y no es configurable. Como resultado, si tiene varios servidores de autenticación en la autorización en cadena y la autenticación de usuario tarda más de 3 minutos, el usuario no se autenticará.

#### Requisitos previos

- [Desplazarse a la pantalla VPN-Plus de SSL](#).
- [Agregar una red privada para usarla con VPN-Plus de SSL en una puerta de enlace Edge](#).
- Si planea habilitar la autenticación del certificado del cliente, compruebe que se haya añadido un certificado de CA a la puerta de enlace Edge. Consulte [Agregar un certificado de CA a la puerta de enlace Edge para la verificación de confianza de certificados SSL](#).

## Procedimiento

- 1 Haga clic en la pestaña **VPN-Plus de SSL** y en **Autenticación**.
- 2 Haga clic en **Local**.
- 3 Configure los ajustes del servidor de autenticación.
  - a (opcional) Habilite y configure la política de contraseña.

Opción	Descripción
<b>Habilitar política de contraseñas</b>	Active la aplicación de la configuración de la política de contraseñas que configure aquí.
<b>Longitud de la contraseña</b>	Introduzca las cantidades mínima y máxima de caracteres que se permiten para la contraseña.
<b>Cantidad mínima de letras</b>	(Opcional) Escriba la cantidad mínima de caracteres alfabéticos que se requieren en la contraseña.
<b>Cantidad mínima de dígitos</b>	(Opcional) Escriba la cantidad mínima de caracteres numéricos que se requieren en la contraseña.
<b>Cantidad mínima de caracteres especiales</b>	(Opcional) Escriba la cantidad mínima de caracteres especiales, como la Y comercial (&), la almohadilla (#), el signo de porcentaje (%), entre otros, que sean necesarios en la contraseña.
<b>La contraseña no debe contener el ID de usuario</b>	(Opcional) Habilite esta opción para exigir que la contraseña no contenga el identificador de usuario.
<b>La contraseña caduca en</b>	(Opcional) Escriba la cantidad máxima de días de vigencia de la contraseña, antes de que el usuario deba cambiarla.
<b>Notificación de caducidad en</b>	(Opcional) Escriba la cantidad de días antes del valor de <b>La contraseña caduca en</b> que se notifica al usuario que la contraseña está a punto de caducar.

- b (opcional) Habilite y configure la política de bloqueo de cuentas.

Opción	Descripción
<b>Habilitar política de bloqueo de cuentas</b>	Active la aplicación de la configuración de la política de bloqueo de cuentas que configure aquí.
<b>Recuento de reintentos</b>	Introduzca la cantidad de veces que un usuario puede intentar acceder a la cuenta.
<b>Duración del reintento</b>	Introduzca el período en minutos durante el que la cuenta del usuario se bloquea tras intentos de inicio de sesión incorrectos. Por ejemplo, si especifica <b>Recuento de reintentos</b> como 5 y <b>Duración del reintento</b> como 1 minuto, la cuenta del usuario se bloqueará tras 5 intentos de inicio de sesión incorrectos en 1 minuto.
<b>Duración del bloqueo</b>	Introduzca el período durante el cual la cuenta del usuario permanecerá bloqueada. Una vez transcurrido ese tiempo, la cuenta se desbloqueará automáticamente.

- c En la sección Estado, habilite este servidor de autenticación.

- d (opcional) Configure la autenticación secundaria.

Opciones	Descripción
Usar este servidor para la autenticación secundaria	(Opcional) Especifique si desea utilizar el servidor como segundo nivel de autenticación.
Finalizar sesión si la autenticación no es correcta	(Opcional) Especifique si desea cerrar la sesión de VPN cuando se produzca un error en la autenticación.

- e Haga clic en **Conservar**.

- 4 (opcional) Para habilitar la autenticación de certificación de clientes, haga clic en **Cambiar certificado**, active el botón de alternancia de habilitación, seleccione el certificado de CA que desea utilizar y haga clic en **Aceptar**.

#### Pasos siguientes

Agregue usuarios locales al servidor de autenticación local para que puedan conectarse con VPN-Plus de SSL. Consulte [Añadir usuarios de VPN-Plus de SSL al servidor local de autenticación de VPN-Plus de SSL](#).

Cree un paquete de instalación que contenga el cliente SSL para que los usuarios remotos puedan instalarlo en los sistemas locales. Consulte [Agregar un paquete de instalación del cliente VPN-Plus de SSL](#).

### Añadir usuarios de VPN-Plus de SSL al servidor local de autenticación de VPN-Plus de SSL


Utilice la pantalla **Usuarios** en la pestaña **VPN-Plus de SSL** para agregar cuentas de usuarios remotos al servidor local de autenticación para el servicio VPN de SSL de la puerta de enlace Edge.

**Nota** Si aún no se ha configurado un servidor de autenticación local, al agregar un usuario en la pantalla **Usuarios**, se agregará automáticamente un servidor de autenticación local con valores predeterminados. A continuación, se puede utilizar el botón Editar en la pantalla **Autenticación** para ver y editar los valores predeterminados. Para obtener información sobre el uso de la pantalla **Autenticación**, consulte [Configurar un servicio de autenticación para VPN-Plus de SSL en una puerta de enlace Edge](#).

#### Requisitos previos

[Desplazarse a la pantalla VPN-Plus de SSL](#).

#### Procedimiento

- En la pestaña **VPN-Plus de SSL**, haga clic en **Usuarios**.
- Haga clic en el botón **Crear** ()



### 3 Configure las siguientes opciones para el usuario.

Opción	Descripción
ID de usuario	Introduzca el identificador del usuario.
Contraseña	Introduzca una contraseña para el usuario.
Vuelva a escribir la contraseña	Vuelva a introducir la contraseña.
Nombre	(Opcional) Introduzca el nombre del usuario.
Apellido	(Opcional) Introduzca el apellido del usuario.
Descripción	(Opcional) Introduzca una descripción para el usuario.
Habilitado	Especifique si el usuario está habilitado o deshabilitado.
La contraseña nunca caduca	(Opcional) Especifique si desea conservar la misma contraseña para este usuario durante un tiempo indefinido.
Permitir cambio de contraseña	(Opcional) Especifique si desea permitir que el usuario cambie la contraseña.
Cambiar contraseña la próxima vez que se inicie sesión	(Opcional) Especifique si desea que este usuario cambie la contraseña la próxima vez que inicie sesión.

### 4 Haga clic en **Conservar**.

### 5 Repita los pasos para agregar más usuarios.

#### Pasos siguientes

Agregue usuarios locales al servidor de autenticación local para que puedan conectarse con VPN-Plus de SSL. Consulte [Añadir usuarios de VPN-Plus de SSL al servidor local de autenticación de VPN-Plus de SSL](#).

Cree un paquete de instalación que contenga el cliente SSL para que los usuarios remotos puedan instalarlo en los sistemas locales. Consulte [Agregar un paquete de instalación del cliente VPN-Plus de SSL](#).

### Agregar un paquete de instalación del cliente VPN-Plus de SSL

Utilice la pantalla Paquetes de instalación de la pestaña **VPN-Plus de SSL** para crear paquetes de instalación con nombre del cliente VPN-Plus de SSL para los usuarios remotos.

Puede agregar un paquete de instalación del cliente VPN-Plus de SSL a la puerta de enlace Edge. Se le pedirá a los nuevos usuarios que descarguen e instalen este paquete cuando inicien sesión para utilizar la conexión de VPN por primera vez. Cuando se agregan, estos paquetes de instalación del cliente se pueden descargar desde el FQDN de la interfaz pública de la puerta de enlace Edge.

Puede crear paquetes de instalación que se ejecuten en sistemas operativos Windows, Linux y Mac. Si necesita parámetros de instalación diferentes para cada cliente VPN de SSL, cree un paquete de instalación para cada configuración.

#### Requisitos previos


[Desplazarse a la pantalla VPN-Plus de SSL](#)

## Procedimiento

1 En la pestaña **VPN-Plus de SSL** del portal para tenants, haga clic en **Paquetes de instalación**.

2 Haga clic en el botón **Agregar** ().

3 Configure los ajustes del paquete de instalación.

Opción	Descripción
Nombre del perfil	Introduzca un nombre de perfil para este paquete de instalación. Este nombre se mostrará al usuario remoto para identificar esta conexión VPN de SSL para la puerta de enlace Edge.
Puerta de enlace	Introduzca la dirección IP o el FQDN de la interfaz pública de la puerta de enlace Edge. La dirección IP o el FQDN que se introduzcan están enlazados al cliente VPN de SSL. Cuando se instale el cliente en el sistema local del usuario remoto, se mostrará esta dirección IP o FQDN en ese cliente VPN de SSL. Para enlazar interfaces de vínculo superior de puerta de enlace Edge adicionales a este cliente VPN de SSL, haga clic en el botón <b>Agregar</b> (  ) para agregar filas, y especifique los puertos y las direcciones IP o los FQDN de la interfaz.
Puerto	(Opcional) Para modificar el valor de puerto predeterminado que se muestra, haga doble clic en el valor e introduzca uno nuevo.
Windows Linux Mac	Seleccione los sistemas operativos para los que desea crear paquetes de instalación.
Descripción	(Opcional) Escriba una descripción para el usuario.
Habilitado	Especifique si este paquete está habilitado o deshabilitado.

4 Seleccione los parámetros de instalación de Windows.

Opción	Descripción
Iniciar cliente al iniciar sesión	Se inicia el cliente VPN de SSL cuando el usuario remoto inicia sesión en el sistema local.
Permitir recordar la contraseña	El cliente puede recordar la contraseña de usuario.
Habilitar instalación en modo silencioso	Se ocultan los comandos de instalación de los usuarios remotos.
Ocultar adaptador de red del cliente SSL	Se oculta el adaptador de VPN-Plus de SSL de VMware, el cual se instala en el equipo del usuario remoto junto con el paquete de instalación del cliente VPN de SSL.
Ocultar icono de la bandeja del sistema del cliente	Se oculta el icono de la bandeja de VPN de SSL que indica si la conexión VPN está activa o no.
Crear icono en el escritorio	Se crea un icono en el escritorio del usuario para invocar el cliente SSL.

Opción	Descripción
<b>Habilitar funcionamiento en modo silencioso</b>	Se oculta la ventana en la que se indica que se completó la instalación.
<b>Validación del certificado de seguridad del servidor</b>	El cliente VPN de SSL valida el certificado de servidor VPN de SSL antes de establecer la conexión segura.

5 Haga clic en **Conservar**.

#### Pasos siguientes

Edite la configuración del cliente. Consulte [Editar la configuración del cliente VPN-Plus de SSL](#).

### Editar la configuración del cliente VPN-Plus de SSL

Utilice la pantalla **Configuración del cliente** de la pestaña **VPN-Plus de SSL** para personalizar el modo en el que el túnel del cliente VPN de SSL debe responder cuando el usuario remoto inicia sesión en VPN de SSL.

#### Requisitos previos

[Desplazarse a la pantalla VPN-Plus de SSL](#)

#### Procedimiento

- 1 En la pestaña **VPN-Plus de SSL**, haga clic en **Configuración del cliente**.
- 2 Seleccione una opción de **Modo de túnel**.
  - En el modo de túnel dividido, solo el tráfico de VPN fluye por la puerta de enlace Edge.
  - En el modo de túnel completo, la puerta de enlace Edge se convierte en la puerta de enlace predeterminada para el usuario remoto y todo el tráfico (por ej., VPN, local e Internet) fluye por la puerta de enlace Edge.
- 3 Si selecciona el modo de túnel completo, introduzca la dirección IP de la puerta de enlace predeterminada que utilizan los clientes de los usuarios remotos y, opcionalmente, seleccione si desea excluir el tráfico de la subred local para evitar que fluya a través del túnel VPN.
- 4 (opcional) Deshabilite la reconexión automática.
 

La opción **Habilitar reconexión automática** está habilitada de forma predeterminada. Si la reconexión automática está habilitada, el cliente VPN de SSL volverá a conectar automáticamente a los usuarios cuando se desconecten.
- 5 (opcional) De manera opcional, puede habilitar la capacidad de que el cliente notifique a los usuarios remotos cuando existe una actualización de cliente disponible.
 

Esta opción está deshabilitada de forma predeterminada. Si habilita esta opción, los usuarios remotos pueden elegir instalar la actualización.
- 6 Haga clic en **Guardar cambios**.

## Personalizar la configuración general de VPN-Plus de SSL para una puerta de enlace Edge

De forma predeterminada, el sistema establece algunos ajustes de VPN-Plus de SSL para una puerta de enlace Edge en el entorno de vCloud Director. Puede utilizar la pantalla **Configuración general** en la pestaña **VPN-Plus de SSL** en el portal para tenants de vCloud Director para personalizar esta configuración.

### Requisitos previos

[Desplazarse a la pantalla VPN-Plus de SSL.](#)

### Procedimiento

- 1 En la pestaña **VPN-Plus de SSL**, haga clic en **Configuración general**.
- 2 Edite la configuración general según corresponda para satisfacer las necesidades de la organización.

Opción	Descripción
Evitar varios inicios de sesión con el mismo nombre de usuario	Active esta opción para restringir un usuario remoto de modo que disponga de una sola sesión de inicio de sesión activa con el mismo nombre de usuario.
Compresión	Active esta opción para habilitar la compresión de datos inteligente basada en TCP y aumentar la velocidad de la transferencia de datos.
Habilitar registro	Active esta opción para mantener un registro del tráfico que pasa por la puerta de enlace VPN de SSL. El registro está habilitado de forma predeterminada.
Forzar teclado virtual	Active esta opción para exigir que los usuarios remotos utilicen un teclado virtual (en pantalla) solamente para introducir información de inicio de sesión.
Aleatorizar las teclas del teclado virtual	Active esta opción para que el teclado virtual tenga un diseño de teclas aleatorio.
Tiempo de espera de sesión inactiva	Introduzca el tiempo de espera de sesión inactiva en minutos. Si no se detecta ninguna actividad en una sesión de usuario durante el período especificado, el sistema desconectará la sesión de usuario. El valor predeterminado del sistema es 10 minutos.
Notificación del usuario	Escriba el mensaje que se mostrará a los usuarios remotos después de iniciar sesión.
Habilitar acceso a la URL pública	Active esta opción para permitir que los usuarios remotos accedan a sitios que no se configuraron explícitamente para el acceso de usuarios remotos.
Habilitar tiempo de espera forzado	Active esta opción para que el sistema desconecte a los usuarios remotos después de que se cumpla el período que especifique en el campo <b>Tiempo de espera forzado</b> .
Tiempo de espera forzado	Escriba el período de tiempo de espera en minutos. Este campo se muestra cuando se activa el botón de alternancia <b>Habilitar tiempo de espera forzado</b> .

- 3 Haga clic en **Guardar cambios**.

## Configurar VPN de IPsec

Las puertas de enlace Edge en un entorno de vCloud Director son compatibles con el protocolo de seguridad de Internet (Internet Protocol Security, IPsec) de sitio a sitio para proteger túneles VPN entre redes de centros de datos virtuales de organización, o bien entre una red de centros de datos virtuales de organización y una dirección IP externa. Es posible configurar el servicio VPN de IPsec en una puerta de enlace Edge.

El escenario más común implica configurar una conexión de VPN de IPsec desde una red remota hasta el centro de datos virtual de organización. El software NSX proporciona capacidades de VPN de IPsec para una puerta de enlace Edge, incluida la compatibilidad con la autenticación de certificados, el modo de clave compartida previamente, y el tráfico de unidifusión de IP entre este mismo elemento y los enrutadores VPN remotos. También puede configurar varias subredes para establecer conexiones a través de túneles de IPsec a la red interna detrás de una puerta de enlace Edge. Al configurar varias subredes para conectarse a la red interna a través de túneles de IPsec, dichas subredes y la red interna detrás de la puerta de enlace Edge no deben tener rangos de direcciones que se superpongan.

---

**Nota** Si los elementos remotos y locales de mismo nivel en un túnel IPsec tienen direcciones IP superpuestas, es posible que el reenvío de tráfico a través del túnel no sea uniforme en función de si hay rutas conectadas locales y rutas asociadas automáticamente.

---

Se admiten los siguientes algoritmos de VPN de IPsec:

- AES (AES128-CBC)
- AES256 (AES265-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Grupo Diffie-Hellman 2)
- DH-5 (Grupo Diffie-Hellman 5)
- DH-14 (Grupo Diffie-Hellman 14)

---

**Nota** No se admiten protocolos de enrutamiento dinámico con VPN de IPsec. Al configurar un túnel de VPN de IPsec entre una puerta de enlace Edge del centro de datos virtual de organización y una red VPN de puerta de enlace física en un sitio remoto, no se puede configurar el enrutamiento dinámico para esa conexión. El enrutamiento dinámico en el vínculo superior de puerta de enlace Edge no puede obtener la dirección IP de ese sitio remoto.

---

Como se describe en el tema correspondiente a la *información general de VPN de IPsec* en la *guía de administración de NSX*, la cantidad máxima de túneles admitidos en una puerta de enlace Edge se determina mediante el tamaño configurado: compacta, grande, extragrande y cuádruple. Para ver el tamaño de la puerta de enlace Edge, inicie sesión en la consola web de vCloud Director, desplácese hasta la puerta de enlace Edge y use la acción **Propiedades** para ver la configuración de la puerta de enlace Edge. Consulte la *Guía del administrador de vCloud Director* para obtener información sobre el uso de la consola web de vCloud Director.

La configuración de VPN de IPsec en una puerta de enlace Edge es un proceso de varios pasos.

---

**Nota** Si hay un firewall entre los endpoints del túnel, después de configurar el servicio VPN de IPsec, actualice las reglas de firewall para permitir los siguientes protocolos IP y puertos UDP:

- Protocolo IP ID 50 (ESP)
  - Protocolo IP ID 51 (AH)
  - Puerto UDP 500 (IKE)
  - Puerto UDP 4500
- 

## Procedimiento

### 1 Desplazarse a la pantalla VPN de IPsec

En la pantalla **VPN de IPsec**, puede comenzar a configurar el servicio de VPN con IPsec de una puerta de enlace Edge.

### 2 Configurar conexiones de sitio de VPN de IPsec para la puerta de enlace Edge

Utilice la pantalla **Sitios de VPN de IPsec** del portal para tenants de vCloud Director con el fin de configurar los ajustes necesarios para crear una conexión de VPN de IPsec entre el centro de datos virtual de organización y otro sitio mediante las capacidades de VPN de IPsec de la puerta de enlace Edge.

### 3 Habilitar el servicio VPN de IPsec en una puerta de enlace Edge

Cuando se configura al menos una conexión VPN de IPsec, se puede habilitar el servicio VPN de IPsec en la puerta de enlace Edge.

### 4 Especificar la configuración de VPN de IPsec global

Utilice la pantalla **Configuración global** para configurar la autenticación de VPN de IPsec en el nivel de puerta de enlace Edge. En esta pantalla, puede establecer una clave compartida previamente global y habilitar la autenticación de certificados.

## Desplazarse a la pantalla VPN de IPsec

En la pantalla **VPN de IPsec**, puede comenzar a configurar el servicio de VPN con IPsec de una puerta de enlace Edge.

## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **VPN > VPN de IPsec**.

## Pasos siguientes

Utilice la pantalla **Sitios de VPN de IPsec** para configurar una conexión de VPN de IPsec. Para poder habilitar el servicio VPN de IPsec en la puerta de enlace Edge, se debe configurar al menos una conexión. Consulte [Configurar conexiones de sitio de VPN de IPsec para la puerta de enlace Edge](#).

## Configurar conexiones de sitio de VPN de IPsec para la puerta de enlace Edge

Utilice la pantalla **Sitios de VPN de IPsec** del portal para tenants de vCloud Director con el fin de configurar los ajustes necesarios para crear una conexión de VPN de IPsec entre el centro de datos virtual de organización y otro sitio mediante las capacidades de VPN de IPsec de la puerta de enlace Edge.

Cuando configure una conexión de VPN de IPsec entre sitios, la conexión se configura desde el punto de vista de la ubicación actual. Para configurar la conexión de VPN correctamente, es necesario comprender los conceptos en el contexto del entorno de vCloud Director.


- Las subredes locales y del mismo nivel especifican las redes a las que se conecta la VPN. Cuando se especifican dichas subredes en las configuraciones de sitios de VPN de IPsec, indique un rango de redes en lugar de una dirección IP específica. Utilice el formato CIDR (por ejemplo, **192.168.99.0/24**).
- El identificador del mismo nivel es un identificador que identifica de manera exclusiva el dispositivo remoto que finaliza la conexión de VPN (por lo general, su dirección IP pública). Para elementos del mismo nivel con autenticación de certificados, este identificador debe ser el nombre distintivo que se ha definido en el certificado del elemento del mismo nivel. Para elementos del mismo nivel de PSK, este identificador puede ser cualquier cadena. Una práctica recomendada en NSX es utilizar la dirección IP pública del dispositivo remoto o el FQDN como el identificador del mismo nivel. Si la dirección IP del mismo nivel es de otra red de centros de datos virtuales de organización, introduzca la dirección IP nativa del mismo nivel. Si NAT está configurada para el elemento del mismo nivel, debe escribir la dirección IP privada del elemento del mismo nivel.
- El endpoint del mismo nivel especifica la dirección IP pública del dispositivo remoto al que se va a conectar. El endpoint del mismo nivel puede ser una dirección diferente del identificador del mismo nivel si no se puede acceder directamente a la puerta de enlace del elemento del mismo nivel desde Internet, sino que se conecta a través de otro dispositivo. Si NAT está configurada para el elemento del mismo nivel, debe escribir la dirección IP pública que utilizan los dispositivos para NAT.

- El identificador local especifica la dirección IP pública de la puerta de enlace Edge del centro de datos virtual de organización. Puede introducir una dirección IP o un nombre de host junto con el firewall de la puerta de enlace Edge.
- El endpoint local especifica la red en el centro de datos virtual de organización en la que transmite la puerta de enlace Edge. Por lo general, la red externa de la puerta de enlace Edge es el endpoint local.

#### Requisitos previos

- [Desplazarse a la pantalla VPN de IPsec.](#)
- [Configurar VPN de IPsec.](#)
- Si decide utilizar un certificado global como el método de autenticación, compruebe que la autenticación de certificados esté habilitada en la pantalla **Configuración global**. Consulte [Especificar la configuración de VPN de IPsec global](#).

#### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 En la pestaña **VPN de IPsec**, haga clic en **Sitios de VPN de IPsec**.
- 3 Haga clic en el botón **Agregar** ().
- 4 Configure los ajustes de la conexión de VPN de IPsec.

Opción	Acción
<b>Habilitado</b>	Habilite esta conexión entre los dos endpoints de VPN.
<b>Habilitar confidencialidad directa total (PFS)</b>	<p>Habilite esta opción para que el sistema genere claves públicas exclusivas para todas las sesiones de VPN de IPsec que inician los usuarios.</p> <p>La habilitación de PFS garantiza que el sistema no cree un vínculo entre la clave privada de la puerta de enlace Edge y cada clave de sesión.</p> <p>El compromiso de una clave de sesión solo afectará a los datos que se intercambian en la sesión específica protegida por dicha clave. No se puede utilizar el compromiso de la clave privada del servidor para descifrar las sesiones archivadas o las futuras.</p> <p>Cuando se habilita PFS, las conexiones de VPN de IPsec a esta puerta de enlace Edge experimentan una ligera sobrecarga de procesamiento.</p> <p><b>Importante</b> No deben utilizarse las claves de sesión exclusivas para obtener claves adicionales. Asimismo, ambos lados del túnel VPN de IPsec deben admitir PFS para que funcione.</p>
<b>Nombre</b>	(Opcional) Escriba un nombre para la conexión.



Opción	Acción
ID local	<p>Introduzca la dirección IP externa de la instancia de puerta de enlace Edge, la cual es la dirección IP pública de la puerta de enlace Edge.</p> <p>La dirección IP es la que se utiliza para el identificador del mismo nivel en la configuración de VPN de IPsec en el sitio remoto.</p>
Endpoint local	<p>Introduzca la red que es el endpoint local para esta conexión.</p> <p>El endpoint local especifica la red en el centro de datos virtual de organización en la que transmite la puerta de enlace Edge. Por lo general, la red externa es el endpoint local.</p> <p>Si agrega un túnel de IP a IP con una clave compartida previamente, el identificador local y la IP de endpoint local pueden ser iguales.</p>
Subredes locales	<p>Introduzca las redes que se compartirán entre los sitios y separe las subredes con comas si desea especificar varias.</p> <p>Introduzca un rango de redes (no una dirección IP específica). Para ello, escriba la dirección IP con el formato CIDR (por ejemplo, <b>192.168.99.0/24</b>).</p>
ID del mismo nivel	<p>Introduzca un identificador del mismo nivel para identificar de manera exclusiva el sitio del mismo nivel.</p> <p>El identificador del mismo nivel es un identificador que identifica de manera exclusiva el dispositivo remoto que finaliza la conexión de VPN (por lo general, su dirección IP pública).</p> <p>Para elementos del mismo nivel con autenticación de certificados, el identificador debe ser el nombre distintivo en el certificado del elemento del mismo nivel. Para elementos del mismo nivel de PSK, este identificador puede ser cualquier cadena. Una práctica recomendada en NSX consiste en utilizar la dirección IP pública o el FQDN del dispositivo remoto como el identificador del mismo nivel.</p> <p>Si la dirección IP del mismo nivel es de otra red de centros de datos virtuales de organización, introduzca la dirección IP nativa del mismo nivel. Si NAT está configurada para el elemento del mismo nivel, debe escribir la dirección IP privada del elemento del mismo nivel.</p>
Endpoint del mismo nivel	<p>Introduzca la dirección IP o el FQDN del sitio del mismo nivel, que es la dirección de acceso público del dispositivo remoto al que se va a conectar.</p> <p><b>Nota</b> Cuando NAT está configurada para el elemento del mismo nivel, escriba la dirección IP pública que el dispositivo utiliza para NAT.</p>
Subredes del mismo nivel	<p>Introduzca la red remota a la que se conecta la VPN y separe las subredes con comas si desea especificar varias.</p> <p>Introduzca un rango de redes (no una dirección IP específica). Para ello, escriba la dirección IP con el formato CIDR (por ejemplo, <b>192.168.99.0/24</b>).</p>
Algoritmo de cifrado	<p>Seleccione el tipo de algoritmo de cifrado del menú desplegable.</p> <p><b>Nota</b> El tipo de cifrado que seleccione debe coincidir con el tipo de cifrado que se ha configurado en el dispositivo VPN del sitio remoto.</p>

Opción	Acción
Autenticación	<p>Seleccione una autenticación. Las opciones son las siguientes:</p> <ul style="list-style-type: none"> <li>■ <b>PSK</b></li> </ul> <p>La clave compartida previamente (Pre Shared Key, PSK) especifica que la clave secreta compartida entre la puerta de enlace Edge y el sitio del mismo nivel se utilizará para la autenticación.</p> <ul style="list-style-type: none"> <li>■ <b>Certificado</b></li> </ul> <p>La autenticación de certificados especifica que el certificado definido en el nivel global se utilizará para la autenticación. Esta opción no está disponible a menos que se haya configurado el certificado global en la pantalla <b>Configuración global</b> de la pestaña <b>VPN de IPsec</b>.</p>
Cambiar clave compartida	(Opcional) Al actualizar la configuración de una conexión existente, puede activar esta opción para que el campo <b>Clave compartida previamente</b> esté disponible, de modo que pueda actualizar la clave compartida.
Clave compartida previamente	<p>Si ha seleccionado <b>PSK</b> como el tipo de autenticación, escriba una cadena secreta alfanumérica, la cual puede ser una cadena con una longitud máxima de 128 bytes.</p> <p><b>Nota</b> La clave compartida debe coincidir con la clave que está configurada en el dispositivo VPN del sitio remoto. Una práctica recomendada consiste en configurar una clave compartida si algún sitio anónimo se va a conectar con el servicio VPN.</p>
Mostrar clave compartida	(Opcional) Habilite esta opción para que la clave compartida se muestre en la pantalla.
Grupo Diffie-Hellman	<p>Seleccione el esquema de criptografía que permite al sitio del mismo nivel y a esta puerta de enlace Edge establecer un secreto compartido en un canal de comunicaciones no seguro.</p> <p><b>Nota</b> El grupo Diffie-Hellman debe coincidir con la configuración del dispositivo VPN del sitio remoto.</p>
Extensión	<p>(Opcional) Escriba una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>■ <code>securelocaltrafficbyip=IPAddress</code>: permite redirigir el tráfico local de la puerta de enlace Edge a través del túnel VPN de IPsec.</li> </ul> <p>Este el valor predeterminado.</p> <ul style="list-style-type: none"> <li>■ <code>passthroughSubnets=PeerSubnet/IPAddress</code>: permite admitir la superposición de subredes.</li> </ul>

5 Haga clic en **Conservar**.

6 Haga clic en **Guardar cambios**.

La operación para guardar puede tardar un minuto en completarse.

#### Pasos siguientes

Configure la conexión para el sitio remoto. Debe configurar la conexión de VPN de IPsec en ambos lados de la conexión: el centro de datos virtual de organización y el sitio del mismo nivel.

Habilite el servicio VPN de IPsec en esta puerta de enlace Edge. Cuando haya configurado al menos una conexión de VPN de IPsec, podrá habilitar el servicio. Consulte [Habilitar el servicio VPN de IPsec en una puerta de enlace Edge](#).

## Habilitar el servicio VPN de IPsec en una puerta de enlace Edge

Cuando se configura al menos una conexión VPN de IPsec, se puede habilitar el servicio VPN de IPsec en la puerta de enlace Edge.

### Requisitos previos

- [Desplazarse a la pantalla VPN de IPsec](#).
- Compruebe que se ha configurado al menos una conexión de VPN de IPsec para esta puerta de enlace Edge. Consulte los pasos descritos en [Configurar conexiones de sitio de VPN de IPsec para la puerta de enlace Edge](#).

### Procedimiento

- 1 En la pestaña **VPN de IPsec**, haga clic en **Estado de activación**.
- 2 Haga clic en el **Estado del servicio VPN de IPsec** para habilitar el servicio VPN de IPsec.
- 3 Haga clic en **Guardar cambios**.

### Resultados

El servicio VPN de IPsec de la puerta de enlace Edge está activo.

## Especificar la configuración de VPN de IPsec global

Utilice la pantalla **Configuración global** para configurar la autenticación de VPN de IPsec en el nivel de puerta de enlace Edge. En esta pantalla, puede establecer una clave compartida previamente global y habilitar la autenticación de certificados.

Una clave compartida previamente global se utiliza para los sitios cuyo endpoint del mismo nivel se establece como **cualquiera**.

### Requisitos previos

- Si tiene intención de habilitar la autenticación de certificados, compruebe que existe al menos un certificado de servicio y los certificados firmados por CA correspondientes en la pantalla **Certificados**. No se pueden utilizar certificados autofirmados para VPN de IPsec. Consulte [Agregar un certificado de servicio a la puerta de enlace Edge](#).
- [Desplazarse a la pantalla VPN de IPsec](#).

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.

2 En la pestaña **VPN de IPsec**, haga clic en **Configuración global**.

3 (opcional) Establezca una clave compartida previamente global:

- a Habilite la opción **Cambiar clave compartida**.
- b Introduzca una clave compartida previamente.

La clave compartida previamente (PSK) global la comparten todos los sitios cuyo endpoint del mismo nivel se haya establecido como `any` (cualquiera). Si ya se ha establecido una PSK global, cambiarla a un valor vacío y guardarla no tendrá ningún efecto en la configuración existente.

- c (opcional) Opcionalmente, habilite **Mostrar clave compartida** para que la clave compartida previamente sea visible.
- d Haga clic en **Guardar cambios**.

4 Configure la autenticación de certificados:

- a Active **Habilitar autenticación de certificado**.
- b Seleccione los certificados de servicio, las CRL y los certificados de CA adecuados.
- c Haga clic en **Guardar cambios**.

#### Pasos siguientes

Opcionalmente, puede habilitar el registro para el servicio VPN de IPsec de la puerta de enlace Edge. Consulte [Estadísticas y logs para una puerta de enlace Edge](#).

## Configurar VPN de capa 2

Las puertas de enlace Edge en un entorno de vCloud Director admiten VPN de capa 2. VPN de capa 2 permite ampliar el centro de datos virtual de organización al permitir que las máquinas virtuales conserven la conectividad de red sin necesidad de cambiar la dirección IP entre ubicaciones geográficas. El servicio VPN de capa 2 se puede configurar en una puerta de enlace Edge.

El software NSX proporciona las capacidades de VPN de capa 2 para una puerta de enlace Edge. La VPN de capa 2 permite configurar un túnel entre dos sitios. Las máquinas virtuales permanecen en la misma subred a pesar de moverse entre estos sitios, lo que permite ampliar el centro de datos virtual de organización mediante la extensión de su red con VPN de capa 2. Una puerta de enlace Edge en un sitio puede proporcionar todos los servicios a las máquinas virtuales en el otro sitio.

Para crear el túnel VPN de capa 2, debe configurar un servidor VPN de capa 2 y un cliente VPN de capa 2. Como se describe en la *guía de administración de NSX*, el servidor VPN de capa 2 es la puerta de enlace Edge de destino y el cliente VPN de capa 2 es la puerta de enlace Edge de origen. Después de configurar los ajustes de VPN de capa 2 en cada puerta de enlace Edge, debe habilitar el servicio VPN de capa 2 en el servidor y el cliente.

---

**Nota** Las puertas de enlace Edge deben contener una red de centros de datos virtuales de organización enrutada, que se debe haber creado como una subinterfaz. Consulte *Guía del administrador de vCloud Director* para conocer los pasos de creación de una red de centros de datos virtuales de organización enrutada externa.

---

## Desplazarse a la pantalla VPN de capa 2

Para comenzar a configurar el servicio VPN de capa 2 de una puerta de enlace Edge, debe desplazarse a la pantalla **VPN de capa 2**.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Desplácese hasta **VPN > VPN de capa 2**.

### Pasos siguientes

Configure el servidor de VPN de capa 2. Consulte [Configurar la puerta de enlace Edge como un servidor VPN de capa 2](#).

## Configurar la puerta de enlace Edge como un servidor VPN de capa 2

El servidor VPN de capa 2 es la instancia de NSX Edge de destino a la que se conectará el cliente VPN de capa 2.

Tal como se describe en la *guía de administración de NSX*, puede conectar varios sitios del mismo nivel a este servidor VPN de capa 2.

---

**Nota** Al cambiar la configuración del sitio, la puerta de enlace Edge interrumpe y vuelve a establecer todas las conexiones existentes.

---

### Requisitos previos


- Compruebe que la puerta de enlace Edge tiene una red de centros de datos virtuales de organización enrutada que se haya configurado como una subinterfaz en la puerta de enlace Edge. Consulte *Guía del administrador de vCloud Director* para conocer los pasos de creación de una red de centros de datos virtuales de organización enrutada externa.
- [Desplazarse a la pantalla VPN de capa 2](#).

- Si desea enlazar un certificado de servicio a la conexión de VPN de capa 2, compruebe que el certificado de servidor ya se ha cargado en la puerta de enlace Edge. Consulte [Agregar un certificado de servicio a la puerta de enlace Edge](#).
- Debe configurar la dirección IP de escucha del servidor, el puerto de escucha, el algoritmo de cifrado y al menos un sitio del mismo nivel para habilitar el servicio VPN de capa 2.

#### Procedimiento

- 1 En la pestaña **VPN de capa 2**, seleccione **Servidor** para el modo de VPN de capa 2.
- 2 En la pestaña **Servidor global**, ajuste los detalles de configuración global del servidor VPN de capa 2.

Opción	Acción
IP de escucha	Seleccione la dirección IP principal o secundaria de una interfaz externa de la puerta de enlace Edge.
Puerto de escucha	Edite el valor que se muestra según las necesidades de su organización. El puerto predeterminado para el servicio VPN de capa 2 es 443.
Algoritmo de cifrado	Seleccione el algoritmo de cifrado para la comunicación entre el servidor y el cliente.
Detalles del certificado de servicio	Haga clic en <b>Cambiar certificado del servidor</b> para seleccionar el certificado que se enlazará al servidor VPN de capa 2. En la ventana <b>Cambiar certificado del servidor</b> , active <b>Validar certificado de servidor</b> , seleccione un certificado de servidor de la lista y haga clic en <b>Aceptar</b> .

- 3 Para configurar los sitios del mismo nivel, haga clic en la pestaña **Sitios de servidor**.
- 4 Haga clic en el botón **Agregar** ().
- 5 Configure los ajustes para un sitio del mismo nivel de VPN de capa 2.

Opción	Acción
Habilitado	Habilite este sitio del mismo nivel.
Nombre	Introduzca un nombre único para el sitio del mismo nivel.
Descripción	(Opcional) Escriba una descripción.
ID de usuario	Introduzca el nombre de usuario y la contraseña con los que se autenticará el sitio del mismo nivel.
Contraseña	
Confirmar contraseña	Las credenciales de usuario en el sitio del mismo nivel deben ser las mismas que las del lado cliente.

Opción	Acción
Interfaces extendidas	<p>Seleccione al menos una subinterfaz que se extenderá con el cliente.</p> <p>Las subinterfaces que se pueden seleccionar son aquellas redes de centros de datos virtuales de organización que se han configurado como subinterfaces en la puerta de enlace Edge.</p>
Dirección de puerta de enlace de optimización de salida	<p>(Opcional) Si la puerta de enlace predeterminada para máquinas virtuales es la misma en los dos sitios, introduzca las direcciones IP de puerta de enlace de las subinterfaces para las que desea enrutar o bloquear el tráfico de forma local en el túnel VPN de capa 2.</p>

6 Haga clic en **Conservar**.

7 Haga clic en **Guardar cambios**.

La operación para guardar puede tardar un minuto en completarse.

#### Pasos siguientes

Habilite el servicio VPN de capa 2 en esta puerta de enlace Edge. Consulte [Habilitar el servicio VPN de capa 2 en una puerta de enlace Edge](#).

## Configurar la puerta de enlace Edge como un cliente VPN de capa 2

El cliente VPN de capa 2 es la instancia de NSX Edge de origen que inicia la comunicación con la instancia de NSX Edge de destino (el servidor VPN de capa 2).

#### Requisitos previos

- [Desplazarse a la pantalla VPN de capa 2](#).
- Si este cliente VPN de capa 2 se conecta con un servidor VPN de capa 2 que usa un certificado de servidor, compruebe que el certificado de CA correspondiente esté cargado en la puerta de enlace Edge para habilitar la validación del certificado de servidor para este cliente VPN de capa 2. Consulte [Agregar un certificado de CA a la puerta de enlace Edge para la verificación de confianza de certificados SSL](#).

#### Procedimiento

- 1 En la pestaña **VPN de capa 2**, seleccione **Cliente** para el modo de VPN de capa 2.
- 2 En la pestaña **Cliente global**, ajuste los detalles de configuración global del cliente VPN de capa 2.

Opción	Descripción
Dirección de servidor	Introduzca la dirección IP del servidor VPN de capa 2 al que se conectará este cliente.
Puerto de servidor	<p>Introduzca el puerto del servidor VPN de capa 2 al que se debe conectar el cliente.</p> <p>El puerto predeterminado es 443.</p>
Algoritmo de cifrado	Seleccione el algoritmo de cifrado para comunicarse con el servidor.

Opción	Descripción
<b>Interfaces extendidas</b>	<p>Seleccione las subinterfaces que se ampliarán al servidor.</p> <p>Las subinterfaces que se pueden seleccionar son las redes de centros de datos virtuales de organización que se han configurado como subinterfaces en la puerta de enlace Edge.</p>
<b>Dirección de puerta de enlace de optimización de salida</b>	(Opcional) Si la puerta de enlace predeterminada para las máquinas virtuales es la misma en los dos sitios, escriba las direcciones IP de puerta de enlace de las subinterfaces o las direcciones IP a las que no debe fluir el tráfico a través del túnel.
<b>Detalles del usuario</b>	Introduzca el identificador de usuario y la contraseña para la autenticación con el servidor.

**3 Haga clic en **Guardar cambios**.**

La operación para guardar puede tardar un minuto en completarse.

**4 (opcional) Para configurar las opciones avanzadas, haga clic en la pestaña **Cliente avanzado**.**

**5 Si esta instancia de Edge de cliente VPN de capa 2 no tiene acceso directo a Internet y necesita llegar a la instancia de Edge de servidor VPN de capa 2 mediante un servidor proxy, especifique la configuración de proxy.**

Opción	Descripción
<b>Habilitar proxy seguro</b>	Seleccione esta opción para habilitar el proxy seguro.
<b>Dirección</b>	Introduzca la dirección IP del servidor proxy.
<b>Puerto</b>	Introduzca el puerto del servidor proxy.
<b>Nombre de usuario</b>	Introduzca las credenciales de autenticación del servidor proxy.
<b>Contraseña</b>	

**6 Para habilitar la validación de certificación de servidores, haga clic en **Cambiar certificado de CA** y seleccione el certificado de CA correspondiente.**

**7 Haga clic en **Guardar cambios**.**

La operación para guardar puede tardar un minuto en completarse.

**Pasos siguientes**

Habilite el servicio VPN de capa 2 en esta puerta de enlace Edge. Consulte [Habilitar el servicio VPN de capa 2 en una puerta de enlace Edge](#).



## Habilitar el servicio VPN de capa 2 en una puerta de enlace Edge

Cuando se configuran los ajustes obligatorios de VPN de capa 2, se puede habilitar el servicio VPN de capa 2 en la puerta de enlace Edge.

**Nota** Si ya se configuró HA en esta puerta de enlace Edge, asegúrese de que la puerta de enlace Edge contenga más de una interfaz interna configurada. Si existe una sola interfaz y ya ha sido utilizada para la capacidad HA, se producirá un error en la configuración de VPN de capa 2 en la misma interfaz interna.

### Requisitos previos

- Si esta puerta de enlace Edge es un servidor VPN de capa 2, la instancia de NSX Edge de destino, compruebe que se hayan configurado los ajustes obligatorios del servidor VPN de capa 2 y al menos un sitio del mismo nivel de VPN de capa 2. Consulte los pasos descritos en [Configurar la puerta de enlace Edge como un servidor VPN de capa 2](#).
- Si esta puerta de enlace Edge es un cliente VPN de capa 2, la instancia de NSX Edge de origen, compruebe que se hayan configurado los ajustes del cliente VPN de capa 2. Consulte los pasos descritos en [Configurar la puerta de enlace Edge como un cliente VPN de capa 2](#).
- [Desplazarse a la pantalla VPN de capa 2](#).

### Procedimiento

- 1 En la pestaña **VPN de capa 2**, haga clic en el botón de alternancia **Habilitar**.
- 2 Haga clic en **Guardar cambios**.

### Resultados

Se activará el servicio VPN de capa 2 de la puerta de enlace Edge.

### Pasos siguientes

Cree reglas de firewall o NAT en el lado del firewall orientado a Internet para que el servidor VPN de capa 2 pueda conectarse con el cliente VPN de capa 2.

## Quitar la configuración del servicio VPN de capa 2 de una puerta de enlace Edge

Es posible quitar la configuración existente del servicio VPN de capa 2 de la puerta de enlace Edge. Esta acción también deshabilita el servicio VPN de capa 2 en la puerta de enlace Edge.

### Requisitos previos

[Desplazarse a la pantalla VPN de capa 2](#)

### Procedimiento

- 1 Desplácese hasta la parte inferior de la pantalla VPN de capa 2 y haga clic en **Eliminar configuración**.

2 Para confirmar la eliminación, haga clic en **Aceptar**.

### Resultados

Se deshabilitará el servicio VPN de capa 2 y se quitarán los detalles de configuración de la puerta de enlace Edge.

## Administración de certificados SSL

El software NSX en el entorno de vCloud Director ofrece la capacidad de utilizar certificados de capa de sockets seguros (Secure Sockets Layer, SSL) con los túneles VPN-Plus de SSL y VPN de IPsec que se configuran para las puertas de enlace Edge.

Las puertas de enlace Edge del entorno de vCloud Director admiten certificados autofirmados, certificados firmados por una entidad de certificación (Certification Authority, CA) y certificados generados y firmados por una CA. Es posible generar solicitudes de firma de certificados (Certificate Signing Request, CSR), importar los certificados, administrar los certificados importados y crear listas de revocación de certificados (Certificate Revocation List, CRL).

## Acerca del uso de certificados con el centro de datos virtual de organización

Puede administrar certificados para las siguientes áreas de redes del centro de datos virtual de organización de vCloud Director.

- Los túneles VPN de IPsec entre una red de centros de datos virtuales de organización y una red remota.
- Las conexiones VPN-Plus de SSL entre usuarios remotos con redes privadas y recursos web del centro de datos virtual de organización.
- Un túnel VPN de 2 capas entre dos puertas de enlace Edge de NSX.
- Los servidores virtuales y los servidores de grupos configurados para el equilibrio de carga en el centro de datos virtual de organización.

## Cómo utilizar certificados de cliente

Puede crear un certificado de cliente mediante un comando CAI o una llamada de REST. A continuación, puede distribuir este certificado a los usuarios remotos, quienes pueden instalarlo en sus navegadores web.

La ventaja principal de la implementación de certificados de cliente consiste en que se puede almacenar un certificado de cliente de referencia para cada usuario remoto y se puede comparar con el certificado de cliente que presenta el usuario remoto. Para impedir que un usuario determinado se conecte en el futuro, puede eliminar el certificado de referencia de la lista de certificados de cliente del servidor de seguridad. Al eliminar el certificado, se denegarán las conexiones de ese usuario.

## Generar una solicitud de firma de certificado para una puerta de enlace Edge

Para poder solicitar un certificado firmado de una entidad de certificación o crear un certificado autofirmado, es necesario generar una solicitud de firma del certificado (Certificate Signing Request, CSR) para la puerta de enlace Edge.

Una solicitud CSR es un archivo codificado que se debe generar en una puerta de enlace NSX Edge para la que se requiere un certificado SSL. El uso de una CSR estandariza la manera en que las empresas envían sus claves públicas junto con la información para identificar sus nombres de empresa y nombres de dominio.

La solicitud CSR se genera con un archivo de clave privada coincidente que se debe conservar en la puerta de enlace Edge. La solicitud CSR contiene la clave pública coincidente y otros datos, como el nombre, la ubicación y el nombre de dominio de la organización.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Certificados**.
- 3 En la pestaña **Certificados**, haga clic en **CSR**.
- 4 Configure las siguientes opciones para la solicitud CSR:

Opción	Descripción
<b>Nombre común</b>	<p>Escriba el nombre de dominio completo (FQDN) de la organización para la que planea utilizar el certificado (por ejemplo, <code>www.ejemplo.com</code>).</p> <p>No incluya los prefijos <code>http://</code> ni <code>https://</code> en el nombre común.</p>
<b>Unidad de organización</b>	<p>Utilice este campo para distinguir entre las divisiones dentro de su organización de vCloud Director con las que se asocia este certificado. Por ejemplo, Ingeniería o Ventas.</p>
<b>Nombre de organización</b>	<p>Escriba el nombre con el que está registrada legalmente la empresa.</p> <p>La organización enumerada debe ser el responsable legal del registro del nombre de dominio en la solicitud de certificado.</p>
<b>Localidad</b>	<p>Escriba la ciudad o localidad donde se registró legalmente la empresa.</p>
<b>Nombre del estado o de la provincia</b>	<p>Escriba el nombre completo (no utilice abreviaturas) del estado, de la provincia, de la región o del territorio donde se registró legalmente la empresa.</p>
<b>Código de país</b>	<p>Escriba el nombre del país donde se registró legalmente la empresa.</p>
<b>Algoritmo de clave privada</b>	<p>Escriba el tipo de clave, RSA o DSA, para el certificado.</p> <p>Por lo general, se utiliza RSA. El tipo de clave define el algoritmo de cifrado para la comunicación entre los hosts.</p>
<p><b>Nota</b> VPN-Plus de SSL admite solamente certificados RSA.</p>	

Opción	Descripción
Tamaño de clave	<p>Escriba el tamaño de la clave en bits.</p> <p>El valor mínimo es de 2048 bits.</p>
Descripción	(Opcional) Escriba una descripción para el certificado.

**5** Haga clic en **Conservar**.

El sistema generará la solicitud CSR y agregará una nueva entrada con el tipo CSR a la lista en pantalla.

### Resultados

En la lista en pantalla, al seleccionar una entrada con el tipo CSR, se mostrarán los detalles de la CSR en la pantalla. Puede copiar los datos de la CSR con formato PEM que se muestran y enviarlos a una entidad de certificación (Certificate Authority, CA) para obtener un certificado firmado por CA.

### Pasos siguientes

Utilice la solicitud CSR para crear un certificado de servicio mediante una de estas dos opciones:

- Transmita la solicitud CSR a una entidad de certificación para obtener un certificado firmado por una CA. Cuando la entidad de certificación le envíe el certificado firmado, importe el certificado al sistema. Consulte [Importar el certificado firmado por CA correspondiente a la solicitud CSR generada para una puerta de enlace Edge](#).
- Utilice la solicitud CSR para crear un certificado autofirmado. Consulte [Configurar un certificado de servicio autofirmado](#).

## Importar el certificado firmado por CA correspondiente a la solicitud CSR generada para una puerta de enlace Edge

Después de generar una solicitud de firma del certificado (Certificate Signing Request, CSR) y obtener el certificado firmado por una entidad de certificación en función de esa CSR, puede importar el certificado firmado por CA para que lo utilice la puerta de enlace Edge.

### Requisitos previos

Compruebe que ha obtenido el certificado firmado por CA correspondiente a la solicitud CSR. Si la clave privada en el certificado firmado por CA no coincide con la de la CSR seleccionada, se producirá un error en el proceso de importación.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Certificados**.

- 3 Seleccione la solicitud CSR de la tabla en pantalla para la que desea importar el certificado firmado por CA.
- 4 Importe el certificado firmado.
  - a Haga clic en **Certificado firmado generado para CSR**.
  - b Proporcione los datos PEM del certificado firmado por CA.
    - Si los datos se encuentran en un archivo PEM en un sistema al que puede desplazarse, haga clic en el botón **Cargar** para buscar el archivo y seleccionarlo.
    - Si puede copiar y pegar los datos PEM, pegue los datos en el campo **Certificado firmado (formato PEM)**.

Incluya las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.
  - c (opcional) Escribir una descripción.
  - d Haga clic en **Conservar**.

---

**Nota** Si la clave privada en el certificado firmado por CA no coincide con la de la CSR seleccionada en la pantalla Certificados, se producirá un error en el proceso de importación.

---

## Resultados

El certificado firmado por CA con el tipo Certificado de servicio se mostrará en la lista en pantalla.

## Pasos siguientes

Adjunte el certificado firmado por CA a los túneles VPN-Plus de SSL o VPN de IPsec según sea necesario. Consulte [Configurar ajustes de un servidor VPN de SSL](#) y [Especificar la configuración de VPN de IPsec global](#).

## Configurar un certificado de servicio autofirmado

Puede configurar certificados de servicio autofirmados con las puertas de enlace Edge para utilizarlos en sus capacidades relacionadas con VPN. Puede crear, instalar y administrar certificados autofirmados.

Si el certificado de servicio se muestra en la pantalla Certificados, puede especificar ese certificado de servicio al configurar las opciones relacionadas con la VPN de la puerta de enlace Edge. VPN presenta el certificado de servicio especificado a los clientes con acceso a VPN.

## Requisitos previos

Compruebe que exista al menos una CSR disponible en la pantalla **Certificados** para la puerta de enlace Edge. Consulte [Generar una solicitud de firma de certificado para una puerta de enlace Edge](#).

## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Certificados**.
- 3 Seleccione la CSR en la lista que desea utilizar para este certificado autofirmado y haga clic en **Autofirmar CSR**.
- 4 Escriba la cantidad de días que será válido el certificado autofirmado.
- 5 Haga clic en **Conservar**.

El sistema generará un certificado autofirmado y agregará una nueva entrada con el tipo Certificado de servicio a la lista en pantalla.

## Resultados

El certificado autofirmado quedará disponible en la puerta de enlace Edge. En la lista en pantalla, al seleccionar una entrada con el tipo Certificado de servicio, se mostrarán sus detalles en la pantalla.

## Agregar un certificado de CA a la puerta de enlace Edge para la verificación de confianza de certificados SSL

Al agregar un certificado de CA a una puerta de enlace Edge, es posible verificar la confianza de los certificados SSL que se presentan a la puerta de enlace Edge para la autenticación, por lo general, los certificados de cliente que se utilizan en las conexiones de VPN a la puerta de enlace Edge.

Por lo general, se agrega el certificado raíz de la empresa o la organización como un certificado de CA. Un uso típico es VPN de SSL, donde se deben autenticar los clientes VPN con certificados. Los certificados de cliente pueden distribuirse a los clientes VPN y, cuando los clientes VPN se conectan, se validan sus certificados de cliente con el certificado de CA.

---

**Nota** Al agregar un certificado de CA, generalmente se configura una lista de revocación de certificados (Certificate Revocation List, CRL) relevante. La CRL protege contra los clientes que presentan certificados revocados. Consulte [Agregar una lista de revocación de certificados a una puerta de enlace Edge](#).

---

## Requisitos previos

Compruebe que los datos de certificado de CA se encuentran en formato PEM. En la interfaz de usuario, puede pegar los datos PEM del certificado de CA, o desplazarse hasta un archivo que contenga los datos y esté disponible en la red desde el sistema local.

## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Certificados**.
- 3 Haga clic en **Certificado de CA**.
- 4 Proporcione los datos del certificado de CA.
  - Si los datos se encuentran en un archivo PEM en un sistema al que puede desplazarse, haga clic en el botón **Cargar** para buscar el archivo y seleccionarlo.
  - Si puede copiar y pegar los datos PEM, pegue los datos en el campo **Certificado de CA (formato PEM)**.  
  
Incluya las líneas `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----`.
- 5 (opcional) Escribir una descripción.
- 6 Haga clic en **Conservar**.

## Resultados

El certificado de CA con el tipo Certificado de CA se mostrará en la lista en pantalla. Este certificado de CA ahora se puede especificar al configurar las opciones relacionadas con VPN de la puerta de enlace Edge.

## Agregar una lista de revocación de certificados a una puerta de enlace Edge

Una lista de revocación de certificados (Certificate Revocation List, CRL) es una lista de certificados digitales que la entidad de certificación (Certificate Authority, CA) emisora asegura se han revocado, a fin de que los sistemas se puedan actualizar para que no confíen en los usuarios que presenten dichos certificados revocados. Puede agregar CRL a la puerta de enlace Edge.

Como se describe en la *guía de administración de NSX*, la CRL contiene los siguientes elementos:

- Los certificados revocados y los motivos de la revocación
- Las fechas de emisión de los certificados
- Las entidades que emitieron los certificados
- Una fecha propuesta para la próxima versión

Cuando un usuario potencial intenta acceder a un servidor, el servidor permite o deniega el acceso basado en la entrada de CRL para ese usuario en particular.

## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Certificados**.
- 3 Haga clic en **CRL**.
- 4 Proporcione los datos de la CRL.
  - Si los datos se encuentran en un archivo PEM en un sistema al que puede desplazarse, haga clic en el botón **Cargar** para buscar el archivo y seleccionarlo.
  - Si puede copiar y pegar los datos PEM, pegue los datos en el campo **CRL (formato PEM)**.  
Incluya las líneas `-----BEGIN X509 CRL-----` y `-----END X509 CRL-----`.
- 5 (opcional) Escribir una descripción.
- 6 Haga clic en **Conservar**.

## Resultados

La CRL se mostrará en la lista en pantalla.

## Agregar un certificado de servicio a la puerta de enlace Edge

Cuando se agregan certificados de servicio a una puerta de enlace Edge, dichos certificados se pueden utilizar en la configuración relacionada con VPN de la puerta de enlace Edge. Es posible agregar un certificado de servicio a la pantalla **Certificados**.

### Requisitos previos

Compruebe que el certificado de servicio y su clave privada se encuentren en formato PEM. En la interfaz de usuario, puede pegar los datos PEM o desplazarse hasta un archivo que contenga los datos y esté disponible en la red desde el sistema local.

## Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Certificados**.
- 3 Haga clic en **Certificado de servicio**.
- 4 Introduzca los datos con formato PEM del certificado de servicio.
  - Si los datos se encuentran en un archivo PEM en un sistema al que puede desplazarse, haga clic en el botón **Cargar** para buscar el archivo y seleccionarlo.



- Si puede copiar y pegar los datos PEM, pegue los datos en el campo **Certificado de servicio (formato PEM)**.

Incluya las líneas -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.

5 Introduzca los datos con formato PEM de la clave privada del certificado.

- Si los datos se encuentran en un archivo PEM en un sistema al que puede desplazarse, haga clic en el botón **Cargar** para buscar el archivo y seleccionarlo.
- Si puede copiar y pegar los datos PEM, pegue los datos en el campo **Clave privada (formato PEM)**.

Incluya las líneas -----BEGIN RSA PRIVATE KEY----- y -----END RSA PRIVATE KEY-----.

6 Escriba una frase de contraseña de clave privada y confírmela.

7 (opcional) Escribir una descripción.

8 Haga clic en **Conservar**.

#### Resultados

El certificado con el tipo Certificado de servicio se mostrará en la lista en pantalla. Este certificado de servicio ahora se puede seleccionar al configurar las opciones relacionadas con VPN de la puerta de enlace Edge.

## Objetos de agrupamiento personalizados

El software NSX del entorno de vCloud Director proporciona la capacidad de definir conjuntos y grupos de determinadas entidades, que puede utilizar más adelante cuando especifique otras configuraciones relacionadas con la red, como en las reglas de firewall.

### Crear un conjunto de direcciones IP para usarlas en las reglas de firewall y la configuración de retransmisión de DHCP

Un conjunto de direcciones IP es un grupo de direcciones IP que se puede crear en el nivel de un centro de datos virtual de organización. Es posible utilizar un conjunto de direcciones IP como origen o destino en una regla de firewall o en una configuración de retransmisión de DHCP.

Para crear un conjunto de direcciones IP, utilice la página **Objetos de agrupamiento** del portal para tenants de vCloud Director. La página **Objetos de agrupamiento** está disponible en las pantallas Servicios y Puerta de enlace Edge.


## Procedimiento

- 1 Abra la página Objetos de agrupamiento.

Opción	Acción
<b>Abrir a través de servicios de puerta de enlace Edge</b>	<ol style="list-style-type: none"> <li>a Desplácese hasta <b>Redes &gt; Instancias de Edge</b>.</li> <li>b Seleccione la puerta de enlace Edge que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>c Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>
<b>Abrir a través de servicios de seguridad</b>	<ol style="list-style-type: none"> <li>a Desplácese hasta <b>Redes &gt; Seguridad</b>.</li> <li>b Seleccione el servicio de seguridad que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>c Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>

- 2 Haga clic en la pestaña **Conjuntos de direcciones IP**.

En la pantalla se muestran los conjuntos de direcciones IP que ya están definidos.

- 3 Para agregar un conjunto de direcciones IP, haga clic en el botón **Crear** ().
- 4 Introduzca un nombre y, si lo desea, una descripción para el conjunto de direcciones IP y las direcciones IP que desea incluir en el conjunto.
- 5 (opcional) Si desea especificar el conjunto de direcciones IP mediante la página **Objetos de agrupamiento** en la pantalla Servicios, utilice el botón de alternancia **Herencia** para habilitar la herencia y permitir la visibilidad en los alcances subyacentes.

Herencia está habilitada de forma predeterminada.

- 6 Para guardar este conjunto de direcciones IP, haga clic en **Conservar**.

## Resultados

El nuevo conjunto de direcciones IP puede seleccionarse como el origen o el destino en las reglas de firewall o en las configuraciones de retransmisión de DHCP.

## Crear un conjunto de direcciones MAC para utilizarlas en las reglas de firewall

Un conjunto de direcciones MAC es un grupo de direcciones MAC que se puede crear en un nivel de centro de datos virtual de una organización. Los conjuntos de direcciones MAC se pueden usar como origen o como destino en una regla de firewall.

Para crear un conjunto de direcciones MAC, utilice la página **Objetos de agrupamiento** del portal para tenants de vCloud Director. La página Objetos de agrupamiento está disponible en las pantallas **Servicios** y **Puerta de enlace Edge**.

## Procedimiento

- 1 Abra la página Objetos de agrupamiento.

Opción	Acción
<b>Abrir a través de servicios de puerta de enlace Edge</b>	<ol style="list-style-type: none"> <li>a Desplácese hasta <b>Redes &gt; Instancias de Edge</b>.</li> <li>b Seleccione la puerta de enlace Edge que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>c Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>
<b>Abrir a través de servicios de seguridad</b>	<ol style="list-style-type: none"> <li>a Desplácese hasta <b>Redes &gt; Seguridad</b>.</li> <li>b Seleccione el servicio de seguridad que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>c Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>

- 2 Haga clic en la pestaña **Conjuntos de direcciones MAC**.

En la pantalla se muestran los conjuntos de direcciones MAC que ya están definidos.

- 3 Para agregar un conjunto de direcciones MAC, haga clic en el botón **Crear** ()

- 4 Escriba un nombre para el conjunto, una descripción (opcional) y las direcciones MAC que se incluirán en el conjunto.

- 5 (opcional) Si va a especificar el conjunto de direcciones MAC mediante la página **Objetos de agrupamiento** en la pantalla **Servicios**, utilice el botón de alternancia **Herencia** para habilitar la herencia y permitir la visibilidad en alcances subyacentes.

Herencia está habilitada de forma predeterminada.

- 6 Para guardar el conjunto de direcciones MAC, haga clic en **Conservar**.

## Resultados

El nuevo conjunto de direcciones MAC puede seleccionarse como el origen o el destino en las reglas de firewall.

## Ver los servicios disponibles para reglas de firewall

Puede ver la lista de servicios disponibles para su uso en reglas de firewall. En este contexto, un servicio es una combinación de un protocolo y un puerto.

Puede ver los servicios disponibles en la página Objetos de agrupamiento del portal para tenants de vCloud Director. La página Objetos de agrupamiento está disponible en las pantallas Servicios y Puerta de enlace Edge.

No se pueden agregar nuevos servicios a la lista mediante el portal para tenants. El conjunto de servicios disponibles para su uso lo gestiona el administrador del sistema de vCloud Director.

## Procedimiento

- 1 Abra la página Objetos de agrupamiento.

Opción	Acción
<b>Abrir a través de servicios de puerta de enlace Edge</b>	<ol style="list-style-type: none"> <li>Desplácese hasta <b>Redes &gt; Instancias de Edge</b>.</li> <li>Seleccione la puerta de enlace Edge que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>
<b>Abrir a través de servicios de seguridad</b>	<ol style="list-style-type: none"> <li>Desplácese hasta <b>Redes &gt; Seguridad</b>.</li> <li>Seleccione el servicio de seguridad que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>

- 2 Haga clic en la pestaña **Servicios**.

## Resultados

Los servicios disponibles se muestran en la pantalla.

## Ver los grupos de servicios disponibles para reglas de firewall

Puede ver la lista de grupos de servicios disponibles para su uso en reglas de firewall. En este contexto, un servicio es una combinación de un protocolo y un puerto, mientras que un grupo de servicios incluye servicios u otros grupos de servicios.

Puede ver los grupos de servicios disponibles en la página Objetos de agrupamiento del portal para tenants de vCloud Director. La página Objetos de agrupamiento está disponible en las pantallas Servicios y Puerta de enlace Edge.

No se pueden crear grupos de servicios mediante el portal para tenants. El conjunto de grupos de servicios disponibles para su uso lo gestiona el administrador del sistema de vCloud Director.

## Procedimiento

- 1 Abra la página Objetos de agrupamiento.

Opción	Acción
<b>Abrir a través de servicios de puerta de enlace Edge</b>	<ol style="list-style-type: none"> <li>Desplácese hasta <b>Redes &gt; Instancias de Edge</b>.</li> <li>Seleccione la puerta de enlace Edge que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>
<b>Abrir a través de servicios de seguridad</b>	<ol style="list-style-type: none"> <li>Desplácese hasta <b>Redes &gt; Seguridad</b>.</li> <li>Seleccione el servicio de seguridad que desea editar y haga clic en <b>Configurar servicios</b>.</li> <li>Haga clic en <b>Objetos de agrupamiento</b>.</li> </ol>

- 2 Haga clic en la pestaña **Grupos de servicios**.

## Resultados

Los grupos de servicios disponibles se muestran en la pantalla. La columna Descripción muestra los servicios agrupados en cada grupo de servicios.

## Estadísticas y logs para una puerta de enlace Edge

Es posible ver las estadísticas y los logs de una puerta de enlace Edge.

### Ver estadísticas

Puede ver las estadísticas en la pantalla **Servicios de puerta de enlace Edge**.

#### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Estadísticas**.
- 3 Desplácese por las pestañas en función del tipo de estadísticas que desee ver.

Opción	Descripción
<b>Conexiones</b>	La pantalla Conexiones proporciona visibilidad operativa. Esta pantalla muestra gráficos sobre el tráfico que fluye en las interfaces de la puerta de enlace Edge seleccionada, así como estadísticas de conexión de los servicios de firewall y de equilibrador de carga. Seleccione el período para el que desea ver las estadísticas.
<b>VPN de IPsec</b>	La pantalla VPN de IPsec muestra el estado y las estadísticas de VPN de IPsec, así como el estado y las estadísticas de cada túnel.
<b>VPN de capa 2</b>	La pantalla VPN de capa 2 muestra el estado y las estadísticas de la VPN de capa 2.

### Habilitar registro

Es posible habilitar el registro de una puerta de enlace Edge. Además de habilitar el registro para las funciones de las que desea recopilar datos de registro, si desea completar la configuración, debe tener un servidor syslog para recibir los datos de registro recopilados. Cuando configura un servidor syslog en la pantalla Configuración de Edge, puede acceder a los datos registrados desde dicho servidor syslog.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

## Procedimiento

### 1 Abra los servicios de puerta de enlace Edge.

- a Desplácese hasta **Redes > Instancias de Edge**.
- b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.

### 2 En la pestaña **Configuración de Edge**, haga clic en el botón **Editar servidor syslog**.

Puede personalizar el servidor syslog para los registros relacionados con redes de la puerta de enlace Edge para los servicios que tienen habilitado el registro.

Si el administrador del sistema de vCloud Director ya configuró un servidor syslog para el entorno de vCloud Director, el sistema utilizará ese servidor syslog de forma predeterminada y mostrará su dirección IP en la pantalla **Configuración de Edge**.

### 3 Habilite el registro para cada función.

- En la pestaña **NAT**, haga clic en el botón **Regla DNAT** y active el botón de alternancia **Habilitar registro**.

Registra la traducción de direcciones.

- En la pestaña **NAT**, haga clic en el botón **Regla SNAT** y active el botón de alternancia **Habilitar registro**.

Registra la traducción de direcciones.

- En la pestaña **Enrutamiento**, haga clic en **Configuración de enrutamiento** y, en Configuración de enrutamiento dinámico, active el botón de alternancia **Habilitar registro**.

Registra las actividades de enrutamiento dinámico. En el menú desplegable **Nivel de registro**, puede seleccionar el límite inferior del nivel de estado de mensaje para registrar.

- En la pestaña **Equilibrador de carga**, haga clic en **Configuración global** y active el botón de alternancia **Habilitar registro**.

Registra el flujo de tráfico del equilibrador de carga. En el menú desplegable **Nivel de registro**, puede seleccionar el límite inferior del nivel de estado de los mensajes que desea registrar.

- En la pestaña **VPN**, vaya a **VPN de IPSec > Configuración de registro** y active el botón de alternancia **Habilitar registro**.

Registra el flujo de tráfico entre la subred local y una subred del mismo nivel. En el menú desplegable **Nivel de registro**, puede seleccionar el límite inferior del nivel de estado de mensaje para registrar.

- En la pestaña **VPN-Plus de SSL**, haga clic en **Configuración general** y active el botón de alternancia **Habilitar registro**.

Mantiene un registro del tráfico que pasa a través de la puerta de enlace VPN de SSL.

- En la pestaña **VPN-Plus de SSL**, haga clic en **Configuración del servidor** y active el botón de alternancia **Habilitar registro**.

Registra las actividades que se producen en el servidor de VPN de SSL para syslog. En el menú desplegable **Nivel de registro**, puede seleccionar el límite inferior del nivel de estado de los mensajes que desea registrar.

## Habilitar el acceso de la línea de comandos SSH a una puerta de enlace Edge

Es posible habilitar el acceso de línea de comandos SSH a una puerta de enlace Edge.

### Procedimiento

- 1 Abra los servicios de puerta de enlace Edge.
  - a Desplácese hasta **Redes > Instancias de Edge**.
  - b Seleccione la puerta de enlace Edge que desea editar y haga clic en **Configurar servicios**.
- 2 Haga clic en la pestaña **Configuración de Edge**.
- 3 Configure los ajustes de SSH.

Opción	Descripción
<b>Nombre de usuario</b>	Introduzca las credenciales para el acceso de SSH a esta puerta de enlace Edge.
<b>Contraseña</b>	De forma predeterminada, el nombre de usuario de SSH es <b>admin</b> .
<b>Vuelva a escribir la contraseña</b>	
<b>Caducidad de contraseña</b>	Introduzca el período de caducidad de la contraseña (en días).
<b>Titular de inicio de sesión</b>	Introduzca el texto que se mostrará a los usuarios cuando inicien una conexión de SSH a la puerta de enlace Edge.

- 4 Active el botón de alternancia **Habilitado**.

### Pasos siguientes

Configure las reglas de firewall o NAT correspondientes para permitir un acceso SSH a esta puerta de enlace Edge.

## Trabajar con etiquetas de seguridad

Las etiquetas de seguridad son etiquetas que se pueden asociar a una máquina virtual o a un grupo de máquinas virtuales. Las etiquetas de seguridad están diseñadas para usarse con grupos de seguridad. Una vez que se crean las etiquetas de seguridad, estas se asocian a un grupo de seguridad que se puede utilizar en reglas de firewall. Puede crear, editar o asignar una etiqueta de seguridad definida por el usuario. También puede ver las máquinas virtuales o los grupos de seguridad a los que se ha aplicado una etiqueta de seguridad determinada.


Un caso de uso común para las etiquetas de seguridad consiste en agrupar objetos de forma dinámica para simplificar las reglas de firewall. Por ejemplo, puede crear varias etiquetas de seguridad diferentes en función del tipo de actividad que espera que se produzca en una máquina virtual determinada. Crea una etiqueta de seguridad para los servidores de base de datos y otra para los servidores de correo electrónico. A continuación, aplica la etiqueta adecuada a las máquinas virtuales que alojan servidores de base de datos o servidores de correo electrónico. Posteriormente, puede asignar la etiqueta a un grupo de seguridad y escribir una regla de firewall correspondiente a ella, en la que aplica una configuración de seguridad diferente dependiendo de si la máquina virtual ejecuta un servidor de base de datos o un servidor de correo electrónico. Más adelante, si cambia la funcionalidad de la máquina virtual, puede quitarla de la etiqueta de seguridad en lugar de modificar la regla de firewall.

## Crear y asignar etiquetas de seguridad

Puede crear una etiqueta de seguridad y asignarla a una máquina virtual o a un grupo de máquinas virtuales.

Cree una etiqueta de seguridad y asígnela a una máquina virtual o a un grupo de máquinas virtuales.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 Haga clic en el botón **Crear** () e introduzca un nombre para la etiqueta de seguridad.
- 5 (opcional) Escriba una descripción para la etiqueta de seguridad.
- 6 (opcional) Asigne la etiqueta de seguridad a una máquina virtual o a un grupo de máquinas virtuales.

En el menú desplegable **Examinar objetos del tipo**, la opción **Máquinas virtuales** está seleccionada de forma predeterminada.

- a Seleccione una máquina virtual del panel de la izquierda.
- b Para asignar la etiqueta de seguridad a la máquina virtual seleccionada, haga clic en la flecha derecha.

La máquina virtual se mueve al panel de la derecha se le asigna la etiqueta de seguridad.

- 7 Cuando termine de asignar la etiqueta a las máquinas virtuales seleccionadas, haga clic en **Conservar**.



## Resultados

Se crea la etiqueta de seguridad y, si se ha elegido esta opción, se asigna a las máquinas virtuales seleccionadas.

## Pasos siguientes

Las etiquetas de seguridad están diseñadas para funcionar con un grupo de seguridad. Para obtener más información sobre cómo crear grupos de seguridad, consulte [Crear un grupo de seguridad](#).

## Cambiar la asignación de etiquetas de seguridad

Después de crear una etiqueta de seguridad, puede asignarla manualmente a las máquinas virtuales. También puede editar una etiqueta de seguridad para quitarla de las máquinas virtuales a las que ya se ha asignado.

Si ha creado las etiquetas de seguridad, puede asignarlas a las máquinas virtuales. Puede utilizar etiquetas de seguridad con el fin de agrupar máquinas virtuales para escribir reglas de firewall. Por ejemplo, puede asignar una etiqueta de seguridad a un grupo de máquinas virtuales con datos altamente confidenciales.

## Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea editar y

haga clic en el botón **Editar** ()

- 5 Seleccione máquinas virtuales del panel de la izquierda y asígneles la etiqueta de seguridad haciendo clic en la flecha derecha.

Las máquinas virtuales del panel de la derecha se asignan a la etiqueta de seguridad.

- 6 Seleccione máquinas virtuales del panel de la derecha y quíteles la etiqueta haciendo clic en la flecha izquierda.

Las máquinas virtuales en el panel de la izquierda no tienen la etiqueta de seguridad asignada.

- 7 Cuando haya terminado de agregar los cambios, haga clic en **Conservar**.

## Resultados

La etiqueta de seguridad se asigna a las máquinas virtuales seleccionadas.

### Pasos siguientes

Las etiquetas de seguridad están diseñadas para funcionar con un grupo de seguridad. Para obtener más información sobre cómo crear grupos de seguridad, consulte [Crear un grupo de seguridad](#).

## Ver las etiquetas de seguridad aplicadas

Puede ver las etiquetas de seguridad aplicadas a máquinas virtuales del entorno. También puede ver las etiquetas de seguridad aplicadas a grupos de seguridad en el entorno.

### Requisitos previos

Se debe haber creado una etiqueta de seguridad y debe haberse aplicado a una máquina virtual o a un grupo de seguridad.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Vea las etiquetas asignadas en la pestaña **Etiquetas de seguridad**.
  - a En la pestaña **Etiquetas de seguridad**, elija la etiqueta de seguridad para la que desea ver asignaciones y haga clic en el icono **Editar**.
  - b En **Asignar/desasignar MV** puede ver la lista de máquinas virtuales asignadas a la etiqueta de seguridad.
  - c Haga clic en **Descartar**.
- 4 Vea las etiquetas asignadas en la pestaña **Grupos de seguridad**.
  - a Haga clic en la pestaña **Objetos de agrupamiento** y haga clic en **Grupos de seguridad**.
  - b Seleccione un grupo de seguridad.
  - c En la lista bajo **Incluir miembros**, puede ver la etiqueta de seguridad asignada a un grupo de seguridad.

### Resultados


Puede ver las etiquetas de seguridad existentes, así como las máquinas virtuales y los grupos de seguridad asociados. De este modo, puede determinar una estrategia de creación de reglas de firewall basadas en etiquetas y grupos de seguridad.

## Editar una etiqueta de seguridad

Puede editar una etiqueta de seguridad definida por el usuario.

Si cambia el entorno o la función de una máquina virtual, es aconsejable que utilice una etiqueta de seguridad diferente para que las reglas de firewall sean correctas en la nueva configuración de máquina. Por ejemplo, si tiene una máquina virtual en la que ya no almacena datos confidenciales, se aconseja asignar una etiqueta de seguridad diferente para que las reglas de firewall que se aplican a datos confidenciales ya no se ejecuten en la máquina virtual.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea editar.
- 5 Haga clic en el botón **Editar** ().
- 6 Edite el nombre y la descripción de la etiqueta de seguridad.
- 7 Asigne la etiqueta a las máquinas virtuales que seleccione o elimine la asignación de estas.
- 8 Para guardar los cambios, haga clic en **Conservar**.

#### Pasos siguientes

Si edita una etiqueta de seguridad, es posible que también deba editar reglas de firewall o un grupo de seguridad asociado. Para obtener más información acerca de los grupos de seguridad, consulte [Trabajar con grupos de seguridad](#).

## Eliminar una etiqueta de seguridad

Puede eliminar una etiqueta de seguridad definida por el usuario.

Es aconsejable eliminar una etiqueta de seguridad si cambia la función o el entorno de la máquina virtual. Por ejemplo, si tiene una etiqueta de seguridad para bases de datos de Oracle, pero decide utilizar un servidor de base de datos diferente, puede quitar la etiqueta de seguridad para que las reglas de firewall que se aplican a las bases de datos de Oracle ya no se ejecuten en la máquina virtual.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Redes**, seleccione **Seguridad**.
- 2 Seleccione un servicio de seguridad y haga clic en **Configurar servicios**.
- 3 Haga clic en la pestaña **Etiquetas de seguridad**.
- 4 En la lista de etiquetas de seguridad, seleccione la etiqueta de seguridad que desea eliminar.

5 Haga clic en el botón **Eliminar** ().

6 Para confirmar la eliminación, haga clic en **Aceptar**.

#### Resultados

Se eliminará la etiqueta de seguridad.

#### Pasos siguientes

Si elimina una etiqueta de seguridad, es posible que también deba editar las reglas de firewall o un grupo de seguridad asociado. Para obtener más información acerca de los grupos de seguridad, consulte [Trabajar con grupos de seguridad](#).

## Trabajar con grupos de seguridad

Un grupo de seguridad es una colección de activos u objetos de agrupamiento, como máquinas virtuales, redes de centros de datos virtuales de organización o etiquetas de seguridad.

Los grupos de seguridad pueden tener criterios de pertenencia dinámica basados en etiquetas de seguridad, nombre de máquina virtual, nombre de sistema operativo invitado de máquina virtual o nombre de host invitado de máquina virtual. Por ejemplo, todas las máquinas virtuales que tengan la etiqueta de seguridad “web” se agregarán automáticamente a un grupo de seguridad específico destinado a servidores web. Después de crear un grupo de seguridad, se aplica una política de seguridad a dicho grupo.

## Crear un grupo de seguridad

Puede crear grupos de seguridad definidos por el usuario.


#### Requisitos previos

Si desea utilizar etiquetas de seguridad con los grupos de seguridad, [Crear y asignar etiquetas de seguridad](#).

#### Procedimiento

- 1 Abra los servicios de seguridad.
  - a Desplácese hasta **Redes > Seguridad**.
  - b Seleccione el VDC de organización en el que desea aplicar la configuración de seguridad y haga clic en **Configurar servicios**.


El portal para tenants abrirá Servicios de seguridad.
- 2 Desplácese hasta **Objetos de agrupamiento > Grupos de seguridad**.

Se abrirá la página **Grupos de seguridad**.
- 3 Haga clic en el botón **Crear** (.

- 4 Escriba un nombre y, si lo desea, una descripción para el grupo de seguridad.

La descripción se muestra en la lista de grupos de seguridad, por lo que agregar una descripción significativa puede facilitar la rápida identificación del grupo de seguridad.

- 5 (opcional) Agregue un conjunto de miembros dinámicos.

- a Haga clic en el botón **Agregar** () que aparece en Conjuntos de miembros dinámicos.
- b Seleccione **Cualquiera** o **Todo** para buscar coincidencias con cualquiera de los criterios de la instrucción o con todos ellos, respectivamente.
- c Introduzca el primer objeto para el que se buscarán coincidencias.  
Las opciones son **Etiqueta de seguridad**, **Nombre de SO invitado de MV**, **Nombre de MV** y **Nombre de host invitado de MV**.
- d Seleccione un operador, por ejemplo, **Contiene**, **Comienza con** o **Termina con**.
- e Introduzca un valor.
- f (opcional) Para agregar otra instrucción, use un operador booleano **And** u **Or**.

- 6 (opcional) Incluya miembros.

- a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
- b Para incluir un objeto en la lista Incluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.

- 7 (opcional) Excluya miembros.

- a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
- b Para incluir un objeto en la lista Excluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.

- 8 Haga clic en **Conservar** para guardar los cambios.

La operación puede tardar un minuto en completarse.

## Resultados

Ahora es posible utilizar el grupo de seguridad en reglas (por ejemplo, reglas de firewall).

## Editar un grupo de seguridad

Puede editar los grupos de seguridad definidos por el usuario.

## Procedimiento

- 1 Abra los servicios de seguridad.
  - a Desplácese hasta **Redes > Seguridad**.
  - b Seleccione el VDC de organización en el que desea aplicar la configuración de seguridad y haga clic en **Configurar servicios**.

El portal para tenants abrirá Servicios de seguridad.

- 2 Desplácese hasta **Objetos de agrupamiento > Grupos de seguridad**.


Se abrirá la página **Grupos de seguridad**.

- 3 Seleccione el grupo de seguridad que desea editar.


Debajo de la lista de grupos de seguridad se muestran los detalles del grupo de seguridad.

- 4 (opcional) Edite el nombre y la descripción del grupo de seguridad.


- 5 (opcional) Agregue un conjunto de miembros dinámicos.



- a Haga clic en el botón **Agregar** () que aparece en **Conjuntos de miembros dinámicos**.
- b Seleccione **Cualquiera** o **Todo** para buscar coincidencias con cualquiera de los criterios de la instrucción o con todos ellos, respectivamente.
- c Introduzca el primer objeto para el que se buscarán coincidencias.

Las opciones son **Etiqueta de seguridad**, **Nombre de SO invitado de MV**, **Nombre de MV** y **Nombre de host invitado de MV**.
- d Seleccione un operador, por ejemplo, **Contiene**, **Comienza con** o **Termina con**.
- e Introduzca un valor.
- f (opcional) Para agregar otra instrucción, use un operador booleano **And** u **Or**.

- 6 (opcional) Para editar un conjunto de miembros dinámicos, haga clic en el icono **Editar** () que aparece junto al conjunto de miembros que desee modificar.

- a Aplique los cambios necesarios al conjunto de miembros dinámicos.
- b Haga clic en **Aceptar**.


- 7 (opcional) Para eliminar un conjunto de miembros dinámicos, haga clic en el icono **Eliminar** () que aparece junto al conjunto de miembros que desee borrar.

- 8 (opcional) Para editar la lista de miembros incluidos, haga clic en el icono **Editar** () que aparece junto a la lista Incluir miembros.
  - a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
  - b Para incluir un objeto en la lista Incluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.
  - c Para excluir un objeto de la lista Incluir miembros, seleccione el objeto del panel derecho y muévelo al panel izquierdo haciendo clic en la flecha izquierda.
- 9 (opcional) Para editar la lista de miembros excluidos, haga clic en el icono **Editar** () que aparece junto a la lista Excluir miembros.
  - a En el menú desplegable **Examinar objetos del tipo**, seleccione el tipo de objetos, como **Máquinas virtuales**, **Redes de VDC de organización**, **Conjuntos de direcciones IP**, **Conjuntos de direcciones MAC** o **Etiquetas de seguridad**.
  - b Para incluir un objeto en la lista Excluir miembros, seleccione el objeto del panel izquierdo y muévelo al panel derecho haciendo clic en la flecha derecha.
  - c Para excluir un objeto de la lista Excluir miembros, seleccione el objeto del panel derecho y muévelo al panel izquierdo haciendo clic en la flecha izquierda.
- 10 Haga clic en **Guardar cambios**.  
Se guardarán los cambios realizados en el grupo de seguridad.

## Eliminar un grupo de seguridad

Puede eliminar un grupo de seguridad definido por el usuario.

### Procedimiento

- 1 Abra los servicios de seguridad.
  - a Desplácese hasta **Redes > Seguridad**.
  - b Seleccione el VDC de organización en el que desea aplicar la configuración de seguridad y haga clic en **Configurar servicios**.  
El portal para tenants abrirá Servicios de seguridad.
- 2 Desplácese hasta **Objetos de agrupamiento > Grupos de seguridad**.  
Se abrirá la página **Grupos de seguridad**.
- 3 Seleccione el grupo de seguridad que desea eliminar.
- 4 Haga clic en el botón **Eliminar** ()
- 5 Para confirmar la eliminación, haga clic en **Aceptar**.

## Resultados

Se eliminará el grupo de seguridad.



# Usar discos independientes y revisar políticas de almacenamiento

## 7

Para crear y administrar discos independientes y revisar las políticas de almacenamiento del centro de datos virtual de organización, puede usar el portal para tenants de vCloud Director.

Este capítulo incluye los siguientes temas:

- [Crear y usar discos independientes](#)
- [Revisar las propiedades de la política de almacenamiento](#)

## Crear y usar discos independientes

Los discos independientes son discos virtuales autónomos que se crean en los VDC de organización. Los **administradores de la organización** y los usuarios que tengan los derechos correspondientes pueden crear, quitar y actualizar discos independientes, así como conectarlos a máquinas virtuales.

Cuando crea un disco independiente, este se asocia con un VDC de organización, pero no con una máquina virtual. Después de crear el disco en un VDC, un administrador o el propietario del disco pueden asociarlo a cualquier máquina virtual implementada en el VDC mediante vCloud API.

El propietario del disco también puede modificar las propiedades del disco, desasociarlo de una máquina virtual y quitarlo del VDC. Los **administradores del sistema** y los **administradores de la organización** tienen los mismos derechos que el propietario del disco para usarlo y modificarlo.

## Crear un disco independiente

Puede crear un disco independiente y asociarlo a una máquina virtual en otro momento.

Para crear un disco independiente, debe especificar el nombre y el tamaño de este. Si lo desea, puede incluir una descripción y especificar un perfil de almacenamiento para que lo use el disco.

### Requisitos previos

Debe tener una función **Administrador de organización** o derechos de propietario de disco.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, seleccione **Discos independientes** en el panel izquierdo.

- 2 Haga clic en **Nuevo**.
- 3 Introduzca un nombre y, si lo desea, una descripción del disco.
- 4 Seleccione la política de almacenamiento del menú desplegable **Política de almacenamiento**.
- 5 Introduzca el tamaño del disco independiente en bytes.
- 6 Seleccione el tipo y el subtipo de bus de los menús desplegables **Tipo de bus** y **Subtipo de bus**, respectivamente, y haga clic en **Guardar**.

#### Pasos siguientes

Utilice la API de vCloud para adjuntar el disco independiente a una máquina virtual. Consulte *Guía de programación de vCloud API para proveedores de servicios* en [VMware {code}](#).

## Editar un disco independiente

Después de crear el disco, puede modificar el nombre, la descripción, la política de almacenamiento y el tamaño de este.

#### Requisitos previos

Debe tener una función **Administrador de organización** o derechos de propietario de disco.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, seleccione **Discos independientes** en el panel izquierdo.
- 2 Seleccione el disco que desea modificar y haga clic en **Editar**.
- 3 Edite la configuración, como el nombre, la descripción, la política de almacenamiento y el tamaño en bytes.
- 4 Haga clic en **Guardar**.

## Eliminar un disco independiente

#### Requisitos previos

Debe tener una función **Administrador de organización** o derechos de propietario de disco.

#### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar y, en **Almacenamiento**, seleccione **Discos independientes** en el panel izquierdo.
- 2 Seleccione el disco que desea eliminar y haga clic en **Eliminar**.
- 3 Haga clic en **Aceptar**.

## Revisar las propiedades de la política de almacenamiento

Puede revisar las políticas de almacenamiento y sus detalles.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar.
- 2 En **Almacenamiento**, haga clic en **Políticas de almacenamiento**.  
Aparecerá la lista de las políticas de almacenamiento disponibles.
- 3 Para ver los detalles de una política de almacenamiento, haga clic en el nombre de esta.
- 4 Revise los detalles en las pestañas **General** y **Metadatos**, y haga clic en **Aceptar**.

# Revisar las propiedades del centro de datos virtual



Como **administrador de organización**, puede revisar las propiedades del centro de datos virtual.

Este capítulo incluye los siguientes temas:

- [Revisar las propiedades del centro de datos virtual](#)
- [Revisar los metadatos del centro de datos virtual](#)

## Revisar las propiedades del centro de datos virtual

Puede revisar las propiedades de los centros de datos virtuales asignados a la organización.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar.
- 2 En **Configuración**, haga clic en **General**.

### Resultados

Puede revisar las propiedades del centro de datos virtual, como el nombre, la descripción y el estado. La información de métricas sobre el centro de datos incluye modelo de asignación, vCPU y uso de memoria y CPU.

## Revisar los metadatos del centro de datos virtual

vCloud Director ofrece un componente de uso general para asociar metadatos definidos por el usuario con un objeto. Si el administrador del sistema ha creado metadatos para el centro de datos virtual de la organización, puede revisar los metadatos del centro de datos de la organización.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En la pantalla del panel **Centros de datos virtuales**, haga clic en la tarjeta del centro de datos virtual que desea explorar.
- 2 En **Configuración**, haga clic en **Metadatos**.  
Aparecerá la lista de los metadatos disponibles.

# Trabajar con SDDC y proxies de SDDC

## 9

A partir de vCloud Director 9.7, se puede acceder a un entorno de vCenter Server desde vCloud Director. vCloud Director puede actuar como un servidor proxy HTTP y proporcionar acceso a los componentes del entorno de vSphere subyacente.

En vCloud Director, un centro de datos definido por software (Software-Defined Data Center, SDDC) encapsula un entorno de vCenter Server completo. Un SDDC puede incluir uno o varios proxies de SDDC que proporcionan acceso a diferentes componentes del entorno subyacente. El **administrador del sistema** puede publicar uno o varios SDDC en su organización. Puede usar los proxies de SDDC contenedores para acceder a la interfaz de usuario o a la API de los componentes con proxy.

Este capítulo incluye los siguientes temas:

- [Configurar el navegador con la configuración de proxy](#)
- [Activar o desactivar un proxy de SDDC](#)
- [Iniciar sesión en la interfaz de usuario de un componente de SDDC con proxy](#)

## Configurar el navegador con la configuración de proxy

Para poder acceder a la interfaz de usuario de un componente de vSphere con proxy, debe configurar el navegador para que use los proxies de SDDC publicados en su organización.

Para configurar el navegador para que use los proxies de SDDC publicados, descargue e importe un archivo .PAC.

---

**Nota** Deberá repetir este procedimiento cada vez que el **administrador del sistema** publique un SDDC de su organización (o bien elimine su publicación), así como cada vez que el **administrador del sistema** agregue o elimine un proxy del SDDC. Cuando el conjunto de SDDC y los proxies de SDDC se modifican, también lo hace el archivo .PAC.

---


Si algunos componentes con proxy utilizan certificados autofirmados, deberá agregar los certificados al navegador.

### Requisitos previos

- Compruebe si el **administrador del sistema** publicó al menos una instancia de vCenter Server dedicada y habilitada en su organización.

- Compruebe si el **administrador del sistema** publicó **SDDC\_VIEW** y los derechos **Token: administrar** en la organización, y si su función incluye estos derechos.
- Compruebe si el **administrador del sistema** publicó y habilitó el complemento de la **extensión CPOM** en su organización. Este complemento proporciona la función para ver y utilizar centros de datos de vSphere dedicados en vCloud Director Tenant Portal.

#### Procedimiento

- 1 En el menú principal () , seleccione **Centros de datos**.
- 2 En el panel **SDDC**, haga clic en **Descargar configuración de proxy (.PAC)**.
- 3 Configure el navegador para que utilice el archivo **.PAC** descargado.  
Consulte las instrucciones de usuario del navegador.
- 4 En la tarjeta del SDDC de destino, haga clic en **Activar proxy predeterminado**.
- 5 Si el componente con proxy predeterminado utiliza certificados autofirmados, agréguelos al navegador.
  - a En la tarjeta del SDDC de destino, haga clic en **Más** y, a continuación, haga clic en **Descargar certificado de proxy predeterminado (.PEM)**.
  - b Importe el certificado **.PEM** descargado al navegador.  
Consulte las instrucciones de usuario del navegador.
- 6 Si un componente con proxy que no es predeterminado utiliza certificados autofirmados, agréguelos al navegador.
  - a En la tarjeta del SDDC de destino, haga clic en **Más** y en **Administrar proxies**.
  - b Si el proxy de destino no está activado, seleccione el botón de radio junto al nombre del proxy y haga clic en **Activar**.
  - c Seleccione el botón de radio junto al nombre de proxy de destino y haga clic en **Descargar certificado (.PEM)**.
  - d Importe el certificado **.PEM** descargado al navegador.  
Consulte las instrucciones de usuario del navegador.

## Activar o desactivar un proxy de SDDC

Para generar un token a fin de acceder a un componente de SDDC con proxy, se debe activar este proxy. Se activará un proxy para la sesión de usuario actual. Si se desactiva un proxy o se agota el tiempo de espera de la sesión de usuario, el proxy deja de estar activo y el token deja de funcionar.

---


**Nota** Es posible que existan limitaciones sobre la cantidad de servidores proxy activos simultáneos. Para obtener información, consulte al **administrador del sistema**.

---

### Requisitos previos

Si desea activar un proxy, compruebe que el **administrador del sistema** haya habilitado este proxy.

### Procedimiento

- 1 En el menú principal () , seleccione **Centros de datos**.
- 2 Active un proxy.
  - Para activar el proxy predeterminado, en la tarjeta del SDDC de destino, haga clic en **Activar proxy predeterminado**.
  - Para activar un proxy que no sea el predeterminado, siga estos pasos:
    - a En la tarjeta del SDDC de destino, haga clic en **Más** y, a continuación, haga clic en **Administrar servidores proxy**.
    - b Seleccione el botón de radio junto al nombre del proxy de destino y haga clic en **Activar**.
- 3 Desactive un proxy.
  - Para desactivar el proxy predeterminado, en la tarjeta del SDDC de destino, haga clic en **Más** y, a continuación, haga clic en **Desactivar proxy predeterminado**.
  - Para activar un proxy que no sea el predeterminado:
    - a En la tarjeta del SDDC de destino, haga clic en **Más** y, a continuación, haga clic en **Administrar servidores proxy**.
    - b Seleccione el botón de radio junto al nombre del proxy de destino y haga clic en **Desactivar**.

### Resultados

Si activó un proxy, [Iniciar sesión en la interfaz de usuario de un componente de SDDC con proxy](#).


## Iniciar sesión en la interfaz de usuario de un componente de SDDC con proxy

Es posible acceder a la interfaz de usuario de un componente de SDDC con proxy mediante una cuenta de vCloud Director.

### Requisitos previos

- [Configurar el navegador con la configuración de proxy](#)
- Active el proxy de destino. Consulte [Activar o desactivar un proxy de SDDC](#).

### Procedimiento

- 1 En el menú principal () , seleccione **Centros de datos**.



## 2 Abra el proxy.

- Para abrir el proxy predeterminado, haga clic en **Copiar token de acceso y abrir**.
- Para abrir un proxy que no sea el predeterminado, siga estos pasos:
  - En la tarjeta del SDDC de destino, haga clic en **Más** y, a continuación, haga clic en **Administrar servidores proxy**.
  - Haga clic en el botón de radio junto al proxy de destino y, a continuación, haga clic en **Copiar token de acceso y abrir**.

El token de acceso se copiará en el portapapeles. Se abrirá una nueva pestaña y se le solicitará la autenticación en el proxy.

## 3 En el cuadro de texto **Nombre de usuario**, introduzca el nombre de usuario de vCloud Director y el nombre de su organización con el formato *vCD\_user\_name@organization\_name*.

Por ejemplo, **johndoe@orgOne**.

## 4 En el cuadro de texto **Contraseña**, pegue el token de acceso copiado.

## 5 Haga clic en **Aceptar**.

### Resultados

Se abrirá la interfaz de usuario del componente con proxy.

# Trabajar con plantillas de vApp

# 10

Una plantilla de vApp es una imagen de máquina virtual cargada con un sistema operativo, aplicaciones y datos. Estas plantillas garantizan que las máquinas virtuales estén configuradas correctamente en toda la organización. Las plantillas de vApp se añaden a los catálogos.

Este capítulo incluye los siguientes temas:

- [Ver una plantilla de vApp](#)
- [Crear una plantilla de vApp desde un archivo OVF](#)
- [Descargar una plantilla de vApp](#)
- [Eliminar una plantilla de vApp](#)

## Ver una plantilla de vApp

Puede ver la lista de plantillas de vApp disponibles en los catálogos a los que tiene acceso. Puede ver una plantilla de vApp y explorar las máquinas virtuales que contiene.

Puede acceder solo a las plantillas de vApp que se incluyen en los elementos de catálogo que se han compartido con usted. Para obtener más información acerca del uso compartido de catálogos, consulte [Compartir un catálogo](#).


### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Plantillas de vApp** en el panel izquierdo.


La lista de plantillas se muestra en una vista de cuadrícula.

- 2 (opcional) Configure la vista de cuadrícula para que contenga los elementos que desea ver.
  - a En la vista de cuadrícula, haga clic en el icono de editor de cuadrícula (  ) que aparece debajo de la lista de plantillas de vApp.
  - b Seleccione los elementos que desea incluir en la vista de cuadrícula, como la versión, el estado, el catálogo, el propietario, etc.
  - c Haga clic en **Aceptar**.

La cuadrícula muestra los elementos seleccionados para cada plantilla de vApp en la lista.

- 3 Para ver las máquinas virtuales incluidas en una plantilla de vApp, haga clic en el nombre de la plantilla de vApp.

Las máquinas virtuales que se incluyen en la plantilla de vApp se muestran en una cuadrícula.

- 4 (opcional) Para seleccionar los elementos que desea ver en la vista de cuadrícula, haga clic en el icono de editor de cuadrícula (  ) que aparece debajo de la lista de máquinas virtuales.
  - a Seleccione los elementos que desea incluir en la vista de cuadrícula.
  - b Haga clic en **Aceptar**.

## Crear una plantilla de vApp desde un archivo OVF

Puede cargar un paquete OVF para crear una plantilla de vApp en un catálogo.

vCloud Director admite las especificaciones de Open Virtualization Format (OVF) y Open Virtualization Appliance (OVA). Si carga un archivo OVF que incluya propiedades OVF para personalizar sus máquinas virtuales, dichas propiedades se conservarán en la plantilla de vApp. Para obtener más información acerca de la creación de paquetes OVF, consulte la *Guía del usuario de herramientas OVF* y la *Guía del usuario de VMware vCenter Converter*.

### Requisitos previos


Esta operación requiere los derechos incluidos en la función **Autor de catálogo** predefinida o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal (  ), seleccione **Bibliotecas** y elija **Plantillas de vApp** en el panel izquierdo.

La lista de plantillas se muestra en una vista de cuadrícula.

- 2 Haga clic en **Agregar**.

- 3 Introduzca una dirección URL para el archivo OVF o haga clic en el icono **Cargar** () para ir hasta una ubicación accesible desde el equipo y, a continuación, seleccione el archivo de plantilla OVF/OVA.  
  
La ubicación puede ser el disco duro local, un recurso compartido de red o una unidad de CD/DVD. Las extensiones de archivo admitidas incluyen `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` y `.strings`. Si opta por cargar un archivo OVF, que hace referencia a más archivos de los que intenta cargar, por ejemplo, un archivo VMDK, debe examinar y seleccionar todos los archivos.
- 4 Verifique los detalles de la plantilla OVF/OVA que va a implementar y haga clic en **Siguiente**.
- 5 Introduzca un nombre y, si lo desea, una descripción de la plantilla de vApp y haga clic en **Siguiente**.
- 6 En el menú desplegable **Catálogo**, seleccione el catálogo al que desea agregar la plantilla.
- 7 Revise la configuración de la plantilla de vApp y haga clic en **Finalizar**.

#### Resultados

La nueva plantilla de vApp aparecerá en la vista de cuadrícula de plantillas.



## Descargar una plantilla de vApp

Puede descargar una plantilla de vApp desde un catálogo como un archivo OVA en la máquina local.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Autor de catálogo** predefinida o un conjunto de derechos equivalente.

#### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Plantillas de vApp** en el panel izquierdo.  
  
La lista de plantillas se muestra en una vista de cuadrícula.
- 2 Haga clic en la barra de listas () que se encuentra a la izquierda de la plantilla de vApp que desea descargar y seleccione **Descargar**.

---

**Nota** Puede descargar plantillas de vApp de los catálogos de la organización. Si es administrador de la organización, puede descargar plantillas de vApp de un catálogo público. De lo contrario, el botón **Descargar** estará atenuado.

---

- 3 (opcional) Para preservar los UUID y las direcciones MAC de las máquinas virtuales en el paquete OVA descargado, active la casilla de verificación **Proteger información de identidad**.

- 4 Haga clic en **Aceptar** y espere hasta que finalice la descarga.

El archivo OVA se guarda en la ubicación de descarga predeterminada del navegador web.

## Eliminar una plantilla de vApp

Puede eliminar una plantilla de vApp de un catálogo de organización. Si el catálogo está publicado, la plantilla de vApp también se eliminará de los catálogos públicos.


### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Autor de vApp** predefinida o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Plantillas de vApp** en el panel izquierdo.

La lista de plantillas se muestra en una vista de cuadrícula.

- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda de la plantilla de vApp que desea eliminar y seleccione **Eliminar**.

- 3 Confirme la eliminación.

La plantilla de vApp eliminada se quitará de la vista de cuadrícula.

# Trabajar con archivos de medios

# 11

Un catálogo permite cargar, copiar, mover o editar las propiedades de los archivos de medios.

Este capítulo incluye los siguientes temas:

- [Cargar archivos de medios](#)
- [Eliminar un archivo de medios](#)
- [Descargar un archivo de medios](#)



## Cargar archivos de medios

Puede cargar en un catálogo nuevos archivos de medios o versiones nuevas de los archivos de medios existentes. Los usuarios con acceso al catálogo pueden abrir los archivos de medios con sus máquinas virtuales.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Medios y otros** en el panel izquierdo.  
La lista de archivos de medios se muestra en una vista de cuadrícula.
- 2 Haga clic en **Agregar**.
- 3 En el menú desplegable **Catálogo**, seleccione el catálogo en el que desea cargar el archivo de medios.
- 4 Introduzca un nombre para el archivo de medios.  
Si no introduce un nombre, el cuadro de texto de nombre se rellenará automáticamente con el nombre del archivo de medios.
- 5 Haga clic en el icono de carga () para examinar y seleccionar el archivo de imagen de disco (por ejemplo, un archivo `.iso`).

## 6 Haga clic en **Aceptar**.

Cuando se inicie la carga, el archivo de medios aparecerá en la cuadrícula.

### Pasos siguientes

En función del tamaño del archivo, la carga podría tardar en completarse. Puede supervisar el estado de la carga en la vista **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).



## Eliminar un archivo de medios

Puede eliminar del catálogo los archivos de medios que ya no desee utilizar.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Medios y otros** en el panel izquierdo.  
La lista de archivos de medios se muestra en una vista de cuadrícula.
- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda del archivo de medios que desea eliminar y seleccione **Eliminar**.
- 3 Confirme la eliminación.  
El archivo de medios eliminado se quitará de la vista de cuadrícula.


## Descargar un archivo de medios


Puede descargar un archivo de medios desde un catálogo.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Medios y otros** en el panel izquierdo.  
La lista de archivos de medios se muestra en una vista de cuadrícula.

- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda del archivo de medios que desea descargar y seleccione **Descargar**.

Se inicia la tarea de descarga y el archivo se guarda en la ubicación de descarga predeterminada del navegador web.

#### **Pasos siguientes**

En función de cuál sea el tamaño del archivo, esta descarga podría tardar algún tiempo en completarse. Puede supervisar el estado de la descarga en el panel **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).



# Trabajar con catálogos

# 12

Un catálogo es el lugar donde se guardan plantillas de vApp y archivos de medios en una organización. Los administradores de organización y los autores de catálogos pueden crear catálogos en una organización. El contenido del catálogo se puede compartir con otros usuarios u organizaciones de la instalación de vCloud Director, o bien se puede publicar de forma externa para que puedan acceder a él las organizaciones fuera de la instalación de vCloud Director.

vCloud Director contiene catálogos privados, compartidos y de acceso externo. Los catálogos privados incluyen plantillas de vApp y los archivos de medios que puede compartir con otros usuarios de la organización. Si un administrador del sistema habilita el uso compartido de catálogos para la organización, podrá compartir un catálogo de organización para crear un catálogo al que puedan acceder otras organizaciones de la instalación de vCloud Director. Si un administrador del sistema habilita la publicación externa de catálogos para la organización, puede publicar un catálogo de organización para que puedan acceder a él organizaciones fuera de la instalación de vCloud Director. Una organización fuera de la instalación de vCloud Director debe suscribirse a un catálogo publicado de forma externa para poder acceder a su contenido.

Puede cargar un paquete OVF directamente a un catálogo, guardar una vApp como una plantilla de vApp o importar una plantilla de vApp desde vSphere. Consulte [Crear una plantilla de vApp desde un archivo OVF](#) y [Guardar una vApp como plantilla de vApp en un catálogo](#).

Los miembros de una organización pueden acceder a plantillas de vApp y a archivos de medios que son propios o que se han compartido con ellos. Los administradores de organización y administradores del sistema pueden compartir un catálogo con todos los socios de una organización o con usuarios y grupos específicos de una organización. Consulte [Compartir un catálogo](#).

Este capítulo incluye los siguientes temas:

- [Ver catálogos](#)
- [Crear un catálogo](#)
- [Compartir un catálogo](#)
- [Eliminar un catálogo](#)
- [Administrar metadatos de un catálogo](#)
- [Publicar un catálogo](#)
- [Suscribirse a un catálogo externo](#)




- [Actualizar la dirección URL de ubicación y la contraseña de un catálogo suscrito](#)
- [Sincronizar un catálogo suscrito](#)

## Ver catálogos

Puede acceder a catálogos compartidos con usted en la organización. Puede acceder a catálogos públicos si un administrador de la organización ha hecho que sean accesibles en la organización.

El acceso al catálogo se controla mediante el uso compartido de catálogos, no mediante los derechos de su función. Puede acceder únicamente a los catálogos o los elementos de catálogo que se han compartido con usted. Para obtener más información, consulte [Compartir un catálogo](#).

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.
- 2 (Opcional) Configure la vista de cuadrícula para que contenga los elementos que desea ver.
  - a En la vista de cuadrícula, haga clic en el icono del editor de cuadrícula () que aparece debajo de la lista de catálogos.
  - b Seleccione los elementos que desea incluir en la vista de cuadrícula, como la versión, la descripción, el estado, etc.
  - c Haga clic en **Aceptar**.
 La cuadrícula muestra los elementos seleccionados para cada catálogo.
- 3 (Opcional) En la vista de cuadrícula, use la barra de listas () para mostrar las acciones que puede realizar en cada catálogo.  
Por ejemplo, puede compartir o eliminar un catálogo.


## Crear un catálogo

Puede crear catálogos nuevos y asociarlos con una política de almacenamiento.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.
- 2 Haga clic en **Nuevo** para crear un catálogo nuevo.

- 3 Escriba el nombre y, si lo desea, una descripción del catálogo.
- 4 (opcional) Determine si desea asignar una política de almacenamiento al catálogo y elija una.
- 5 Haga clic en **Aceptar**.

#### Resultados

El catálogo nuevo aparecerá en la vista de cuadrícula en la pestaña **Catálogos**.

## Compartir un catálogo

Puede compartir un catálogo con todos los miembros de la organización o con miembros específicos.


#### Requisitos previos

- Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.
- Debe ser el propietario del catálogo.

#### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.

La lista de catálogos se muestra en una vista de cuadrícula.

- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda del catálogo que desea compartir y seleccione **Compartir**.

La lista de usuarios que pueden acceder al catálogo se muestra en la vista de cuadrícula de la ventana **Compartir catálogo**.

- 3 Haga clic en **Agregar** para compartir el catálogo con otros usuarios.

Opción	Descripción
Compartir con todos en esta organización	Conceda acceso a todos los usuarios y los grupos de la organización.
Compartir con usuarios y grupos específicos	Seleccione los usuarios o los grupos a quienes desee conceder acceso al catálogo y haga clic en <b>Agregar</b> .

#### 4 Seleccione el nivel de acceso.

Opción	Descripción
<b>Solo lectura</b>	Los usuarios que pueden acceder a este catálogo tienen acceso de lectura a las plantillas de vApp y los archivos ISO del catálogo.
<b>Leer/escribir</b>	Los usuarios que pueden acceder a este catálogo tienen acceso de lectura a las plantillas de vApp y los archivos ISO del catálogo, y pueden agregar al catálogo plantillas de vApp y archivos ISO.
<b>Control total</b>	Los usuarios con acceso a este catálogo tienen control total sobre el contenido y la configuración del catálogo.

#### 5 Haga clic en **Aceptar**.

Los usuarios o los grupos que ahora pueden acceder al catálogo aparecen en la vista de cuadrícula del cuadro de diálogo **Compartir catálogo**.

#### 6 (opcional) Elija compartir el acceso de solo lectura con los administradores de todas las demás organizaciones.

#### 7 Haga clic en **Guardar**.

#### Resultados

En la pestaña **Catálogos**, cambiará el estado Compartido de este catálogo en la vista de cuadrícula.

## Eliminar un catálogo

Puede eliminar un catálogo de una organización.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Autor de catálogo** o un conjunto de derechos equivalente.

**Nota** El catálogo no debe contener plantillas de vApp ni archivos de medios. Puede mover estos elementos a otro catálogo o eliminarlos.

#### Procedimiento

#### 1 En el menú principal () , seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.

La lista de catálogos se muestra en una vista de cuadrícula.

#### 2 Haga clic en la barra de listas () que se encuentra a la izquierda del catálogo que desea eliminar y seleccione **Eliminar**.



#### 3 Confirme la eliminación.

El elemento de catálogo eliminado se quitará de la vista de cuadrícula.

## Administrar metadatos de un catálogo

Como **administrador de organización** o **propietario de catálogo**, puede crear o actualizar los metadatos de los catálogos que posea.

### Procedimiento

- 1 En el menú principal (  ), seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.
- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda de un catálogo y seleccione **Metadatos**.  
Los metadatos del catálogo seleccionado se mostrarán en una vista de cuadrícula.
- 3 (opcional) Para agregar metadatos, haga clic en **Agregar**.
  - a Introduzca el nombre de los metadatos.  
Este debe ser diferente de los nombres de los metadatos asociados a este objeto.
  - b Seleccione el tipo de metadatos, como **Texto**, **Número**, **Fecha y hora** o **Sí o No**.
  - c Introduzca el valor de los metadatos.
  - d Haga clic en **Guardar**.
- 4 (opcional) Actualice los metadatos existentes.  
No se puede actualizar el nombre de los metadatos.
  - a Actualice el tipo de metadatos.
  - b Introduzca un nuevo valor de metadatos.
  - c Haga clic en **Guardar**.
- 5 (opcional) Elimine los metadatos existentes.
  - a Haga clic en el icono Eliminar.
  - b Haga clic en **Guardar**.

## Publicar un catálogo

Si el **administrador del sistema** le ha otorgado acceso a catálogos, podrá publicar un catálogo de forma externa para hacer que sus plantillas de vApp y archivos de medios estén disponibles para que puedan suscribirse organizaciones fuera de la instalación de vCloud Director.

### Requisitos previos

Compruebe que el **administrador del sistema** ha habilitado la publicación de catálogos externos para la organización y le ha otorgado acceso a los catálogos.

### Procedimiento

- 1 En el menú principal (≡), seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.
- 2 Haga clic en la barra de listas (⋮) que se encuentra a la izquierda del catálogo que desea publicar y seleccione **Publicar configuración**.
- 3 Seleccione **Habilitar publicación** y, si lo desea, escriba una contraseña para acceder al catálogo.  
Únicamente se admiten caracteres ASCII.
- 4 Haga clic en **Guardar**.

## Suscribirse a un catálogo externo

Puede suscribirse a un catálogo externo y, por tanto, crear una copia de solo lectura de un catálogo publicado de forma externa. No puede modificar los catálogos suscritos.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- El **administrador del sistema** debe conceder a su organización permiso para poder suscribirse a catálogos externos.

### Procedimiento

- 1 En el menú principal (≡), seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.
- 2 Haga clic en **Nuevo** para crear un catálogo nuevo.
- 3 Escriba el nombre y, si lo desea, una descripción del catálogo.
- 4 Elija suscribirse a un catálogo externo y proporcione la dirección URL de suscripción.
- 5 Escriba la contraseña opcional para acceder al catálogo.
- 6 Determine si desea descargar automáticamente el contenido del catálogo externo.
- 7 Haga clic en **Aceptar**.



## Actualizar la dirección URL de ubicación y la contraseña de un catálogo suscrito

Después de crear un catálogo suscrito, puede actualizar la URL de ubicación y la contraseña del catálogo suscrito.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Debe haber creado un catálogo suscrito.
- El **administrador del sistema** debe conceder a su organización permiso para poder suscribirse a catálogos externos.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.
- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda de un catálogo suscrito y seleccione **Configuración de suscripción**.  
Si no se trata de un catálogo suscrito, la opción aparecerá atenuada.
- 3 Actualice la dirección URL de ubicación y la contraseña para este catálogo suscrito.
- 4 Determine si desea descargar automáticamente el contenido del catálogo externo.
- 5 Haga clic en **Guardar**.

## Sincronizar un catálogo suscrito


Después de crear un catálogo suscrito, puede sincronizarlo con el catálogo original para determinar si hay cambios. Por ejemplo, si cambian los metadatos del catálogo original, cuando realiza la sincronización, se actualizan los metadatos del catálogo suscrito.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Debe haber creado un catálogo suscrito.
- El **administrador del sistema** debe conceder a su organización permiso para poder suscribirse a catálogos externos.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Catálogos** en el panel izquierdo.  
La lista de catálogos se muestra en una vista de cuadrícula.

- 2 Haga clic en la barra de listas (  ) que se encuentra a la izquierda de un catálogo suscrito y seleccione **Sincronizar**.

Si no se trata de un catálogo suscrito, la opción aparecerá atenuada.

El catálogo suscrito se sincronizará con el original.



# Trabajar con plantillas de centros de datos virtuales de organización

# 13

Como administrador de organización o si es titular de cualquier función que tiene derechos para ver y crear instancias de plantillas de centro de datos virtual de organización, puede crear centros de datos virtuales de organización adicionales.

Una plantilla de centro de datos virtual de organización especifica una configuración para un centro de datos virtual de organización y, de forma opcional, una puerta de enlace Edge y una red de centros de datos virtuales de organización. Los administradores del sistema pueden permitir a los administradores de organización crear estos recursos en sus organizaciones. Para ello crearán plantillas de centros de datos virtuales de organización y las compartirán con estas organizaciones.

Al crear y compartir plantillas de centros de datos virtuales, los administradores del sistema pueden habilitar el aprovisionamiento de autoservicio de centros de datos virtuales de organización a la vez que conservan el control administrativo sobre la asignación de recursos del sistema como, por ejemplo, centros de datos virtuales de proveedor y redes externas.

Los administradores del sistema crean plantillas de centro de datos virtual de organización y proporcionan a diferentes organizaciones acceso a las plantillas mediante la interfaz web de vCloud Director. Consulte *Gestionar plantillas de centros de datos virtuales de organización* en la *Guía del Administrador de vCloud Director*. Si se ha proporcionado a su organización acceso a plantillas de centro de datos virtual, puede utilizar el portal para tenants de vCloud Director para crear centros de datos virtuales a partir de las plantillas disponibles.

Este capítulo incluye los siguientes temas:

- [Ver plantillas disponibles del centro de datos virtual](#)
- [Crear un centro de datos virtual a partir de una plantilla](#)

## Ver plantillas disponibles del centro de datos virtual

Puede ver las plantillas de centro de datos virtual de organización que un administrador del sistema ha creado para usted.

Vea las plantillas de centro de datos virtual antes de crear un nuevo centro de datos virtual de organización a partir de una plantilla de centro de datos virtual.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Administrador de organización** o una función que tenga derechos para ver y crear instancias de plantillas de centros de datos virtuales de organización.

### Procedimiento

- ◆ En el menú principal () , seleccione **Bibliotecas** y elija **Plantillas de VDC** en el panel izquierdo.

La lista de plantillas de centros de datos virtuales se muestra en una vista de cuadrícula.

### Pasos siguientes

Revise las descripciones de las plantillas de centro de datos virtual de organización y seleccione la plantilla desde la que desea crear un nuevo centro de datos virtual de organización.

## Crear un centro de datos virtual a partir de una plantilla

Puede crear un centro de datos virtual de organización a partir de una plantilla de centros de datos virtuales que el administrador del sistema haya creado.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función predefinida **Administrador de organización** o una función que tenga derechos para ver y crear instancias de plantillas de centros de datos virtuales de organización.

### Procedimiento

- 1 En el menú principal () , seleccione **Bibliotecas** y elija **Plantillas de VDC** en el panel izquierdo.

La lista de plantillas de centros de datos virtuales se muestra en una vista de cuadrícula.

- 2 Seleccione una plantilla y haga clic en **Nuevo VDC**.
- 3 Introduzca un nombre del centro de datos virtual y, si lo desea, una descripción.
- 4 Haga clic en **Crear**.

### Resultados

Se genera una instancia de creación del nuevo centro de datos virtual de organización, la que puede tardar unos minutos. Puede ver el progreso de la tarea en el panel **Tareas recientes**.

### Pasos siguientes

Puede administrar el centro de datos virtual de organización recién creado mediante la creación de máquinas virtuales y vApps, la administración de la configuración de red y seguridad, entre otras acciones.

# Administración de usuarios, grupos y funciones

# 14

Puede agregar administradores de organización a vCloud Director de forma individual o como parte de un grupo LDAP. También puede agregar y modificar las funciones que determinan los derechos que tiene un usuario dentro de su organización.

---

**Importante** Debe ser un **administrador de organización** para administrar usuarios, grupos y funciones dentro de la organización. El **administrador del sistema** puede publicar una o varias funciones globales para el tenant y, como **administrador de organización**, puede verlas en la lista de roles. Esas funciones son, por ejemplo, **Autor de catálogo**, **Autor de vApp**, **Usuario de vApp**, **Administrador de organización**, etc. No puede modificar las funciones de tenant globales predefinidas, pero puede crear y actualizar funciones de tenant personalizadas similares, y asignarlas a los usuarios dentro de su tenant.

---

Este capítulo incluye los siguientes temas:

- [Administración de usuarios](#)
- [Administración de grupos](#)
- [Funciones y derechos](#)

## Administración de usuarios

Desde el portal para tenants, es posible crear, editar, importar y eliminar usuarios. Además, también se pueden desbloquear las cuentas de usuario si un usuario intentó iniciar sesión con una contraseña incorrecta y, como resultado, bloqueó su propia cuenta de usuario.


### Crear un usuario

Puede crear un usuario dentro de la organización de vCloud Director.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.

- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.  
Se muestra la lista de usuarios.
- 3 Haga clic en **Crear**.
- 4 (opcional) Introduzca un nombre de usuario y la configuración de contraseña del usuario.  
La longitud mínima de contraseña es de seis caracteres.
- 5 Seleccione si desea habilitar el usuario tras la creación.
- 6 Seleccione la función que desea asignar al usuario.

El menú **Funciones disponibles** consta de una lista de funciones predefinidas y las funciones personalizadas que usted o el administrador del sistema pueden haber creado.

Función predefinida	Descripción
<b>Autor de vApp</b>	Los derechos asociados a la función predefinida <b>Autor de vApp</b> permiten a un usuario usar catálogos y crear vApps.
<b>Solo acceso a la consola</b>	Los derechos asociados a la función predefinida <b>Solo acceso a la consola</b> permiten a un usuario ver el estado y las propiedades de máquinas virtuales, así como utilizar el sistema operativo invitado.
<b>Usuario de vApp</b>	Los derechos asociados a la función predefinida <b>Usuario de vApp</b> permiten a un usuario utilizar vApps existentes.
<b>Administrador de organización</b>	Un usuario con la función predefinida <b>Administrador de organización</b> puede utilizar el portal para tenants de vCloud Director o vCloud API para administrar usuarios y grupos en la organización y asignarles funciones, incluida la función predefinida <b>Administrador de organización</b> . Un <b>administrador de organización</b> puede utilizar vCloud API para crear o actualizar objetos de función que son locales para la organización. Otras organizaciones no pueden ver las funciones que un <b>administrador de organización</b> haya creado o modificado.
<b>Aplazar a proveedor de identidad</b>	Los derechos asociados a la función predefinida <b>Aplazar a proveedor de identidad</b> se determinan en función de la información aportada por el proveedor de identidad OAuth o SAML del usuario. Para poder ser incluido cuando se asigna a un usuario la función <b>Aplazar a proveedor de identidad</b> , el nombre de función suministrado por el proveedor de identidad debe coincidir con una función o un nombre definidos en la organización de manera exacta, y con distinción de mayúsculas y minúsculas.
<b>Autor de catálogo</b>	Los derechos asociados a la función predefinida <b>Autor de catálogo</b> permiten a un usuario crear y publicar catálogos.

- 7 (opcional) Introduzca la información de contacto, como el nombre, la dirección de correo electrónico, el número de teléfono y el identificador de mensajería instantánea.
- 8 (opcional) Introduzca la cuota de máquina virtual para el usuario.  
La cuota determina cuántas máquinas virtuales y máquinas virtuales en ejecución puede administrar el usuario. Seleccione **Sin límite** si desea proporcionar al usuario un número ilimitado de máquinas virtuales.
- 9 Haga clic en **Guardar**.


## Importar usuarios

Para agregar usuarios a las organizaciones, puede importar un usuario LDAP o un usuario SAML, y asignarles una función determinada.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Compruebe que cuenta con una conexión válida a un servidor LDAP o que [Capítulo 15 Habilitar el uso de un proveedor de identidad SAML en la organización](#). Para obtener información, consulte *Guía del administrador de vCloud Director*.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.  
Se muestra la lista de usuarios.
- 3 Haga clic en **Importar usuarios**.
- 4 Seleccione el origen desde el que desea importar los usuarios.

Solo verá el servidor SAML o el servidor LDAP de origen que configuró como proveedor de identidad.

Origen	Acción
LDAP	<p>Importe usuarios de un servidor LDAP.</p> <ol style="list-style-type: none"> <li>a Introduzca un nombre completo o parcial en el cuadro de texto y haga clic en <b>Buscar</b>.</li> <li>b Seleccione los usuarios que desea importar y haga clic en <b>Agregar</b>.</li> </ol>
SAML	<p>Importe usuarios de un servidor SAML. Introduzca los nombres de los usuarios que desea importar.</p> <p>Los nombres de usuario deben tener el formato de identificador de nombre que admita el proveedor de identidad SAML configurado para esta organización.</p> <p><b>Nota</b> Si utiliza vCenter Single Sign-On como proveedor de identidad SAML, los nombres de usuario que importe de un dominio de vCenter Single Sign-On deben tener el formato de nombre principal de usuario (User Principal Name, UPN); por ejemplo, jdoe@mydomain.com.</p> <p>Utilice una línea nueva para cada nombre de usuario.</p>

- 5 Seleccione la función que desea asignar a los usuarios que va a importar.
- 6 Haga clic en **Guardar**.


## Modificar un usuario

Como administrador de organización, puede modificar la contraseña, el contacto y los ajustes de cuota de la máquina virtual de un usuario existente. Además, también puede cambiar la función del usuario.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.  
Se muestra la lista de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del usuario que desea editar y haga clic en **Modificar**.
- 4 Actualice la configuración que desee modificar.
  - a Cambie la contraseña según sea necesario.
  - b Seleccione si desea habilitar o deshabilitar el usuario.
  - c Actualice la función de usuario.
  - d Actualice la información de contacto, como el nombre, la dirección de correo electrónico, el número de teléfono y el identificador de mensajería instantánea.
  - e Edite la cuota de máquina virtual para el usuario.
- 5 Haga clic en **Guardar**.


## Deshabilitar o habilitar una cuenta de usuario

Puede deshabilitar una cuenta de usuario para evitar que el usuario inicie sesión en vCloud Director. Para eliminar un usuario, primero debe deshabilitar su cuenta.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.  
Se muestra la lista de usuarios.

- 3 Para deshabilitar una cuenta de usuario, haga clic en el botón de radio junto al nombre de usuario, haga clic en **Deshabilitar** confirme que desea deshabilitar la cuenta.
- 4 Para habilitar una cuenta de usuario que ya ha deshabilitado, haga clic en el botón de radio junto al nombre de usuario y haga clic en **Habilitar**.


## Eliminar un usuario

Puede eliminar un usuario de la organización de vCloud Director si elimina la cuenta de usuario.

### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Deshabilite la cuenta que desea eliminar.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.  
Se muestra la lista de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del usuario que desea eliminar y haga clic en **Eliminar**.
- 4 Para confirmar que desea eliminar la cuenta de usuario, haga clic en **Aceptar**.


## Desbloquear una cuenta de usuario bloqueada

Si se habilitó una política de bloqueo en la organización de vCloud Director, se bloquea una cuenta de usuario tras un número determinado de intentos de inicio de sesión no válidos. Puede desbloquear la cuenta de usuario bloqueada. La práctica recomendada es cambiar la contraseña del usuario y desbloquear la cuenta.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Usuarios**.  
Se muestra la lista de usuarios.
- 3 Haga clic en el botón de radio junto al nombre de usuario y seleccione **Desbloquear**.

## Administración de grupos

Si tiene una conexión válida a un servidor LDAP o ha habilitado la organización para que utilice un proveedor de identidad SAML, puede importar un grupo LDAP o un grupo SAML. También se puede editar o eliminar un grupo importado.


### Importar un grupo

Para agregar un grupo de usuarios, puede importar un grupo LDAP o un grupo SAML.

#### Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Compruebe que cuenta con una conexión válida a un servidor LDAP o que [Capítulo 15 Habilitar el uso de un proveedor de identidad SAML en la organización](#). Para obtener información, consulte *Guía del administrador de vCloud Director*.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.  
Se muestra la lista de grupos de usuarios.
- 3 Haga clic en **Importar grupo**.
- 4 Seleccione el origen desde el que desea importar el grupo de usuarios.

Solo verá el servidor SAML o el servidor LDAP de origen que configuró como proveedor de identidad.

Origen	Acción
LDAP	<p>Importe usuarios de un servidor LDAP.</p> <ol style="list-style-type: none"> <li>a Introduzca un nombre completo o parcial en el cuadro de texto y haga clic en <b>Buscar</b>.</li> <li>b Seleccione los usuarios que desea importar y haga clic en <b>Agregar</b>.</li> </ol>
SAML	<p>Importe grupos de usuarios de un servidor SAML. Introduzca los nombres de los grupos que desea importar.</p> <p>Utilice una línea nueva para cada nombre de grupo.</p>

- 5 Seleccione la función que desea asignar al grupo de usuarios que va a importar.
- 6 Haga clic en **Guardar**.

### Eliminar un grupo

Puede eliminar un grupo de la organización de vCloud Director si elimina su grupo LDAP.




Cuando se elimina un grupo LDAP, los usuarios que tienen una cuenta vCloud Director basada solo en su pertenencia al grupo se deshabilitan y no pueden iniciar sesión.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.  
Se muestra la lista de grupos de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del grupo que desea eliminar y haga clic en **Eliminar**.
- 4 Para confirmar que desea eliminar el grupo, haga clic en **Aceptar**.


## Editar un grupo

Puede editar un grupo desde el portal para tenants de vCloud Director.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Grupos**.  
Se muestra la lista de grupos de usuarios.
- 3 Haga clic en el botón de radio junto al nombre del grupo que desea eliminar y, luego, haga clic en **Editar**.
- 4 Edite el grupo según sea necesario.
  - a Cambie la descripción.
  - b Cambie la función de los miembros del grupo según sea necesario.
- 5 Haga clic en **Guardar**.

## Funciones y derechos

vCloud Director utiliza funciones y derechos para determinar las acciones que un usuario puede realizar en una organización. vCloud Director incluye una serie de funciones predefinidas con derechos específicos.

Los **administradores del sistema** y los **administradores de organización** deben asignar una función a cada usuario o grupo. El mismo usuario puede tener una función diferente en organizaciones diferentes. Los **administradores del sistema** pueden crear funciones y modificar las funciones existentes para todo el sistema, mientras que los **administradores de organización** solo pueden crear y modificar funciones para la organización que administran.

El portal para tenants de vCloud Director permite a los **administradores de organización** administrar las funciones de su organización. Si un **Administrador del sistema** publica en su organización una o varias funciones de tenant predefinidas, como **administrador de organización**, podrá ver esas funciones pero no podrá modificarlas. Sin embargo, puede crear funciones de tenant personalizadas con derechos similares y asignarlas a los usuarios dentro de su organización.

Para obtener más información acerca de las funciones predefinidas y sus derechos, consulte [Funciones predeterminadas y sus derechos](#).

## Funciones predeterminadas y sus derechos

Cada función predefinida de vCloud Director contiene un conjunto predeterminado de derechos necesarios para realizar las operaciones incluidas en los flujos de trabajo más comunes. De forma predeterminada, todas las funciones de tenant globales predefinidas se publican en todas las organizaciones del sistema.

### Funciones de proveedor predefinidas

De forma predeterminada, las funciones de proveedor que únicamente son locales en la organización de proveedor son las funciones **Administrador del sistema** y **Sistema multisitio**. Los **administradores del sistema** pueden crear funciones de proveedor personalizadas adicionales.

#### Administrador del sistema

La función **Administrador del sistema** solo existe en la organización del proveedor. La función **Administrador del sistema** incluye todos los derechos del sistema. Las credenciales de **Administrador del sistema** se establecen durante el proceso de instalación y configuración. Un **Administrador del sistema** puede crear cuentas adicionales de usuario y de administrador del sistema en la organización de proveedor.

#### Sistema multisitio

Se utiliza para ejecutar el proceso de latido para implementaciones multisitio. Esta función solo tiene un derecho, **Multisitio: Operaciones del sistema**, el cual le permite realizar una solicitud de vCloud API que recupera el estado del miembro remoto de una asociación de sitios.

## Funciones globales de tenant predefinidas

De forma predeterminada, las funciones globales de tenant predefinidas y los derechos que contienen se publican en todas las organizaciones. Los **Administradores del sistema** pueden cancelar la publicación de derechos y funciones globales de tenant en organizaciones individuales. Los **Administradores del sistema** pueden editar o eliminar funciones globales de tenant predefinidas. Los **administradores del sistema** pueden crear y publicar funciones globales de tenant adicionales.

### Administrador de organización

Una vez creada una organización, un **Administrador del sistema** puede asignar la función **Administrador de organización** a cualquier usuario de la organización. Un usuario con la función predefinida **Administrador de organización** puede utilizar la consola web de vCloud Director, el portal para tenants o vCloud OpenAPI para administrar usuarios y grupos en la organización, y asignarles funciones, incluida la función predefinida **Administrador de organización**. Otras organizaciones no pueden ver las funciones que un **administrador de organización** haya creado o modificado.

### Autor de catálogo

Los derechos asociados con la función **Autor de catálogo** predefinida permiten a los usuarios crear y publicar catálogos.

### Autor de vApp

Los derechos asociados a la función predefinida **Autor de vApp** permiten a un usuario usar catálogos y crear vApps.

### Usuario de vApp

Los derechos asociados a la función predefinida **Usuario de vApp** permiten a un usuario utilizar vApps existentes.

### Solo acceso a la consola

Los derechos asociados a la función predefinida **Solo acceso a la consola** permiten a un usuario ver el estado y las propiedades de máquinas virtuales, así como utilizar el sistema operativo invitado.

### Aplazar a proveedor de identidad

Los derechos asociados a la función predefinida **Aplazar a proveedor de identidad** se determinan en función de la información aportada por el proveedor de identidad OAuth o SAML del usuario. Para poder ser incluido cuando a un usuario o grupo se le asigna la función **Aplazar a proveedor de identidad**, el nombre de función o grupo suministrado por el proveedor de identidad debe coincidir exactamente, incluyendo mayúsculas y minúsculas, con un nombre de función o grupo definido en la organización.

- Si un proveedor de identidad OAuth define al usuario, a este se le asignan las funciones indicadas en la matriz de `roles` del token OAuth del usuario.

- Si un proveedor de identidad SAML define al usuario, a este se le asignan las funciones indicadas en el atributo SAML cuyo nombre aparece en el elemento `RoleAttributeName`, el cual se encuentra en el elemento `SamlAttributeMapping` de la instancia de `OrgFederationSettings` de la organización.

Si al usuario se le asigna la función **Aplazar a proveedor de identidad**, pero en la organización no hay disponible ningún nombre de función o grupo que coincida, el usuario podrá iniciar sesión en la organización, pero no tendrá ningún derecho. Si un proveedor de identidad asocia a un usuario con una función de nivel de sistema, como **Administrador del sistema**, ese usuario podrá iniciar sesión en la organización, pero no tendrá ningún derecho. Deberá asignar manualmente una función a esos usuarios.

A excepción de la función **Aplazar a proveedor de identidad**, todas las funciones predefinidas incluyen un conjunto de derechos predeterminados. Solo un **Administrador del sistema** puede modificar los derechos de una función predefinida. Si un **Administrador del sistema** modifica una función predefinida, los cambios se propagan a todas las instancias de esa función en el sistema.

## Derechos en funciones globales de tenant predefinidas

Diferentes derechos son comunes a varias funciones globales predefinidas. Estos derechos se conceden de forma predeterminada a todas las organizaciones nuevas y están disponibles para su uso en otras funciones que ha creado el **Administrador de organización**.

Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
Catálogo: Agregar una vApp desde mi nube	X	X	X		
Catálogo: Permitir publicaciones externas o suscripciones para los catálogos	X	X			
Catálogo: Cambiar propietario	X				
Catálogo: Crear o eliminar un catálogo	X	X			
Catálogo: Editar propiedades del catálogo	X	X			
Catálogo: Compartir un catálogo con otras organizaciones	X	X			
Catálogo: Compartir un catálogo con usuarios o grupos dentro de la organización actual	X	X			
Catálogo: Ver catálogos privados y compartidos dentro de la organización actual	X	X	X		
Catálogo: Ver catálogos compartidos de otras organizaciones	X				

**Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director (continuación)**

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
Elemento de catálogo: Agregar a mi nube	X	X	X	X	
Elemento de catálogo: Copiar o mover una plantilla de vApp o medio	X	X	X		
Elemento de catálogo: Crear o cargar una plantilla de vApp o medio	X	X			
Elemento de catálogo: Editar plantilla de vApp o medios	X	X			
Elemento de catálogo: Habilitar descarga de plantilla/medio de vApp	X	X			
Elemento de catálogo: Ver plantillas de vApp o medios	X	X	X	X	
Entidad personalizada: Ver todas las instancias de entidad personalizada de la organización	X				
Entidad personalizada: Ver instancia de entidad personalizada	X				
Disco: Cambiar propietario	X	X			
Disco: Crear disco	X	X	X		
Disco: Eliminar disco	X	X	X		
Disco: Editar propiedades de disco	X	X	X		
Disco: Ver propiedades de disco	X	X	X	X	
Firewall distribuido: Configurar reglas de firewall distribuido	X				
Firewall distribuido: Habilitar/deshabilitar firewall distribuido	X				
Firewall distribuido: Ver reglas de firewall distribuido	X				
Clúster de Edge: Ver clúster de Edge	X				
Clúster de Edge: Administrar clúster de Edge	X				
Puerta de enlace: Configurar servidor Syslog	X				
Puerta de enlace: Configurar el registro del sistema	X				

**Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director (continuación)**

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
Puerta de enlace: Convertir en puerta de enlace avanzada	X				
Puerta de enlace: Ver puerta de enlace	X				
Puerta de enlace: Habilitar enrutamiento distribuido	X				
Puerta de enlace: Importar puerta de enlace Edge	X				
Servicios de puerta de enlace: Configuración de enrutamiento de BGP					
Servicios de puerta de enlace: Configuración de DHCP	X				
Servicios de puerta de enlace: Configuración de firewall	X				
Servicios de puerta de enlace: Configuración de VPN de IPsec	X				
Servicios de puerta de enlace: Configuración de VPN de capa 2					
Servicios de puerta de enlace: Configuración de equilibrador de carga	X				
Servicios de puerta de enlace: Configuración de NAT	X				
Servicios de puerta de enlace: Configuración de enrutamiento de OSPF	X				
Servicios de puerta de enlace: Configuración de acceso remoto	X				
Servicios de puerta de enlace: Configuración de VPN de SSL	X				
Servicios de puerta de enlace: Configuración de enrutamiento estático	X				
Servicios de puerta de enlace: Solo vista de enrutamiento de BGP	X				
Servicios de puerta de enlace: Solo vista de DHCP	X				
Servicios de puerta de enlace: Solo vista de firewall	X				
Servicios de puerta de enlace: Solo vista de VPN de IPsec	X				

**Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director (continuación)**

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
Servicios de puerta de enlace: Solo vista de VPN de capa 2	X				
Servicios de puerta de enlace: Solo vista de equilibrador de carga	X				
Servicios de puerta de enlace: Solo vista de NAT	X				
Servicios de puerta de enlace: Solo vista de enrutamiento de OSPF	X				
Servicios de puerta de enlace: Solo vista de acceso remoto	X				
Servicios de puerta de enlace: Solo vista de VPN de SSL	X				
Servicios de puerta de enlace: Solo vista de enrutamiento estático	X				
General: Control de administrador	X				
General: Vista de administrador	X				
General: Enviar notificación	X				
Túnel híbrido: Adquirir ticket de control	X				
Túnel híbrido: Adquirir ticket de túnel desde la nube	X				
Túnel híbrido: Adquirir ticket de túnel a la nube	X				
Túnel híbrido: Crear túnel desde la nube	X				
Túnel híbrido: Crear túnel a la nube	X				
Túnel híbrido: Eliminar túnel desde la nube	X				
Túnel híbrido: Eliminar túnel a la nube	X				
Túnel híbrido: Actualizar etiqueta de endpoint del túnel desde la nube	X				
Túnel híbrido: Ver la configuración del servidor de túnel de nube	X				
Túnel híbrido: Ver túnel desde la nube	X				
Túnel híbrido: Ver túnel a la nube	X				

**Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director (continuación)**

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
Organización: Permitir acceso a todos los VDC de organización	X				
Organización: Editar lista de control de acceso de los VDC de organización	X				
Organización: Editar configuración de federación	X				
Organización: Editar política de concesiones	X				
Organización: Editar asociaciones de organización	X				
Organización: Editar propiedades de red de organización	X				
Organización: Editar configuración de OAuth de la organización	X				
Organización: Editar propiedades de la organización	X				
Organización: Editar política de contraseña	X				
Organización: Editar política de cuotas	X				
Organización: Editar configuración SMTP	X				
Organización: Importar implícitamente usuario/grupo de IdP mientras se edita ACL de VDC	X				
Organización: Ver lista de control de acceso de los VDC de organización	X				
Organización: Ver ACL del catálogo	X	X			
Organización: Ver redes de organización	X				
Organización: Ver organizaciones	X	X	X		
Organización: Ver ACL de la vApp	X	X	X	X	
VDC de organización: Editar nombre y descripción de VDC de la organización	X				
VDC de organización: Editar regla de afinidad de MV y MV	X	X	X		
VDC de organización: Editar propiedades ampliadas de VDC de organización	X				



**Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director (continuación)**

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
VDC de organización: Administrar firewall	X				
VDC de organización: Establecer política de almacenamiento predeterminada	X				
VDC de organización: Ver políticas de recursos informáticos para un VDC de organización	X	X	X	X	
VDC de organización: Ver propiedades ampliadas de VDC de organización	X				
Red de VDC de organización: Ver propiedades	X				
Red de organización VDC: Editar propiedades	X				
Red de organización VDC: Importar red	X				
VDC de organización: Ver VDC de organización	X				
Plantilla de VDC de organización: Crear instancias de las plantillas de VDC de organización	X				
Plantilla de VDC de organización: Ver plantillas de VDC	X				
Red del proveedor: Ver red del proveedor	X				
Red del proveedor: Crear/eliminar red del proveedor	X				
Función: Crear/actualizar/eliminar una función	X				
Biblioteca de servicios: Ver servicios que componen la biblioteca de servicios	X				
Usuario: Ver grupo o usuario	X				
Extensión de VCD: Ver información del complemento de portal para tenants	X	X	X	X	
Grupo de VDC: Ver grupo de VDC	X				
Grupo de VDC: Configurar grupo de VDC	X				
Supervisión de MV: Ver métricas históricas para la organización	X				
Supervisión de MV: Ver métricas históricas para el VDC de organización	X				

**Tabla 14-1. Derechos incluidos en las funciones de tenant globales de vCloud Director (continuación)**

Nombre del derecho	Administrador de organización	Autor de catálogo	Autor de vApp	Usuario de vApp	Solo acceso a la consola
vApp: Obtener acceso a la consola de MV	X	X	X	X	X
vApp: Permitir el dominio de asignación de metadatos en vCenter Server	X	X	X		
vApp: Cambiar propietario	X				
vApp: Cambiar propietario de la plantilla de vApp	X	X			
vApp: Copiar una vApp	X	X	X	X	
vApp: Crear o volver a configurar vApp	X	X	X		
vApp: Crear, revertir o quitar una instantánea	X	X	X	X	
vApp: Eliminar una vApp	X	X	X	X	
vApp: Descargar una vApp	X	X	X		
vApp: Editar/ver las opciones de inicio de máquinas virtuales	X	X	X		
vApp: Editar CPU de MV	X	X	X		
vApp: Editar disco duro de MV	X	X	X		
vApp: Editar memoria de MV	X	X	X		
vApp: Editar red de MV	X	X	X	X	
vApp: Editar propiedades de MV	X	X	X	X	
vApp: Editar propiedades de vApp	X	X	X	X	
vApp: Editar política de recursos informáticos de la máquina virtual	X	X	X		
vApp: Administrar configuración de contraseña de MV	X	X	X	X	X
vApp: Compartir una vApp	X	X	X	X	
vApp: Iniciar, detener, suspender o restablecer una vApp	X	X	X	X	
vApp: Cargar una vApp	X	X	X		
vApp: Ver métricas de MV	X		X	X	

Para obtener información sobre los nuevos derechos que incluye vCloud Director 9.7, consulte [#unique\\_269](#).


## Crear una función de tenant personalizada

Los administradores de organización pueden utilizar el portal para tenants para crear objetos de función de tenant personalizada en las organizaciones que administran.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Funciones**.  
Se muestra la lista de funciones.
- 3 Haga clic en **Agregar**.
- 4 Escriba un nombre y, si lo desea, una descripción de la función.
- 5 Expanda los derechos de la función y selecciónelos.

Los derechos se agrupan en categorías y subcategorías que permiten ver o administrar objetos.

Opción	Descripción
<b>Control de acceso</b>	Derechos que controlan el acceso para ver y administrar determinados objetos.
<b>Administración</b>	Derechos que controlan el acceso administrativo.
<b>Proceso</b>	Derechos que controlan el acceso y la administración de los centros de datos virtuales de organización y de proveedor, las vApps, las plantillas de centros de datos virtuales de organización, los grupos de máquinas virtuales y la supervisión de máquinas virtuales.
<b>Extensiones</b>	Derechos que controlan el acceso a complementos y extensiones de vCloud Director adicionales.
<b>Infraestructura</b>	Derechos que controlan el acceso y la administración de los objetos de infraestructura, como los almacenes de datos, los discos, los hosts, etc.
<b>Bibliotecas</b>	Derechos que controlan el acceso y la administración de los catálogos y sus elementos.
<b>Red</b>	Derechos que controlan el acceso y la administración de la configuración de red.

- 6 Haga clic en **Guardar**.

## Editar una función de tenant personalizada


Los administradores de organización pueden utilizar el portal para tenants con el fin de editar objetos de funciones de tenant personalizadas en las organizaciones que administran.

Como administrador de organización, solo puede ver las funciones de tenant globales que un administrador del sistema ha publicado en su organización. No puede editar las funciones de tenant globales.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Funciones**.  
Se muestra la lista de funciones.
- 3 Haga clic en el botón de radio junto a la función que desea editar y haga clic en **Editar**.
- 4 Modifique la configuración de la función según sea necesario.
  - a Cambie el nombre y, si lo desea, la descripción de la función.
  - b Edite los derechos de la función.
- 5 Haga clic en **Guardar**.


## Eliminar una función

Los administradores de organización pueden utilizar el portal para tenants para eliminar objetos de función en las organizaciones que administran.

#### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, debajo de **Control de acceso**, haga clic en **Funciones**.  
Se muestra la lista de funciones.
- 3 Haga clic en el botón de radio junto a la función que desea eliminar y haga clic en **Eliminar**.
- 4 Haga clic en **Aceptar** para confirmar que desea eliminar la función.

# Habilitar el uso de un proveedor de identidad SAML en la organización

# 15

Habilite en la organización el uso de un proveedor de identidad de Lenguaje de marcado de aserción de seguridad (SAML), también denominado inicio de sesión único, para importar de él usuarios y grupos y permitir a los usuarios importados iniciar sesión en la organización con las credenciales establecidas en dicho proveedor.

Cuando importa los usuarios y grupos, el sistema extrae una lista de atributos del token SAML, si está disponible, y los usa para interpretar la información correspondiente sobre el usuario que intenta iniciar sesión.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

El atributo funciones se puede configurar.

Se necesita información relacionada con el grupo si un usuario no se ha importado directamente, pero se espera que dicho usuario pueda iniciar sesión debido a que pertenece a grupos importados. Un usuario puede pertenecer a varios grupos y, por tanto, puede tener varias funciones durante una sesión.

Si se asigna la función **Aplazar a proveedor de identidad** a un grupo o un usuario importados, las funciones se asignan con base en la información recopilada a partir del atributo Funciones del token. Si se utiliza un atributo diferente, este nombre de atributo solo se puede configurar mediante el uso de la API, y únicamente el atributo Funciones es configurable. Si se utiliza la función **Aplazar a proveedor de identidad**, pero no se puede extraer información de funciones, el usuario puede iniciar sesión, pero no tiene derechos para realizar actividades.


## Requisitos previos

- Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.
- Compruebe que tiene acceso a un proveedor de identidad compatible con SAML 2.0.

- Compruebe que recibe los metadatos necesarios del proveedor de identidad SAML. Debe importar los metadatos a vCloud Director de forma manual o como un archivo XML. Los metadatos deben incluir la siguiente información:
  - La ubicación del servicio de inicio de sesión único
  - La ubicación del servicio de cierre de sesión único
  - La ubicación del certificado X.509 del servicio

Para obtener información sobre la configuración y la adquisición de metadatos de un proveedor de identidad SAML, consulte la documentación relativa a su proveedor de identidad SAML.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Proveedores de identidad**, haga clic en **SAML**.
- 3 Haga clic en **Editar**.
- 4 En la pestaña **Proveedor de servicios**, introduzca el ID de entidad.

El ID de entidad es el identificador único de su organización para el proveedor de identidades. Puede utilizar el nombre de la organización, o cualquier otra cadena que cumpla los requisitos del proveedor de identidad SAML.

---

**Importante** Una vez que se especifica un ID de entidad, no puede eliminarlo. Para cambiar el ID de entidad, debe realizar una reconfiguración completa de SAML para su organización. Para obtener más información sobre los ID de entidad, consulte el documento relacionado con [las aserciones y los protocolos del Lenguaje de marcado de aserción de seguridad \(SAML\) 2.0 de OASIS](#).

---

- 5 Haga clic en el vínculo **Metadatos** para descargar los metadatos de SAML de su organización. Los metadatos descargados deben proporcionarse como están al proveedor de identidades.
- 6 Revise la fecha de caducidad del certificado y, si lo desea, haga clic en Volver a generar para volver a generar el certificado utilizado para firmar los mensajes de la federación. El certificado se incluye en los metadatos de SAML y se utiliza para el cifrado y la firma. El cifrado o la firma pueden ser necesarios dependiendo de cómo se establezca la confianza entre su organización y el proveedor de identidad SAML.
- 7 En la pestaña **Proveedor de identidad**, habilite el botón de alternancia **Utilizar proveedor de identidad SAML**.
- 8 Copie y pegue los metadatos SAML que recibió del proveedor de identidad en el cuadro de texto o haga clic en **Cargar** para buscar y cargar los metadatos desde un archivo XML.
- 9 Haga clic en **Guardar**.

### Pasos siguientes

- Configure el proveedor SAML con los metadatos de vCloud Director. Consulte la documentación relativa al proveedor de identidad SAML y la *Guía de instalación y actualización de vCloud Director*.
- Importe usuarios y grupos de su proveedor de identidad SAML. Consulte [Capítulo 14 Administración de usuarios, grupos y funciones](#).

# Administrar la organización

# 16

Como **administrador de organización**, puede modificar varias opciones de configuración en la organización, como: nombre de la organización, configuración de correo electrónico, configuración de dominio, metadatos, políticas, etc.

Este capítulo incluye los siguientes temas:

- Editar el nombre y la descripción de la organización
- Modificar la configuración de correo electrónico
- Probar la configuración SMTP
- Modificar la configuración de dominio para las máquinas virtuales de la organización
- Trabajar con varios sitios
- Configurar y administrar implementaciones multisitio
- Entender las concesiones
- Modificar las políticas de concesión de la vApp y la plantilla de vApp dentro de la organización
- Modificar las cuotas predeterminadas para las máquinas virtuales en la organización
- Modificar las políticas de cuenta de usuario y contraseña en la organización


## Editar el nombre y la descripción de la organización

Puede editar el nombre completo y la descripción de la organización.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **General**.

Se mostrará la lista de los ajustes generales, como el nombre de la organización, la URL predeterminada, el nombre completo y la descripción.



- 3 Para modificar el nombre completo y la descripción de la organización, haga clic en **Editar**.
- 4 Aplique los cambios necesarios y haga clic en **Guardar**.

## Modificar la configuración de correo electrónico


Puede revisar y modificar la configuración de correo electrónico predeterminada que se estableció cuando el administrador del sistema creó la organización.

vCloud Director envía alertas por correo electrónico cuando debe comunicar información importante (por ejemplo, cuando un almacén de datos se está quedando sin espacio). De forma predeterminada, una organización envía alertas de correo electrónico a los administradores del sistema o a una lista de direcciones de correo electrónico especificadas en el nivel del sistema mediante un servidor SMTP definido en dicho nivel. Puede modificar la configuración de correo electrónico en el nivel de organización si desea que vCloud Director envíe alertas para esa organización a un conjunto de direcciones de correo electrónico distinto al especificado en el nivel del sistema o si desea que la organización utilice un servidor SMTP para enviar alertas diferente del especificado en el nivel del sistema.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **Correo electrónico**.  
Aparecerá la configuración de correo electrónico de la organización.
- 3 Haga clic en **Editar**.
- 4 Edite la configuración del servidor SMTP en la pestaña **Servidor SMTP**.
  - a Seleccione si desea utilizar un servidor SMTP personalizado o el predeterminado.
  - b Si decide utilizar un servidor SMTP personalizado, escriba la dirección IP o el nombre de host de DNS del servidor SMTP en el cuadro de texto **Nombre del servidor SMTP**.
  - c (opcional) Introduzca el puerto del servidor SMTP.
  - d (opcional) Seleccione si desea solicitar la autenticación y escriba un nombre de usuario y una contraseña.
- 5 Para editar la configuración de notificaciones, haga clic en la pestaña **Configuración de notificación**.
  - a Utilice la configuración de notificaciones personalizada.
  - b Introduzca la dirección de correo electrónico que aparece como remitente de los correos electrónicos de la organización.

- c (opcional) Introduzca el texto que se usará como prefijo del asunto del correo electrónico.
- d (opcional) Seleccione si desea enviar notificaciones a todos los administradores de la organización o a direcciones de correo electrónico específicas.
- e (opcional) Si decide enviar notificaciones a direcciones de correo electrónico específicas, introduzca las direcciones separadas por comas.

6 Haga clic en **Guardar**.


## Probar la configuración SMTP

Después de modificar la configuración de correo electrónico de la organización, puede probar la configuración de SMTP.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **Correo electrónico**.  
Aparecerá la configuración de correo electrónico de la organización.
- 3 Haga clic en **Probar**.
- 4 Introduzca una dirección de correo electrónico de destino y la contraseña del servidor SMTP para probar la configuración de SMTP y haga clic en el botón **Probar**.


## Modificar la configuración de dominio para las máquinas virtuales de la organización

Puede establecer un dominio predeterminado de Windows al que se puedan unir las máquinas virtuales creadas en su organización. Las máquinas virtuales podrán unirse siempre a aquellos dominios para los que tengan credenciales, independientemente de si especifica un dominio predeterminado.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **Personalización de invitado**.

3 Habilite la unión de dominio para las máquinas virtuales de la organización.

4 Introduzca el nombre de dominio, el nombre de usuario y la contraseña.

Las credenciales que introduzca se aplican a un usuario de dominio convencional, no a un administrador de dominio.

5 (opcional) Introduzca una unidad organizativa de cuenta.

6 Haga clic en **Guardar**.

## Trabajar con varios sitios

La función multisitio de vCloud Director permite a un proveedor de servicios o a un tenant de varias instalaciones (grupos de servidores) de vCloud Director distribuidas geográficamente administrar y supervisar dichas instalaciones y sus organizaciones como entidades únicas.

El portal para tenants de vCloud Director ofrece a los **administradores de organización** una manera de asociar organizaciones en sitios asociados.

Para obtener más información sobre las asociaciones de sitios, consulte la *Guía del administrador de vCloud Director*.

## Configurar y administrar implementaciones multisitio

Después de que un **administrador del sistema** haya asociado dos sitios, los **administradores de organización** de cualquier sitio miembro pueden empezar a asociar sus organizaciones.

Para crear una asociación entre dos organizaciones (denominadas Org-A y Org-B en este documento), debe ser un **administrador de organización** de ambas organizaciones, de modo que pueda iniciar sesión en cada organización, recuperar los datos de asociación local y enviar los datos recuperados a la otra organización.

---

**Importante** El proceso de asociación de dos organizaciones se puede desglosar lógicamente en dos operaciones de emparejamiento complementarias. La primera operación (en este ejemplo) empareja Org-A en el sitio A con Org-B en el sitio B. Posteriormente, debe emparejar Org-B en el sitio B con Org-A en el sitio A. La asociación estará incompleta si no se realizan ambos emparejamientos.

---

### Requisitos previos

- Los sitios ocupados por las organizaciones deben estar asociados.
- Debe ser un **administrador del sistema** en ambos sitios o un **administrador de organización** en ambas organizaciones.

## Procedimiento

- 1 Inicie sesión en el portal para tenants de vCloud Director de Org-A en el sitio A para recuperar los datos de asociación local.
  - a Haga clic en **Administración**.
  - b En **Configuración**, haga clic en **Multisitio**.
  - c Para descargar los datos en formato XML, haga clic en **Exportar datos de asociación local**.

El navegador guarda los datos en un archivo en la carpeta Descargas.
- 2 Inicie sesión en el portal para tenants de vCloud Director de Org-B en el sitio B para enviar los datos de asociación local de Org-A en el sitio A.
  - a Haga clic en **Administración**.
  - b En **Configuración**, haga clic en **Multisitio**.
  - c Haga clic en **Crear nueva asociación de organización**.

Envíe los datos de asociación que ha descargado en el [paso 1](#) a Org-B haciendo clic en la flecha de carga situada debajo del cuadro de texto **XML de asociación nueva** y seleccione los datos de asociación local que ha descargado en el [paso 1](#).
  - d Haga clic en **Siguiente** para comprobar y enviar los datos.

El sistema empareja Org-A en el sitio A con Org-B en el sitio B.
  - e Haga clic en **Finalizar** para ver la organización asociada.
  - f Para ver los detalles de la organización asociada o eliminar la asociación, haga clic en la tarjeta **Nombre de organización**.
- 3 Para completar la asociación, repita los pasos 1 y 2 para recuperar los datos de asociación local de Org-B y enviarlos a Org-A.

## Entender las concesiones

La creación de una organización implica la especificación de concesiones. Las concesiones proporcionan un nivel de control sobre el almacenamiento y los recursos informáticos de la organización mediante la especificación de un límite máximo de tiempo de ejecución de las vApps, así como de almacenamiento de las vApps y las plantillas de vApp.

El objetivo de una concesión de tiempo de ejecución es evitar que las vApps inactivas consuman recursos informáticos. Por ejemplo, si un usuario inicia una vApp y se va de vacaciones sin detenerla, la vApp continuará consumiendo recursos.

Una concesión de tiempo de ejecución empieza cuando un usuario inicia una vApp. Cuando una concesión de tiempo de ejecución caduca, vCloud Director detiene la vApp.

El objetivo de una concesión de almacenamiento es evitar que las vApp no utilizadas y las plantillas de vApp consuman recursos de almacenamiento. Una concesión de almacenamiento de vApp empieza cuando un usuario detiene la vApp. La concesión de almacenamiento no afecta a las vApps en ejecución. Una concesión de almacenamiento de plantillas vApp empieza cuando un usuario agrega la plantilla vApp, agrega una plantilla vApp a un espacio de trabajo, descarga, copia o mueve la plantilla de vApp.

Cuando una concesión de almacenamiento caduca, vCloud Director marca la vApp o la plantilla de vApp como caducada, o elimina la vApp o la plantilla de vApp, en función de la política de organización que haya establecido.


## Modificar las políticas de concesión de la vApp y la plantilla de vApp dentro de la organización

Puede revisar y modificar las directivas predeterminadas que el administrador del sistema estableció al crear la organización.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **Políticas**.

Puede ver las políticas predeterminadas que configuró el administrador del sistema.

- 3 Haga clic en **Editar**.
- 4 Edite las concesiones de vApp.

Las concesiones de vApp proporcionan un nivel de control sobre el almacenamiento y los recursos informáticos de la organización mediante la especificación de un límite máximo de tiempo de ejecución y de almacenamiento de las vApps. De igual modo, puede especificar lo que sucede con las vApps cuando caduca la concesión de almacenamiento.

- a Para definir la cantidad de tiempo durante la que se pueden ejecutar las vApps antes de detenerse automáticamente, introduzca la concesión de tiempo de ejecución máxima.
- b Seleccione una acción de caducidad de tiempo de ejecución, como el apagado o la suspensión.
- c Para definir la cantidad de tiempo durante la que permanecen disponibles las vApps detenidas antes de limpiarse automáticamente, introduzca la concesión de almacenamiento máxima.
- d Seleccione una acción de limpieza de almacenamiento, como la eliminación permanente de las vApps o la transferencia de estas a los elementos caducados.

## 5 Edite la concesión de plantillas de vApp.

Las concesiones de plantillas de vApp proporcionan un nivel de control sobre el almacenamiento y los recursos informáticos de la organización mediante la especificación de la cantidad de tiempo máxima que se pueden almacenar las plantillas de vApp. De igual modo, puede especificar lo que sucede con las plantillas de vApp cuando caduca la concesión de almacenamiento.

- a Para definir la cantidad de tiempo durante la que permanecen disponibles las plantillas de vApp antes de limpiarse automáticamente, introduzca la concesión de almacenamiento máxima.
- b Seleccione una acción de limpieza de almacenamiento, como la eliminación permanente de las plantillas de vApp o la transferencia de estas a los elementos caducados.

## 6 Haga clic en **Aceptar**.

# Modificar las cuotas predeterminadas para las máquinas virtuales en la organización


Puede revisar y modificar las políticas de cuota predeterminadas que el administrador del sistema estableció al crear la organización.

Las cuotas determinan el número de máquinas virtuales que cada usuario de la organización puede almacenar y encender en los centros de datos virtuales de la organización. Las cuotas que especifique actuarán como las predeterminadas para todos los nuevos usuarios agregados a la organización. Las cuotas establecidas a nivel de usuario prevalecen sobre las cuotas establecidas a nivel de organización.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **Políticas**.  
Puede ver las políticas predeterminadas que configuró el administrador del sistema.
- 3 Haga clic en **Editar**.
- 4 Elija entre un número ilimitado de máquinas virtuales y un número que especifique.
- 5 Elija entre un número ilimitado de máquinas virtuales encendidas y un número que especifique.
- 6 Haga clic en **Aceptar**.

## Modificar las políticas de cuenta de usuario y contraseña en la organización


Puede revisar y modificar las políticas de cuenta de usuario y contraseña predeterminadas que el administrador del sistema estableció al crear la organización.

Las políticas de cuenta de usuario y contraseña definen el comportamiento de vCloud Director cuando un usuario introduce una contraseña no válida.

### Requisitos previos

Esta operación requiere los derechos incluidos en la función **Administrador de organización** predefinida o un conjunto equivalente de derechos.

### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En **Configuración**, haga clic en **Políticas**.  
Puede ver las políticas predeterminadas que configuró el administrador del sistema.
- 3 Haga clic en **Editar**.
- 4 Habilitar el bloqueo de la cuenta de usuario después de una cantidad de intentos no válidos de inicio de sesión.
- 5 Introduzca el número de intentos de inicio de sesión no válidos antes de que se bloquee la cuenta de usuario.
- 6 Introduzca el intervalo de tiempo en minutos durante el cual el usuario con una cuenta bloqueada no puede volver a iniciar sesión.
- 7 Haga clic en **Aceptar**.

# Trabajar con Biblioteca de servicios

# 17

Los elementos de Biblioteca de servicios de vCloud Director son flujos de trabajo de vRealize Orchestrator que amplían las capacidades de administración de la nube y permiten a los administradores de los proveedores o los tenants supervisar y manipular diferentes servicios.

Este capítulo incluye los siguientes temas:

- [Buscar un servicio](#)
- [Ejecutar un servicio](#)

## Buscar un servicio

En la página **Biblioteca de servicios** del portal para tenants de vCloud Director se muestra el conjunto de flujos de trabajo de vRealize Orchestrator que se han importado en vCloud Director y se han publicado en la organización.

### Requisitos previos

Esta operación requiere que los derechos de la biblioteca de servicios se incluyan en la función de usuario predefinida.

### Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Biblioteca de servicios**.

La lista de servicios se muestra en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre del servicio y una etiqueta que se corresponde con la categoría del servicio donde se importa vRealize Orchestrator.

- 2 En el cuadro de texto **Buscar** que se encuentra en la parte superior de la página, introduzca la primera palabra del nombre del servicio o el nombre de la categoría a la que pertenece el servicio.

a Determine si desea buscar en los nombres del servicio o en las categorías.

Los resultados de la búsqueda se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético.



## Ejecutar un servicio

Los servicios se pueden ejecutar desde la página Biblioteca de servicios del portal para tenants de vCloud Director.

### Requisitos previos

Esta operación requiere que los derechos de la biblioteca de servicios se incluyan en la función de usuario predefinida.

### Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Biblioteca de servicios**.

La lista de servicios se muestra en una vista de tarjeta con 12 elementos por página, organizados por nombre en orden alfabético. Cada tarjeta muestra el nombre del servicio y una etiqueta que se corresponde con la categoría del servicio donde se importa vRealize Orchestrator.

- 2 Busque el servicio que desea ejecutar.
- 3 Haga clic en **Ejecutar** en la tarjeta del servicio.

Se abrirá un cuadro de diálogo nuevo. Debe introducir valores para los parámetros de entrada necesarios del servicio.

- 4 Haga clic en **Finalizar** para confirmar la ejecución del servicio.

### Pasos siguientes

Puede supervisar el estado de la ejecución en la vista **Tareas recientes**. Para obtener más información, consulte [Ver tareas](#).

# Trabajar con definiciones de entidad personalizada

# 18

Las definiciones de entidad personalizada de vCloud Director son tipos de objeto enlazados a tipos de objeto de vRealize Orchestrator. Los usuarios en una organización de vCloud Director pueden poseer, administrar y cambiar dichos tipos en función de sus necesidades. Mediante la ejecución de los servicios, los usuarios de la organización pueden crear instancias de las entidades personalizadas y aplicar acciones a las instancias de los objetos.

Este capítulo incluye los siguientes temas:

- [Buscar una entidad personalizada](#)
- [Editar una definición de entidad personalizada](#)
- [Agregar una definición de entidad personalizada](#)
- [Instancias de entidades personalizadas](#)
- [Asociar una acción a una entidad personalizada](#)
- [Anular la asociación de una acción de una entidad personalizada](#)
- [Publicar una entidad personalizada](#)
- [Eliminar una entidad personalizada](#)

## Buscar una entidad personalizada

Puede buscar esas entidades personalizadas que se han publicado en la organización.

### Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

## Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En el cuadro de texto **Buscar** de la parte superior de la página, introduzca una palabra o un carácter del nombre de la entidad que desea buscar.

Los resultados de la búsqueda se muestran en una vista de tarjetas con doce elementos por página organizados por nombre y en orden alfabético.

## Editar una definición de entidad personalizada

Puede modificar el nombre y la descripción de una entidad personalizada. No es posible modificar el tipo de la entidad o el tipo de objeto de vRealize Orchestrator, al cual esté enlazada la entidad. Son las propiedades predeterminadas de la entidad personalizada. Si desea modificar cualquiera de las propiedades predeterminadas, debe eliminar la definición de entidad personalizada y volver a crearla.

### Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

## Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Editar**.

Se abrirá un cuadro de diálogo nuevo.

- 3 Modifique el nombre o la descripción de la definición de entidad personalizada.
- 4 Haga clic en **Aceptar** para confirmar el cambio.

## Agregar una definición de entidad personalizada

Puede crear una entidad personalizada y asignarla a un tipo de objeto de vRealize Orchestrator existente.

### Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

### Procedimiento


- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 Haga clic en el icono  para agregar una nueva entidad personalizada.

Se abrirá un cuadro de diálogo nuevo.

- 3 Siga los pasos del asistente de **definición de entidad personalizada**.

Paso	
Nombre y descripción	Introduzca un nombre y, si lo desea, una descripción para la nueva entidad. Introduzca un nombre para el tipo de entidad (por ejemplo, <code>sshHost</code> ).
VRO	En el menú desplegable, seleccione la instancia de vRealize Orchestrator que va a utilizar para asignar la definición de entidad personalizada.  <b>Nota</b> Si hay más de un servidor de vRealize Orchestrator, debe crear una definición de entidad personalizada para cada uno de ellos de manera independiente.
Tipo	Haga clic en el icono de la lista de vistas (  ) para desplazarse por los tipos de objeto de vRealize Orchestrator disponibles agrupados por complementos. Por ejemplo, <b>SSH &gt; Host</b> . Si conoce el nombre del tipo, puede introducirlo directamente en el cuadro de texto. Por ejemplo, <code>SSH:Host</code> .
Revisar	Revise los detalles que ha especificado y haga clic en <b>Listo</b> para completar la creación.

### Resultados

La nueva definición de entidad personalizada aparecerá en la vista de tarjetas.

## Instancias de entidades personalizadas

La ejecución de un flujo de trabajo de vRealize Orchestrator con un parámetro de entrada que sea un tipo de objeto que ya esté definido como una definición de entidad personalizada en vCloud Director muestra el parámetro de salida como una instancia de una entidad personalizada.

## Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.


## Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, haga clic en **Instancias**.

Las instancias disponibles se mostrarán en una vista de cuadrícula.

- 3 Haga clic en la barra de listas () que se encuentra a la izquierda de cada entidad para mostrar los flujos de trabajo asociados.

Al hacer clic en un flujo de trabajo, se iniciará una ejecución de flujo de trabajo que tomará la instancia de la entidad como un parámetro de entrada.

## Asociar una acción a una entidad personalizada

Mediante la asociación de una acción a una definición de entidad personalizada, puede ejecutar un conjunto de flujos de trabajo de vRealize Orchestrator en las instancias de una entidad personalizada específica.

## Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

## Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Asociar acción**.

Se abrirá un cuadro de diálogo nuevo.

### 3 Siga los pasos del asistente de **asociación de una entidad personalizada a un flujo de trabajo de VRO**.

Paso	Detalles
Seleccionar flujo de trabajo de VRO	Seleccione uno de los flujos de trabajo enumerados. Estos son los flujos de trabajo disponibles en la página <b>Biblioteca de servicios</b> .
Seleccionar parámetro de entrada de flujo de trabajo	Seleccione un parámetro de entrada disponible de la lista. El tipo de flujo de trabajo de vRealize Orchestrator se asocia al tipo de definición de entidad personalizada.
Revisar asociación	Revise los detalles que ha especificado y haga clic en <b>Listo</b> para completar la asociación.

#### Ejemplo

Por ejemplo, si dispone de una entidad personalizada del tipo `SSH:Host`, puede asociarla al flujo de trabajo `Add a Root Folder to SSH Host` seleccionando el parámetro de entrada `sshHost`, el cual coincide con el tipo de la entidad personalizada.

## Anular la asociación de una acción de una entidad personalizada

Puede quitar un flujo de trabajo de vRealize Orchestrator de la lista de acciones asociadas.

#### Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

#### Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Anular asociación de acción**.

Se abrirá un cuadro de diálogo nuevo.

- 3 Seleccione el flujo de trabajo que desea quitar y haga clic en **Anular asociación de acción**.

El flujo de trabajo de vRealize Orchestrator dejará de estar asociado a la entidad personalizada.

## Publicar una entidad personalizada

Debe publicar una entidad personalizada para que los usuarios de otros tenants u otros proveedores de servicios puedan ejecutar flujos de trabajo usando las instancias de la entidad personalizada como parámetros de entrada.

### Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

### Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Publicar**.

Se abrirá un cuadro de diálogo nuevo.

- 3 Determine si desea publicar la definición de entidad personalizada en los proveedores de servicios, en todos los tenants, o solo en los tenants seleccionados.

- 4 Haga clic en **Guardar** para confirmar el cambio.

La definición de entidad personalizada estará disponible para las partes seleccionadas.

## Eliminar una entidad personalizada

Puede eliminar una definición de entidad personalizada si la entidad personalizada ya no se usa, si esta se ha configurado de forma incorrecta o si desea asignar el tipo de vRealize Orchestrator a otra entidad personalizada.

### Requisitos previos

Esta operación requiere que los derechos de la entidad personalizada se incluyan en la función de usuario predefinida.

## Procedimiento

- 1 Desde el menú principal () , seleccione **Bibliotecas** y, en **Servicios**, seleccione **Definiciones de entidades personalizadas**.

La lista de entidades personalizadas se muestra en una vista de tarjetas con 12 elementos por página organizados por nombre y en orden alfabético. Cada tarjeta muestra el nombre de la entidad personalizada, el tipo de vRealize Orchestrator al que se ha asignado la entidad, el tipo de la entidad y una descripción, si hay una disponible.

- 2 En la tarjeta de la entidad personalizada seleccionada, elija **Acciones > Eliminar**.
- 3 Confirme la eliminación.

La entidad personalizada se eliminará de la vista de tarjetas.